User's Manual

AudioCodes One Voice Operations Center (OVOC)

One Voice Operations Center

Version 8.0



audiocodes

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: March-29-2021

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

Document Name
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
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
91048	Initial document release for 7.8. Reports. FlexPool mode. UMP Quick Connect. Advanced Quality Package teaser. Mediant 500Li. "Advanced Quality Package license missing". SSO limitation. MasterScope status in License Configuration page.
91049	Fixes

LTRT	Description
92000	Fixes
92001	Updated for 7.8.1000. Login as Azure op w MFA. Azure AD dB. Tenant Endpoints Group User Group Name. Authorization Level Settings. Privacy Mode. Tenant Details. Adding a Group. Endpoints Groups filter. Endpoints Groups. Report Results (fixes).
92002	Tenant Details: Multitenancy tab > Operators tab. 'Disable SNMP'. Server Status page - cluster mode. Server Status-Info-Ports status. Update firmware (.cmp) on MC (Media Component) in a Media Cluster (Mediant Cloud Edition (CE) software session border controller (SBC). CentOS version 6 or 8. PM Profile-REST. PM Profile-REST filter. cmp File Details in Software Manager. Users URI Regexp. Links not displayed if >1000 and src/dest outside page.
92003	Icon statuses descriptions corrected.
92004	LDAP Operator Authentication 'Filter'. Future Suspension of operator.
92005	OVOC look-and-feel changed: Colors | Dashboard | Call Details. New screen-shots replaced obsolete. Topology Groups page. Endpoint Groups page. Teams calls (New device|Configuration| Calls| Statistics | Reports). 'Description' for alarms from OVOC server. Filter pages by SNMP API vs. REST parameters. MasterScope>Data Layer Manager.

Table of Contents

1 Introduction 1
About the One Voice Operations Center 1
Benefits 2
Intended Audience 3
Network Architecture 3
ITSP Multi-Tenancy Architecture 3
Enterprise Multi-Tenancy Architecture 4
Non Multi-Tenancy Architecture 4
Elements in Multi-Tenancy Architecture 5
ITSP Customer Multi-Tenant Architecture 6
2 Getting Started 8
Logging in 8
Getting Acquainted with the Dashboard 9
Getting Acquainted with the Network Topology Page 14
Hovering Over a Cluster to Display Information 30
Hovering Over a Device to Display Information 32
Hovering over a Link to Display Information 33
Returning to 'Home' Page by Clicking the AudioCodes Logo 33
Getting Acquainted with the Network Map Page 33
Configuring Operator Authentication 38
Configuring Operator Authentication Centrally using an LDAP Server 39
Configuring Operator Authentication Centrally with a RADIUS Server 42
Viewing Operator Authentication in the Application Information Window 43
Testing Connectivity with the LDAP / RADIUS Server 44
Configuring Operator Authentication Centrally with Azure Active Directory 44
Logging in as an Azure User with Multi Factor Authentication 47
Configuring Operator Authentication Locally, in the OVOC 50
Adding an Operator 52
How Multi Tenancy Impacts Operator Capabilities 53
Adding a 'System' Operator 53
Editing a 'System' Operator 58
Deleting a 'System' Operator 58
Deleting Multiple Operators 58
Suspending a 'System' Operator 58
Releasing a Suspended 'System' Operator 58
Forcing a Password Change 59
Forcing an Operator Logout 59
Adding a 'Tenant' Operator 60
Editing a 'Tenant' Operator 65
Deleting a 'Tenant' Operator 65
Deleting Multiple Operators 66
Suspending a 'Tenant' Operator 66

Releasing a Suspended 'Tenant' Operator 66
Forcing a Password Change 66
Forcing an Operator Logout 67
3 Configuring Global (System) Settings 68
Administration tab 70
Loading the OVOC Server License 70
Making Sure your License Provides the Capabilities you Ordered 71
Allocating Licenses to Tenants 72
Defining # of Administrator-Defined Reports Produced at System Level 74
Authenticating Operators 75
Determining OVOC Server Status 75
Securing Connections with FQDN or IP Address 76
Providing a Description to be Forwarded in Alarm Info 77
Configuring Privacy Mode, Concealing Users Calls Details 78
Uploading a Global Logo to Display in Report Results 78
Customizing Call Storage 79
Customizing Maximum Storage Period 84
Viewing Calls Status 86
Configuration tab 88
Configuring Templates 88
SNMP Connectivity 88
HTTP Connectivity 91
QoE Thresholds 91
QoE Status and Alarms 93
Configuring Alarms Settings 95
Adding Configuration Files to the OVOC's Software Manager 98
Adding the ini File 100
Adding a cmp File 101
Adding a cli File 104
Adding Auxiliary Files 104
Connecting Directly to External Applications 106
Device Manager 106
ARM 107
Data Layer Manager 108
Enabling Automatic Device Backup Periodically 110
Tasks tab 110
Displaying the Status of Tasks Currently Under Execution 111
4 Defining your Network Topology 113
Adding a Tenant 113
Editing a Tenant - Defining a Logo 122
Defining a Tenant Logo - Example 123
Adding a Region 129
Adding AudioCodes Devices 130
Adding AudioCodes Devices Automatically 130

Adding AudioCodes Devices Manually 135
Enabling Initial Connection Provisioning 143
Before Enabling the Feature 144
Enabling the Feature 145
Making Sure First Time Provisioning was Successful 147
Adding a Generic Device Manually 150
Adding a Microsoft Teams Device Manually 151
Adding a Microsoft Skype for Business Device Manually 153
Backing up a Device's Configuration using Backup Manager 157
Manually Backing up a Device's Configuration 157
Saving the Last Backed-up Configuration to your PC 158
Restoring the Last Backed-up Configuration to the Device 159
Adding Links 159
Adding Sites 164
Managing Endpoints 165
Dynamic Allocation of Endpoint Licenses 165
Configuring Endpoints 166
Monitoring Endpoints Status 167
Removing Endpoints from QoE Support 167
Adding an Endpoints Group 168
Adding a Topology Group 172
5 Managing SBC Licenses 174
Adding an SBC to the Floating License 174
Performing Floating License Actions 179
Unmanage 179
Update 180
Reset 180
Register 181
Configuring OVOC-Floating License Service Communications 181
Cloud Mode 182
Configuring Cloud Mode 183
Viewing Floating License Summaries 185
Saving a Usage Data Report to your PC 188
FlexPool Mode 189
Configuring an Alarm Threshold Percentage for FlexPool Mode 189
Configuring SBC Priority - Which to Take out of Service First 189
Determining License Status from Alarms 190
Determining License Status from the Network Summary 191
Migrating from Cloud Mode to FlexPool Mode 194
Fixed License Pool 195
Performing License Pool Actions 198
Applying a License to a Device from the Pool 198
Saving Fixed License Pool Data to CSV File 198
Before Performing 'Manage Device' / 'Update Device' 200

License Pool Alarms 202
6 Assessing Network Health 203
Assessing Health from the Network Summary 203
Assessing Health from the Network Topology Page 208
Filtering to Access Specific Information 212
Filtering by 'Time Range' 213
Filtering by 'Topology' 215
Filtering the Device Floating License Page 218
Filtering by 'Status' 222
Filtering by 'More Filters' 224
Filtering by Groups 225
Determining Network Health from Alarms 227
Configuring Alarm Settings 227
Monitoring Active Alarms to Determine Network Health 227
Performing Management Actions on Active Alarms 227
Filtering by 'Severity' 230
Filtering by 'Source Type' 233
Filtering by 'More Filters' 234
Filtering by 'Type' 235
Filtering by 'Alarm Names' 237
Viewing Journal Alarms to Determine Operator Responsibility 237
Filtering the Alarms Journal by 'More Filters' 238
Viewing History Alarms 240
Filtering by 'Type' 242
Filtering by 'Alarm Names' 244
Forwarding Alarms 244
Forwarding Alarms whose Destination Type is 'SNMP' 252
Forwarding Alarms whose Destination Type is 'Mail' 255
Forwarding Alarms whose Destination Type is 'Syslog' 257
Forwarding Alarms whose Destination Type is 'Notification' 261
Viewing the New Rules in the Alarms Forwarding Page 265
Assessing Network Health in the Statistics Pages 265
Viewing Statistics on Calls over Devices 265
Metrics Bar Charts 267
Statistics Summary 269
Viewing Statistics on Streams over Links 270
Viewing Statistics on Calls over Sites 270
Viewing Statistics on Calls over Endpoints 270
Monitoring Performance 270
Adding a PM Template 271
Adding a PM Profile 276
Starting and Stopping PM Polling 281
Viewing PM Data Resulting from Polling 282
7 Managing your Network 292

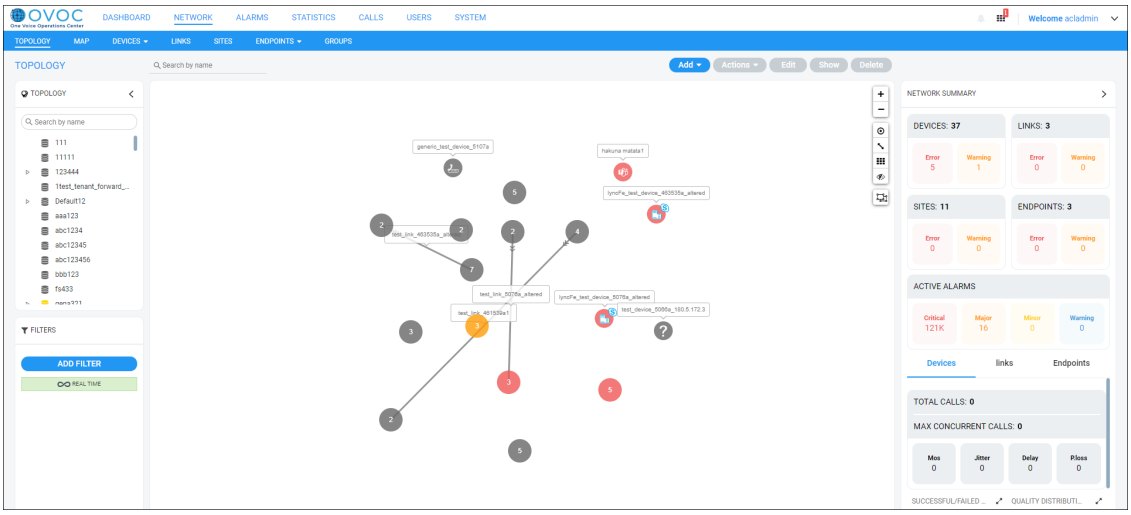
Performing Management Actions 292
Updating Firmware 293
Updating Firmware on Multiple Devices 295
Updating Firmware on a Component in a Media Cluster 295
Resetting a Device 298
Locking or Unlocking a Device 299
Populating Links 300
Moving a Device 301
Backing Up 302
Restoring the Last Backup 303
Setting Configuration Factory Defaults 304
Saving a Device's Configuration File to Flash Memory 304
Saving a Device's Configuration File to the PC 305
Resetting Redundant 305
Performing Switchover 306
Changing Profile 306
Showing Device Information 308
Showing Link Information 310
Showing User Information 311
Editing a Device 313
Deleting a Device 313
Resetting a Device 314
Refreshing a Device's Pool License 315
Monitoring Device-Level Backup and Performing Rollback 315
8 Obtaining Quality Statistics on Calls 316
Accessing the Calls List 316
Filtering by 'Quality' 319
Filtering by 'More Filters' 320
Showing Call Details 324
Details of a Call Made over an AudioCodes SBC 324
Media 325
Signaling 329
Trends 330
SIP Call Flow 331
Details of a Test Call Made over an SBC 334
Call Details Page – Debug File Button 336
Details of a Call Made over Microsoft Skype for Business 336
Media 339
Signaling 342
Details of a Call Made over Microsoft Teams 342
Quality 345
Media tab 347
Network 349
Device 352

Details of a Call Made over an Endpoint Using SIP Publish 353
Media 356
Managing QoE Thresholds Profiles per Tenant 359
Understanding the 3 Sensitivity-Level Profiles 359
Understanding How Call Color is Determined 360
Link Profile as Determinant 360
MOS Metric as Determinant 361
Adding a QoE Thresholds Profile per Tenant 362
Editing a QoE Thresholds Profile per Tenant 365
Deleting a QoE Thresholds Profile per Tenant 365
Managing QoE Status and Alarms per Tenant 366
Adding a QoE Alarm Rule per Tenant 366
Editing a QoE Alarm Rule per Tenant 369
Deleting a QoE Alarm Rule 369
9 Getting Information on Users Experience 370
Adding an Active Directory to the OVOC 370
Editing an Active Directory 373
Deleting an Active Directory 375
Synchronizing an AD with the AD Server 375
Assessing Overall End Users Experience 375
Assessing a Specific End User's Experience 377
Managing End Users 379
Filtering the User Details Page 380
10 Managing Reports 382
Defining a Report 385
Selecting a Metric 392
Viewing a Defined Report 399
Editing a Report 400
Performing Actions on Reports 401
Displaying Report Results 402
'Element (Entity) Statistics' Report Type 403
'Aggregated Statistics Trends' Report Type 404
Viewing a Snapshot of all Reports Statistics 405
Viewing Schedulers and Reports Executed by them 407
Adding a Report Scheduler 409
Editing a Defined Scheduler 412
Showing a Scheduled Report's Results 412
11 AudioCodes IP Network Telephony Equipment 414
12 Adding an Unprivileged User to MSSQL Server 420

1 Introduction

The AudioCodes One Voice Operations Center (referred to as 'OVOC' for short in this document) is a web-based voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application.

Figure 1-1: AudioCodes One Voice Operations Center



OVOC enables administrators to adopt a holistic approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction.

The OVOC's clear GUI design allows network administrators to manage the full lifecycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks that would normally be complex and time-consuming, such as performing root cause analysis, adding new devices to the VoIP network and initiating bulk software updates, can be carried out quickly and easily.

The OVOC uniformly manages, monitors and operates the entire AudioCodes One Voice portfolio, including Media Gateways, Session Border Controllers, Microsoft SBAs and IP Phones.

About the One Voice Operations Center

The OVOC enables customers to adopt an integrated approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction. When deployed in Amazon Web Services (AWS), for example, the OVOC enables AudioCodes partners and systems integrators to provide remote VoIP support and professional services, covering AudioCodes session border controllers, IP phones and other devices, from the cloud.

The OVOC combines several key functions together in a single pane of glass, including:

- New device detection and configuration

- Accurate inventory population
- Automation and mass operation support
- A central, correlated alarm dashboard
- Group-based configuration and update management
- Change documentation and device configuration backup and restore
- Quality monitoring and RCA (root cause analysis)

In addition, the OVOC is fully integrated with AudioCodes Routing Manager (ARM). ARM is a holistic, dynamic routing manager with a design based on software-defined networking principles. It decouples the device layer from the network routing and policy layers, designs VoIP networks automatically, and simplifies routing rules, monitoring and management configuration.

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

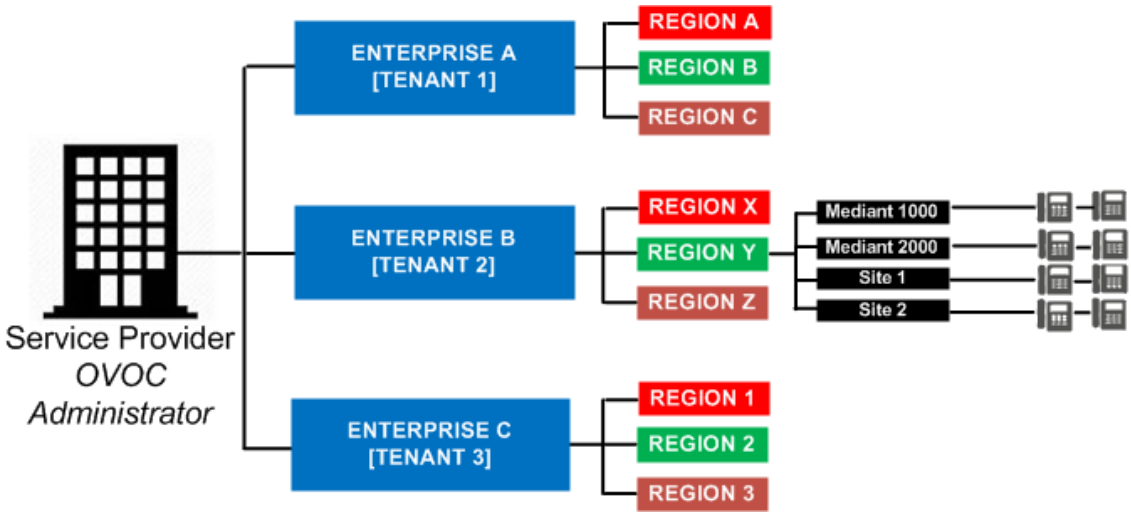
The OVOC features these types of telephony network architecture:

- Multi-Tenancy Architecture (see ITSP Multi-Tenancy Architecture below 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

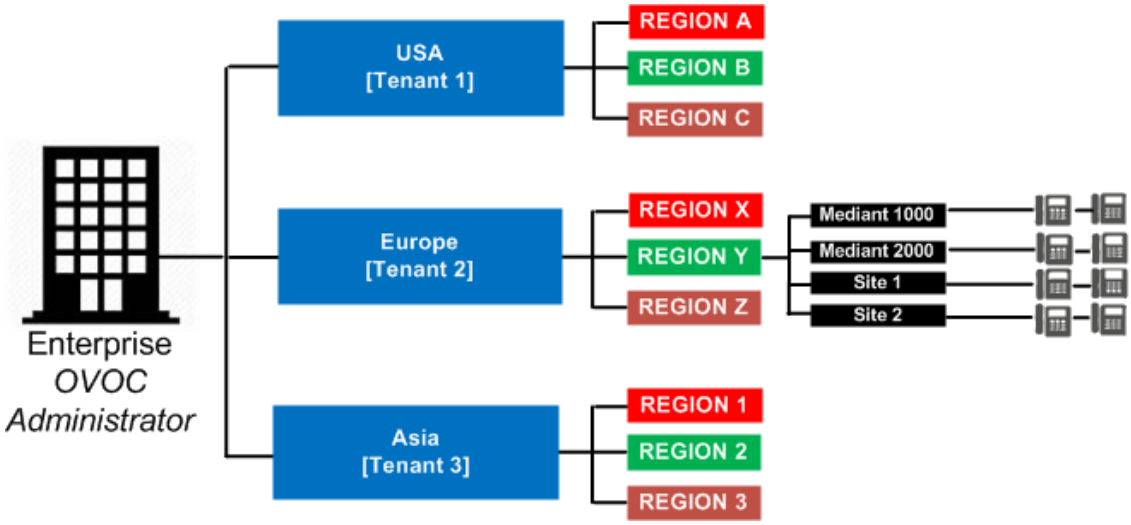


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

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

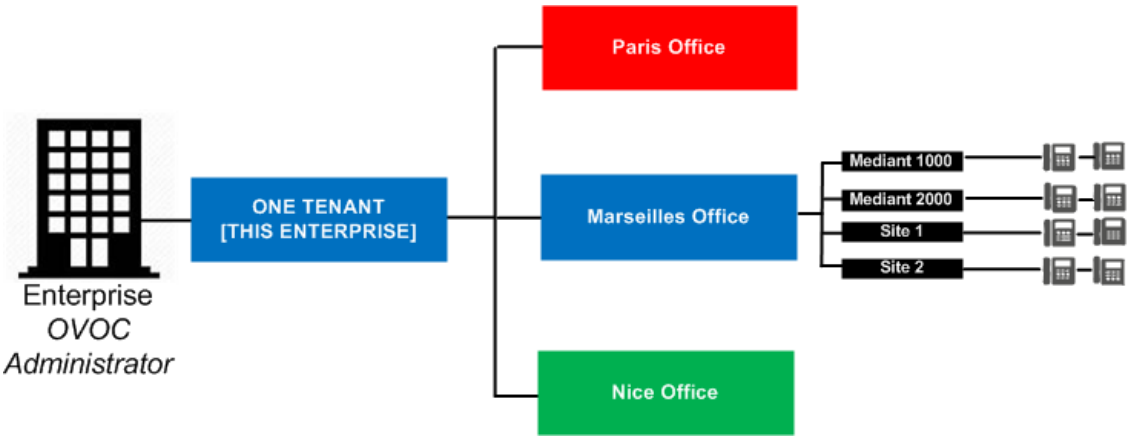


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

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

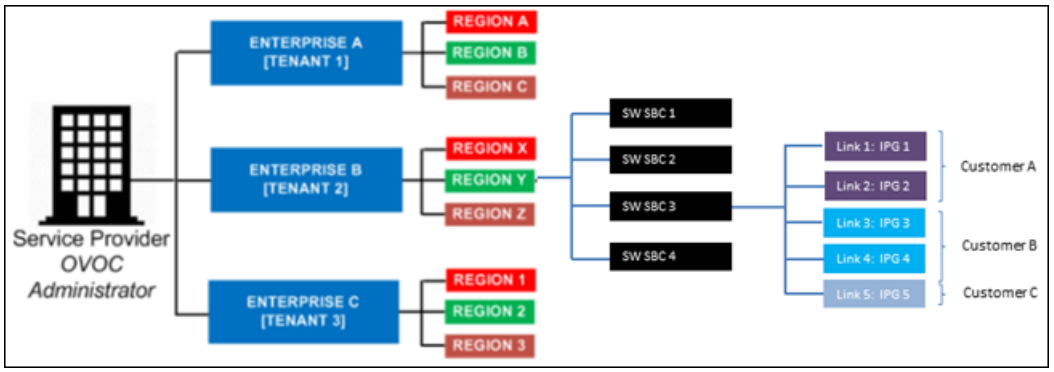
Element	Description
System	An ITSP managing multiple enterprises using a cloud-based or hosted 'global' OVOC application.
Tenant	■ An ITSP's enterprise customer, using only a portion of the OVOC resources and only some of the OVOC entities. Other tenants (the ITSP's other enterprise customers) in the ITSP's multi-tenant network will be invisible to this tenant. ■ An enterprise's regional branch, using only a portion of the OVOC resources and only some of the OVOC entities. ■ An enterprise whose network administrator must define a tenant (that enterprise) under which to define the enterprise's distributed offices.
Entity	Any element which can be managed or used as a whole: ■ Tenant entity (managed/assigned by a specific OVOC tenant) ■ Global entity (managed by the OVOC system; applies to/affects all tenants) ■ System entity (managed /assigned only by the OVOC system)
Resource	Any element that can be partly managed/assigned: ■ Global resource (managed by the OVOC system; applies to/affects all tenants) ■ Tenant resource (portion of the resource)

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

OVOC operators whose security level is 'Monitor Links' *cannot* monitor (in addition to regular monitor-only restrictions):

- Any information related to topology except the links that are attached to the operator (including tenant information / region information and sites, though only names of sites that are used as links, destinations)
- Any information about the source / destination devices except their names, including:
  - Device backups
  - Call flow information

- Caller / callee information except user name representation (either full name, URI, phone number, etc.)
- Legs information (media, signaling, trends) except leg arrows and color (in diagram) of legs not associated with the links attached to the operator
- Diagram media / control information about legs not associated with the links attached to the operator

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 70.

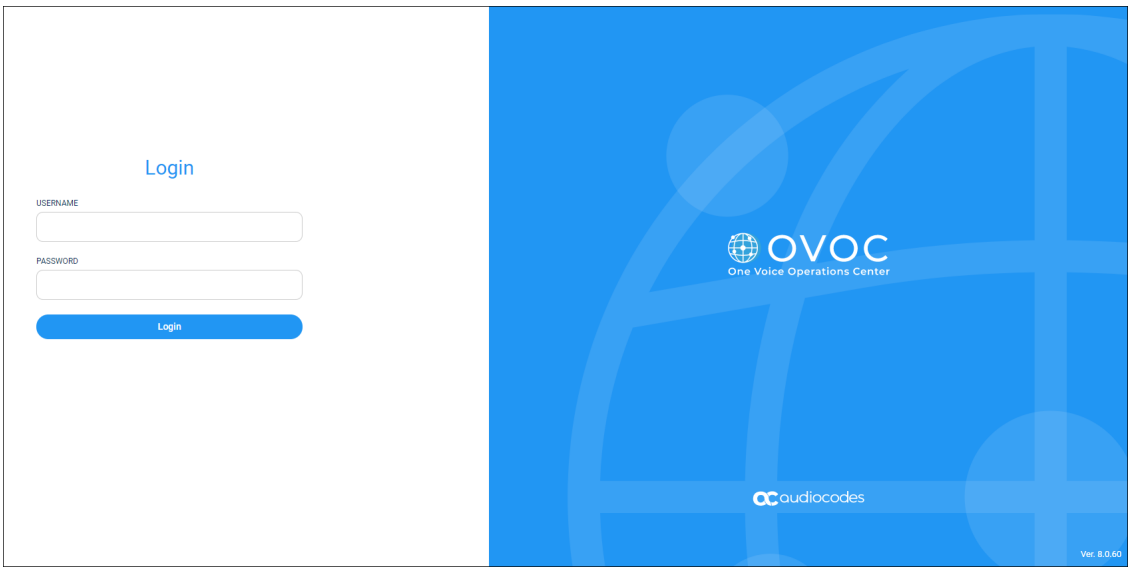
Logging in

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.
- If the operator attempting to log in is an Azure operator and if Multi Factor Authentication is enabled in the Azure configuration for this operator, see Configuring Operator Authentication Centrally with Azure Active Directory on page 44 and Logging in as an Azure User with Multi Factor Authentication on page 47.

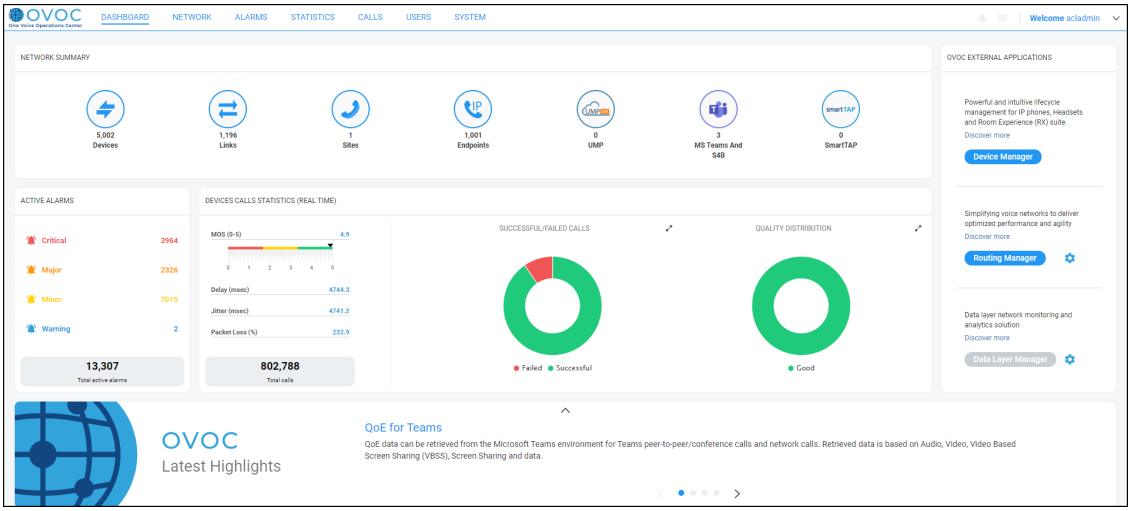
Getting Acquainted with the Dashboard

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

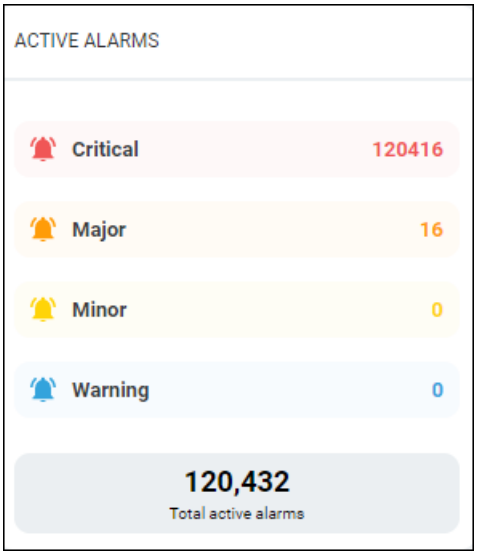
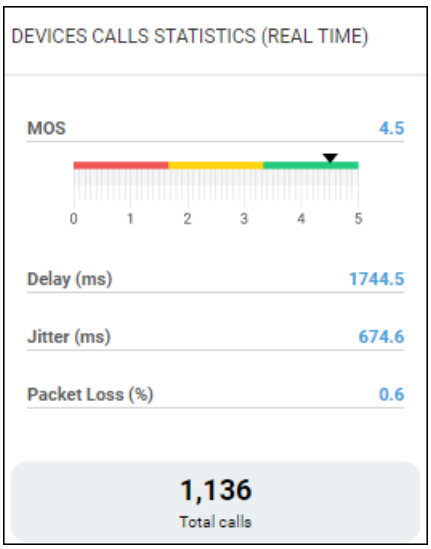


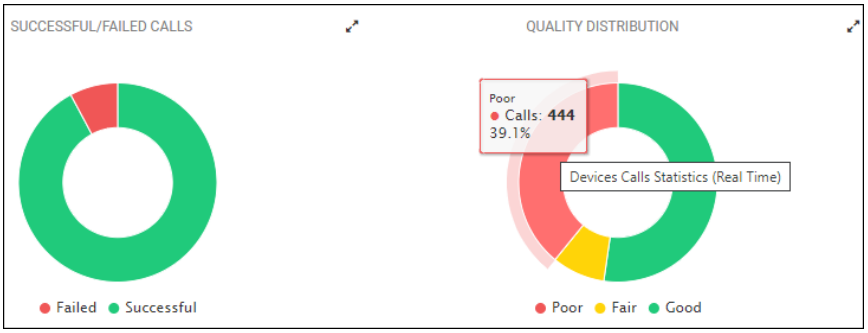
Use the following table as reference:

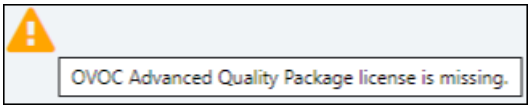
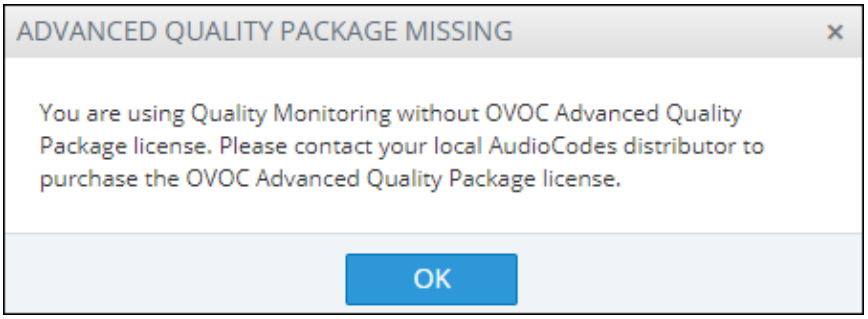
Table 2-1: OVOC Dashboard

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 Adding Links on page 159.

Cluster Icon	Description
	[Sites] Indicates the number of sites currently managed by the OVOC. Click to open the Sites page. See Adding Sites on page 164
	[Endpoints] Indicates the number of endpoints currently managed by the OVOC. Click to open the Endpoints page. See Monitoring Endpoints Status on page 167.
	[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 AudioCodes IP Network Telephony Equipment on page 414.
	[Microsoft Teams and Skype for Business] Indicates the number of Microsoft Teams and 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.
Active Alarms	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.

Cluster Icon	Description
	 ■ Clicking the total number of active alarms in the network opens the Active Alarms page. ■ 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.
Devices Calls Statistics (Real Time)	■ Indicates (1) the total number of calls, in real time and (2) the average MOS, Jitter, Delay and Packet Loss (%) scores:  ✔ Click 'Total calls' to access the Statistics-Aggregated QoE page, displaying QoE statistics on all calls.

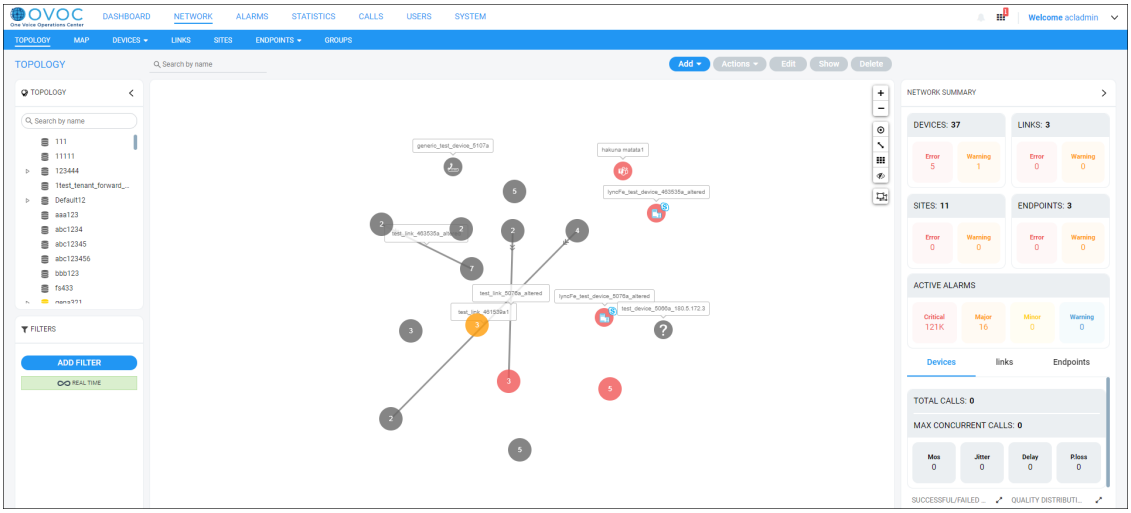
Cluster Icon	Description
	■ Below left: Successful / Failed Calls ■ Below right: Quality Distribution (Good, Fair, Poor)  ✔ Position your mouse above a pie segment to view QoE details. ✔ [Above left] Click a pie segment to directly access those calls whose performance status is FAILED or SUCCESSFUL; the Calls List page opens displaying only those calls. In that page, you can select any call and show its details in the Call Details page. ✔ [Above right] Click a pie segment to directly access those calls whose quality is assessed to be Poor, Fair or Good; the Calls List page opens displaying only calls of that quality. In that page, you can select any call and show its details in the Call Details dynamic tab that opens.
OVOC External Applications	Each external application described next opens in a separate browser tab or browser window depending on the operator's browser settings.
Device Manager	Click the button to quickly access 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.
Routing Manager	Click the button to quickly access the AudioCodes 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

Cluster Icon	Description
	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. 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.
Data Layer Manager	Click the button to quickly access NEC's Data Layer Manager. Applies only to operators who have acquired the app. Data Layer Manager enables quickly and easily accessing the exact network equipment component associated with a voice quality issue - if an issue is detected - and benefiting from root cause analysis.
Notifications 	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.
	Displayed on the Dashboard to notify the operator that an Advanced Quality Package license is missing and should be acquired from AudioCodes. Hovering the cursor over the icon displays a tool tip instructing the operator about the issue.  Clicking the icon opens details about how to troubleshoot the issue. 

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	OVOC-QA-TEAMS Simulator-TEAMS Tring	For detailed information about multi-tenancy architecture, see ITSP Multi-Tenancy Architecture on page 3. = Tenant status is Error when one or more of the following exists: ✔ management status of at least one region is Error

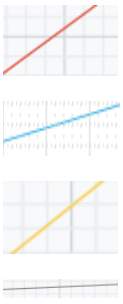
Network Entity	Icon	Explanation
		✔ voice quality status of at least one region is Error ✔ license status of at least one region is Error ✔ license status of the tenant itself is Error due to one of these [Critical] alarms: QoE Devices Overload, QoE Sessions Overload, QoE Endpoints Overload or Endpoints Management Overload. = Tenant status is Warning when one or more of the following exists: ✔ management status of at least one region is Warning ✔ voice quality status of at least one region is Warning ✔ license status of at least one region is Warning ✔ 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. ✔ One of the tenant's AD is disconnected  = Tenant status is OK when all of the following exist: ✔ management status of all regions is OK or Unmonitored ✔ voice quality status of all regions is OK or Unmonitored ✔ license status of all regions is OK or Unmonitored ✔ license status of the tenant itself is free of alarms ✔ All the tenant's ADs are connected  = Tenant status is Unmonitored when all of the following exist: ✔ management status of all regions is

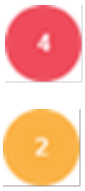
Network Entity	Icon	Explanation
		Unmonitored ✔ voice quality status of all regions is Unmonitored ✔ license status of all regions is Unmonitored
Region		= Region status is Error when one or more of the following exist: ✔ management status of at least one device or site is Error ✔ voice quality status of at least one device or site is Error ✔ license status of at least one device or site is Error = Region status is Warning when one or more of the following exists: ✔ management status of at least one device or site is Warning ✔ voice quality status of at least one device or site is Warning ✔ license status of at least one device or site is Warning = Region status is OK when all of the following exist: ✔ management status of all devices and sites is OK or Unmonitored ✔ voice quality status of all devices and sites is OK or Unmonitored ✔ license status of all devices and sites is OK or Unmonitored = Region status is Unmonitored when all of the following exist: ✔ management status of all devices and sites is Unmonitored ✔ voice quality status of all devices and sites is

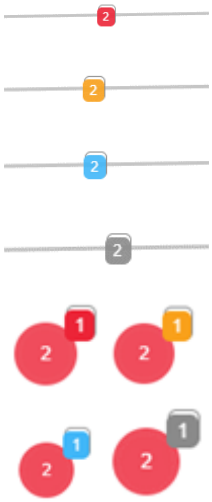
Network Entity	Icon	Explanation
		Unmonitored ✔ license status of all devices and sites is Unmonitored
Device		Indicates an SBC belonging to AudioCodes communicating with the OVOC. Red = Device status is Error when one or more of the following exist: ✔ management status is Error (if device alarms status or connection status is disconnected) ✔ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ✔ License status is Error only if license pool is failed or expired Orange = Device status is Warning when one or more of the following exists: ✔ management status is Warning (if device alarms status or administration status is Warning) ✔ voice quality status is Warning (if control status or media status or connection status is Warning) ✔ 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) Blue = Device status is OK when all of the following exists: ✔ management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) ✔ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined)

Network Entity	Icon	Explanation
		✔ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked
UMP		Indicates the AudioCodes User Management Pack 365 communicating with the OVOC. Red = UMP status is Error when one or more of the following exists: ✔ management status is Error (if UMP alarms status or connection status is disconnected) ✔ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ✔ License status is Error only if license pool is failed or expired Orange = UMP status is Warning when one or more of the following exists: ✔ management status is Warning (if UMP alarms status or administration status is Warning) ✔ voice quality status is Warning (if control status or media status or connection status is Warning) ✔ 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) Blue = UMP status is OK when all of the following exist: ✔ management status is OK - Clear or Undetermined (if UMP alarms status or connection status is OK - Clear or Undetermined) ✔ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined)

Network Entity	Icon	Explanation
		✔ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked
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		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.
Site		Color and status are propagated from the endpoints under the site. Red = Site status is Error when one or more of the following exists: ✔ management status is Error (if site alarms status or connection status is disconnected) ✔ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ✔ License status is Error only if license pool is failed or expired Orange = Site status is Warning when one or more of the following exists: ✔ management status is Warning (if site alarms status or administration status is Warning) ✔ voice quality status is Warning (if control status or media status or connection status is Warning) ✔ 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

Network Entity	Icon	Explanation
		is no voice quality license) Blue = Site status is OK when all of the following exist: ✔ management status is OK - Clear or Undetermined (if site alarms status or connection status is OK - Clear or Undetermined) ✔ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined) ✔ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Gray = Site status is Unmonitored when all of the following exist: ✔ management status of all endpoints is Unmonitored ✔ voice quality status of all endpoints is Unmonitored ✔ license status of all endpoints is Unmonitored
Link		A link joins two devices: Red = Voice quality status is Error when one or more of the following exists: ✔ 'Critical' Control Status ✔ 'Critical' Media Status Orange = Voice quality status is Warning when one or more of the following exists: ✔ 'Major' Control Status ✔ 'Major' Media Status Blue = Voice quality status is OK/Clear when all of the following exists: ✔ Control Status is OK/Clear ✔ Media Status is OK/Clear ✔ Control Status or Media Status is

Network Entity	Icon	Explanation
		Unmonitored Gray = Voice quality status is Unmonitored when both of these exist: ✔ Control Status is Unmonitored ✔ Media Status is Unmonitored **Note**: ✔ If no voice quality license exists, status will be Unmonitored. ✔ Link status does not impact device / region ✔ When the number of links exceeds 1000, only links whose *source and destination are within the visible bounds of the map* are displayed; links are not displayed if their source or destination lies outside the visible bounds of the map. This prevents clutter, facilitating more effective management. ✔ 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. ✔ 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. 
Device clusters		Indicate aggregated clusters of devices (AudioCodes devices as well as non-AudioCodes devices). The numbers indicate how many devices are in the cluster. ■ 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

Network Entity	Icon	Explanation
		Error ■ 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 ■ Blue = all entities in this cluster have a status of OK – see above in this table for the conditions that need to exist for status to be OK ■ Gray = all entities in this cluster have a status of Unmonitored – see above in this table for the conditions that need to exist for status to be Unmonitored
Link clusters		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. ■ 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 ■ 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 ■ Blue square = all links in this cluster have a status of OK – see above in this table for the conditions that need to exist for status to be OK ■ Gray square = all links in this cluster have a voice quality status of Unmonitored – see above in this table for the conditions that need to exist for voice quality status to be Unmonitored
SmartTAP		Indicates the AudioCodes SmartTAP communicating with the OVOC. ■ Red = SmartTAP status is Error when management status is Error (if SmartTAP alarms status or connection status is disconnected)

Network Entity	Icon	Explanation
		■ Orange = SmartTAP status is Warning when management status is Warning (if SmartTAP alarms status or administration status is Warning) ■ 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) ■ Gray = SmartTAP status is Unmonitored when management status is unmonitored

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.

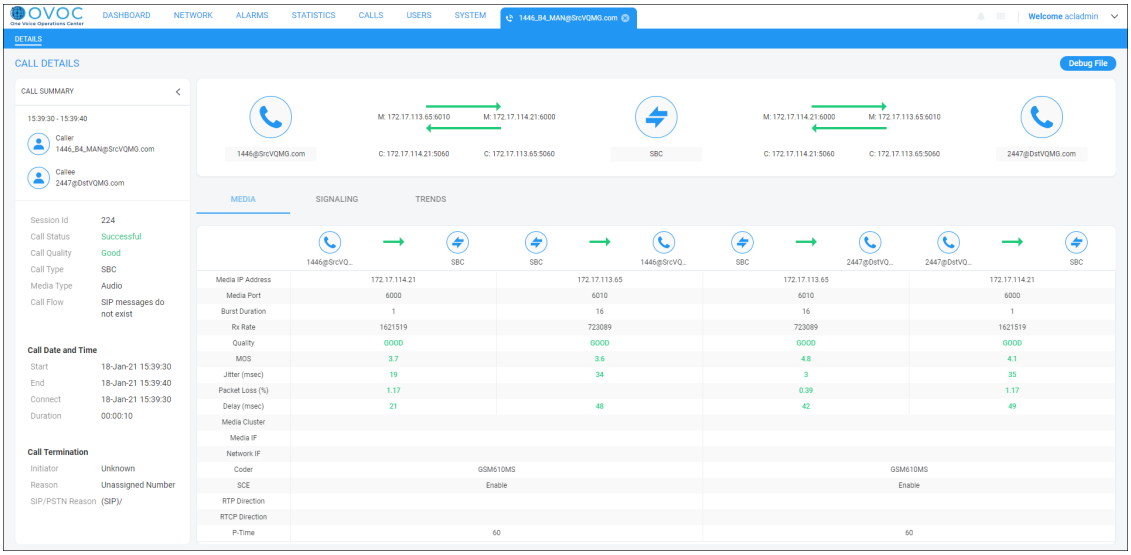
- The **Hide Link Labels** button allows operators to hide the labels of the links in the Network Topology and Network map pages; this reduces clutter for more effective management, especially in networks with many devices and links.
- **Show Clusters**. If more than 200 devices and sites (aggregated) 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 30).

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 324.

For more information about the dynamic tab that is created for user details, see Assessing a Specific End User's Experience on page 377.

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 9.

Table 2-3: Menu Bar

Menu	Tab	Description
Network	**Topology**	The tab's page lets you: ■ Assess at a glance the topology of the network ■ Perform multiple configuration and maintenance actions ■ Select multiple devices (Ctrl+) and perform multiple actions simultaneously (Ctrl+ to deselect) ■ Select multiple links (Ctrl+) and perform multiple actions simultaneously (Shift+ to deselect) ■ Filter out unwanted information to facilitate quick access to specific information The page features two 'modes': ■ Real Time mode. The page continuously refreshes, presenting up-to-date network information. ■ Time Filter. The page presents network information valid for the time defined in a Time Filter but invalid in real time. See Filtering to Access Specific Information on page 212 for information about time filters.
	Map	The tab's page lets you: ■ Assess at a glance the enterprise network's global distribution ■ Filter The page features two 'modes': ■ Real Time mode. The page continuously refreshes, presenting up-to-date network information. ■ Time Filter. The page presents network

Menu	Tab	Description
		information valid for the time defined in a Time Filter but invalid in real time. See Filtering to Access Specific Information on page 212 for information about time filters.
	Devices	The tab lets you: ■ Add a network component: ■ Perform a device action ■ Show device
	Links	Lets you add, edit or delete links.
	Sites	Lets you: ■ add a set of endpoints based on a network subnet ■ edit or delete the SIP clients (phones)
	Endpoints	From the tab's drop-down you can select: ■ Status. Lets you view and monitor the status (Quality of Experience) of phones (for example). ■ Configuration. Lets you directly access the Device Manager to configure phones.
Alarms	**Active**	Always displays all the active alarms in the network, in real time.
	Journal	Displays only the operator activity alarms in the network.
	History	Displays time frame historical alarms (default), according to the filter.
	Forwarding	For detailed information about forwarding alarms, see Filtering by 'Alarm Names' on page 244.
Statistics	**Devices**	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.
	Links	Displays the Links Statistics page. Filters on the page allow operators to specify

Menu	Tab	Description
		■ 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) ■ which links to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	Sites	Displays the Sites Statistics page. Filters on the page allow operators to specify ■ 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) ■ which sites to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	Endpoints	Displays the Endpoints Statistics page. Filters on the page allow operators to specify ■ 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) ■ which endpoints to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	PM Profiles	Facilitates setup of Performance Monitoring capability.
	Reports	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

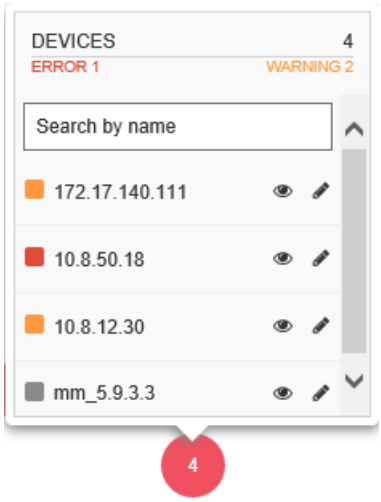
Menu	Tab	Description
		enterprise, and to external authorities associated with the enterprise's network, for accurate diagnosis and correction of degraded sessions and for general network optimization. Opens in another Web page.
Calls	**Calls List**	Displays the Calls List page which presents all the 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.
	QoE Thresholds	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.
	QoE Status & Alarms	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.
Users	**Users Experience**	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.
	User Details	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.
	Active Directories	Lets you add an AD. Displays existing ADs. Allows you to edit and to synchronize with the AD server.
System	**Administration**	Allows performing administration: ■ License

Menu	Tab	Description
		✔ Configuration ✔ System Allocations ✔ Tenants Allocations ✔ Floating License ■ Security ✔ Authentication ✔ Operators ■ OVOC Server
	Configuration	Allows performing OVOC administration: ■ Templates (SNMP Connectivity, HTTP Connectivity, QoE Thresholds, QoE Status & Alarms, Perf Monitoring) ■ Alarms ■ File Manager (Software Manager) ■ OVOC Server ■ Device Backup
	Tasks	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

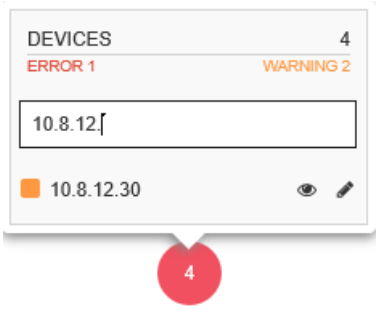
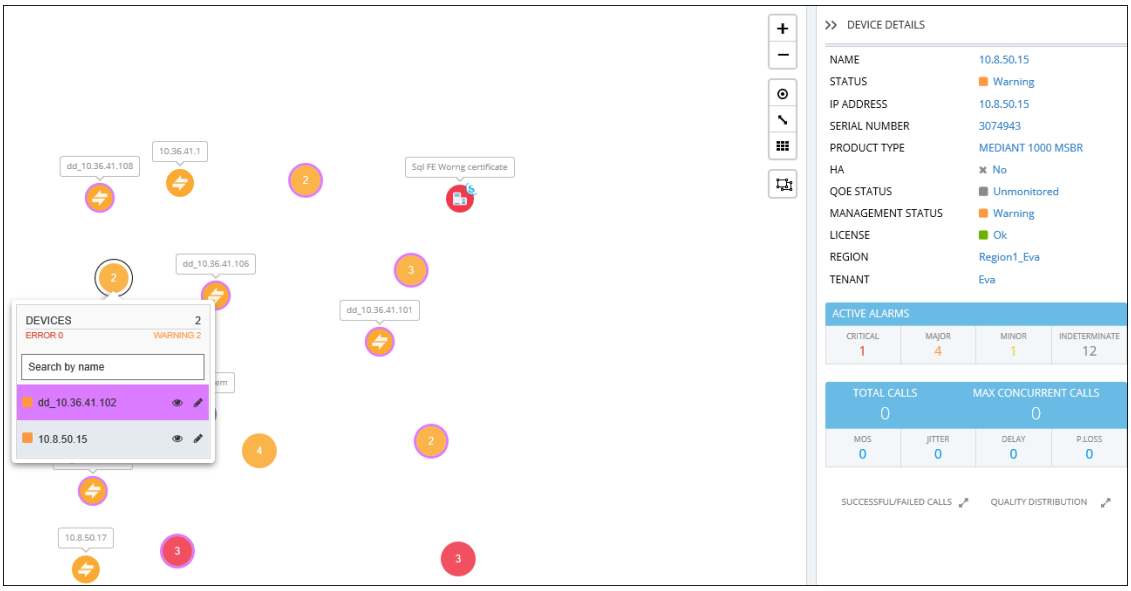
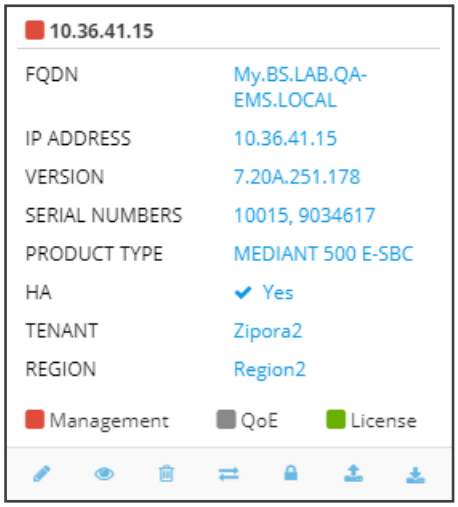


Figure 2-8: Device Details



Hovering Over a Device to Display Information

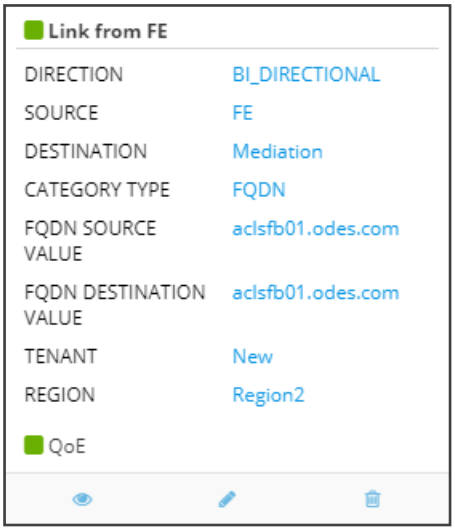
The following figure shows an example of information displayed when hovering over a device.



- 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:

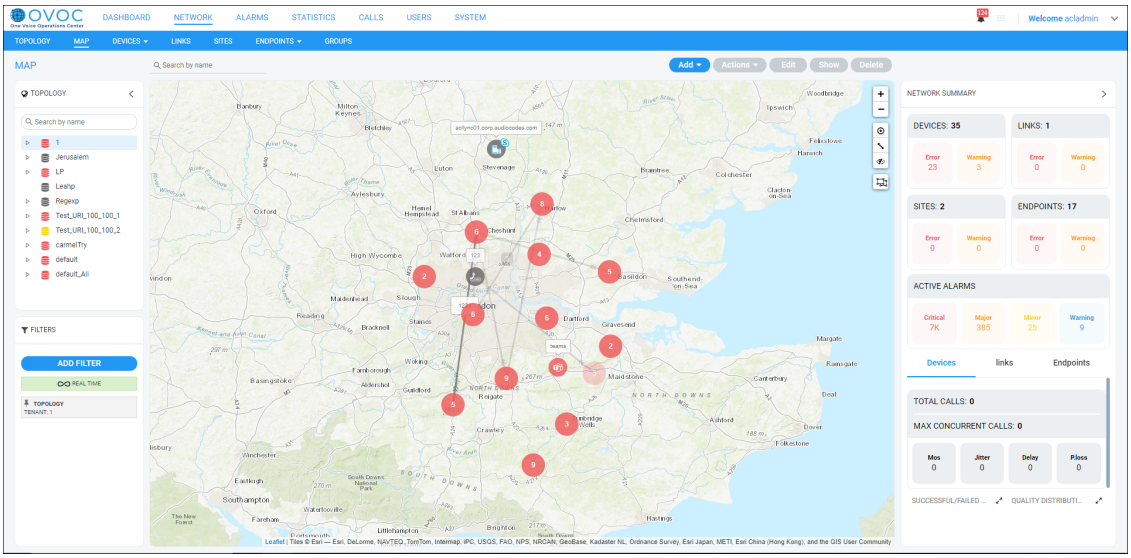


- The logo functions as a 'Home' page button.
- Click it to return to the Network Topology page from any page.
- The feature enhances quick and operator-friendly navigation in the OVOC.

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



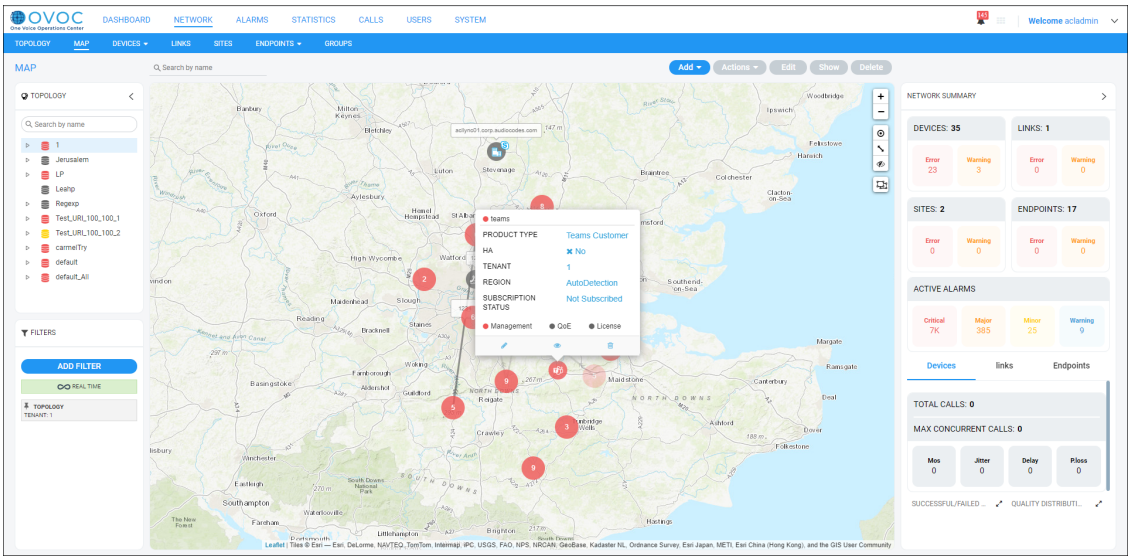
With the exception of cluster icons, entity icons in the Network Map page are identical to those in the Network Topology page described in the table in Getting Acquainted with the Network Topology Page on page 14. A cluster is based on geographical locations of devices in the Network Map page. Clusters 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:

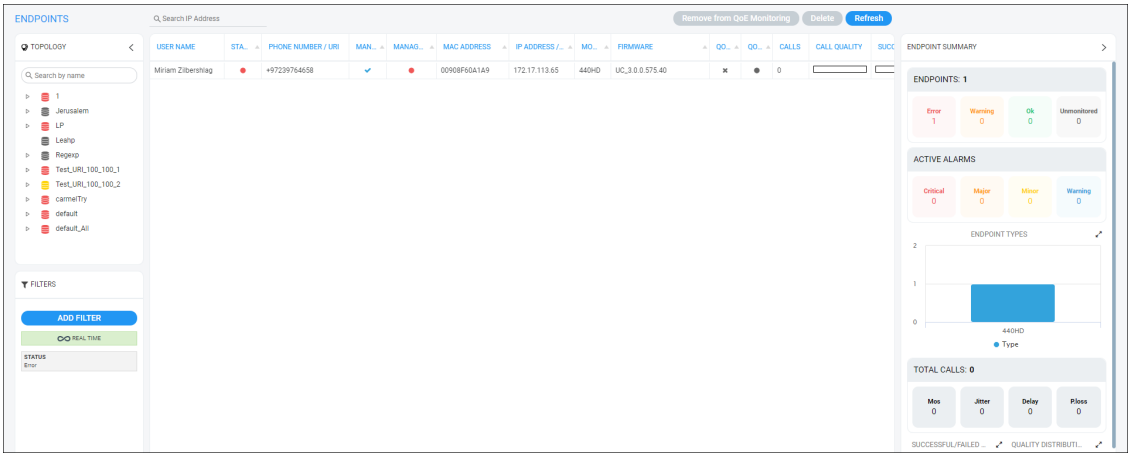
Figure 2-10: Hovering the Cursor over a Network Entity in the Network Map Page



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

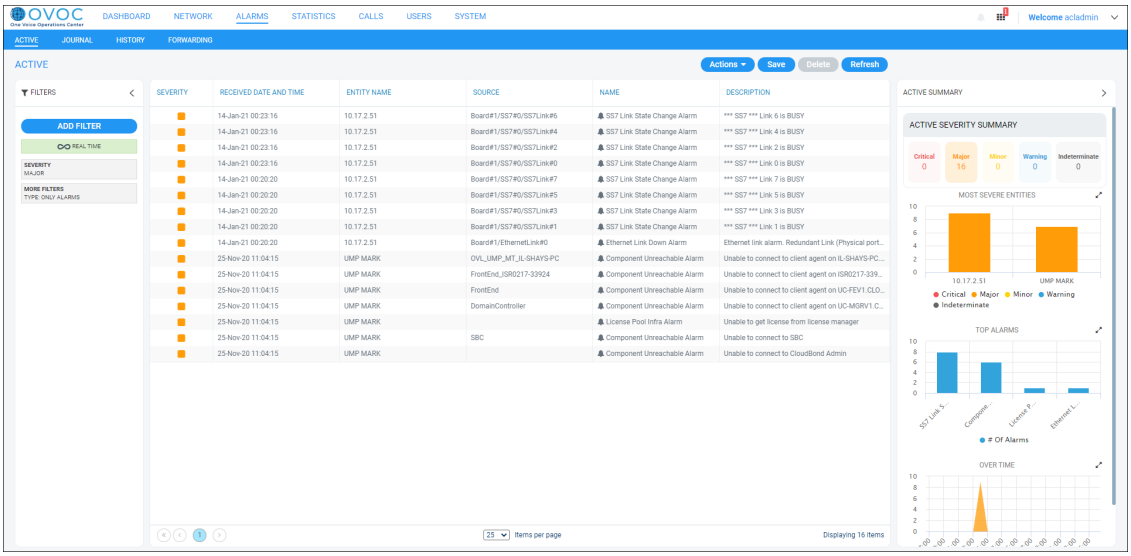
- Determine on how many Devices, Links, Sites and Endpoints, alarms are active.
- Determine which Devices, Links, Sites and Endpoints' status is currently Error / Warning (from the color-coded number). If you click the color-coded number of:
  - **Devices** then the Device Management page opens displaying 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 - 1 Error



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 **Major** in the Active Alarms pane above, click **16**:

Figure 2-12: Alarms Filtered by Severity Level

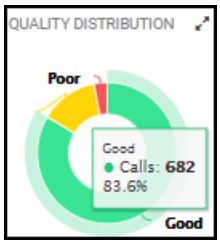


You can select an alarm to view detailed information about it then displayed in the Active Details window on the right side of the page.

In the Network Map page's Network Summary window, the **Devices** | **Links** | **Sites** | **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.

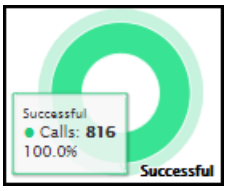
The Quality Distribution pie chart in the Network Summary window allows you to point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose quality was measured to be good, fair or poor respectively:



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).

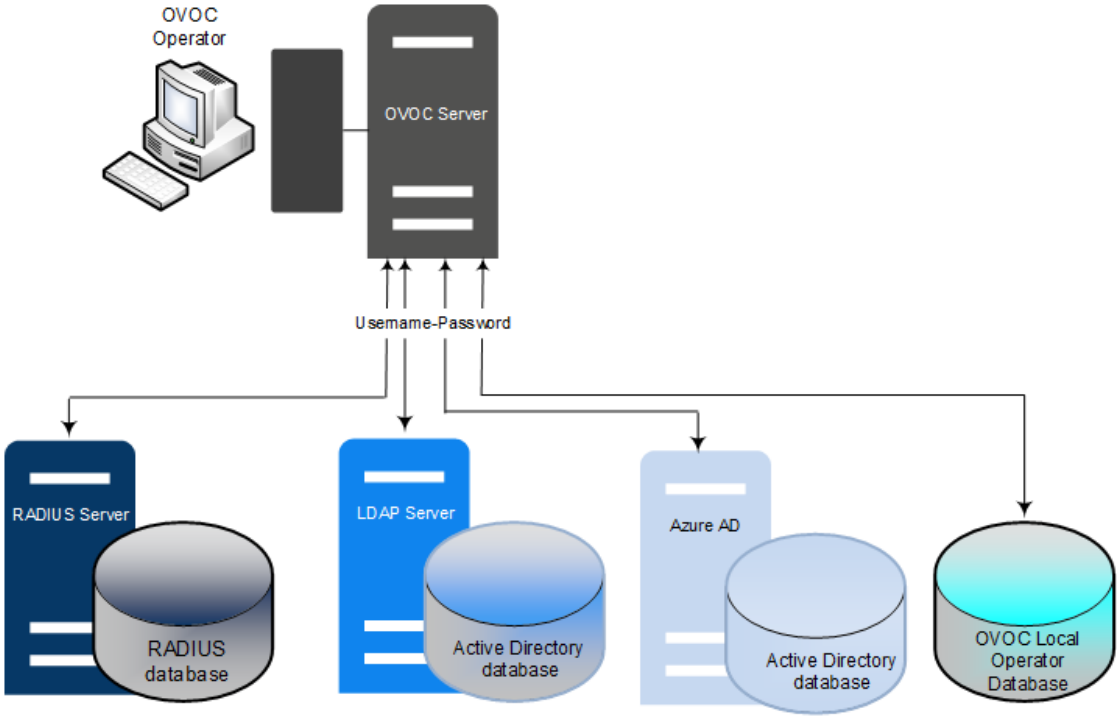
Configuring Operator Authentication

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 42)
- Locally, in the OVOC (see Configuring Operator Authentication Locally, in the OVOC on page 50)

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.

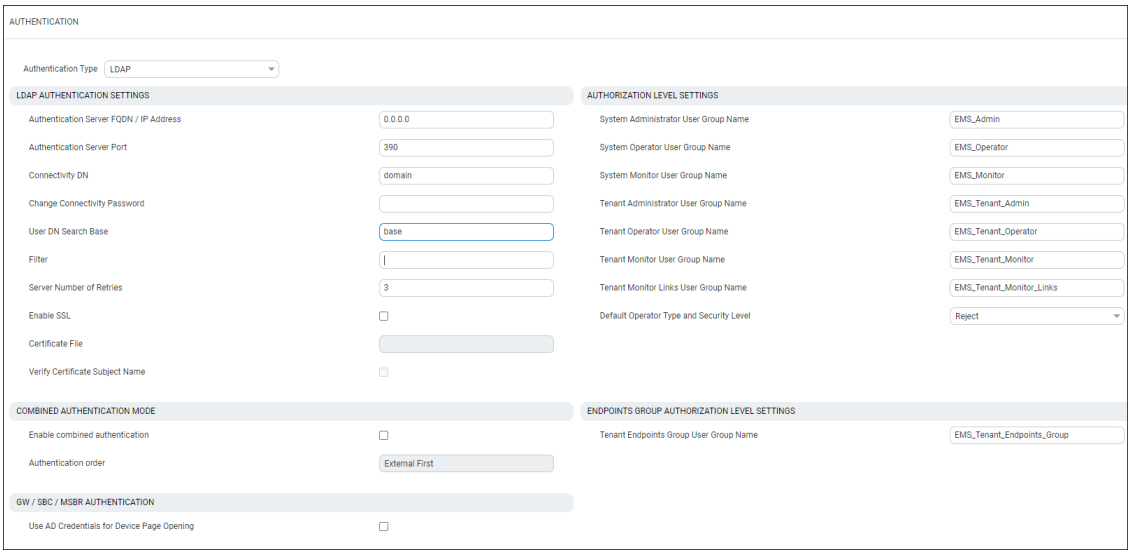
Configuring Operator Authentication Centrally using an LDAP Server

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. If you're not using a standard Microsoft filter such as 'sAMAccountName', configure in this field your own filter with a $ symbol in it, for example, (&(cn=$)(OVOCAuth=TRUE)).
10. Select the 'Enable SSL' option to secure the connection with the LDAP server over SSL; the 'Certificate' drop-down is activated.
11. 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 98.

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.

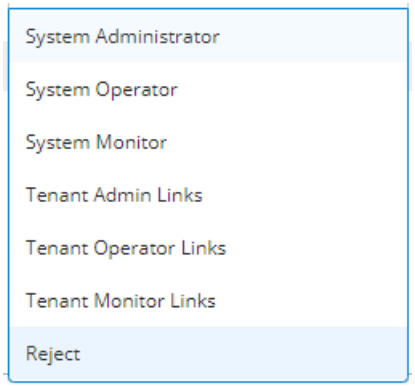
- The parameters below are used to define a User Group in the LDAP server.
- In the Tenant Details screen under the **Operators** tab, the parameter 'LDAP Authentication: Group Name' is used to define a User Group in the OVOC when a tenant level is provisioned (see under Adding a Tenant on page 113).

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 53 and Adding a 'Tenant' Operator on page 60.

12. 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'.
13. 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'.
14. 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'.
15. 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'.
16. 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'.
17. 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'.
18. 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.

19. From the 'Default Operator Type and Security Level' drop-down, select:



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. Under the screen section 'GW / SBC / MSBR Authentication', select the option **Use AD Credentials for Device Page Opening** 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 and login to the GW / SBC / MSBR will be attempted with same AD user name / password instead of the local GW / SBC / MSBR user name / password. Note that the GW / SBC / MSBR must be also be configured to authenticate with the same AD.

22. Under the section 'Endpoints Groups Authorization Level Settings', configure the 'Tenant Endpoints Group User Group Name' parameter. See also Adding an Endpoints Group on page 168.

23. Click **Submit**.

Configuring Operator Authentication Centrally with a RADIUS Server

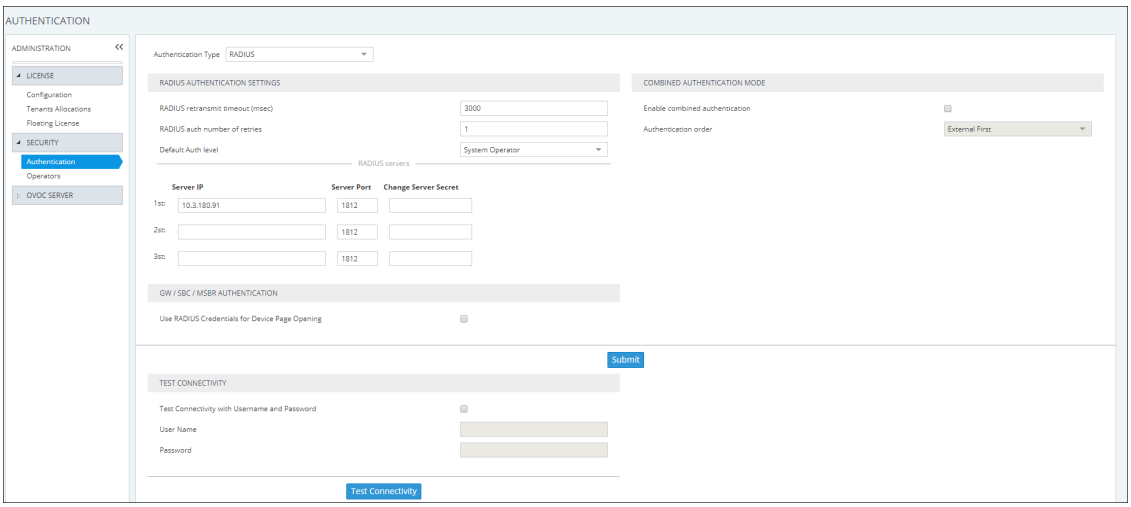
You can centrally configure authentication of OVOC operators using a RADIUS (Remote Authentication Dial-In User Service) server. If you already have centralized user authentication via a RADIUS server, it's recommended to implement it for OVOC operators as well.

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), **Admin**, **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.

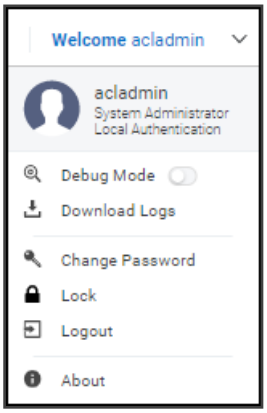
6. Select the **Use RADIUS Credentials for Device Page Opening** option for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the RADIUS server.
7. Under Combined Authentication 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.

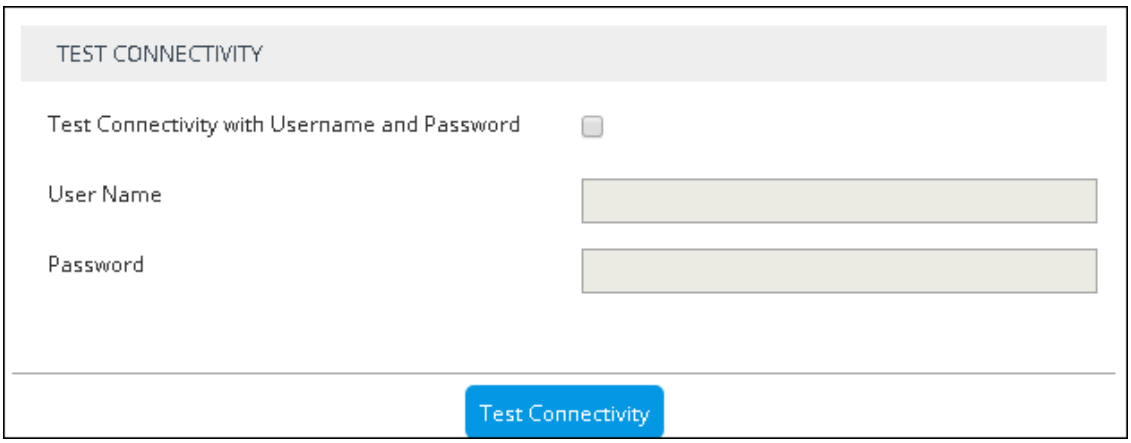
Testing Connectivity with the LDAP / RADIUS Server

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



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.

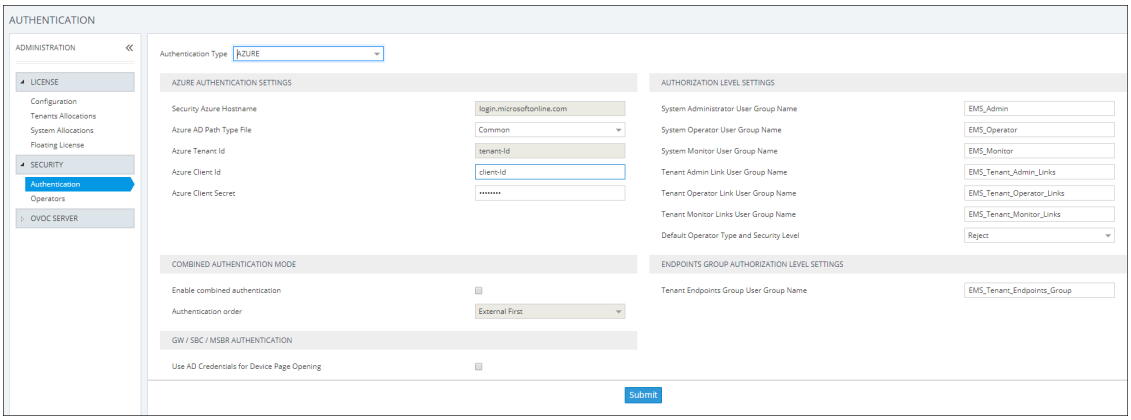
Configuring Operator Authentication Centrally with Azure Active Directory

Authentication of OVOC operators can be centrally configured using the Azure Active Directory (AD). If you already have centralized user authentication via Azure AD, it's recommended to implement it for OVOC operators as well. When an Azure-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 in the Azure AD are shown following. When no security level is configured in the Azure AD, the parameter 'Default Operator Type and Security Level' in the OVOC's Authentication page (when 'Authentication Type' is **AZURE**) determines behavior.

➢ To configure authentication of OVOC operators using Azure AD:

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

Figure 2-17: Authentication - AZURE



2. View the read-only 'Security Azure Hostname' field. It defines the name of the Azure AD host in the cloud. It allows the OVOC to access Azure AD in the cloud.
3. From the 'Azure AD Path Type File' drop-down, select **Organizations** (default) or **Tenant**.
   - If you choose **Tenant**, the field 'Azure Tenant ID' is activated - see the next step. A string *must* be configured for it (mandatory).
   - If you leave at the default (**Organizations**), the OVOC will be able to access Azure AD in the *enterprise network* if a standard service is purchased.
4. View the 'Azure Tenant ID' field. It will be read-only if **Organizations** is selected in the preceding step. The preceding figure shows 'Azure Tenant ID' as a read-only field defined with the string **tenant-Id**. If a new tenant ID is purchased, the OVOC first accesses the cloud via the 'Security Azure Hostname' field and then (via the 'Azure Client ID' field) a specific Azure AD in the enterprise's network.
5. In the 'Azure Client ID' field, enter the ID of the Azure AD client.
6. In the 'Azure Client Secret' field, define the shared secret (password) to allow the OVOC application access to the specific Azure AD (OVOC authentication). Must be cryptically strong. The OVOC will then be capable of accessing the Azure AD.
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 Azure server but it's unavailable, the OVOC connects to the *local* database with the same operator credentials.

   - **External First**: If the Azure server is unavailable when the Azure-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 Azure server.

8. Under the screen section 'GW / SBC / MSBR Authentication', select the option **Use AD Credentials for Device Page Opening** 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 Azure AD and login to the GW / SBC / MSBR will be attempted with same AD user name / password instead of the local GW / SBC / MSBR user name / password. Note that the GW / SBC / MSBR must be also be configured to authenticate with the same AD.

Authorization Level Settings

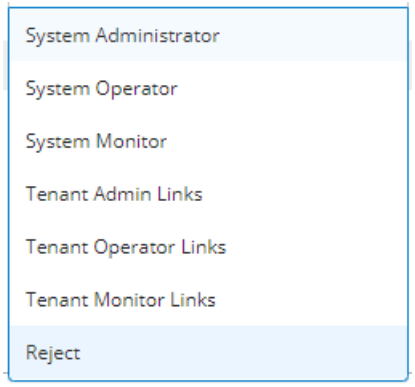


When an operator connects to the OVOC, the OVOC (before allowing the operator access) checks with the Azure AD if the User Group which the operator is associated with in the OVOC, is defined in the Azure AD.

- The parameters below are used to define a User Group in the Azure AD.
- In the Tenant Details screen under the **Multitenancy** tab, the parameter 'AD 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 113).

If the Azure AD 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 53 and Adding a 'Tenant' Operator on page 60.

9. 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'.
10. 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'.
11. 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'.
12. 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'.
13. 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'.
14. 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'.
15. 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.
16. From the 'Default Operator Type and Security Level' drop-down, select:



17. Under the section 'Endpoints Groups Authorization Level Settings', configure the 'Tenant Endpoints Group User Group Name' parameter. See also Adding an Endpoints Group on page 168.
18. Click **Submit**.

> To configure AudioCodes Active Directory on Microsoft Azure, see the 'One Voice Operations Center Integration with Northbound Interfaces Guide'.

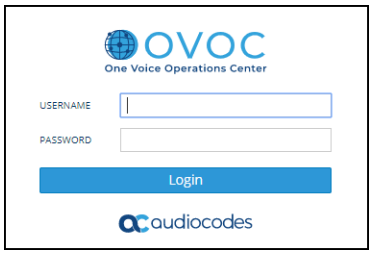
Logging in as an Azure User with Multi Factor Authentication

When logging in to the OVOC, the login process is slightly different if the operator attempting to log in is an Azure operator and if Multi Factor Authentication is enabled for this operator in the Azure configuration, as shown in Configuring Operator Authentication Centrally with Azure Active Directory on page 44.

➢ To log in as an Azure user with Multi Factor Authentication:

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 2-18: Login



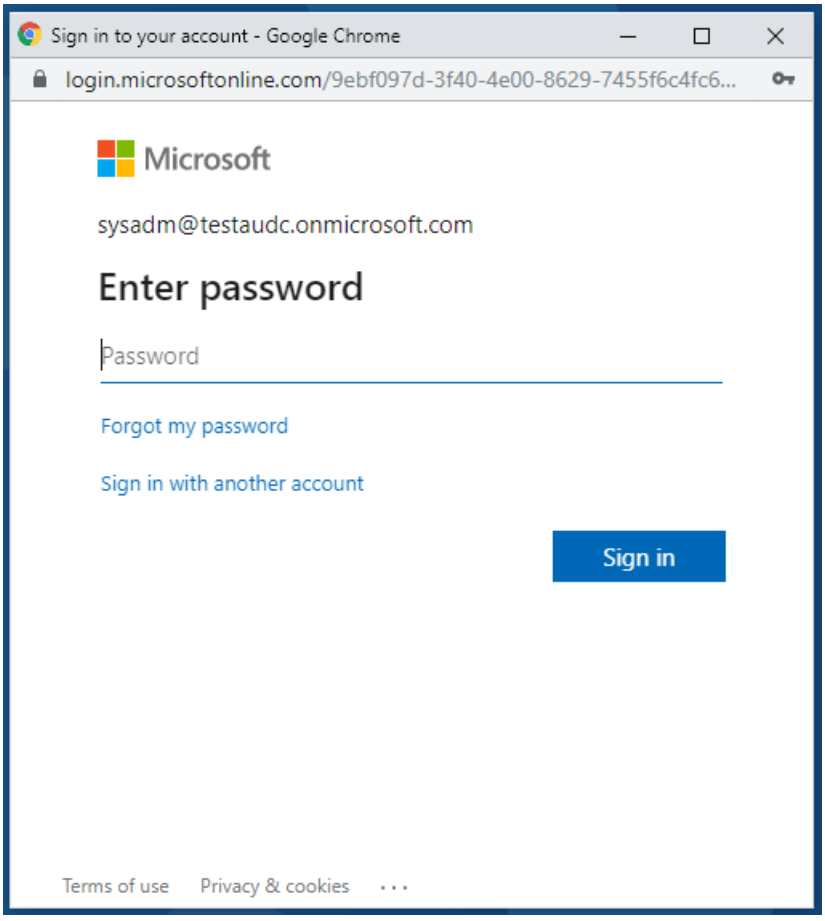
2. Enter your Username and Password and then click **Login**.

Figure 2-19: Azure authentication in progress



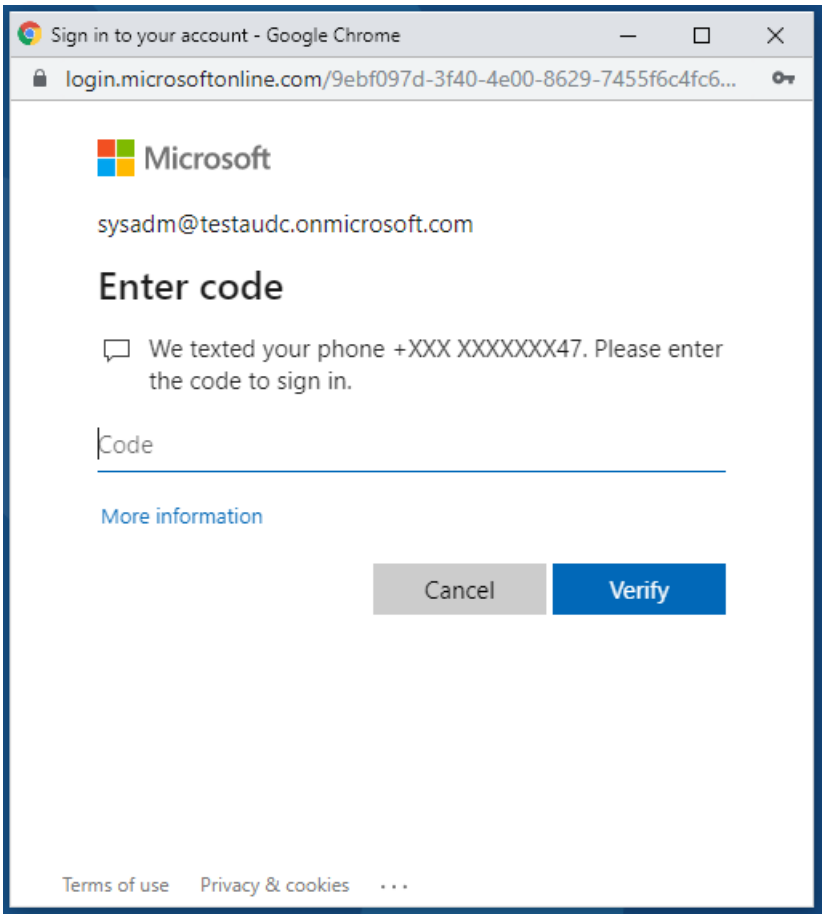
3. During the Azure authentication process, the server detects that Multi Factor Authentication is required and opens an additional window (Microsoft window) in which the operator performs MFA authentication.

Figure 2-20: Microsoft 'Enter password'



4. Enter your Microsoft password and click **Sign in**. The figure below shows the screen that is displayed when the Multi Factor Authentication method is configured to use a code sent to a cellular phone in an SMS. There are other MFA methods besides this one. The MFA method is configured in the Azure Active Directory.

Figure 2-21: Microsoft 'Enter code'



5. In this example of MFA, you'd check your mobile phone, view the code sent to it in the SMS, enter it in the 'Code' field and then click **Verify**.

   The GUI by default displays the Dashboard.

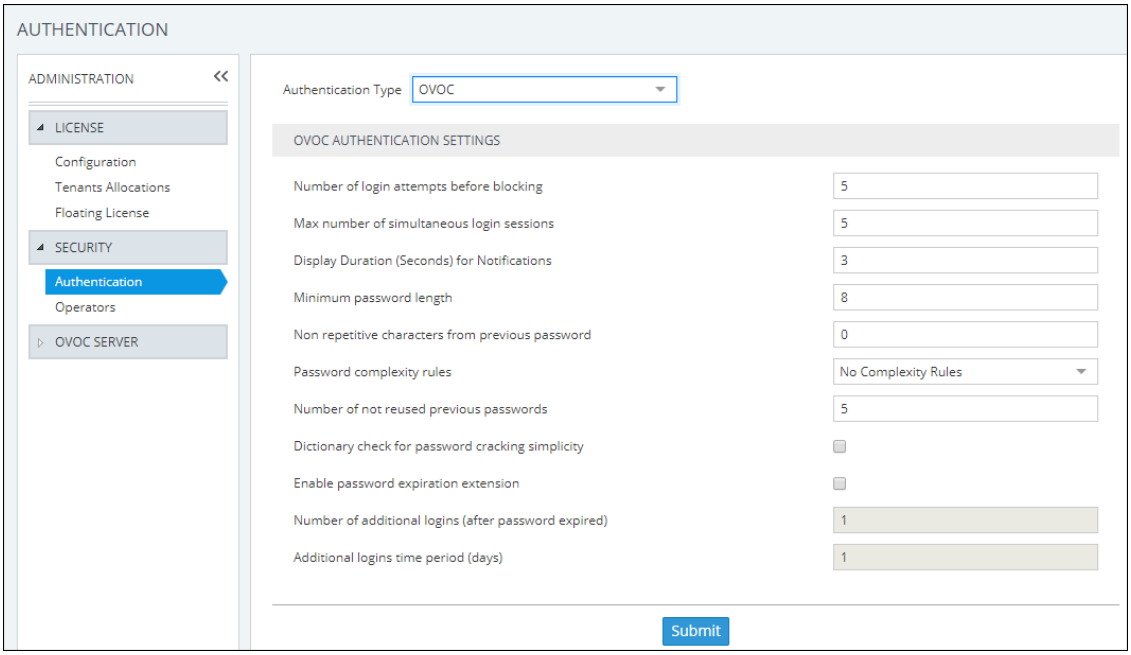
Configuring Operator Authentication Locally, in the OVOC

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 inexpert 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 2-22: Authentication – OVOC



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 Forwarding Alarms whose Destination Type is 'Notification' on page 261.
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: ■ No complexity rules are applied (default) ■ Use Plain or Capital letters, Digits and Special Characters ■ Use Plain and Capital letters, Digits and Special Characters
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 resource-s	Manage tenant resource-s	Monitor system resource-s	Monitor tenant resource-s
System	Admin	Yes, all op types and securit y levels	Yes	Yes	Yes	Yes	Yes
	Operato r	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
	Operato r	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 on the previous page 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').

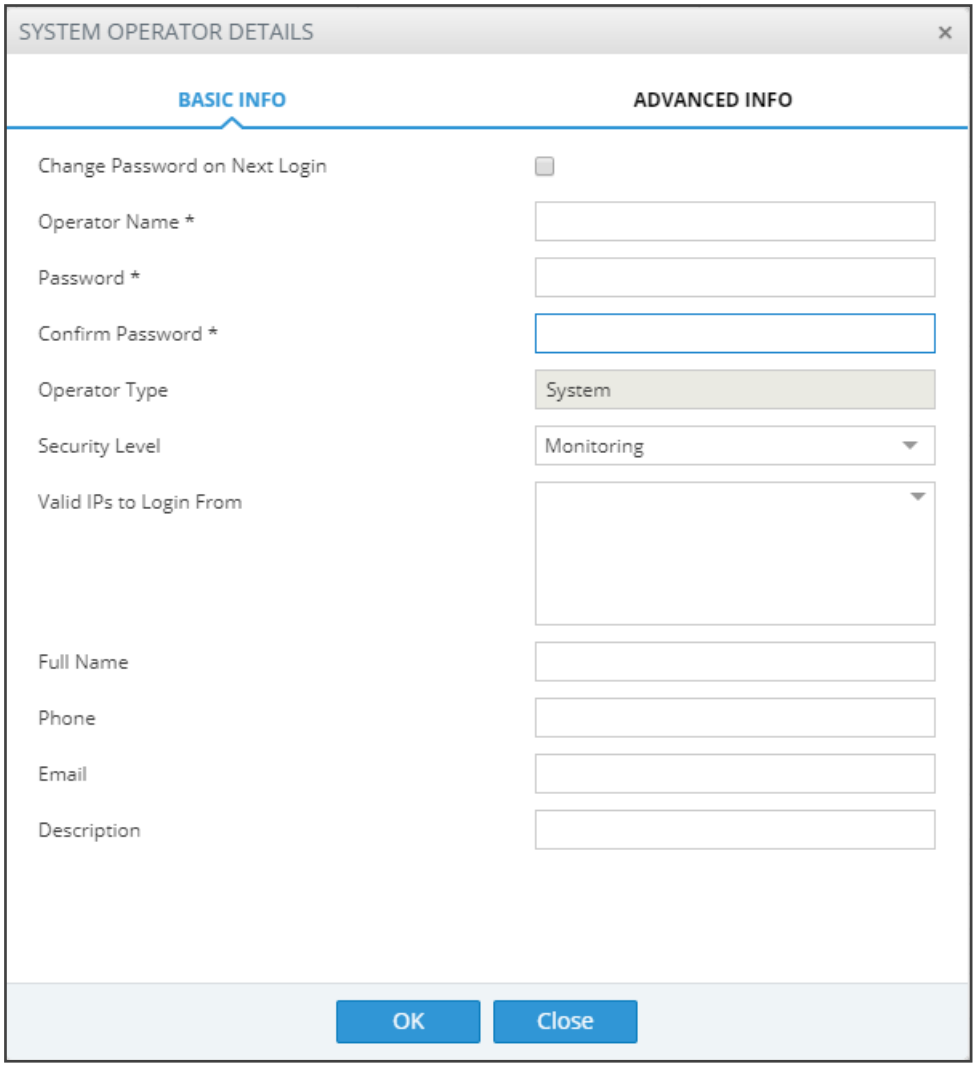


Only a 'system' operator with a security level of 'Admin' can perform tenant management operations (Add/Remove/Update).

➢ 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 2-23: 'System' Operator Settings - Basic Info



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

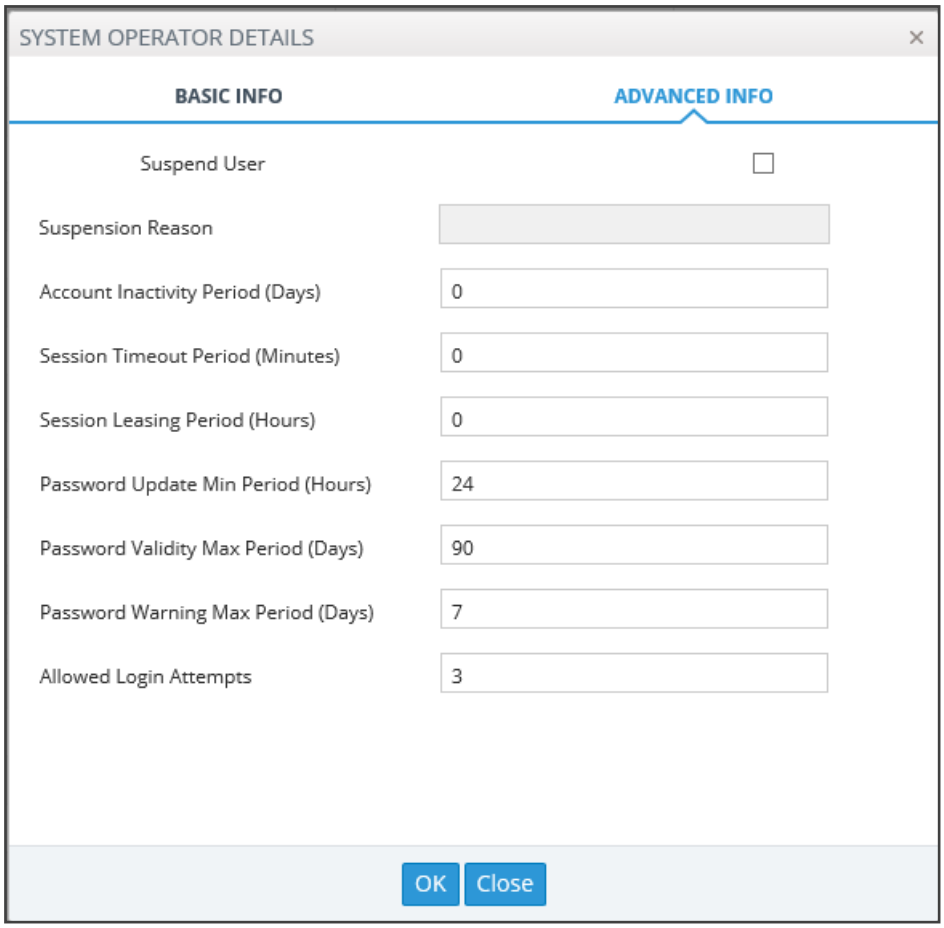
Table 2-7: 'System' Operator Settings - Basic Info

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.

Parameter	Description
User Type	[Read-only] **System** or **Tenant** depending on what you selected in step 2.
Security Level	From the drop-down select: ■ Monitoring (lowest security level) ■ Operator (medium security level) ■ Admin (highest security level) ■ Monitoring Links (Applicable only when adding a 'Tenant' type operator in a deployment whose architecture is ITSP customer multi-tenant architecture - see ITSP Customer Multi-Tenant Architecture on page 6. 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).
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 2-24: 'System' Operator Settings – Advanced Info



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. If you choose **Future Suspension** from the drop-down, the 'Choose suspension date' field is displayed:  Click the calendar icon to define on what date to suspend the 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.

Parameter	Description
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 weeks, their account will not be suspended).
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., clicking, the timer is reset. Default: 0 (GUI always accessible irrespective of 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 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.

6. 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

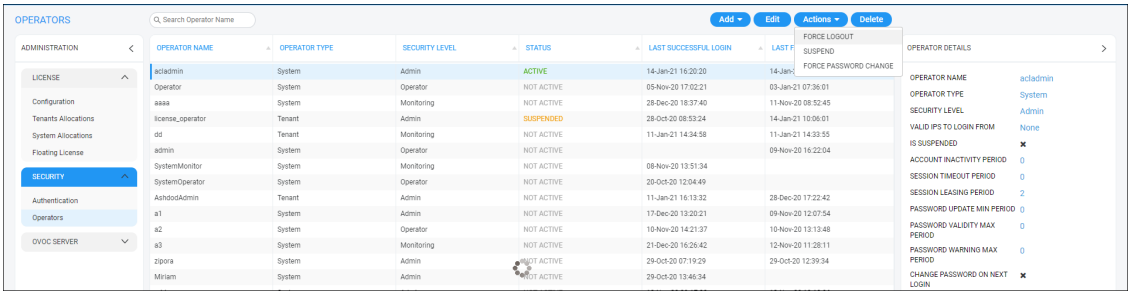
> Applies only to OVOC operators with 'Admin' security level. See Adding an Operator on page 52 for an explanation of the different security levels.

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.

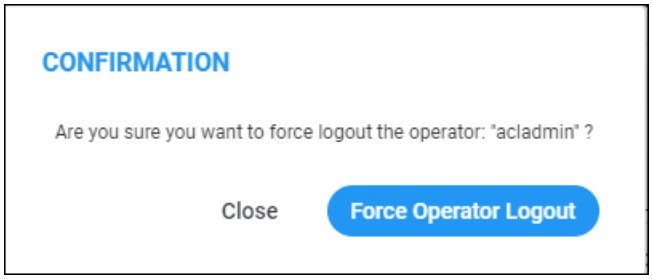
➢ To force an active operator to be logged out:

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

Figure 2-25: Operators page



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**.



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

Adding a 'Tenant' Operator

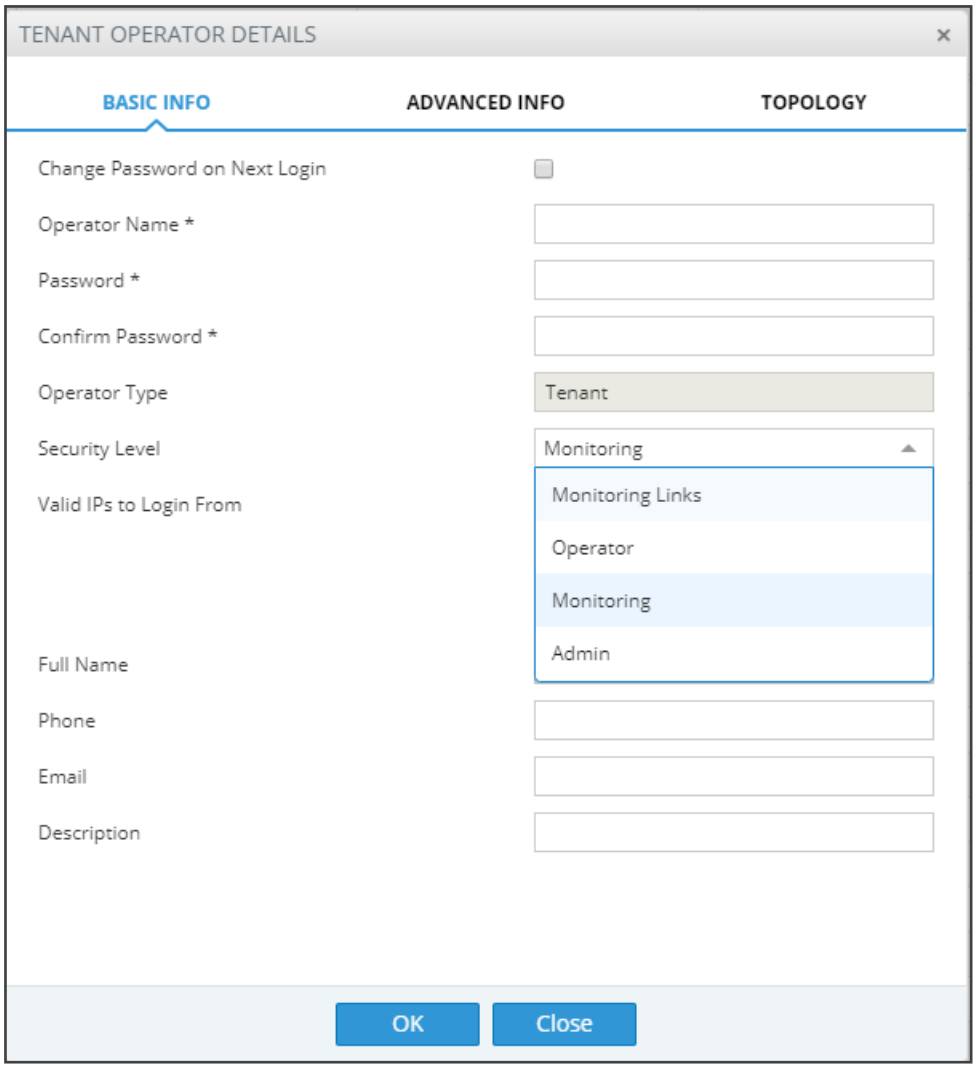
You can add a 'tenant' operator to the OVOC. A 'tenant' operator is typically an enterprise's network administrator whose network does not feature multi-tenancy architecture and whose OVOC application enables management of the enterprise's distributed offices.

> 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:**

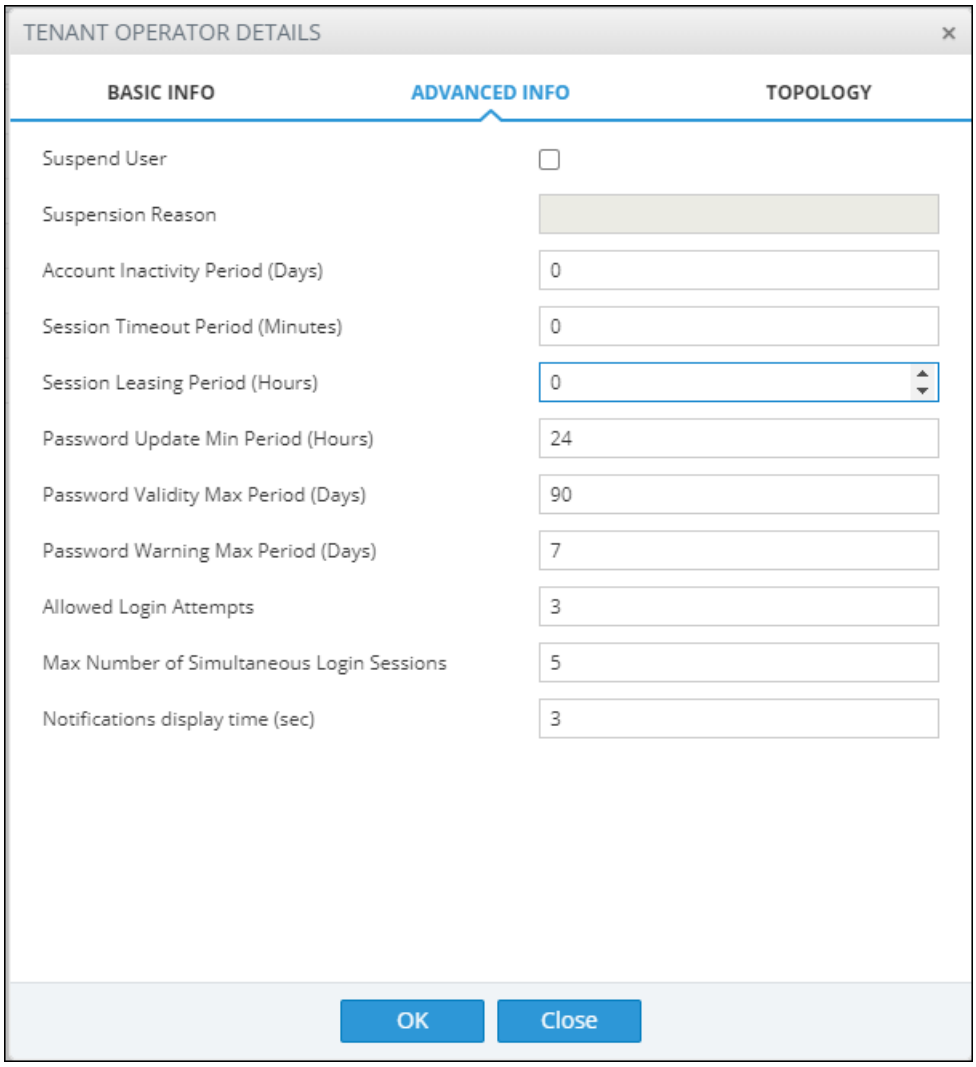
1. In the OVOC, open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Click **Add** and then select **Tenant Operator** from the drop-down menu.

Figure 2-26: 'Tenant' Operator Details – Basic Info



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

Figure 2-27: 'Tenant' Operator Details – Advanced Info



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

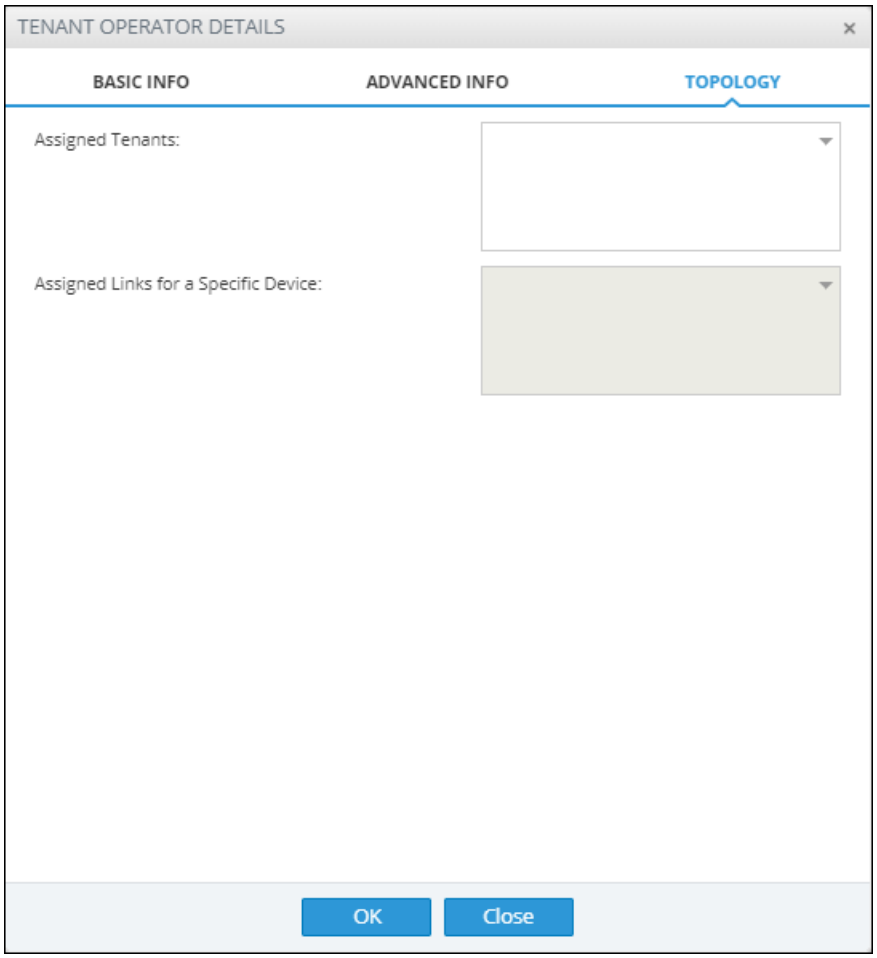
Table 2-9: 'Tenant' Operator Details – Advanced Info

Parameter	Description
Suspend User	Select this option to suspend the 'tenant' operator. If you choose **Future Suspension** from the drop-down, the 'Choose suspension date' field is displayed:  Click the calendar icon to define on what future date to suspend the operator.
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a

Parameter	Description
	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.
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 **Topology**.

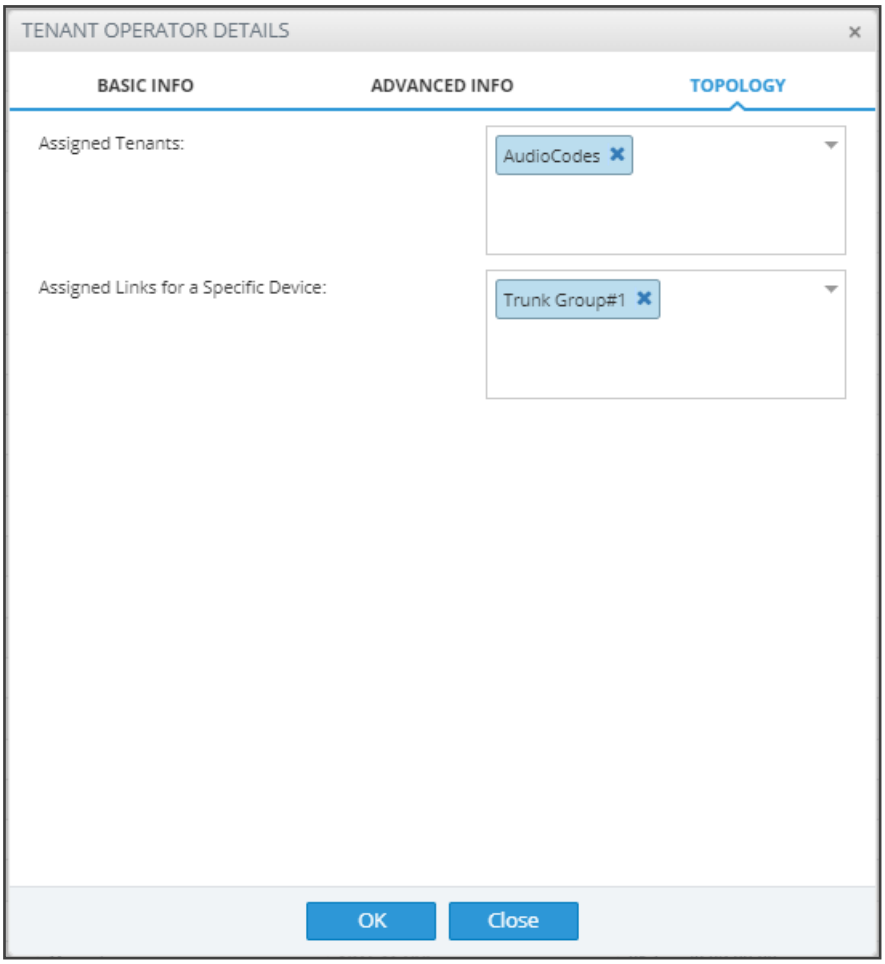
Figure 2-28: 'Tenant' Operator Details – Topology



7. [The screen is only available for the 'tenant' operator]. From the 'Assigned Tenants' drop-down, select a tenant for this operator from the list of tenants defined in the server. Multiple tenants can be selected.
8. [The field 'Assigned Links for a Specific Device' will be displayed only for the operator whose security level is 'Monitoring Links']. From the 'Assigned Links for a Specific Device' drop-down, select links for this operator from the list of links defined in the selected tenant.

- 'Monitoring Links' security level applies only when adding a 'Tenant' type operator in a deployment whose architecture is ITSP customer multi-tenant architecture - see ITSP Customer Multi-Tenant Architecture on page 6.
- 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).

Figure 2-29: 'Tenant' Operator Settings – Tenant Assigned



9. 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

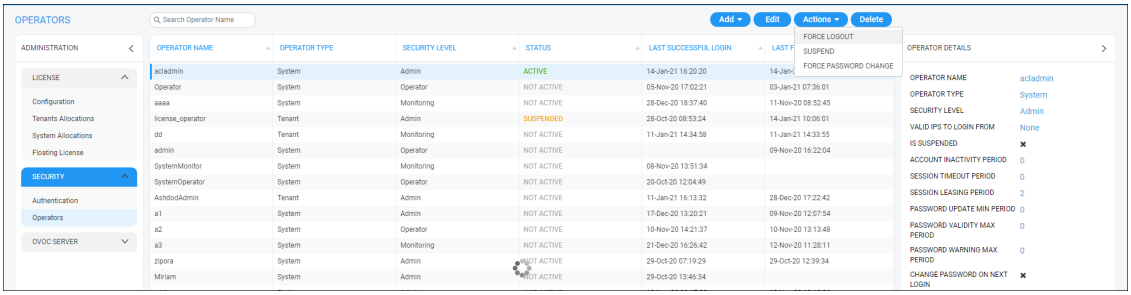
> Applies only to OVOC operators with 'Admin' security level. See Adding an Operator on page 52 for an explanation of the different security levels.

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.

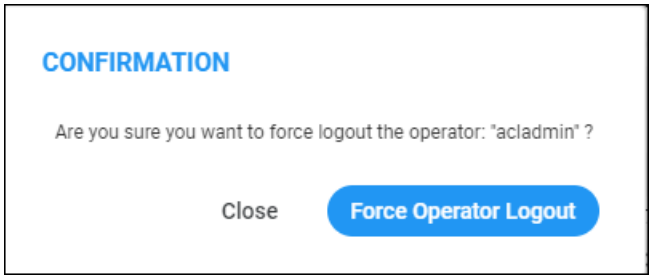
➢ To force an active operator to be logged out:

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

Figure 2-30: Operators page



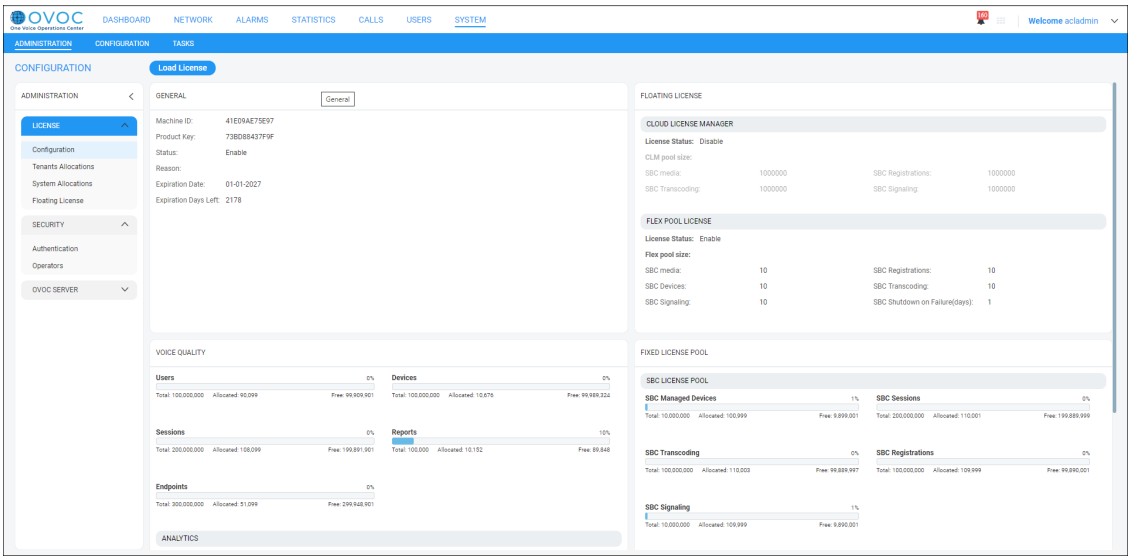
2. Select the active operator to log out; their 'Active' status is indicated in the Status column.
3. From the now enabled 'Actions' drop-down, select **Force Logout**.



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 Making Sure your License Provides the Capabilities you Ordered on page 71 for details.
		Tenants Allocation	See Allocating Licenses to Tenants on page 72 for details.
		System Allocation	See Defining # of Administrator-Defined Reports Produced at System Level on page 74 for details.
		Floating License	See under Managing SBC Licenses on page 174 for details.
	Security	Authentication	Lets you configure LDAP/RADIUS authentication. See Configuring Operator

Tab	Folder	Item	Description
			Authentication on page 38 for details.
		Operators	Lets you add operators to the OVOC. See Adding an Operator on page 52 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 Securing Connections with FQDN or IP Address on page 76.
Configuration	Templates	SNMP Connectivity	See SNMP Connectivity on page 88 for details.
		HTTP Connectivity	See HTTP Connectivity on page 91 for details.
		QoE Thresholds	See QoE Thresholds on page 91 for details.
		QoE Status & Alarms	See QoE Status and Alarms on page 93 for details.
		Perf Monitoring	See Adding a PM Profile on page 276 for details.
	Alarms		See Configuring Alarms Settings on page 95 for details.
	File Manager	Software Manager	See Adding Configuration Files to the OVOC's Software Manager on page 98 for details.
	External Applications		See Connecting Directly to

Tab	Folder	Item	Description
			External Applications on page 106 for details.
	Device Backup		See Enabling Automatic Device Backup Periodically on page 110 for details.
Tasks			See Tasks tab on page 110 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 72 for more information.

Loading the OVOC Server License

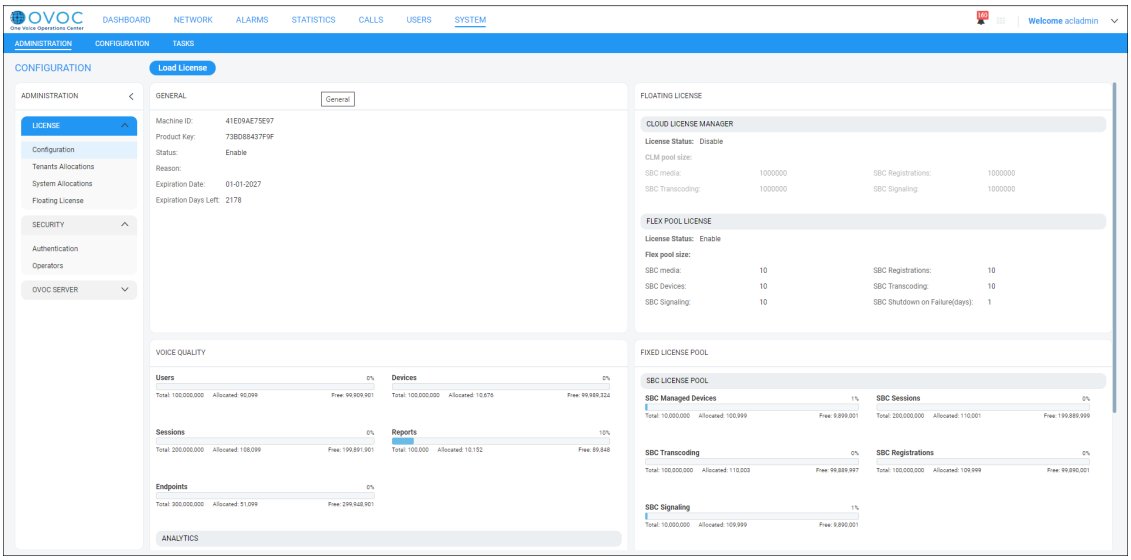
Before Version 7.6.1000, the OVOC Server License could only be loaded to the server using the EMS Server Manager, described in the *One Voice Operations Center IOM Manual*. For operators' convenience, the OVOC Server License as of Version 7.6.1000 can also be loaded from the OVOC GUI to the OVOC server 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 52 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.

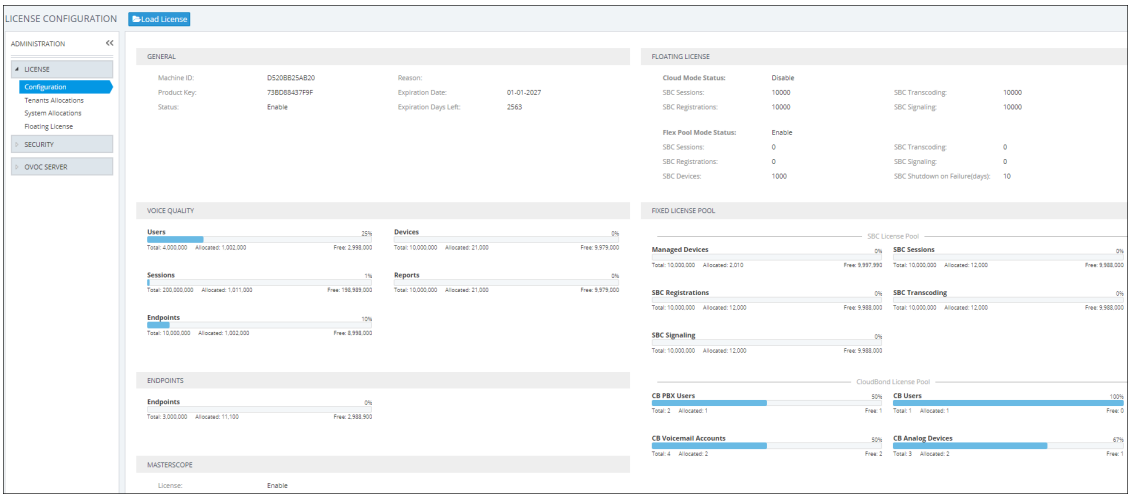
Making Sure your License Provides the Capabilities you Ordered

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



> 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.

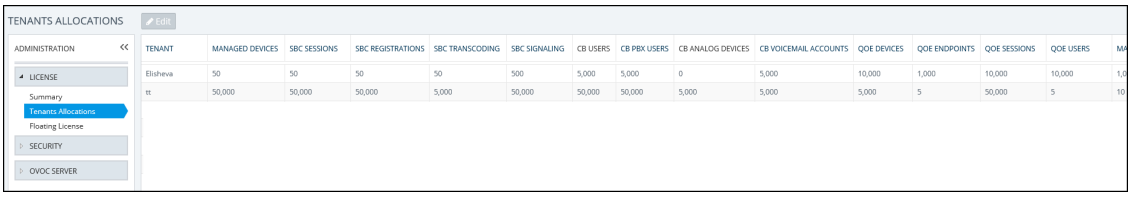
Allocating Licenses to Tenants

After adding tenants as described in Adding a Tenant on page 113, 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 165). The Tenants Allocation page lets you manually allocate licenses to tenants.

➢ To allocate licenses to tenants:

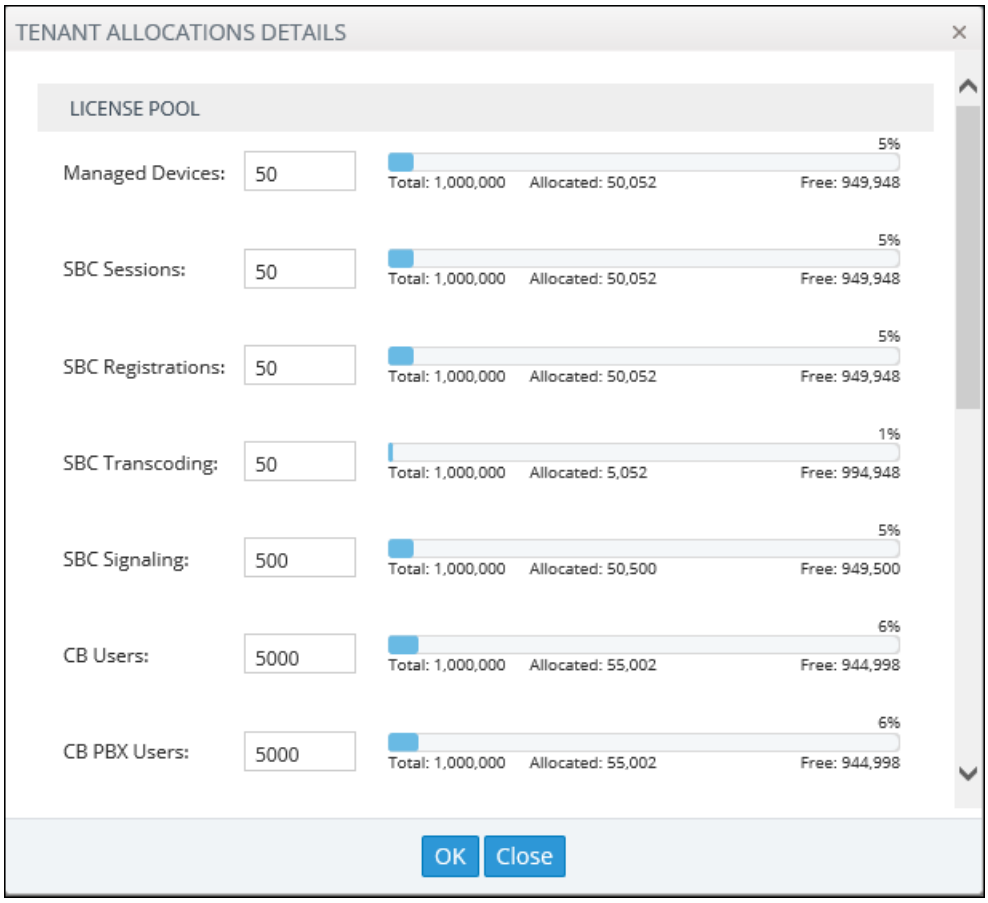
1. Open the Tenants Allocations page (**System** > **Administration** > **License** > **Tenants Allocations**).

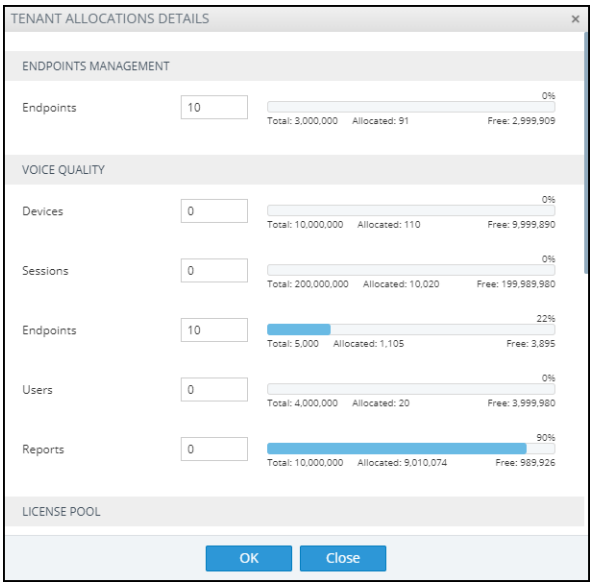
Figure 3-3: Tenants Allocations



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

Figure 3-4: Tenant Allocations Details





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

Defining # of Administrator-Defined Reports Produced at System Level



OVOC's *built-in reports* can be produced without a license but a license is necessary for producing *administrator-defined* reports. See Defining a Report on page 385 for more information.

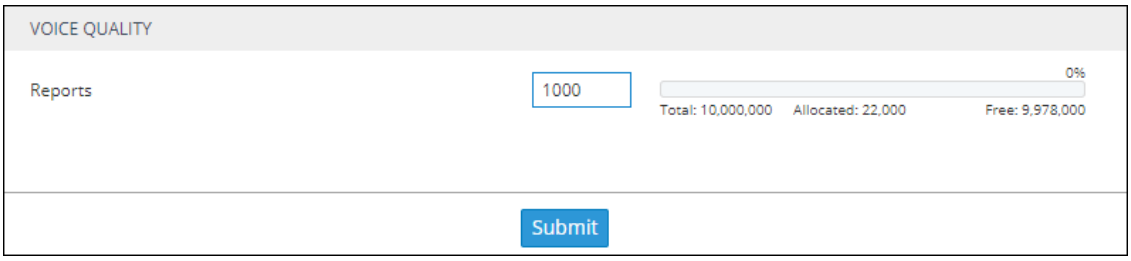
The System Allocations page enables defining the number of administrator-defined reports that can be produced in the OVOC under the license. The value must be allocated to

- tenants as described in Allocating Licenses to Tenants on page 72 (how many administrator-defined reports can be produced in each tenant)
- system as shown here (how many administrator-defined reports can be produced at the system level)

➢ **To define how many operator-defined reports can be produced at the system level:**

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

Figure 3-5: Defining # of administrator-defined reports produced at system level



2. Enter the value you require in the 'Reports' field; the field turns yellow; the 'Allocated' indication increases by the value you entered and the 'Free' indication decreases by the value you entered.
3. Click **Submit**; if operators later exceed this number when defining a new report, they'll receive a notification.

Authenticating Operators

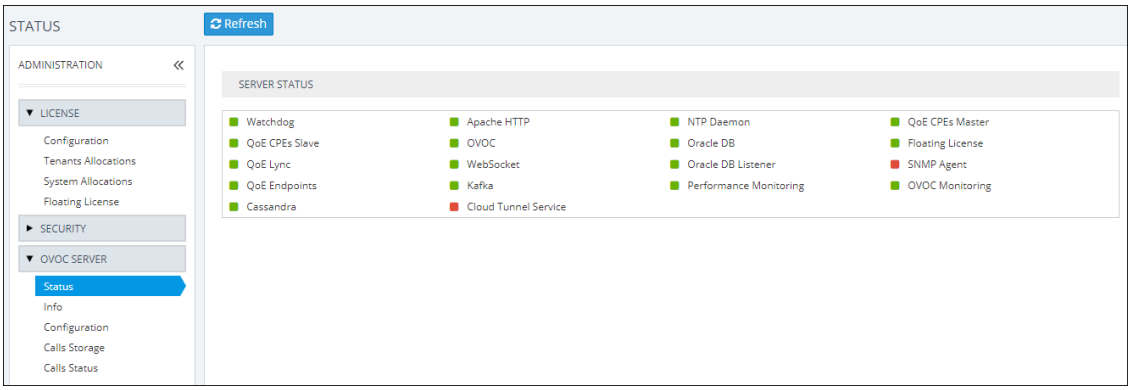
The 'Security' folder's **Authentication** item lets you configure LDAP and RADIUS authentication. See Configuring Operator Authentication on page 38 for detailed information.

The 'Security' folder's **Operators** item lets you add OVOC operators. See Adding an Operator on page 52 for detailed information.

Determining OVOC Server Status

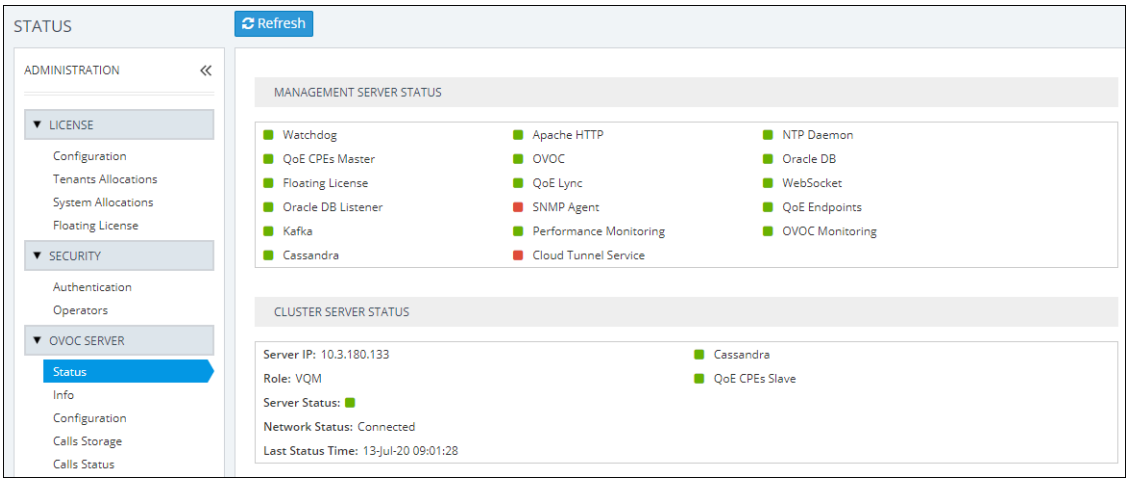
The Server Status page (**System** > **Administration** > **OVOC Server** > **Status**) lets you determine at-a-glance status information about the OVOC server. The feature saves operators from having to log in to the EMS Server Manager. The same information is presented, only in friendlier format.

Figure 3-6: Server Status page



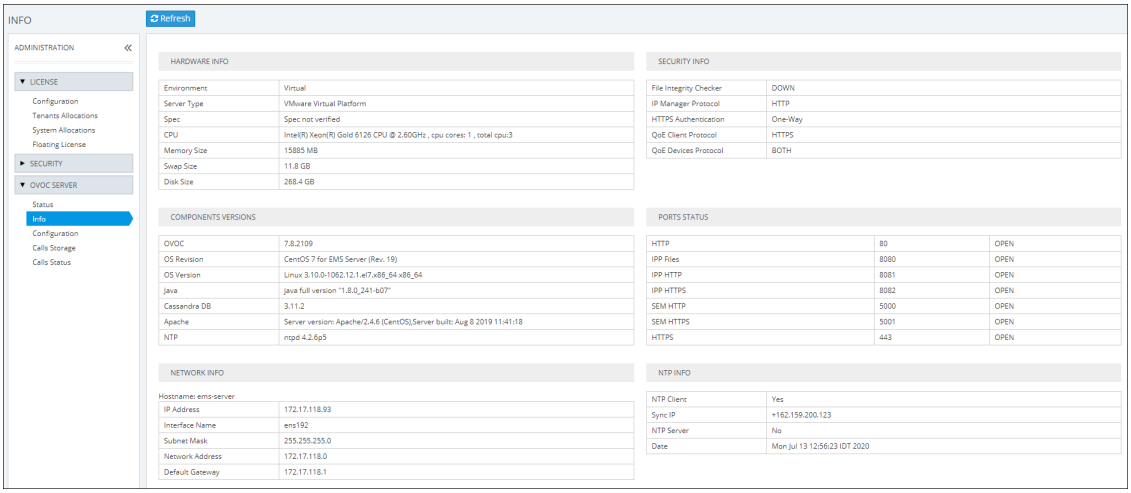
When OVOC cluster mode is installed, the Status page (**System** > **Administration** > **OVOC Server** > **Status**) displays the statuses of all cluster servers. The figure below shows an example of a single additional server but multiple additional servers are supported for high scale capacity.

Figure 3-7: Cluster Server Status



The Server Info page (**System** > **Administration** > **OVOC Server** > **Info**) presents information about the OVOC server including , including hardware info, components versions, NTP info, security info, ports status 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 3-8: Server Info page



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.

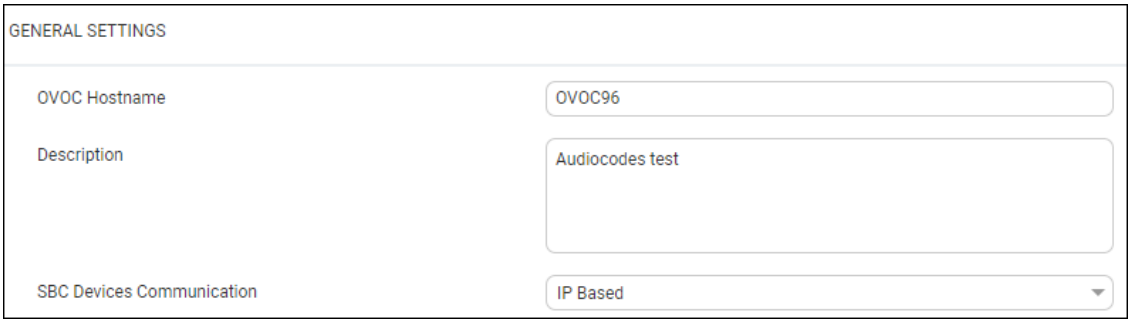
Supported connections are:

- Device - OVOC server
- OVOC - LDAP Active Directory

➢ **To implement the feature:**

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

Figure 3-9: Server Configuration



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

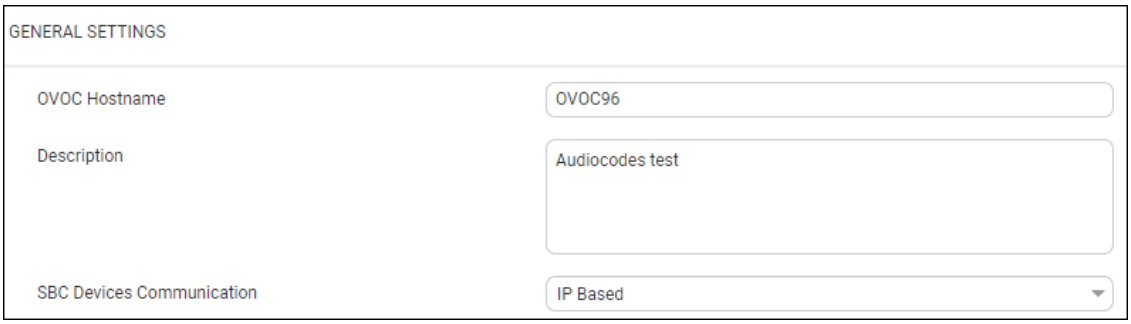
Providing a Description to be Forwarded in Alarm Info

The OVOC allows operators to provide a 'Description' that will be forwarded in the Alarm Info to facilitate more effective management of alarms from the OVOC server.

➢ **To provide the description:**

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

Figure 3-10: Server Configuration



2. In the 'Description' field shown in the preceding figure, configure a description for OVOC server alarms (such as disk space or Oracle partition size) that are forwarded to SNMP destinations. For more information, see the *One Voice Operations Center Northbound Integration Guide*.

The configuration in the 'Description' field should be mirrored in the Alarm Forwarding rule - see under Forwarding Alarms on page 244 for more information. AudioCodes FAEs then use these as *Customer #s*. Each alarm from the OVOC server opens a ticket to AudioCodes or to the customer, depending on with whom the OVOC is deployed.

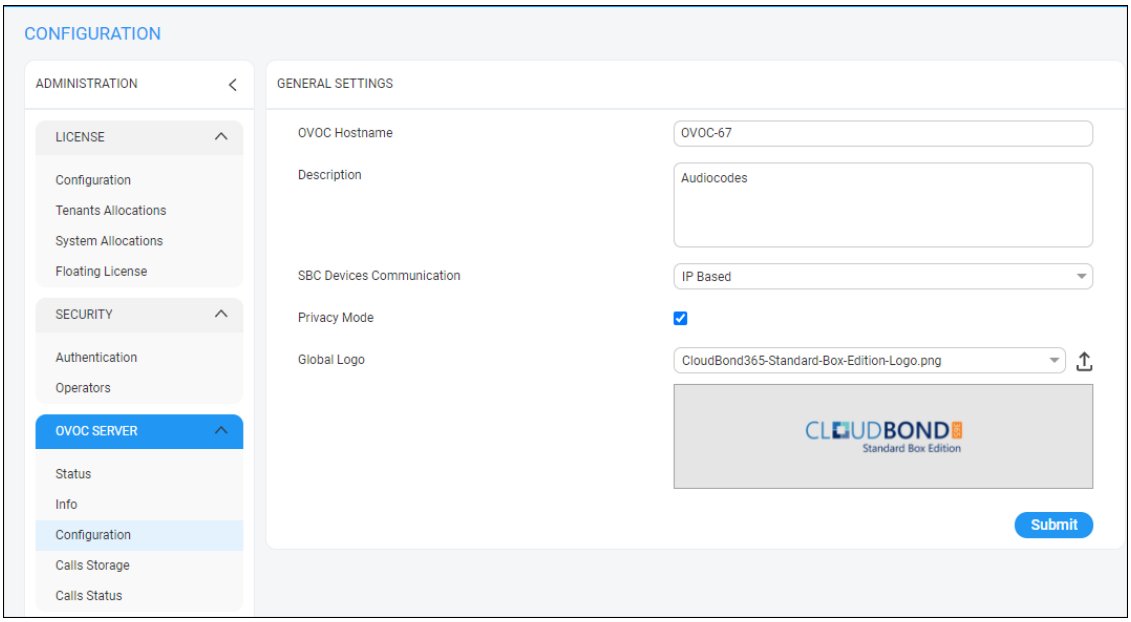
Configuring Privacy Mode, Concealing Users Calls Details

The OVOC allows tenant and system operators whose Security Level is configured as 'Monitor' or 'Operator' to conceal from view call details and user information that is exposed in calls.

➢ To configure Privacy Mode:

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

Figure 3-11: Server Configuration



2. Under General Settings, select the 'Privacy Mode' option and click **Submit**.
   - Last digits in users' phone numbers are concealed from view
   - Information about callers and called parties in the Call Details page is replaced by ***
   - User / URI reports are disabled
   - Specific information on any user cannot be retrieved
   - User tables and statistics are concealed from view
   - SIP ladders and user call information are concealed from view

Uploading a Global Logo to Display in Report Results

Network administrators can upload a global logo to be displayed globally, across all report results irrespective of tenant, from the global (system) settings (**System** > **Administration** > **OVOC Server** > **Configuration**). Logos displayed in report results can facilitate management for network administrators.

➢ To upload a global logo:

1. Open the Server Configuration page (**System** > **Administration** > **OVOC Server** > **Configuration**) and locate the 'Global Logo' parameter under 'General Settings'.

Figure 3-12: Global Logo



2. Click and then navigate to the location in which the image file is stored.
3. Click **Submit**; the logo image file is added to the Software Manager.

- If the logo image file has already been uploaded to the OVOC server and is displayed in the Software Manager, you can select it from the drop-down list.
- See also Defining a Report on page 385 for related information.
- See also Adding Configuration Files to the OVOC's Software Manager on page 98 for related information.
- See also Editing a Tenant - Defining a Logo on page 122 to define a logo to be displayed in report results related to a specific tenant.

Customizing Call Storage

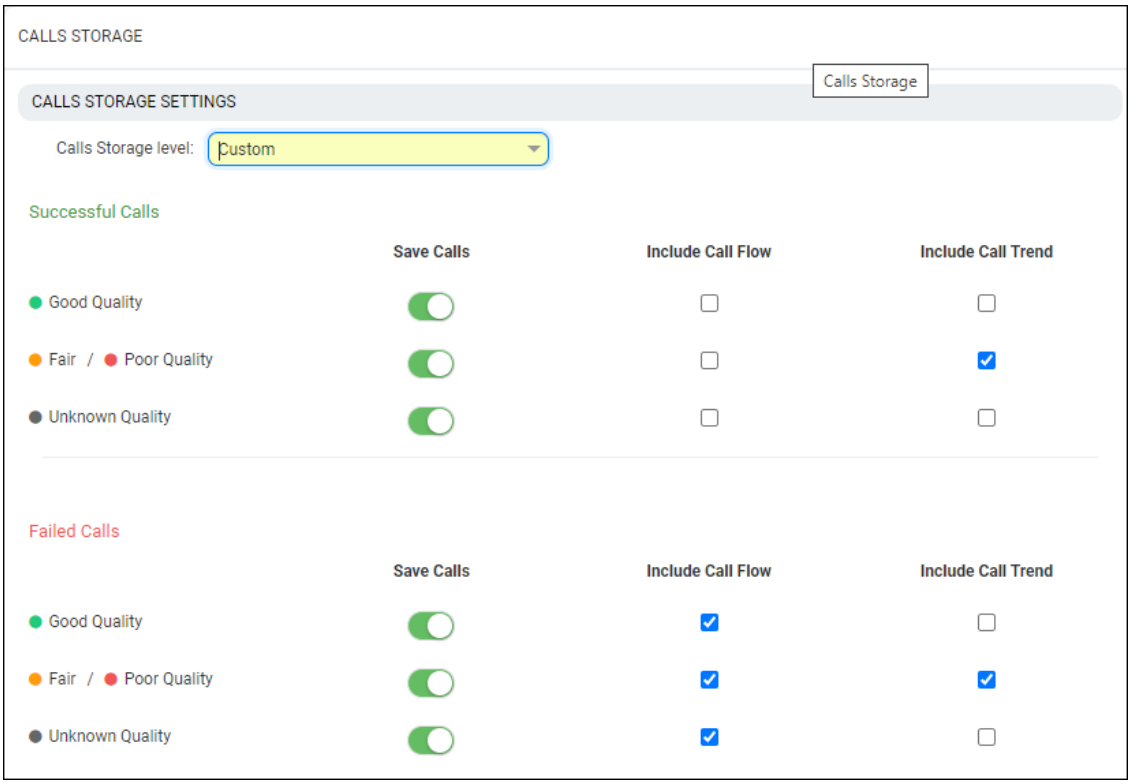
The OVOC's Server Call Storage page allows operators whose security level is configured as 'System' to customize the storage of calls on the OVOC server according to successful calls and/or failed calls (call performance) and the quality of the calls (good, fair/poor and/or unknown) in these two categories.

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 3-13: Calls Storage



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 3-14: Calls Storage Level - Minimal

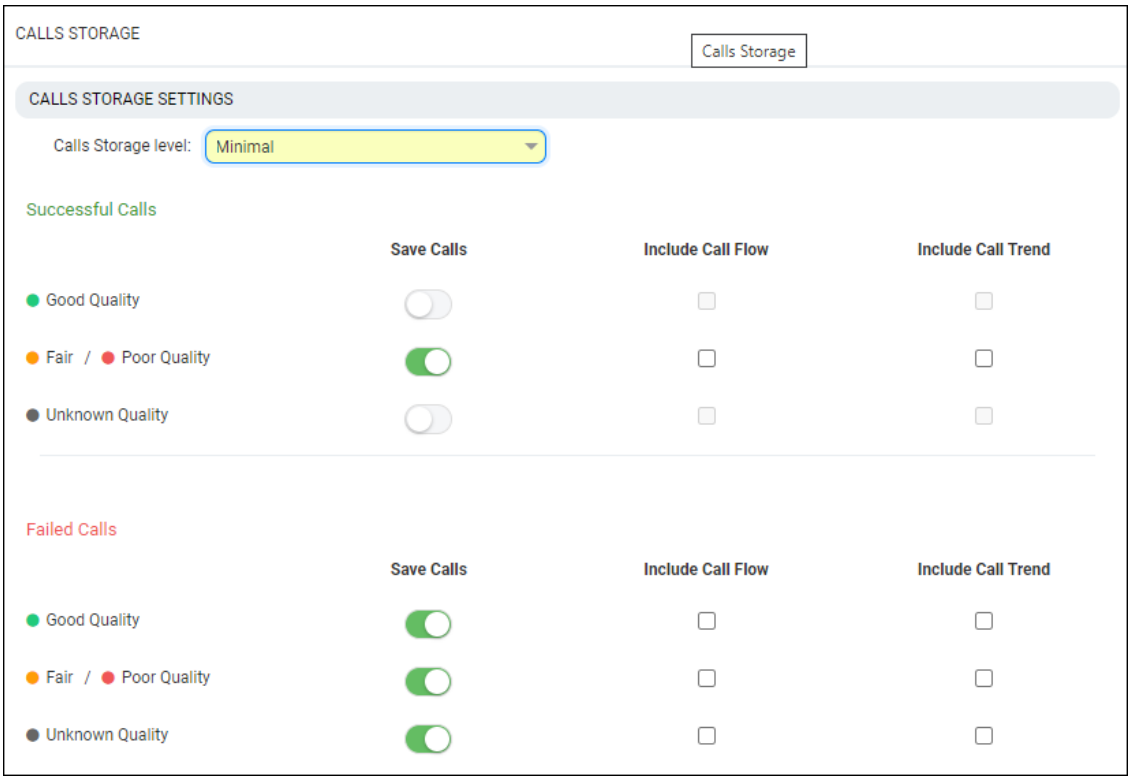
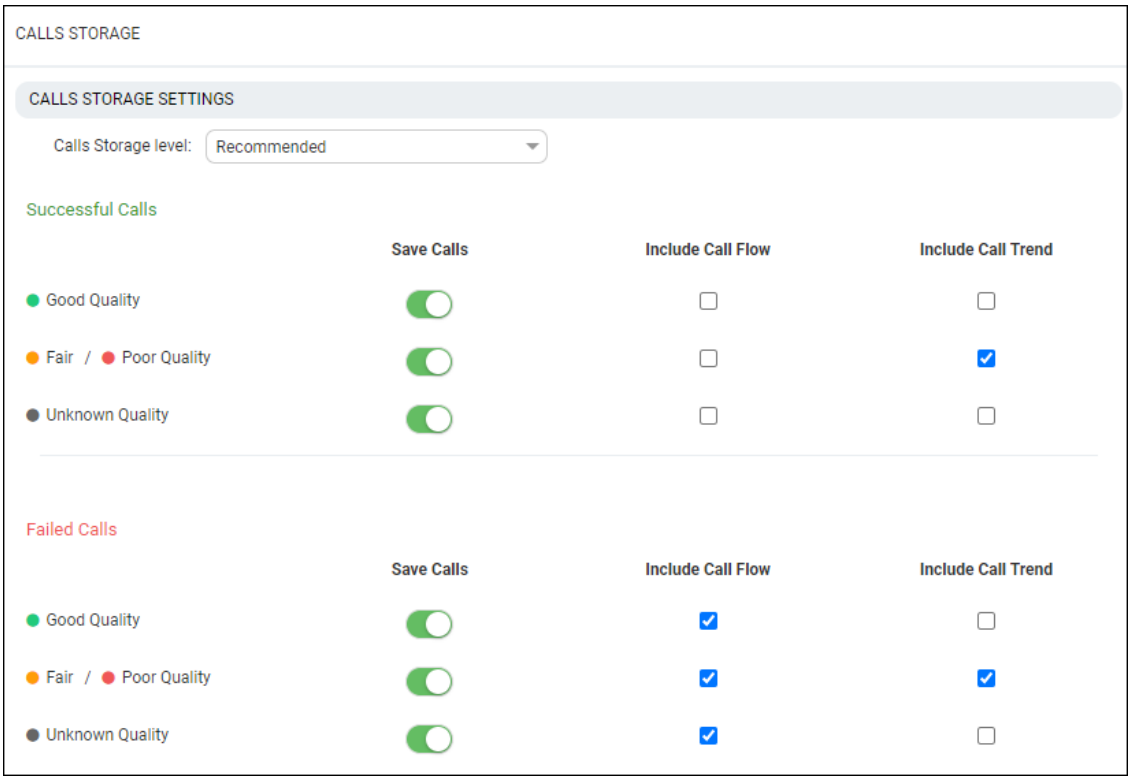


Figure 3-15: Calls Storage Level - Recommended



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
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	Yes	No	Yes

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
	(fair/poor)			
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

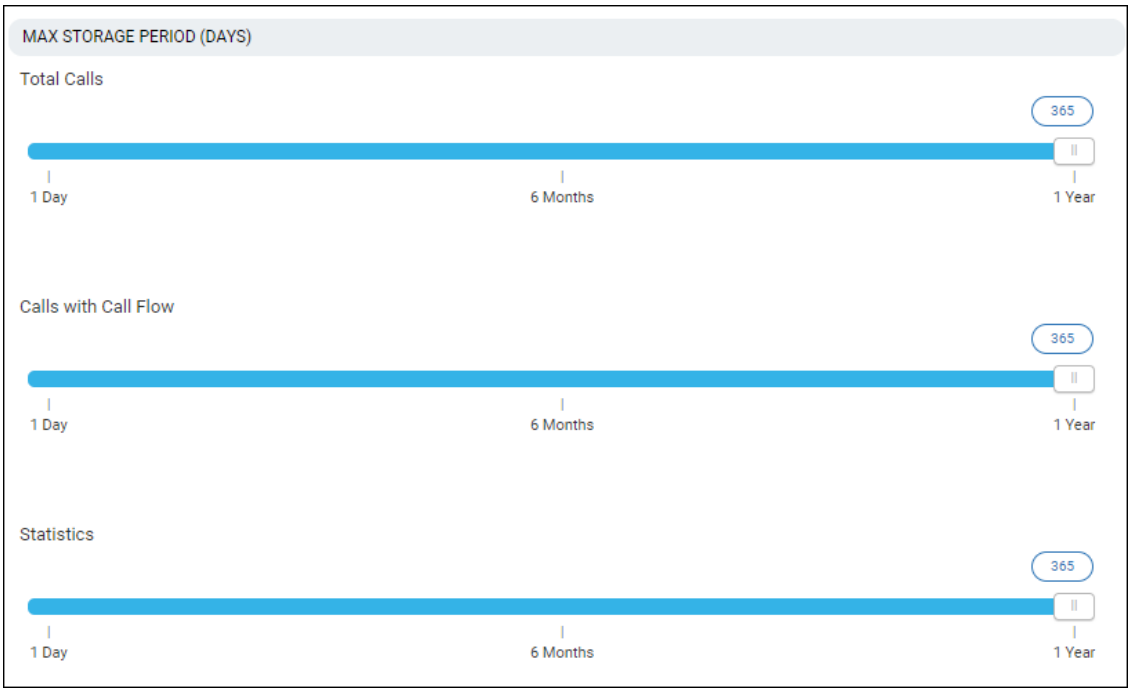
Customizing Maximum Storage Period

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 3-16: 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.

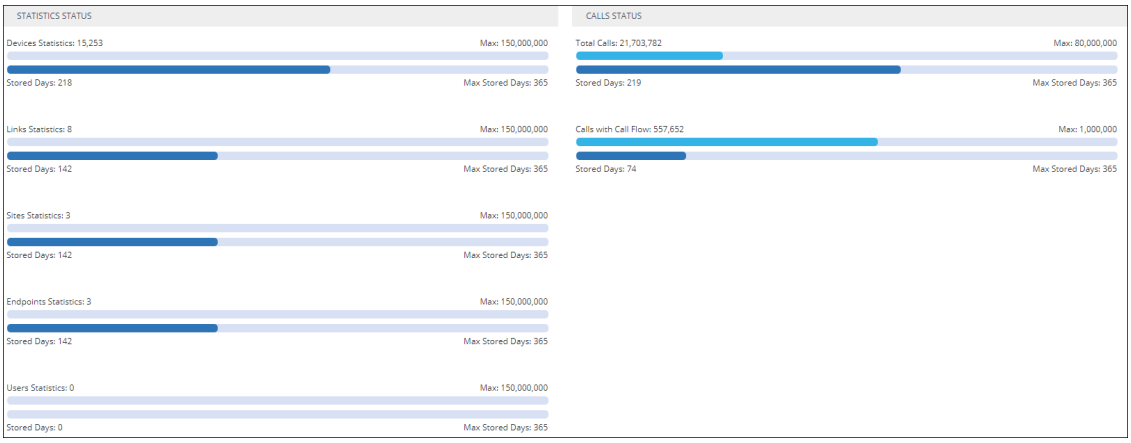
Viewing Calls Status

The Calls Status page displays the statuses of statistics collected on database entities as well as the statuses of statistics collected on calls and on calls with calls flow. Network administrators can use the page as reference to determine OVOC server database status.

➢ To view statuses:

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

Figure 3-17: Server Calls Status



2. [Refer to the preceding figure] View on the left side of the page the statuses of statistics on the following entities (from top to bottom): Devices, Links, Sites, Endpoints and Users.
3. View (for example) the topmost entity displayed: Devices
   - 15,253 statistics on all devices in the network currently saved in the OVOC server database, out of a maximum of 150 million. 15,253 indicates the number of stored statistics per the entity 'Device', per 5 minute interval. [The number of stored statistics per other entities - Links, Sites, Endpoints - per five minute interval, are displayed below 'Devices'].
   - The Maximum Stored Days is indicated as 218 out of a maximum of 365 (configured in the Calls Settings Storage page as shown in Customizing Call Storage on page 79); the oldest statistics on devices in the OVOC server database are 218 days old; after a year's storage, the OVOC deletes the database; only one year maximum is stored.
4. View on the right side of the page the Calls Status section.
   - 21,703,782 indicates the total number of calls currently saved in the OVOC server database out of a maximum of 80 million calls.
   - The Stored Days is indicated as 219 out of a maximum of 365; the oldest calls are 219 days old; after a year's storage, the OVOC deletes calls from the database; only one year is stored.

- 557,652 indicates the calls with call flow (i.e., with SIP ladder) currently saved in the OVOC server database.
- The maximum # of statistics on calls /calls with call flow depends on the server specification (Baremetal, low VM, high VM, etc.).
- The Maximum Stored Days is configured in the Calls Settings Storage page as shown in Customizing Call Storage on page 79.

Configuration tab

The 'Configuration' tab lets you:

- configure global system templates (see Configuring Templates below)
- configure alarms settings (see Configuring Alarms Settings on page 95)
- add software and auxiliary files (see Adding Configuration Files to the OVOC's Software Manager on page 98)
- open external applications (see Connecting Directly to External Applications on page 106)
- back up (see Backing up a Device's Configuration using Backup Manager on page 157)

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 91)
- QoE Thresholds (see QoE Thresholds on page 91)
- QoE Status & Alarms (see QoE Status and Alarms on page 93)
- Performance Monitoring Template (see Adding a PM Template on page 271)

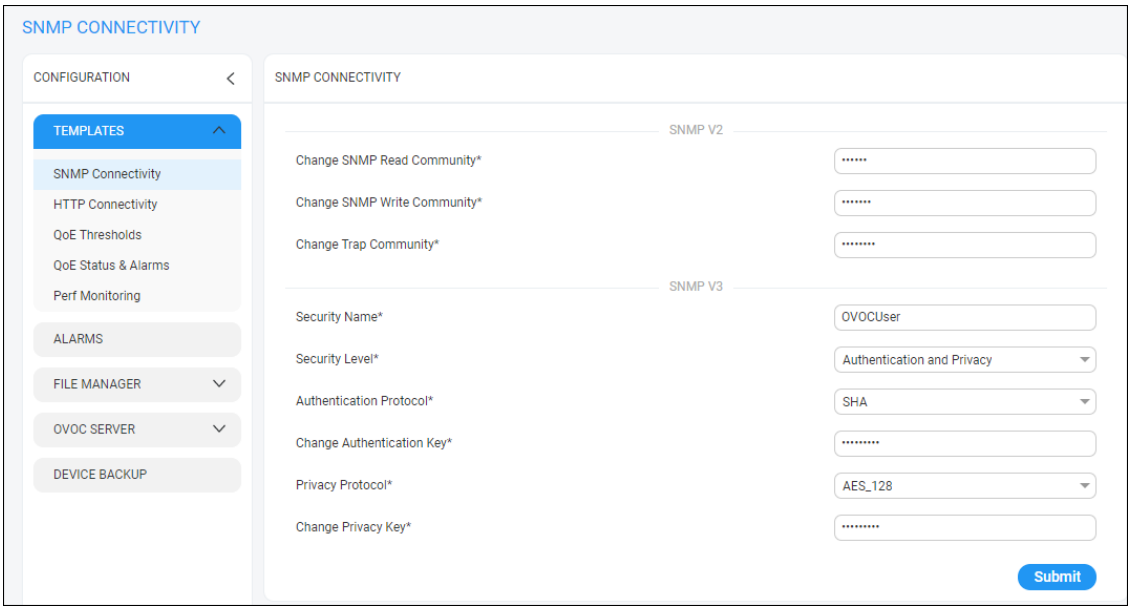
SNMP Connectivity

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 3-18: 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
SNMP v2	
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.
SNMP v3	
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the drop-down, select either: ■ **Authentication and Privacy** (default) ■ **No Security** ■ **Authentication**
Authentication Protocol	From the drop-down, select either:

Parameter	Description
	■ **SHA** (default) ■ **MDS** ■ **No Protocol**
Authentication Key	Enter an Authentication Key. Default: 123456789.
Privacy Protocol	From the drop-down, select either: ■ **AES 128** (default) ■ **DES**
Privacy Key	Enter a Privacy Key. Default: 123456789.

3. Click **Submit**.

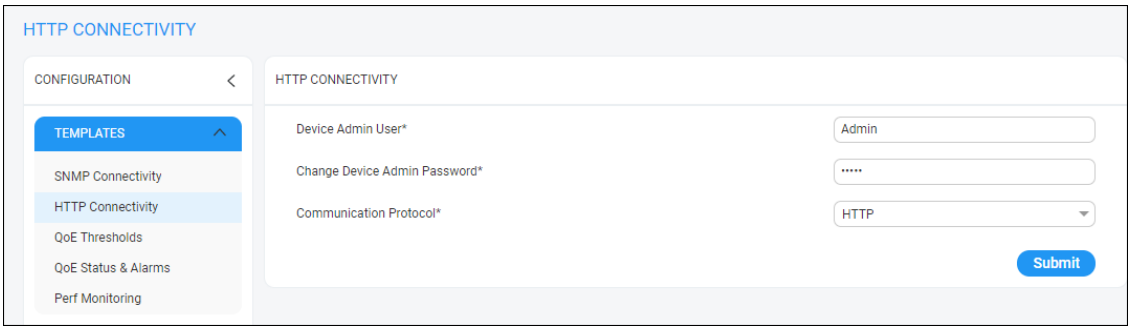
HTTP Connectivity

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 3-19: 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: **Admin**. Password - "Admin".
Device Admin Password	Enter the Web server password. Example: **Admin**.
Default Connectivity	From the drop-down, select either: ■ **HTTP** (default) ■ **HTTPS**

3. Click **Submit**.

QoE Thresholds

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

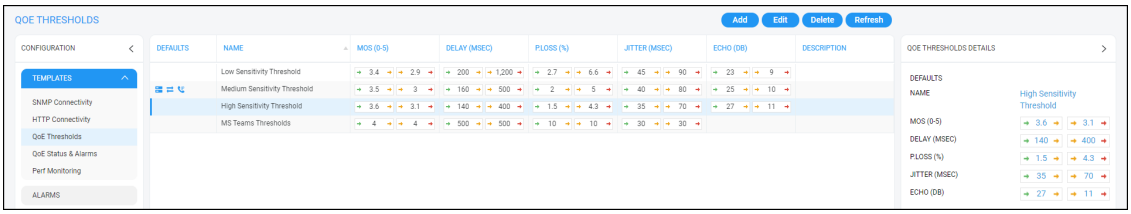
[For information on how to configure QoE Thresholds profiles *per tenant*, see Managing QoE Thresholds Profiles per Tenant on page 359]

Four QoE Thresholds templates (Low Sensitivity | Medium Sensitivity | High Sensitivity | MS Teams) 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 3-20: QoE Thresholds Templates



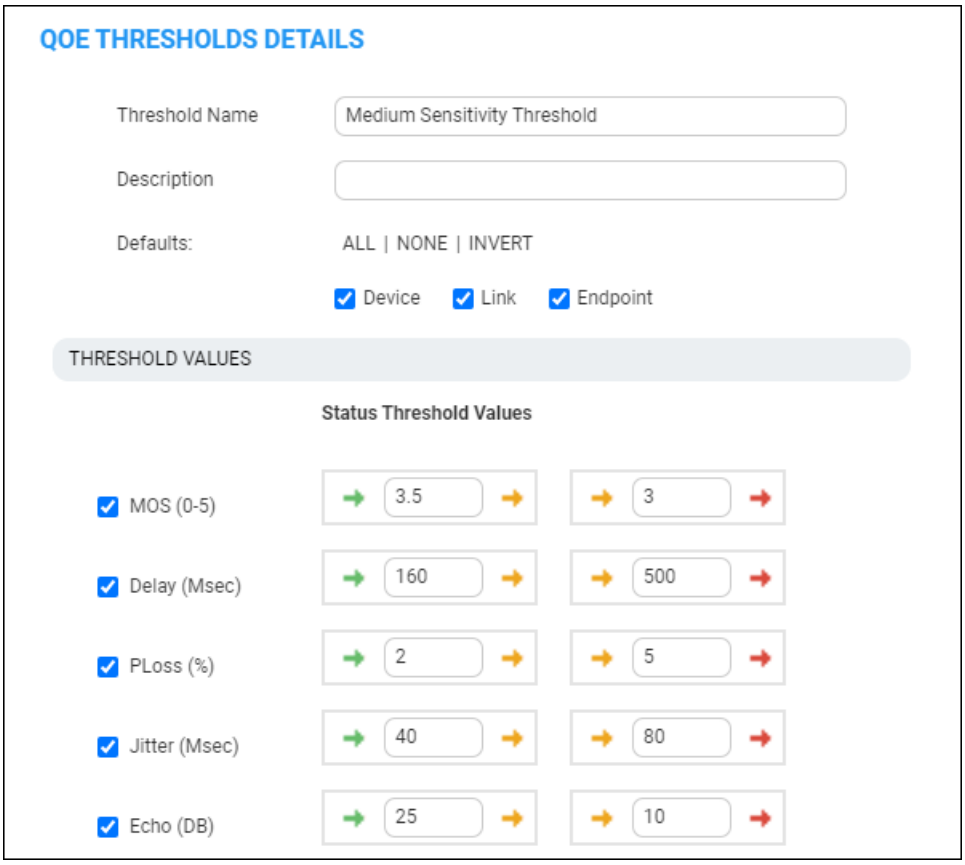
In the page, you can see four *global* (system-wide) QoE thresholds templates displayed. Each consists of threshold values set for the voice quality metrics of MOS, Delay, Packet Loss, Echo and Jitter, for each call quality category of 'Poor', 'Fair' and 'Good'. Use the following table as reference to 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.
MS Teams Threshold	Threshold values representing recommended data for the 'MS Teams' threshold. For Teams devices, AudioCodes recommends you use the Microsoft Teams threshold. It's a threshold that is added by default to each tenant. It enables calculating the quality of Teams calls. Manually attach Teams devices to the threshold as shown under Adding a QoE Thresholds Profile per Tenant on page 362.

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

Figure 3-21: QoE Thresholds Settings



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 366.

➢ 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 3-22: QoE Status and Alarms



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 (%)	**x** **y** indicates that green changes to orange ('Major' severity) when the **x** percentage of failed calls is exceeded and orange changes to red ('Critical' severity) when the **y** percentage of failed calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 366).
Poor Quality Calls (%)	**x** **y** indicates that green changes to orange ('Major' severity) when the **x** percentage of poor quality calls is exceeded and orange

Page Indications	Description
	changes to red ('Critical' severity) when the **y** percentage of poor quality calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 366).
Average Call Duration (seconds)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** seconds call duration is exceeded and orange changes to red ('Critical' severity) when **y** seconds call duration is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 366).
Bandwidth Rule (Kbps)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** bandwidth is exceeded and orange changes to red ('Critical' severity) when **y** bandwidth is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 366).
Maximum Concurrent Calls Rule (#)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** concurrent calls is exceeded and orange changes to red ('Critical' severity) when **y** concurrent calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 366).

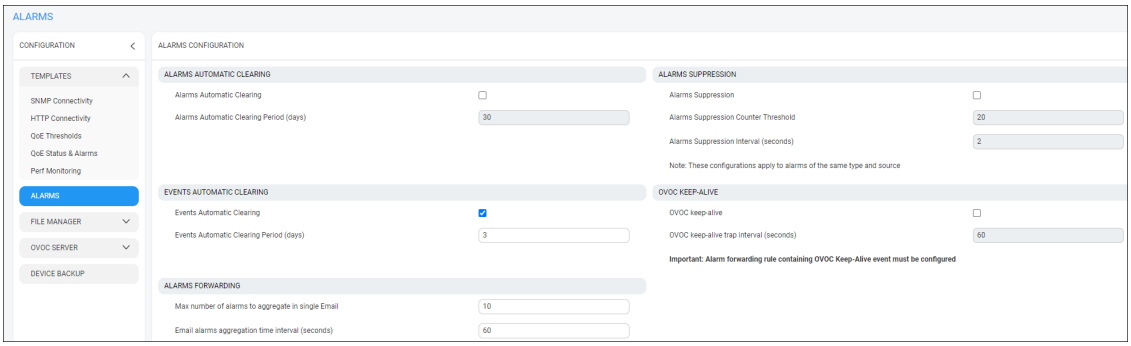
Configuring Alarms Settings

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 3-23: Alarms Settings



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

Table 3-10: Alarms Settings

Setting	Description
Alarms Automatic Clearing	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. Use this setting to prevent historical, dated alarms from cluttering the Alarms page.
Alarms Automatic Clearing Period (Days)	[Only relevant if the 'Alarms Automatic Clearing' option is selected] 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.
Events Automatic Clearing	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). 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.
Events Automatic Clearing Period (days)	Events are by default cleared every three days. You can change the default to suit your requirements.
Max number of alarms to aggregate in single Email	If an alarms forwarding rule is configured (under Alarms > 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

Setting	Description
	60 seconds, then after 60 seconds, five alarms will be raised according to the alarms forwarding rule and five aggregated alarms will be forwarded.
Email alarms aggregation time interval (seconds)	If an alarms forwarding rule is configured (under Alarms > 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.
Alarms Suppression	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.
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

Setting	Description
	different interval to suit your requirements.
Internal Mail Server From Address	If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'From Address'. For example, if you configure **john.brown@enterprisename.com** for this parameter and you configure **John Brown** 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: **john.brown@enterprisename.com < John Brown >** See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under Forwarding Alarms on page 244.
Internal Mail Server Real Name	If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'Real Name'. For example, if you configure **John Brown** for this parameter and you configure **john.brown@enterprisename.com** 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: **john.brown@enterprisename.com < John Brown >** See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under Forwarding Alarms on page 244.

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.)

Logo image files to be displayed in reports results:

- System files (after uploading a global logo file to be displayed in report results as shown in Uploading a Global Logo to Display in Report Results on page 78)
- Tenant file (after uploading a logo image file to be displayed *per specified tenant* in report results as shown in Editing a Tenant - Defining a Logo on page 122)

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)	■ 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. ■ Add a file and assign it to a specific tenant. These files will be visible to both 'tenant' and 'system' operator types. ■ Download any file visible by the tenant (Added by 'tenant' and 'system' operator types) to any device in the tenant. ■ Remove any file added by 'tenant' and 'system' operator types.
Tenant (except operators with 'Monitoring' security level)	■ Add any file. This file will be assigned only to the tenant. These files will be visible to both 'tenant' and 'system' operator types. ■ Download any file visible by the tenant to the devices in the tenant. ■ Remove any file added by a 'tenant' operator type.

- Only one SBC software file (cmp) with the same version for a specific product type can be added to a tenant. The CentOS version can be 6 or 8. See also Adding a cmp File on the next pagefor more information.
- 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

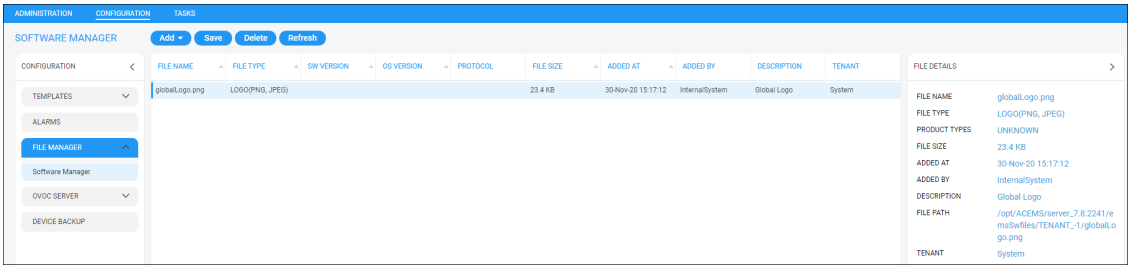
You can add the ini file to the OVOC's Software Manager in order to perform initial configuration of device parameters which cannot be configured after defining the device in the OVOC. When loading the ini file to the device, operators can choose either:

- 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:

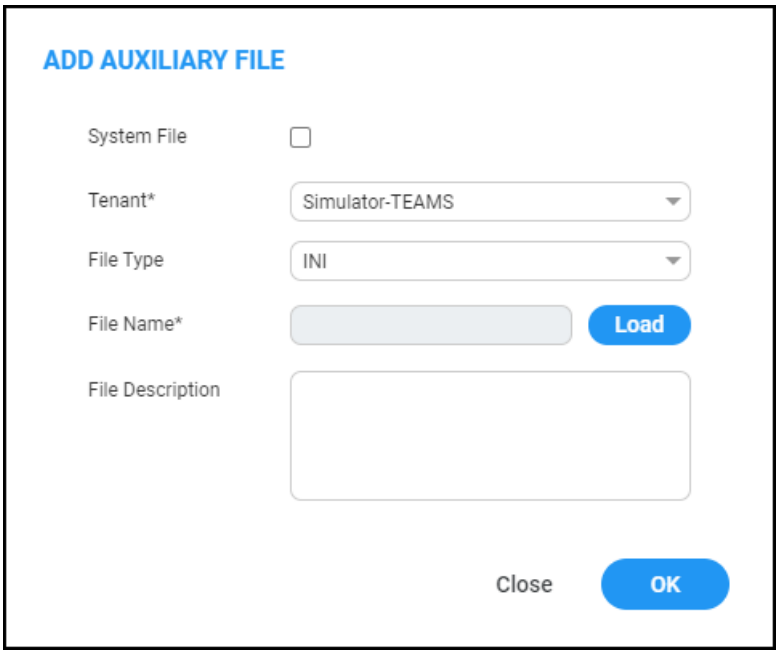
1. Open the Software Manager page (**System** > **Configuration** > **File Manager** > **Software Manager**).

Figure 3-24: Software Manager



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

Figure 3-25: 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 **Load** 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.

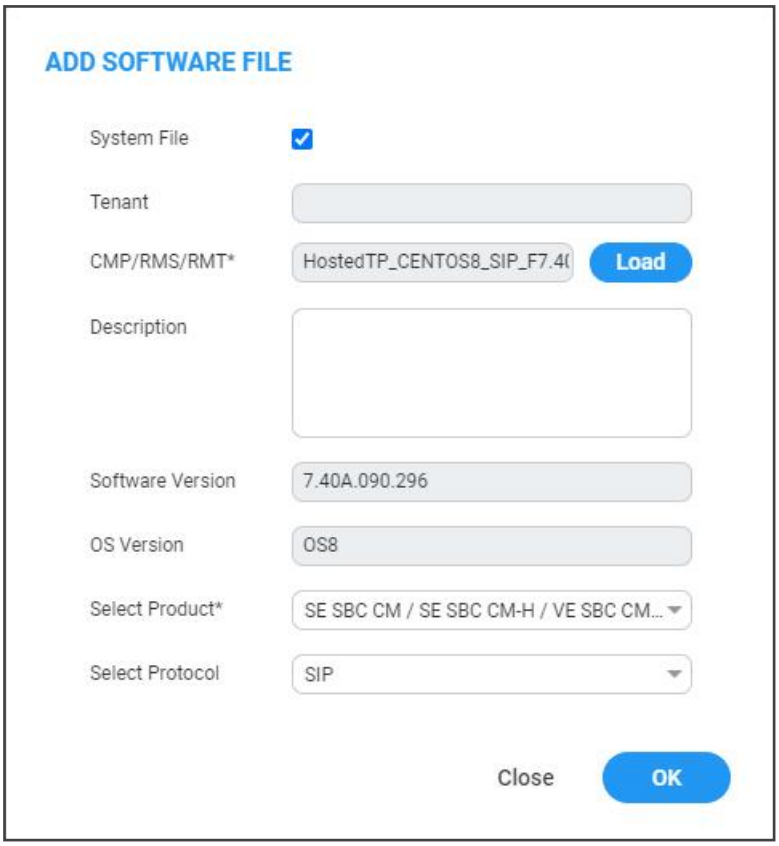
Adding a cmp File

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 3-26: 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 **Load** to navigate 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 read-only 'Software Version' field, view the version of the cmp software file. The field is automatically defined after selecting the cmp or rmt/rms file.
7. In the read-only 'OS Version' field, view the CentOS version for Software SBC (6 or 8).
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.

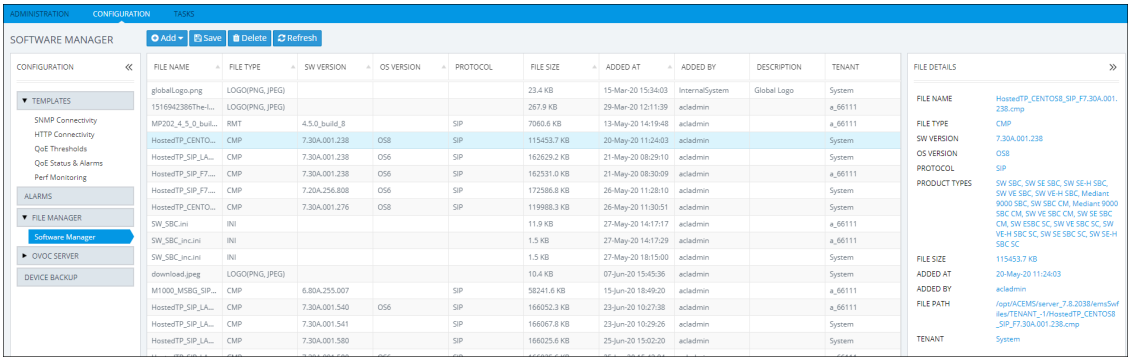
Viewing cmp File Details in Software Manager

After adding firmware (cmp) files to the OVOC to load to devices as shown in Adding a cmp File on the previous page, you can view all files and view each file's details in the Software Manager.

➢ To view cmp files and a file's details:

1. Open the OVOC's Software Manager page (**System** > **Configuration** > **File Manager** > **Software Manager**) and then select the cmp file whose details you want to view.

Figure 3-27: File Details



2. View the columns in the page; they display the same file information as the File Details pane on the right side of the page.
3. Use the table as reference.

Table 3-12: CMP Columns / File Details

Column / File Detail	Description
File name	The name of the file. See also Adding a cmp File on page 101.
File Type	CMP
SW Version	The CMP file version
OS Version	The CentOS version for the Software SBC: ■ OS6 ■ OS8
Protocol	SIP (for example)
File Size	The size of the file, in KB
Added at	The date and time at which the CMP file was added to the Software Manager
Added by	The operator who added the CMP file to the Software Manager
Description	A description of the CMP file. See also Adding a cmp File on page 101.

Column / File Detail	Description
Tenant	The name of the tenant under which the SBC is located.

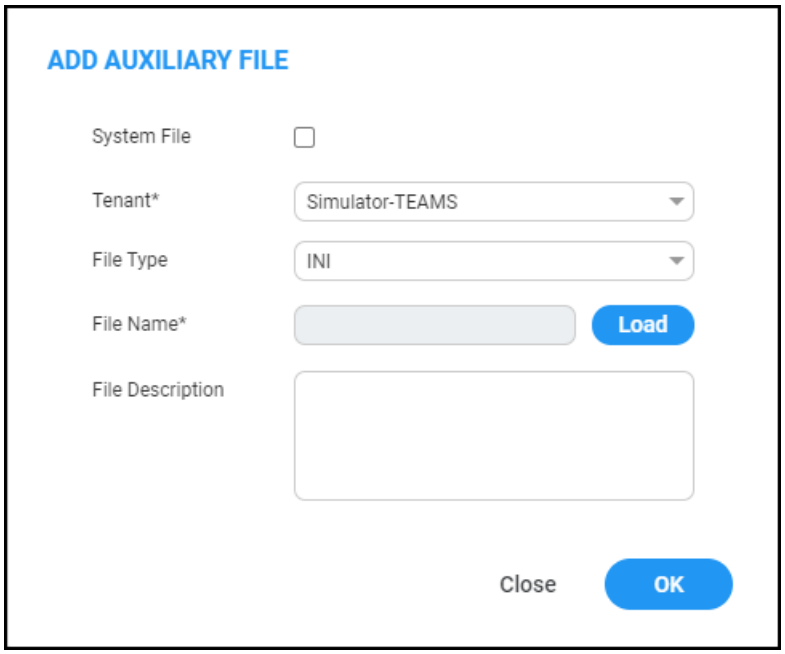
Adding a cli File

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 3-28: Add Auxiliary File



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 **Load** 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.

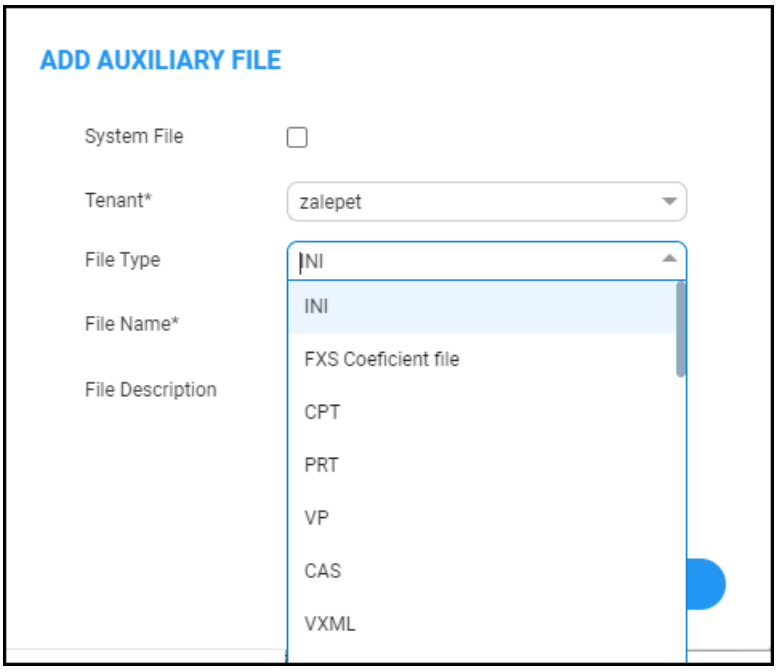
Adding Auxiliary Files

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 3-29: 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 CenterSecurity Guidelines.*
- A logo image file, to be displayed in report results, can also be added in this screen. See also Defining a Report on page 385

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.

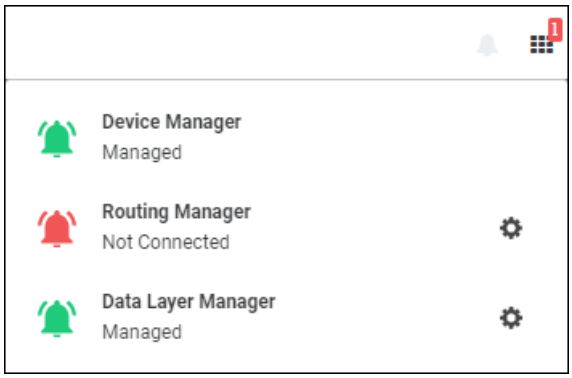
7. Enter a description of the file in the 'File Description' pane for intuitive future file management, and then click **OK**; the file is added to the Software Manager.

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.



- Click the relevant link for single sign-on to:
  - Device Manager (see Device Manager below for more information)
  - Routing Manager (see ARM on the next page for more information)
  - Data Layer Manager (see Data Layer Manager on page 108 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.

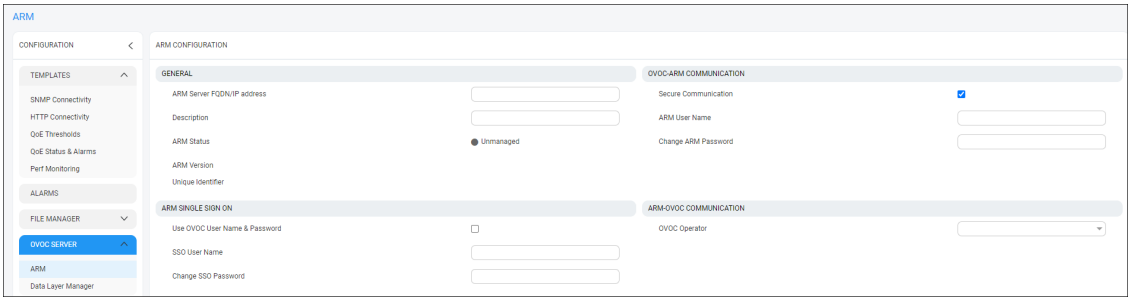
ARM

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 OVOC Server tab (**System** > **Configuration** > **OVOC SERVER**) as shown in the following figure, and then click the **ARM** option.

Figure 3-30: ARM Configuration



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.

Data Layer Manager

The Data Layer Manager page enables connecting directly to NEC's Data Layer Manager 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 the Data Layer Manager. A Data Layer Manager link is then displayed in the Call Details page.

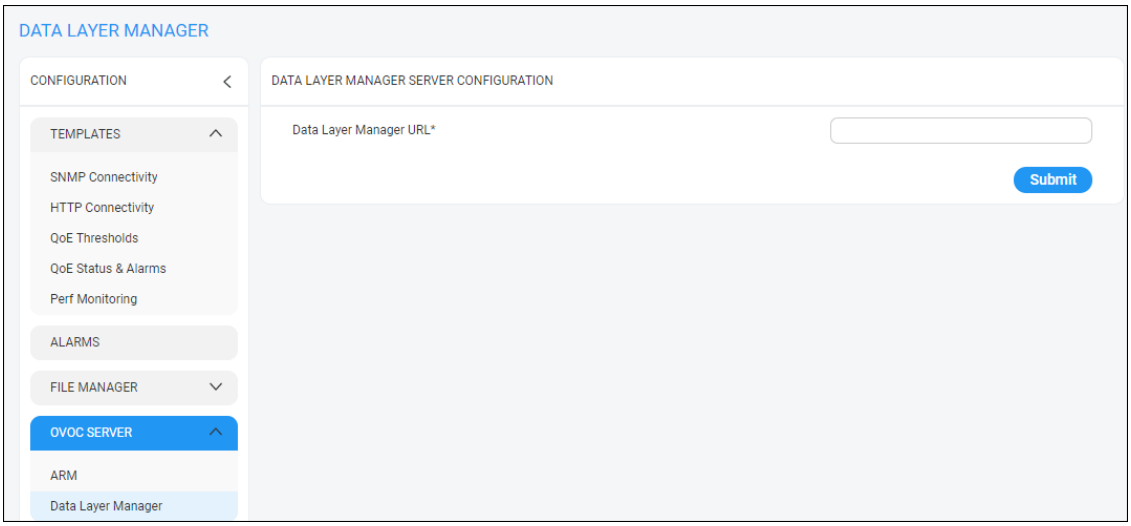


Applies only to operators who have acquired and installed Data Layer Manager.

➢ To enable connecting directly to Data Layer Manager:

1. Open the OVOC Server tab (**System** > **Configuration** > **OVOC**) and then click the **Data Layer Manager** option.

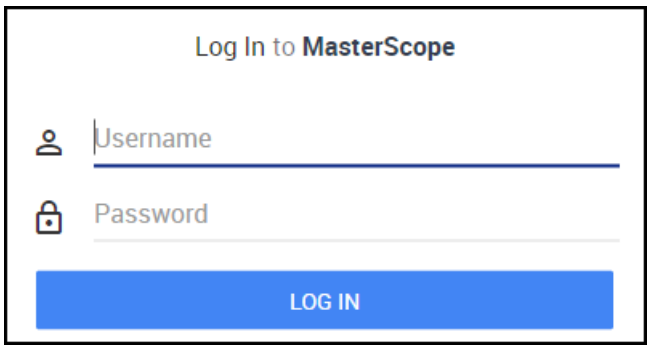
Figure 3-31: Data Layer Manager



2. In the 'Data Layer Manager URL' field, enter the Data Layer Manager IP address or FQDN. This is a string type parameter. Maximum size: 100 characters.
3. Click **Submit**; the **Data Layer Manager** 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.
- Data Layer Manager status as well as the statuses of other applications can be viewed in the menu. The example in the figure under Connecting Directly to External Applications on page 106 indicates that the network is managed by Data Layer Manager and that there are no alarms in the Data Layer Manager-managed network since the link is color-coded green.
- The status of Data Layer Manager in the OVOC license can be viewed in the License Configuration page (see Making Sure your License Provides the Capabilities you Ordered on page 71).
- If a license for Data Layer Manager does not exist, configuration of the Data Layer Manager URL cannot be performed.

4. From the Dashboard page, click the **Data Layer Manager** tab.



The application opens in a new browser tab.

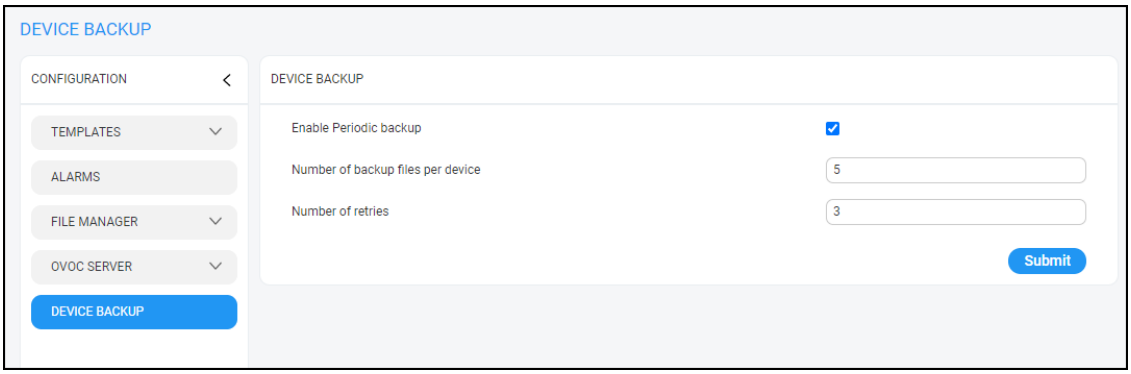
Enabling Automatic Device Backup Periodically

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 3-32: Device Backup



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 157 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

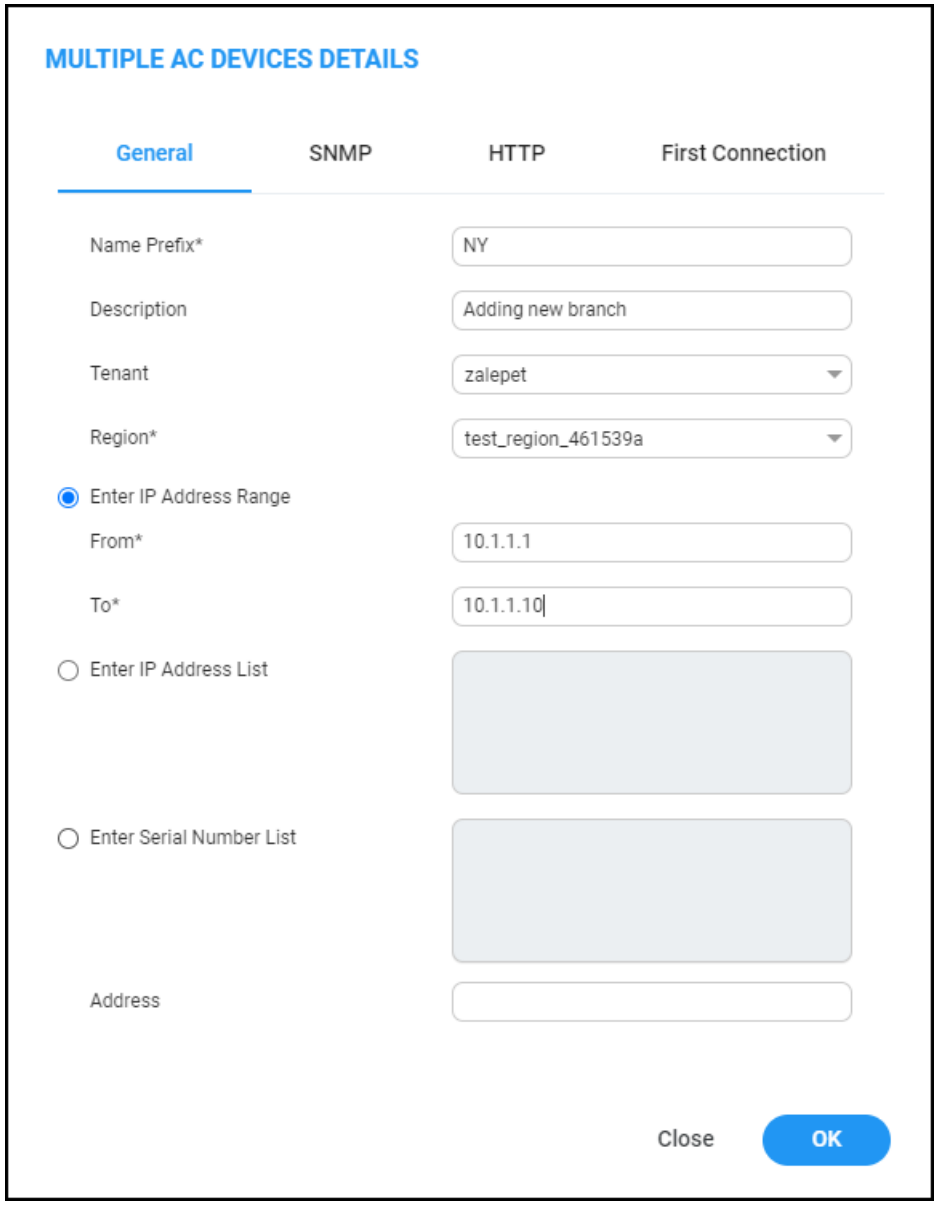
The Tasks page displays asynchronous actions performed by operators, currently under execution. Tasks that are *in progress* are displayed irrespective of how long it takes for them to complete. The OVOC continues to display them 20 minutes after they're completed. They are then removed from the page.

If the operator is not a 'system' operator, *onlytasks performedbythat 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 3-33: Task - Add Multiple AudioCodes Devices



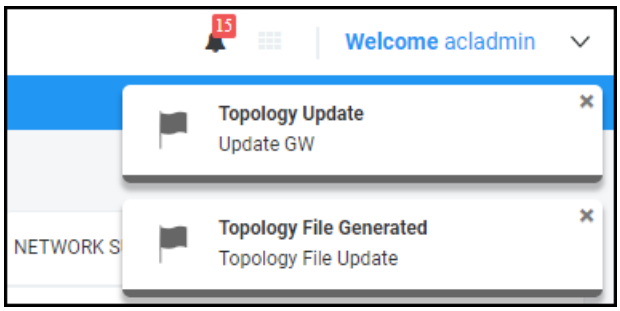
- [Optional] In the 'Address' field, enter the first letters of the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
- After clicking **OK**, a notification pops up in the uppermost right corner indicating the task status.

To configure the *timeout* of the notification pop-up, see Configuring Operator Authentication Locally, in the OVOC on page 50 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. The Tasks page allows you to determine if a task was performed successfully, or, if it's incomplete, what percentage is complete and what percentage remains to be completed.

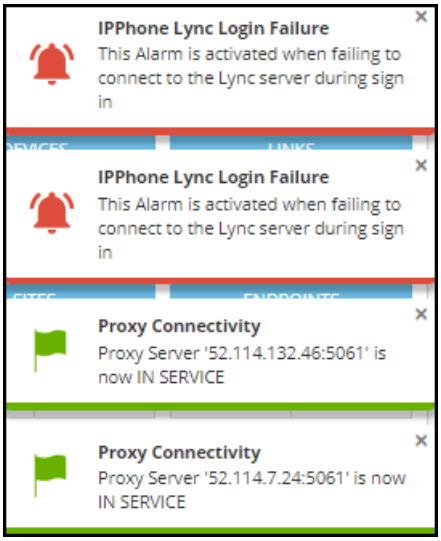
➢ To view the notifications history:

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



The bell icon indicates the *number of notifications not yet 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.

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 3 for details on multi-tenancy vs. non multi-tenancy architecture.

➢ **To add a tenant:**

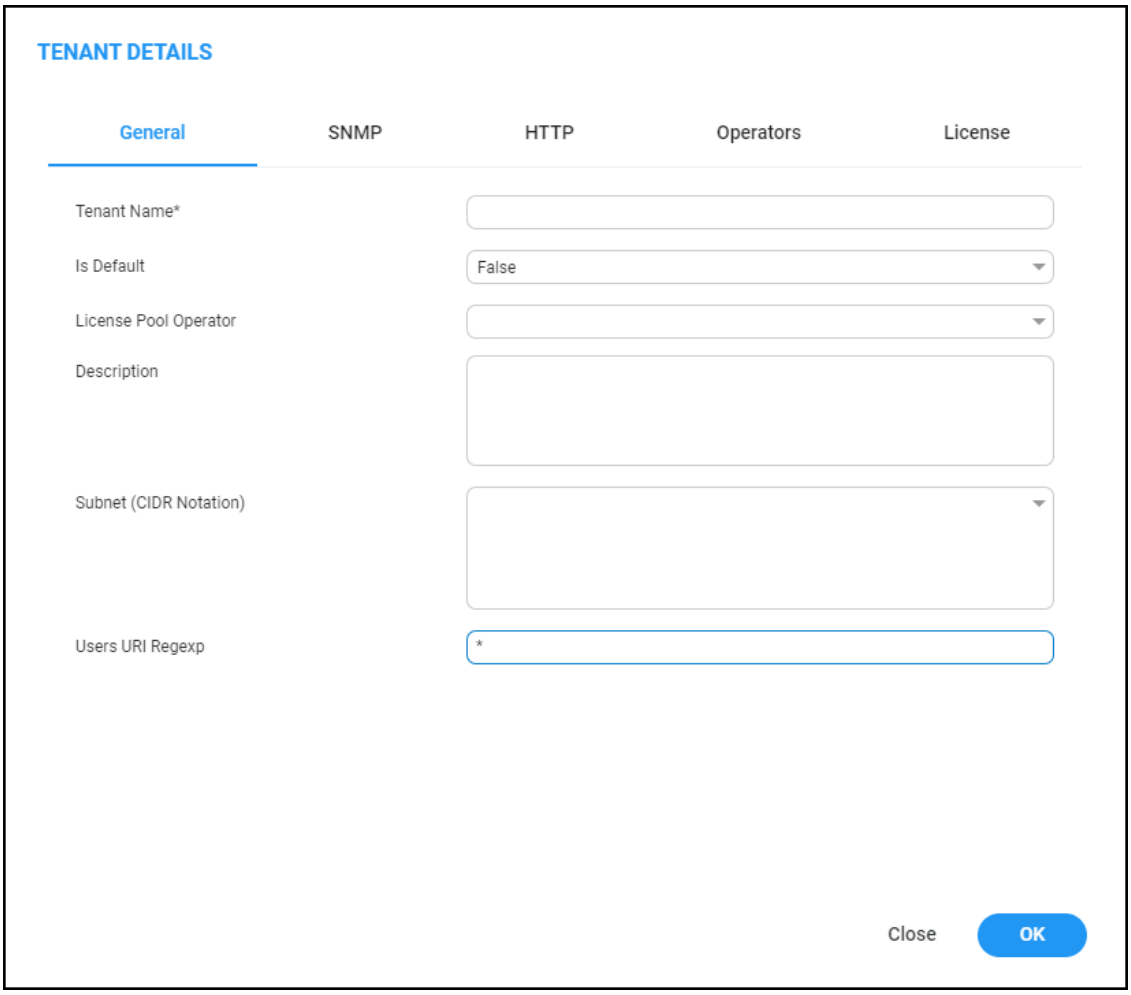
1. In the Network page, click **Add**.

Figure 4-1: Add Tenant



2. Select **Tenant**.

Figure 4-2: Tenant Details - General



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

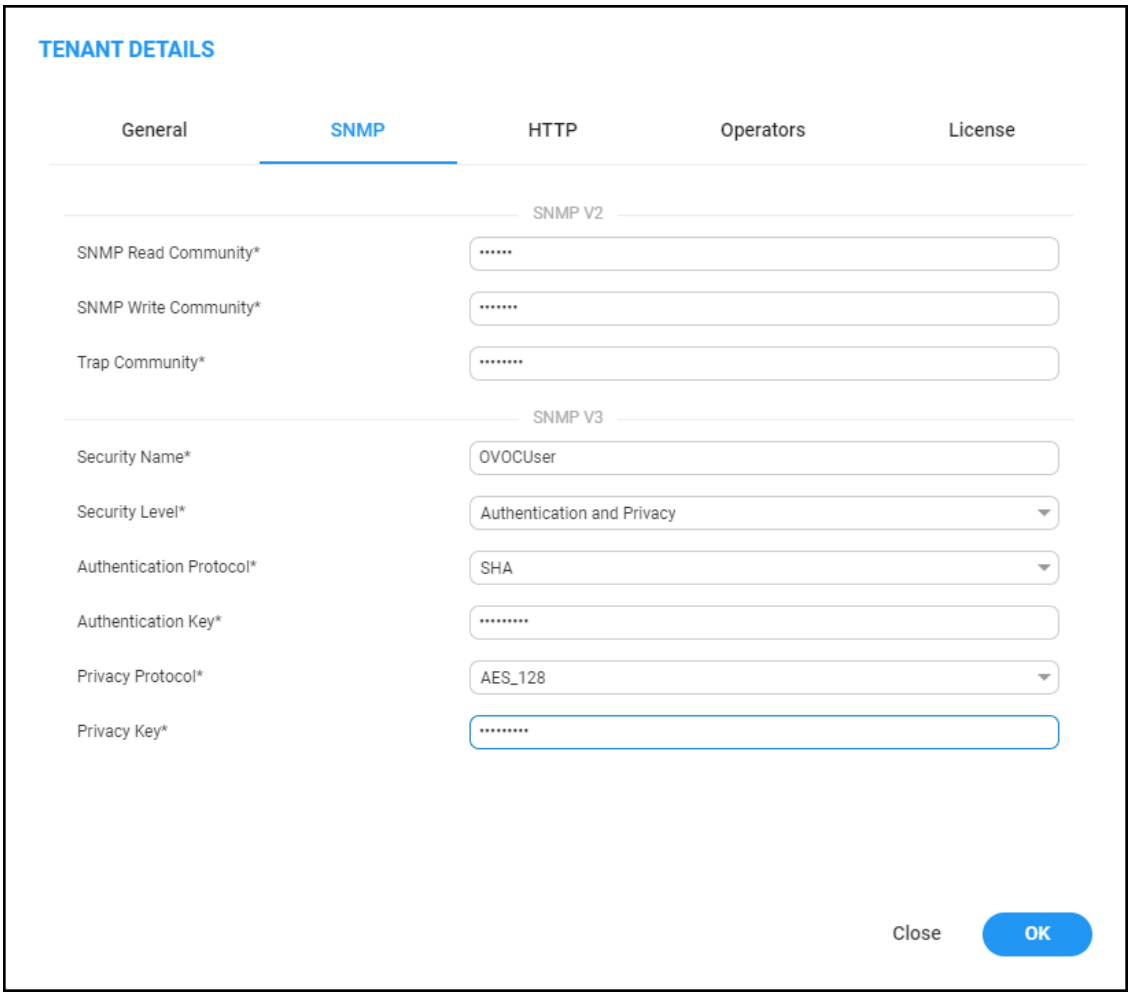
Table 4-1: Tenant Details - General

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 Fixed License Pool on page 195). After selecting a 'tenant' operator, the association cannot be removed (see also Adding a 'Tenant' Operator on page 60) and they're automatically displayed under the **Operators** tab (see following).
Description	Enter a tenant description to facilitate effective management later.

Parameter	Description
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 *region* 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.
Users URI Regexp	The OVOC saves all calls made over managed devices and IP phones (SIP Publish) and allows statistics to be generated on these calls. This parameter facilitates generating statistics *on calls made exclusively from URIs in a specific tenant*. Operators can run a regional expression to find the URIs associated with the specific tenant and then generate statistics exclusively on them. ■ If the field is left undefined (empty), no URIs will be saved for this tenant. ■ If you enter * in the field, all URIs will be saved for this tenant. **Note**: If in a five minute interval there are more than 2000 different URIs, the URI statistics for this five minute interval *will not* be saved.

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

Figure 4-3: Tenant Details – SNMP v2



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

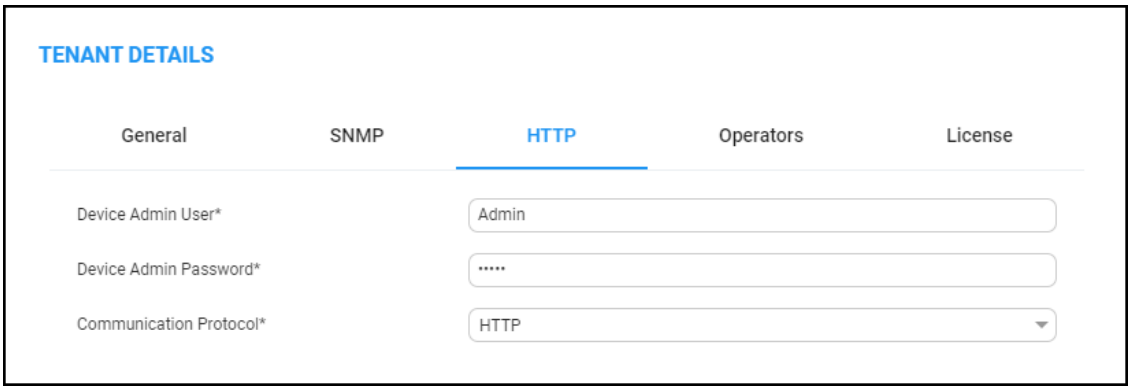
Parameter	Description
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the drop-down, select either: ■ **Authentication and Privacy** (default) ■ **No Security** ■ **Authentication**
Authentication Protocol	From the drop-down, select either: ■ **SHA** (default) ■ **MDS** ■ **No Protocol**
Authentication Key	Enter an Authentication Key. The default is taken from main SNMP template.
Privacy Protocol	From the drop-down, select either: ■ **AES 128** (default) ■ **DES** ■ **The default is taken from main SNMP template**
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



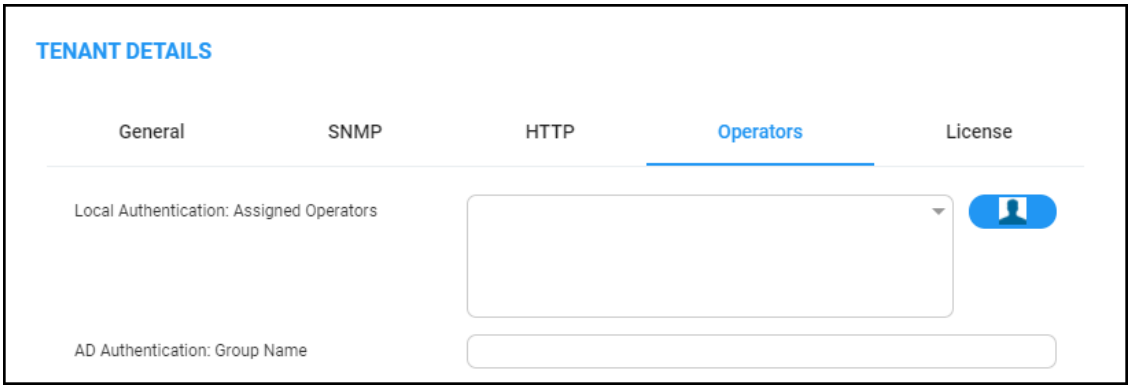
8. Use the following table as reference when configuring the HTTP parameters.

Table 4-4: Tenant Details - HTTP

Parameter	Description
Device Admin User	Enter the device Web server user name. Example: **Admin**. Password - "Admin". The default is taken from the main HTTP template.
Device Admin Password	Enter the Web server password. Example: **Admin**. The default is taken from the main HTTP template.
Connectivity	From the drop-down, select either: ■ **HTTP** (default) ■ **HTTPS** The default is taken from main SNMP template.

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

Figure 4-5: Tenant Details – Operators



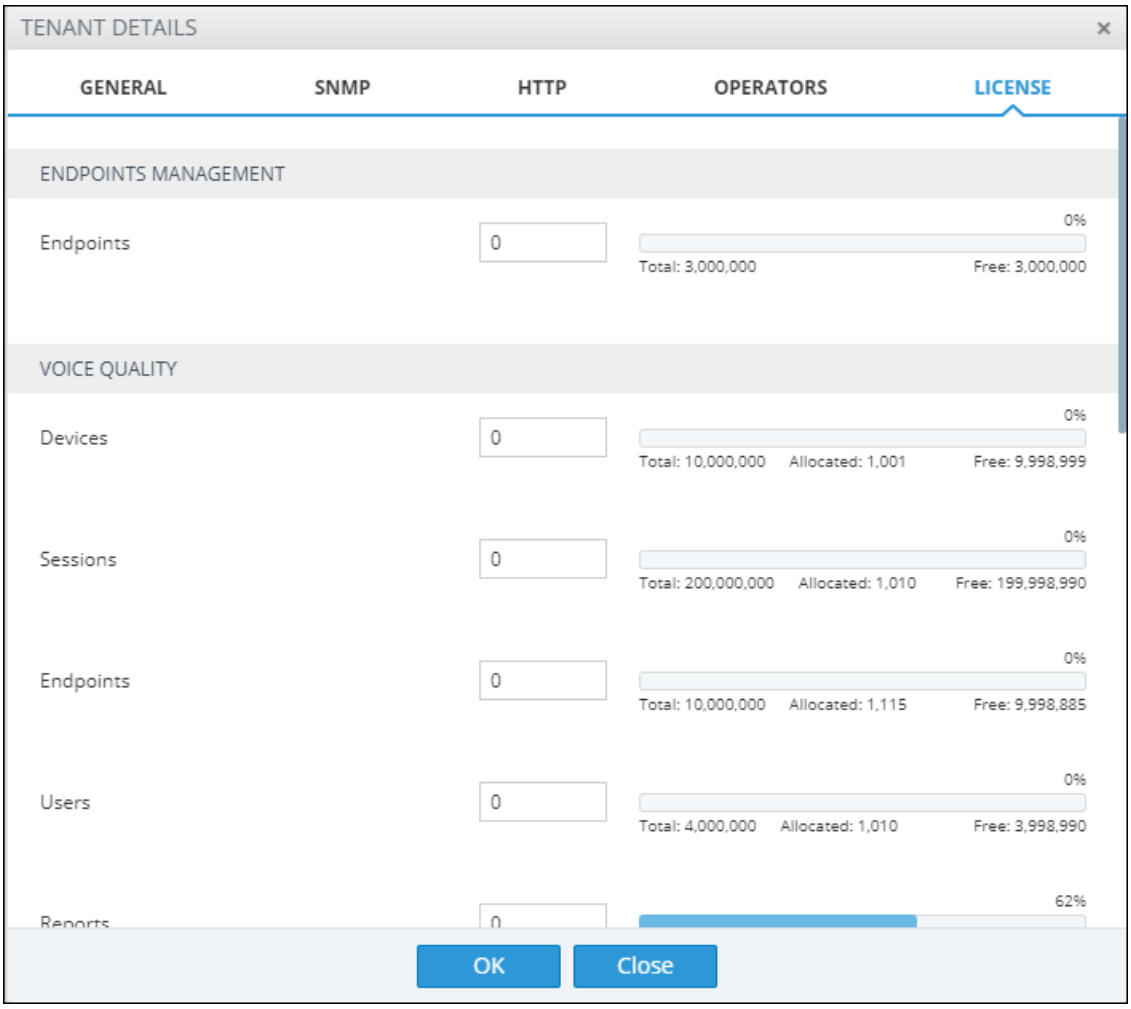
10. Use the following table as reference.

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 Adding a 'Tenant' Operator on page 60 for more information about configuring 'tenant' type operators.
	Operator authentication can be configured locally, in the OVOC (see Configuring Operator Authentication Locally, in the OVOC on page 50). Click the button to add a new 'tenant' type operator; the 'Tenant Operator Details' screen opens (see Adding a 'Tenant' Operator on page 60). The operator is then assigned to the tenant and displayed in the drop-down list.
AD Authentication: Group Name	Applies to 'tenant' type operators. When an operator logs in to the OVOC, the OVOC (before allowing the operator access) checks with the enterprise's Azure Active Directory / LDAP server if the User Group which the operator is associated in the OVOC, tallies with the User Group defined in the AD / LDAP server. If they tally, then when logged in, the operator is assigned with this tenant. See also under: • Configuring Operator Authentication Centrally with Azure Active Directory on page 44 • Configuring Operator Authentication Centrally using an LDAP Server on page 39

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

Figure 4-6: Tenant Details - License



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.

License Pool	Description
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.
Voice Quality	
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.
Reports	 Select the number of reports to allocate to the tenant. In the example here, a total of 5 can be allocated. If 6 are chosen, the indication bar turns red alerting you that the total has been exceeded.
Endpoints Management	
Endpoints	Enter the number of endpoints the Device Manager application supports for this tenant.

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

Editing a Tenant - Defining a Logo

After adding a tenant, the operator can add a logo image to the OVOC, to be displayed:

- in report results generated for the specific tenant
- in the OVOC login screen when the tenant operator logs in to the OVOC
- in the OVOC's main screen
- in the 'About' informational pop-up

The tenant logo displayed in these screens in the OVOC GUI facilitates network management for OVOC operators.

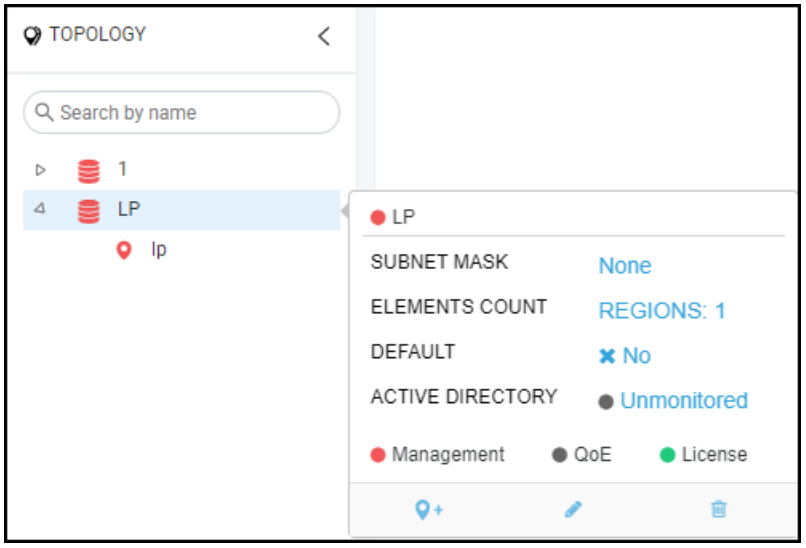
The behavior of the tenant logo is subject to the following circumstances:

- If a tenant operator is assigned to a *single* tenant and that tenant has a logo, when that tenant operator logs in to the OVOC the tenant logo will be displayed in the OVOC's main screen and in the 'About' informational pop-up.
- If a tenant operator is assigned to *more than one* tenant that has a logo or is assigned to *one or more* tenants but *none* of them has a logo, AudioCodes' logo will be displayed when that operator logs in to the OVOC.
- If a system operator logs in to the OVOC, AudioCodes' logo will always be displayed.

➢ To add a logo image:

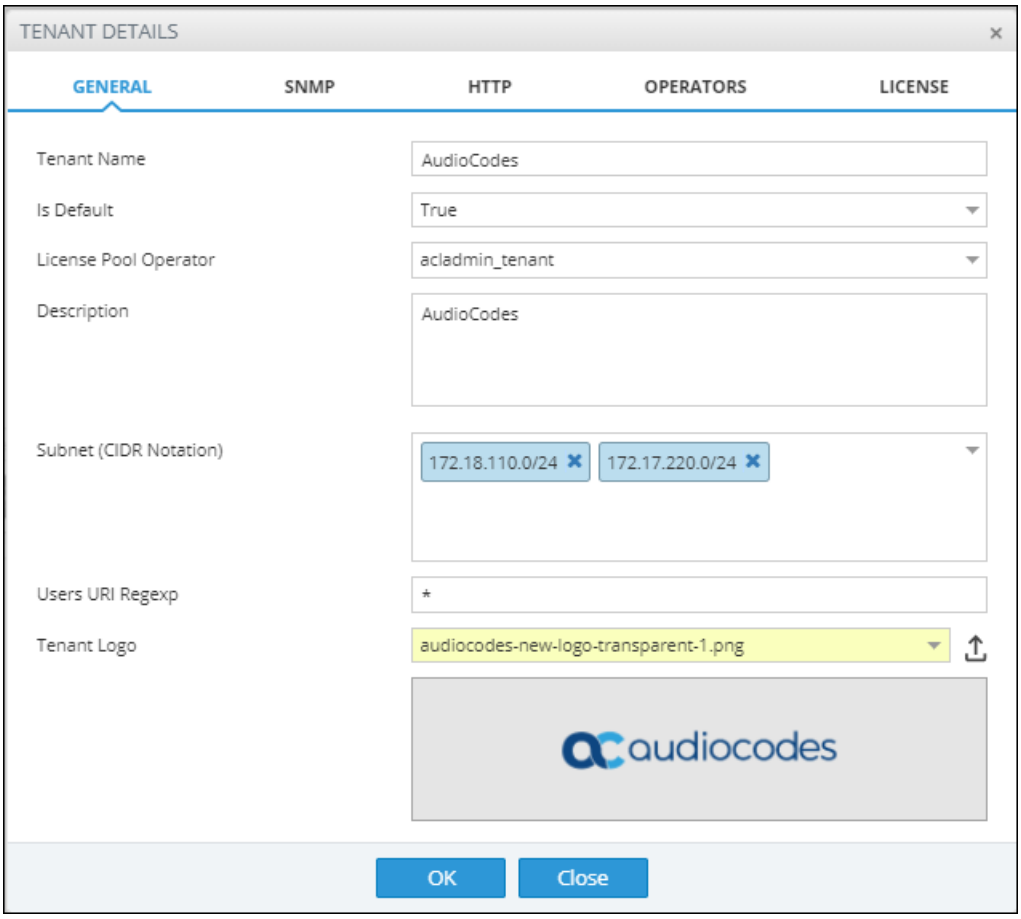
1. In the Network Topology page, hover the mouse over the tenant, click the 'Open menu' drop-down arrow adjacent to it and then click the Edit icon as shown in the figure below.

Figure 4-7: Edit Tenant



2. In the Tenant Details screen shown in the next figure, click ↥ adjacent to the parameter 'Tenant Logo' and then navigate to the location in which the logo image file is stored on your PC.

Figure 4-8: Tenant Details



3. Alternatively, from the 'Tenant Logo' drop-down list select a logo image file. [Note that the options listed will be the same as those you chose for the 'Logo' parameter in the Report screen's **Definition** tab described in Defining a Report on page 385].
4. Click **OK**; the logo image file is added to the Software Manager.

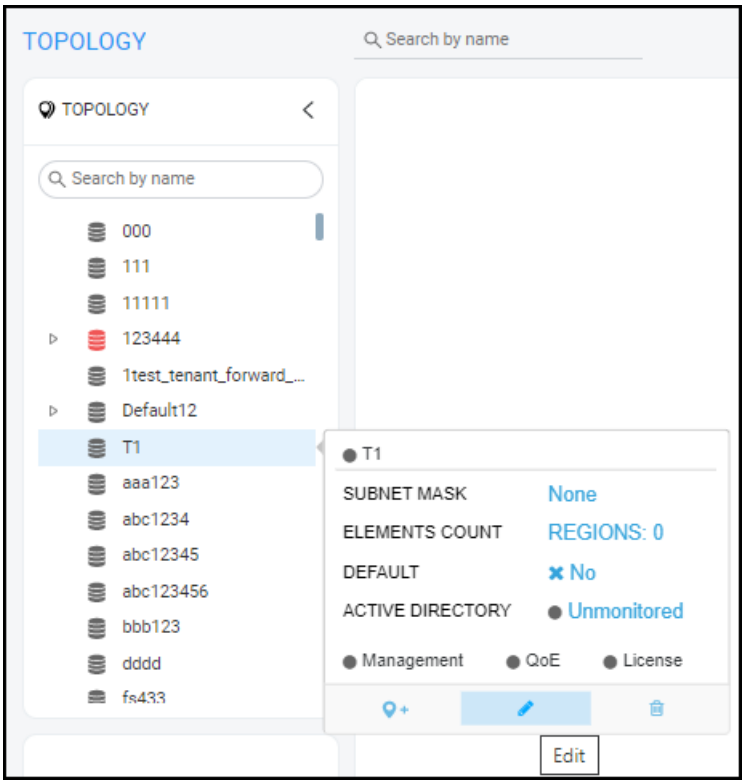
- You can select the file from the 'Tenant Logo' drop-down if already uploaded and displayed in the Software Manager.
- The logo image file can be added to the Software Manager (**Settings** > **Configuration** > **File Manager** > **Software Manager**) as shown in Adding Auxiliary Files on page 104 from the 'File Type' drop-down in the Add Auxiliary File screen.
- See also Adding Configuration Files to the OVOC's Software Manager on page 98 for related information.
- See also Defining a Report on page 385 for related information.
- For information about the other parameters in the Tenant Details screen, use the tables in Adding a Tenant on page 113 for reference.

Defining a Tenant Logo - Example

The example here shows in more detail how to add a tenant logo to the OVOC.

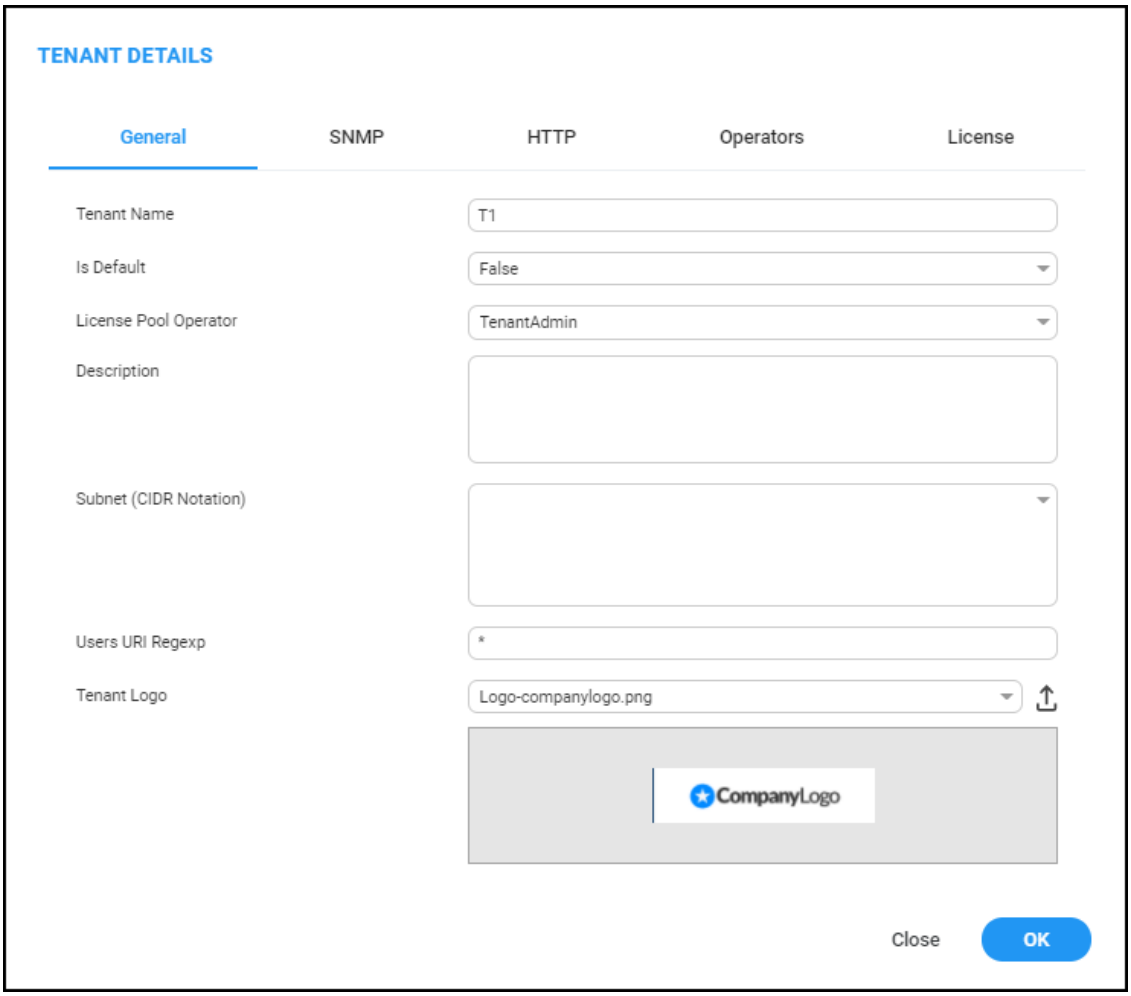
➢ To add a tenant logo to the OVOC:

1. In the Network Topology page tree, click the vertical ellipsis ⋮ next to the tenant and then click the **Edit** icon.



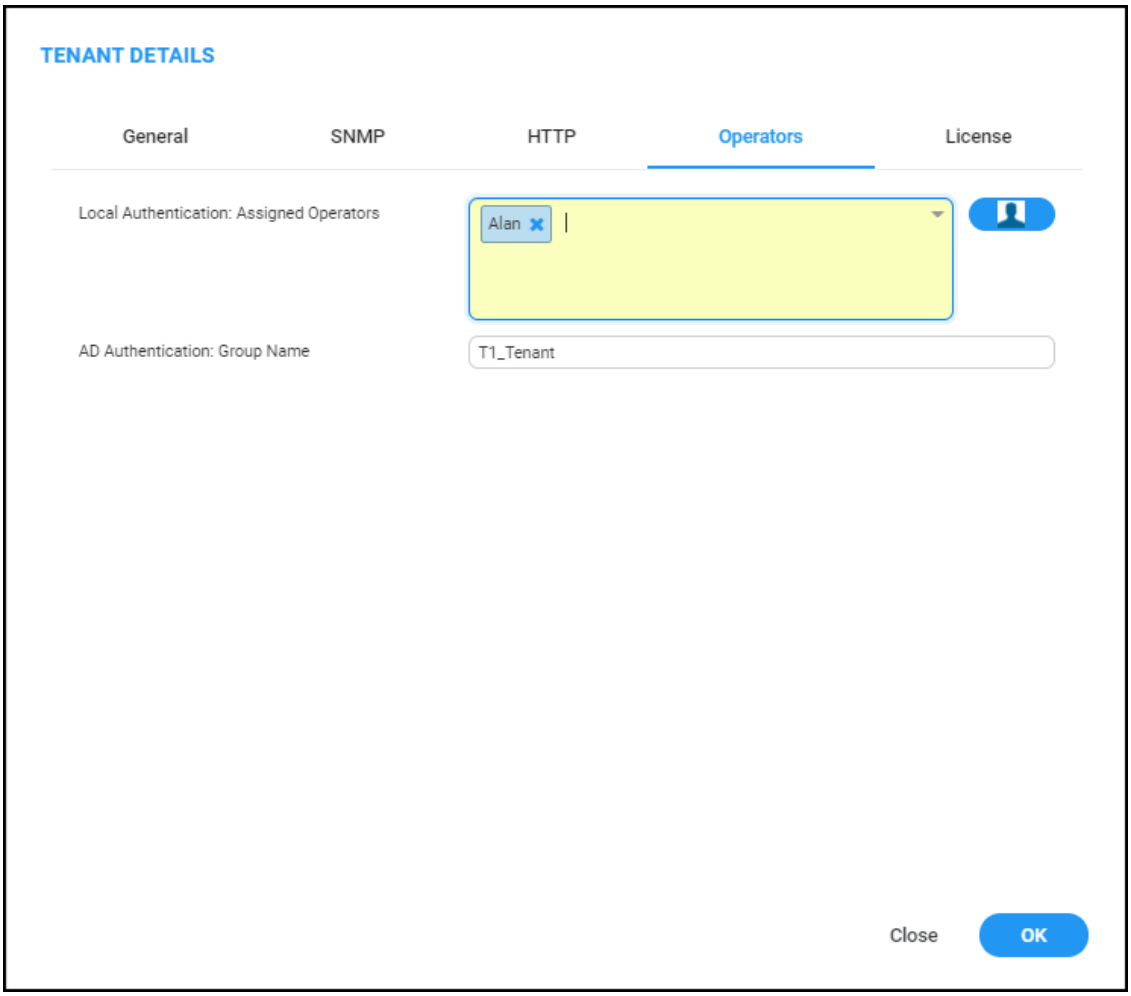
2. In the Tenant Details screen that opens (shown in the next figure), navigate to and select the tenant's logo from the 'Tenant Logo' drop-down or click the upload icon ↥ to upload it online if necessary.

Figure 4-9: Tenant Details - General



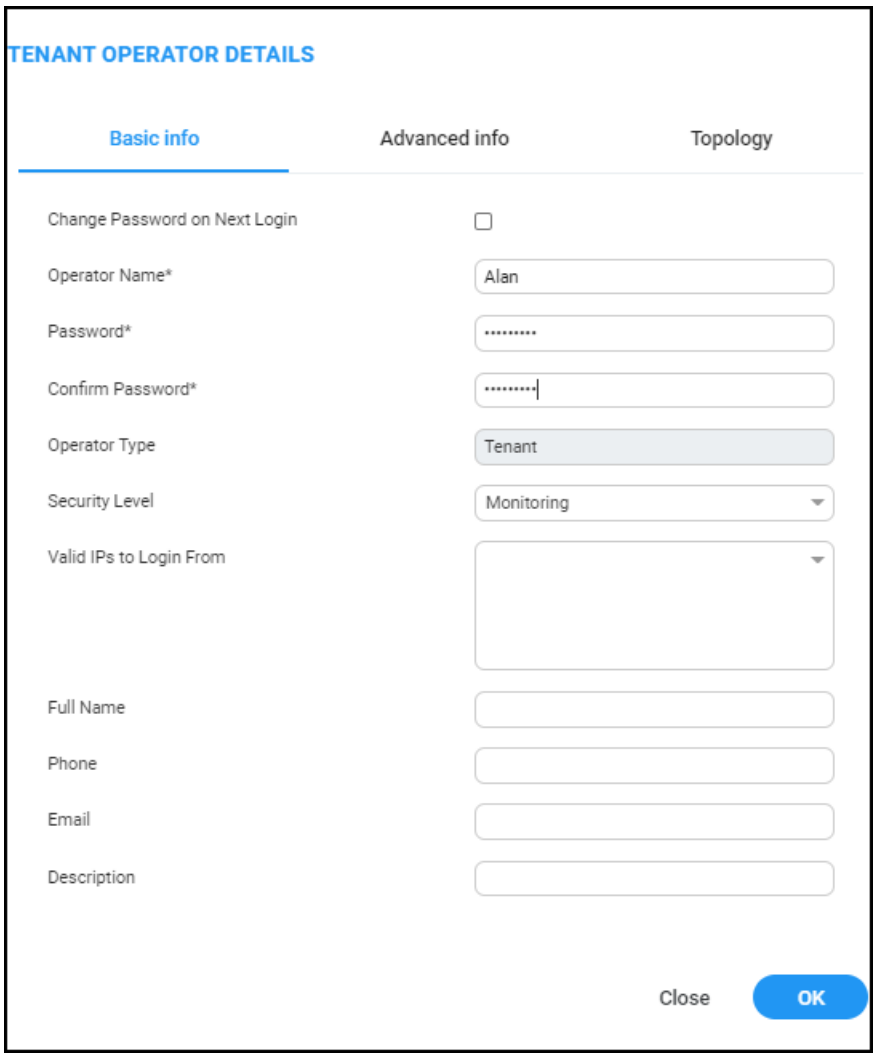
3. Click the **Operators** tab.

Figure 4-10: Tenant Details - Operators



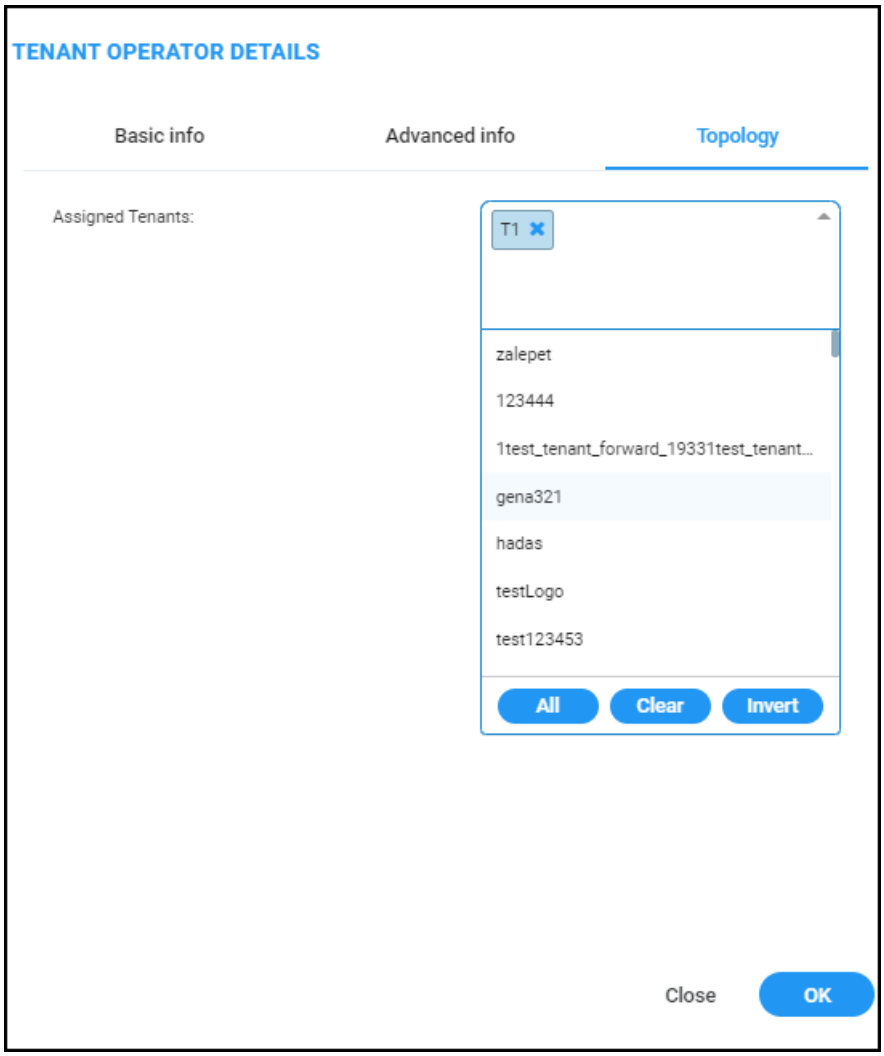
4. Click the operator icon and in the 'Tenant Operator Details' screen that opens, enter the operator's name and credentials under the **Basic Info** tab.

Figure 4-11: Tenant Operator Details - Basic Info



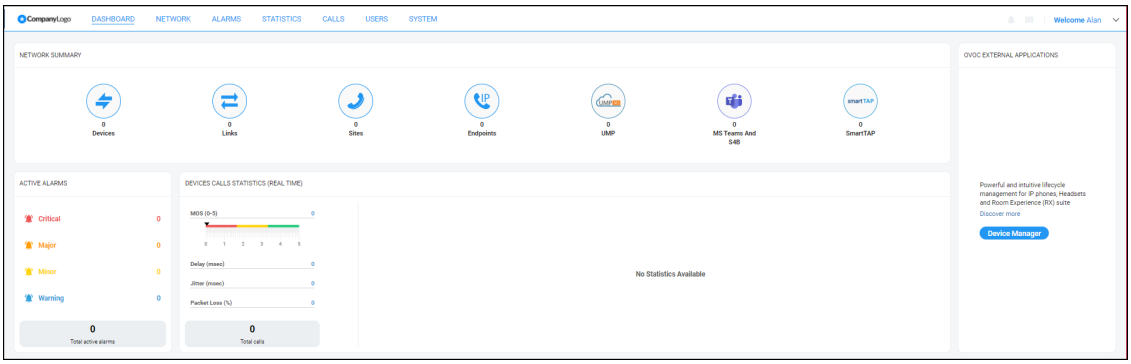
5. Under the **Topology** tab, navigate to and select the tenant to assign to the operator.

Figure 4-12: Tenant Operator Details - Topology



6. Click **OK** and then and then log out as 'System' operator and log in as the newly defined tenant operator. View the tenant logo displayed in the upper left corner of the OVOC GUI.

Figure 4-13: Tenant logo displayed in OVOC GUI



- Multiple tenants can be chosen.
- If you choose a single tenant and that tenant has a logo, you'll view the tenant logo when you log in with that tenant operator.

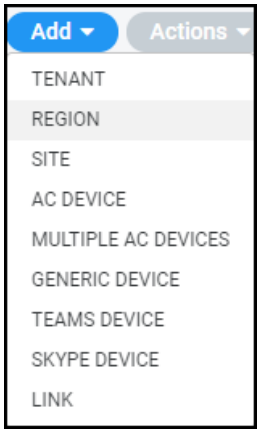
Adding a Region

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:**

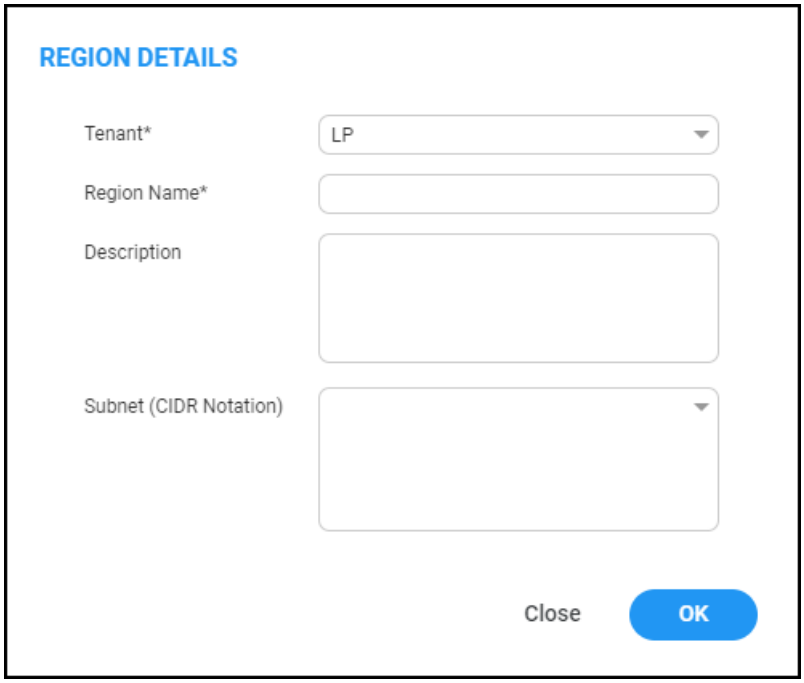
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select Region.

Figure 4-14: Add Region



The Region Details screen opens:

Figure 4-15: Region Details



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 135)
  - **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 143)
  - 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 4-16: Web interface: SNMP Community Strings

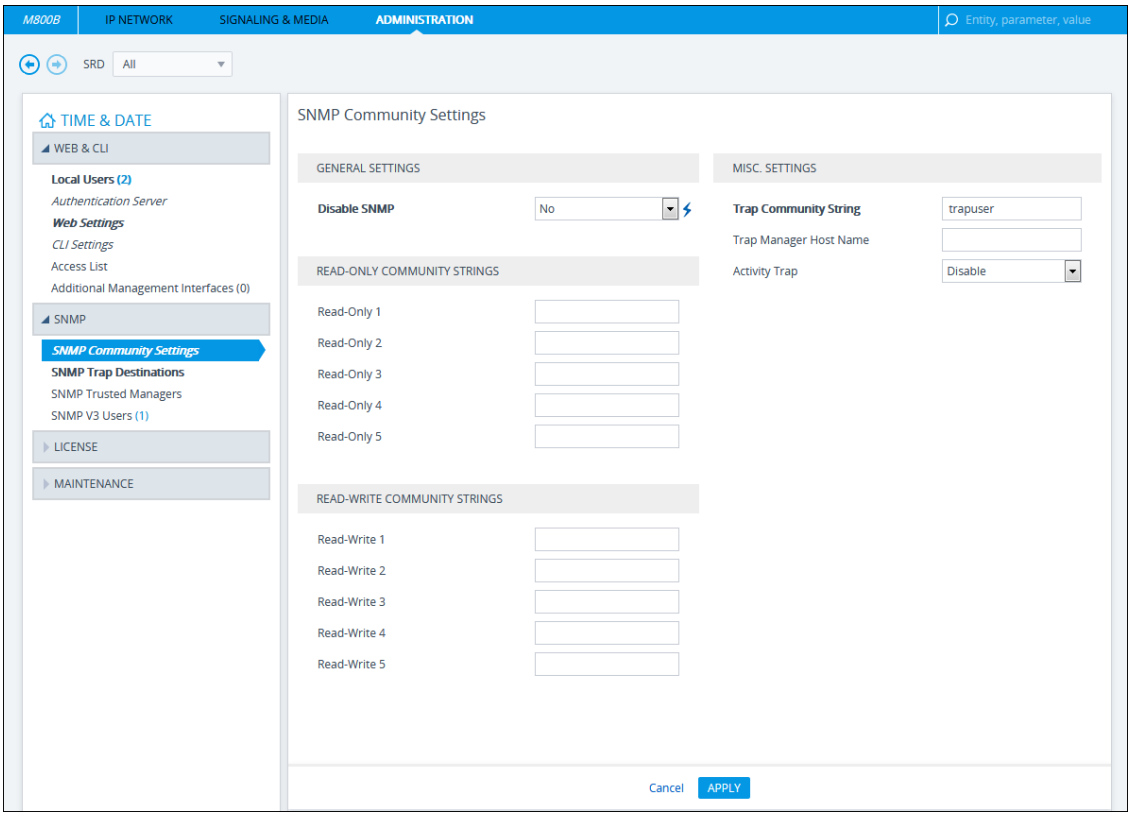
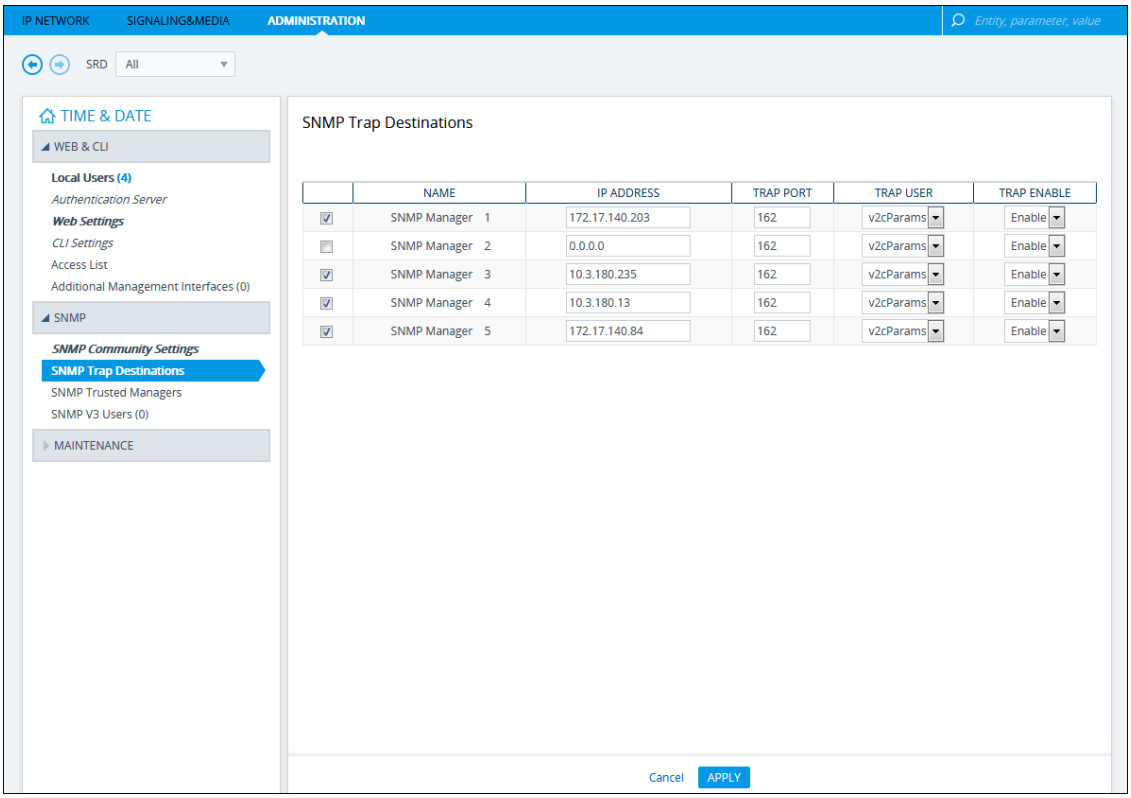


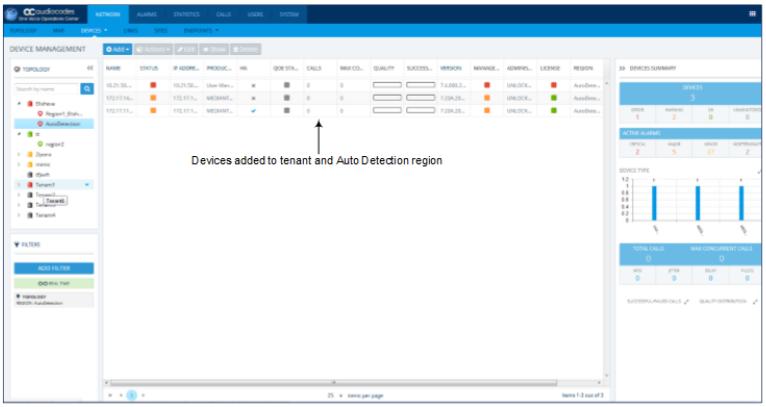
Figure 4-17: Web interface: SNMP Trap Destinations

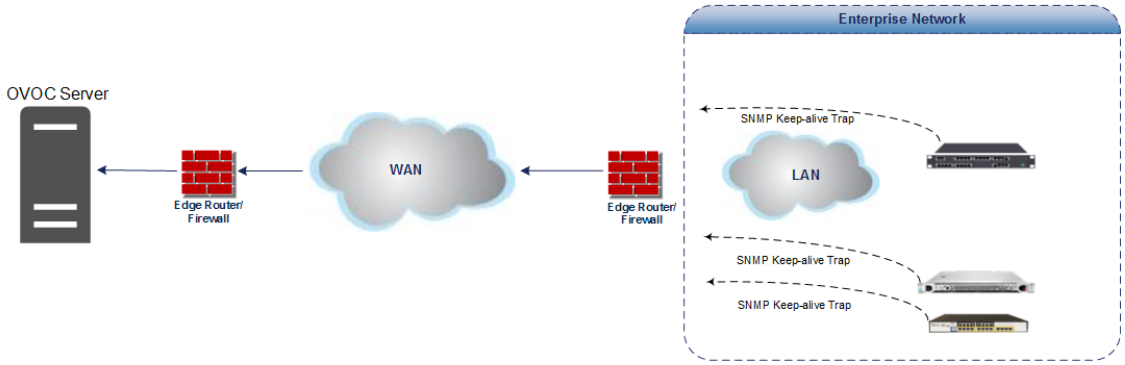


When devices are deployed in a private network using Network Address Translation (NAT), they can connect to the internet so long as their connection with the OVOC server is alive. You

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 4-18: AudioCodes Devices Added to OVOC





- To configure automatic detection with an ini file on multiple devices, use this syntax as an example:

```
SNMPPort_0 = 161SNMPManagerTrapPort_0 = 162
SNMPManagerIsUsed_0 = 1
SNMPManagerTrapSendingEnable_0 = 1
SNMPManagerTableIP_0 = 10.7.6.17
```

- To configure automatic detection with an ini file when devices are behind a NAT, use this syntax as an example:

```
SendKeepAliveTrap = 1
KeepAliveTrapPort = 1161
NatBindingDefaultTimeout = 30
```

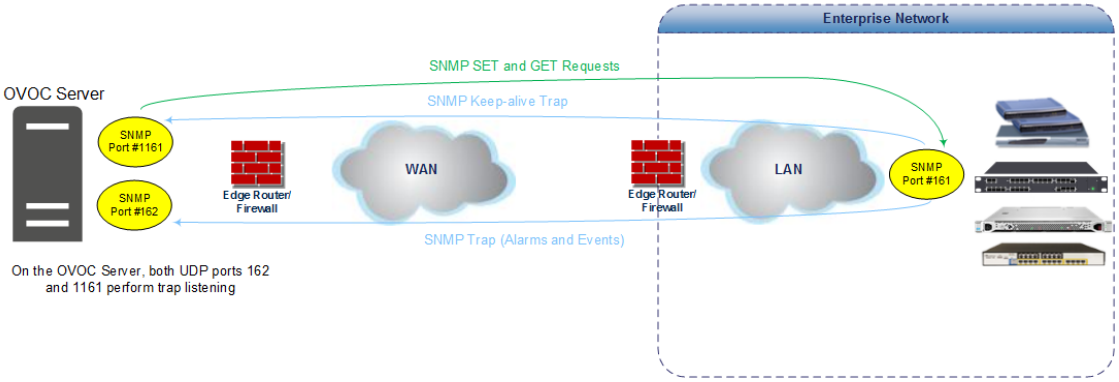
After devices are connected to the power supply and network, they reboot, initialize and send a coldStart trap to the OVOC server. When the coldStart trap (or keep-alive trap, if

configured) is received, the OVOC server connects each device and verifies it's an AudioCodes device.

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

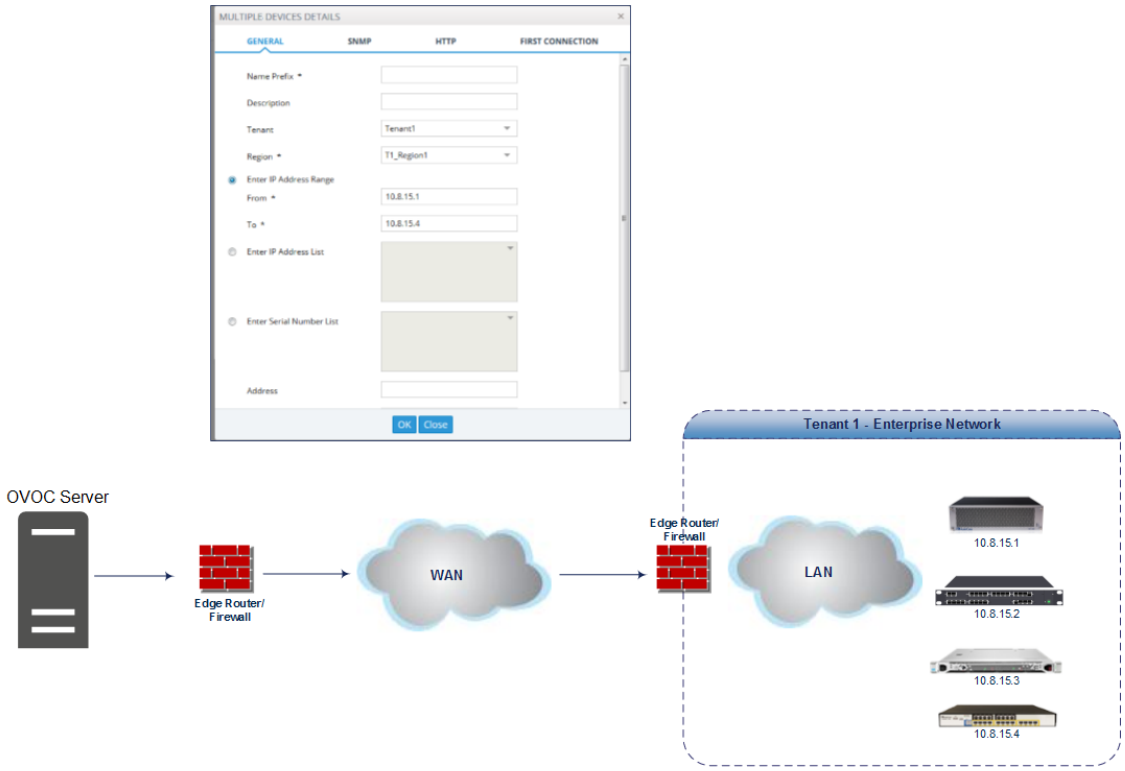
Figure 4-19: OVOC Server and Devices SNMP Connections



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 4-20: Manually Adding Multiple AudioCodes Devices to OVOC



➢ To manually add the devices:

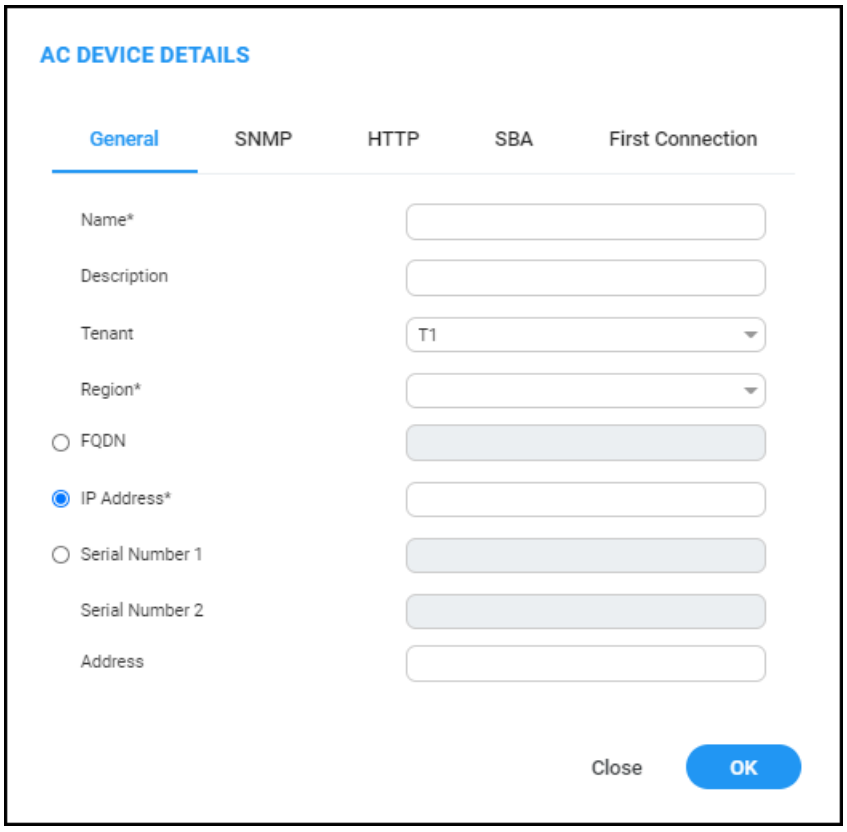
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **AC Device** or **Multiple AC Devices**.

Figure 4-21: AC Device | Multiple AC Devices



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

Figure 4-22: Device Details – General



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 113.
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.

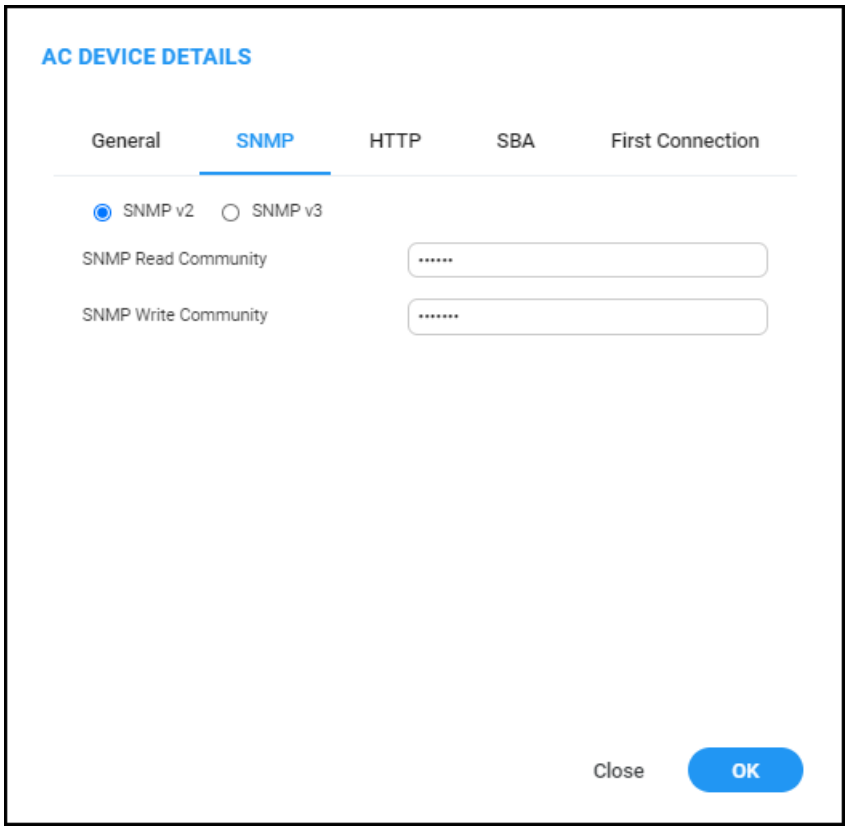
- [Optional] Select and enter the device's **Serial Number**. If selected, the 'FQDN' and 'IP Address' fields will be read-only. You can get the SN from the device's Web interface's Information page. The SN is only necessary for auto-detection. Generally, it is not mandatory to enter the serial number 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.

If the device is installed on the AWS/Azure image, make sure in the device's Web interface that 'Disable SNMP' is changed to **No** (Default: **Yes**).

- To configure SNMPv2, click the **SNMPv2** tab:

Figure 4-23: Device Details – SNMP v2



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.

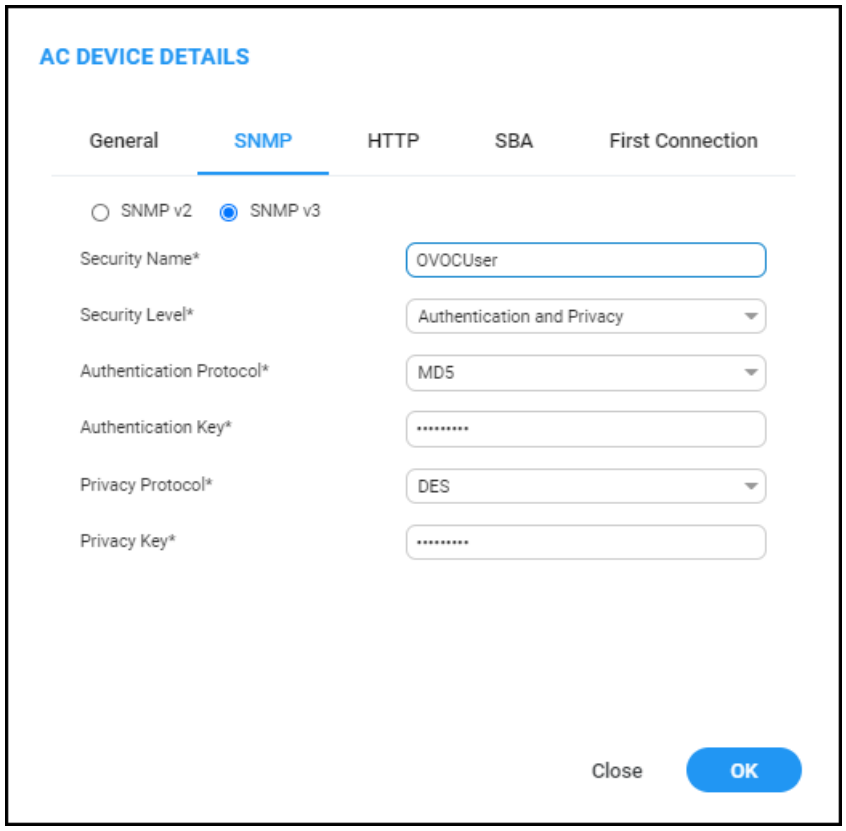
The SNMP connection must be configured on both the OVOC and the device. SNMP parameters include

- 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 4-24: 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.

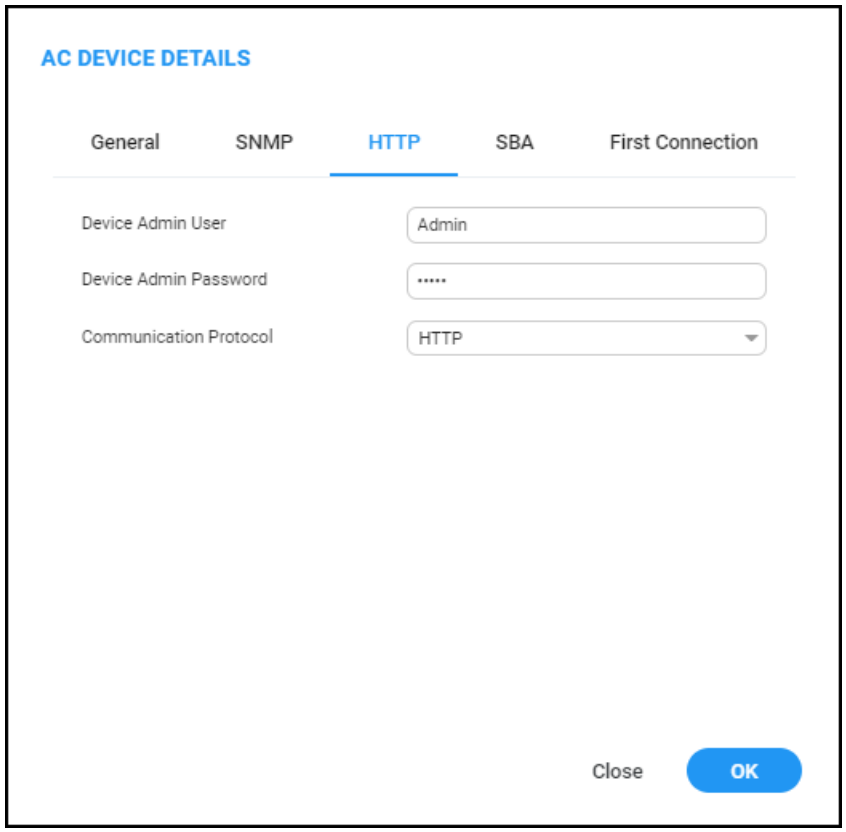
d. From the 'Privacy Protocol' drop-down, leave the default unchanged or select a Privacy Protocol.

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 4-25: AudioCodes Device Details – HTTP



The defaults are taken from the HTTP tenant profile.

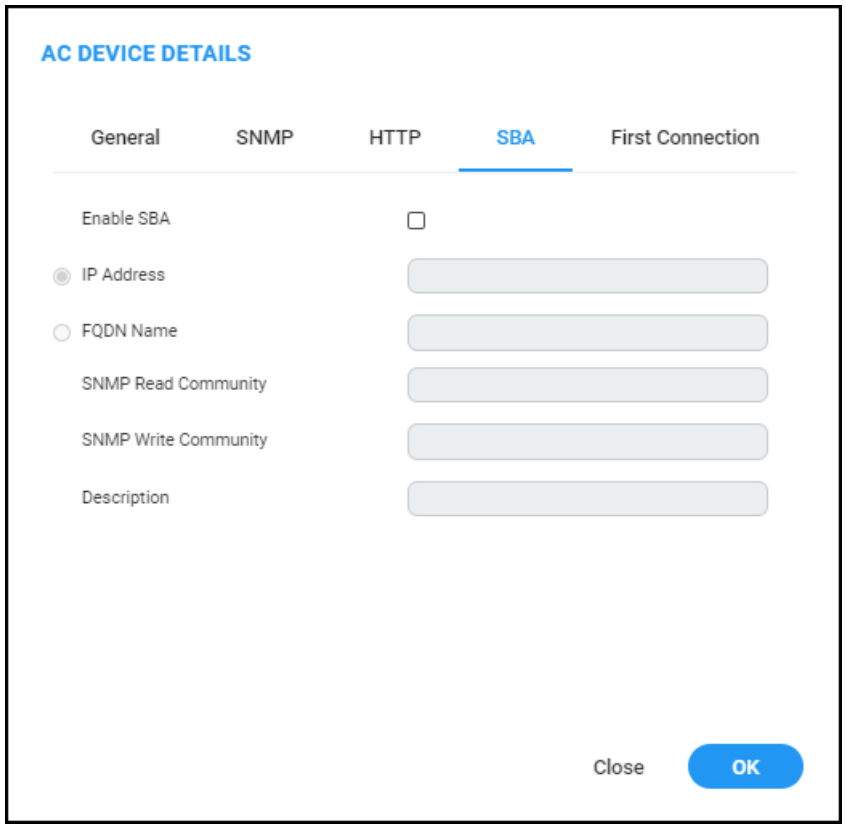
11. [Optional] In the 'Device Admin User' field, enter the device's web server user name and in the 'Device Admin Password' field, enter the web server password.
Example: **Admin**, **Admin**.

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 4-26: AudioCodes Device Details – SBA



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 4-27: 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 on the next page 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 147).

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 98 for details.

Figure 4-28: First Connection: Add AudioCodes Device

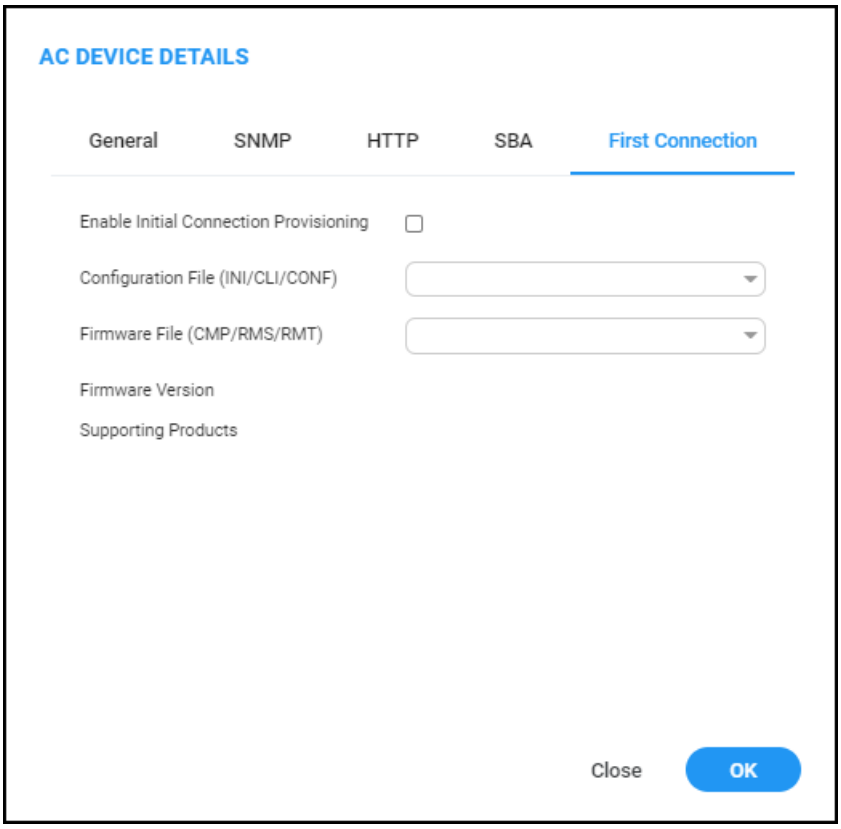
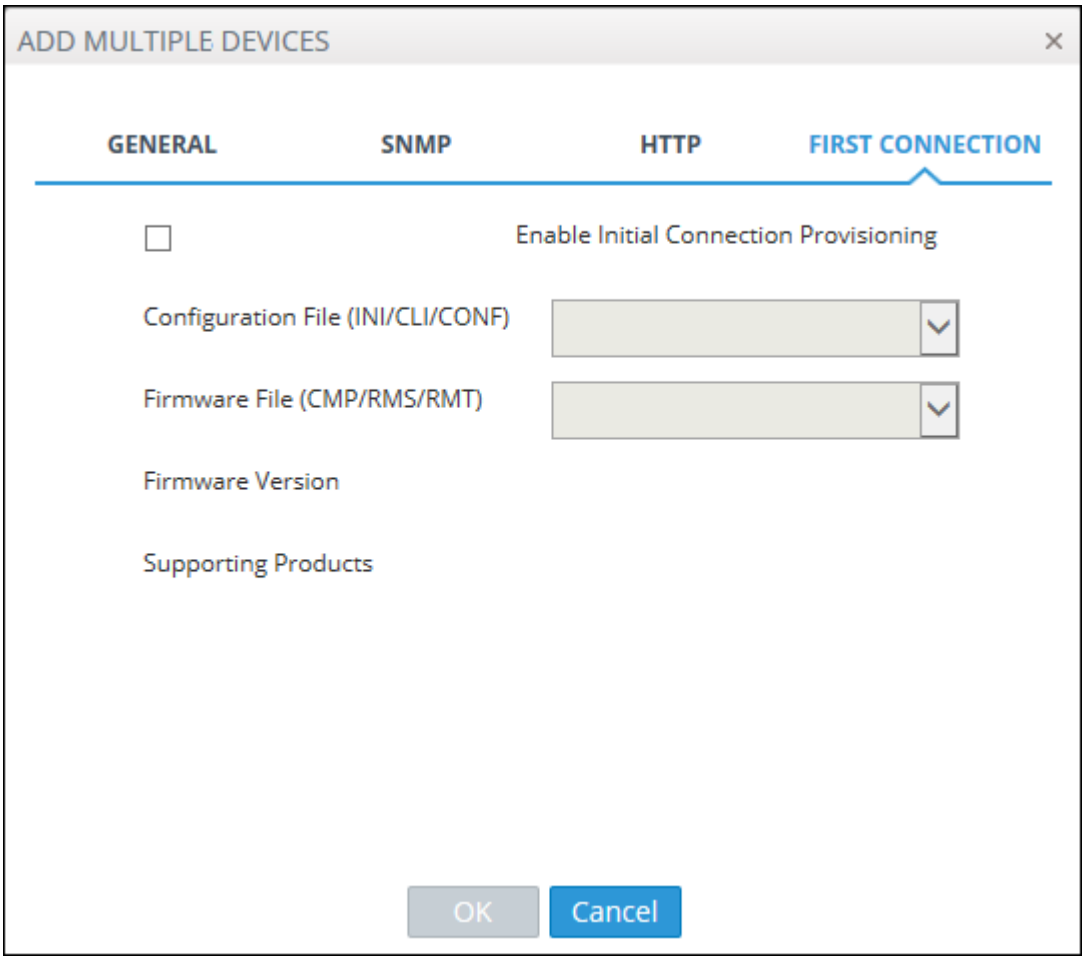


Figure 4-29: First Connection: Add Multiple AudioCodes Devices



➢ **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 130 for related information.

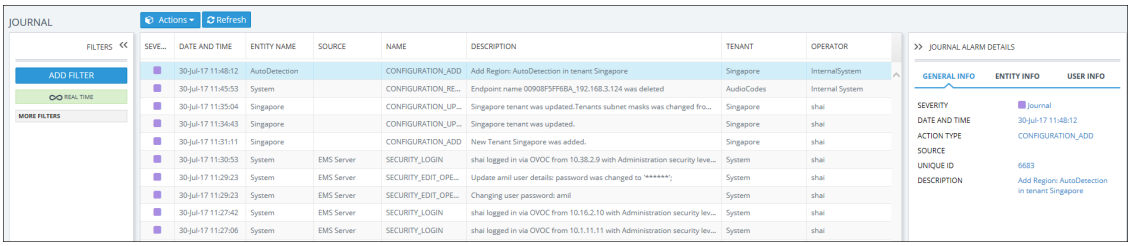
Making Sure First Time Provisioning was Successful

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:**

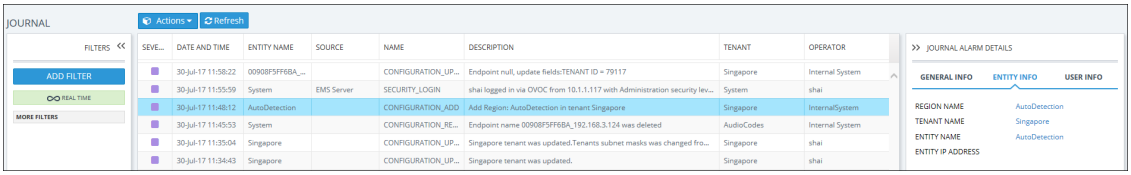
1. Open the Journal page (**Alarms** > **Journal**).

Figure 4-30: Alarms Journal



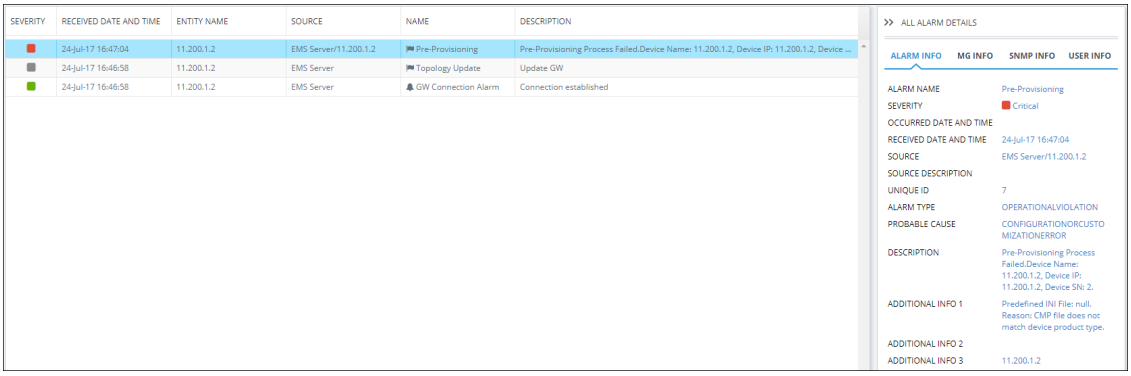
2. Optionally filter the page by Time Range (see Filtering to Access Specific Information on page 212), Topology (see Filtering by 'Topology' on page 215), Source Type (see Filtering by 'Severity' on page 230) or More Filters (see Filtering the Alarms Journal by 'More Filters' on page 238).
3. Locate 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 4-31: Alarms Journal – Entity Info



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

Figure 4-32: Critical Alarm – Initial Connection Provisioning Failed



If Initial Connection Provisioning was unsuccessful, download the configuration or firmware file to the device as shown in Backing Up on page 302.

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.

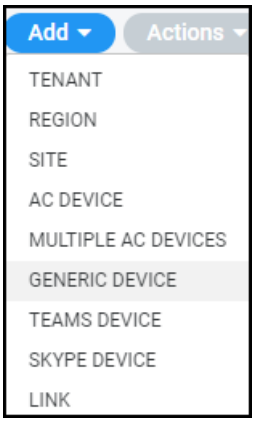
Adding a Generic Device Manually

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

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

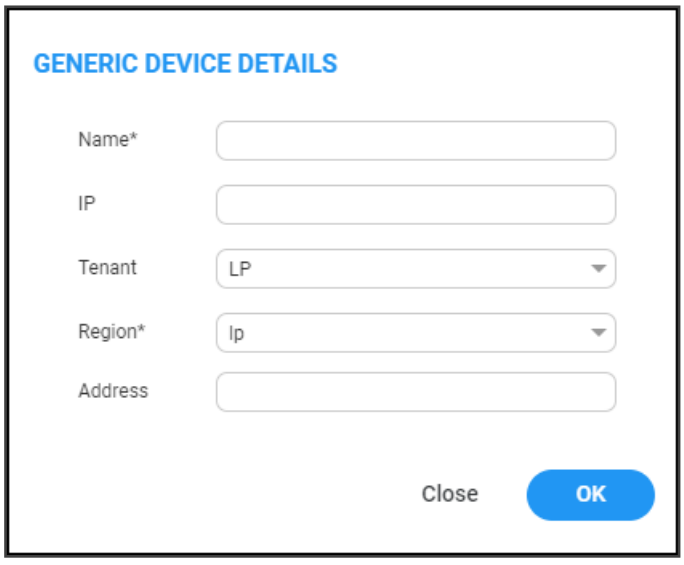
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **Generic Device**.

Figure 4-33: Add Generic Device



The Generic Device Details screen opens:

Figure 4-34: Generic Device Details



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.

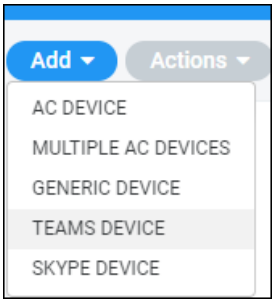
Adding a Microsoft Teams Device Manually

The Microsoft Teams 'device' is Office 365, Microsoft 365 or Azure, i.e., the 'micro' cloud environment purchased by the enterprise. The Microsoft 365 tenant needs to be configured to allow call records permissions (see the *OVOC IOM* for more information) The OVOC will receive call records notifications and accumulate statistics of the Teams tenant.

➢ **To add a device:**

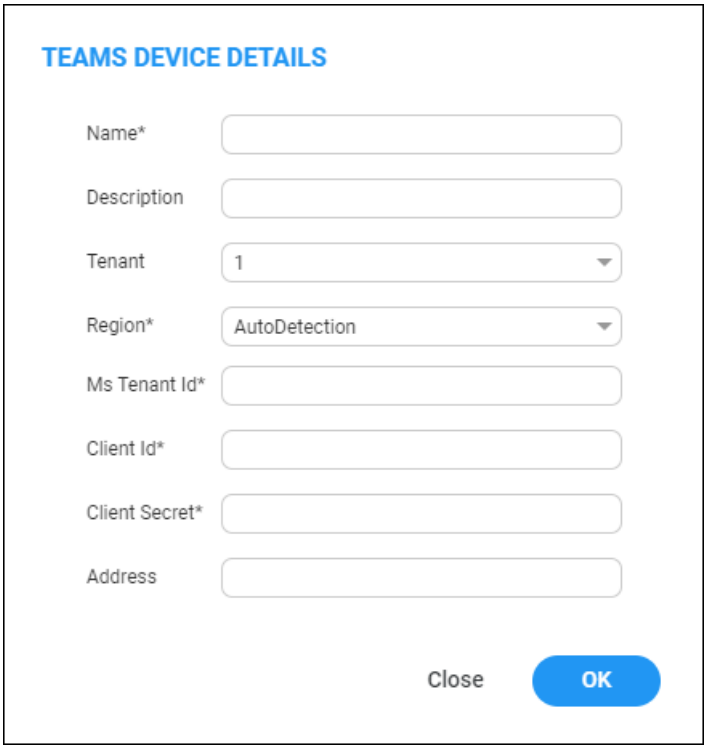
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **Teams Device**.

Figure 4-35: Add Teams Device



The Teams Device Details screen opens.

Figure 4-36: Teams Device Details



3. Define an intuitive name to facilitate operator-friendly management later. Don't use underscores.

4. Enter a Description to facilitate operator-friendly management later.
5. From the 'Tenant' drop-down, select the tenant with which to associate the device.
6. From the 'Region' drop-down, select a region you configured when Adding a Region on page 129.
7. For each enterprise that purchases Office 365 services or any other service, Microsoft defines a 'micro' enterprise cloud with an identifier – a Tenant ID. In the 'MS Tenant ID' field, enter this ID. It represents the 'micro' enterprise cloud: Office 365 / Microsoft 365 / Azure. Defining this environment is necessary for permissions.
8. Microsoft generates a Client ID for a specific application - the OVOC, in this case - to allow the application access with MS Graph API (subscription creation or call record retrieving). In the 'Client ID' field, enter the OVOC application's 'user name'.
9. Microsoft generates a Client ID for a specific application - the OVOC, in this case - to allow the application access with a graph API. In the 'Client Secret' field, define the shared secret - the 'password' - to allow the OVOC application access to the specific 'micro' enterprise cloud. Must be cryptically strong. The OVOC will then be capable of accessing Office 365 / Microsoft 365 / Azure.
10. [Optional] In the 'Address' field, enter the first few letters in the name of the city / country in which to locate the Office 365 / Microsoft 365 / Azure 'micro' cloud, and then select the city / country from the list that pops up.
11. Click **OK**; the device (Office 365 / Microsoft 365 / Azure) is added.

Adding a Microsoft Skype for Business Device Manually

Another 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 420.

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

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

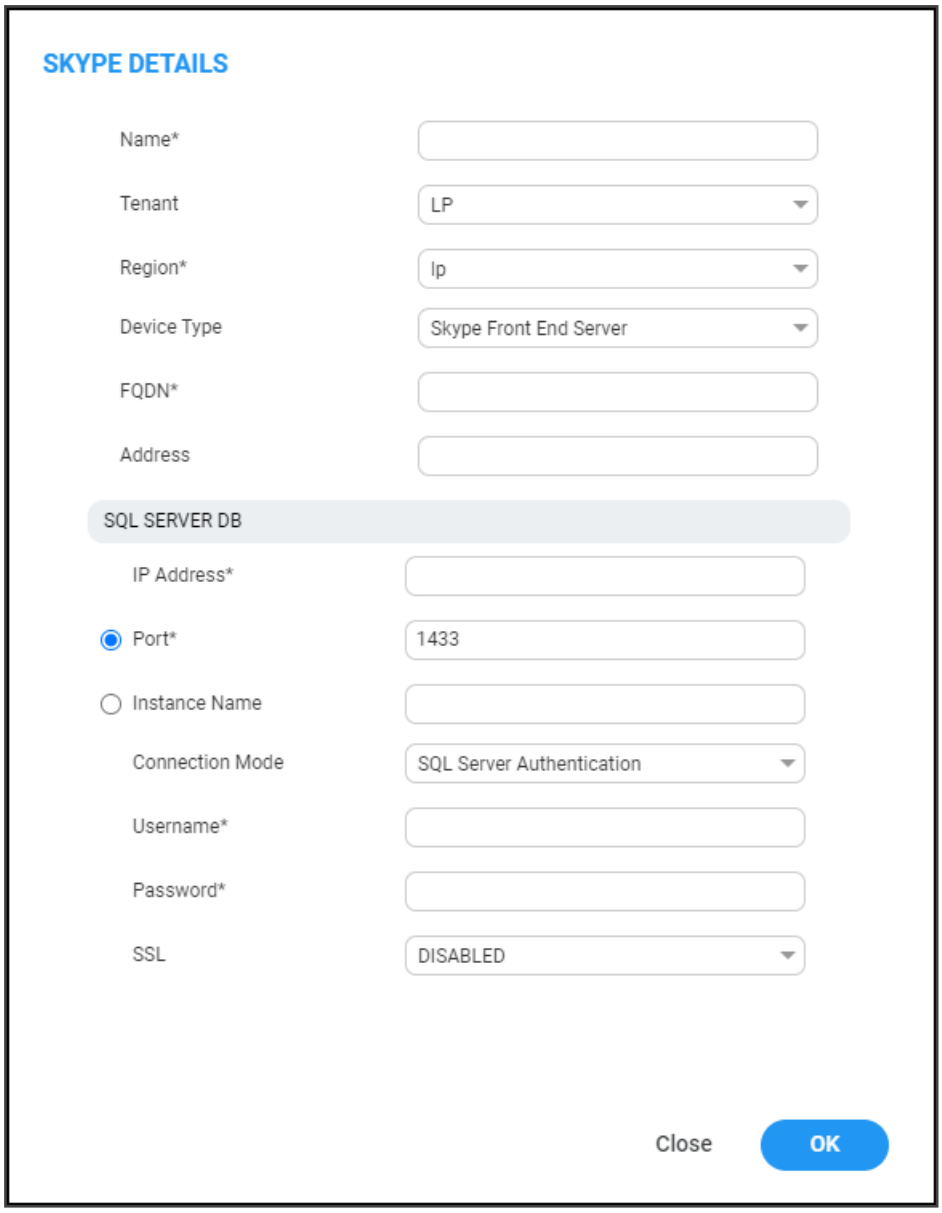
Figure 4-37: Add Skype Device



If the number of licensed users is 10 or below, the option to add a Skype for Business device will not appear. Make sure 11 or more users are licensed before adding a Skype for Business device. Contact your AudioCodes representative if you have an insufficient number and you need to add a Skype for Business device.

The Skype Details screen opens.

Figure 4-38: Skype Details



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 129.
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 OVOC 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 98.

    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 110.

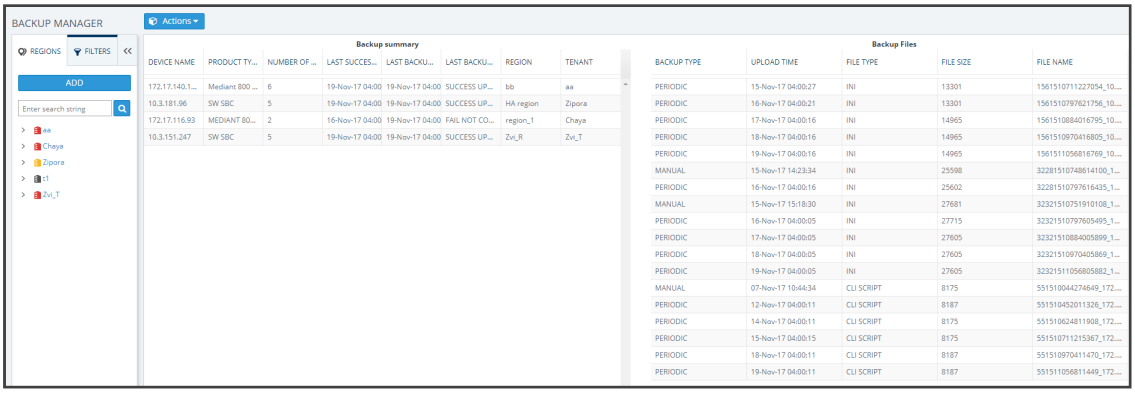
Manually Backing up a Device's Configuration

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 4-39: Backup Manager



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

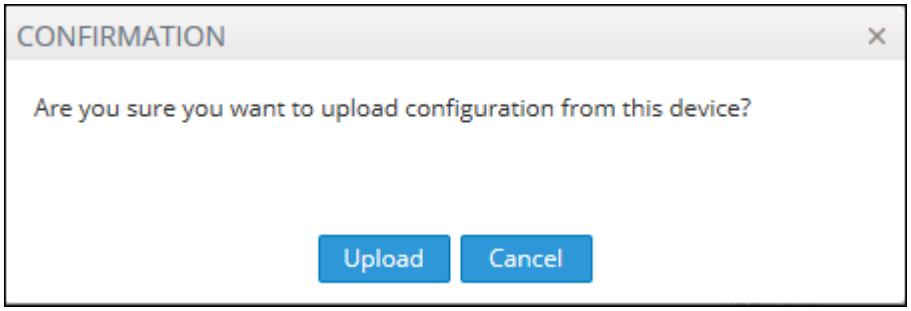
Use the following table as reference to the example.

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
m	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

2. 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.
3. 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 4-40: Backup Manager – Backing up a Device's Configuration – Confirmation Prompt



4. 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:**

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

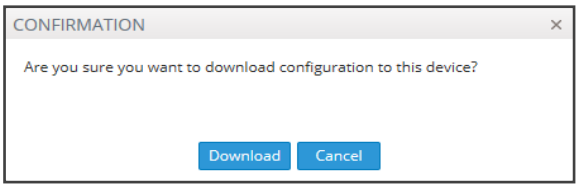
Restoring the Last Backed-up Configuration to the Device

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

➢ **To restore the last backed up configuration to the device:**

1. In the page's Backup Summary pane, select the device whose last backup you want to restore.
2. 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 4-41: Backup Manager – Restoring a Device's Last Backup – Confirmation Prompt



3. 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.

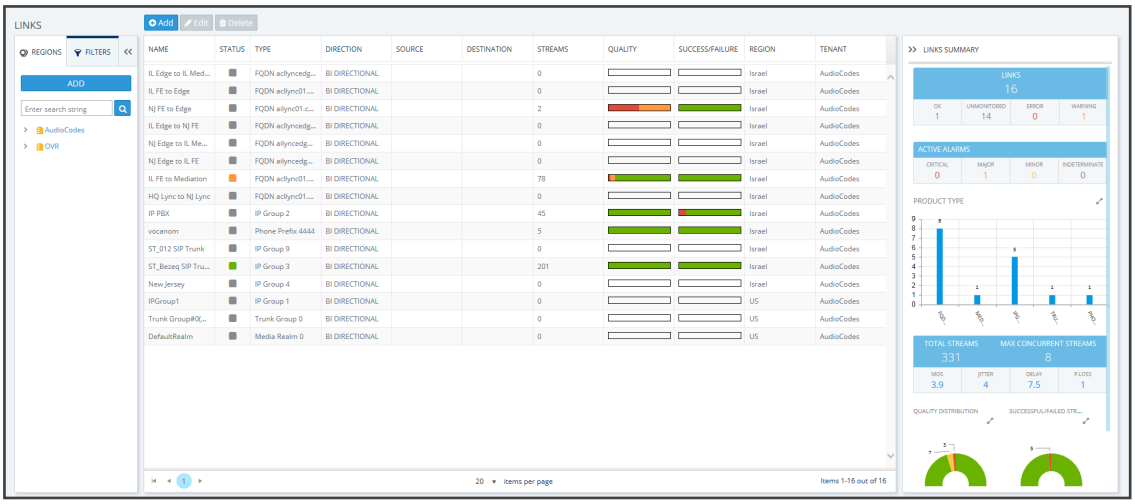
The 'source' device on which key metrics monitoring is based must be an AudioCodes device or Skype for Business device. The second device can be an AudioCodes device, Skype for Business device or a non-AudioCodes device. You can define one or more links between devices. The links are displayed in the 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 316.

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:**

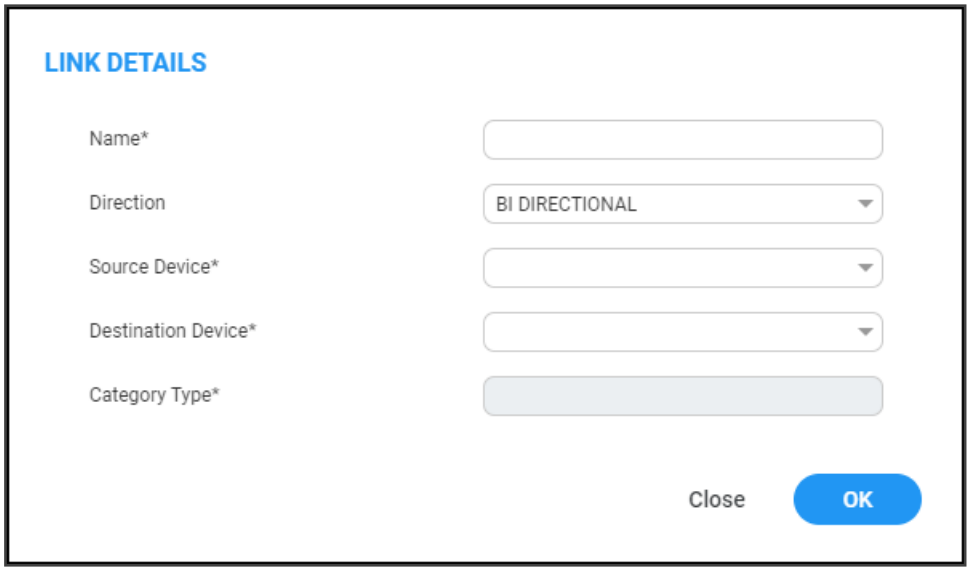
1. After configuring devices, open the Links page (**Network** > **Links**).

Figure 4-42: Links



2. Click **Add**.

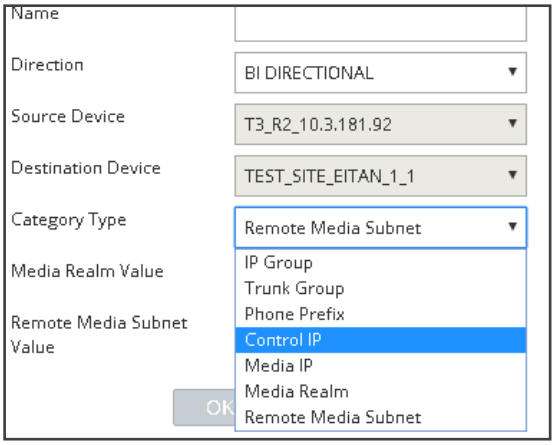
Figure 4-43: Link Details



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 **Bi Directional** (for example), a bi-directional port will be used for this connection.
Source Device	From the drop-down list, select the source device

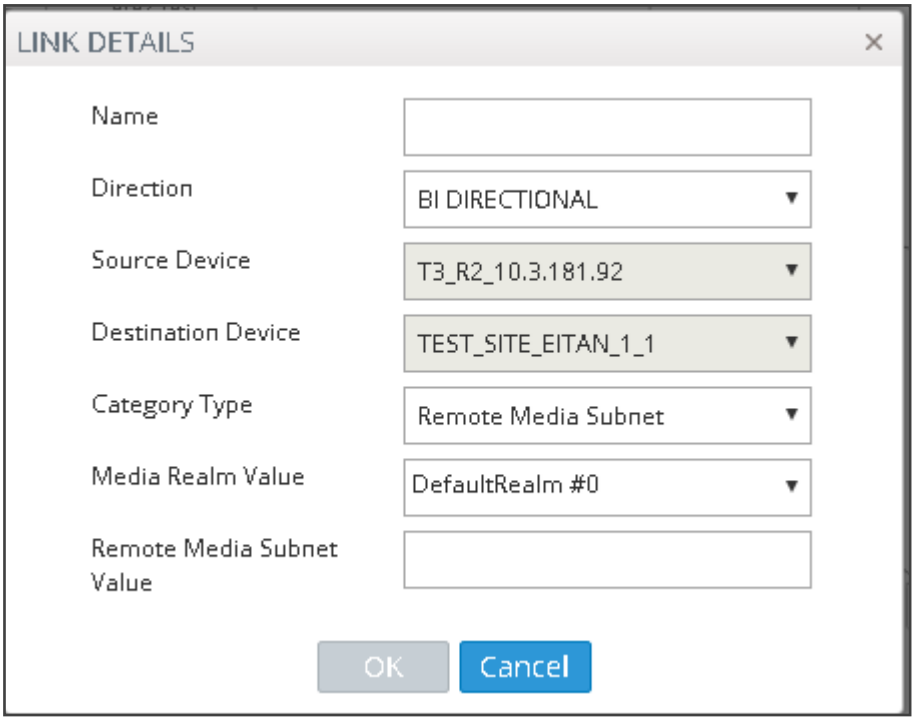
Parameter	Description
	fromwhich to link to the destination device. You can alternatively search for it.
Destination Device	From the drop-down list, select the destination device *to which* to link from the source device. You can alternatively search for it.
The link counts and computes statistics on 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. 
	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

Parameter	Description
	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.



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\\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 OVOC.

- 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.

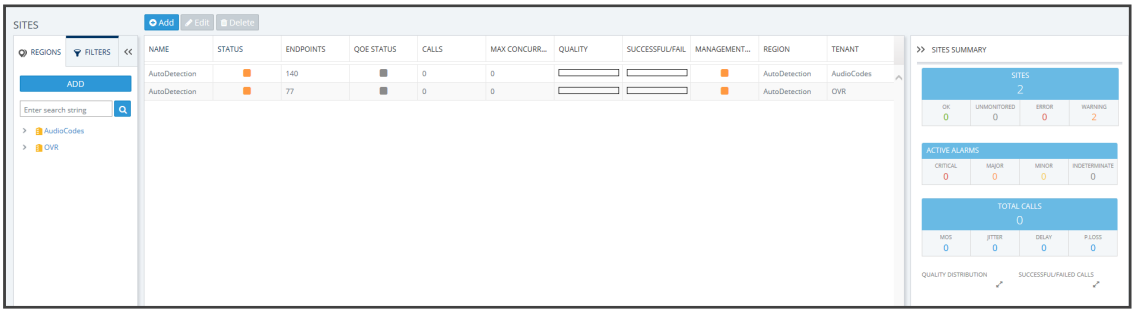
Adding Sites

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:

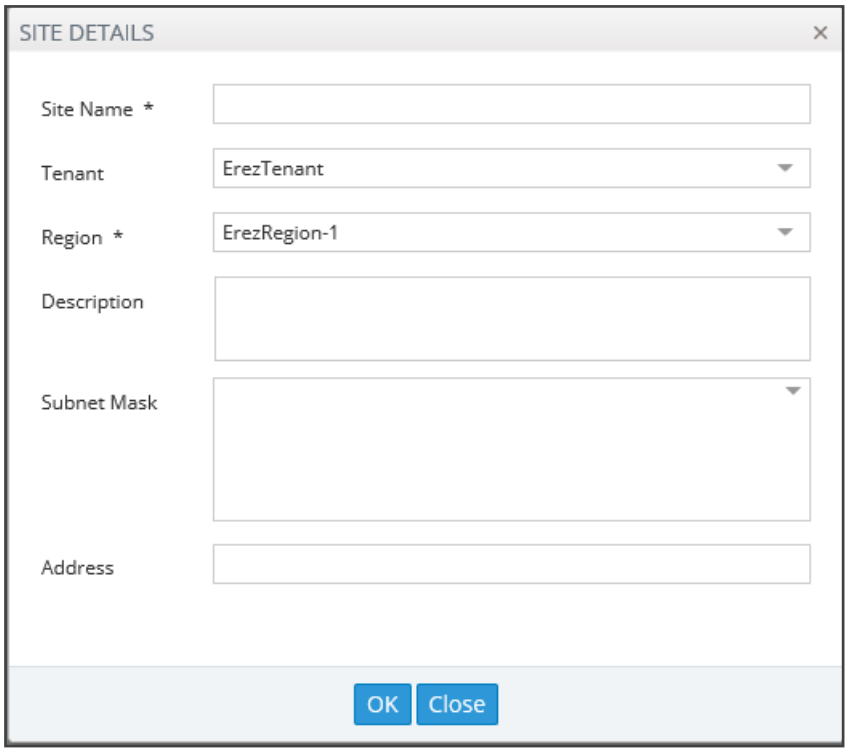
1. After configuring the region under which to locate the site, open the Sites page (**Network** > **Sites**).

Figure 4-44: Sites



2. Click **Add**.

Figure 4-45: Site Details



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

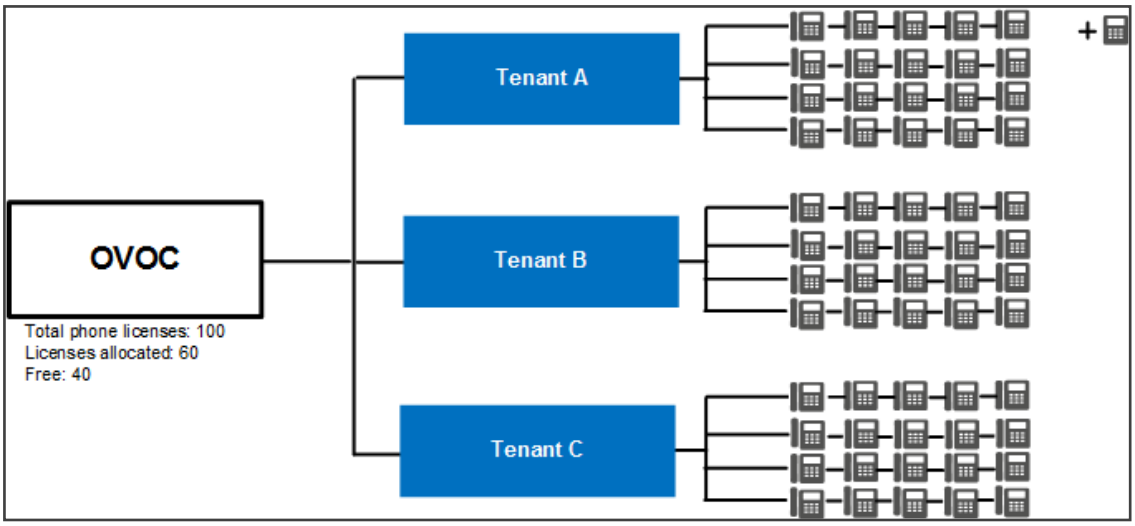
The OVOC supports endpoints management through the directly accessible Device Manager application.

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 4-46: 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.

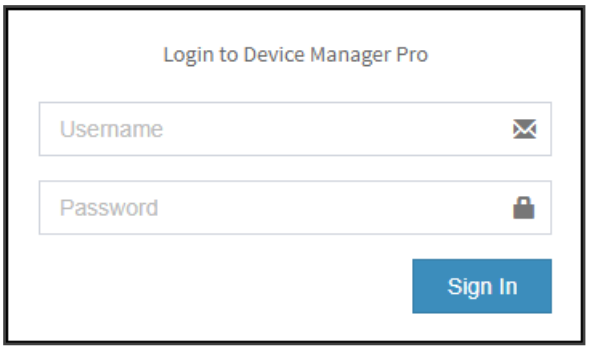
Configuring Endpoints

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

➢ **To access the Device Manager:**

1. From **Network** > **Endpoints**, select **Configurations**.

Figure 4-47: Login to Device Manager Pro



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

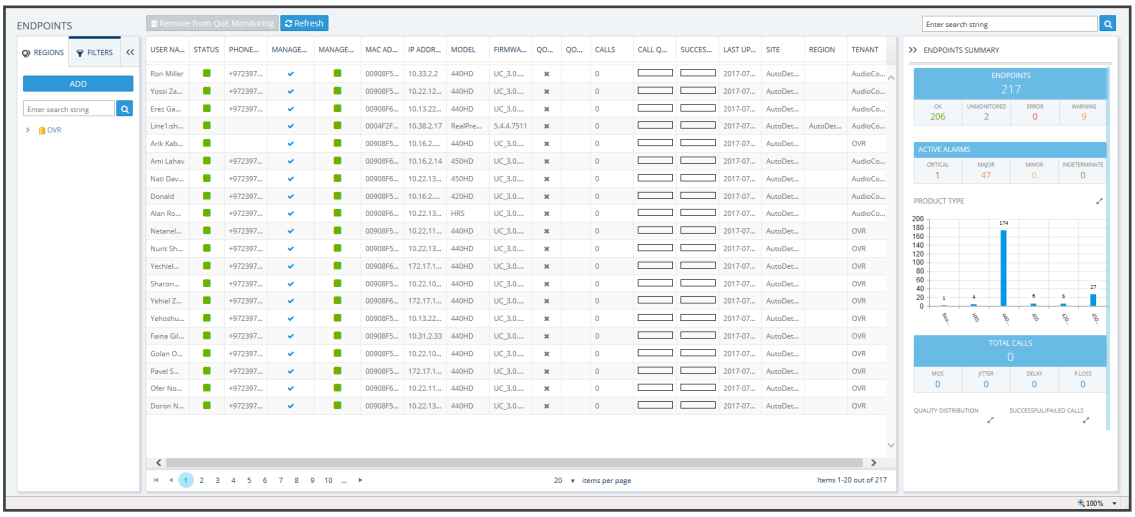
Monitoring Endpoints Status

The OVOC lets you monitor phones statuses.

➢ **To monitor phones statuses:**

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

Figure 4-48: 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 ✓.

Adding an Endpoints Group

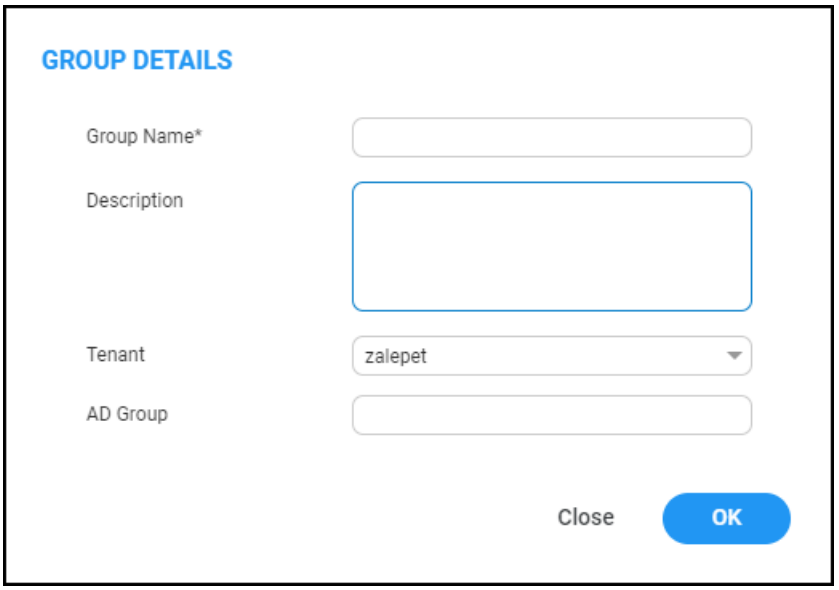
The OVOC allows you to add an endpoints group. After adding a group, use the Device Manager to add endpoints to that group and configure that endpoints group. The OVOC allows viewing added groups; it doesn't allow *adding endpoints*. See the *Device Manager Administrator's Manual* for information on how to add endpoints to groups and configure an endpoints group.

The feature benefits customers who want (for example) 10 of 500 phones in a site in the enterprise organized in a group for a software upgrade to apply exclusively to those 10 phones.

➢ **To add an endpoints group:**

1. Open the Endpoint Groups page (**Network** > **Endpoints** > **Endpoint Groups**) and click the **Add** button.

Figure 4-49: Group Details



2. Define a name for the endpoints group, provide a description to facilitate effective management later and from the 'Tenant' drop-down, select the tenant to which to add the group. Note that the selected tenant can't be changed (in the Group Details screen) after the endpoints group has been added.
3. [Applies only when operator authentication is by Azure AD / LDAP] When an operator logs in to the OVOC, the OVOC (before allowing the operator access) checks with the enterprise's Azure Active Directory / LDAP server if the endpoints group which the operator is associated in the OVOC, tallies with the endpoints group defined in the AD /

LDAP server. In the 'AD Group' field / 'LDAP Group' field, enter the name of the endpoints group. See also:

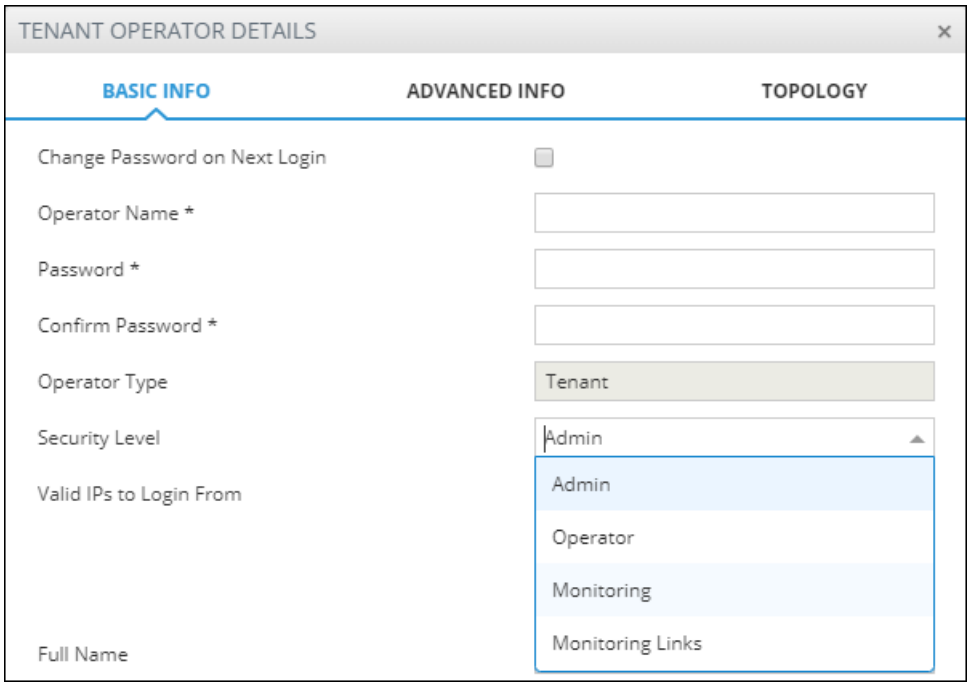
- Configuring Operator Authentication Centrally with Azure Active Directory on page 44
- Configuring Operator Authentication Centrally using an LDAP Server on page 39

Figure 4-50: Endpoint Groups page

NAME	DESCRIPTION	TENANT	ATTACHED MANAGEMENT ENDPOINTS
y_group		y_tenant	0
x_group		x_tenant	0

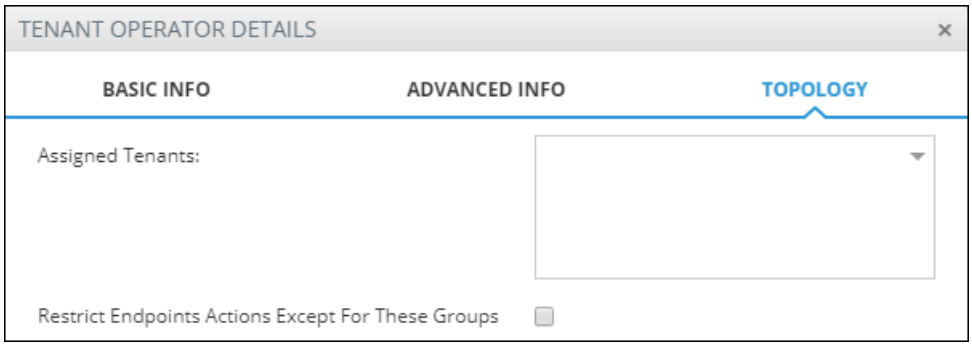
4. Observe in the Groups page shown in the preceding figure that a group named **y_group** has been added to a tenant named **y_tenant** and a group named **x_group** has been added to a tenant named **y_tenant**. Also note from the last column that no endpoints have been added yet (with the Device Manager). To quickly and efficiently locate a group, you can filter the page as shown in Filtering by 'More Filters' on page 224.
5. Configure a tenant operator to manage these groups: Open the Operators page (**System** > **Administration** > **Security** > **Operators**), click **Add** and from the drop-down select **Tenant Operator**.

Figure 4-51: Tenant Operator Details



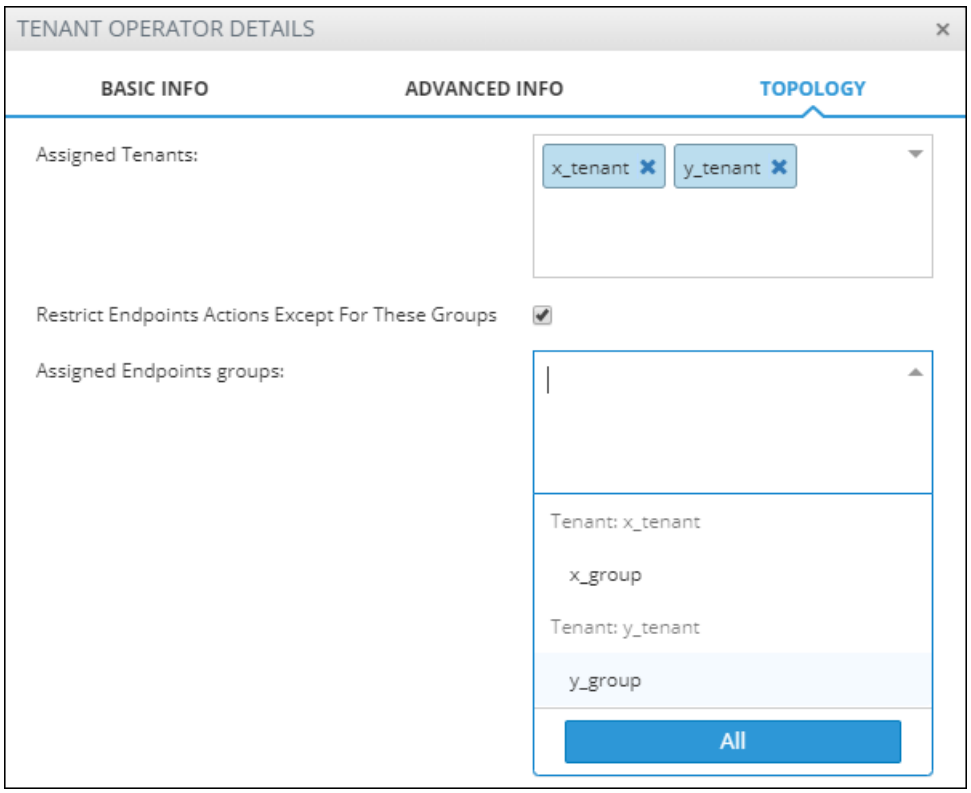
6. From the 'Security Level' drop-down, select **Admin** or **Operator**; *only these two tenant operator security levels allow assigning a group*. Configure the tenant operator details you require, click **OK** and then under the **Topology** tab, view the following:

Figure 4-52: Topology tab



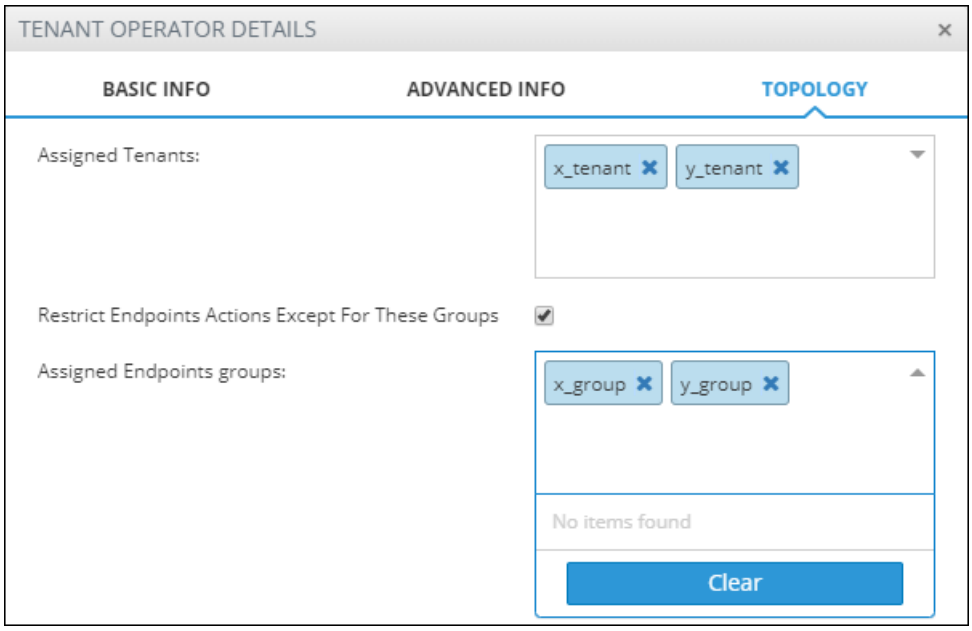
7. Note that if you didn't select **Admin** or **Operator** as the 'Security Level' in the previous step, you won't view the screen shown in the preceding figure. Assign the operator tenants (**x_tenant** and **y_tenant** as shown in the example below), check the box 'Restrict Endpoints Actions Except for These Groups' and in the 'Assigned Endpoints groups' pane that opens, assign groups to the operator tenants.

Figure 4-53: Assigned Tenants | Assigned Groups



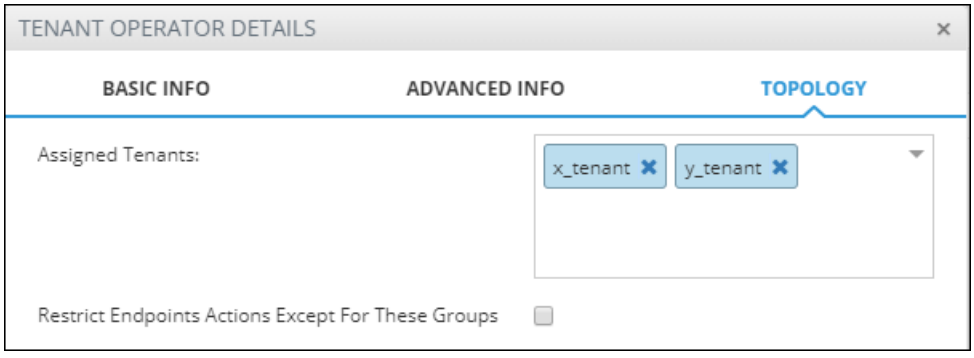
8. Click **OK**.

Figure 4-54: Assigned Endpoints groups



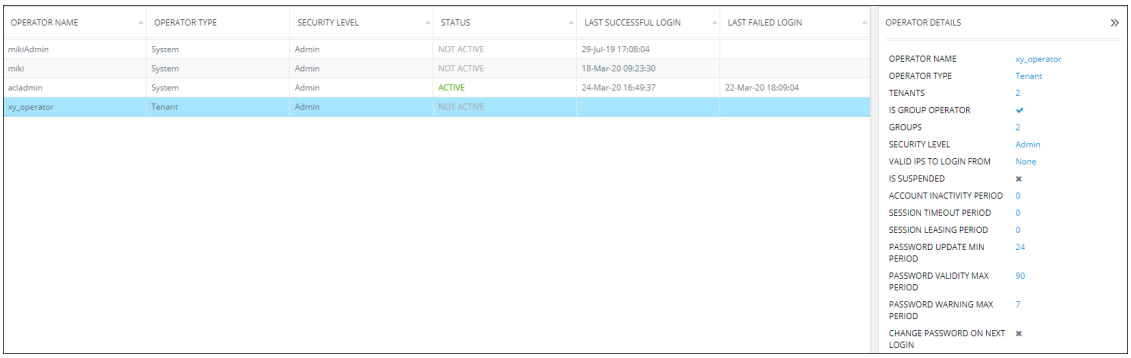
- In the 'Assigned Tenants' field, if you delete an assigned tenant then all groups assigned to that tenant will be deleted.
- When you check the 'Restrict Endpoints Actions Except For These Groups' check box, the Assign Endpoints Groups pane is displayed showing all the available assigned endpoints groups for this operator.
- When you clear the 'Restrict Endpoints Actions Except For These Groups' check box, all selected assigned endpoints groups are removed.
- Any update to an operator's assigned groups will only take effect the next login (if you're updating the groups of the operator currently logged in).

Figure 4-55: Removed groups



9. In the Operators page (**System** > **Administration** > **Security** > **Operators**), select the tenant operator that was added and view in the Operator Details pane on the right side of the page, the number of groups and tenants assigned to that operator.

Figure 4-56: Operators



If the parameter 'Is Group Operator' in the Operator Details pane is ticked as shown in the preceding figure, that operator can delete groups assigned to that operator's assigned tenants (only). The OVOC therefore allows adding, editing and deleting groups. Adding endpoints to groups and configuring those groups is performed in the Device Manager. See the *Device Manager Administrator's Manual* for information on how to add endpoints to groups and to configure endpoints groups.

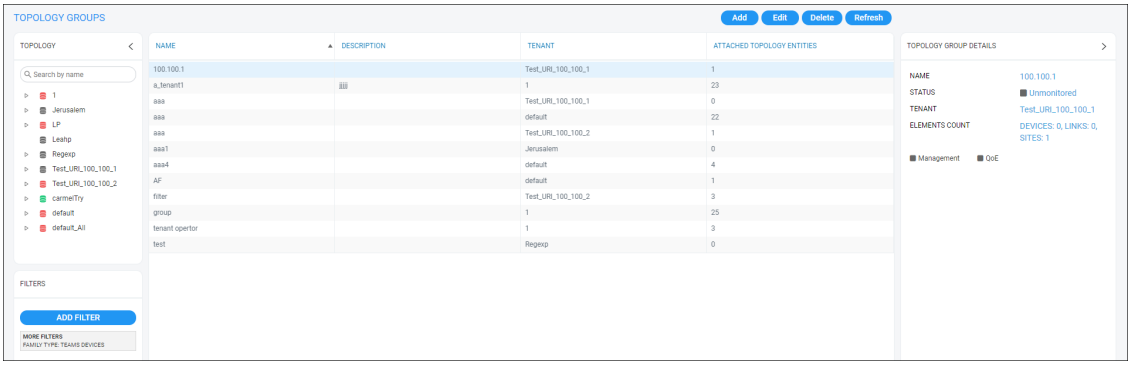
Adding a Topology Group

The OVOC allows you to add a logical group to which you can attach topology entities of your choice (devices, links, sites) so that you can then (for example) produce a report specifically on those topology entities in that group.

➢ To add a topology group:

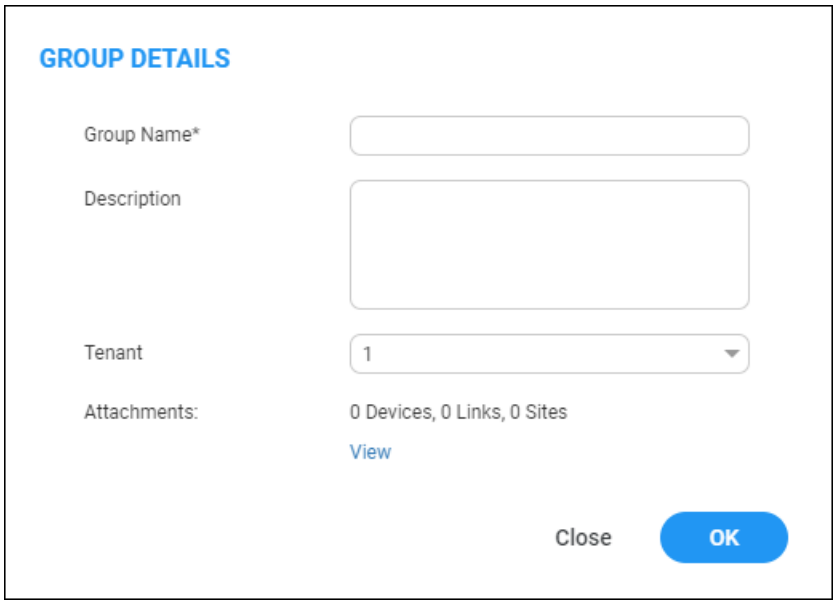
1. Open the Topology Groups page (**Network** > **Groups**).

Figure 4-57: Topology Groups



2. Click the **Add** button.

Figure 4-58: Group Details



3. Define a name for the group, provide a description to facilitate effective management later and from the 'Tenant' drop-down, select the tenant to which to add the group. Note that the selected tenant can't be changed (in the Group Details screen) after the group has been added.
4. Click the **View** link.

Figure 4-59: View



5. Navigate to and select the entities to attach and click **OK**..
6. Observe in the Topology Groups page that the group was added to the tenant. Also note from the last column how many topology entities you attached. To quickly and efficiently locate a group in the Topology Groups page, you can filter the page as shown in Filtering by 'More Filters' on page 224.

5 Managing SBC Licenses

SBC licenses can be managed using:

- **Two Floating License modes:**
  - *Cloud mode*. Replaced the legacy way of using the OVOC Advanced Monitoring package. Requires SBCs loaded with version 7.2.202 or later and OVOC version 7.4.3000 or later. See Cloud Mode on page 182 for more information.

    -OR-
  - *FlexPool mode*. Alternative licensing mode that (1) supports a Floating License across a network (2) doesn't require a connection to the public cloud (3) gracefully enforces license limits and (4) interrupts service if license limits are exceeded. Requires SBCs loaded with version 7.2.256.300 or later and OVOC version 7.8 or later. See FlexPool Mode on page 189 for more information.
- **Fixed License Pool** (see Fixed License Pool on page 195)
  - Recommended when multiple SBCs are deployed and *centrally managed*
  - 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* for more information.

Adding an SBC to the Floating License

Applies to both Floating License modes: Cloud mode *and* FlexPool mode.

Before adding an SBC to a 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 143 for more information.
- Manually from the AC Device page (**Network** > **Add** > **AC Device**).
- Using the SBC's Web interface.

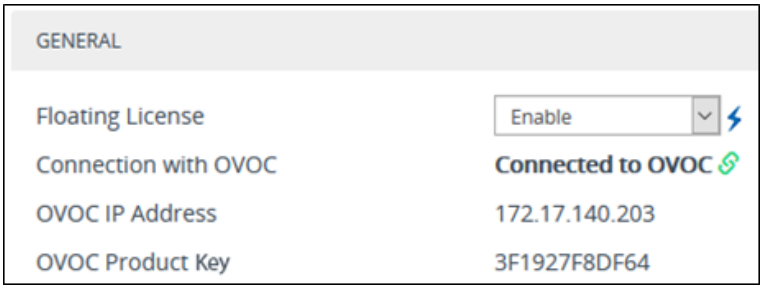
Floating License does not require configuring an open license on the SBC (obtained by ordering one of the device float CPNs, i.e., SW/M500/FLOAT).
The SBC is authorized by the OVOC to operate in a Floating License mode with no resource restrictions.

To manage a device using a Floating License mode, the device must be properly managed by the OVOC, i.e., the SBC must have a valid OVOC license.

➢ To add an SBC to a Floating License:

1. In the device's Web interface, open the Floating License page (**Setup** menu > **Administration** tab > **License** folder > **Floating License**).
2. From the 'Floating License' drop-down list, select **Enable**.

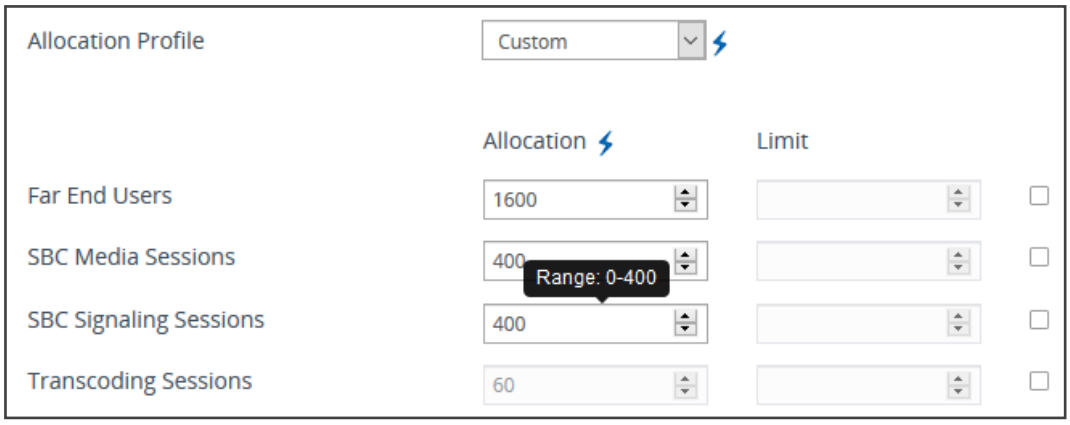
Figure 5-1: Enable Floating License



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 5-2: Maximum Capacity for Each SBC License Type

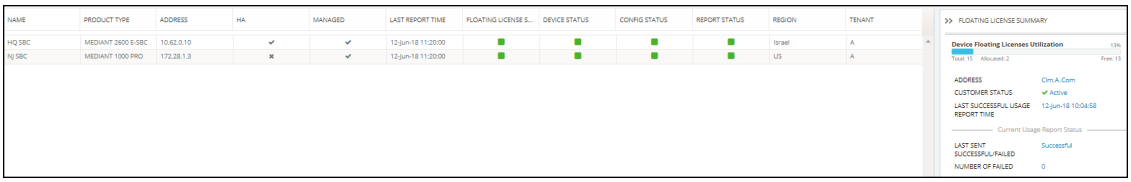


When configuring your own customized profile (i.e., using the **Custom** option), the Transcoding Session capacity license cannot be changed in the 'Allocation' field, but you can reduce the license using its corresponding 'Limit' field.

- 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**.
7. 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 5-3: Device Floating License Page – Newly Added SBC Appears in the List



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

Table 5-1: Floating License Page Column Descriptions (Applies to Cloud *and* FlexPool Modes unless Otherwise Stated)

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 Floating License is enabled / disabled in the device.	
Last Report Time	Indicates the date and time that the last usage report was sent from the device to the OVOC.	
Floating License Status	Indicates the global device status reflecting the Device Status, Config Status and Report Status states.	
	Green	**OK:** Device Status, Config Status and Report Status are green.
	Red	**Error** or **Config Error:** Indicates Device Status, Config Status or Report Status errors (red).
	Grey	**Unmanaged:** Device is unmanaged by OVOC **Unmonitored:** Device is unmonitored by OVOC
Device Status	Green	**Connected:** Device is successfully connected to the Floating License OVOC service.
	Red	**Rejected:** Device Floating License has been revoked by the Cloud Floating License service and as a result the device's CAC is reset to 0. **Not Connected**: Device is unable to establish a connection with the Floating License OVOC service (CAC 0) **Temporarily Disconnected**: Device is temporarily disconnected from the Floating License OVOC service due to problems with the HTTPS TCP connection.
	Grey	**Unmanaged:** The device is currently not managed by the OVOC Floating License service. **Unmonitored:** The device is currently

Column	Description	
		unmonitored by the OVOC Floating License service. **Not Applicable:** The device was loaded with the Floating License feature disabled. The operator must enable the feature on the SBC device and reset it.
Config Status	Green	**Success:** Indicates that the device's SNMP configuration is successfully updated.
	Red	**Failure:** 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	**Not applicable:** Indicates that the device was added to the OVOC but is not yet managed. **Unmonitored:** Indicates that the device is currently unmonitored by OVOC.
Report Status	Green	**OK:** Indicates that a report was successfully sent from the device to the OVOC for the last reporting interval.
	Yellow	**Over License**. Applies only to FlexPool. Indicates that one or more features (Media Sessions, Transcoding, Registrations, Signaling) has exceeded license limits and that an 'overLicense' status on at least one of the exceeded feature was sent from OVOC to the device.
	Red	**Failed:** Indicates there's a problem with reports sent from the device to the OVOC (missing / failed). **Failed & Over License**: [Applies only to FlexPool] Combines the two preceding statuses. Indicates that after the device's last successful report, the device received an 'overLicense' response from the OVOC and since then there has been a problem with reports from this device (missing / failed). **Not Registered**. Indicates that the device has not

Column	Description	
		yet successfully registered to the OVOC Floating License service.
	Grey	**Unmonitored:** Indicates that the device is currently unmonitored by OVOC.
Priority	Only applies to FlexPool mode. Either **High**, **Normal** or **Low**. Shows the priority configured by the operator by which SBCs are taken out of service if the FlexPool mode license is exceeded. See Configuring SBC Priority - Which to Take out of Service First on page 189 for more information.	
Region	Indicates the device's region.	
Tenant	Indicates the device's tenant.	

9. 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



Applies to both Floating License modes, Cloud mode and FlexPool mode, unless otherwise stated.

Here're the Actions you can perform in the Device Floating License page (**Network** > **Devices** > **Floating License**):

- Unmanage (see here)
- Update (see here)
- Reset (see Reset on the next page)
- Register (see Register on page 181) [only applies to Cloud mode]

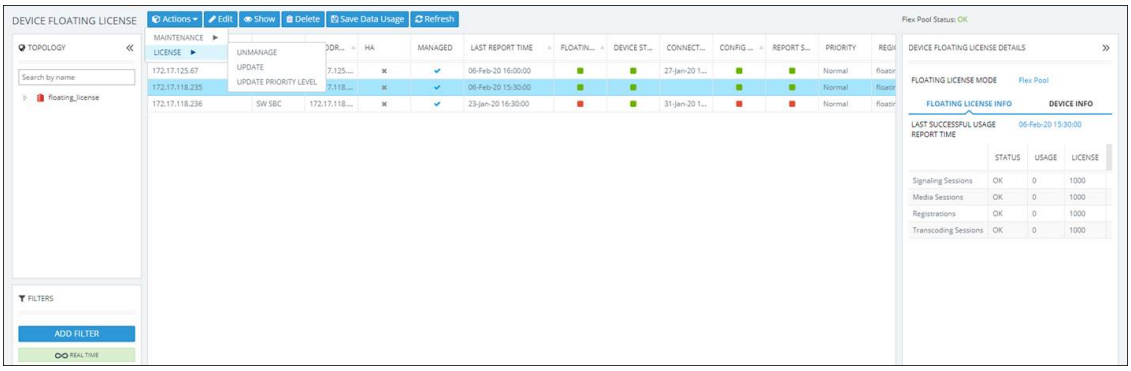
Unmanage

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 (**Network** > **Devices** > **Floating License**), select the SBC to unmanage and then from the Actions drop-down menu, select **License > Unmanage**.

Figure 5-4: Device Floating License Page – Unmanage Action



Update

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

➢ To perform an update action:

- In the Device Floating License page (**Network** > **Devices** > **Floating License**), select the SBC for which to perform an update and then from the Actions drop-down menu, select **License** > **Update**.

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).

➢ To perform a reset action:

- In the Device Floating License page (**Network** > **Devices** > **Floating License**), select the SBC for which to perform a reset and then from the Actions drop-down menu, select **Maintenance** > **Reset**.

Register

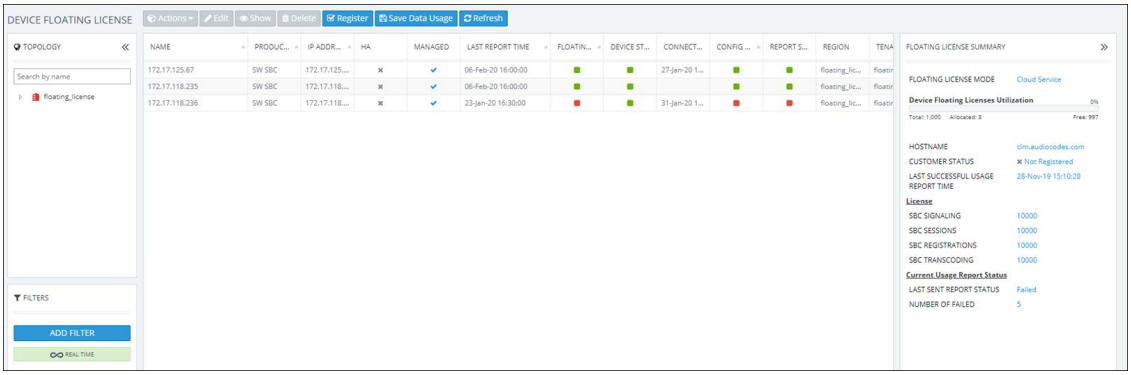
This action allows the network administrator to perform random registration to the Floating License Cloud mode service for the OVOC.

> Only applies to Cloud mode. Does not apply to FlexPool mode.

➢ To perform a register action:

- In the Device Floating License page (**Network** > **Devices** > **Floating License**), press the **Register** button shown in the figure below.

Figure 5-5: Register



Configuring OVOC-Floating License Service Communications

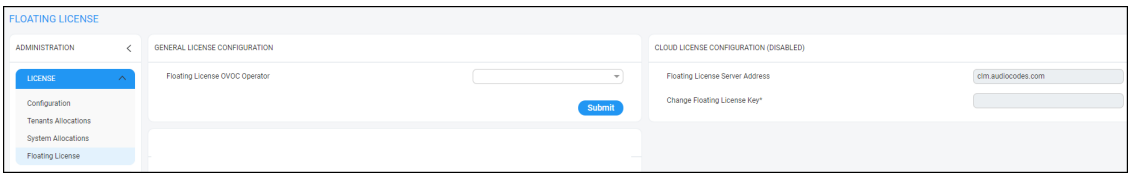
> Applies to both Floating License modes (Cloud mode and FlexPool mode) unless otherwise stated.

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 5-6: Floating License



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

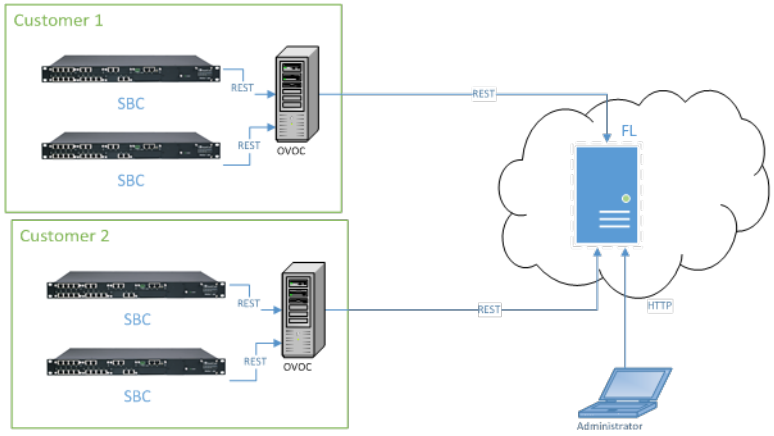
Table 5-2: Device Floating License Configuration Parameter Descriptions

Parameter	Description
Floating License OVOC Operator	Specifies the OVOC operator with REST authorization to receive and respond to REST requests from SBCs.
Floating License Server Address	[Applies only to Cloud mode; N/A to FlexPool mode] Specifies the server address of the Floating License Service platform: **CLM.audiocodes.com** (default)
Change Floating License Key	[Applies only to Cloud mode; N/A to FlexPool mode] 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 (**System** > **Administration** > **License** > **Summary**).

Cloud Mode

Cloud mode can be configured on AudioCodes SBCs and the OVOC. Cloud mode replaced the legacy method of using the OVOC Advanced Monitoring package. Cloud mode requires SBCs loaded with version 7.2.202 or later and OVOC version 7.4.3000 or later. For more information, see also the device's *User's Manual*.

Figure 5-7: Cloud Mode Network



Here's how Cloud mode 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 Cloud mode 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 mode 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.

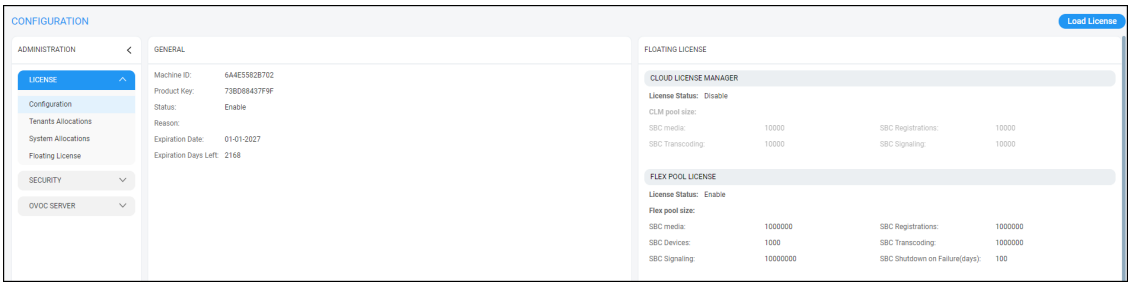
Configuring Cloud Mode

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

➢ To configure the OVOC:

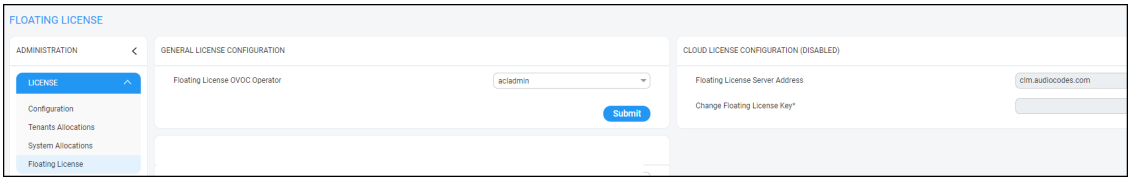
1. Add a new OVOC operator of type 'System' dedicated to the Floating License (i.e., 'Floating License_User').
   - They must have Admin or Operator security level
   - Password expiration must be set to never expire
   - SBCs use them to communicate with the OVOC for the floating license reports
2. 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 the status is **Enable**.

Figure 5-8: Cloud License Manager Status



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

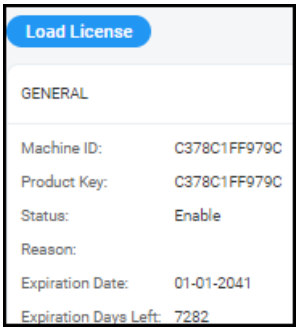
Figure 5-9: Floating License



4. Configure the parameters like this:

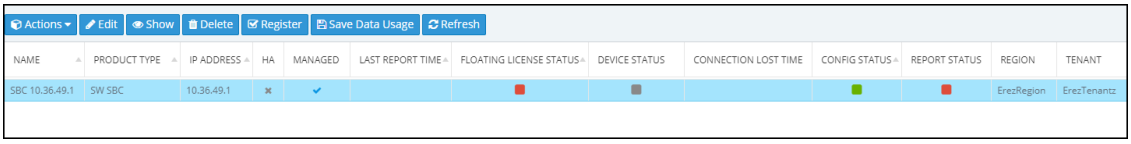
- **Floating License OVOC Operator**: Use the new operator you configured here.
- **Floating License Server Address**: Set to: **clm.audiocodes.com**
- **Change Floating License Key**: Set to the OVOC Product Key. To find out the OVOC Product Key, view the string in the License Configuration screen (**System**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

Figure 5-10: Product Key



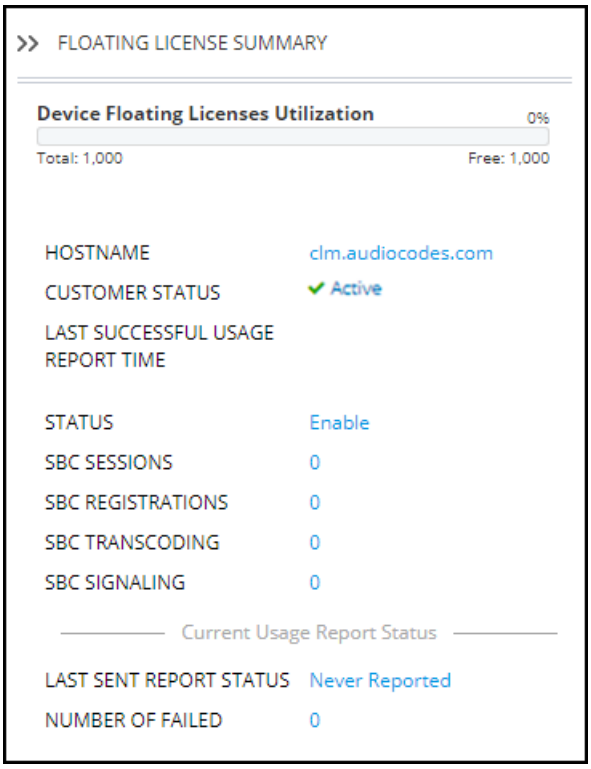
5. Open the Device Floating License page (**Network** > **Devices** > **Floating License**).

Figure 5-11: Device Floating License Page



- 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 5-12: Customer Status



A new OVOC with an old Feature Key will show zeros in the screen when operating in Cloud mode. Reactivating the product key and reinstalling the Feature Key solves the issue.

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 187)
- Device Info pane (see Viewing Device Info on page 187)

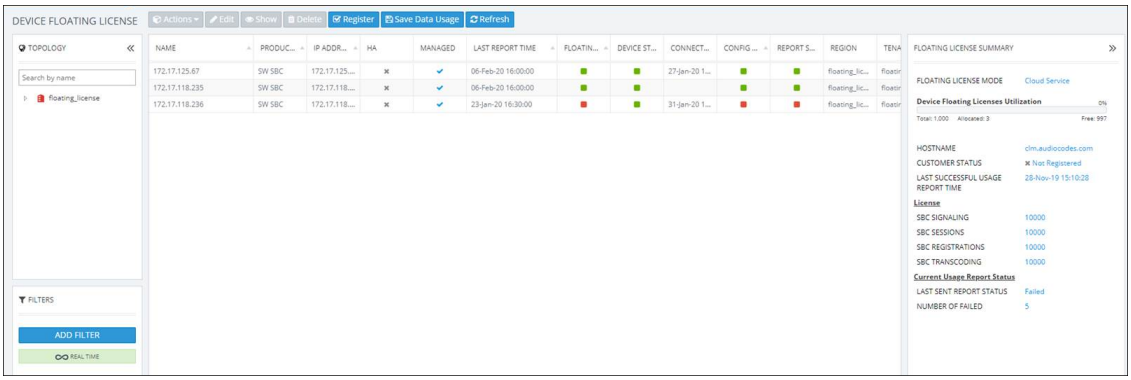
Device Floating License Utilization Pane

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 5-13: 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
Device Floating Licenses Utilization	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.
Hostname	Indicates the IP address or FQDN of Floating License Service.
Customer Status	Indicates the state of the connection with the Floating License service. **OK** - Indicates that a successful connection with the Floating License service has been established. **Blocked** - Customer account has been blocked by the Floating License service. **Unknown** - Status is undetermined by the OVOC **Not Registered** - OVOC has not registered successfully to the Floating License Cloud mode service
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.
License	Displays a summary of the license features SBC Signaling, SBC Sessions, SBC Registrations and SBC Transcoding.
Last Sent Report Status	Indicates whether the last attempt to send a usage report to the Floating License Cloud service was successful.

License Utilization	Description
Number of Failed	Indicates the number of failed attempts to send usage reports to the Floating License Cloud service

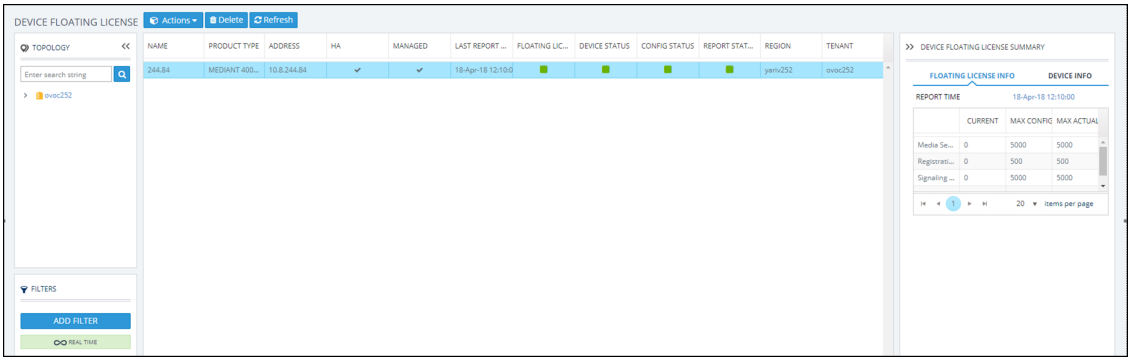
Viewing Floating License Info

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



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.

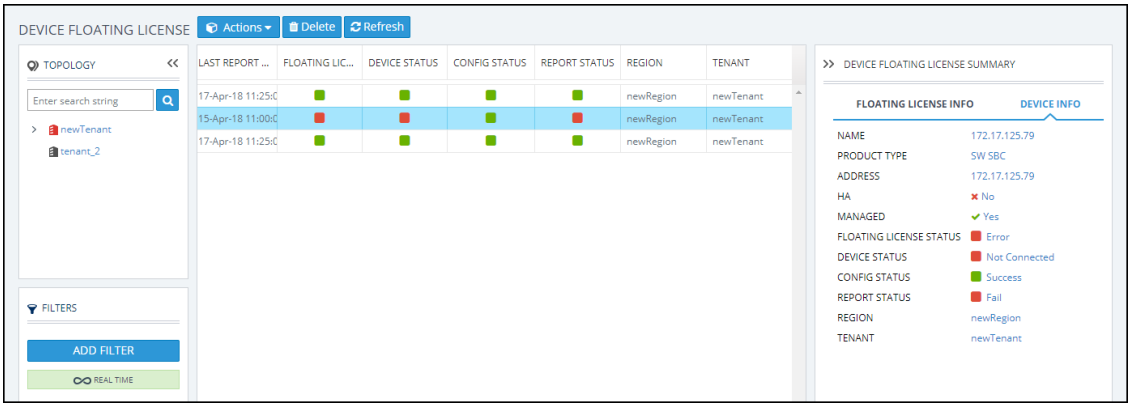
Viewing Device Info

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 5-15: Device Floating License Summary – Device Info



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

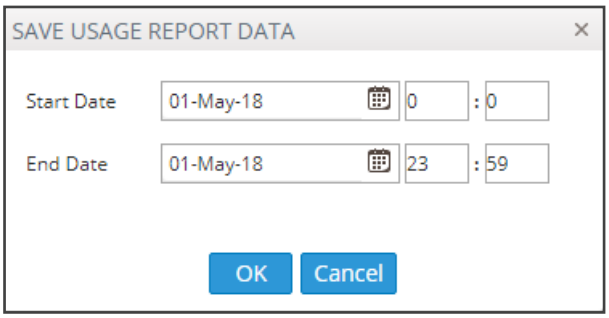
This feature allows customers to save reports to CSV file. Each report includes the currently configured license session values and the device's HA state.

> In Cloud mode, reports are *always* sent to the cloud. In both Cloud mode and FlexPool mode, reports are always sent from the SBC to the OVOC.

➢ **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 5-16: Save Usage Report Data



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**.

FlexPool Mode

After adding an SBC to the Floating License as shown in Adding an SBC to the Floating License on page 174 and configuring OVOC-Floating License service communications as shown in Configuring OVOC-Floating License Service Communications on page 181, FlexPool mode can be configured on SBCs and the OVOC. FlexPool is an alternative licensing mode provided by AudioCodes that (1) supports a Floating License across a network (2) doesn't require a connection to the public cloud (3) gracefully enforces license limits and (4) interrupts service if license limits are exceeded. FlexPool mode is supported from SBC version 7.2.256.300 or later.

FlexPool mode is a system-level feature; it's not applicable per tenant.

FlexPool mode is different to Cloud mode: There's no Cloud License Manager component and customer limits are enforced by limiting service rather than by post-usage billing. SBCs and the OVOC are the components involved in FlexPool mode.

If an SBC or OVOC failure occurs or if a network issue occurs, FlexPool mode continues to provide customer service for a period of grace.

Configuring an Alarm Threshold Percentage for FlexPool Mode

The OVOC enables operators to configure an alarm threshold percentage for FlexPool mode.

➢ **To configure an alarm threshold percentage for FlexPool mode:**

1. Open the Floating License page (**System** > **Administration** > **License** > **Floating License**) and locate the FlexPool Configuration section.

Figure 5-17: FlexPool Configuration



2. Optionally change the default of 85% to a different alarm threshold percentage according to preference. Range: 0-100.

If for example you leave the configuration at the default of 85%, the OVOC will raise an alarm for each license parameter whose current total sum of licensing usage is above 85% but below the license violation threshold. See also Determining License Status from Alarms on the next page.

Configuring SBC Priority - Which to Take out of Service First

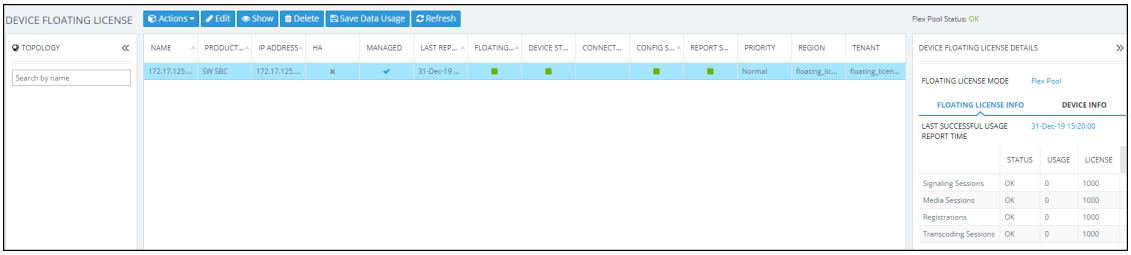
The OVOC uses a priority configured by operators to determine the order by which SBCs are taken out of service if the FlexPool mode license is exceeded. Priority values are High, Normal

or Low.

➢ To configure SBC priority:

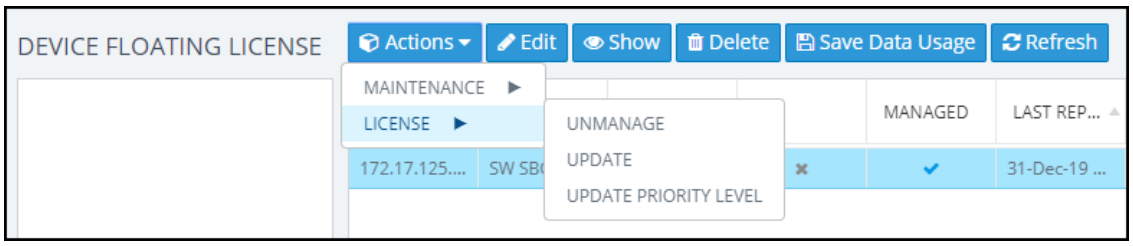
1. Open the Device Floating License page (**Network** > **Devices** > **Floating License**).

Figure 5-18: Device Floating License

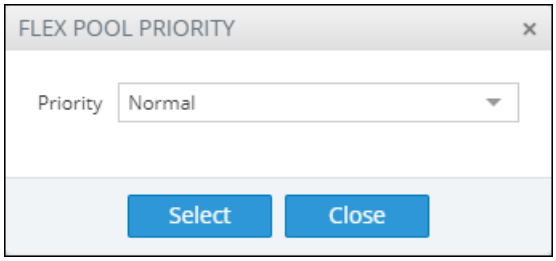


2. Select the SBC whose priority you want to configure and from the **Actions** button drop-down, select **License** > **Update Priority Level**.

Figure 5-19: Update Priority Level



3. From the 'Priority' drop-down in the FlexPool Priority prompt shown in the figure below, select either **Normal** (default), **High** or **Low**.



If overuse of the license occurs, the OVOC gradually starts taking SBCs out of service based on the priority defined by the operator. After capacity is restored, SBC service resumes.

Determining License Status from Alarms

The OVOC sends alarms that allow network administrators to determine license status. For more information, see the *One Voice Operations Center Alarms Guide*. When OVOC is started up or reset, it closes these alarms if they exist.

The 'Alarm on % of utilization' parameter can be

- configured by the 'System' type operator whose security level is defined as 'Admin'
- viewed by the 'System' type operator whose security level is defined as 'Admin', 'Operator' or 'Monitor'

If service is interrupted, the SBC sends a FlexPool License Alarm and closes it after service resumes to normal.

Determining License Status from the Network Summary

The Floating License Summary pane in the OVOC's Device Floating License page allows network administrators to determine at a glance the status of their FlexPool mode license.

➢ To view the summary:

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

Figure 5-20: Device Floating License Page

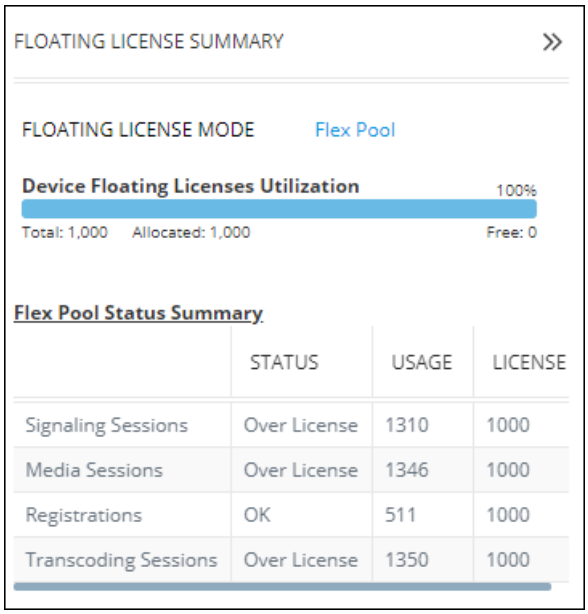


2. Locate the Floating License Summary pane on the right. *Above the pane*, view the **FlexPool Status** indication. In the preceding figure, 'FlexPool Status' indicates **OK**. This is a *system-level status indication* summarizing the **FlexPool Status Summary** table displayed in the Floating License Summary pane. Three possible statuses can be displayed:
   - **OK** [The statuses of all features in the **FlexPool Status Summary** table are 'OK']
   - **Warning** [The status of at least one feature in the **FlexPool Status Summary** table is 'Warning' and the status of none is 'Over License']
   - **Over License** [The status of at least one of the features in the **FlexPool Status Summary** table is 'Over License']

➢ To access the Floating License Summary pane:

- Open the Device Floating License page (**Network** > **Devices** > **Floating License**) and locate the Floating License Summary pane on the right.

Figure 5-21: Floating License Summary - FlexPool



The pane indicates:

- Floating License mode: **FlexPool**
- Device Floating Licenses Utilization: Total, Allocated and Free; indicates *the number of SBCs* using this service, i.e., *the number of SBCs* operating under FlexPool mode. Note that this is *not an indication of pool size*.
- FlexPool Status Summary
  - The status, usage and license limit of each dimension covered by the license: Signaling Sessions, Media Sessions, Registrations and Transcoding Sessions; other dimensions still require an appropriate license on the SBC so if (for example) you want to enable Microsoft Teams, you'll need a license on the SBC in addition to the FlexPool License. SBC capacity and features are still subject to the configuration of the SBC profile user and the device's capacity; although FlexPool License mode is a network-wide license, you can still limit the capacity of individual SBCs using the device's Web interface.
  - Status is OK, Warning (alarm sent according to the value configured for 'Alarm Threshold Configuration') or Over License (the limit has been exceeded and service has been stopped).
  - Usage column: Displays the aggregated consumption of each license dimension across all SBCs running under FlexPool mode. If usage exceeds the value defined in the license, the SBC stops service until a successful response is received from the OVOC indicating that usage no longer exceeds that value. The OVOC *gradually* stops the service according to the priority assigned to the SBCs as shown in Configuring SBC Priority - Which to Take out of Service First on page 189.

License information can be accessed from the License Configuration page accessed from **System** > **Administration** > **License** > **Configuration**:

Figure 5-22: FlexPool Mode Status



The preceding figure shows the *size allocated to each FlexPool mode license dimension*, i.e., the size of each dimension you have in your FlexPool mode license. Note that **SBC Shutdown on Failure (days)** indicates *number of days*; if a failure occurs in the reports sent between the device and OVOC and the issue isn't fixed within the number of days displayed, the device will shut down FlexPool mode service and will not allow new calls.

Migrating from Cloud Mode to FlexPool Mode



Applies to customers currently using Cloud mode whose version of the OVOC is earlier than 7.8 and whose SBC version is earlier than 7.2.256.

➢ To migrate from Cloud mode to FlexPool mode:

1. Upgrade the OVOC to version 7.8 (see the *OVOC IOM Manual*).
2. Upgrade the SBCs to version 7.2.256 (see the *SBC User's Manual*).
3. Replace the OVOC license with FlexPool mode (see the *OVOC IOM Manual*).
4. Restart the OVOC.



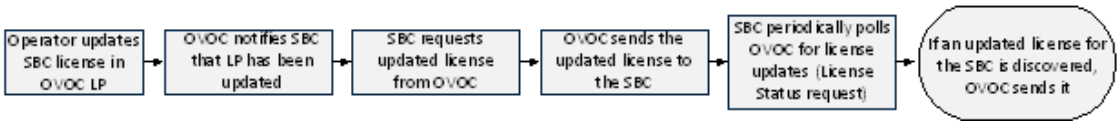
Customers *can* replace the license *before* upgrading the SBCs but then SBCs that do not support FlexPool mode will fail to report to the OVOC (because a continuous connection between the OVOC and SBCs needs to be maintained). Customers will then have up to 90 days to upgrade their SBCs. Contact your AudioCodes representative if necessary. This is not the recommended migration procedure.

Fixed License Pool

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.

> Only a 'tenant' operator can manage the Fixed License Pool. To configure a 'tenant' operator, see License Pool Operator on page 114 for more information.

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:

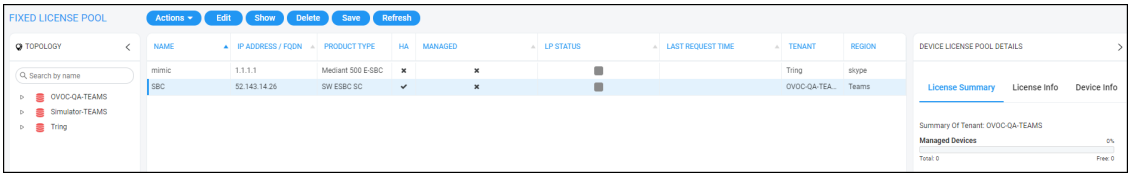
- allocate licenses to any SBC managed by the OVOC
- move licenses from any SBC back to the License Pool
- move licenses from one SBC to another
- purchase additional licenses for the pool at any time

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** > **Fixed License Pool**).

Figure 5-23: Fixed License Pool



2. 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

Icon	Description
	License Pool status is APPLY NEEDED
	License Pool status is APPLY IN PROGRESS
	License Pool status is RESET NEEDED

3. Click the **Refresh** button.

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

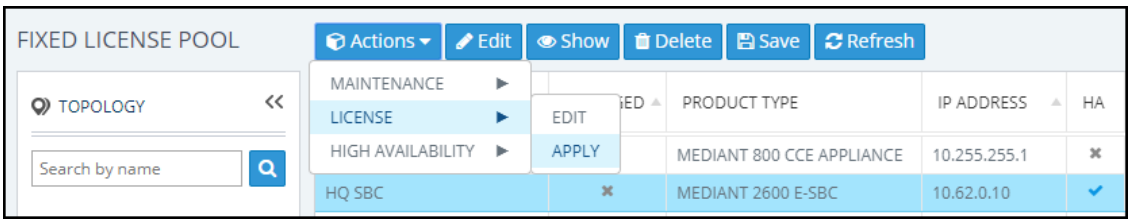
You can apply a license to a device.

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

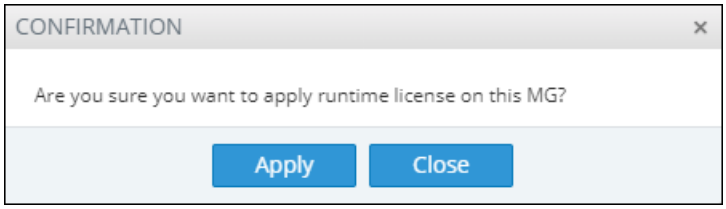
➢ To apply a license to a device:

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

Figure 5-24: Apply License



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



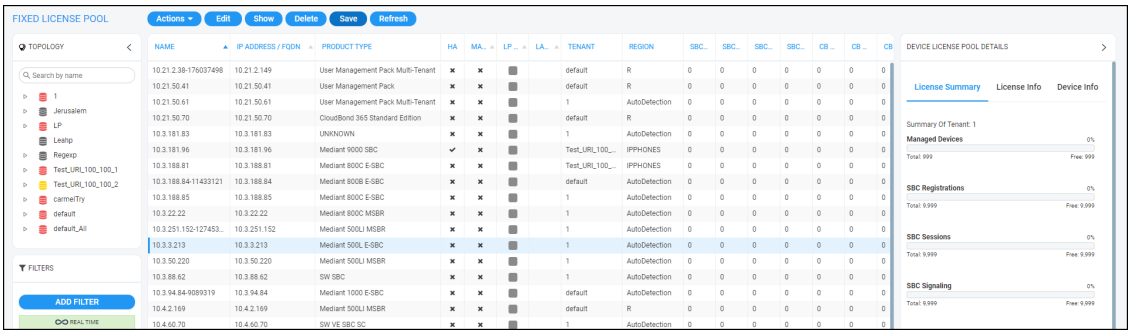
Saving Fixed License Pool Data to CSV File

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.

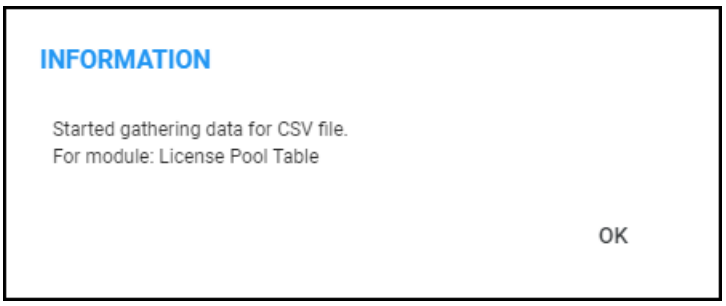
➢ To export Fixed License Pool data to a CSV file:

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

Figure 5-25: Fixed License Pool

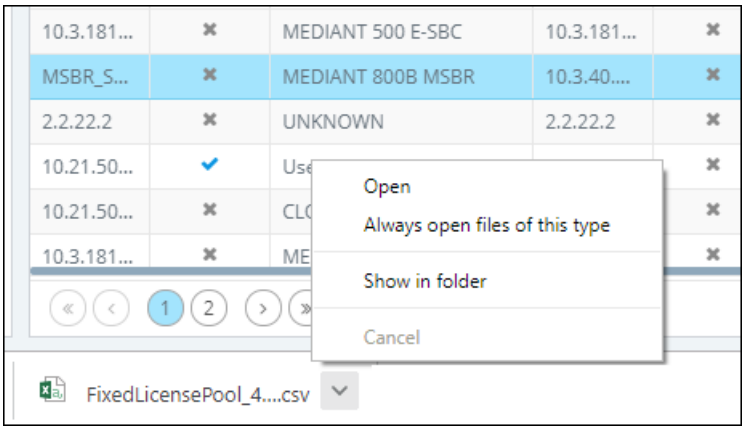


2. Select the device and click **Save**.



3. Click **OK**; locate the saved CSV file whose icon is displayed in the lower left corner, 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:

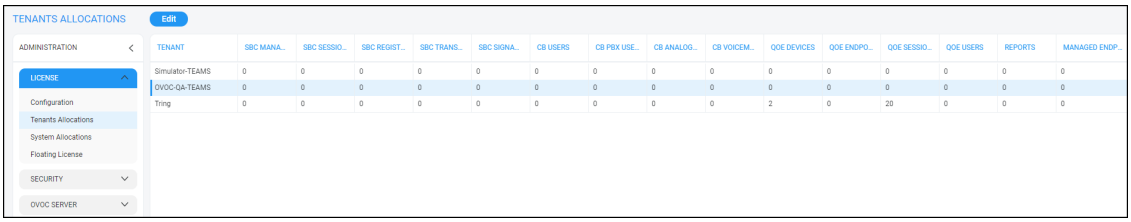
- sbcSession_pool
- sbcSession_local
- sbcSession_actual
- sbcSession_active

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 5-26: 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, is not blocked and expiration is 'Never expired' (recommended): In the Network Topology page, select the tenant in the navigation tree, click ⋮ and choose the edit option:

Figure 5-27: Edit Tenant

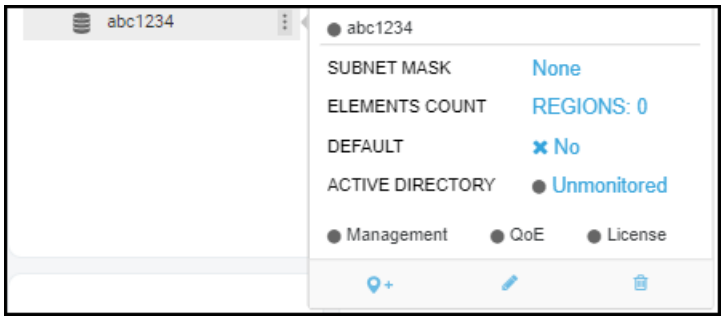
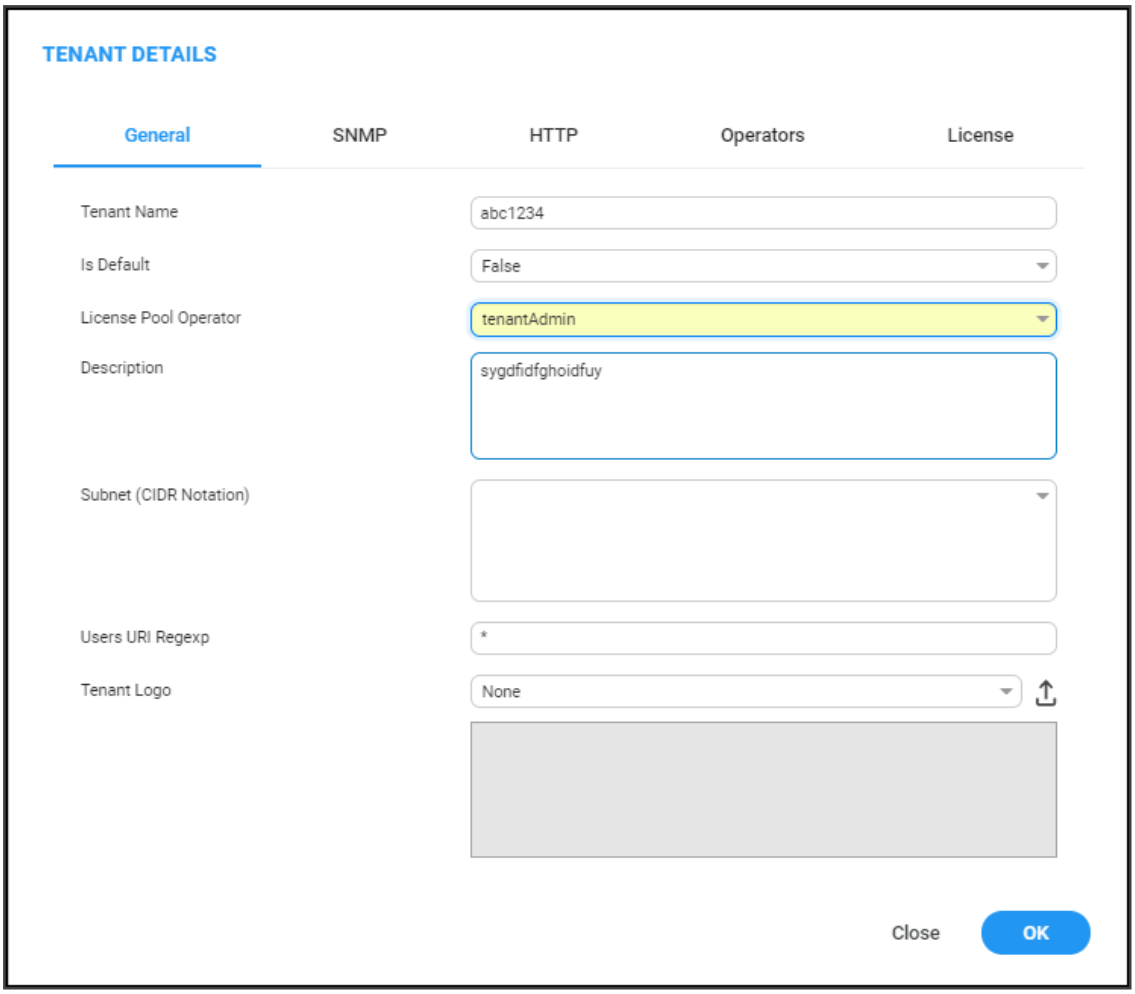
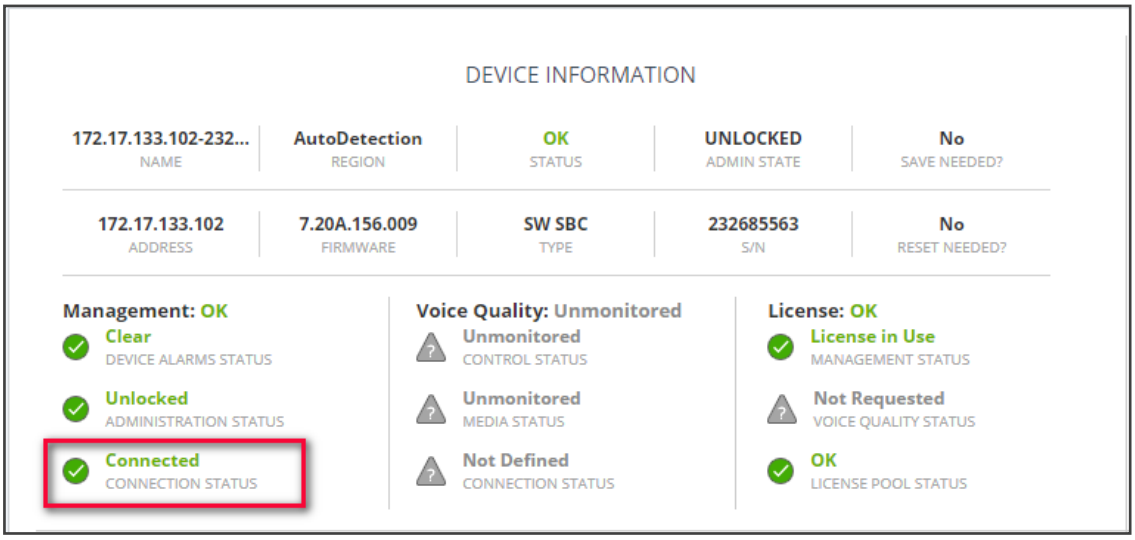


Figure 5-28: Make Sure 'License Pool Operator' is Valid



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

Figure 5-29: Make Sure the Device is Connected to the OVOC



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*.

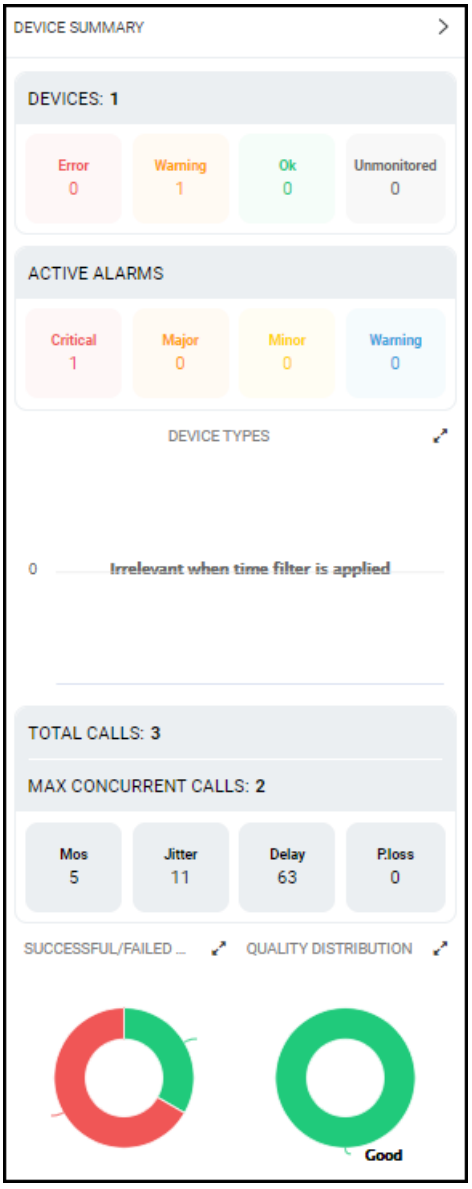
6 Assessing Network Health

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.

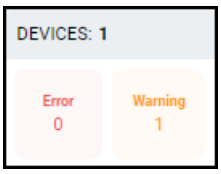
Figure 6-1: Network Summary

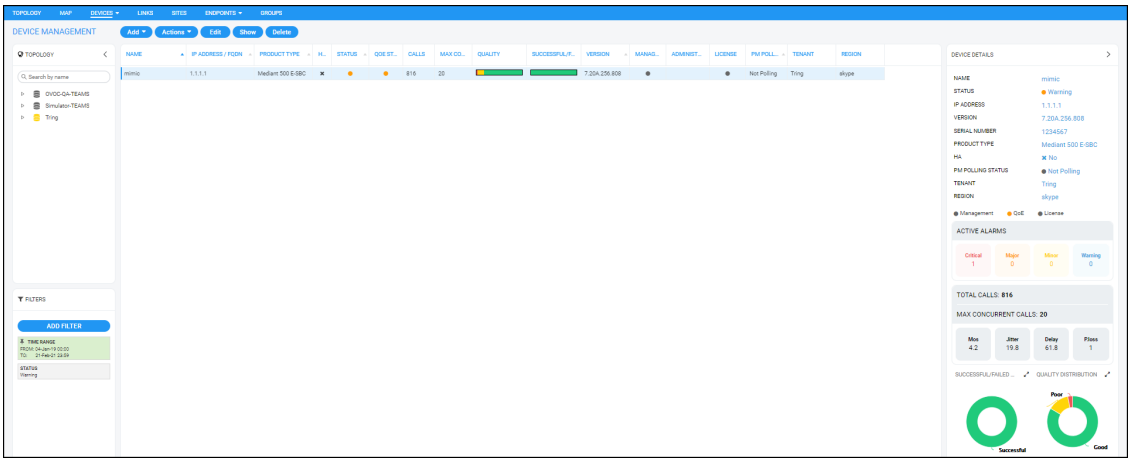


- The four upper Network Summary panes display:
  - The count of Devices, Links, Sites and Endpoints on which alarms are currently active.

- 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

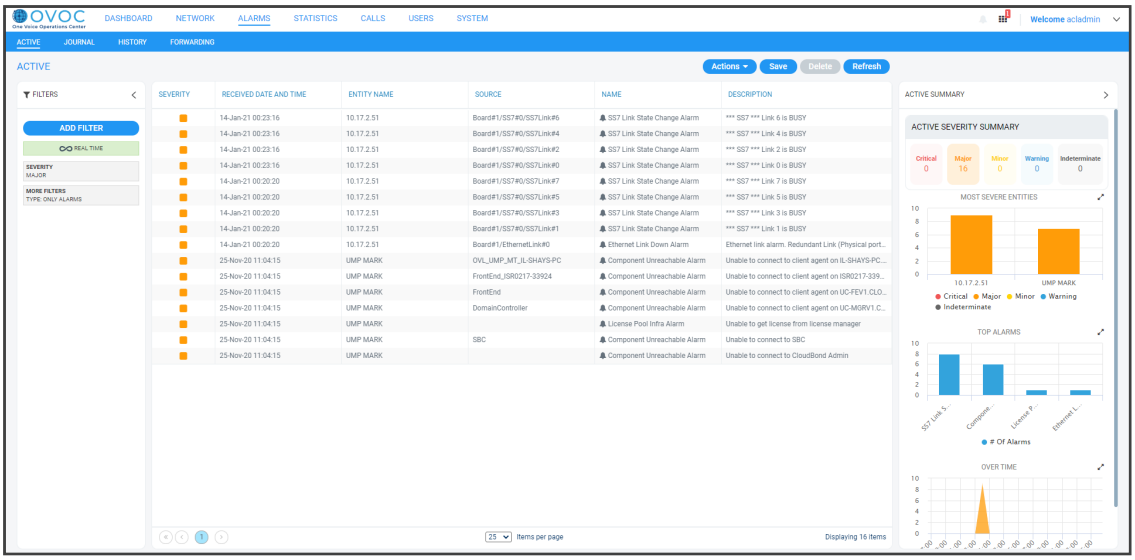
Figure 6-2: Example: 1 Device Warning





- 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

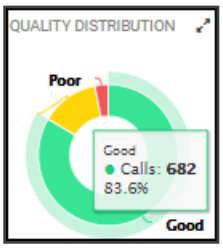


You can select an alarm in the page to view detailed information about it in the All Alarm Details pane on the right side of the page.

- 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

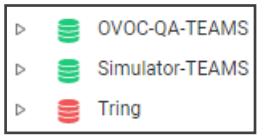
  - Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over endpoints in the network whose quality was measured to be good, fair or poor respectively.

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:



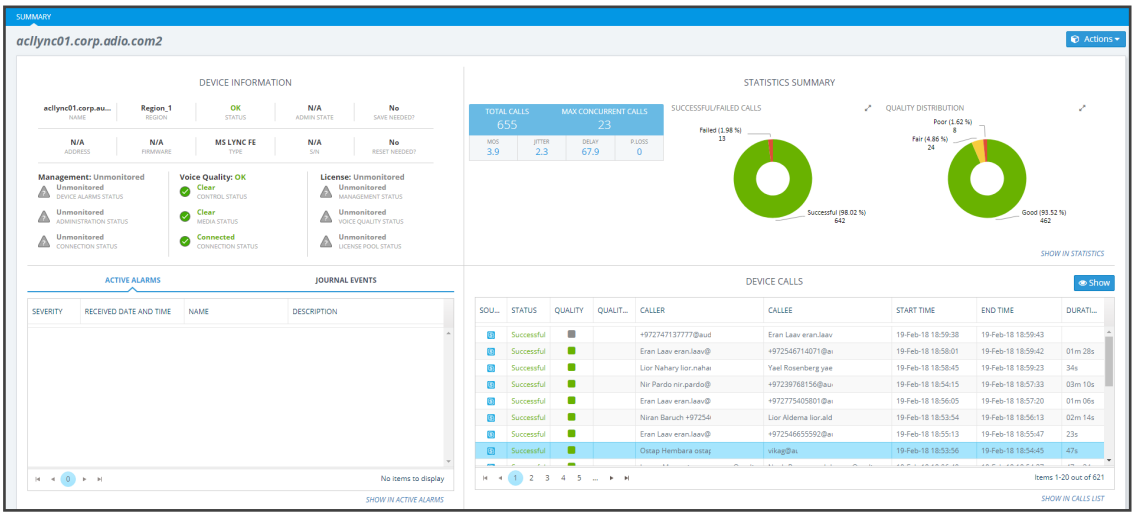
A red-coded tenant icon indicates that there is an alarm in the tenant, or that an OVOC threshold for voice quality has been exceeded in the tenant. This is the first-level navigation level.

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.	■ Critical ■ Major ■ Minor ■ Warning ■ Indeterminate ■ Clear
	Administration Status	Indicates the status of the device's administration	■ Locked ■ Unlocked
	Connection Status	Indicates the status of the device's SNMP connectivity	■ Connected ■ Not Connected
Voice Quality	Control Status	Indicates the status of the calls control as defined in the QoE Status and Alarm rule for this device	■ Unmonitored ■ Clear ■ Major ■ Critical
	Media Status	Indicates the status of the calls media as defined in the QoE Status and Alarm rule for this device	■ Unmonitored ■ Clear ■ Major ■ Critical
	Connection Status	Indicates the status of the QoE connection	■ Not Defined – the device never connected for calls sending ■ Connected – device is currently connected and sending calls ■ Not Connected – device was disconnected;

Info About	Status Type	Description	Values
			possible reasons: time synchronization between device and OVOC server, device was connected but for some reason closed the connection (disabled QoE reporting)
License	Management Status	Indicates the status of the license management	■ Not Defined ■ Managed - device license contains management license ■ Unmanaged - device license does not contain management license
	Voice Quality Status	Indicates the status of the voice quality	■ Not Requested – device does not require a Voice Quality License ■ Managed – device requires and receives a Voice Quality License from the OVOC server ■ Unmanaged – device requires a Voice Quality license but the OVOC server can't assign a license for this device
	OVOC License Status	Indicates the status of the OVOC license	■ Unmanaged ■ If License Pool is configured (same status as the status in the Fixed License Pool table)

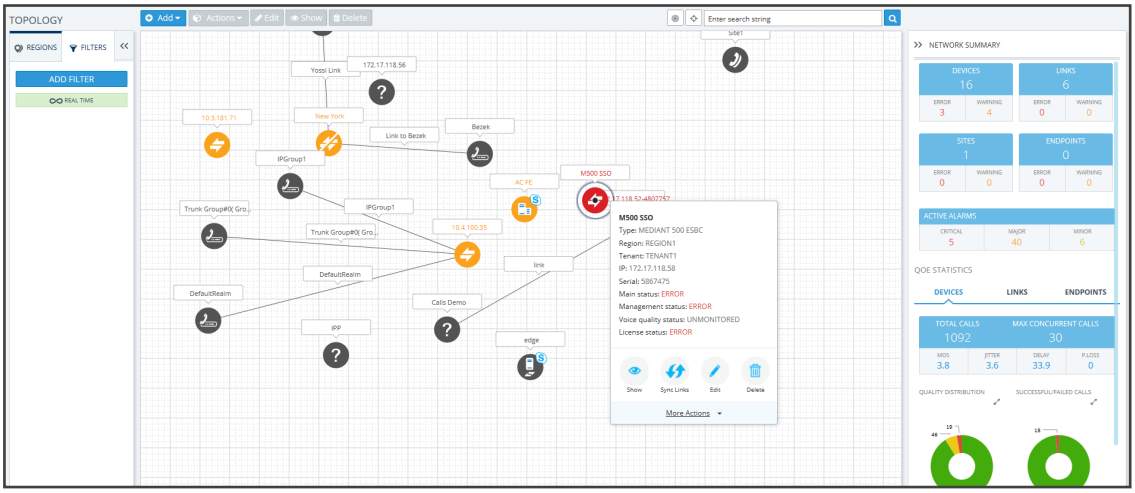
Info About	Status Type	Description	Values
			■ If Floating License is configured (same status as the status in the Floating License table)

- For information about the page section 'Device Calls', see Accessing the Calls List on page 316. 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 265 and specifically Statistics Summary on page 269. 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 227 and Viewing Journal Alarms to Determine Operator Responsibility on page 237. 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



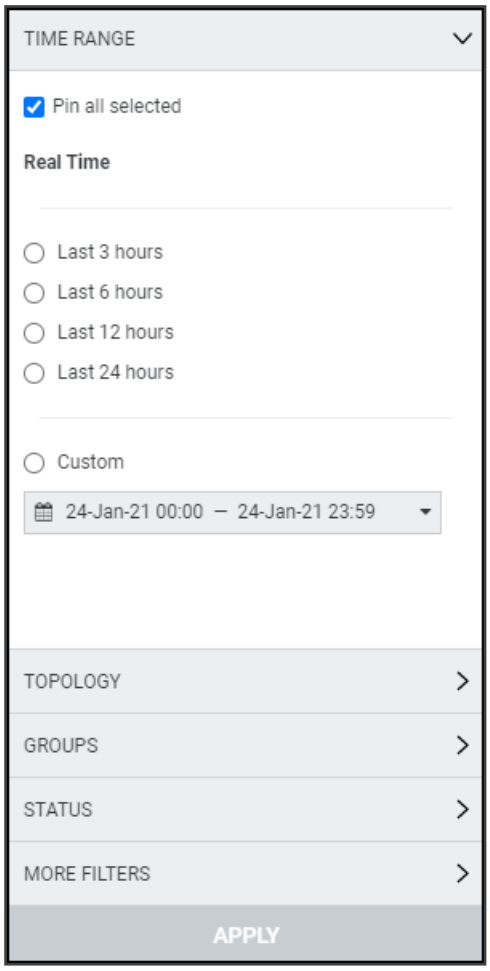


- **Real Time**. Pages by default display real time network information. Pages continuously refresh, presenting up-to-date network information – statistics|calls|history alarms - collected over the last 3 hours (default).
- **Add Filter** > **Time Range**. The page displays network information collected 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.

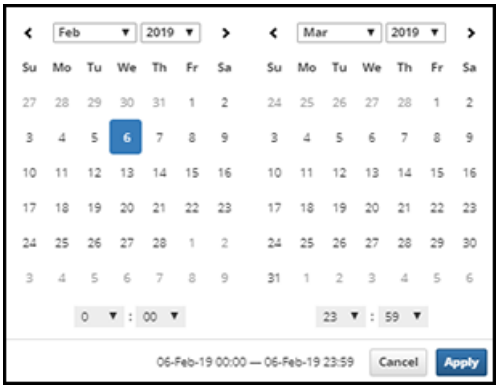
Figure 6-6: Time Range Filter



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 *in every page* whose tab you click. If you clear the option, the filter will only apply *locally* - 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 |	Select one of these 'quick' filters in order to present only network data

Filter Feature	Description
12 | 24 hours	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 **Custom** and then click the drop-down field below it.  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 **Apply**.
Apply	Click to implement the filter. To remove the filter if necessary, click the **Back to real time** 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

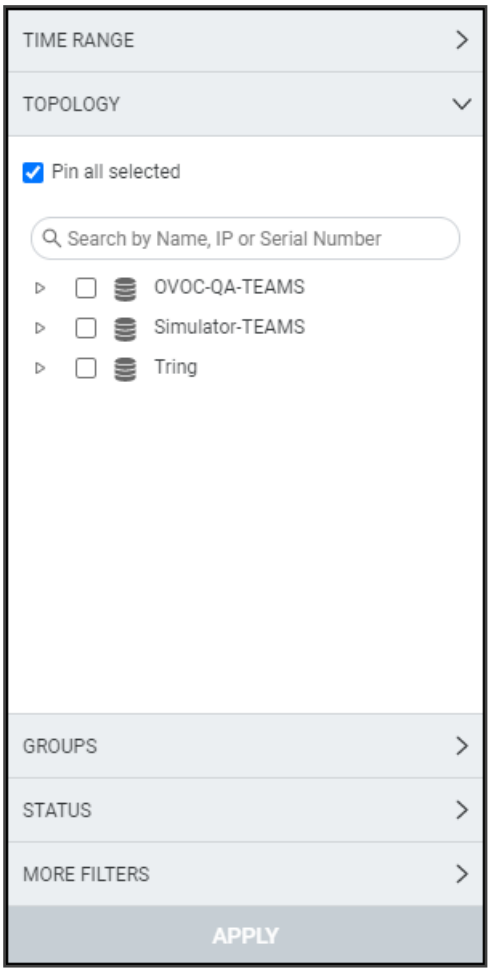
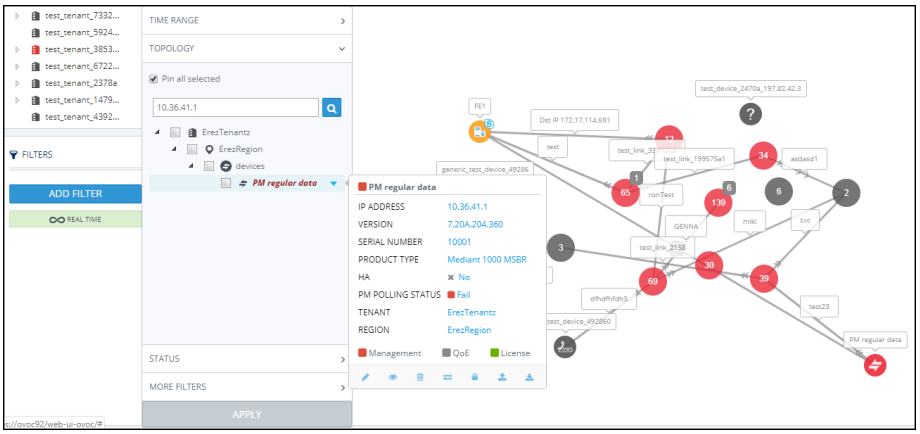


Table 6-3: Topology Filter

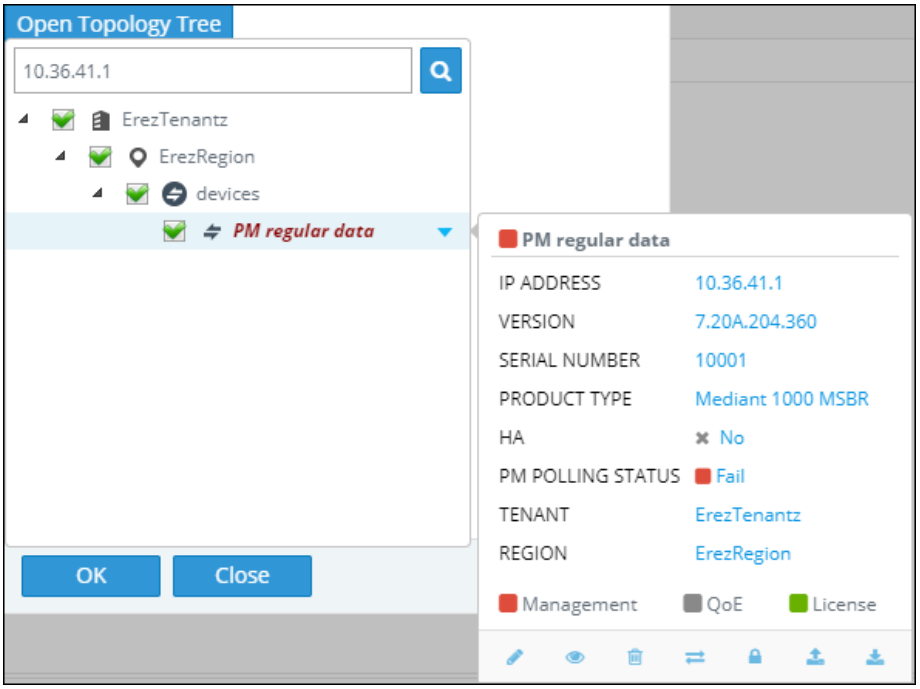
Filter Feature	Description
Pin all selected	Select this option (default) in order to 'preserve' the filter; the filter will remain displayed in every screen whose tab you click. If you clear the option, the filter will only apply to the screen in which you apply the filter. The feature facilitates troubleshooting. After the filter is applied, the OVOC becomes non real time.
Search	■ Enter a search string; all information is filtered out except for the information related specifically to the string you entered. ■ In every page in which there is a Topology filter, you can search according to IP address or serial number.

Filter Feature	Description
	• 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.



■ 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.

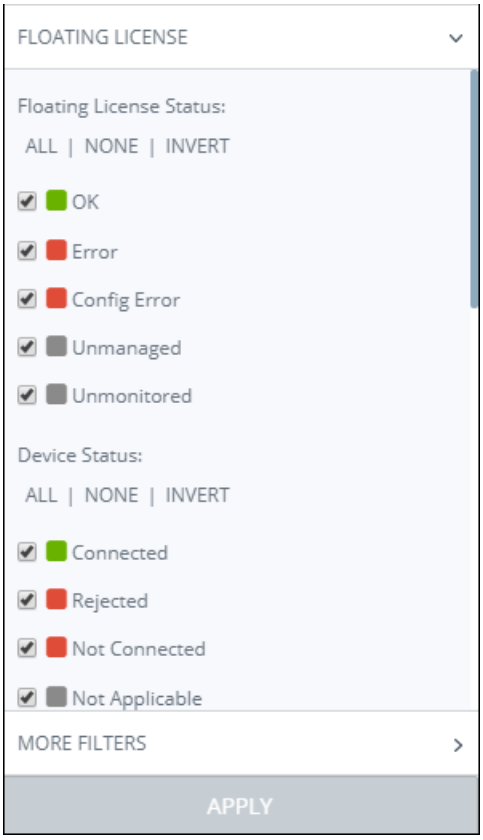
Note that the option to search per IP address and Serial Number is available in all pages / windows in which there is a Topology tree. In the Alarms Forwarding Rules Details screen, for example, the **Open Topology Tree** button opens a window whose search field can be searched per IP address and SN.

Filter Feature	Description
	
'Tenant'	Filters the page according to the tenant. At least one tenant is always defined – see Network Architecture on page 3 for an explanation of multi-tenancy architecture. Allows you to filter further, according to entities defined under the tenant.

Filtering the Device Floating License Page

The 'Floating License' filter enables you to filter the Floating License page (**Network** > **Devices** > **Floating License**). The feature improves network management experience in the page, especially when managing large networks with high numbers of devices and licenses.

Figure 6-8: Filters in the Device Floating License Page



All status filters are selected by default.

The page can be filtered per

- **Floating License Status** (OK | Error | Config Error | Unmanaged | Unmonitored)
- **Device Status** (Connected | Rejected | Not Connected|Not Applicable |Temporary Disconnected | Unmonitored)
- **Report Status** (OK | Over License | Failed | Failed & Over License | Not Registered | Unmonitored)
- **Config Status** (Success | Failure | Not Applicable | Unmonitored)
- **Managed** (Yes | No | Unmonitored)

The feature for example allows network administrators *per status* to

- Click ALL filters and then clear one
- Click NONE and then select one

- Select a few and then click INVERT; only those that weren't selected will then be selected
- Click NONE to clear all
- Click ALL to select all
- Click ALL, deselect a few and then invert the selection; the deselected will then be selected
- Etc.

Use the following table as reference.

Table 6-4: Status Filters

Filter	Description
Floating License Status	
OK (green)	Select to display entities whose Device Status, Config Status and Report Status are ok.
Error (red)	Select to display entities whose Device Status, Config Status and Report Status are errored.
Config Error (red)	Select to display entities whose Device Status, Config Status or Report Status
Unmanaged (grey)	Select to display entities that are unmanaged by OVOC
Unmonitored (grey)	Select to display entities that are unmonitored by OVOC
Device Status	
Connected (green)	Select to display entities that are successfully connected to the Floating License OVOC service.
Rejected (red)	Select to display entities whose Device Floating License has been revoked by the Cloud Floating License service and as a result the device's CAC is reset to 0.
Not Connected (red)	Select to display entities that are unable to establish a connection with the Floating License OVOC service (CAC 0)
Not Applicable (grey)	Select to display entities that were loaded with the Floating License feature disabled on the SBC device.
Temporary Disconnected (red)	Select to display entities that are temporarily disconnected from the Floating License OVOC service due to problems with the HTTPS TCP connection.

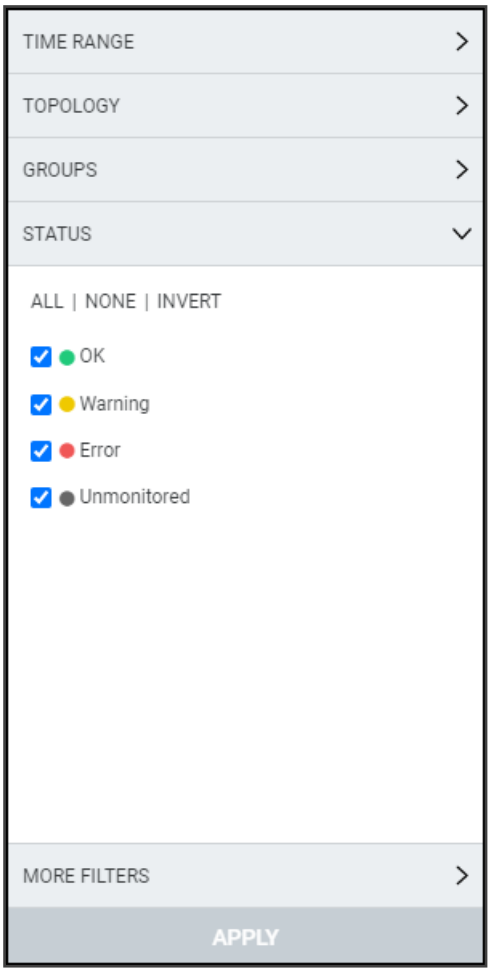
Filter	Description
Unmonitored (grey)	Select to display entities that are currently unmonitored by the OVOC Floating License service.
Report Status	
OK (green)	Select to display entities for whom a report was successfully sent from the device to the OVOC for the last reporting interval.
Over License (yellow)	Select to display entities that have exceeded license limits.
Failed (red)	Select to display entities for whom there was a reporting failure for the last reporting interval.
Failed & Over License (red)	Select to display entities that have exceeded license limits and for whom there was a reporting failure for the last reporting interval.
Not Registered (grey)	Select to display entities that are currently unregistered by the OVOC.
Unmonitored (grey)	Select to display entities that are currently unmonitored by the OVOC.
Config Status	
Success (green)	Select to display entities whose SNMP configuration is successfully updated.
Failure (red)	Select to display entities whose SNMP configuration has not been updated successfully. For example, the Floating License REST operator's user password or username has not been updated correctly.
Not Applicable (grey)	Select to display entities that were added to the OVOC but which are not yet managed.
Unmonitored (grey)	Select to display entities that are currently unmonitored by OVOC.
Managed	
Yes (green)	Select to display entities managed by the Floating License service server.
No (red)	Select to display entities that are not managed by the Floating License service server.

Filter	Description
Unmonitored (grey)	Select to display entities that are currently unmonitored by the OVOC.

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 6-9: Alarm 'Status' Filter



Use the following table as reference.

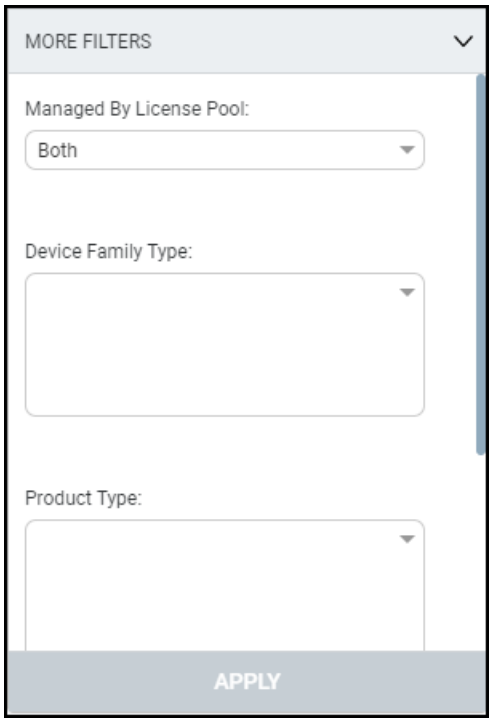
Table 6-5: Status Filter

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 6-10: More Filters



Use the following table as reference.

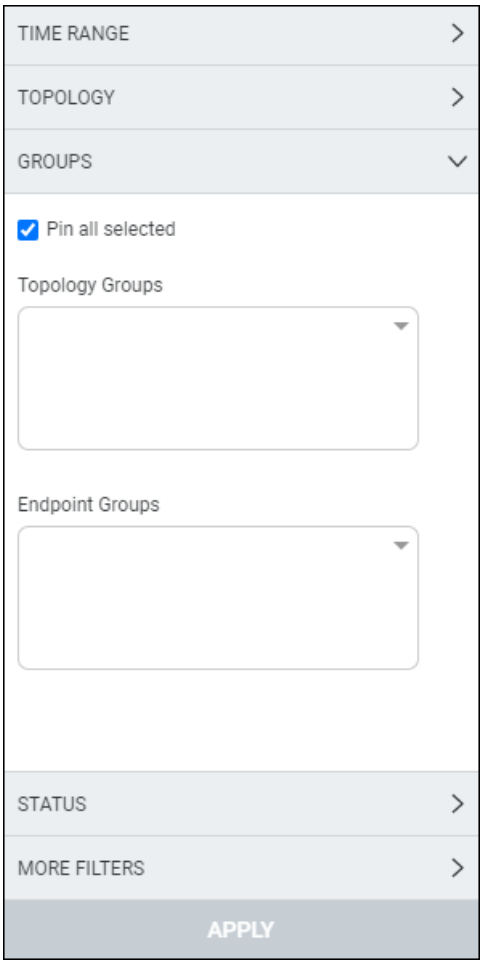
Table 6-6: More Filters - Network Topology Page

Filter	Description
Managed by license pool	From the drop-down list, select either **Both**, **Managed** or **Not managed**.
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 **IPGroup**, **Trunk Group**, **Phone Prefix**, **Control IP**, **Media IP**, **Media Realm** or **Remote Media Subnet** to display on the page.

Filtering by Groups

The OVOC's Endpoints Groups page (**Network** > **Endpoints** > **Groups**) allows the operator to filter OVOC pages according to Endpoints Groups.

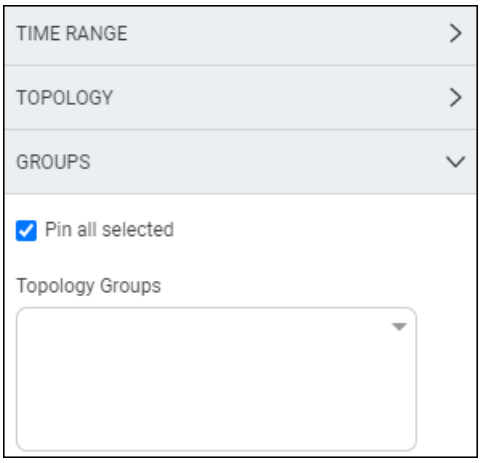
Figure 6-11: Add Filter > Groups > Endpoint Groups



- From the drop-down in the Endpoint Groups pane, select an Endpoint Group according to which to filter. See also Adding an Endpoints Group on page 168 for more information about the page.

The OVOC's Topology Groups page (**Network** > **Groups**) allows the operator to filter OVOC pages according to Topology Groups.

Figure 6-12: Add Filter > Groups > Topology Groups



- From the drop-down in the Topology Groups pane, select a Topology Group according to which to filter. See also Adding a Topology Group on page 172 for more information about adding a Topology Group.

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 95.

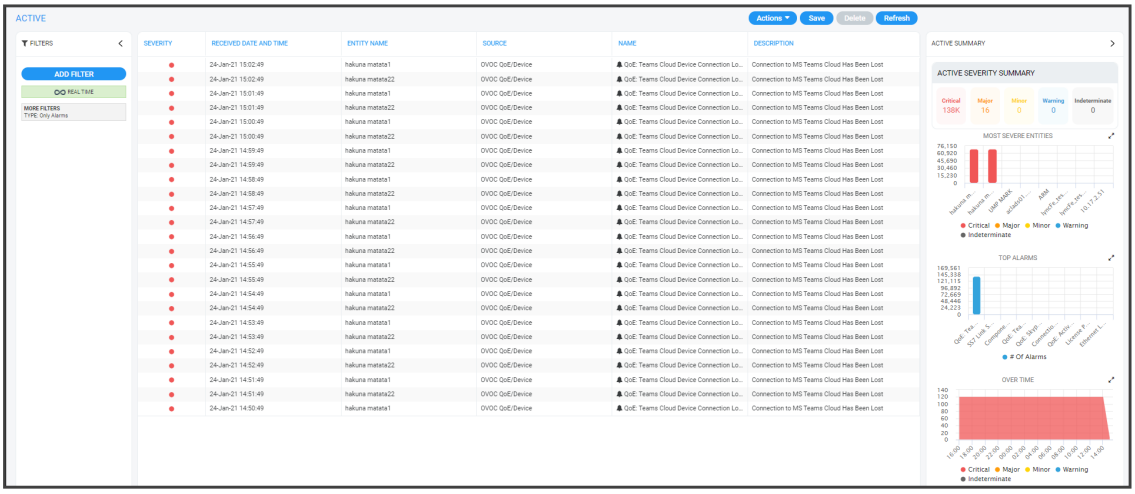
Monitoring Active Alarms to Determine Network Health

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 6-13: Active Alarms Summary



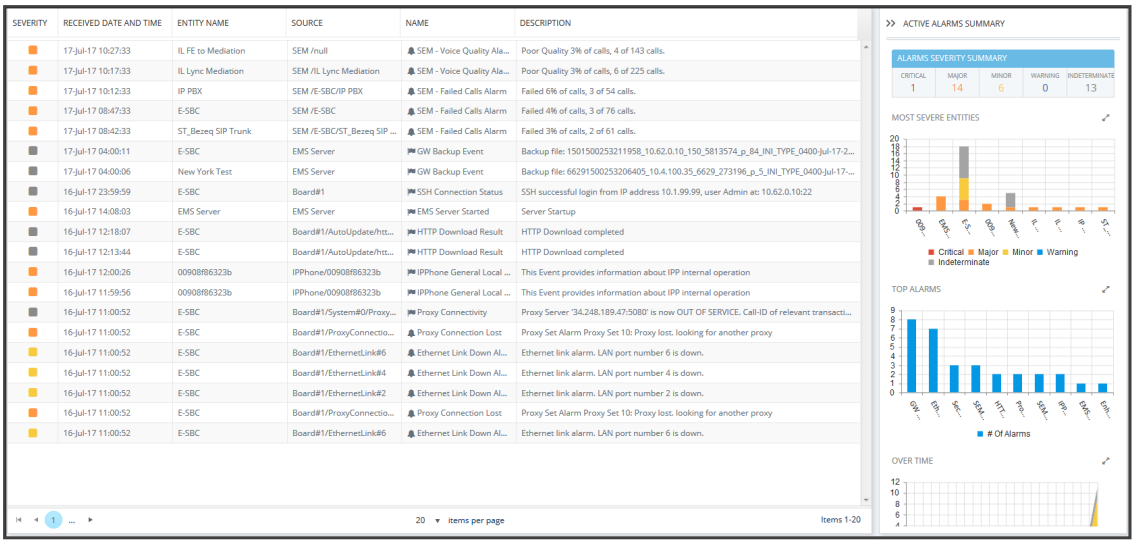
Performing Management Actions on Active Alarms

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:

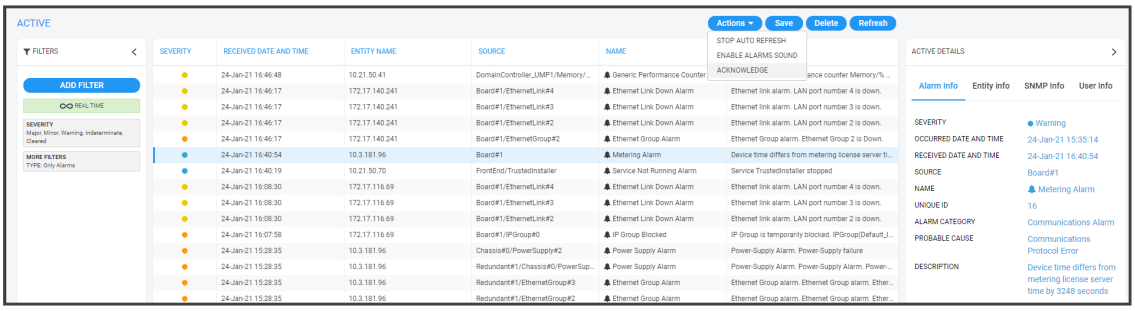
1. Open the Active Alarms page (**Alarms** > **Active**).

Figure 6-14: Alarms - Active



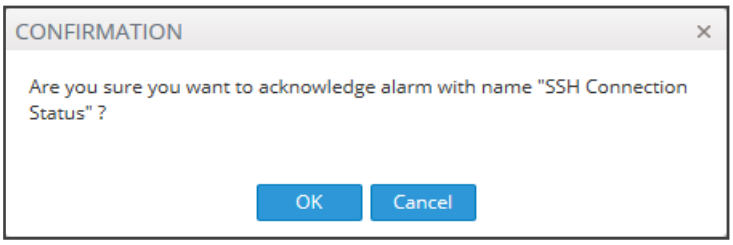
2. Optionally filter the page by Topology (see Filtering by 'Topology' on page 215), Severity (see Filtering by 'Status' on page 222), Source Type (see Filtering by 'Severity' on page 230), or More Filters (see Filtering by 'More Filters' on page 234), and then select an alarm or multiple alarms and click **Actions**.

Figure 6-15: Alarms - Actions



3. Select **Acknowledge** to acknowledge an alarm.

Figure 6-16: Acknowledge Alarm Confirmation

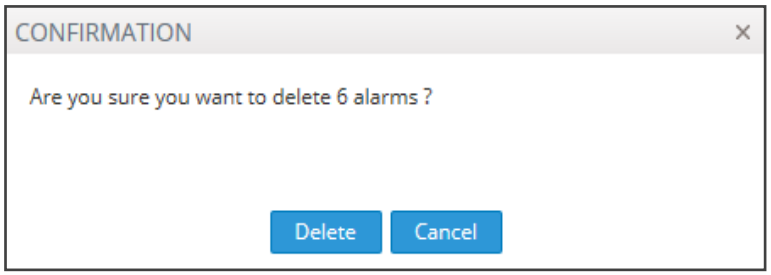


4. Select the **Save** button to save alarms to file for future reference.

➢ 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 6-17: 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**.

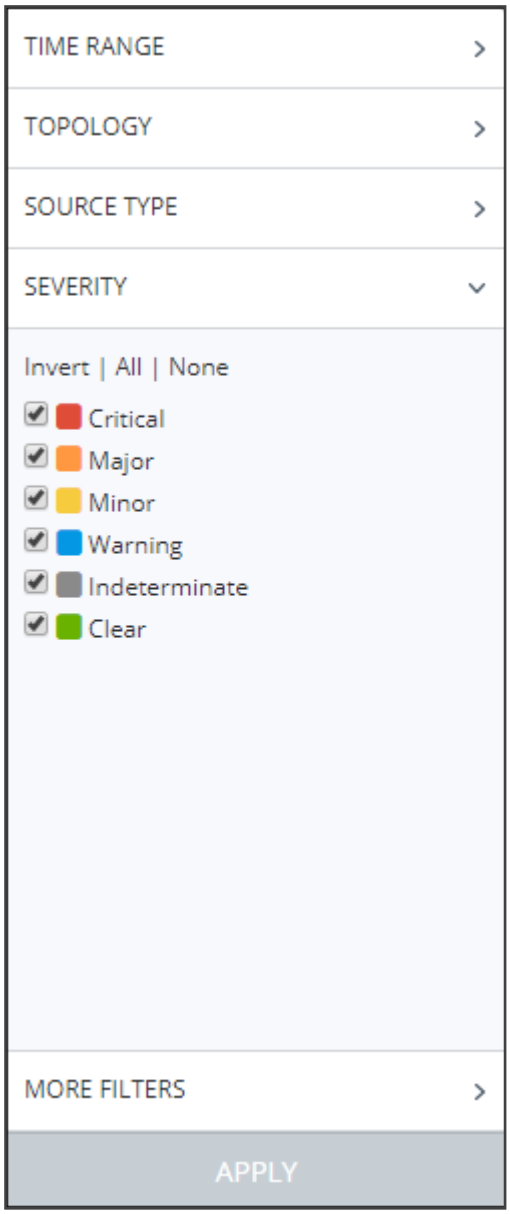
➢ To stop automatic refresh:

- 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 6-18: Alarm 'Severity' Filter



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.

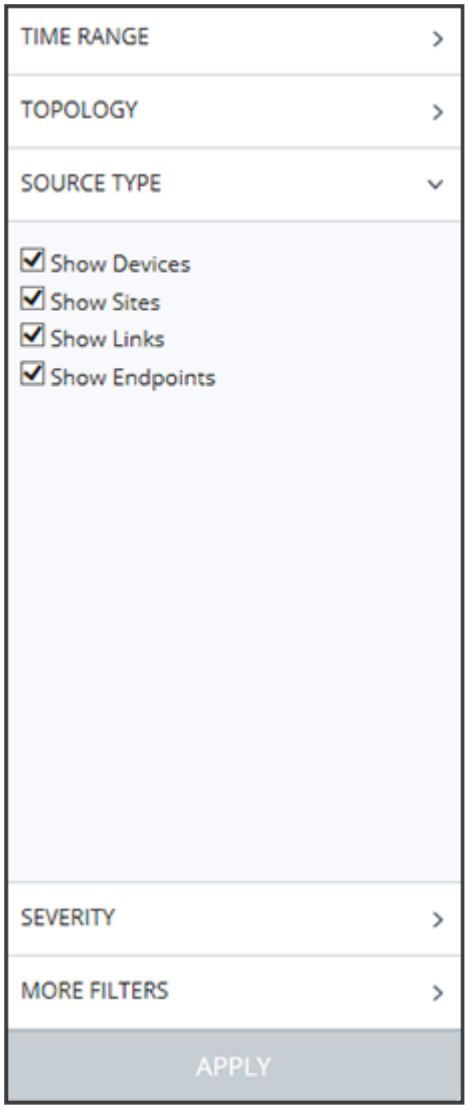
Table 6-7: Severity Filter

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 6-19: 'Source Type' Filter



Use the following table as reference.

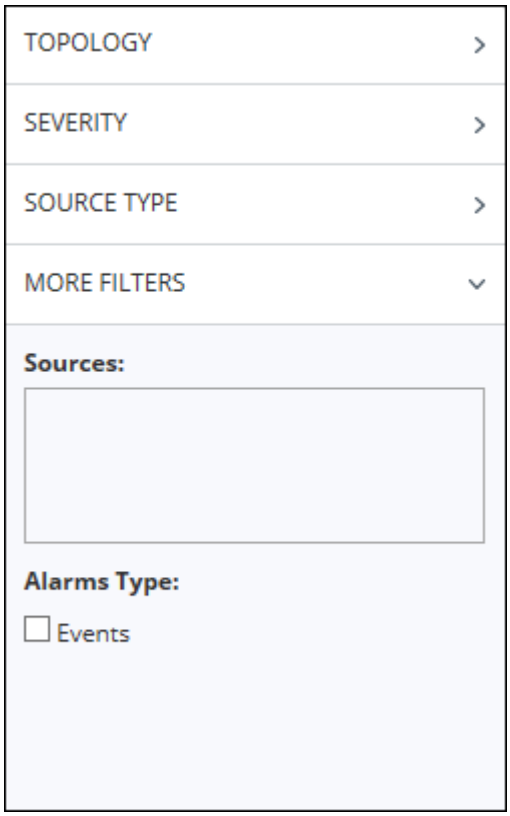
Table 6-8: 'Source Type' Filter

Filter	Description
Show Devices	Displays only calls whose report was sent to the OVOC *from devices*.
Show Sites	Displays only calls whose SIP Publish report was sent by endpoints to the OVOC *from sites*.

Filter	Description
Show Links	Displays only calls transmitted *through links*.
Show Endpoints	Displays only calls whose SIP Publish report was sent to the OVOC *from endpoints*.

Filtering by 'More Filters'

Figure 6-20: More Filters – Alarms Active Page



Use the following table as reference.

Table 6-9: 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.

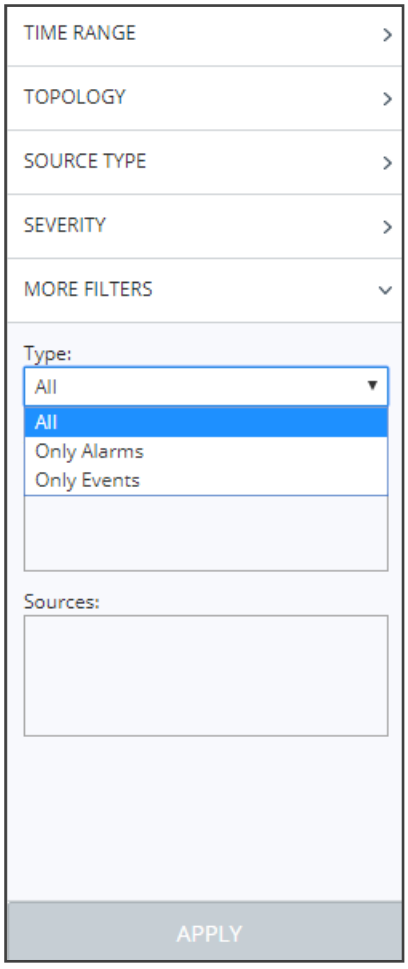
Filtering by 'Type'

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':

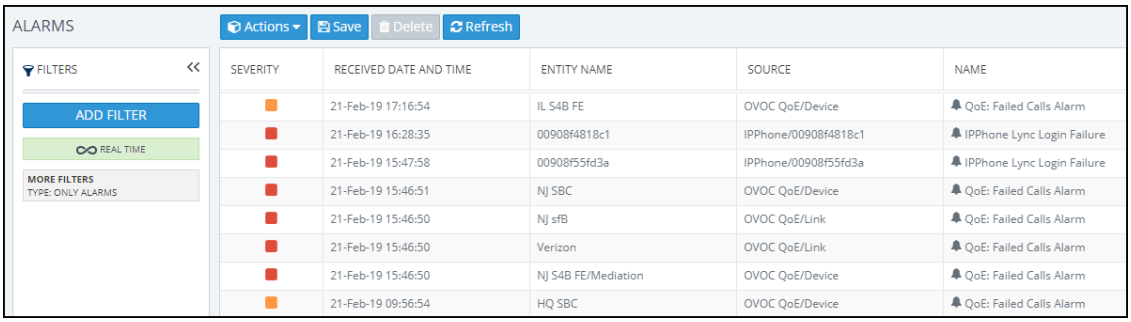
1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' drop-down, select **All**, **Only Alarms** or **Only Events**.

Figure 6-21: 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 6-22: Type - Only Alarms - Bells in 'Name' Column

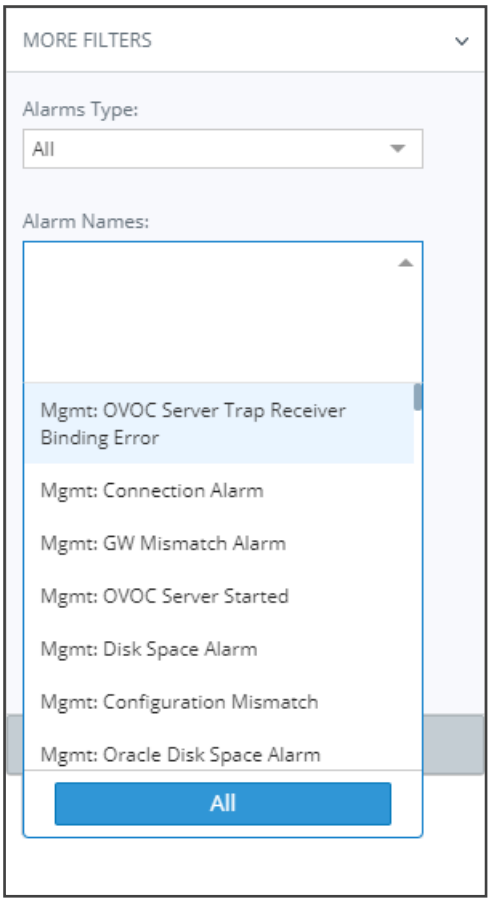


Filtering by 'Alarm Names'

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.

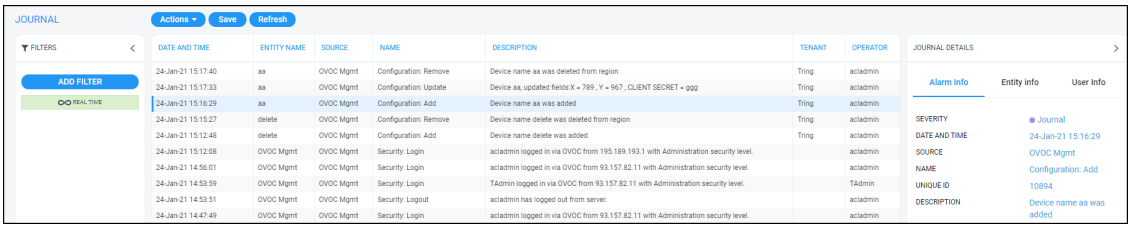


- In the Alarms Forwarding Rule screen (**Alarms** > **Forwarding** > **Add**), click the tab **Rule Conditions** and then from the 'Alarm Names' drop-down, select the alarm.

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 240).

Figure 6-23: Journal Alarms

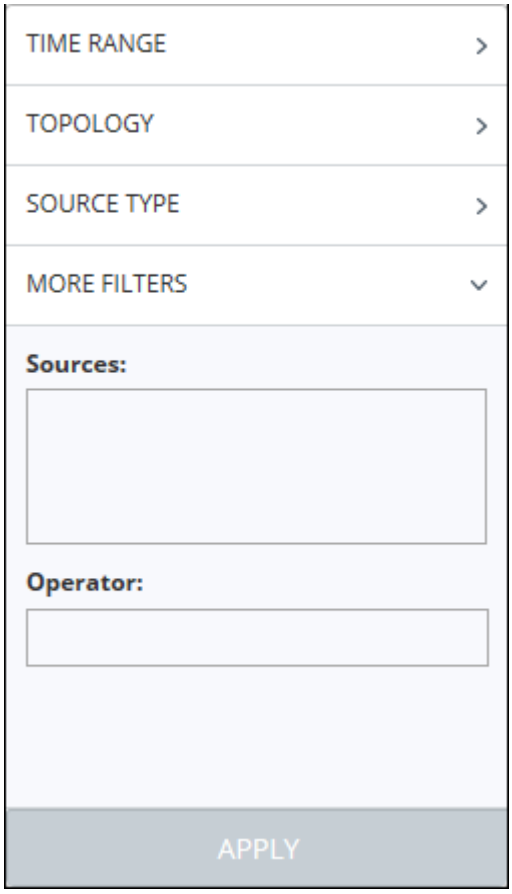


The Journal Alarms page reflects *all actions* performed by network administrators in AudioCodes' *Device Manager*. Records of network administrator actions are sent from the Device Manager to the OVOC server to be displayed in the OVOC Journal Alarms page. See also AudioCodes' *Device Manager Administrator's Manual*.

Filtering the Alarms Journal by 'More Filters'

You can filter the Alarms Journal page by 'More Filters'.

Figure 6-24: More Filters – Alarms Journal Page



Use the following table as reference.

Table 6-10: 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.

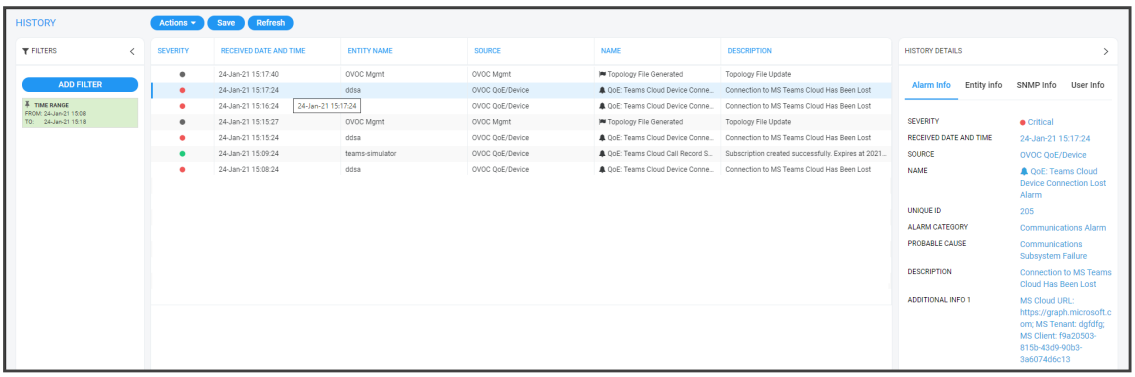
Viewing History Alarms

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:

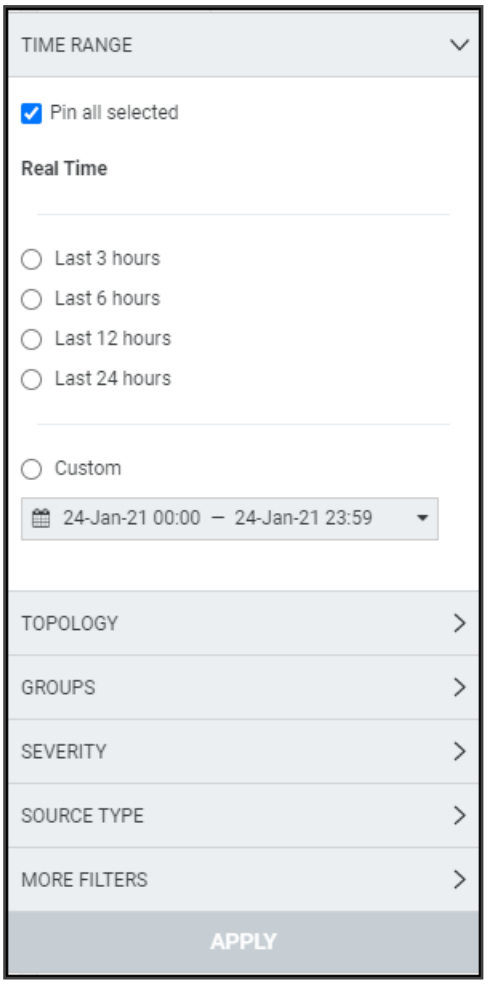
1. Open the History page (**Alarms** > **History**).

Figure 6-25: 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 212.

Figure 6-26: Alarms Page Filters



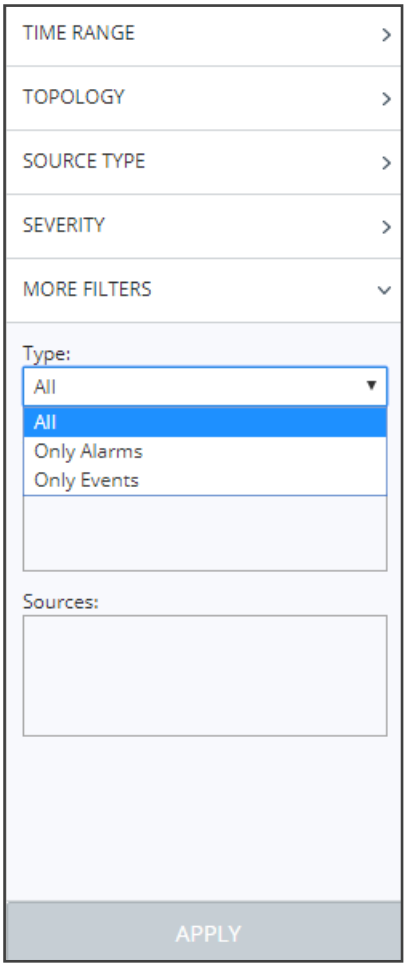
Filtering by 'Type'

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':

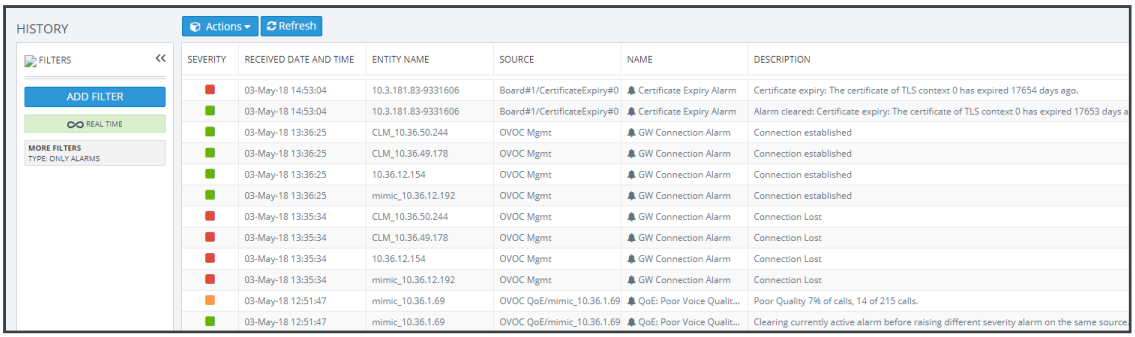
1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' drop-down, select **All**, **Only Alarms** or **Only Events**.

Figure 6-27: 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 6-28: History Alarms - Type Filter



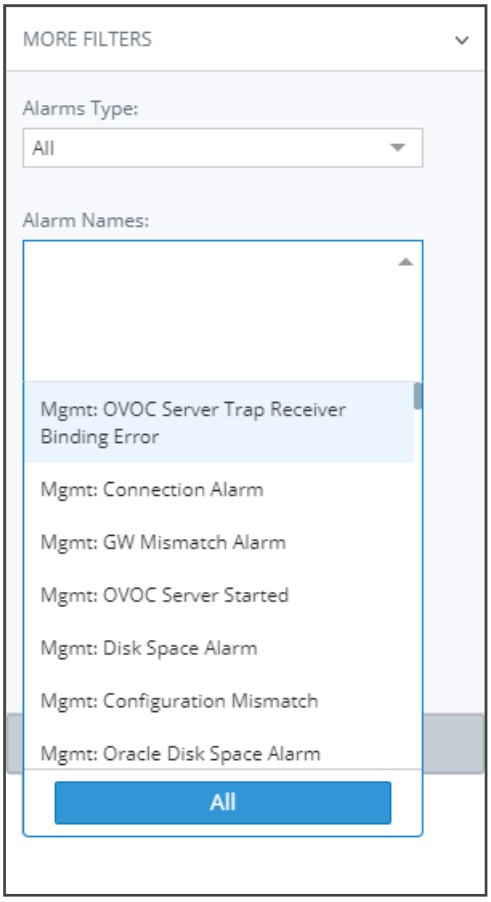
Filtering by 'Alarm Names'

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 6-29: '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:

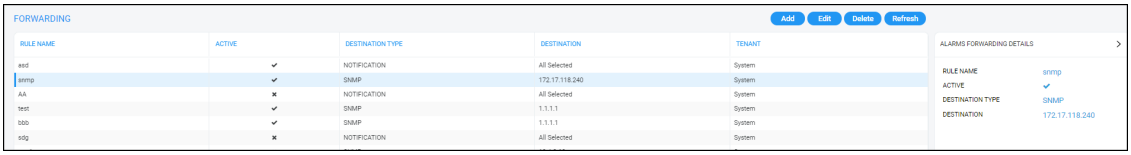
- SNMP Notifications (SNMP 1 / SNMP 2) - see Forwarding Alarms whose Destination Type is 'SNMP' on page 252
- External Mail / Internal Mail - see Forwarding Alarms whose Destination Type is 'Mail' on page 255

- Syslog - see Forwarding Alarms whose Destination Type is 'Syslog' on page 257
- Notification - see Forwarding Alarms whose Destination Type is 'Notification' on page 261

➢ To configure alarm forwarding:

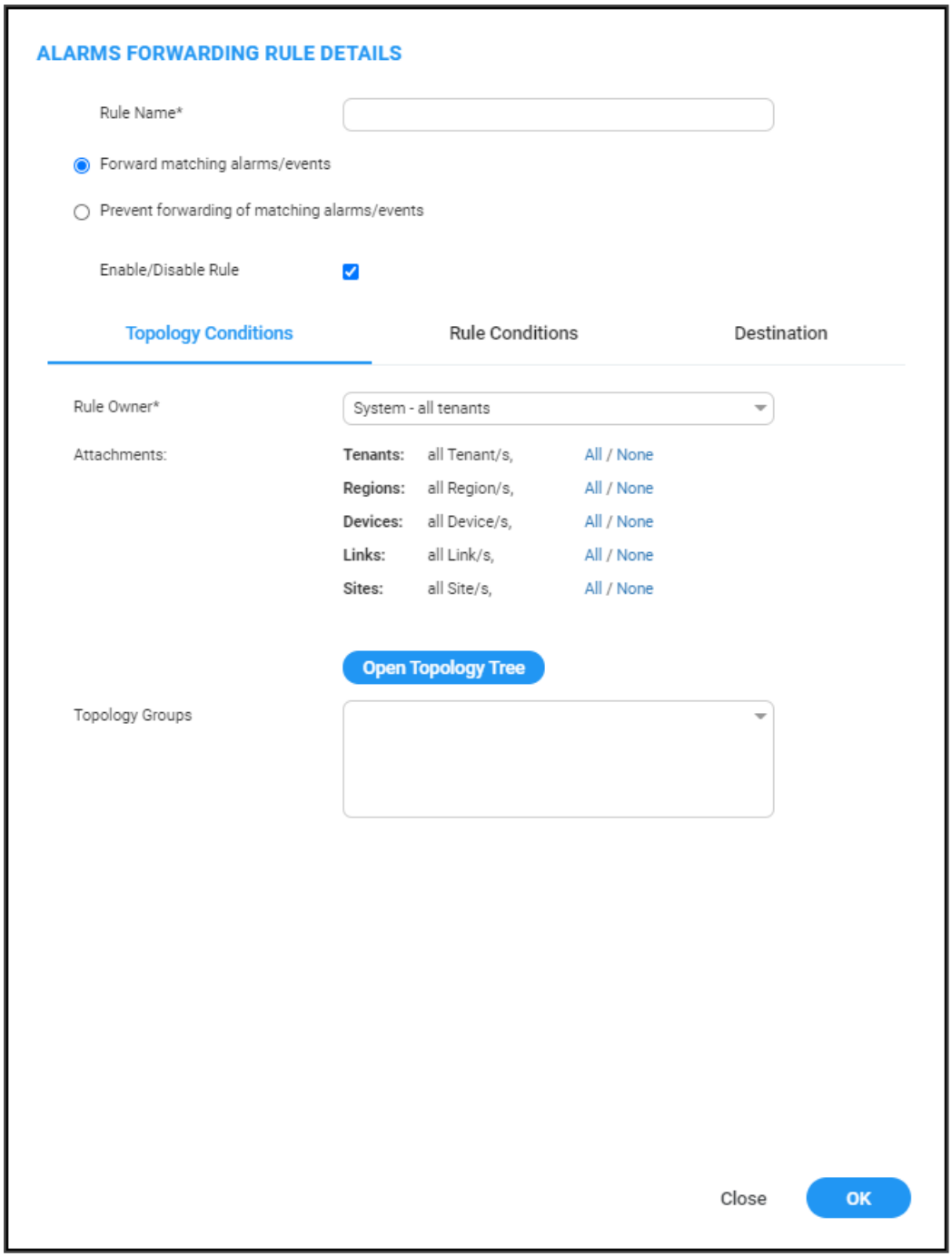
1. Open the Alarms Forwarding page (**Alarms** > **Forwarding**).

Figure 6-30: Alarms Forwarding Page



2. Click **Add**.

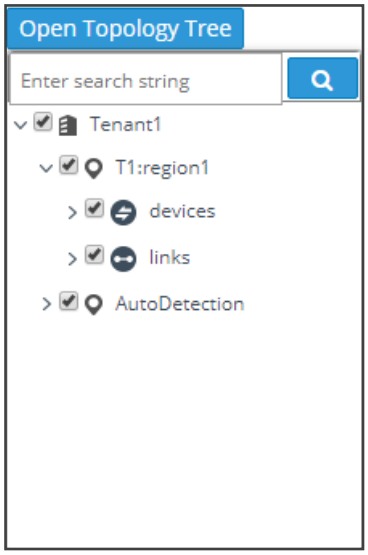
Figure 6-31: Alarms Forwarding Rule Details – Topology Conditions



3. Configure the Topology Conditions using the following table as reference:

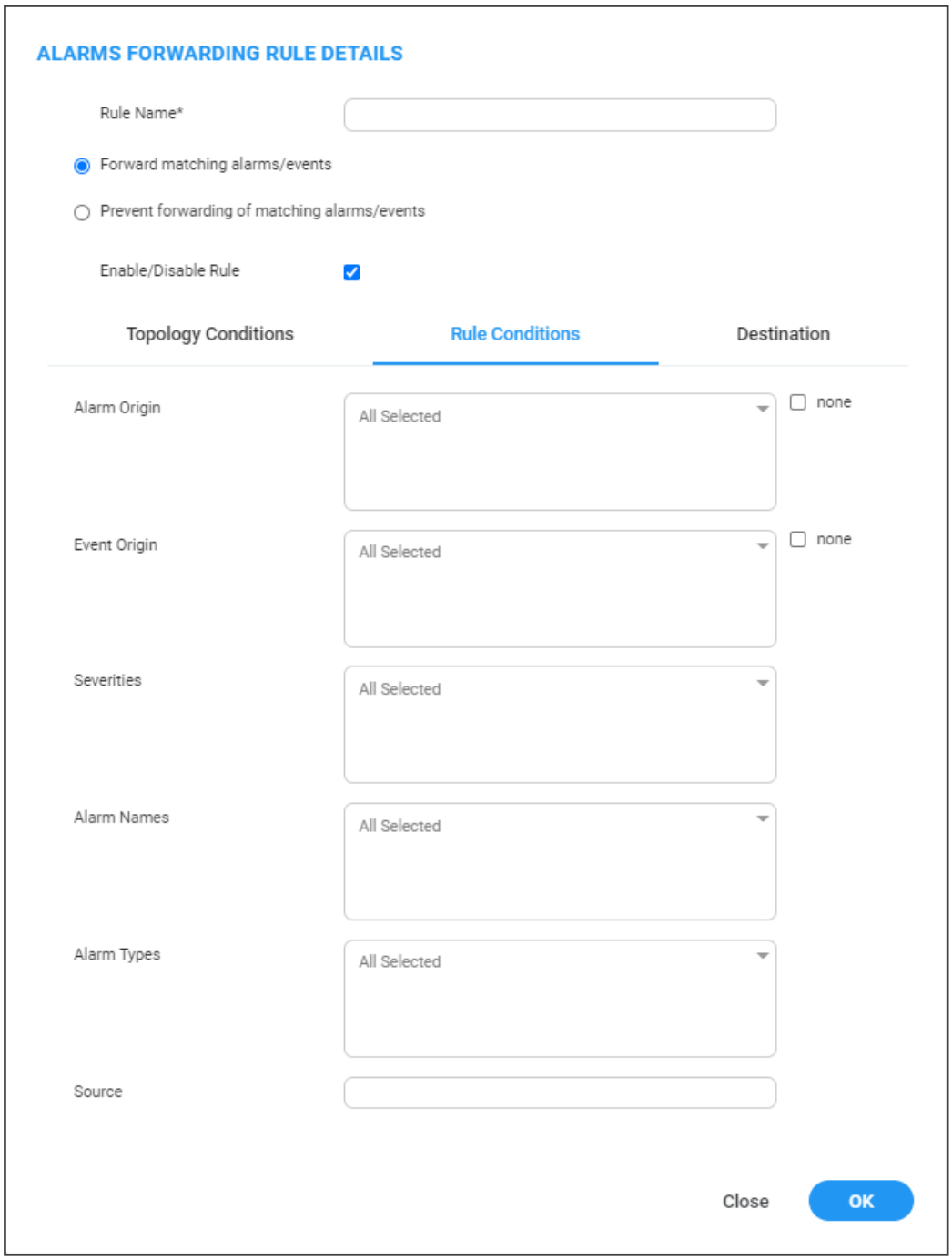
Table 6-11: Alarms Forwarding – Topology Conditions

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	Allows or prevents forwarding alarms depending on the destination you select. If you select **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' drop-down under the **Rule Conditions** tab, then minor alarms are not forwarded. See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 227
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met. See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 227
Rule Owner	From the drop-down, select **System – all tenants**; the rule will then apply to *all tenants* and to all regions/links/devices/sites under all tenants. Here's what you'll then view next to 'Attachments': **all Tenant/s, all Region/s, all Device/s, all Link/s, all Site/s** If you select *a specific tenant* from the drop-down, the rule will apply by default to *all* entities *under that specified tenant*. Click **Open Topology Tree** and then click **>** to view the entities under that tenant and if you want, to change the default.

Parameter	Description
	 Only the operator assigned to that tenant can view and change it. The **All**/**None** filters next to 'Attachments' allow you to quickly specify to which entities rule forwarding will apply, if not to all.

4. Click the **Rule Conditions** tab.

Figure 6-32: Alarms – Forwarding – Rule Details



5. Configure the screen using the following table as reference.

Table 6-12: Forwarding Alarms – Rule Details - 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	Allows or prevents forwarding alarms depending on the destination you select. If you select **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' drop-down under the **Rule Conditions** tab, then minor alarms are not forwarded. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 227
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 227
Alarm Origin	Select the origin from which alarms will be forwarded: ■ Management ■ QoE ■ Devices ■ Endpoints ■ ARM ■ VIP Endpoints Users
Event Origin	Select the origin from which events will be forwarded: ■ Management ■ QoE ■ Devices ■ Endpoints ■ ARM ■ VIP Endpoints Users

Parameter	Description
Severities	From the 'Severities' drop-down, select the severity level of the alarms you want to receive: ■ Warning ■ Minor ■ Major ■ Critical ■ Indeterminate Default: All Selected.
Alarm Names	Allows forwarding alarms according to specific alarm names. For example, if you select **Power Supply Failure** then only this alarm will be forwarded. Default: **All Selected**. The search field lets you find an alarm according to name or origin.
Alarm Types	Allows forwarding alarms according to specific alarm types. For example, if you select **communicationsAlarm** then only this alarm type will be forwarded. Default: **All Selected**. 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 6-33: Alarms – Forwarding – Destination Type - SNMP v2

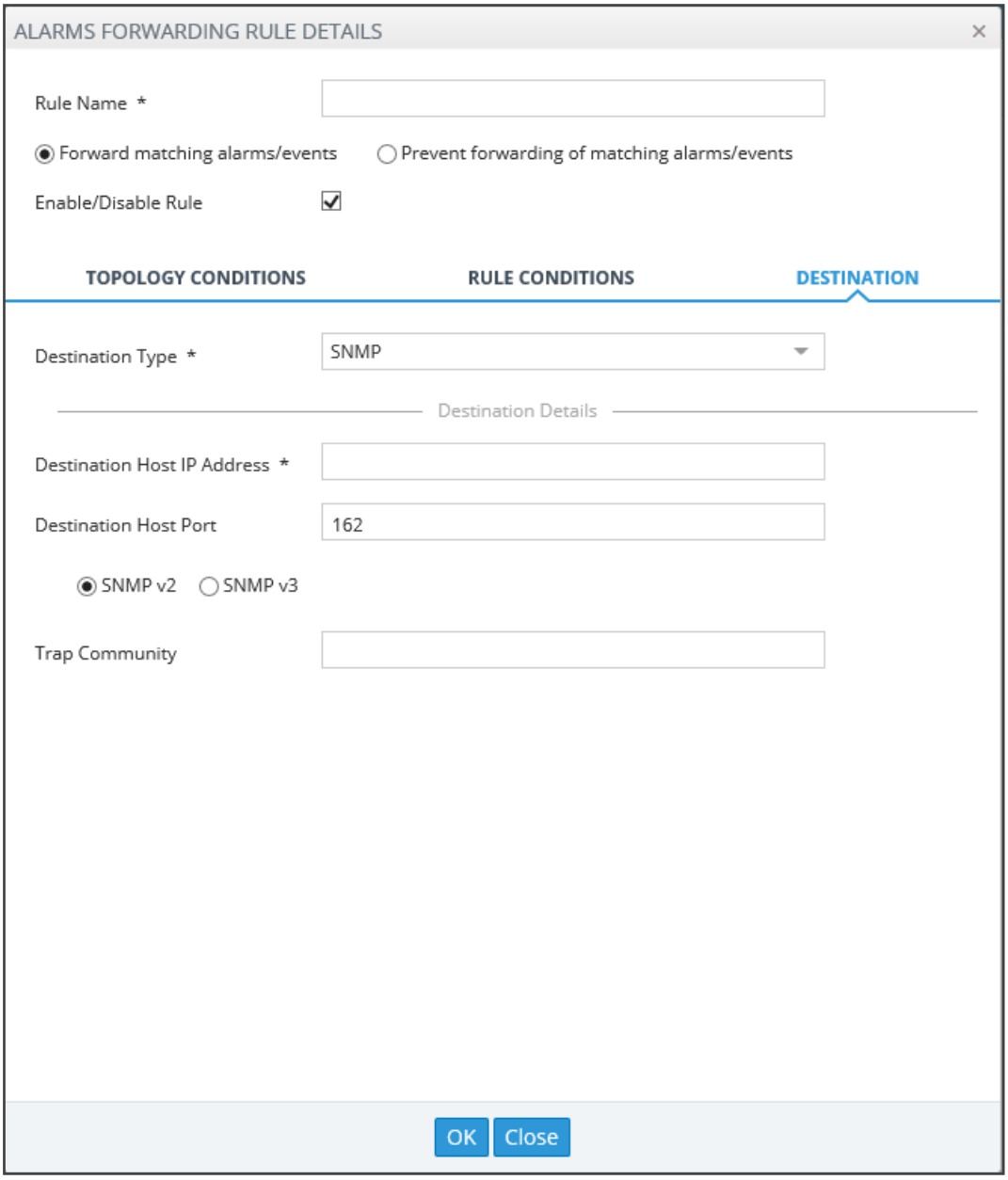
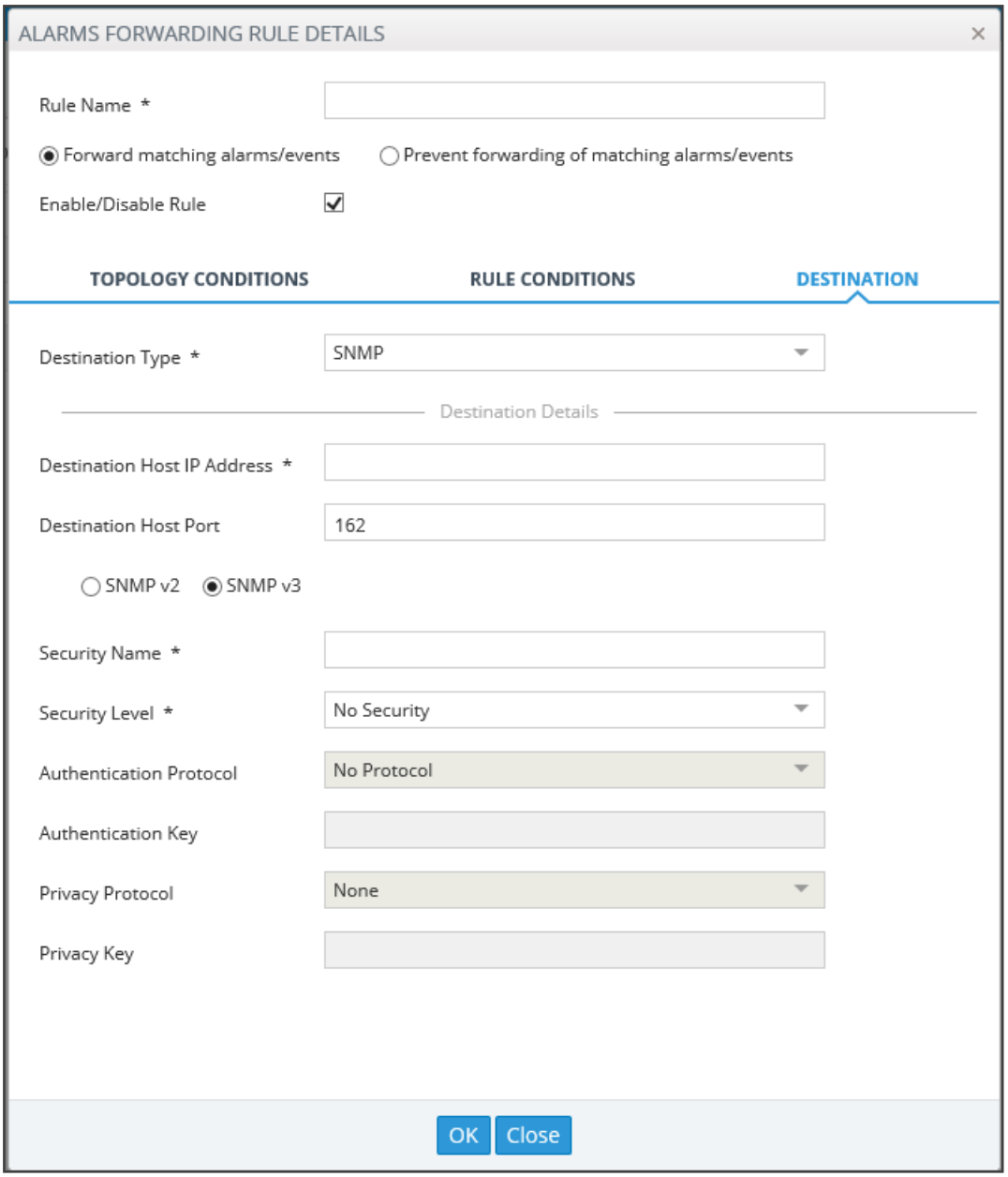


Figure 6-34: Alarms – Forwarding – Destination Type - SNMP v3



Use the following table as reference for the 'Destination Type' parameter.

Table 6-13: Forwarding Alarms – Destination

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or-	Allows or prevents forwarding alarms depending on the destination you select. If you select **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' drop-down under the **Rule Conditions** tab, then minor alarms are not forwarded.

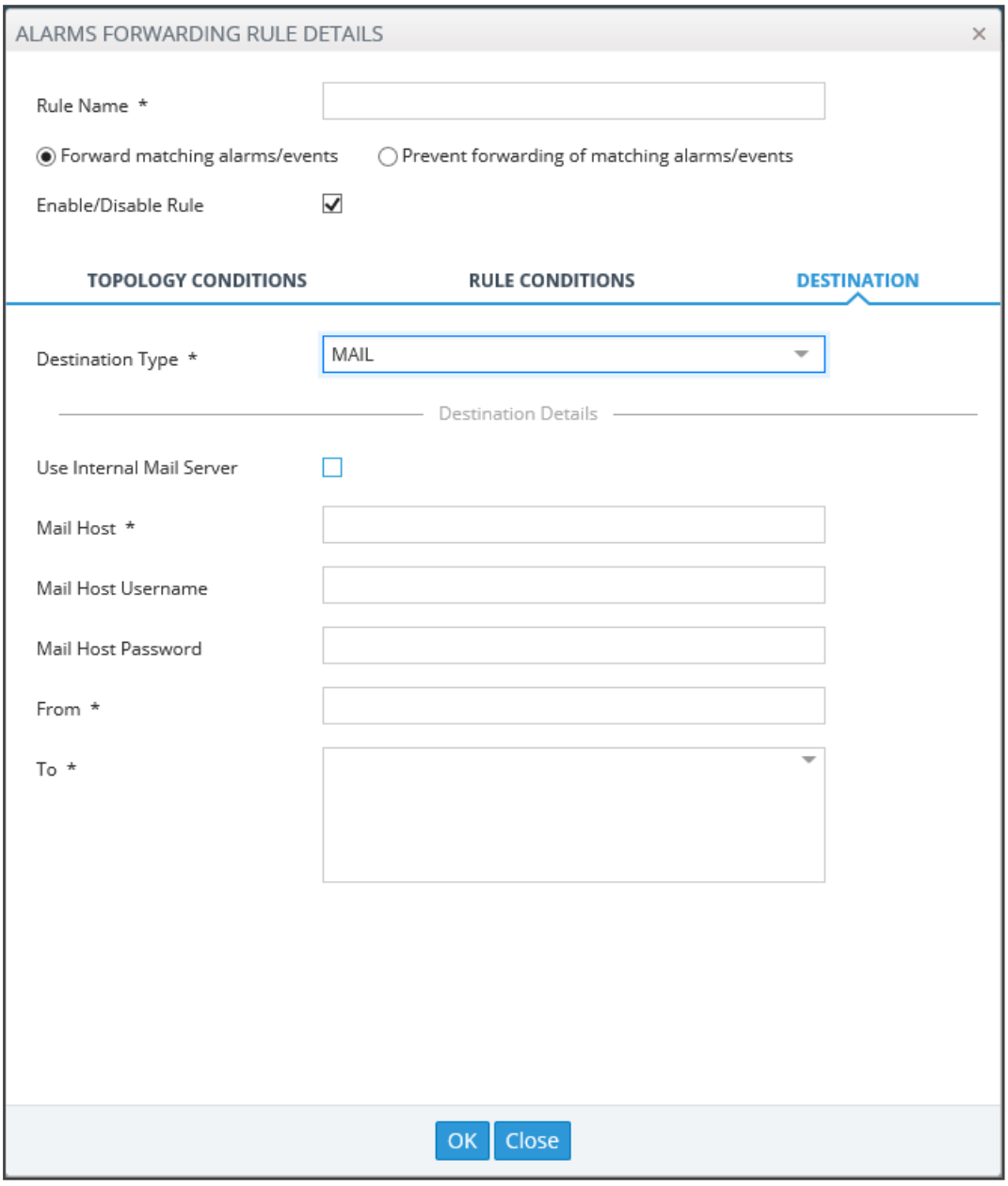
Parameter	Description
Prevent forwarding matching alarms/events	See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Destination Type	Determines the format in which the alarm or event will be forwarded. From the drop-down, select ■ SNMP (default) ✔ SNMP v2 ✔ SNMP v3 ■ MAIL ■ SYSLOG

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 6-35: Alarms Forwarding Rule Details – Destination – Mail



2. Select the **Use Internal Mail Server** option.

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

Table 6-14: Forwarding Alarms - Destination – Mail

Parameter	Description
Use Internal Mail Server	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. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Mail Host	Enter the **Mail Host IP address or FQDN (e.g.**, smtp.office365.com).
Mail Host Username	Enter the **mail host username**.
Mail Host Password	Enter the **mail host password**.
From	Enter the **e-mail address** the recipient will see when the mail arrives. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
To	Enter the **list of email addresses** (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. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95

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: Includes all fields that appear in the Alarm Item

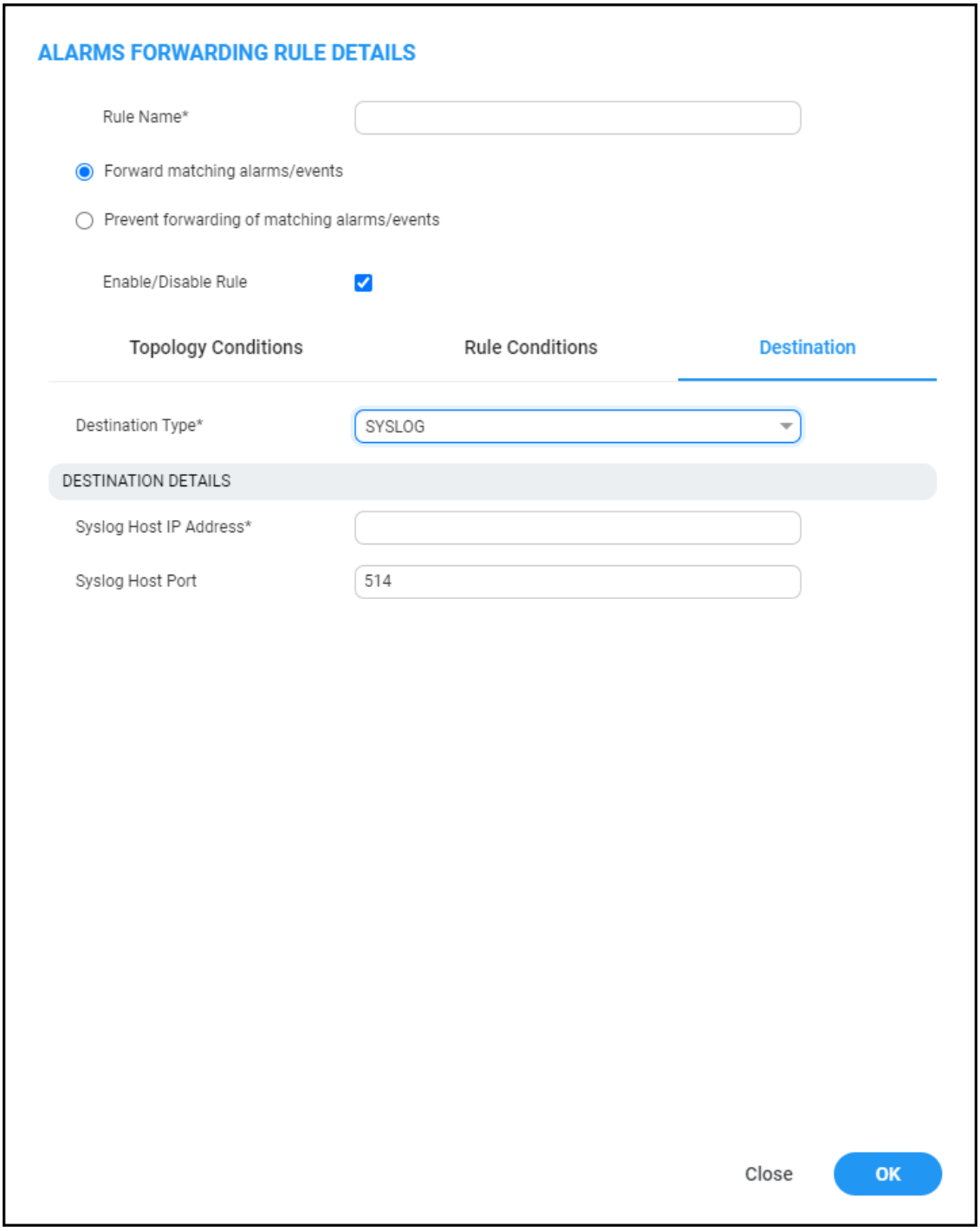
Forwarding Alarms whose Destination Type is 'Syslog'

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 6-36: Destination Type 'Syslog'



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

Table 6-15: 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 **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' drop-down under the **Rule Conditions** tab, then minor alarms are not forwarded. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
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.

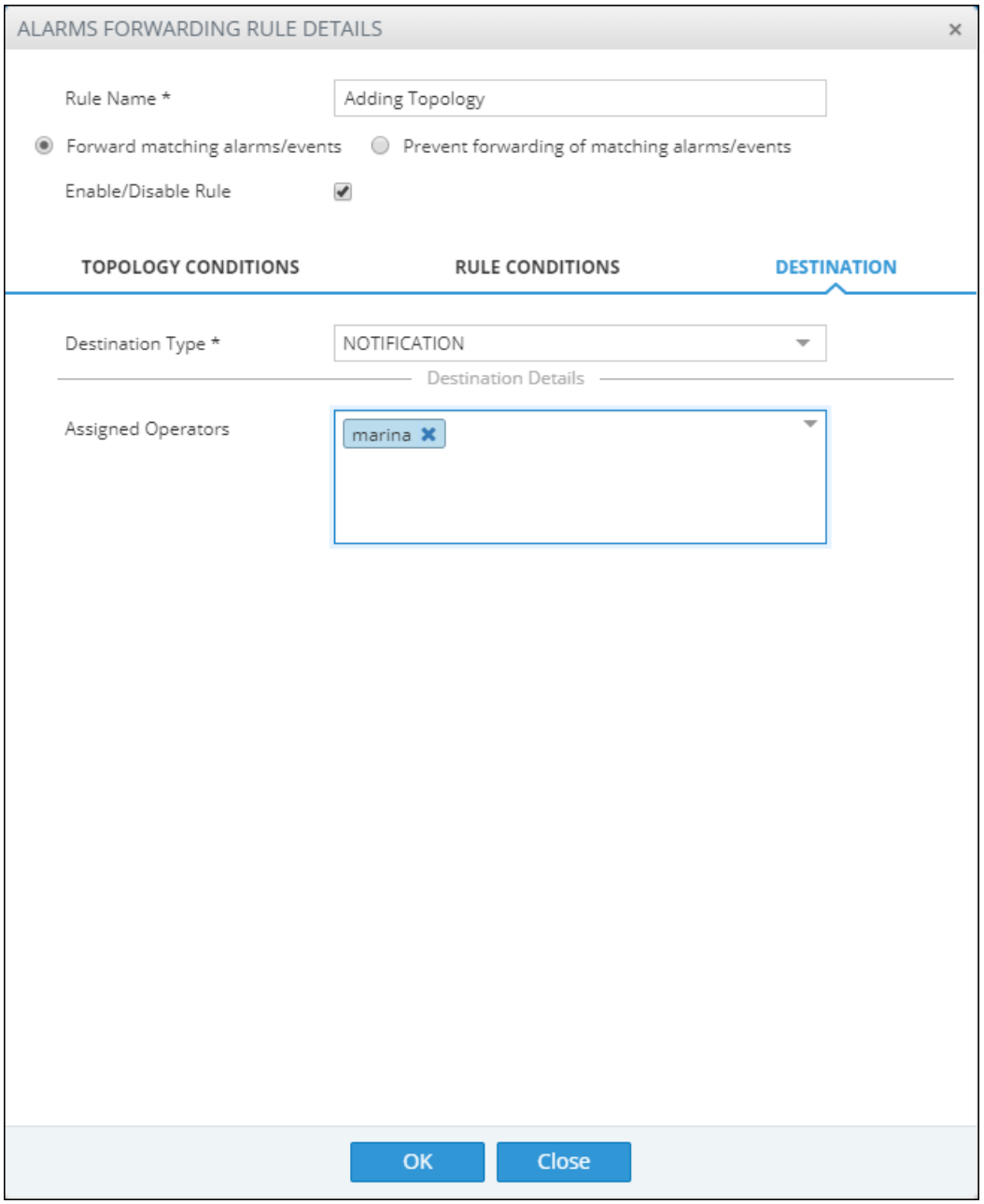
Forwarding Alarms whose Destination Type is 'Notification'

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 6-37: Destination Type 'Notification'



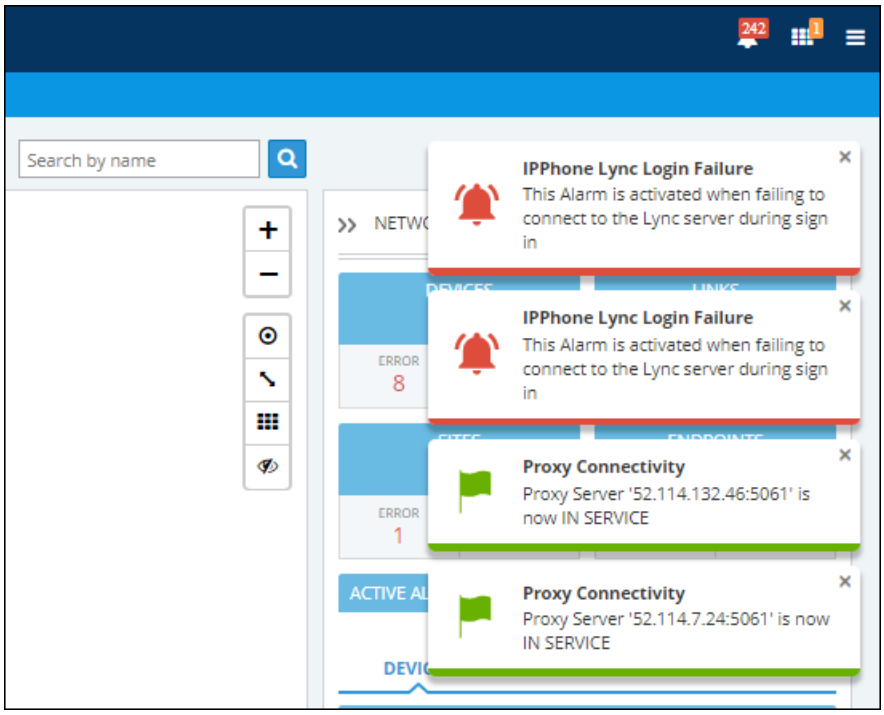
2. Configure the parameters using the table as reference.

Table 6-16: 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 **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' drop-down under the **Rule Conditions** tab, then minor alarms are not forwarded. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 95
Assigned Operators	Under 'Destination Details', configure the operator (or operators) to whom you want the alarm notifications to be forwarded. **Note:** ■ Operators whose security level is 'Admin' can assign notifications to any operator / all operators. ■ Operators whose security level is 'Operator' can assign notifications only to themselves.

3. Click **OK**; notifications will automatically pop up in the uppermost right corner in the GUIs of all assigned operators, when alarms are received.

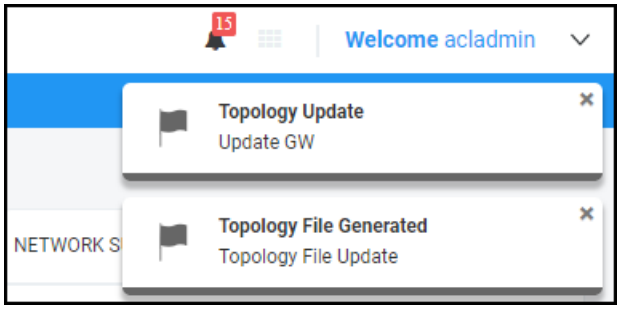
Figure 6-38: Notifications Pop-up



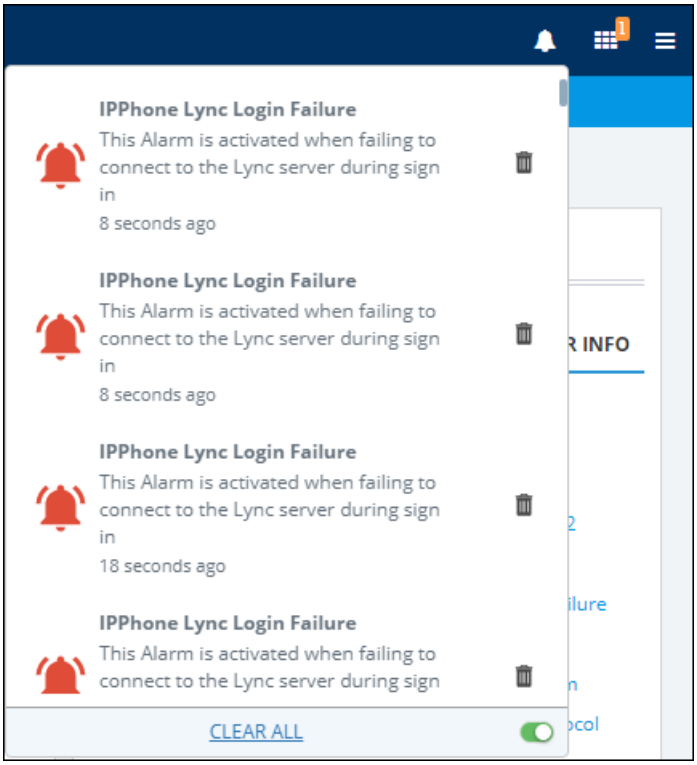
To configure the *timeout* of notification pop-ups, see Configuring Operator Authentication Locally, in the OVOC on page 50 and refer to the parameter 'Notifications display time (sec)'. The default is 3 seconds. Configuring the parameter to 0 disables the feature.

➢ **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.

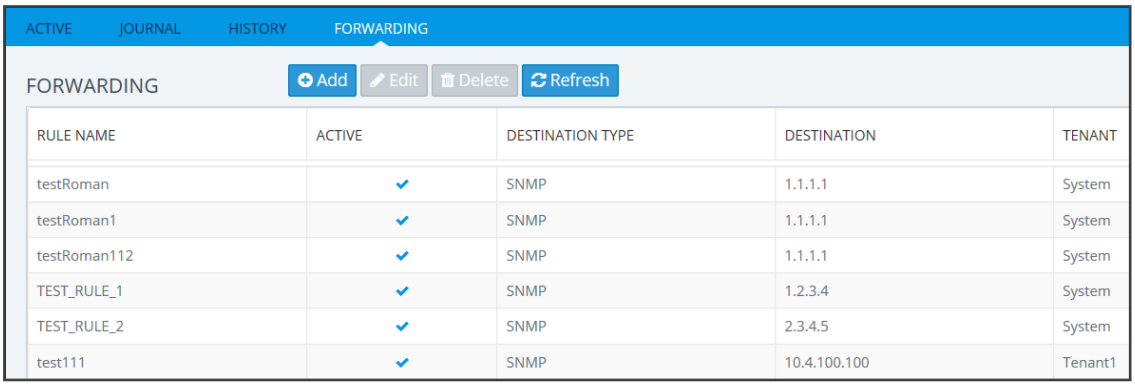


3. In the list, you can delete a notification, clear all notifications or click a notification to open the Alarms History page displaying that alarm.
4. Scroll down to view earlier notifications. Most recent notifications are listed first. Every notification indicates how long ago it was listed, e.g., **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 6-39: New Rules in the Alarms Forwarding Page



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 6-40: Devices Statistics



You can optionally filter the page by Time Range (see Filtering to Access Specific Information on page 212) and Topology (see Filtering by 'Topology' on page 215).

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 269)

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 212 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 6-41: Calls Quality Bar Chart



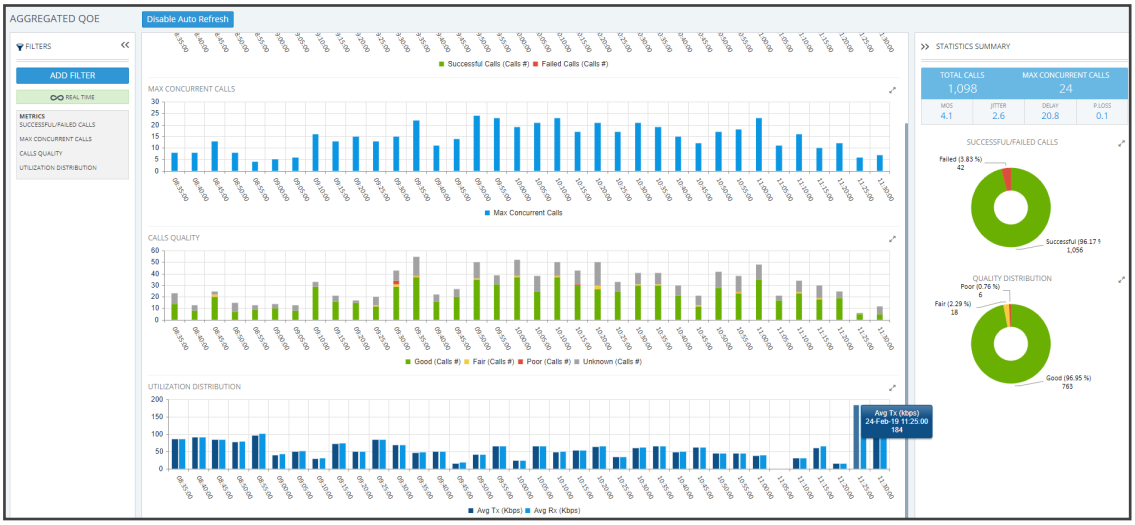
Compare charts. If, for example, you identify a correlation over time between 'Poor' voice quality and Jitter, then Jitter is the reason for the poor voice quality.

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 6-42: Utilization Distribution Bar Chart



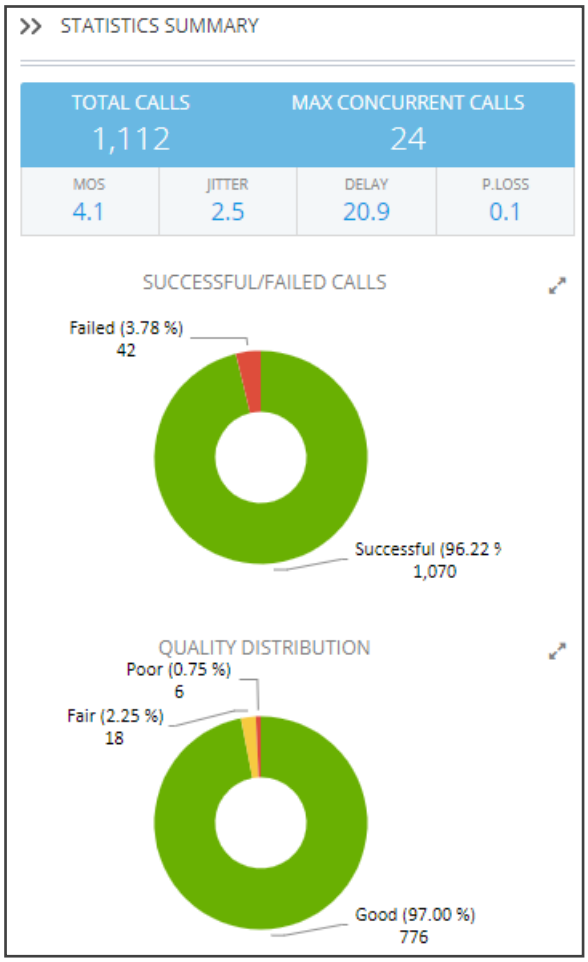
- Average Call Duration (ACD) chart shows distribution of ACD in the network over time. Point your mouse over a bar to determine average call duration in that time interval.
- MOS chart. Point your mouse over a bar to determine the average MOS scored in that time interval.
- Packet Loss chart. Point 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 6-43: 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 265). You can optionally filter the page by Time Range (see Filtering to Access Specific Information on page 212) and Topology (see Filtering by 'Topology' on page 215).

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 265. 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 212) and Topology (see Filtering by 'Topology' on page 215).

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 265). 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 212) and Topology (see Filtering by 'Topology' on page 215).

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 276.

➢ **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.

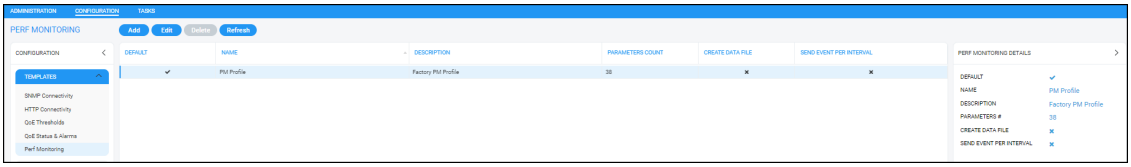
➢ **To set up PM *per specific device*:**

- 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

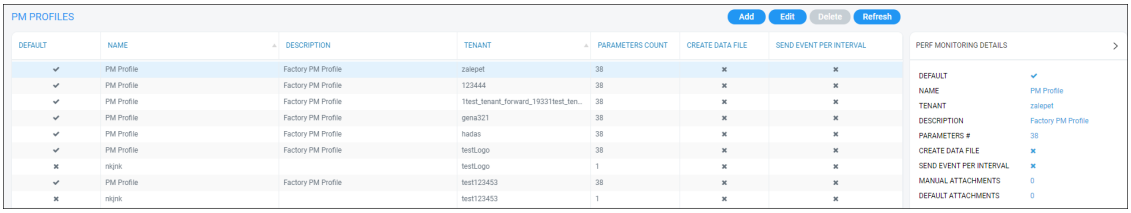
The OVOC includes an AudioCodes-provided *default* Performance Monitoring (PM) template. Parameters (metrics) selected in the default are those most frequently requested by AudioCodes enterprise and ITSP customers. The OVOC displays the default PM template in the Perf Monitoring page (**System** > **Configuration** > **Templates** > **Perf Monitoring**).

Figure 6-44: Perf Monitoring



- 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.

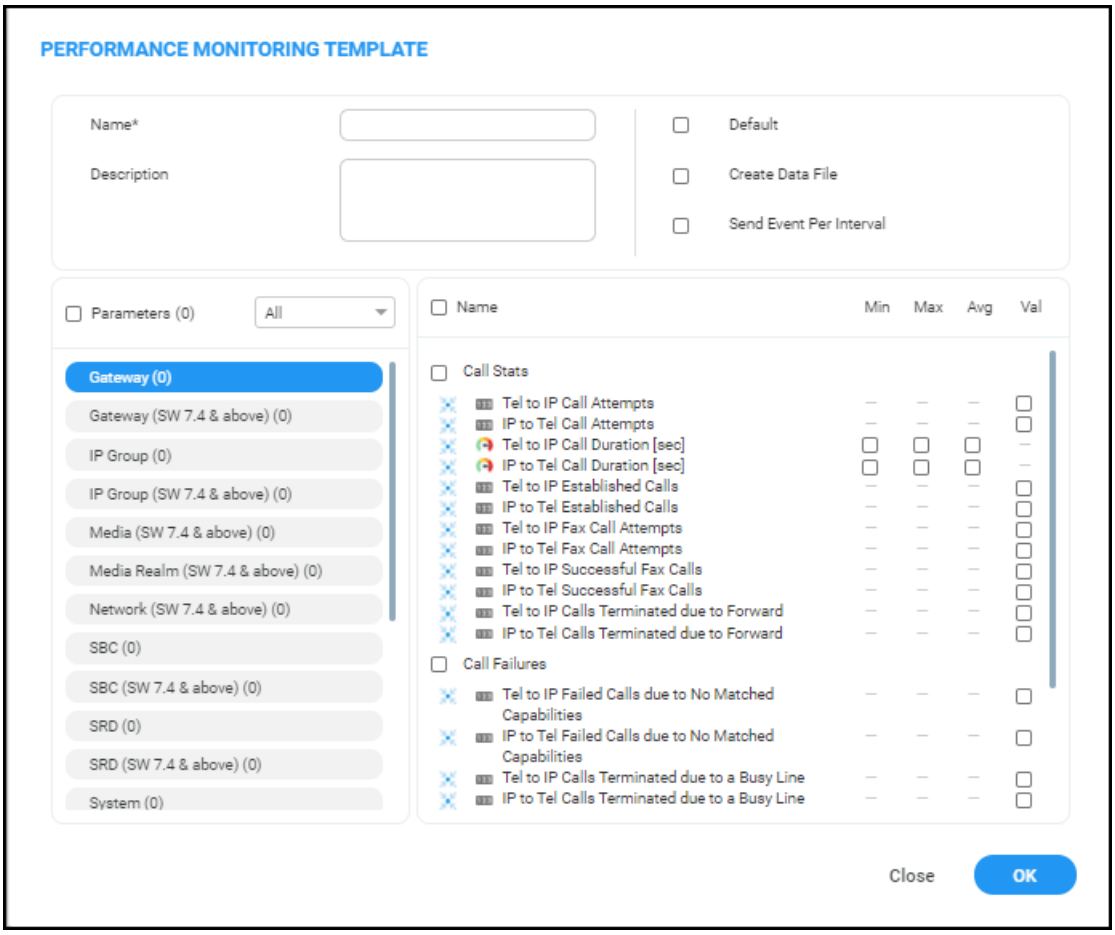
Figure 6-45: PM Profiles



➢ To add a PM template:

1. Open the Perf Monitoring page (**System** > **Configuration** > **Templates** > **Perf Monitoring**) and click **Add**.

Figure 6-46: Add PM Template

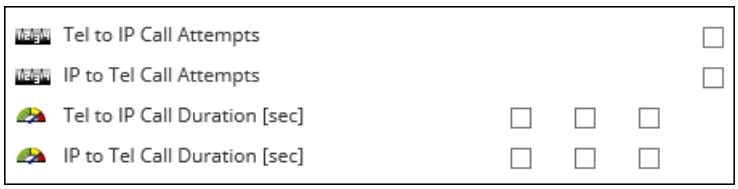


2. Configure the PM template using the table below as reference.

Table 6-17: 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 *always displays one default* 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

Parameter	Description
	deleted. Every time you add a tenant, all PM templates listed in the Perf Monitoring page are *duplicated as PM profiles* in the PM Profiles page (**Statistics** > **PM Monitoring**) and all PM profiles listed in the PM Profiles page are *automatically allocated to that newly added 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 this 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.
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': ■ System (0) - Click the tab to select or clear the check box **DSP Utilization** gauge. ■ SBC (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the counter **Tel to IP Call Attempts** and the gauge **Tel to IP Call Duration**, and / or the check boxes under 'Other Stats', e.g., **Media Legs.** ■ Gateway (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the **G711 Active Calls** gauge and the **Attempted Calls** counter, and / or the check boxes under 'Other Stats', e.g., **Media Legs**. ■ Network (0) - Click the tab to select or clear check boxes under 'Global', for example, the gauge **Net Util KBytes Tx** and the counter **Incoming Discarded Pkts**. ■ IP Group (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge **Invite Dialogs** and / or the check boxes under 'Other Stats', e.g., the counter **Subscribe Dialogs**. ■ Trunk Group (0) - Click the tab to select or clear the check box under 'Call Stats', i.e., the gauge **Call Duration**, the check box

Parameter	Description
	under 'Call Failures', i.e., the counter **No Resources Calls**, and / or the check boxes under 'Trunk Stats', e.g., the counter **All Trunks Busy Time**. ■ SRD (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge **ASR**. See the *SNMP Reference Guide* for detailed information about each PM parameter. 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 *User's Manual*.
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include *most but not all* 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)],	In the Call Stats pane shown in the next figure, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are *counters*. A single value (Val) is displayed after they're measured, i.e., # of counted call attempts.  In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are *gauges*. 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.

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.

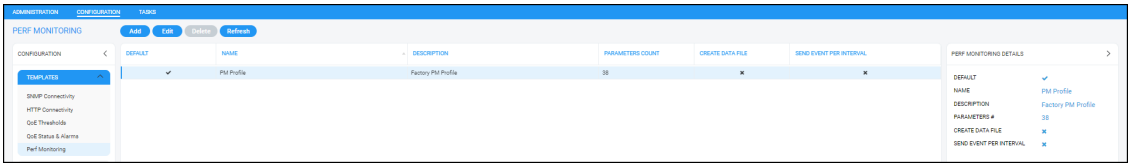
3. Click **OK** (or **Close** to exit without saving the template).

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 below

➢ To view PM templates:

- Open the PM Templates page (**System** > **Configuration** > **Templates** > **Perf Monitoring**).

Figure 6-47: Performance Monitoring Templates



➢ 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

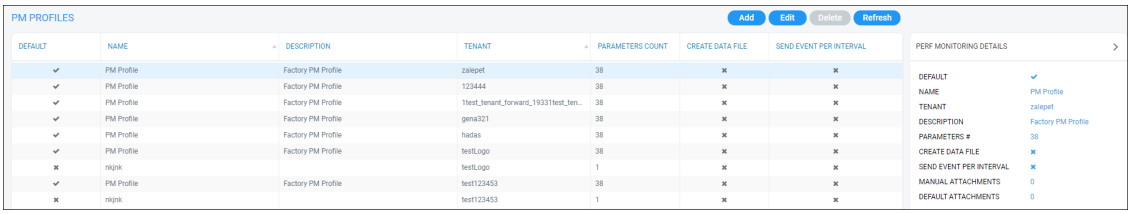
PM templates are *duplicated as PM profiles* in the PM Profiles page (**Statistics** > **PM Profiles**). Every time you add a new tenant, the default PM template together with all other templates (if you configured other templates) are automatically duplicated as profiles in the PM Profiles page and 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:

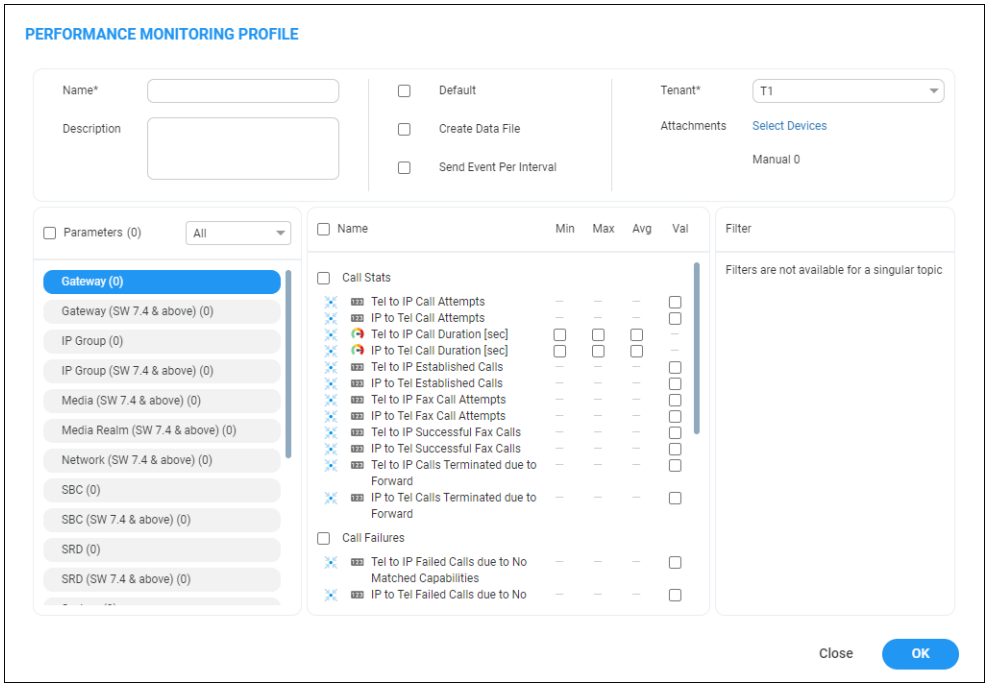
1. Open the PM Profiles page (**Statistics** > **PM Profiles**).

Figure 6-48: PM Profiles



2. Click **Add**.

Figure 6-49: PM Profile

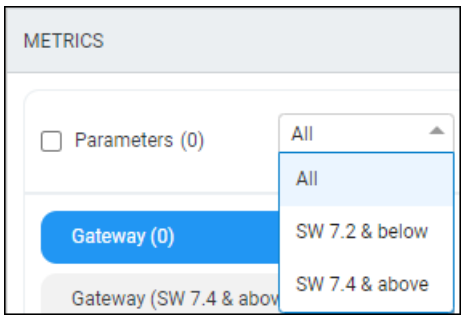


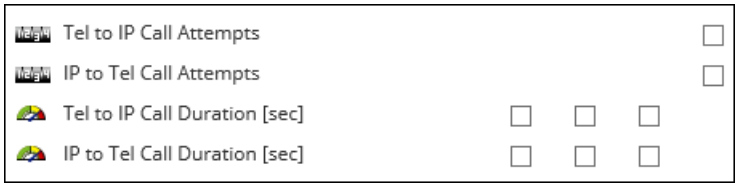
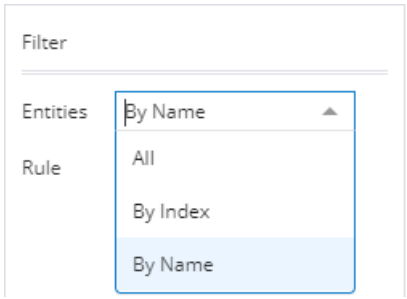
3. Configure a profile using the following table as reference.

Table 6-18: 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 the U.K. The description can help orient operators in complex networks.
Default	The PM Profiles page *always displays one default* 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

Parameter	Description
	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.
Attachments	The **Devices** link gives operators the option to *manually select a specific device* to which to attach this PM profile.
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 parameter categories are displayed: ■ System (0) - Click the tab to select or clear the check box **DSP Utilization** gauge. ■ SBC (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the counter **Tel to IP Call Attempts** and the gauge **Tel to IP Call Duration**, and / or the check boxes under 'Other Stats', e.g., **Media Legs.** ■ Gateway (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the **G711 Active Calls** gauge and the **Attempted Calls** counter, and / or the check boxes under 'Other Stats', e.g., **Media Legs**. ■ Network (0) - Click the tab to select or clear check boxes under 'Global', for example, the gauge **Net Util KBytes Tx** and the counter **Incoming Discarded Pkts**. ■ IP Group (0) - Click the tab to select or clear the check boxes

Parameter	Description
	under 'Call Stats', e.g., the gauge **Invite Dialogs** and / or the check boxes under 'Other Stats', e.g., the counter **Subscribe Dialogs**. ■ Trunk Group (0) - Click the tab to select or clear the check box under 'Call Stats', i.e., the gauge **Call Duration**, the check box under 'Call Failures', i.e., the counter **No Resources Calls**, and / or the check boxes under 'Trunk Stats', e.g., the counter **All Trunks Busy Time**. ■ SRD (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge **ASR**. Note you can configure the OVOC to sample by either: ■ **SW 7.2 and below** (i.e., via the SNMP API; applies to performance parameters of devices whose software version is 7.2 and earlier) -OR- ■ **SW 7.4 and above** (i.e., via REST parameters; applies to performance parameters of devices whose software version is 7.4 and later) -OR- ■ **All** (**SW 7.2 and below***and* **SW 7.4 and above**) (default) To configure this, click the 'Parameters (0)' field drop-down and select: 
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include *most but not all* PM metrics in your profile, select 'Name' (all check boxes will be selected) and then clear those to exclude.
Min Max Av Value	In the Call Stats pane shown in the figure below, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are *counters*. A single value (Val) is displayed after they're measured, i.e., the # of counted call attempts.

Parameter	Description
	 In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are *gauges*. 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.
Filter	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.  For example, after selecting tab 'IP Group' and then selecting **By Name**, enter a regular expression in the 'Rule' field that is displayed, e.g., **^B**; all IP groups whose names begin with **B** will be polled. The **By Index** filter enables you to filter specific indexes in the group to be polled; if you enter **9** (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.

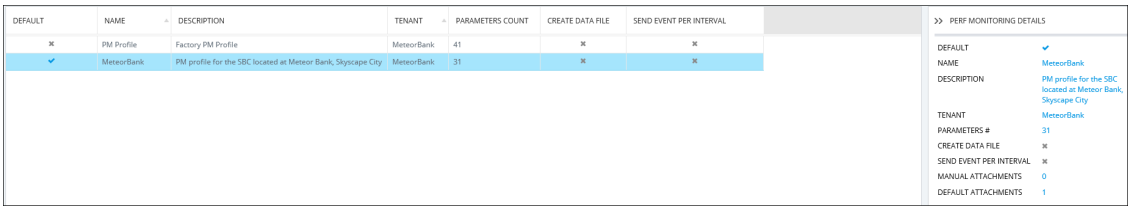
Thresholds are configured at the SBC level in the device's Web interface, in the Open Device page. See the device's *User's Manual* for more information. Thresholds can alternatively be configured in an ini file and loaded to the device in the OVOC's Software Manager. When a PM parameter value in the device crosses the configured threshold, the device generates an event that is sent to the OVOC.

Click **OK** (or **Close** to exit without saving the profile).

➢ To view PM profiles:

1. Open the PM Profiles page (**Statistics** > **PM Profiles**).

Figure 6-50: PM Profiles



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.

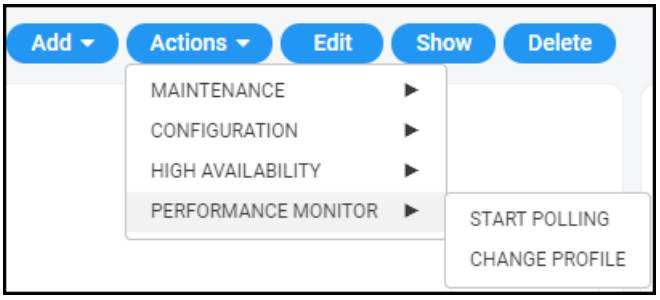
Starting and Stopping PM Polling

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 polling:

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.

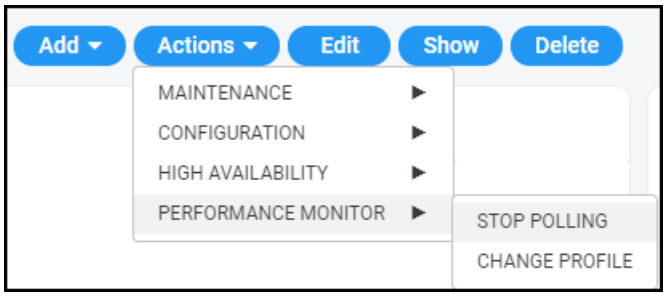
Figure 6-51: Start Polling



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.

3. After at least 15 minutes (the default polling interval), stop the polling.

Figure 6-52: Stop Polling



4. View the results of the poll.
   - See Viewing PM Data Resulting from Polling below

Viewing PM Data Resulting from Polling

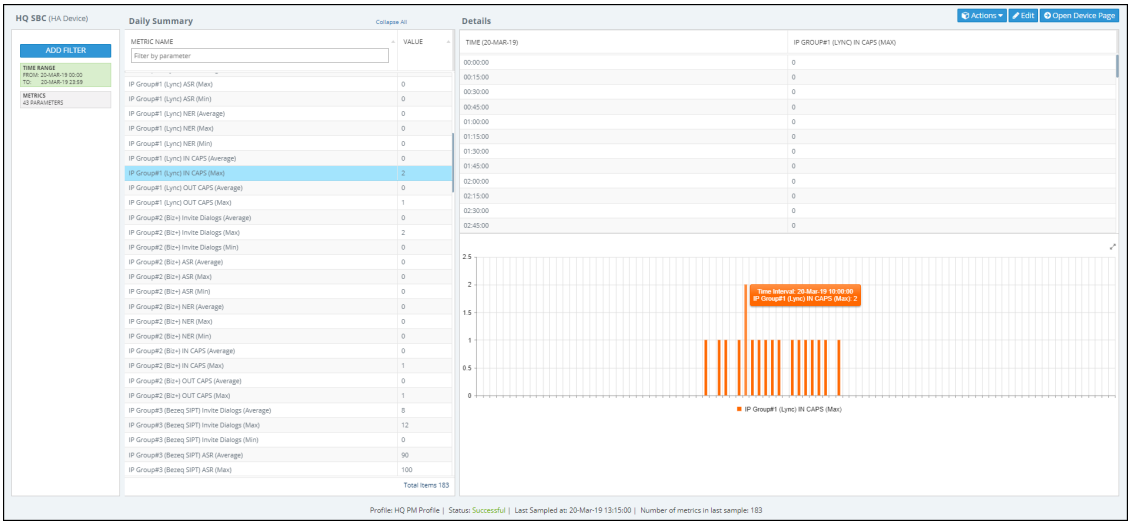
After polling a device (see Starting and Stopping PM Polling on the previous page), operators can view PM data resulting from polling in:

- 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:

1. Open the Device Management page (**Network** > **Devices** > **Manage**), select the device whose PM data you want to view, and then click the **Show** button.
2. In the device's dynamic tab's Summary page, click the **Statistics** tab.

Figure 6-53: Device Dynamic tab - Statistics



[Refer to the figure]

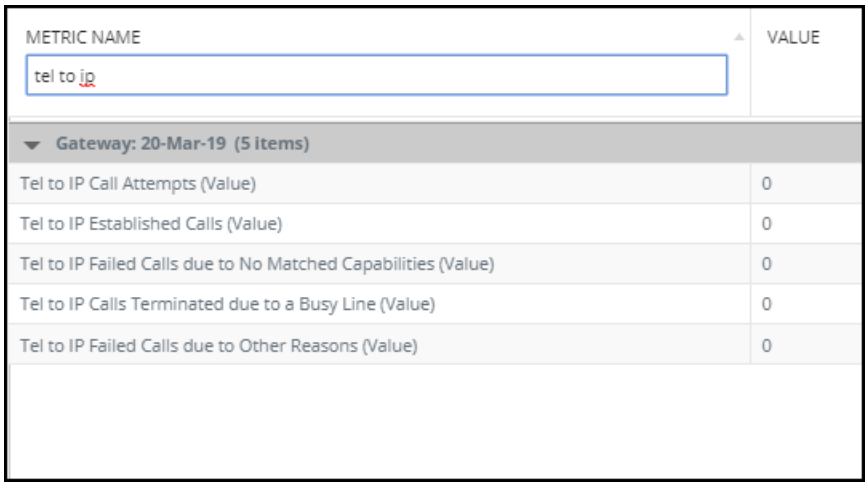
- Device Name (HQ SBC) [left side of page]
- ADD FILTER

- **Time Range**; click to select a different one; the default is the last 24 hours, 00:00 to 23:59
- **Metrics** (parameters); click to select fewer, more or different metrics; defaults are taken from this device's PM profile. Note that if REST is indicated in a category name, the OVOC samples the parameters under it using REST (applies to devices whose version is 7.4 and later). If a category name does not indicate REST, the OVOC samples the parameters under it using SNMP (applies to devices whose version is prior to 7.4).

■ 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 6-54: Filter by parameter

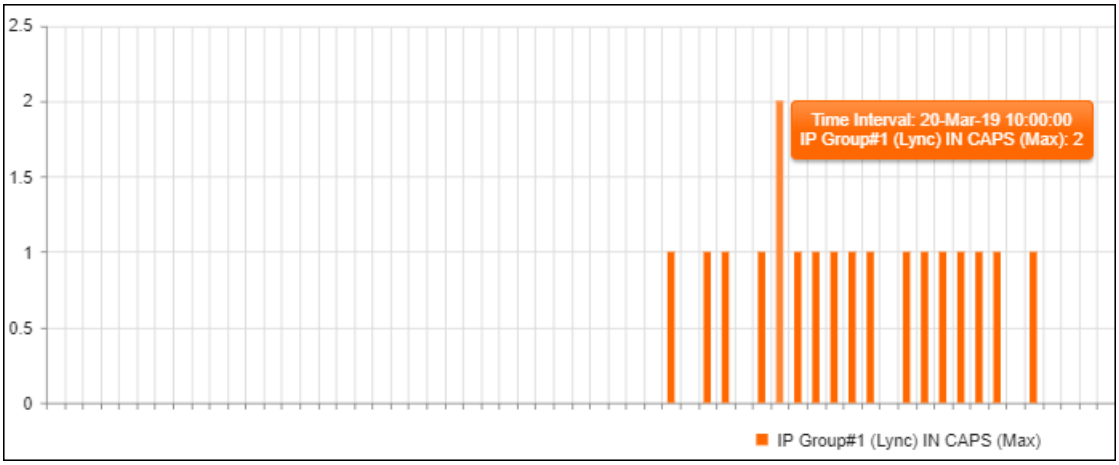


- a summary of metric values measured over the Time Range; the default is 24 hours, from 00:00 to 23:59; the list is structured per entity

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

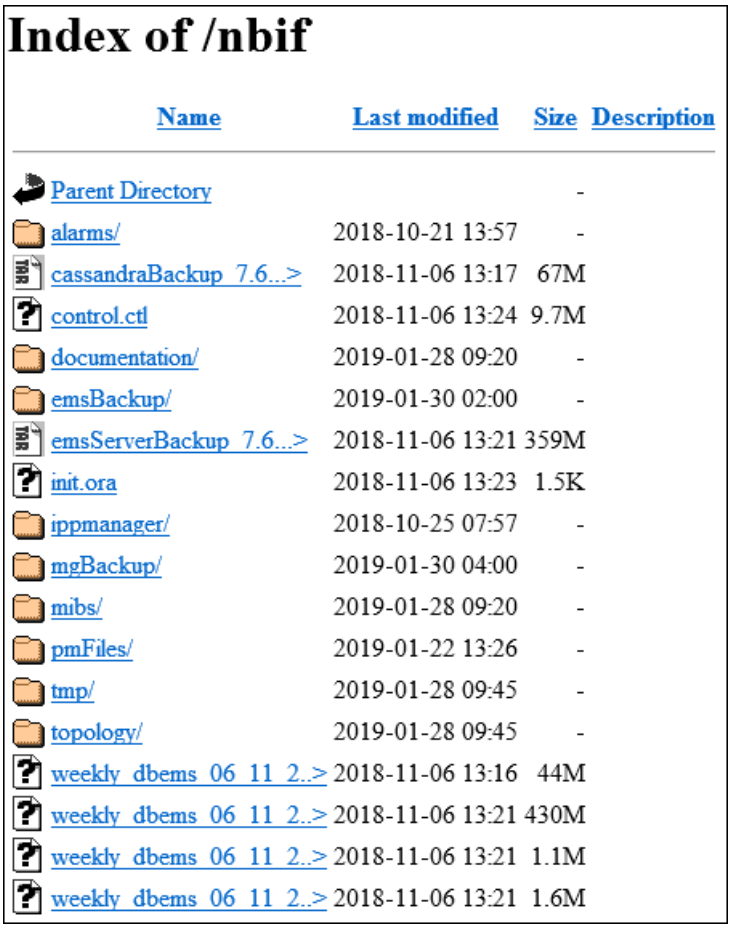
➢ To view PM data in a data file:

- 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 6-55: NBIF Index

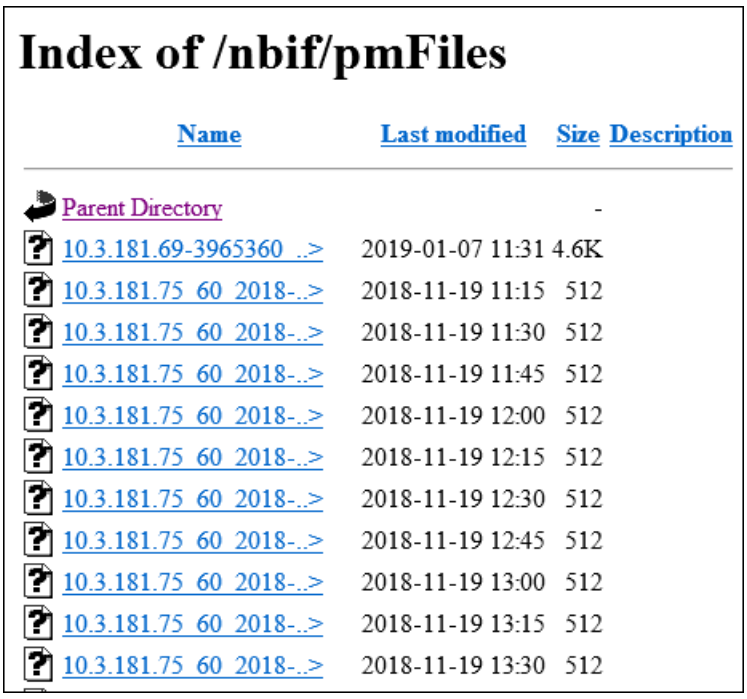


Index of /nbif

Name	Last modified	Size	Description
Parent Directory		-	
alarms/	2018-10-21 13:57	-	
cassandraBackup_7.6...>	2018-11-06 13:17	67M	
control.ctl	2018-11-06 13:24	9.7M	
documentation/	2019-01-28 09:20	-	
emsBackup/	2019-01-30 02:00	-	
emsServerBackup_7.6...>	2018-11-06 13:21	359M	
init.ora	2018-11-06 13:23	1.5K	
ippmanager/	2018-10-25 07:57	-	
mgBackup/	2019-01-30 04:00	-	
mibs/	2019-01-28 09:20	-	
pmFiles/	2019-01-22 13:26	-	
tmp/	2019-01-28 09:45	-	
topology/	2019-01-28 09:45	-	
weekly_dbems_06_11_2..>	2018-11-06 13:16	44M	
weekly_dbems_06_11_2..>	2018-11-06 13:21	430M	
weekly_dbems_06_11_2..>	2018-11-06 13:21	1.1M	
weekly_dbems_06_11_2..>	2018-11-06 13:21	1.6M	

2. In the NBIF index, click the entry **pmFiles**.

Figure 6-56: NBIF Index - pmFiles



Index of /nbif/pmFiles

Name	Last modified	Size	Description
Parent Directory		-	
10.3.181.69-3965360_..>	2019-01-07 11:31	4.6K	
10.3.181.75_60_2018-..>	2018-11-19 11:15	512	
10.3.181.75_60_2018-..>	2018-11-19 11:30	512	
10.3.181.75_60_2018-..>	2018-11-19 11:45	512	
10.3.181.75_60_2018-..>	2018-11-19 12:00	512	
10.3.181.75_60_2018-..>	2018-11-19 12:15	512	
10.3.181.75_60_2018-..>	2018-11-19 12:30	512	
10.3.181.75_60_2018-..>	2018-11-19 12:45	512	
10.3.181.75_60_2018-..>	2018-11-19 13:00	512	
10.3.181.75_60_2018-..>	2018-11-19 13:15	512	
10.3.181.75_60_2018-..>	2018-11-19 13:30	512	

- File-naming convention:

- File Name Format: DeviceName_NodeId_TimeInterval.xml
- Time Interval Format: yyyy-MM-dd_TimeZone_HHmm
- Example: M4K1_123456_2018-04-16_IST_1200.xml

3. Open the file of the period whose PM metrics you want to view.

Figure 6-57: 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>
acPMSIPSBCAttemptedCallsVal</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>
         <topic>
```

- XML file format:

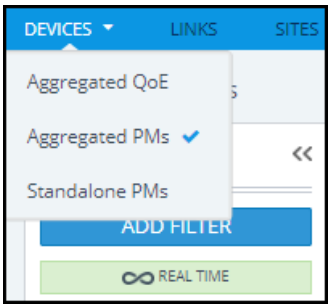
First-Level Info	Second-Level Info	Third-Level Info	Fourth-Level Info
Basic Device Info	Tenant Name	Region Name	-
	Device Name		
	Device IP Address		
	Serial Number (x2 if HA)		
	Product Type		
	Software Version		
Time Period	From Time	-	-
	To Time		
Profile Data	Profile ID	-	-
	Profile Name		
	Dictionary 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 6-58: Selecting 'Aggregated PMs'



2. In the Aggregated PMs page that opens, you're prompted 'Missing Topology and Metrics Filter'. Click **Add Filter**.

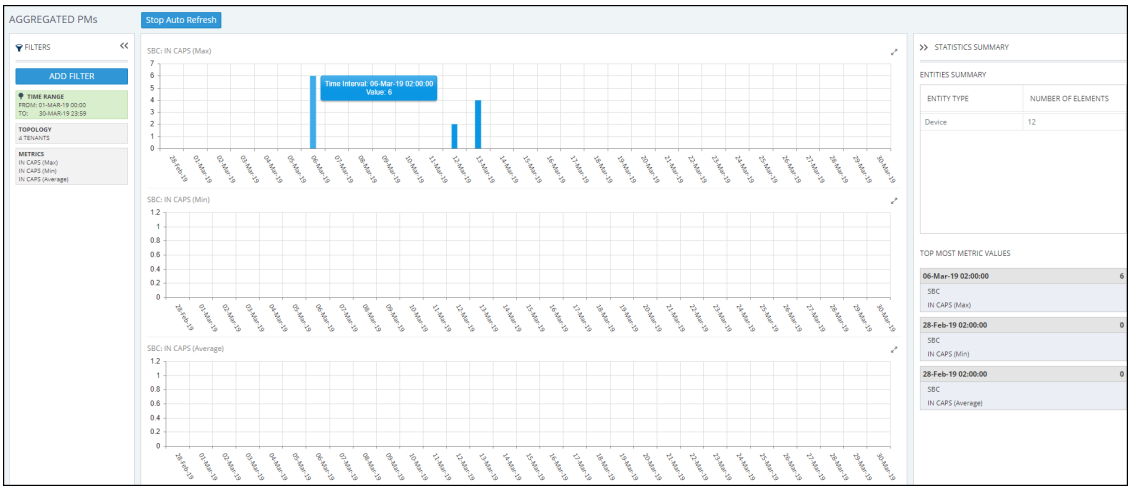
   a. Change the 'Time Range' or leave it unchanged at the default (the preceding 24 hours, i.e., 00:00 to 23:59).

   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 276 as reference.

3. View the aggregated PMs then displayed.

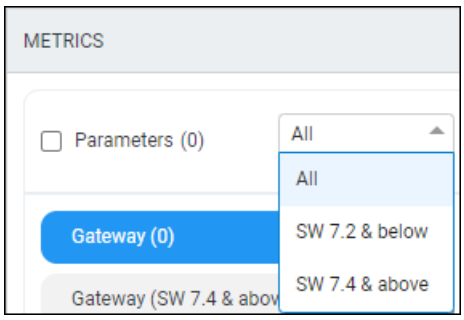
Figure 6-59: Aggregated PMs



[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; also available is an option to filter metrics (parameters) by:
    - **SW 7.2 and below** (i.e., via the SNMP API) -OR-
    - **SW 7.4 and above** (i.e., via REST parameters) -OR-

- **All (SW 7.2 and below *and* SW 7.4 and above)**



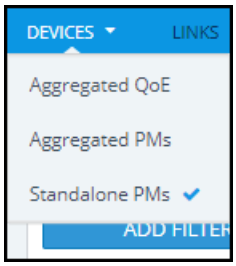
- Bar charts (middle of page):
  - each chart displays a metric (parameter); scroll down to view all
  - aggregated results are displayed in bars
  - if there are no aggregated results found or if the topmost metric value is 0, no bars are displayed
  - pointing the cursor over a bar displays a tool 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 6-60: Selecting 'Standalone PMs'



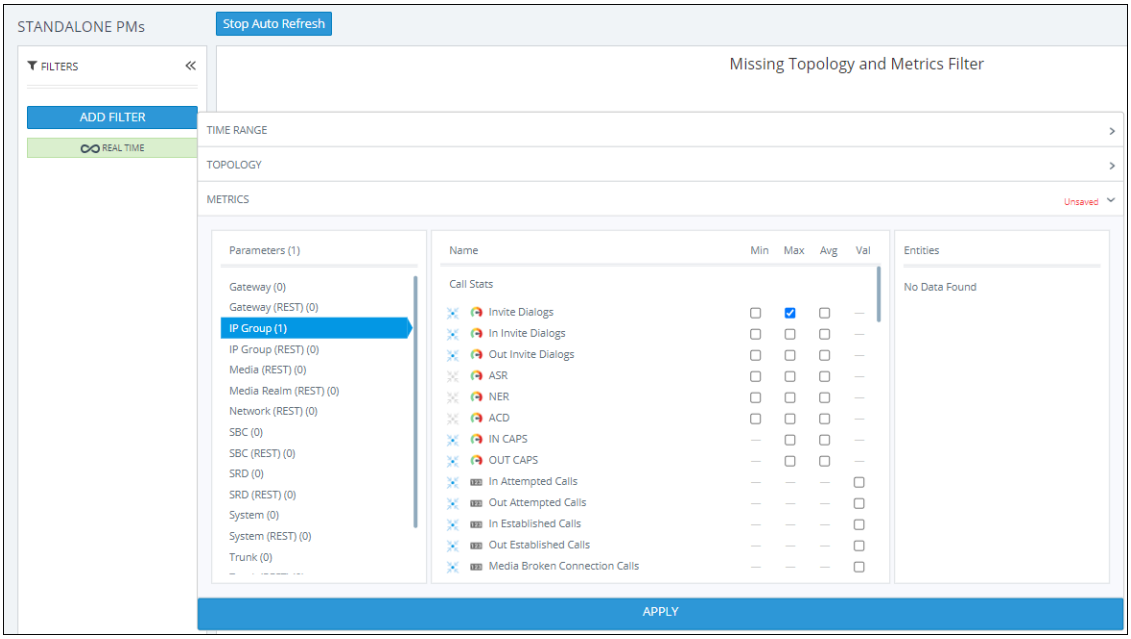
2. In the Standalone PMs page that opens, you're prompted 'Missing Topology and Metrics Filter'. Click **Add Filter**.

   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.

Figure 6-61: Standalone PMs

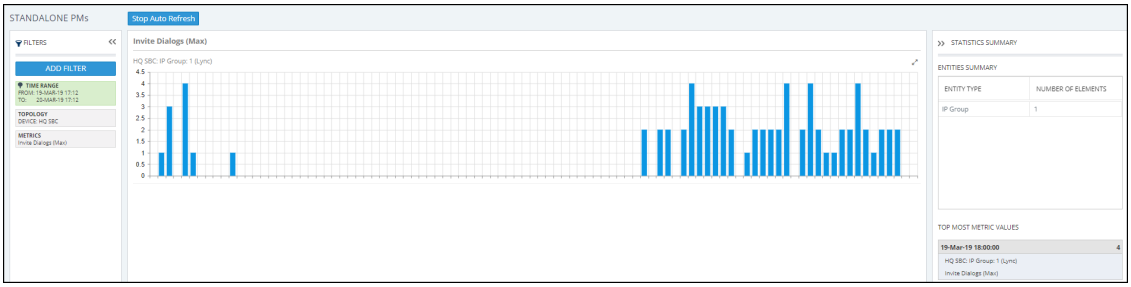


If REST is indicated in a category name as shown in the preceding figure, the OVOC samples the parameters under it using REST (applies to devices whose version is 7.4 and later). If a category name does not indicate REST, the OVOC samples the parameters under it using SNMP (applies to devices whose version is prior to 7.4).

d. In the 'Entitles' 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 6-62: 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.

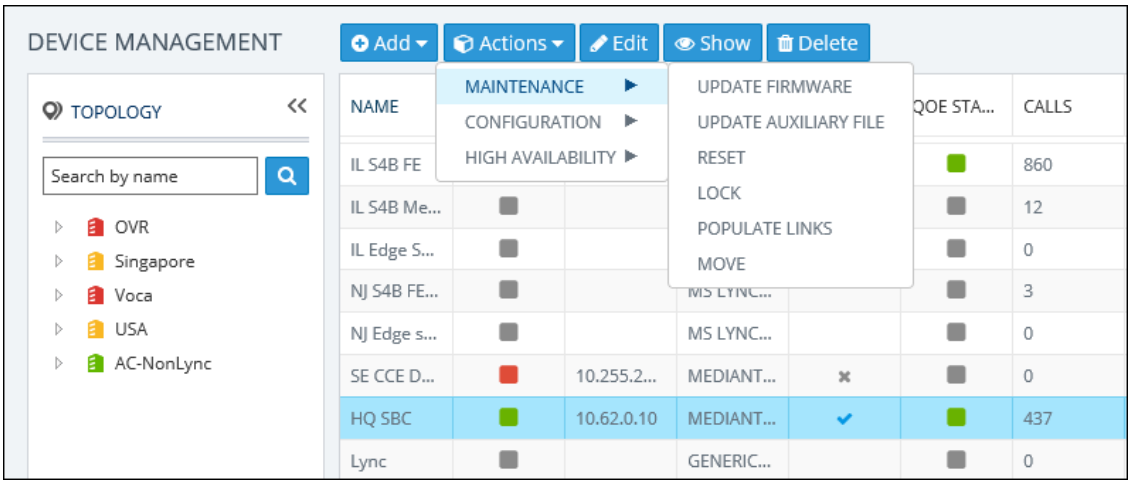
Performing Management Actions

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 295)
  - Reset (see Resetting a Device on page 298)
  - Lock or Unlock (see Locking or Unlocking a Device on page 299)
  - Populate Links (see Populating Links on page 300)
  - Move (see Moving a Device on page 301)
- **Configuration**

- Backup (see Backing Up on page 302)
- Restore Last Backup (restore a device's configuration) (see Restoring the Last Backup on page 303)
- Restore Default Configuration (see Setting Configuration Factory Defaults on page 304)
- Save Configuration to Flash (see Saving a Device's Configuration File to Flash Memory on page 304)
- Save Current Configuration to File (see Saving a Device's Configuration File to the PC on page 305)

- **Performance Monitor**
  - Start Polling (see Starting and Stopping PM Polling on page 281)
  - Change Profile (see Changing Profile on page 306)
- **High Availability**
  - Reset Redundant (see Resetting Redundant on page 305)
  - Switchover (see Performing Switchover on page 306)

4. Use also the following dedicated buttons to perform management actions:
   - **Show** device information (see Showing Device Information on page 308)
   - **Show** link information (see Showing Link Information on page 310)
   - **Show** user information (see Showing User Information on page 311)
   - **Edit** a device (see Editing a Device on page 313)
   - **Delete** a device (see Deleting a Device on page 313)

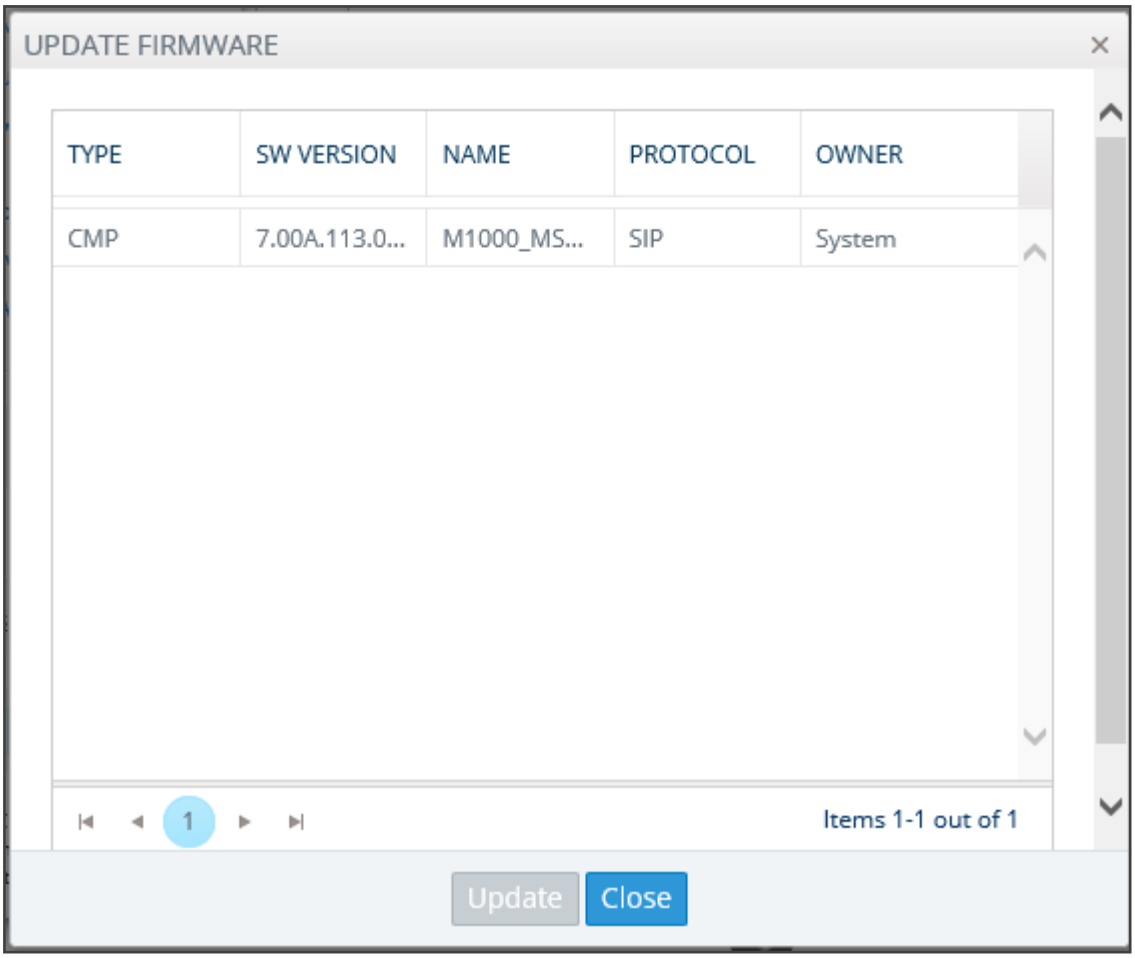
Updating Firmware

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**.

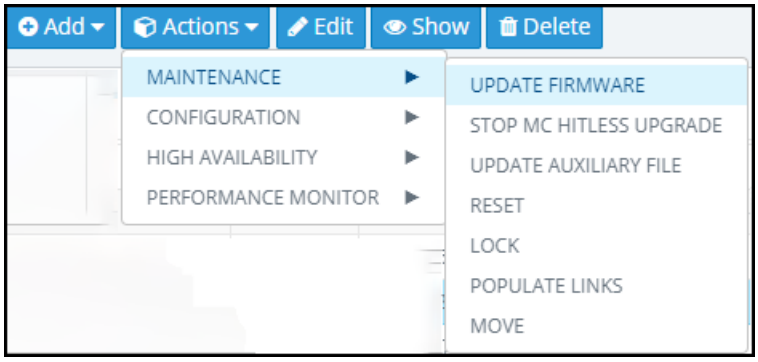
Updating Firmware on a Component in a Media Cluster

The OVOC lets you update the firmware (the .cmp firmware version file) on an AudioCodes MC (Media Component) in an AudioCodes Media Cluster (AudioCodes Mediant Cloud Edition (CE) software session border controller (SBC).

➢ To update the firmware:

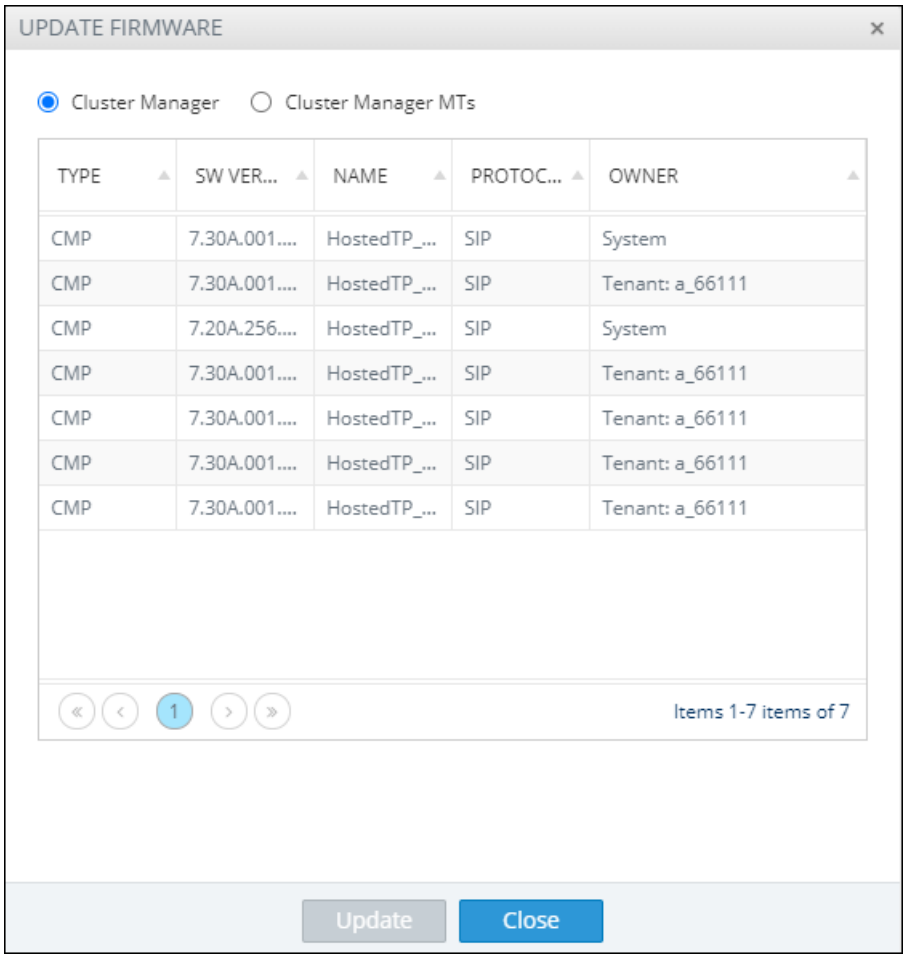
1. In the Device Management page (**Network** > **Devices** > **Manage**), select the device.
2. From the **Actions** drop-down, select **Maintenance** and then **Update Firmware**.

Figure 7-3: Device Management - Update Firmware



3. In the Update Firmware screen that opens, view the different .cmp firmware version files.

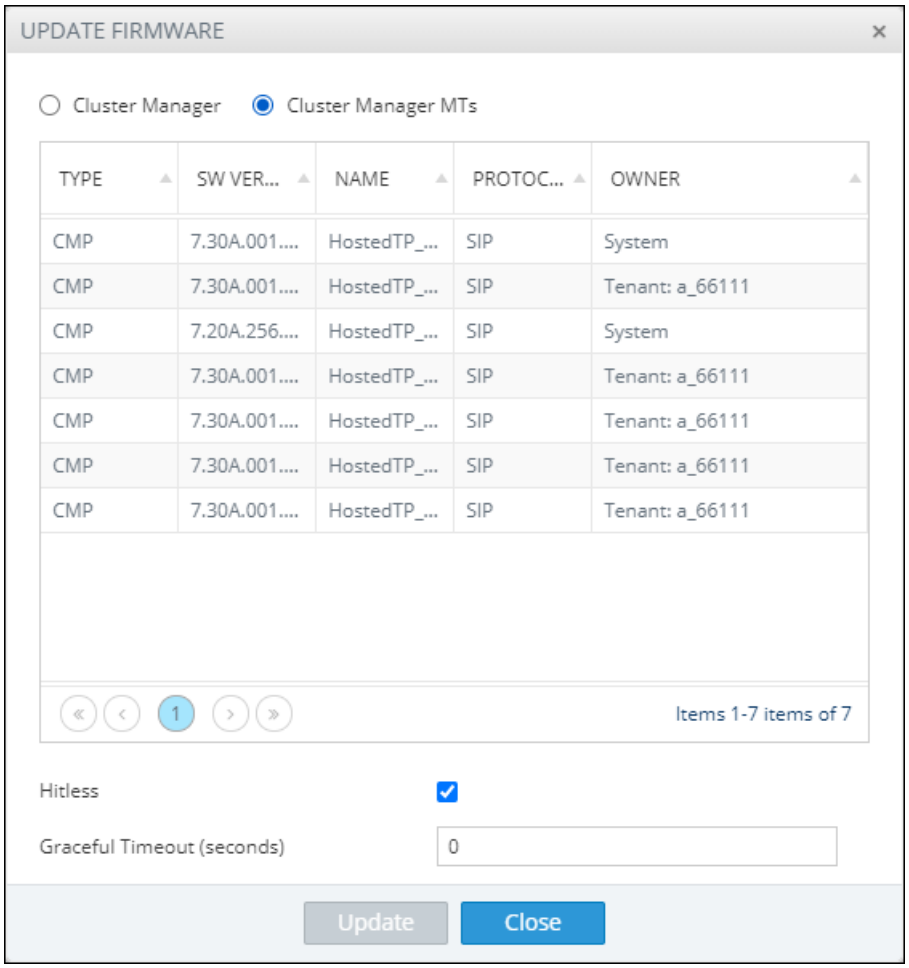
Figure 7-4: Update Firmware - Cluster Manager



4. **Select Cluster Manager** as shown in the preceding figure or **Cluster Manager MTs** as shown in the next figure.

- **Cluster Manager** is AudioCodes' Media Cluster (AudioCodes Mediant Cloud Edition (CE) software session border controller (SBC) which conveys the media).
- **Cluster Manager MTs** are the components in a cluster to which multiple upgrade can be performed.
- The .cmp firmware version file differs from component to component. There are only two options but they're for all MT components of each MTC; either hosted CMPs or Mediant 4000.
  - ✔ SW ESBC SC
  - ✔ SW VE SBC SC
  - ✔ SW SE SBC SC
  - ✔ SW VE-H SBC SC
  - ✔ SW SE-H SBC SC
  - ✔ SW SE CM
  - ✔ SW 9000 SBC CM
  - ✔ SW VE SBC CM
  - ✔ SW SE SBC CM

Figure 7-5: Update Firmware - Cluster Manager MTs



The Cluster Manager upgrade is a regular upgrade only for the selected MTC device in OVOC

5. Select the **Hitless** option for the firmware upgrade to be performed on one component at a time. The firmware upgrade is performed on component 1 and then when finished, on component 2, etc. This upgrade is slower than the non-hitless option.
6. Clear the **Hitless** option for the upgrade to be non-hitless; all components are upgraded at once; this option is faster than the hitless option.

Hitless only applies to MT upgrade

7. Optionally enter a value for **Graceful Timeout (seconds)**. If the upgrade is performed when calls are in progress, the value you enter defines how much time to wait for the calls to end before the OVOC begins the upgrade.

Graceful Timeout only applies to MT upgrade

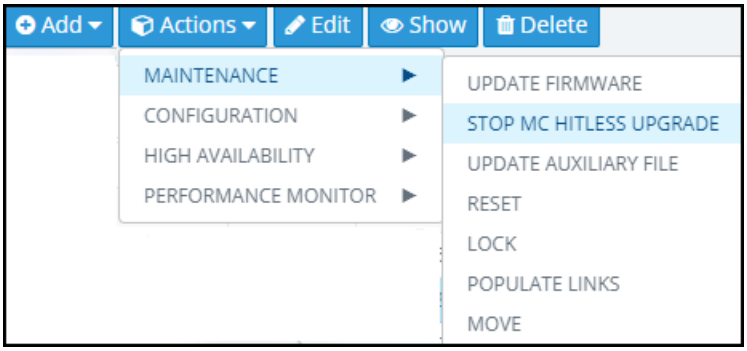
8. Select the firmware file you require and click the enabled **Update** button.

➢ To stop the upgrade:

> Stop Upgrade only applies to MT upgrade

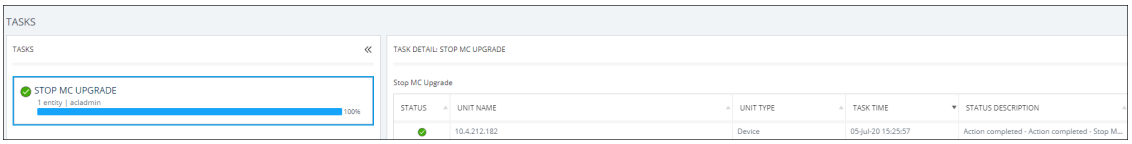
1. In the Device Management page (**Network** > **Devices** > **Manage**), select the device.
2. From the **Actions** drop-down, select **Maintenance** and then **Stop MC Hitless Upgrade**.

Figure 7-6: Stop MC Hitless Upgrade



3. In the Tasks page (**System** > **Tasks**), you'll view two tasks:
   a. the upgrade task (showing how many upgrades succeeded if a multiple component upgrade was performed, job status, i.e., how many out of how many are performed, which ones are, which ones aren't).
   b. the stopped task (shown in the next figure)

Figure 7-7: Tasks



For more information about the Tasks page, see Tasks tab on page 110

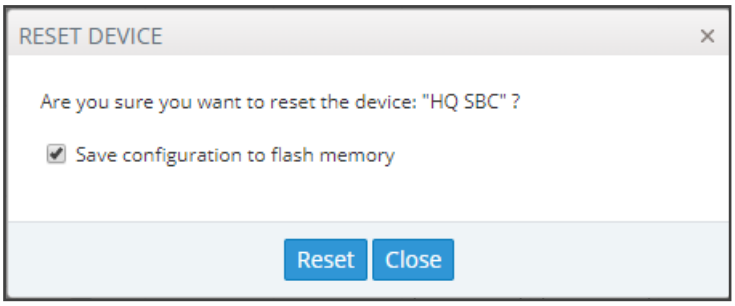
Resetting a Device

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 7-8: 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**.

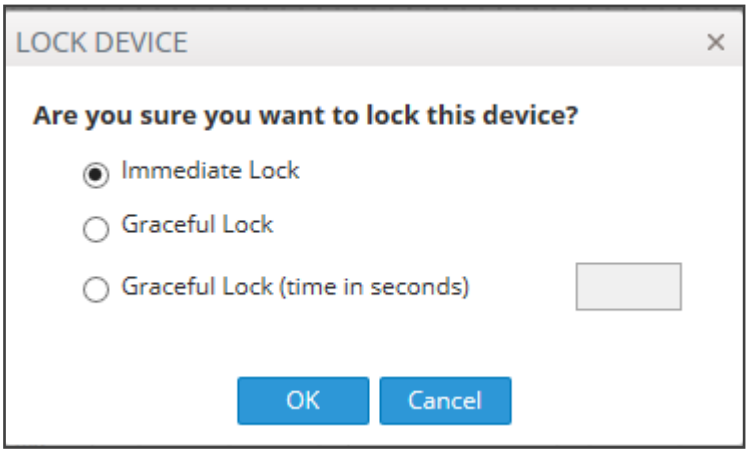
Locking or Unlocking a Device

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 7-9: Lock Device



3. Select either:
   - **Immediate Lock**. The device is locked regardless of traffic. Any existing traffic is terminated immediately.

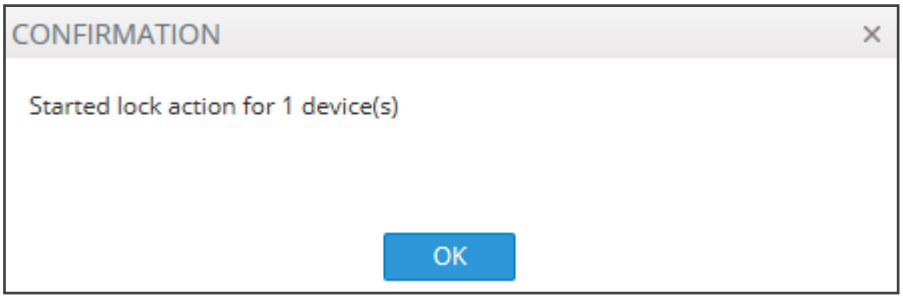
- **Graceful Lock**. Existing calls first complete and only then is the device locked. No new traffic is accepted.
- **Graceful Lock (time in seconds)**. The device is locked only after the time configured in the adjacent field. During this time, no new traffic is accepted. If no traffic exists and the 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 7-10: 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 159] 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.

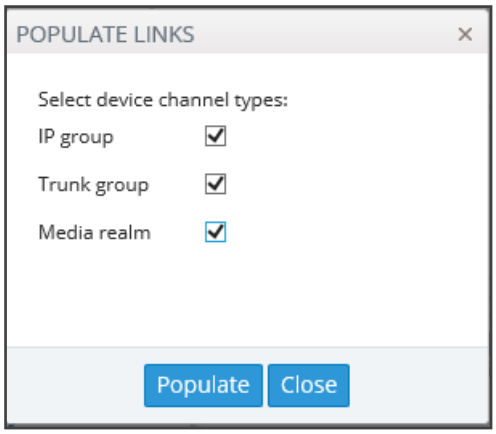
Example:

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 7-11: 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.

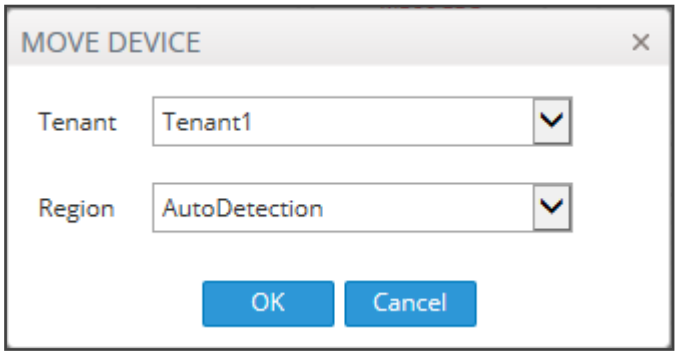
Moving a Device

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 7-12: Move Device



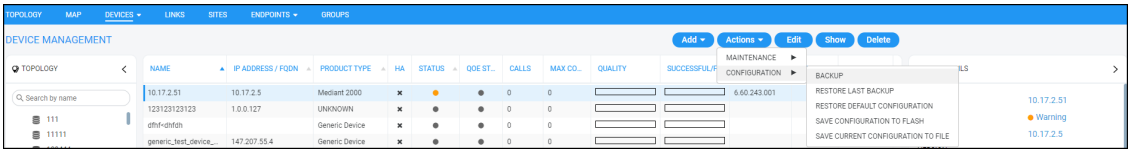
3. From the 'Tenant' drop-down, select from the list of tenants the tenant to move the device to (see Adding a Tenant on page 113 for information on how to add a tenant).
4. From the 'Region' drop-down, select from the list of regions the region to move the device to (see Adding a Region on page 129 for information on how to add a region).
5. If the device is an HA device, configure 'Reset redundant'.
6. Click **OK**.

Backing Up

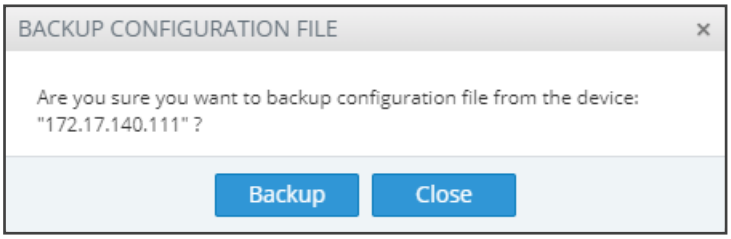
You can back up a device's configuration file to the server.

➢ To back up a device's configuration file to the server:

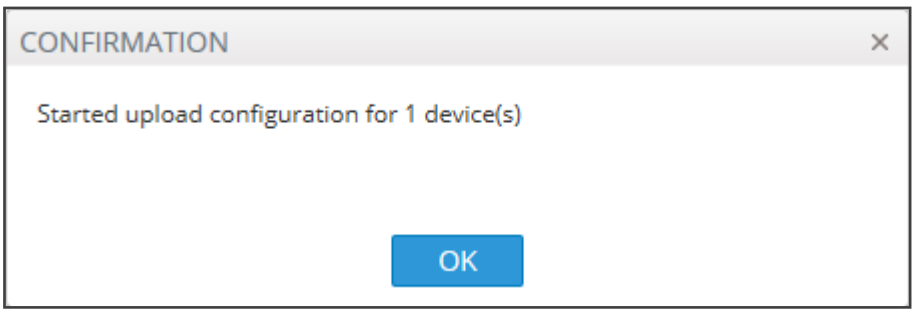
1. Open the Device Management page (**Network** > **Devices > Manage**) and select the device from which to upload the software configuration file to the server.
2. Click **Actions** and from the drop-down choose the 'Configuration' sub-menu.



3. Select the **Backup** option.



4. In the Backup Configuration File prompt, click **Backup**.



5. Click **OK**; the latest file is uploaded to the server from the device.

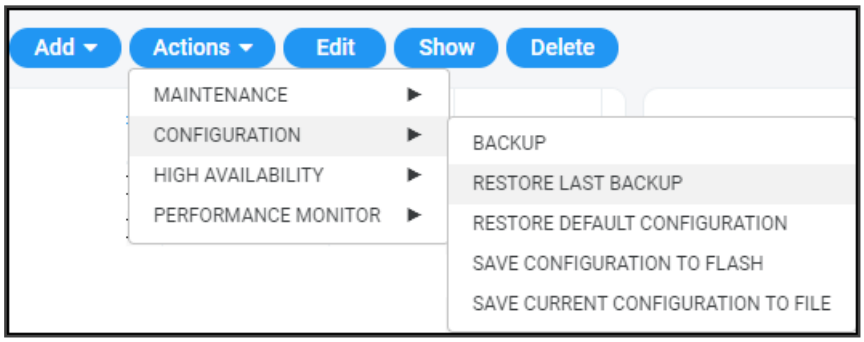
- If the device selected is an MSBR, the latest cli file is uploaded.
- If the device selected is an MP-202 or MP-204, the latest conf file is uploaded.
- If the device selected is any other AudioCodes device (except CloudBond and UMP), the latest ini file is uploaded.

Restoring the Last Backup

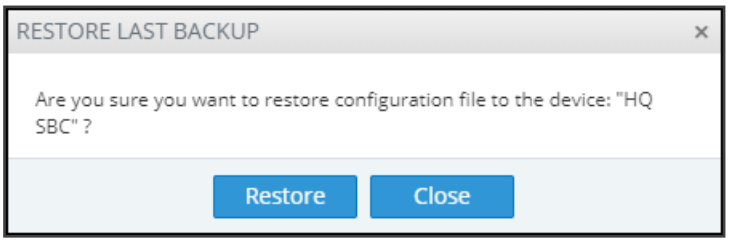
You can restore or download the latest software configuration file, backed up on the server, to the device.

➢ **To download the latest backup software configuration file to the device:**

1. Open the Device Management page (**Network** > **Devices** > **Manage**) and select the device to which to restore the latest backed-up software configuration file.
2. Click **Actions** and from the drop-down, choose the 'Configuration' sub-menu.



3. Select the **Restore Last Backup** option.



4. In the prompt, click **Restore**.
5. 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.

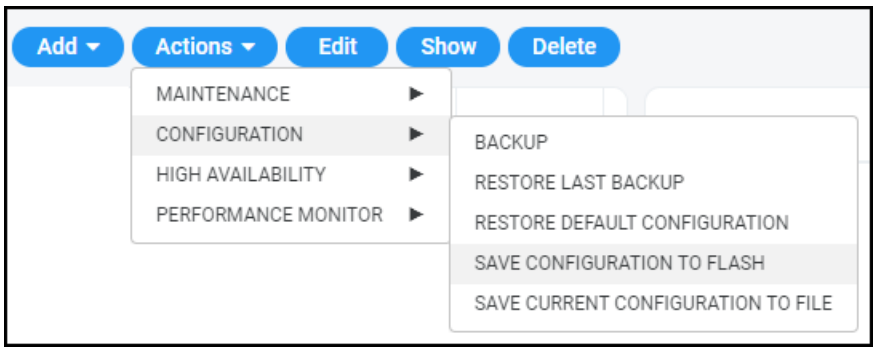
Saving a Device's Configuration File to Flash Memory

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 298) or before powering down, in order to ensure configuration changes you made are retained.

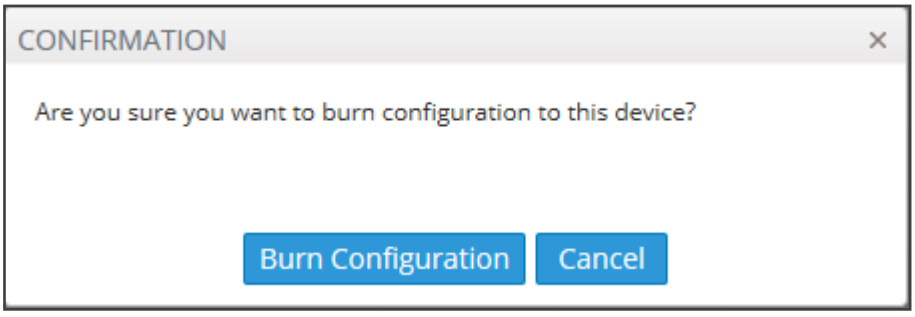
➢ **To save (burn) a device's software configuration to the device's flash memory:**

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 7-13: Saving Configuration to Flash



3. From the sub-menu, select **Save Configuration to Flash**.



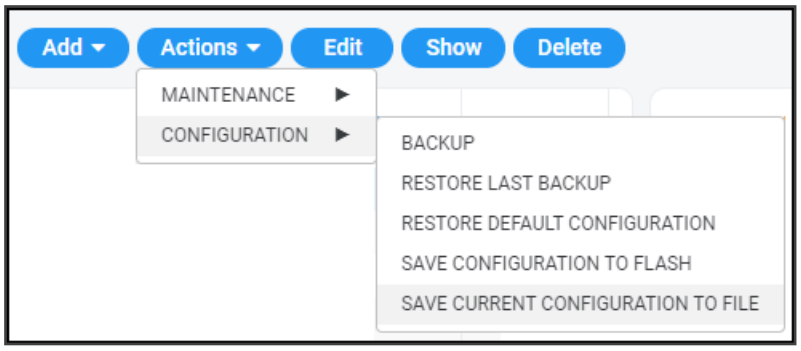
> Saving configuration to flash may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see Locking or Unlocking a Device on page 299).

Saving a Device's Configuration File to the PC

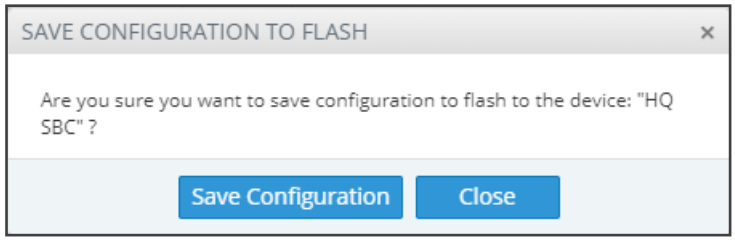
You can save the current configuration of a device to your PC.

➢ 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**.



2. From the Actions menu, select **Save Config File**.



3. 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

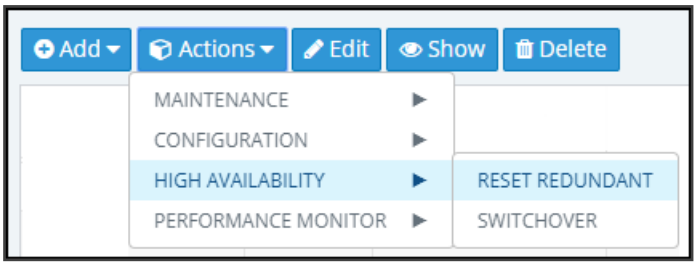
You can reset a device's redundant chassis.

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:

1. 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 7-14: 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 298 for more information.

Performing Switchover

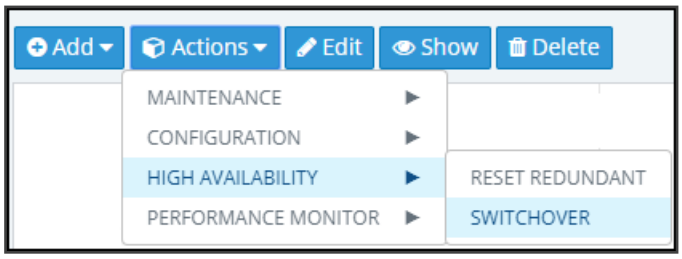
This only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

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 activated **Actions** button.

Figure 7-15: Actions – Switchover



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 276. A profile determines how the OVOC monitors network | device performance. A profile determines:

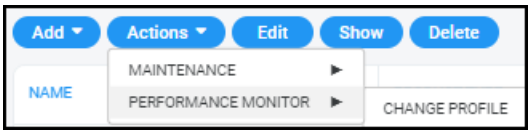
- What's monitored [which network | device parameters]

- How frequently [how often they're polled]
- When an alarm is issued [at what parameter threshold]
- Alarm severity [if a parameter threshold is exceeded]

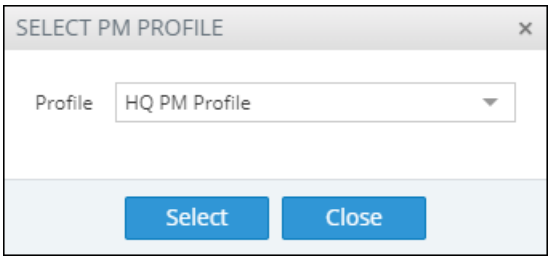
➢ To change profile:

1. In the Device Management page (**Network** > **Devices**), click the **Actions** button and select **Performance Monitor** > **Change Profile**.

Figure 7-16: Change Profile



2. From the drop-down list, choose the profile (template) according to which to poll the device for PM metrics, and then click **Select**.



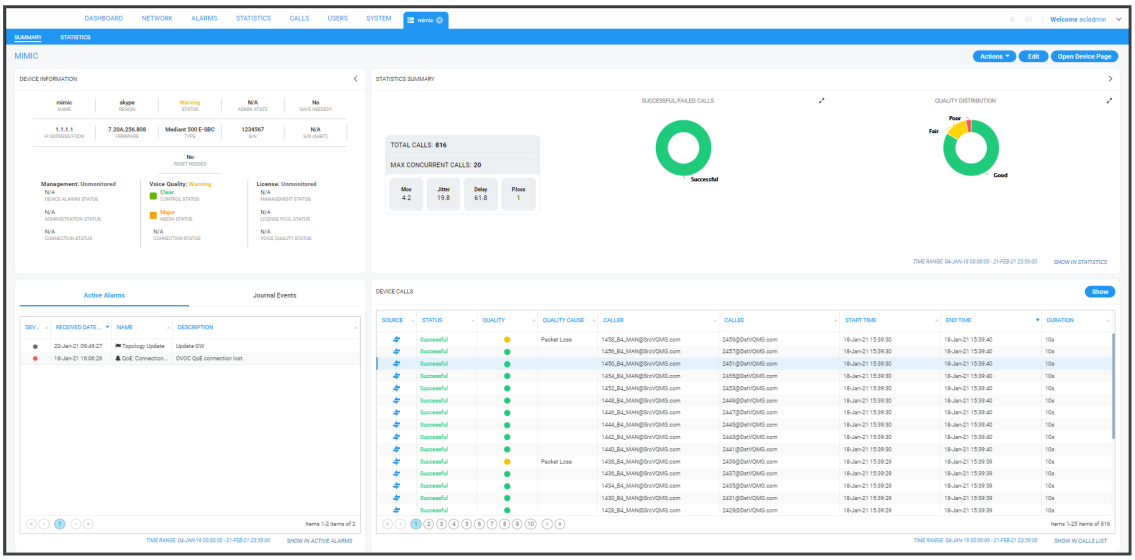
Showing Device Information

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.

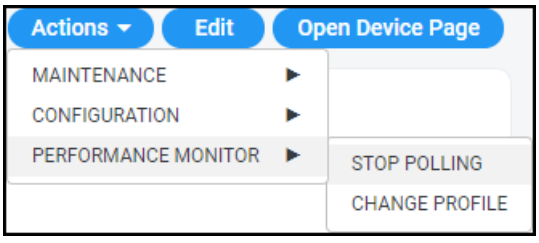
Figure 7-17: Show Device Information



The page displays information related to active alarms on the device, journal events, statistics summary and calls made over the device.

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.

2. Click the **Actions** button to access the same actions available in the Network Topology page and Network Devices page, including **Performance Monitoring** > **Stop Polling** | **Change Profile**.



See also Starting and Stopping PM Polling on page 281 and Changing Profile on page 306.

3. Click the **Edit** button to edit the device in the AC Device Details screen.

4. Click the **Open Device Page** button to open the device's Web interface. Only devices whose version is 7.0 and later support SSO.

- If the device's version is 7.0 or later, the Web interface opens in the browser *with* SSO.
- If the device's version is earlier than 7.0, the Web interface opens in the browser *without* SSO. These include CloudBond devices and SmartTAP (all versions).
- If devices are behind a NAT or if the URL for CloudBond and SmartTAP is unknown, the **Open Device Page** button will not be displayed .

5. 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.
6. 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 324 for more information).

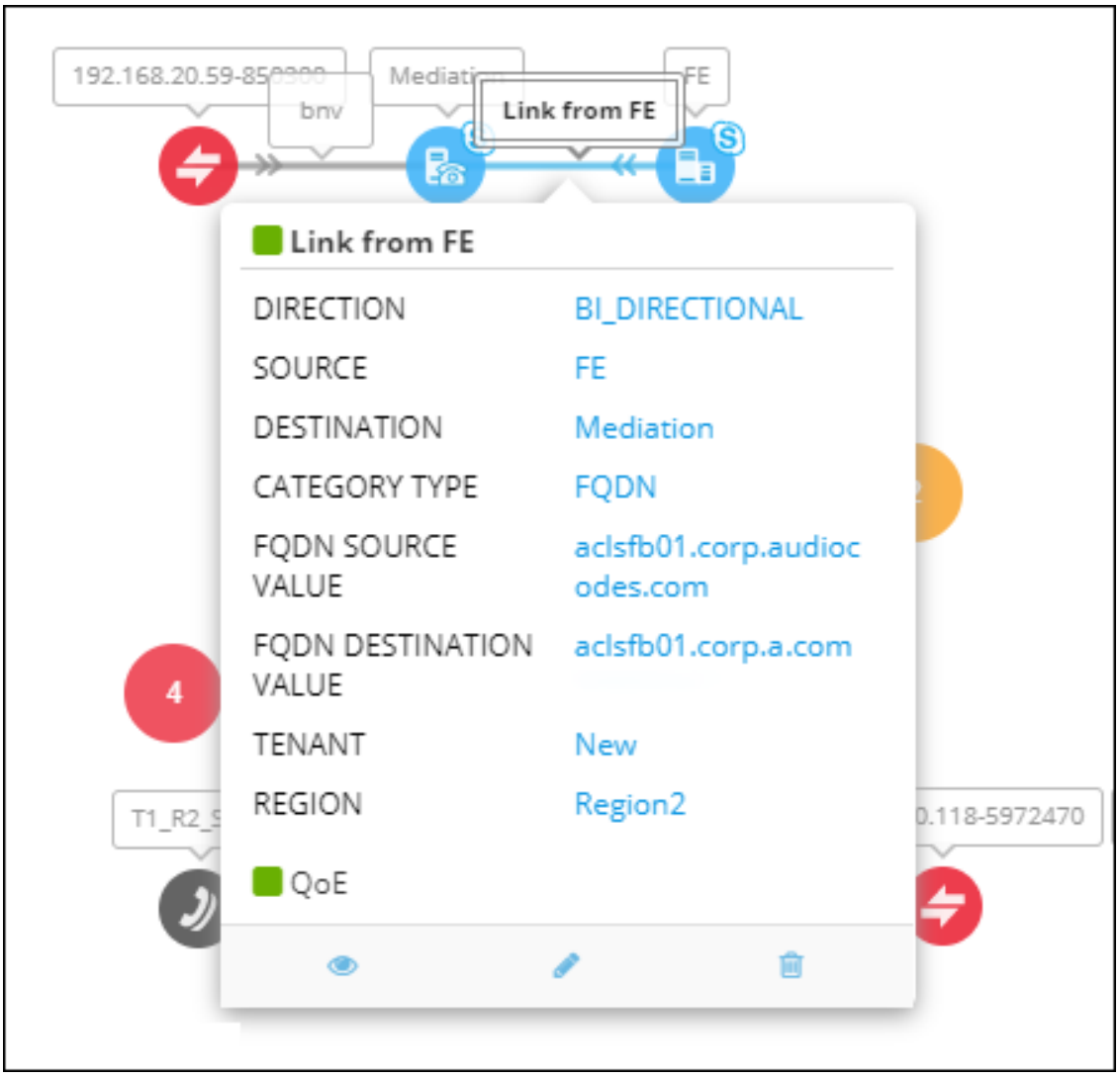
Showing Link Information

The OVOC lets operators quickly retrieve and assess information related to any link in the network.

➢ To show link information:

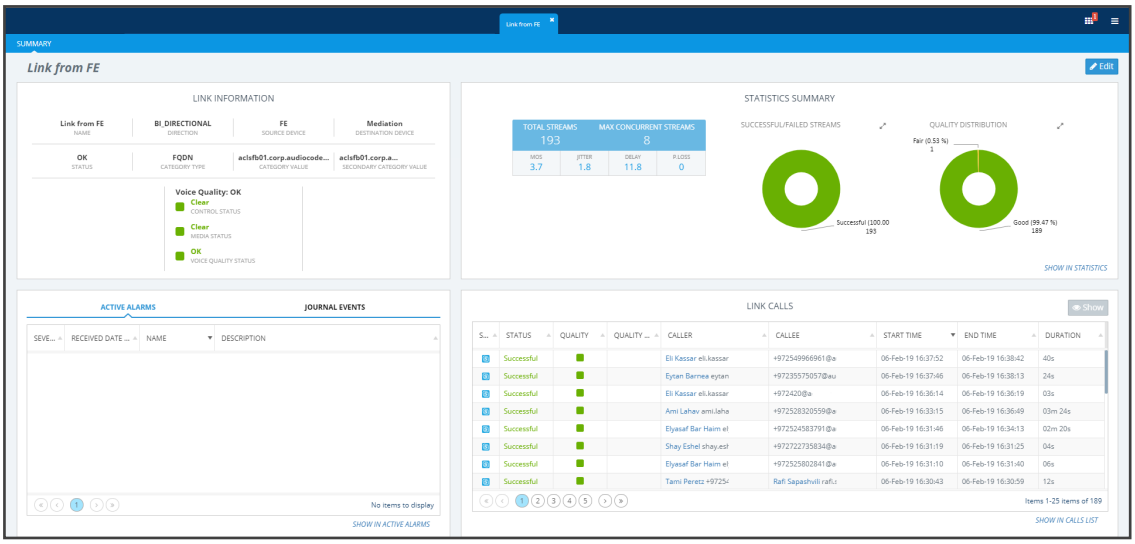
1. In the Network page under the **Topology** or **Links** tab, select the link and click the **Show** button. Alternatively, under the **Topology** tab, hover your mouse device over the link label and from the pop-up menu select the icon 👁.

Figure 7-18: Show Link Information



The link's Summary page opens.

Figure 7-19: Link's Summary Page



2. The page displays information about active alarms on the link, journal events, statistics summary and calls made over the link.
3. 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.
4. 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.
5. 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 324 for more information).

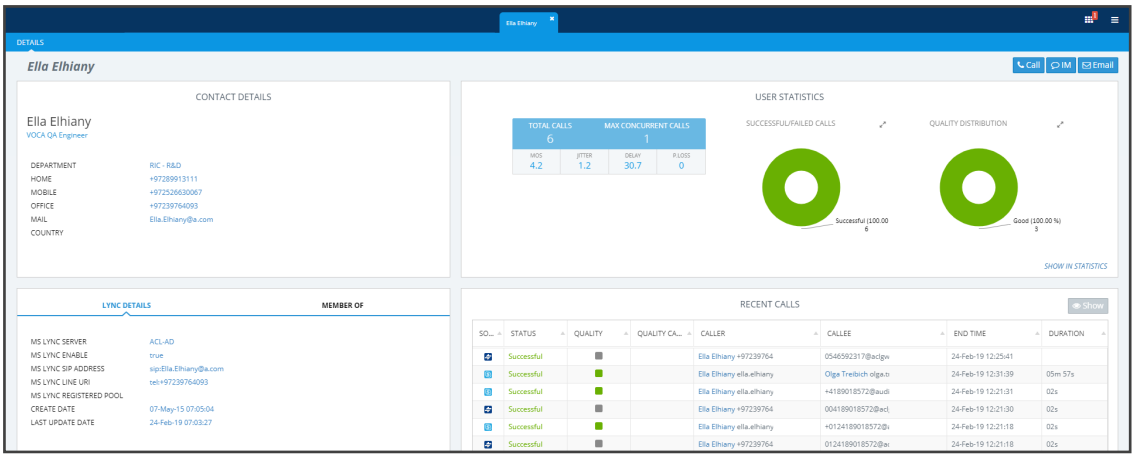
Showing User Information

The OVOC lets operators quickly retrieve and assess telephony information related to any user.

➢ To show telephony information about a user:

1. In the Users page under the **Users Experience** or **User Details** tab, select a user and click **Show**.

Figure 7-20: Showing Information about a User



2. 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 324 for more information).

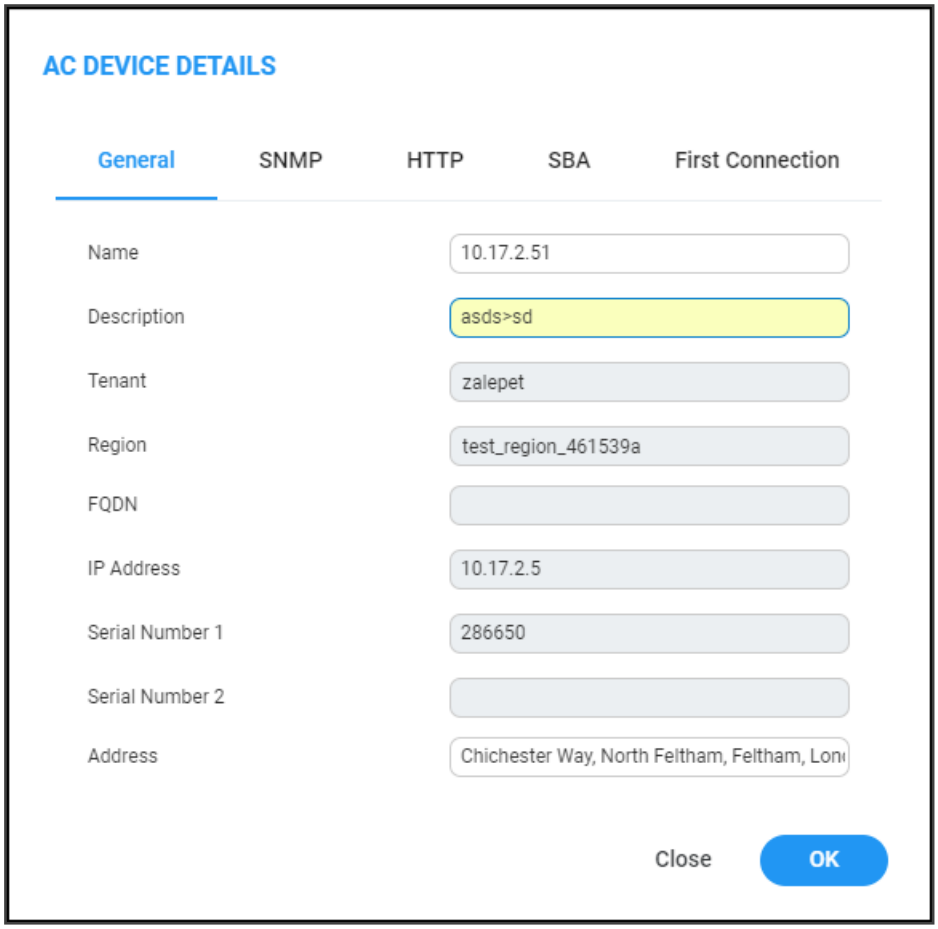
Editing a Device

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 7-21: Device Details



2. Edit the device's details. For more information, see Adding AudioCodes Devices Automatically on page 130.
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**.

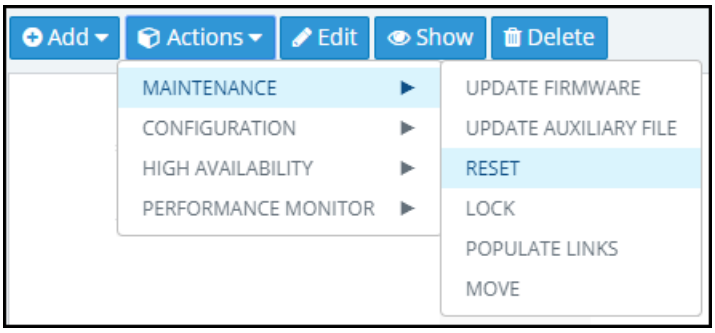
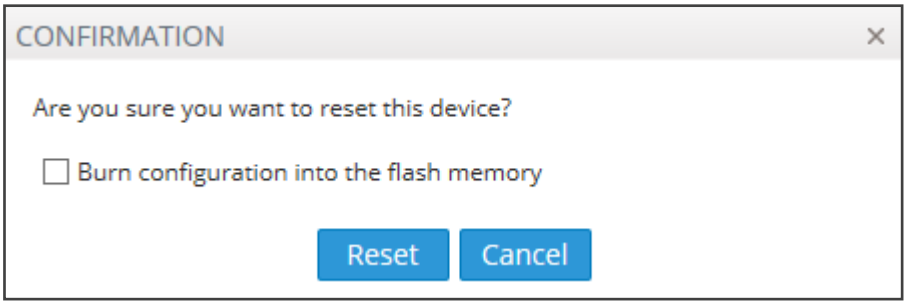


Figure 7-22: Reset Device – Confirmation



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 304 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 157.

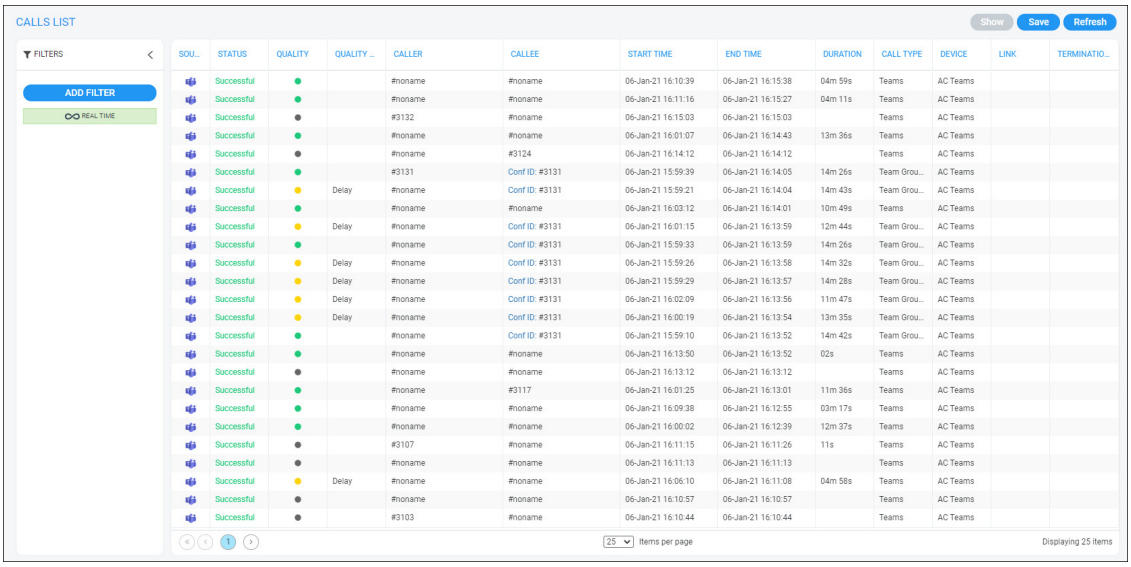
8 Obtaining Quality Statistics on Calls

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 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 212), Topology (see Filtering by 'Topology' on page 215), Source Type (see Filtering by 'Severity' on page 230), Quality (see Filtering by 'Quality' on page 319) or More Filters (see Filtering by 'More Filters' on page 320).

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 Teams indicates the call is from Microsoft Skype for Business indicates the call is from an AudioCodes device.

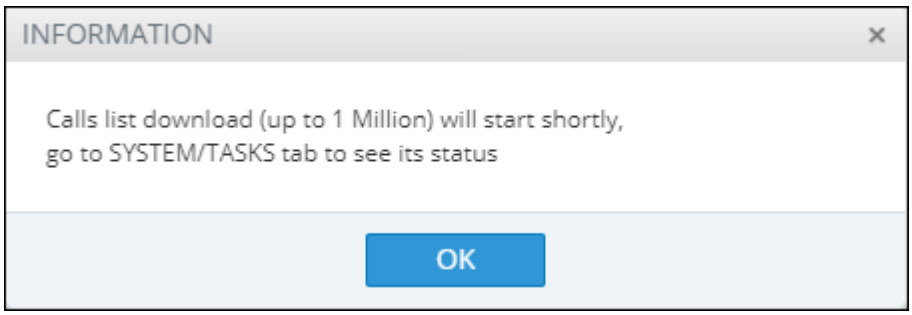
Column	Description	
	indicates the call is from an AudioCodes IP phone.	
Status	Indicates call control status: **Successful** or **Failed**	
Quality	Indicates the call quality: Green = Good, Yellow = Fair, Red = Poor, Gray = Unknown	
Quality Cause	Delay (msec)	Delay (or latency) - the time it takes for 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 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.	

Column	Description
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.



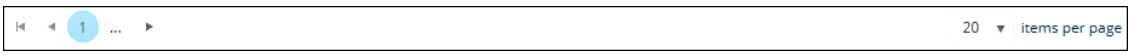
An SBC call (exclusively) whose duration is longer than three hours (e.g., the session of a participant in a Skype for Business conference call over an SBC) or an SBC call that is incompletely reported to the OVOC server won't be displayed in the Calls List.

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):

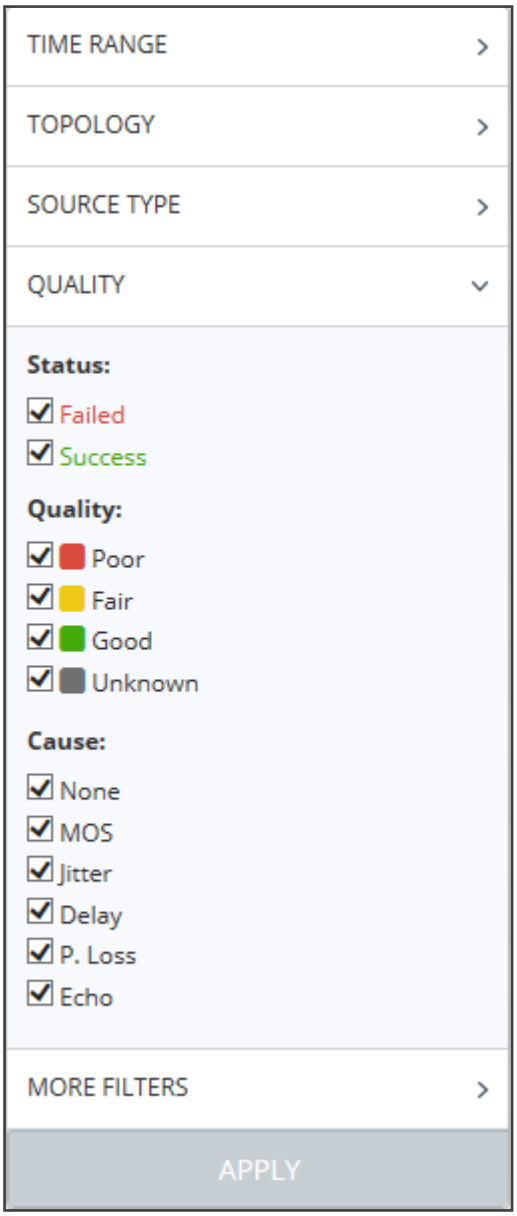
- Click the **|◂ Go to the first page** to return to the first page from any page.
- Click the **Go to the previous page** arrow to return to the page before the presently displayed page.
- Click **... [More pages]** to the left of the page number or **... [More pages]** to the right of the page number 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



Use the following table as reference.

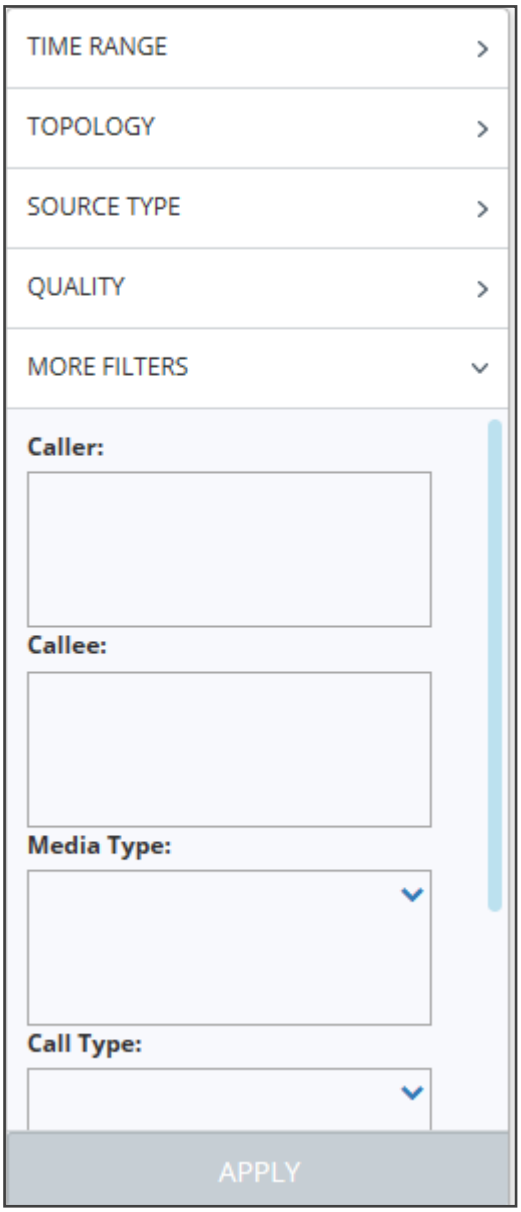
Table 8-2: 'Quality' Filter

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 *whose quality was poor/fair because there was a delay on the line*.

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



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.
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

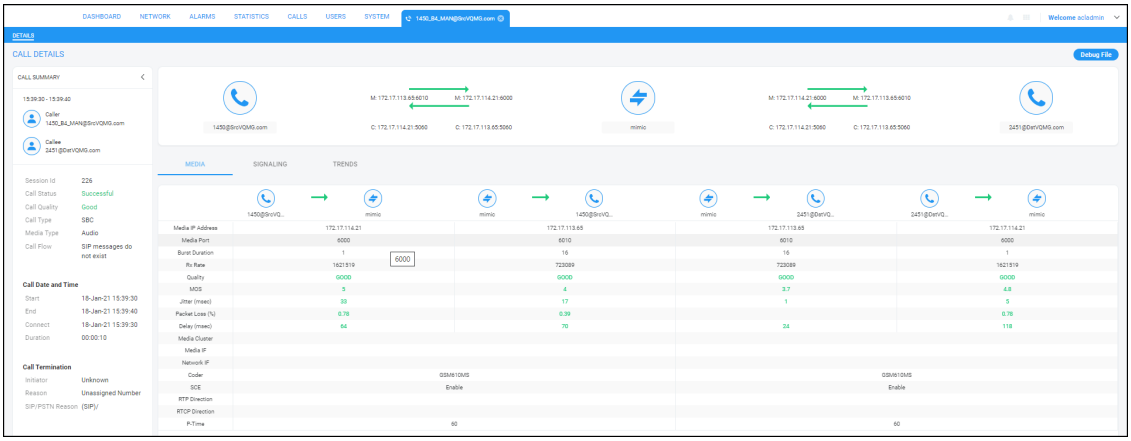
Filter	Description
	type), Video, Data, Audio Video, Chat, Audio V150 (currently unsupported), Text, Unknown or All (and then optionally remove unwanted media types). By default, all media types are selected.
Call Type	From the drop-down list, select the call type to display on the page, or enter a search string. Select either GW (Gateway), Teams, Teams Group Call, SBC, Skype Conference, Endpoint, Test SBC, HTTP, IP2IP or Skype. 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.
Termination Reason	Enter the reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason. Some AudioCodes termination reasons are: ■ Reason Not Relevant ■ Unassigned Number ■ Invalid Information Element Content ■ The remote equipment received an unexpected message that does not correspond to the current state of the connection. ■ Recovery on Timer Expiry ■ Protocol Error Unspecified ■ Unknown Error ■ Q931 Last Reason Some MS Skype for Business Termination Reasons are: ■ OK. Indicates the request was successful. ■ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed. ■ No Notification ■ Multiple Choices ■ Moved Permanently ■ Moved Temporarily ■ Use Proxy

Filter	Description
	■ Alternative Service

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 212), Topology (see Filtering by 'Topology' on page 215), Source Type (see Filtering by 'Severity' on page 230), Quality (see Filtering by 'Quality' on page 319) and / or More Filters (see Filtering by 'More Filters' on page 320), 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

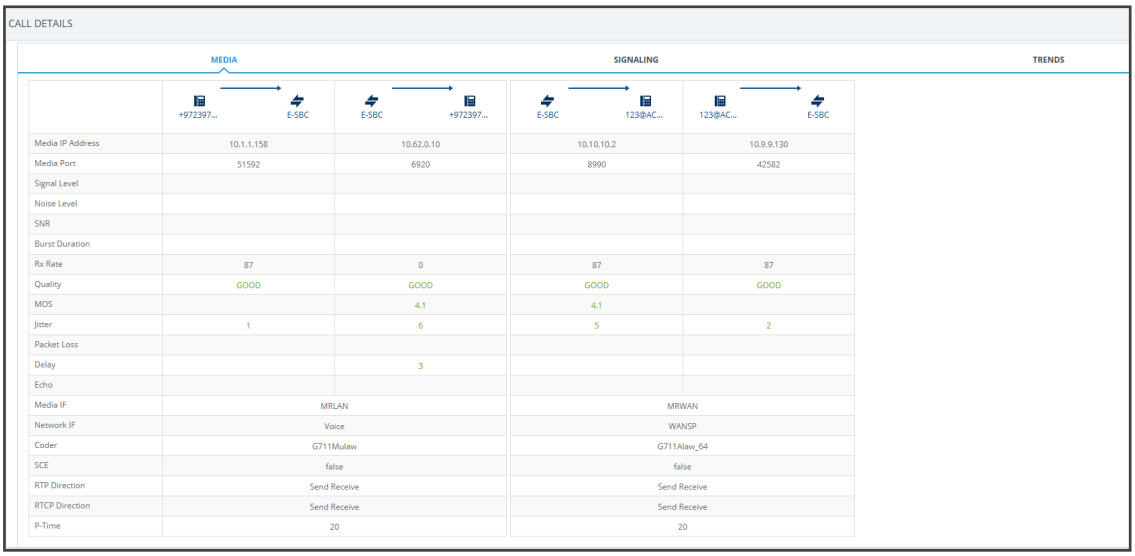
Page Sub-division	Description
(Uppermost) Call summary	Displays parameters and values identical to those displayed in the Calls List page.
(Middle) Graphic illustration	Displays a graphical illustration of voice quality on each leg of the call, on both the caller and callee side. Each leg is: ■ Connected via the VoIP cloud to the device ■ Color-coded to indicate quality (green = good, yellow = fair, red = poor, grey = unknown)

Page Sub-division	Description
	■ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)
(Lowermost) Three tabs	Each opens a page displaying detailed information: ■ Media (see Media below) (includes Quality) ■ Signaling (see Signaling on page 329) ■ Trend (see Trends on page 330) (Only displayed if there is a trend; if there is not a trend, the tab is not displayed) ■ SIP Ladder (see SIP Call Flow on page 331)

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



Use the following table as reference to the parameters displayed under the Media tab.

Table 8-5: Media Parameters

Parameter	Description
Media IP Address	■ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ■ The IP address of the destination host / media network.

Parameter	Description
Media Port	■ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ■ Port of the destination host / media network.
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.
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

Parameter	Description
	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: **SIMcmxLAN (n)**, where **n** 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).
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.

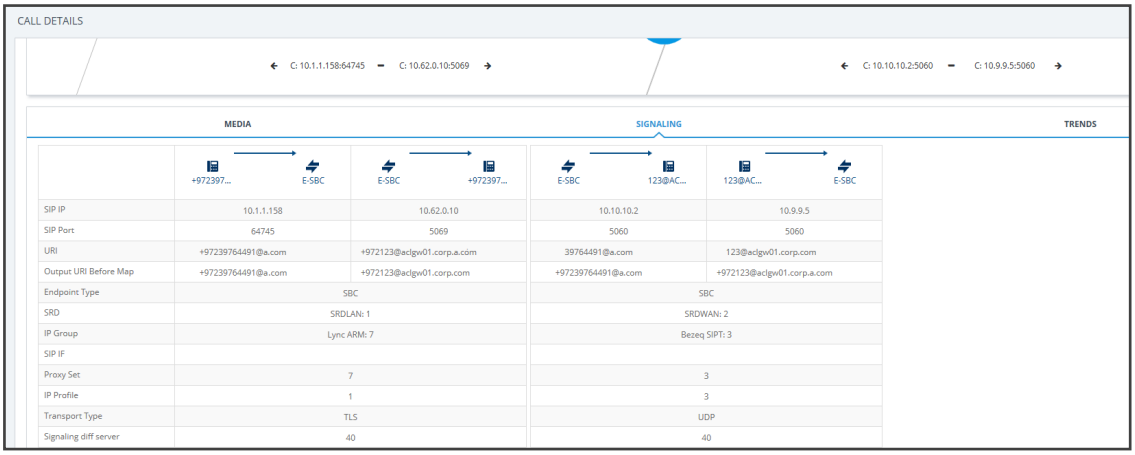
1. Local QoE values of MOS, Jitter, Packet loss, Delay and MOS are calculated by the SBC based on RTP packets it receives from the 'remote peer'
2. The SBC reports this information to the OVOC using an XML-based, proprietary protocol
3. The OVOC displays the information it receives (indicated by **1** in the preceding figure)
4. 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)
5. The SBC forwards QoE information (if received) from the 'remote peer' to the OVOC, as described in point 2 above
6. The OVOC displays the information it receives (indicated by **2** in the preceding figure) (from 'SBC' to 'remote peer')
7. 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



Use the following table as reference to the parameters displayed under the Signaling tab.

Table 8-6: Signaling Parameters

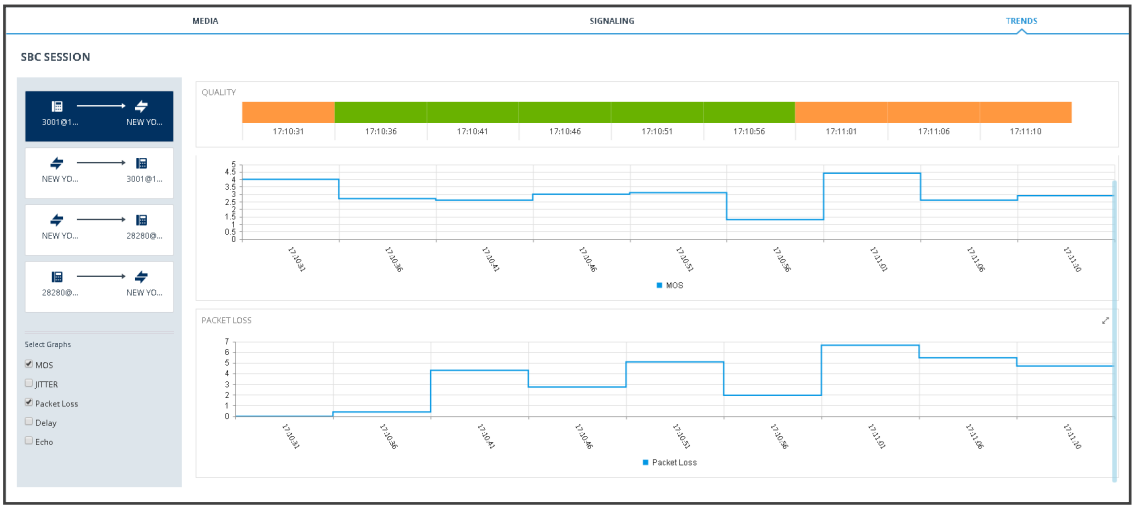
Parameter	Description
SIP IP	The call's caller/callee (source/destination) IP address.
SIP Port	The port number used for the SIP call.
URI	The URI (Uniform Resource Identifier) of the caller/callee (source/destination). The SIP URI is the user's SIP phone number (after manipulation, if any). The SIP 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: **someSRD (n)**, where **n** following the displayed name is the number indicating the SRD's index used to facilitate network configuration.

Parameter	Description
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.
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.

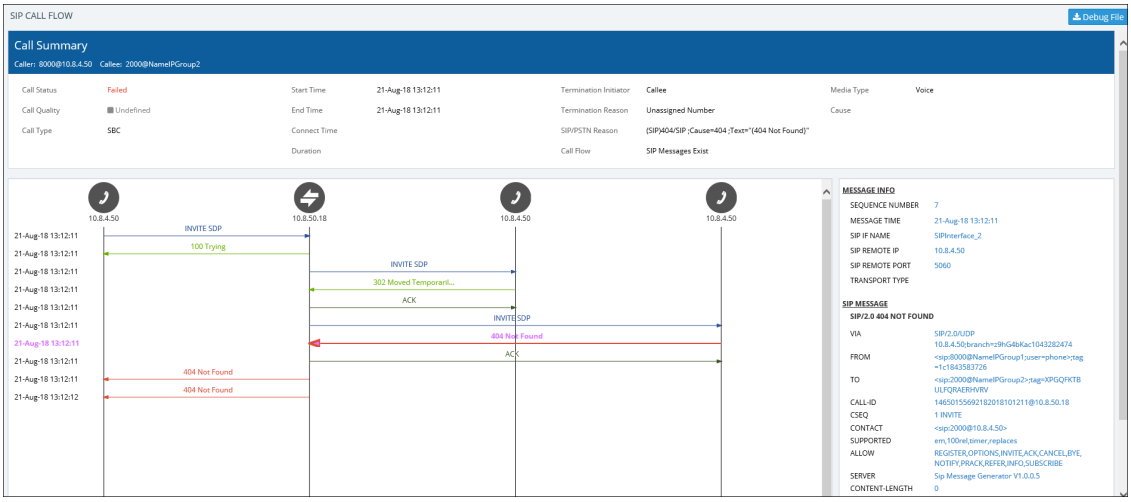
➢ **To compare one voice quality metric with another across different legs:**

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

Color	Error Response
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

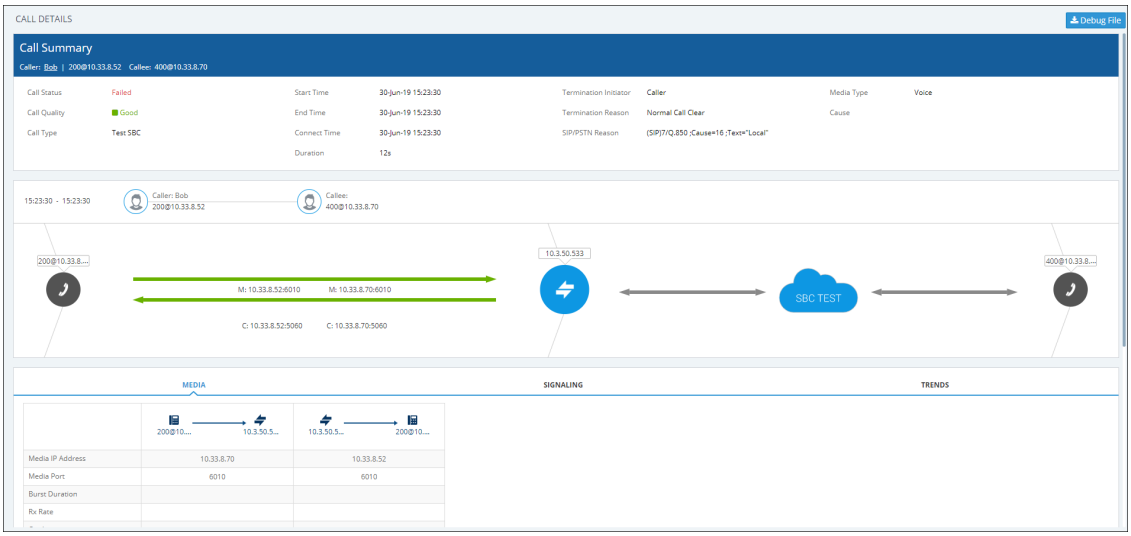
Table 8-8: SIP Message Color Codes

Color	SIP Message
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 320), 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	**Successful** or **Failed**
Call Quality	**Good** | **Fair** | **Poor** 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

Page Section	Description	
	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 *User's Manual* for more information about Termination Reason.	
SIP PSTN Reason	The reason why the call was terminated. See the device's *User's Manual* 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 OVOC 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

Page Section	Description	
		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	■ Indicates the time the call started and ended ■ Visualizes a caller in a call with a callee, including full names and email addresses ■ Displays each leg of the call, on both caller and callee side. ■ Each leg is: ✔ Connected to a device ✔ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✔ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)	
(Lowermost) Two tabs	Each opens a page displaying detailed information: ■ Media (see Media on page 356) ■ Signaling (see Signaling on page 329)	

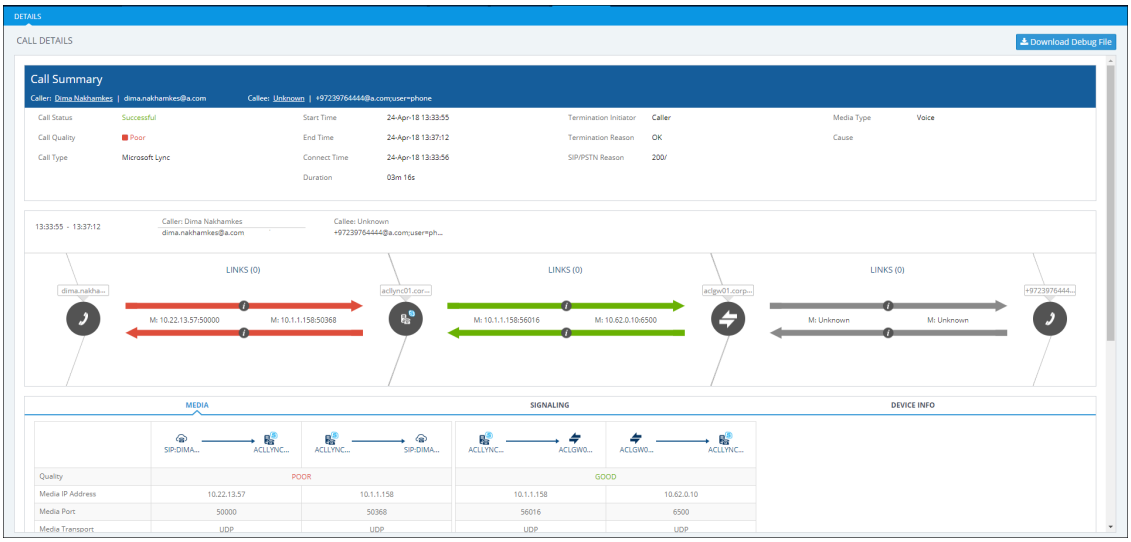
Call Details Page – Debug File Button

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	**Successful** or **Failed**
Call Quality	**Good** | **Fair** | **Poor** 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	The reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason.

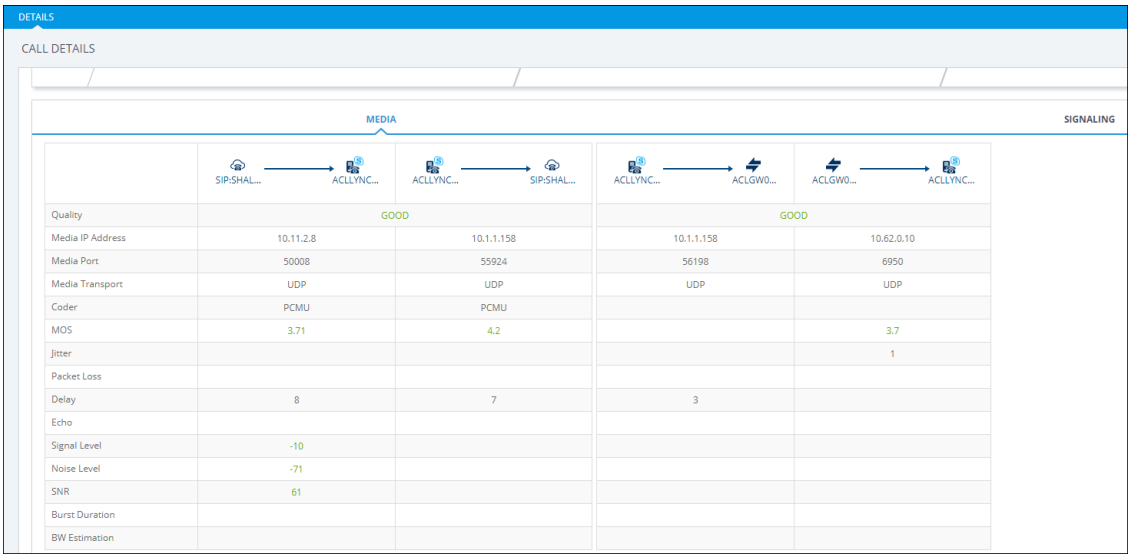
Page Section	Description	
	Some Skype for Business Termination Reasons are: ■ OK. Indicates the request was successful. ■ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed. ■ No Notification ■ Multiple Choices ■ Moved Permanently ■ Moved Temporarily ■ Use Proxy ■ Alternative Service	
SIP PSTN Reason	The reason why the call was terminated. See the device's *User's Manual* for more information about Termination 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 OVOC to voice calls made over a VoIP network

Page Section	Description	
		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	■ Indicates the time the call started and ended ■ Visualizes a caller in a call with a callee, including full names and email addresses ■ Displays each leg of the call, on both caller and callee side. ■ Each leg is: ✔ Connected to a device ✔ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✔ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)	
(Lowermost) Two tabs	Each opens a page displaying detailed information: ■ Media (see Media below) ■ Signaling (see Signaling on page 329)	

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



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: **Good** | **Fair** | **Poor**
Media IP Address	■ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ■ The IP address of the destination host / media network.
Media Port	■ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ■ Port of the destination host / media network.
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	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

Parameter	Description
	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.
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



Use the following table as reference to the parameters displayed under the Signaling tab.

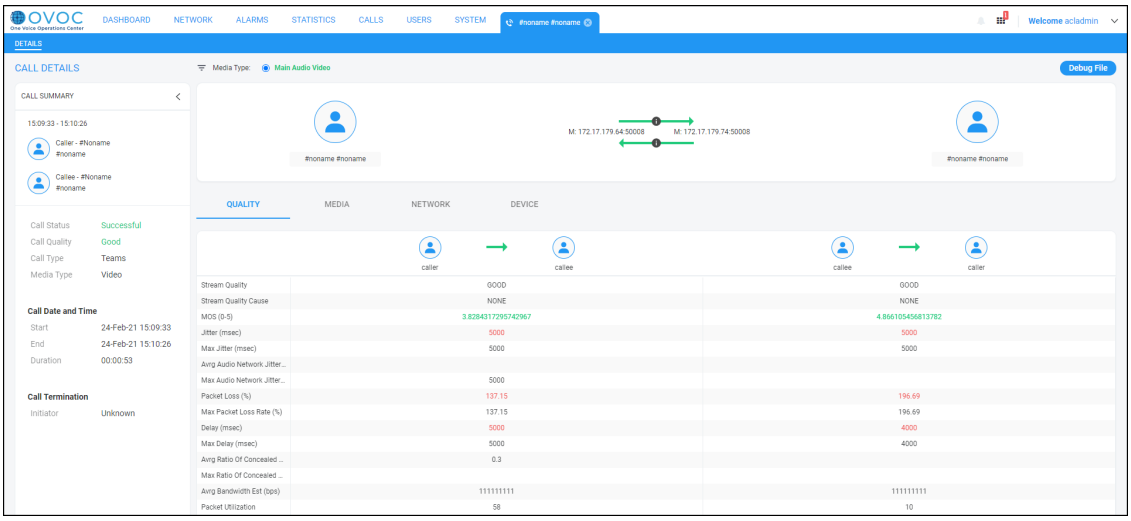
Table 8-12: Signaling Parameters

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 Microsoft Teams

The following figure shows the details of a call made over Microsoft Teams. 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 - Microsoft Teams



If there's an issue of poor quality with a call over Microsoft Teams, 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. Use this table as reference:

Table 8-13: Call Details - Microsoft Teams

Page Section	Description	
Call Summary (Top Left)	Indicates the caller's full name and email address and callee's full name and email address.	
Call Status	**Successful** or **Failed**	
Call Quality	**Good** | **Fair** | **Poor** voice quality	
Call Type	Teams	
Media Type	Audio, Video, Video Based Screen Sharing, Data	
Start	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.	
End	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Duration	The duration of the call, in seconds.	
Call Termination	See Microsoft's documentation for more information.	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay

Page Section	Description	
		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.
	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 OVOC 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
(Top) Graphic illustration	■ Indicates the time the call started and ended ■ Visualizes a caller in a call with a callee, including full names and email addresses ■ Displays each leg of the call, on both caller and callee side. ■ Each leg is: ✔ Connected to a device ✔ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, gray = unknown) ✔ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)	

Page Section	Description
(Lowermost) Three tabs	Each tab opens a page displaying detailed information: ■ Quality (see Quality below) ■ Media (Media tab on page 347) ■ Network (see Network on page 349) ■ Device (see Device on page 352)

Microsoft Graph API currently does not report PSTN steams. Refer instead to SBC QoE reports for PSTN streams.

Quality

Click the **Quality** tab to display information about the media stream between two endpoints in a call. Use the following table as reference to the parameters displayed.

Table 8-14: Quality Parameters

Parameter	Description
Stream Quality	The quality of the media stream. Poor, Fair or Good.
Stream Quality Cause	Defines the quality of calls made using Microsoft Teams services. Streams are classified as Good, Poor, or Unclassified based on the values of the available key quality metrics. The metrics and conditions used to classify stream are shown in https://docs.microsoft.com/en-us/microsoftteams/stream-classification-in-call-quality-dashboard. For information about "Poor Due To" dimensions that can be used to understand which metric is responsible for a Poor classification, see https://docs.microsoft.com/en-us/microsoftteams/dimensions-and-measures-available-in-call-quality-dashboard.
MOS (0-5)	Average Network Mean Opinion Score degradation for stream. Represents how much the network loss and jitter has impacted the quality of received audio.
Jitter	Average jitter for the stream computed as specified in RFC 3550, denoted in ISO 8601 format. For example, 1 second is denoted as 'PT1S', where 'P' is the duration designator, 'T' is the time designator, and 'S' is the second designator.
Max Jitter	Maximum of network jitter computed over 20 second windows during the session.

Parameter	Description
Average Audio Network Jitter	Average jitter for the stream computed as specified in RFC 3550, denoted in ISO 8601 format. For example, 1 second is denoted as 'PT1S', where 'P' is the duration designator, 'T' is the time designator, and 'S' is the second designator.
Max Audio Network Jitter	Maximum of audio network jitter computed over each of the 20 second windows during the session, denoted in ISO 8601 format. For example, 1 second is denoted as 'PT1S', where 'P' is the duration designator, 'T' is the time designator, and 'S' is the second designator.
Packet Loss (%)	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Average packet loss rate for stream.
Maximum Packet Loss Rate	Maximum packet loss rate for stream. Values grouped by range. 0.1 indicates 10% packet loss. Example value: 023: [0.09 - 0.1] If the value is blank, possible reasons are (1) No packet loss data was reported by the endpoint receiving the stream (2) Packet utilization for a given stream is less than 100 packets.
Delay (msec)	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.
Max Delay (msec)	Maximum network propagation round-trip time computed as specified in RFC 3550, denoted in ISO 8601 format. For example, 1 second is denoted as 'PT1S', where 'P' is the duration designator, 'T' is the time designator, and 'S' is the second designator.
Average Ratio of Concealed Samples	Ratio of the number of audio frames with samples generated by packet loss concealment to the total number of audio frames. Values grouped by range. 0.1 indicates 10% of frames contained concealed samples. Example value: 015: [0.01 - 0.02) If the value is blank, possible reasons are (1) the value was not reported by the receiver of the stream (2) the stream was not an audio stream.
Max Ratio of Concealed Samples	The maximum seen number of audio frames with samples generated by packet loss concealment to the total number of audio frames. Values grouped by range. 0.1 indicates 10% of frames contained concealed samples. Example value: 015: [0.01 - 0.02)

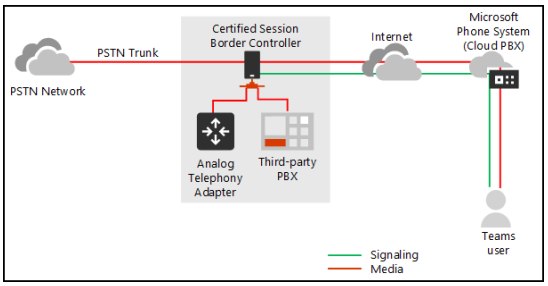
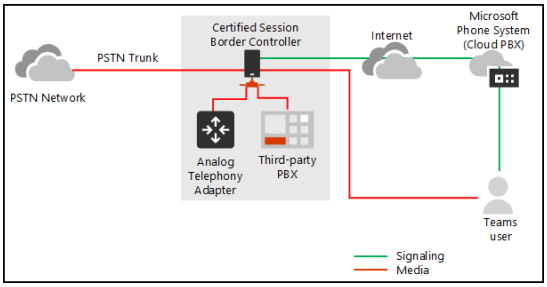
Parameter	Description
Average Bandwidth Estimation (bps)	Average estimated bandwidth available between first and second endpoint in bits per second. Example value: 026: [260000 - 270000] If the value is blank, possible reasons are (1) Transport type was not reported (2) The media path was not established.
Packet Utilization	Number of Real-Time Transport Protocol (RTP) packets sent in the session.

Media tab

Click the **Media** tab to display information about the media stream between two endpoints in a call. Use the following table as reference to the parameters displayed.

Table 8-15: Media Parameters

Parameter	Description
Stream ID	Unique identifier for the stream.
Start Date Time	UTC time when the stream started. The DateTimeOffset type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 would look like this: '2014-01-01T00:00:00Z'.
End Date Time	UTC time when the stream ended. The DateTimeOffset type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 would look like this: '2014-01-01T00:00:00Z'
Was Media Bypassed	Set to 'True' or 'False'. Enables shortening the path of media traffic and reducing the number of hops in transit for better performance. Media is kept between the SBC and the client instead of sending it via the Microsoft Phone System. To configure media bypass, the SBC and the client must be in the same location or network. Without media bypass, when a client makes or receives a call, both signaling and media

Parameter	Description
	flow between the SBC, the Microsoft Phone System, and the Teams client, as shown in the following diagram:  But let's assume that a user is in the same building or network as the SBC. For example, assume a user who is in a building in Frankfurt makes a call to a PSTN user: ■ *Without media bypass*, media will flow via either Amsterdam or Dublin (where Microsoft datacenters are deployed) and back to the SBC in Frankfurt. The datacenter in Europe is selected because the SBC is in Europe, and Microsoft uses the datacenter closest to the SBC. While this approach does not affect call quality due to optimization of traffic flow within Microsoft networks in most geographies, the traffic has an unnecessary loop. ■ *With media bypass*, the media is kept directly between the Teams user and the SBC as shown in the following diagram:  Media bypass leverages protocols called Interactive Connectivity Establishment (ICE) on the Teams client and ICE lite on the SBC.

Parameter	Description
	These protocols enable Direct Routing to use the most direct media path for optimal quality. ICE and ICE Lite are WebRTC standards. For detailed information about these protocols, see RFC 5245.

Network

Click the **Network** tab to display information about the network used in the call. Use the following table as reference to the parameters displayed.

Table 8-16: Network Parameters

Parameter	Description
MAC Address	The media access control (MAC) address of the media endpoint's network device.
IP Address	IP address of the media endpoint.
Port	Network port number used by media endpoint.
Relay IP Address	Network port number allocated on the media relay server by the media endpoint.
Relay Port	Network port number allocated on the media relay server by the media endpoint.
Reflexive IP Address	IP address of the media endpoint as seen by the media relay server. This is typically the public internet IP address associated to the endpoint.
Subnet	Subnet used for media stream by the media endpoint.
Delay Event Ratio	Fraction of the call that the media endpoint detected the network delay was significant enough to impact the ability to have real-time two-way communication.
Bandwidth Low Event Ratio	Fraction of the call that the media endpoint detected the available bandwidth or bandwidth policy was low enough to cause poor quality of the audio sent.
Received Quality Event Ratio	Fraction of the call that the media endpoint detected the network was causing poor quality of the audio received.
Sent Quality	IP address of the media endpoint as seen by the media relay server. This

Parameter	Description
Event Ratio	is typically the public internet IP address associated to the endpoint.
DNS Suffix	DNS suffix associated with the network adapter of the media endpoint.
Link Speed (bps)	Link speed in bits per second reported by the network adapter used by the media endpoint.
Connection Type	Type of network used by the media endpoint. Possible values are: unknown, wired, wifi, mobile, tunnel, unknownFutureValue.
Basic Service Set Identifier	The wireless LAN basic service set identifier (BSSID) of an endpoint used to connect to the network.
Wi-Fi Band	Wi-Fi band used as reported by the endpoint. Example value: 5.0 Ghz Possible reasons for blank values: ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Battery Charge (%)	Estimated remaining battery charge in percentage [0-99] reported by the endpoint. Values grouped by range. 0 indicates that the device was plugged in. Example value: 081: [90 - 100) Possible reasons for blank values: ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Channel	Wi-Fi channel used by the endpoint. Example value: 10 Possible reasons for blank values: ■ Wi-Fi was not used ■ The channel was not reported
Wi-Fi Microsoft Driver	Name of the Microsoft Wi-Fi driver used reported by the endpoint. Value may be localized based on the language used by the endpoint. Example value: Microsoft Hosted Network Virtual Adapter Possible reasons for blank values: ■ Wi-Fi wasn't used by the endpoint

Parameter	Description
	■ The driver information was not reported
Wi-Fi Microsoft Driver Version	Version of Microsoft Wi-Fi driver reported by the endpoint. Example value: Microsoft:10.0.14393.0 Possible reasons for blank values: ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported
Wi-Fi Radio Type	Type of Wi-Fi radio used by the endpoint. HRDSSS is equivalent to 802.11b. Example value: 802.11ac Possible reasons for blank values: ■ Wi-Fi wasn't used ■ The driver information was not reported
Wi-Fi Signal Strength (%)	Wi-Fi signal strength in percentage [0-100] reported by the endpoint. Example value: 081: [90 - 100) Possible reasons for blank values: ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Vendor Driver	Vendor and name of WiFi driver reported by the first endpoint. Example value: Contoso Dual Band Wireless-AC Driver. Possible reasons for blank values: ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported
Wi-Fi Vendor Driver Version	Version of Microsoft WiFi driver reported by the first endpoint. Example value: Microsoft:10.0.14393.0 Possible reasons for blank values: ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported

Device

Click the **Device** tab to display information about the device (microphone, speaker, camera, etc.) used in the call. Use the following table as reference to the parameters displayed.

Table 8-17: Device Parameters

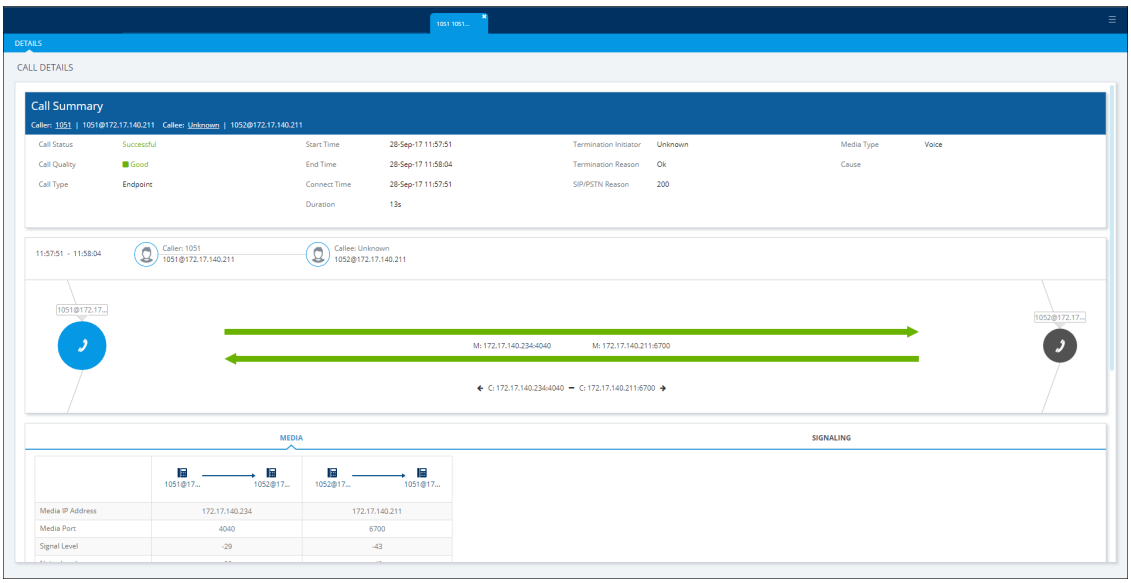
Parameter	Description
Capture Device Driver	Name of the capture device driver used by the endpoint in the form of "manufacturer : version". For: Audio streams = driver used for the microphone Video streams = driver used for the camera Video-based-screen-sharing and app sharing streams = blank Example value: Microsoft: 10.0.14393.0 Possible reasons for blank values: ■ Data was not reported by the endpoint ■ The media path was not established ■ The stream was video-based screen sharing or application sharing
Capture Device Name	Name of the capture device used by the media endpoint.
Capture Not Functioning Event Ratio	Fraction of the call that the media endpoint detected the capture device was not working properly.
CPU Insufficent Event Ratio	Fraction of the call that the media endpoint detected the CPU resources available were insufficient and caused poor quality of the audio sent and received.
Howling Event Count	Number of times during the call that the media endpoint detected howling or screeching audio.
Mic Glitch Rate	Glitches per 5 minute interval for the media endpoint's microphone.
Received Noise Level	Average energy level of received audio for audio classified as mono noise or left channel of stereo noise by the media endpoint.
Received Signal Level	Average energy level of received audio for audio classified as mono speech, or left channel of stereo speech by the media endpoint.
Render Device Driver	Name of the render device driver used by the media endpoint.

Parameter	Description
Render Device Name	Name of the render device used by the media endpoint.
Sent Noise Level	Average energy level of sent audio for audio classified as mono noise or left channel of stereo noise by the media endpoint.
Sent Signal Level	Average energy level of sent audio for audio classified as mono speech, or left channel of stereo speech by the media endpoint.
Speaker Glitch Rate	Glitches per 5 minute internal for the media endpoint's loudspeaker.

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 8-15: Call Details – Over an Endpoint Using SIP Publish



Use the following table as reference.

Table 8-18: 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	**Successful** or **Failed**

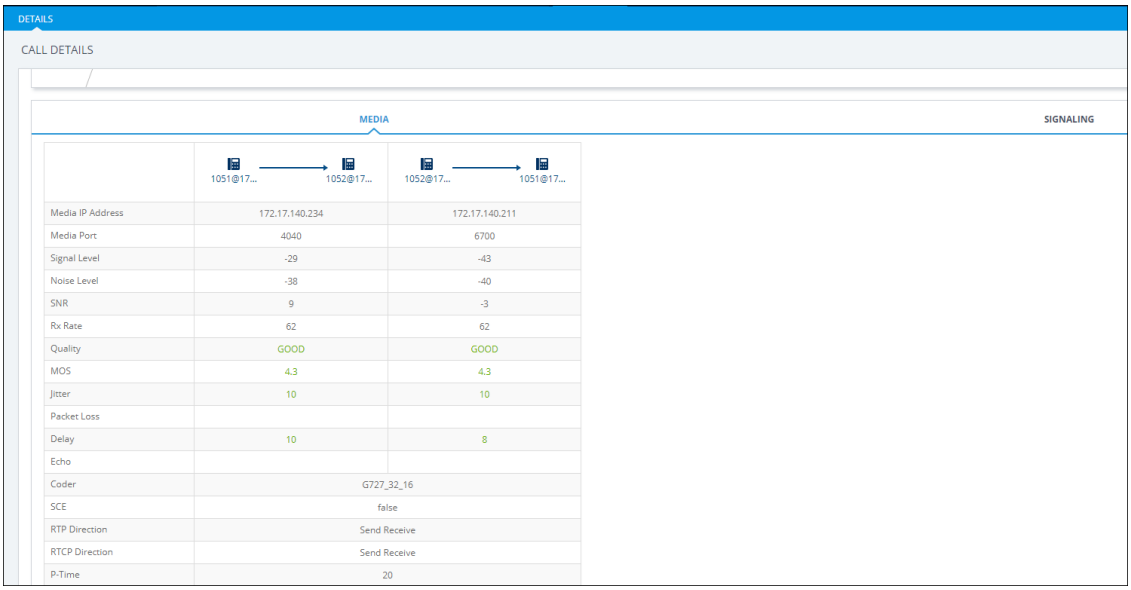
Page Section	Description	
Call Quality	**Good** | **Fair** | **Poor** voice quality	
Call Type	Endpoint	
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.	
End Time	The precise time (hour, minutes and seconds) and 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 *User's Manual* for more information about Termination Reason.	
SIP PSTN Reason	The reason why the call was terminated. See the device's *User's Manual* 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.

Page Section	Description	
	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 OVOC 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	■ Indicates the time the call started and ended ■ Visualizes a caller in a call with a callee, including full names and email addresses ■ Displays each leg of the call, on both caller and callee side. ■ Each leg is: ✔ Connected to a device ✔ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✔ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)	
(Lowermost) Two tabs	Each opens a page displaying detailed information: ■ Media (see Media on the next page) ■ Signaling (see Signaling on page 329)	

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 8-16: Media



Use the following table as reference.

Table 8-19: Media Parameters

Parameter	Description
Media IP Address	■ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ■ The IP address of the destination host / media network.
Media Port	■ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ■ Port of the destination host / media network.
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).

Parameter	Description
	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: 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 (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	RTCP Directional Control. Controlled internally by the device according to

Parameter	Description
Direction	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

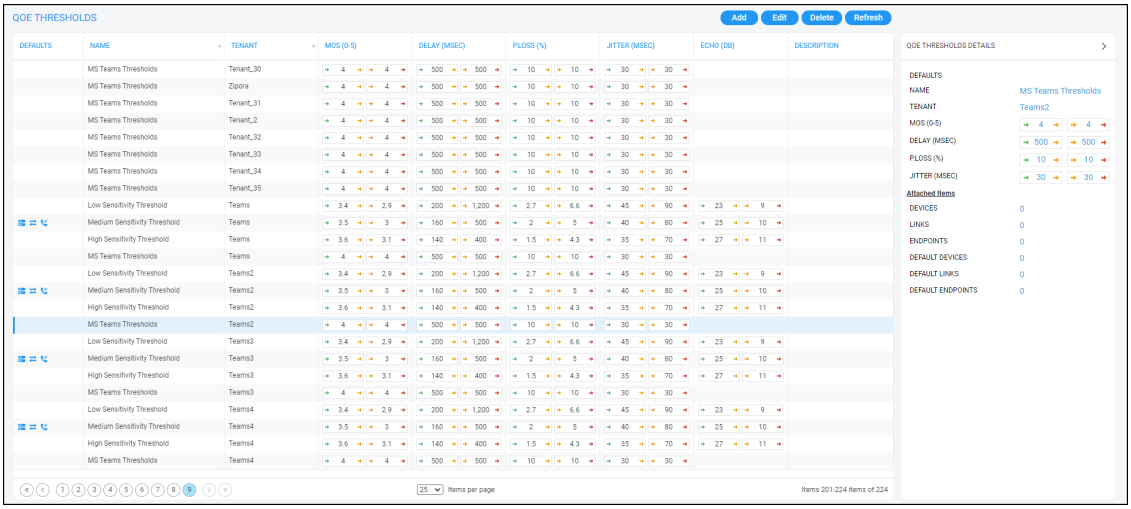
The QoE Thresholds page lets you adding a profile of Quality of Experience threshold values, *per tenant*.

For information about adding a *global* (system) QoE Thresholds template, see QoE Thresholds on page 91.

➢ To view QoE thresholds profiles:

- Open the QoE Thresholds page (**Calls** > **QoE Thresholds**).

Figure 8-17: QoE Thresholds Profiles



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 362)
- edit or delete an existing profile (see Editing a QoE Thresholds Profile per Tenant on page 365 and Deleting a QoE Thresholds Profile per Tenant on page 365)

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 8-20: 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
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.

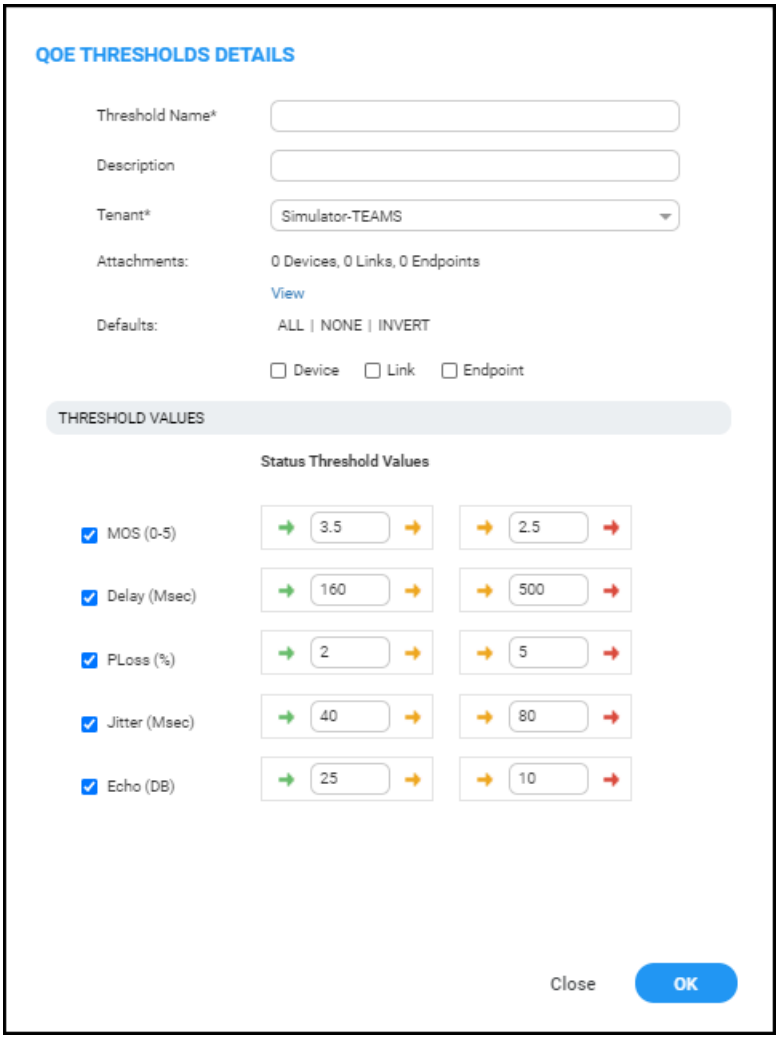
Adding a QoE Thresholds Profile per Tenant

You can add a QoE Thresholds profile.

➢ To add a QoE thresholds profile:

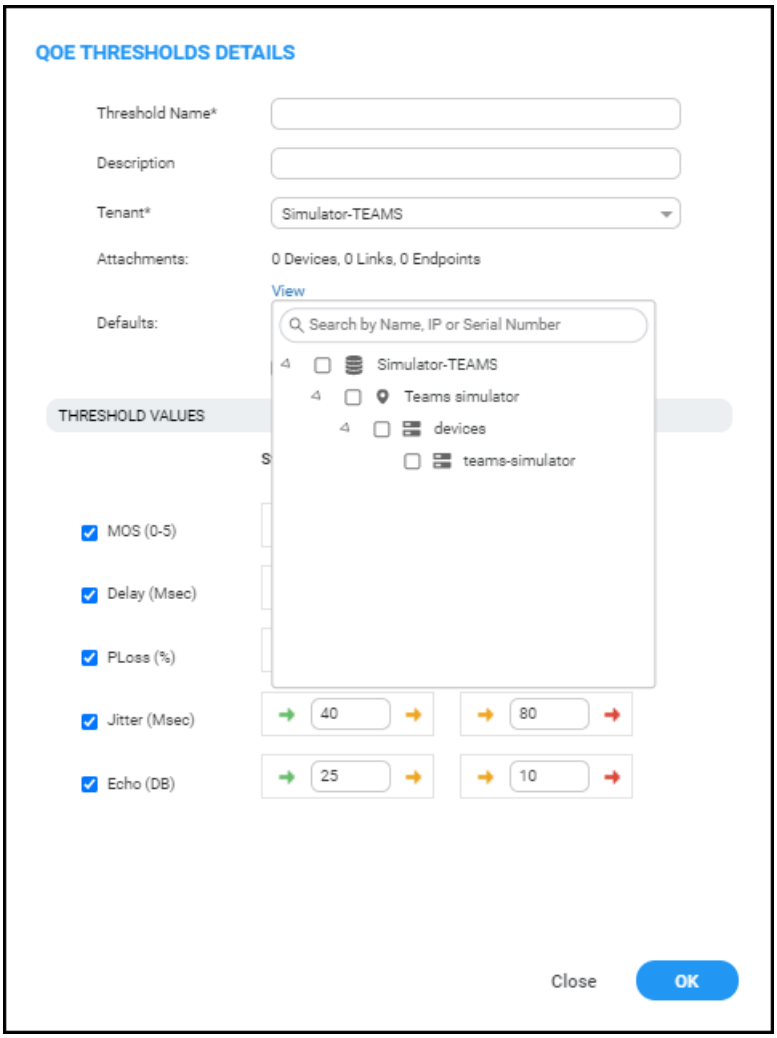
1. Open the QoE Thresholds page (**Calls** > **QoE Thresholds**).
2. Click **Add**.

Figure 8-18: QoE Thresholds Details



3. Provide an intuitive name for the profile. Use the names of the four predefined QoE profiles displayed in the QoE Thresholds screen 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.

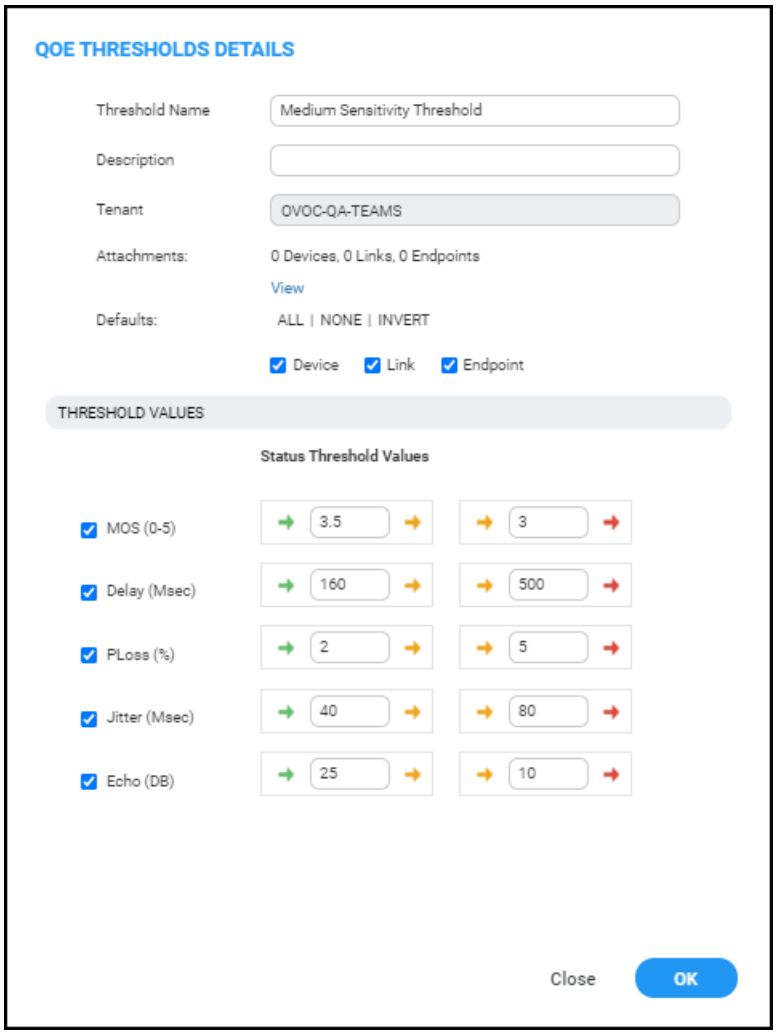
Figure 8-19: Attachments



7. Expand the tenant to navigate to and select the entities to which to attach this QoE thresholds profile (devices, links or endpoints).
8. 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.

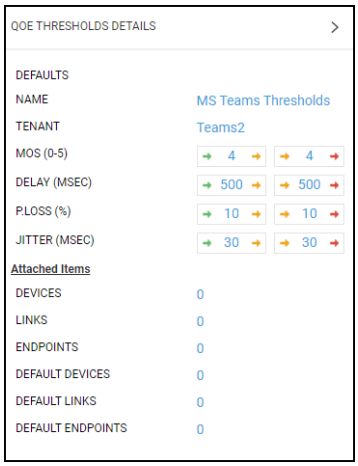
9. Specify which voice quality metrics to include in or exclude from the profile. You can exclude, for example, the metrics of 'MOS', 'Delay' and 'Echo', but include 'Packet Loss' and 'Jitter'. To *exclude* a voice quality metric, clear its check box. By default, all voice quality metrics are included in the profile. 'Echo' does not apply to MS Teams Thresholds.
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 8-20: QoE Thresholds Settings - Medium Sensitivity Threshold



11. Click **OK**; the profile is displayed in the QoE Thresholds page.
12. In the page, select the profile; the QoE Threshold Details pane on the right side of the page is displayed.

Figure 8-21: QoE Thresholds Details



Shown in the preceding figure, the QoE Thresholds Details pane displays under **Attached Items** the number of devices / links / endpoints to which the selected profile is attached, if any.

Also in the QoE Threshold Details pane:

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 362 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

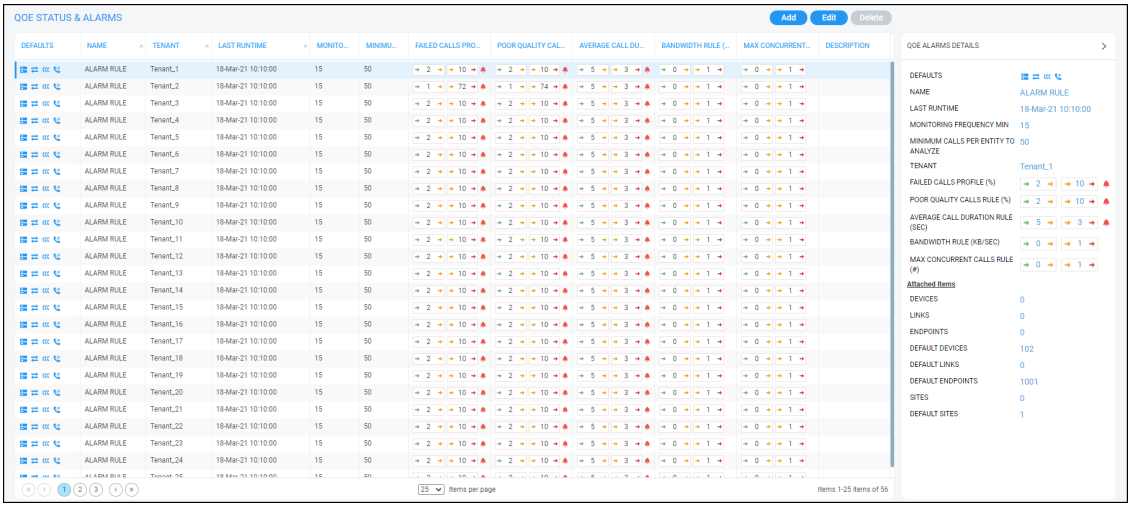
The QoE Status & Alarms page lets you manage QoE statuses and alarms *per tenant*.

For information about managing *global* (*system-wide*) QoE statuses and alarms, see QoE Status and Alarms on page 93.

➢ To view QoE statuses and alarms per tenant:

- Open the QoE Status & Alarms page (**Calls** > **QoE Status & Alarms**).

Figure 8-22: QoE Status & Alarms



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 93 for a detailed description.

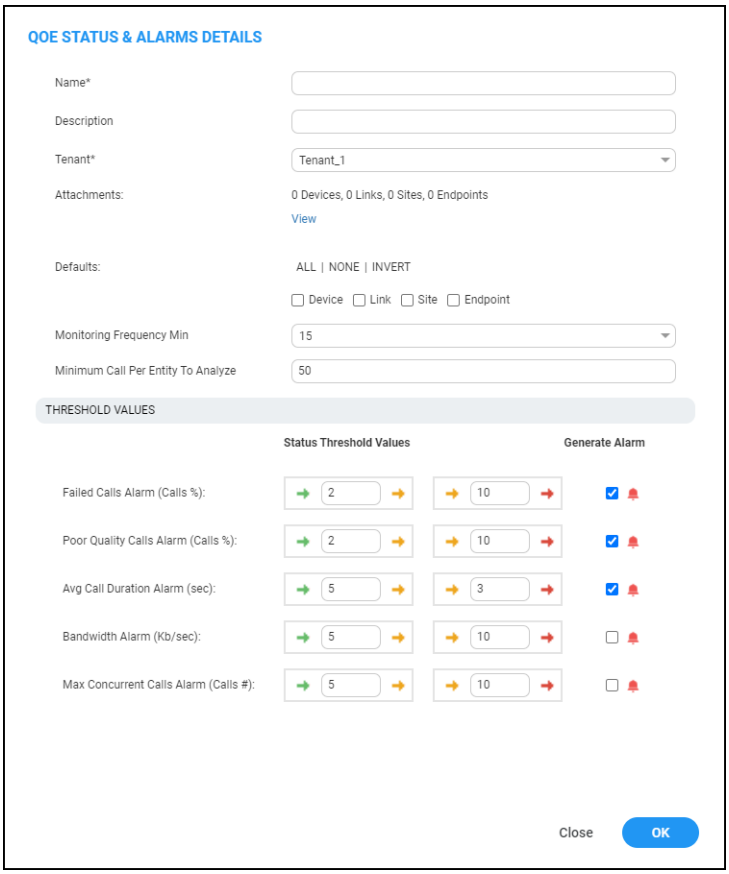
Adding a QoE Alarm Rule per Tenant

You can add a new rule for a QoE alarm per tenant.

➢ To add a new QoE alarm rule per tenant:

1. Open the QoE Status & Alarms Details screen (**Calls** > **QoE Status & Alarms** and then click **Add**).

Figure 8-23: QoE Status & Alarms Details



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

Table 8-21: QoE Status & Alarms Details

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 **View** 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 **Device**, **Link**, **Site** and/or **Endpoint** monitoring filter. ■ If you select **Link**, the links selection pop-up opens; select the links to monitor (the default is **All Selected**). ■ If you select **Device**, the device selection pop-up opens; select the devices to monitor (the default is **All Selected**).
Monitoring Frequency (min)	Determines how frequently the OVOC automatically performs data analysis. Defines every 15 (default), 30 or 60 minutes.

Parameter	Description
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 **Generate Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **5**% of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: **3**% of calls (default); if this threshold is exceeded, the alarm is triggered.
Poor Quality Calls Alarm	Select the **Poor Quality Calls Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **10**% of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: **8**% of calls (default); if this threshold is exceeded, the alarm is triggered.
Avg Call Duration Alarm	Select the **Avg Call Duration Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **5** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered. Major Threshold: **10** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered.
Bandwidth Alarm	Select the **Bandwidth Alarm** 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 **0** Kbps and a maximum of **1000000** Kbps), an alarm of Major severity is triggered. Critical Threshold: if the bandwidth falls below or exceeds the value you configure (minimum of **0** Kbps and a maximum of **1000000** Kbps), an alarm of Critical severity is triggered. ■ You must configure a *higher* value for the *Critical* Threshold than for the Major Threshold. ■ You can configure a minimum of **0** Kbps and a maximum of **1000000** Kbps for either the Critical or the Major Threshold, so long as the value you configure for the *Critical* Threshold is higher than the value you configure for the Major Threshold.
Max Concurrent	Select the **Max Concurrent Calls Alarm** option to active the alarm.

Parameter	Description
Calls Alarm	Clear the option to deactivate the alarm. Major Threshold: if the number of concurrent calls falls below, or exceeds, the value you configure (minimum of **0** and a maximum of **100000**), 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 **0** and a maximum of **100000**), an alarm of Critical severity is triggered. ■ You must configure a *higher* value for the *Critical* Threshold than for the Major Threshold. ■ You can configure a minimum of **0** and a maximum of **1000000** for either the Critical or the Major Threshold, so long as the value you configure for the *Critical* Threshold is higher than the value you configure for the Major Threshold.

3. 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 preceding table 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.

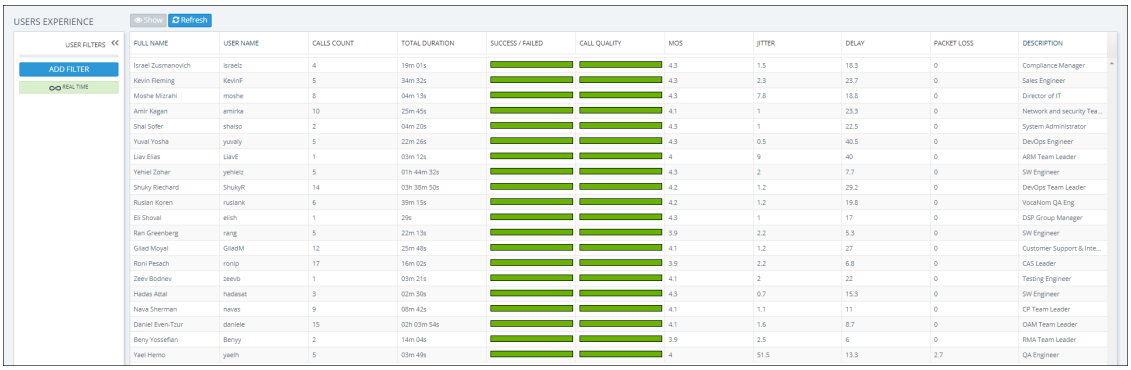
> 'End users' refers to an enterprise's employees. By contrast, 'operators' refers to administrators managing the enterprise's network using the OVOC.

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 375 and Assessing a Specific End User's Experience on page 377 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



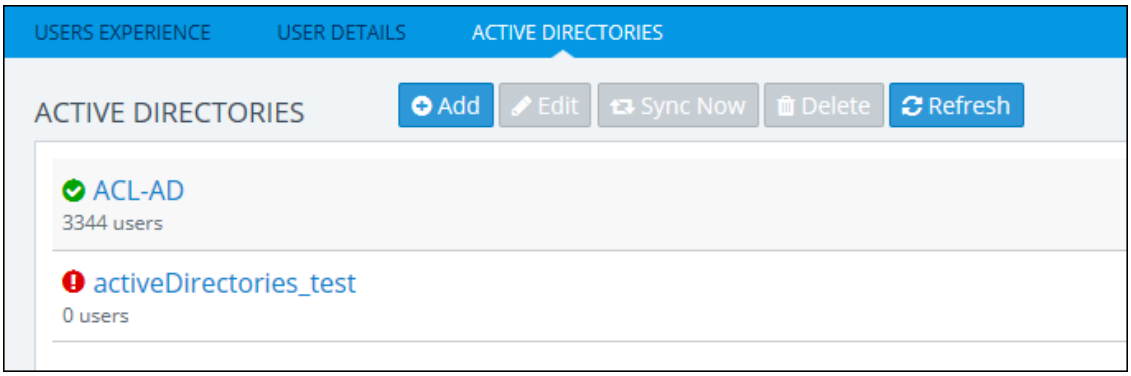
Adding an Active Directory to the OVOC

You can add an Active Directory to the OVOC.

➢ To add an Active Directory to the OVOC:

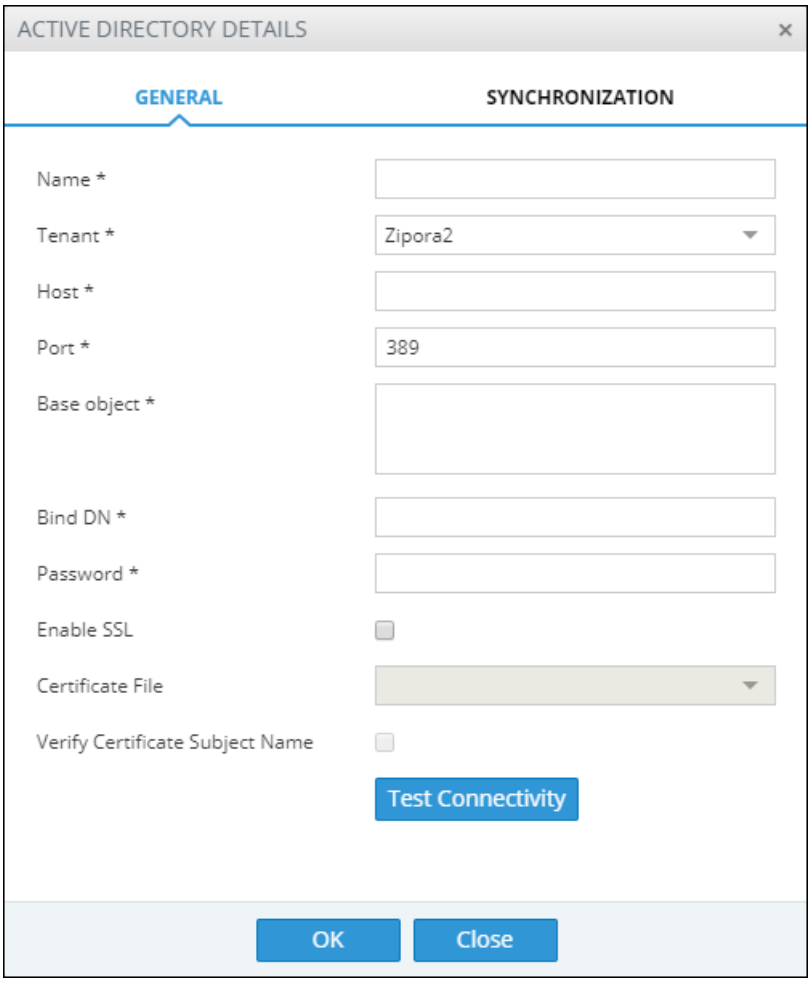
1. Open the Active Directory page (**Users** > **Active Directories**).

Figure 9-2: Active Directories



2. Click **Add**.

Figure 9-3: Active Directory Settings



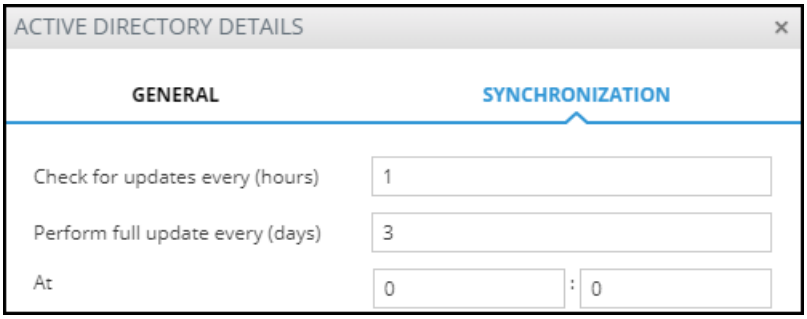
3. Configure the General AD settings using the following table as reference.

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 Adding a Tenant on page 113.
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

Setting	Description
	(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.
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 Adding Configuration Files to the OVOC's Software Manager on page 98.
Test connectivity (NA)	Click to test synchronization of the OVOC and the Active Directory databases. You can alternatively click **Sync Now** 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.



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.
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.

6. Click **OK**.

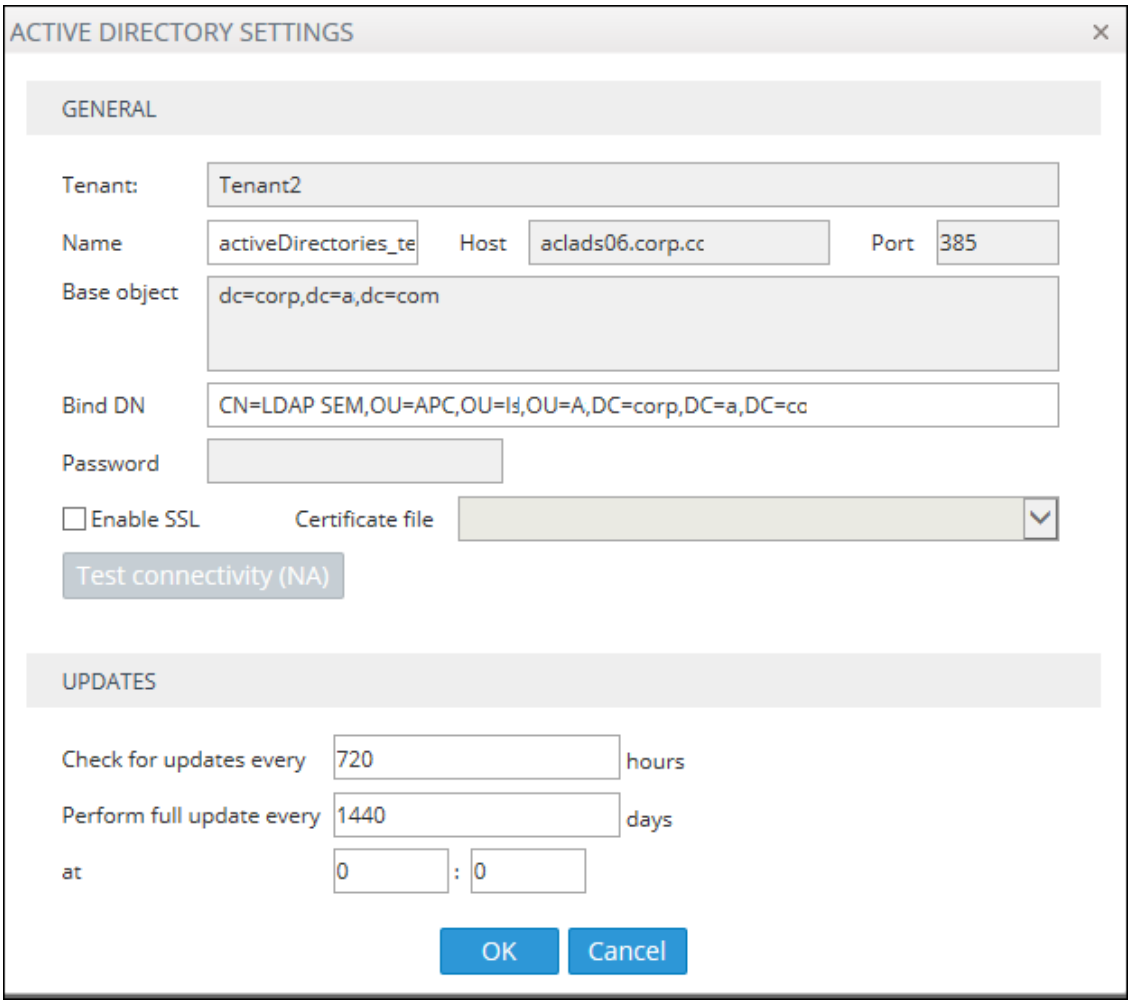
Editing an Active Directory

You can edit an Active Directory after adding one.

➢ **To edit an Active Directory:**

1. Open the Active Directory page (**Users** > **Active Directories**).
2. Select the Active Directory to edit and click now-enabled **Edit** button.

Figure 9-4: Active Directory Settings



3. Edit the parameters using the table Adding an Active Directory to the OVOC on page 370 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.

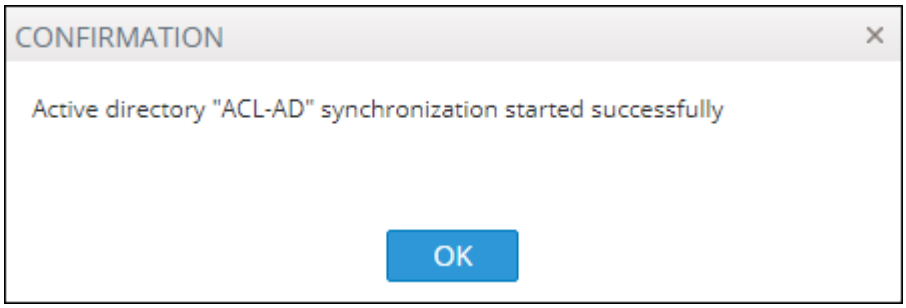
➢ To synchronize an AD with the AD server:

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**.

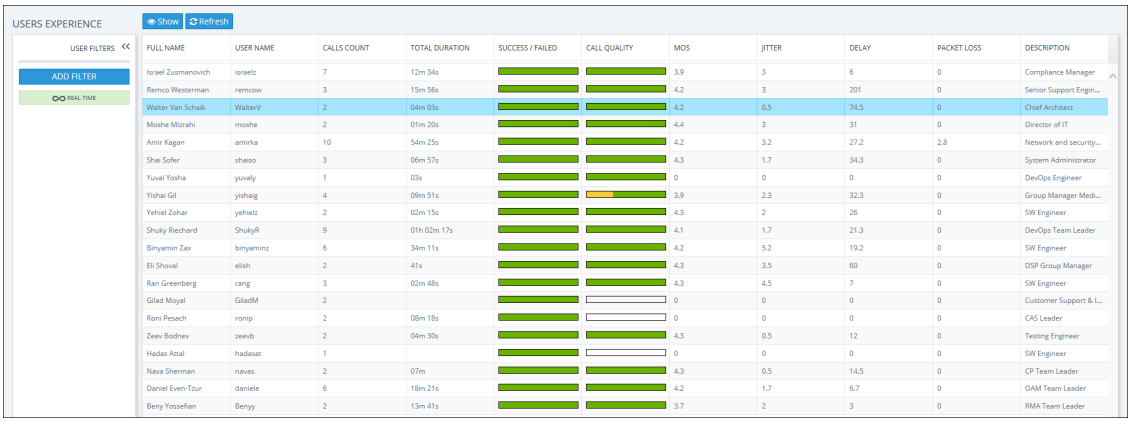
Assessing Overall End Users Experience

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:

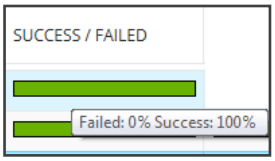
1. Open the Users Experience page (**Users** > **Users Experience**).

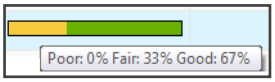
Figure 9-6: Users Experience



2. [Optional] Filter the page to present only information you require. You can filter by Time Range (see Filtering to Access Specific Information on page 212) or by Users (see Filtering the User Details Page on page 380).
3. 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).

Column	Description
	
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 OVOC to voice calls made over a VoIP network at the conclusion of the testing.
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.

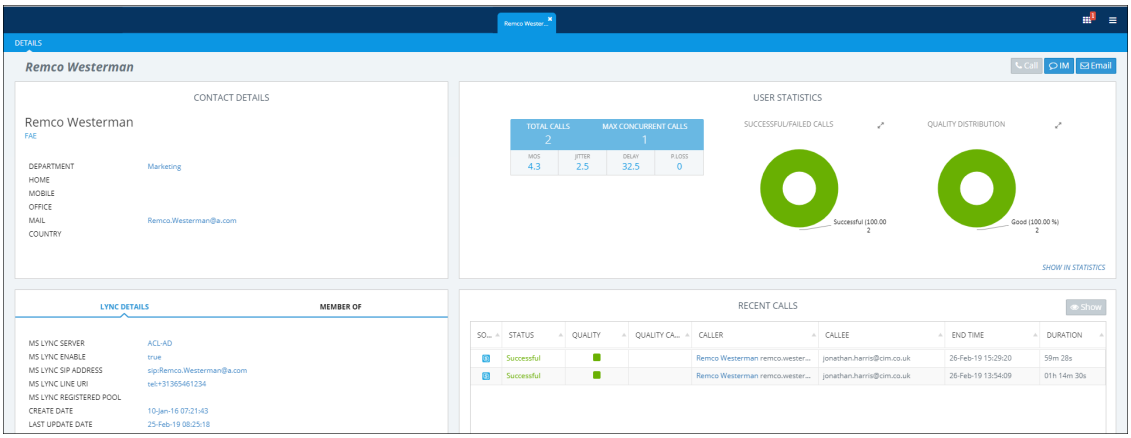
Assessing a Specific End User's Experience

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

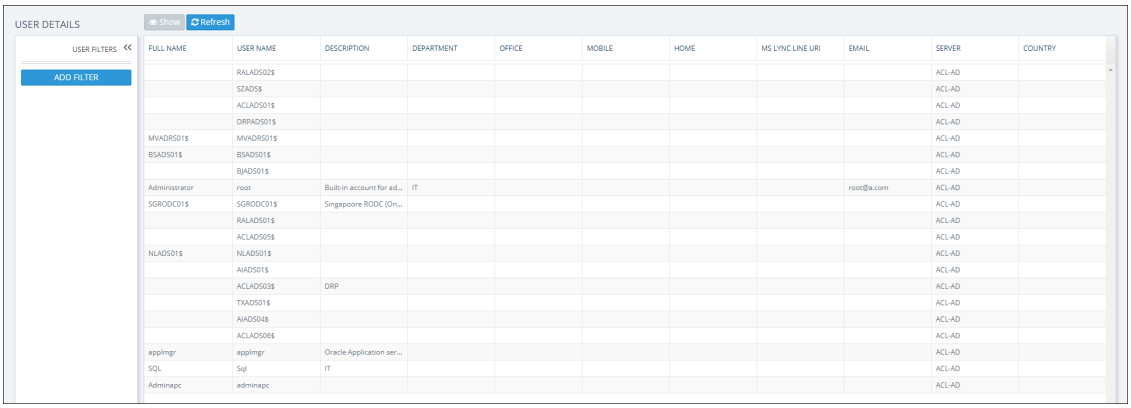
Only OVOC operators with 'Administrator' security level can perform local management of end users.

Usernames 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

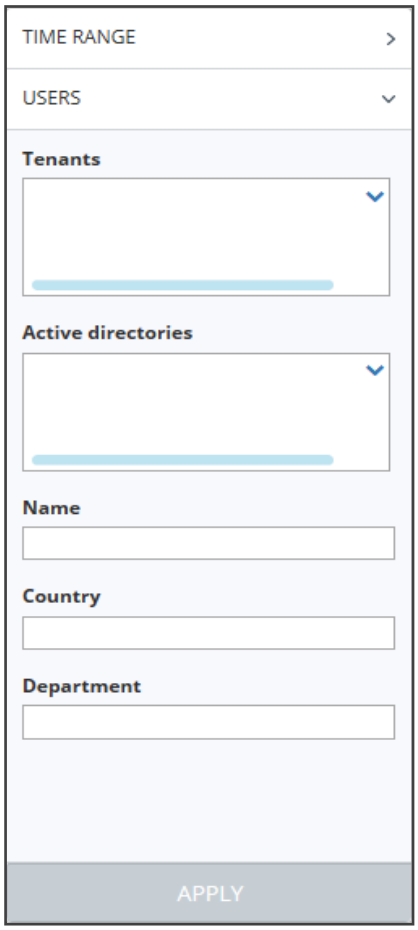


2. Optionally, use filters for quick access to specific users.
3. Obtain contact information about end users from under the columns in the table: Full Name, User Name, Description, Department, Office, Mobile, Home, MS Skype for Business Line URI, Email, Server, Country.

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



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

Filter	Description
	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 Managing Reports

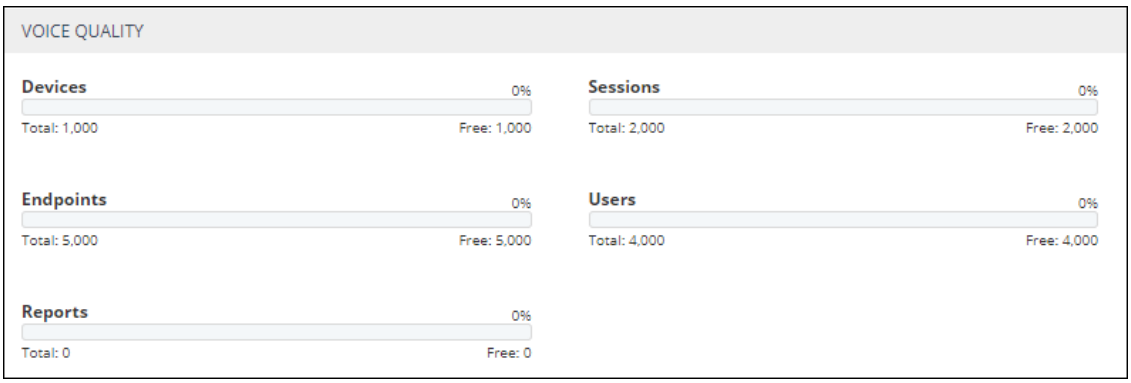
The OVOC allows administrators to produce reports that can be used to distribute information about IP telephony performance and quality of experience across the enterprise and to external authorities, for accurate diagnosis, correction of issues and optimization.

The Reports page lets operators manage reports. Before managing reports, make sure your license covers them.

➢ To make sure your license covers reports:

1. Open the License Configuration page (**System** > **Administration** > **License** > **Configuration**) and under 'Voice Quality', locate 'Reports'.

Figure 10-1: License Configuration - Reports



2. Make sure you have reports capability including system and tenant allocations. Contact your AudioCodes representative if you don't.

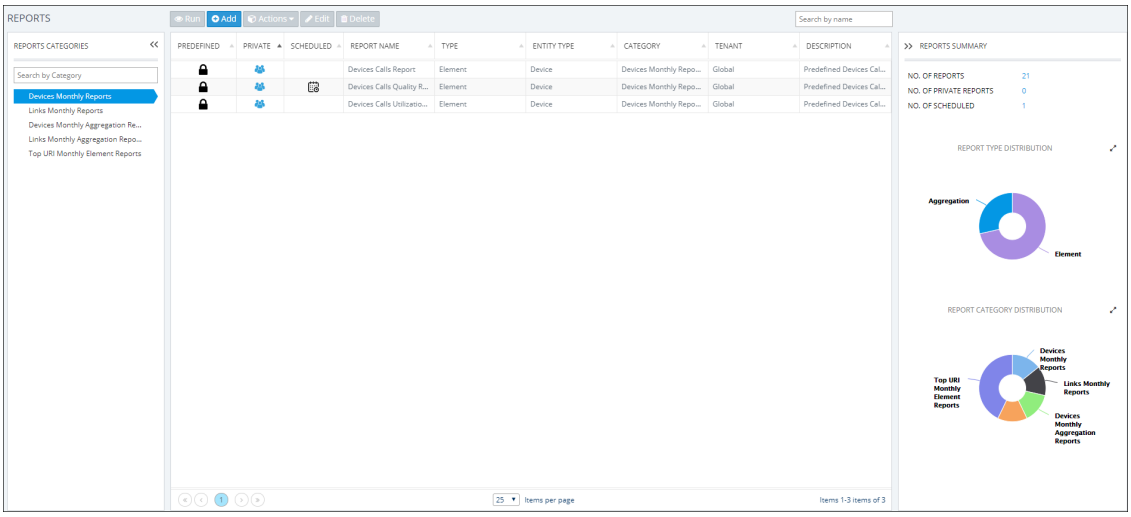
In the Reports page, you can

- manage reports - see below
- define a report - see Defining a Report on page 385
- view a defined report - see Viewing a Defined Report on page 399
- edit a report - see Editing a Report on page 400
- run, export, import, duplicate or delete a report - see Performing Actions on Reports on page 401

➢ To manage reports:

1. Open the Reports page (**Statistics** > **Reports** > **Reports**).

Figure 10-2: Reports page



2. Use the table as reference.

Table 10-1: Reports page

Column	Description
Search by Category	Allows filtering reports displayed in the Reports page according to category. Default: 'All'.
Reports Categories	Select a category according to which reports in the page will be filtered. Following are the default categories: ■ Devices Monthly Reports ■ Links Monthly Reports ■ Devices Monthly Aggregation Reports ■ Links Monthly Aggregation Reports ■ Top URI Monthly Element Reports Any network administrator (Administrator and Operator) who can define a new report can add a new category; the category is made automatically after the report is defined.
Predefined	🔒 indicates a predefined report that is integrated with the OVOC and which cannot be deleted or edited. The column can be sorted. Operators of every security level can view a predefined report but none can edit. 🔓 indicates an administrator-defined report.
Private / Public	👥 indicates that the report is a *public* report; anyone can view, edit and delete it 👤 and 👤 indicate that the report is a *private* report

Column	Description
	indicates that *I am the owner* of this private report and that I can view, edit and delete it; the operator defined as Administrator can view and delete this report (but not edit it). indicates that *I am not the owner* of this private report; the icon is available only for the operator defined as Administrator; only the operator defined as Administrator can view and delete this report. The column can be sorted according to these classifications.
Scheduled	indicates a report that is currently scheduled. The column can be sorted.
Report name	Indicates the name of the report, for example, Devices Calls Report. The column can be sorted. By default, the Reports page is sorted in alphabetical order according to the report names in the 'Report name' column.
Type	Indicates the type of report. Either: ■ **Element [Entity] Statistics**. Default. See 'Element (Entity) Statistics' Report Type on page 403 for more information.'Aggregated Statistics Trends' Report Type on page 404 ■ **Aggregated Statistics Trends**. See 'Aggregated Statistics Trends' Report Type on page 404 for more information. ■ **Trends Statistics Comparison**. See Selecting a Metric on page 392 for more information.
Entity Type	Indicates the type of entity on which the report was created, for example, Device.
Category	Indicates the category according to which the report is categorized, for example, Devices Monthly Reports. The column can be sorted.
Tenant	Indicates the report's scope. The column can be sorted.
Description	Brief description of the report, for example, Predefined Devices Calls Report. The column can be sorted.

3. Optionally locate specific information quickly using the 'Search by name' field; the filter applies to all text columns in the page.

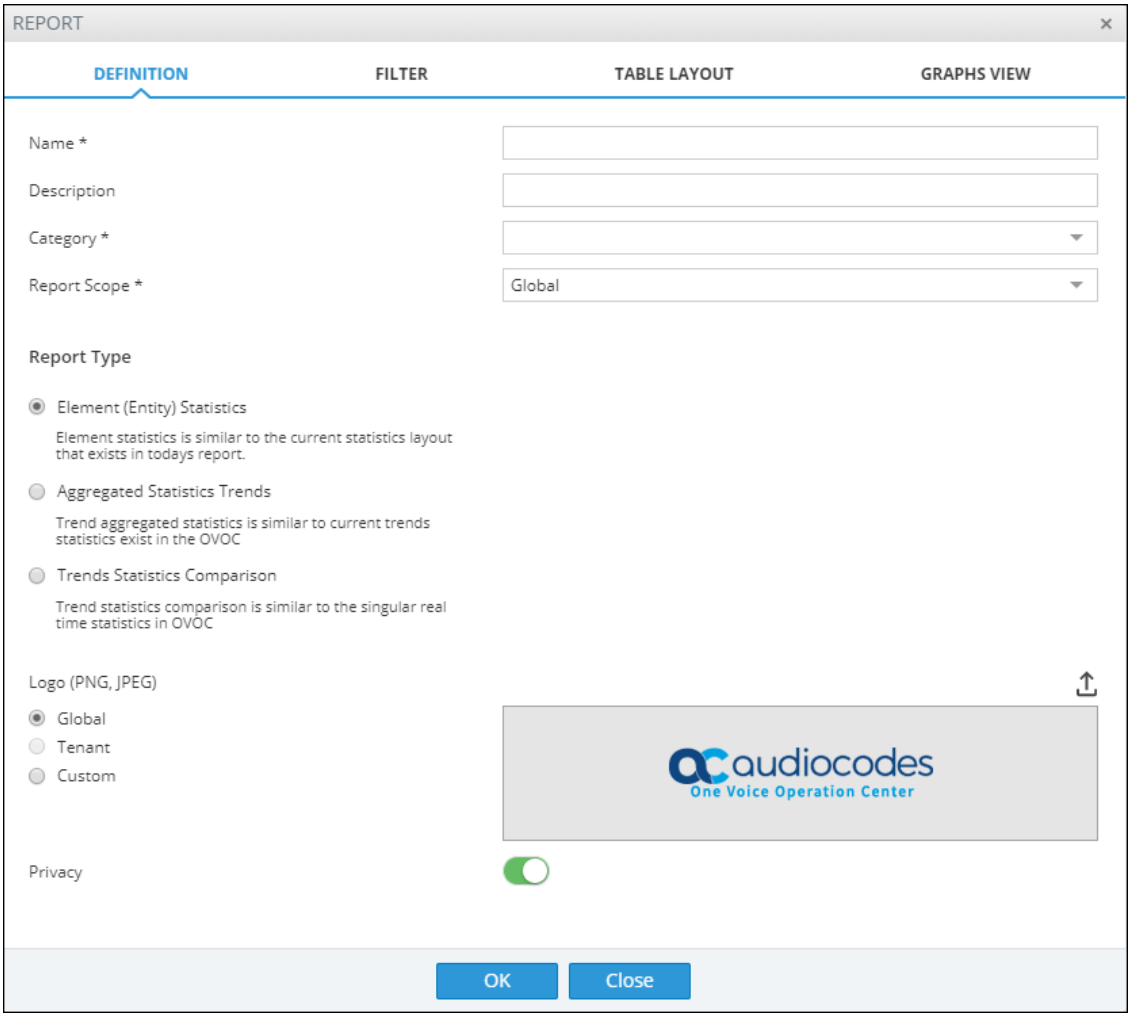
Defining a Report

Reports of three different types - Element (Entity) Statistics, Aggregated Statistics Trends and Trends Statistics Comparison - on devices, links, sites, endpoints, users and / or URIs can be defined for the last hours, days, weeks, months or for a selectable historical day / date. The results of these reports can be used to distribute information about IP telephony performance and quality of experience across the enterprise and to external authorities for diagnosis, correction of issues and network optimization.

➢ To define a report:

1. Open the Reports page (**Statistics** > **Reports** > **Reports**).
2. Click the **Add** button (disabled for operators whose security level is configured as 'Monitor').

Figure 10-3: Add Report - Definition tab



3. Use the table as reference.

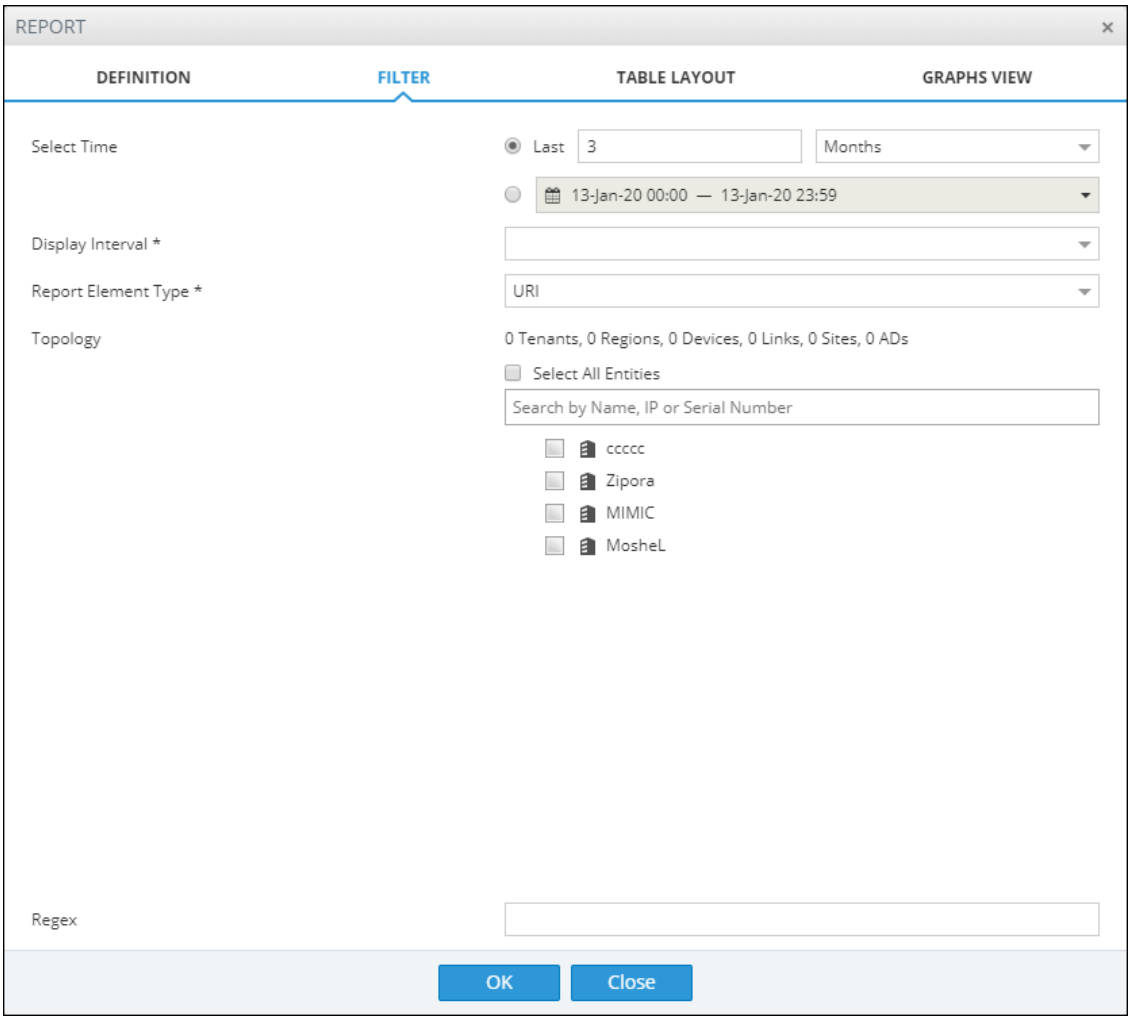
Table 10-2: Report Definition

Column	Description
Name	Enter an intuitive name for the report. Enter a name that will facilitate management later.
Description	Enter a description of the report to facilitate management later.
Category	From the drop-down, select a category from the list of report categories or define a new category.
Report Type	Select the report type option you require. Use the following as reference: ■ Element [Entity] Statistics (Default). Select this option to display a statistics report per element (entity), per defined Filter (tab). ■ Aggregated Statistics Trends. Select this option to generate a statistics report per a defined time interval for all elements (entities) per a defined Filter (tab). ■ Trends Statistics Comparison. Select this option to generate a statistics report per element (entity), for a single metric, per time interval. From the drop-down, select the metric. See Selecting a Metric on page 392 for more information.
Report Scope	Defines the scope of the report. From the drop-down, select either **Global**, **System** or a specific tenant.
Logo (PNG, JPEG)	Enables logos to be displayed in report results thereby facilitating management of reports results later. The preferred logo size is 200X40 pixels. ■ Default: **Global**. The logo image is displayed *globally* across *all report results*, irrespective of tenant. Configure the logo image file in System settings (**System** > **Administration** > **OVOC Server** > **Configuration**) as described in Uploading a Global Logo to Display in Report Results on page 78; the file is added to the Software Manager. ■ Optionally change the default **Global** to **Tenant** but first select a tenant from the 'Report Scope' drop-down; the option then becomes selectable. If you don't select a tenant from the 'Report Scope' drop-down, the option remains deactivated. The logo will only be displayed in report results related to the specified tenant. ✔ Click ⬆ to upload a tenant logo image file; the file is

Column	Description
	added to the Software Manager. You can perform the same operation in the Software Manager; see Adding Auxiliary Files on page 104 for more information. ✔ If you edit a tenant, the logo image file will be listed in the list of available tenant logos to choose from. See Editing a Tenant - Defining a Logo on page 122 for more information. ■ Optionally select the **Custom** option and from the 'Logo (PNG, JPEG)' drop-down then displayed, select a logo image file; this file will only be displayed in the result of this specific report definition. ✔ If the logo image file you require is not listed in the 'Logo (PNG, JPEG)' drop-down, click ⬆ to upload one; the file is then added to the Software Manager.
Privacy	Default: **Private**. Drag to change to **Public**; the text in the screen changes correspondingly.

4. Click the **Filter** tab.

Figure 10-4: Filter tab



5. Define a time filter:

   a. Select the **Last** option and then from the drop-down, select **Hours**, **Days**, **Weeks** or **Months**; enter the number of hours, days, weeks or months for which you require this report -OR-

   b. Select the calendar option and define from what year, month and day / date to what year, month and day / date you require this report.

6. [Only displayed if 'Aggregated Statistics Trends' or 'Trends Statistics Comparison' were selected for parameter 'Report Type' under the **Definition** tab] From the 'Display Interval' drop-down, select how often you want a measurement performed; in the report result, the graph displays the interval.

7. From the 'Report Element Type' drop-down, select the network element on which you want to produce this report:

   - Device
   - Link
   - Site

- Endpoint
- User
- URI

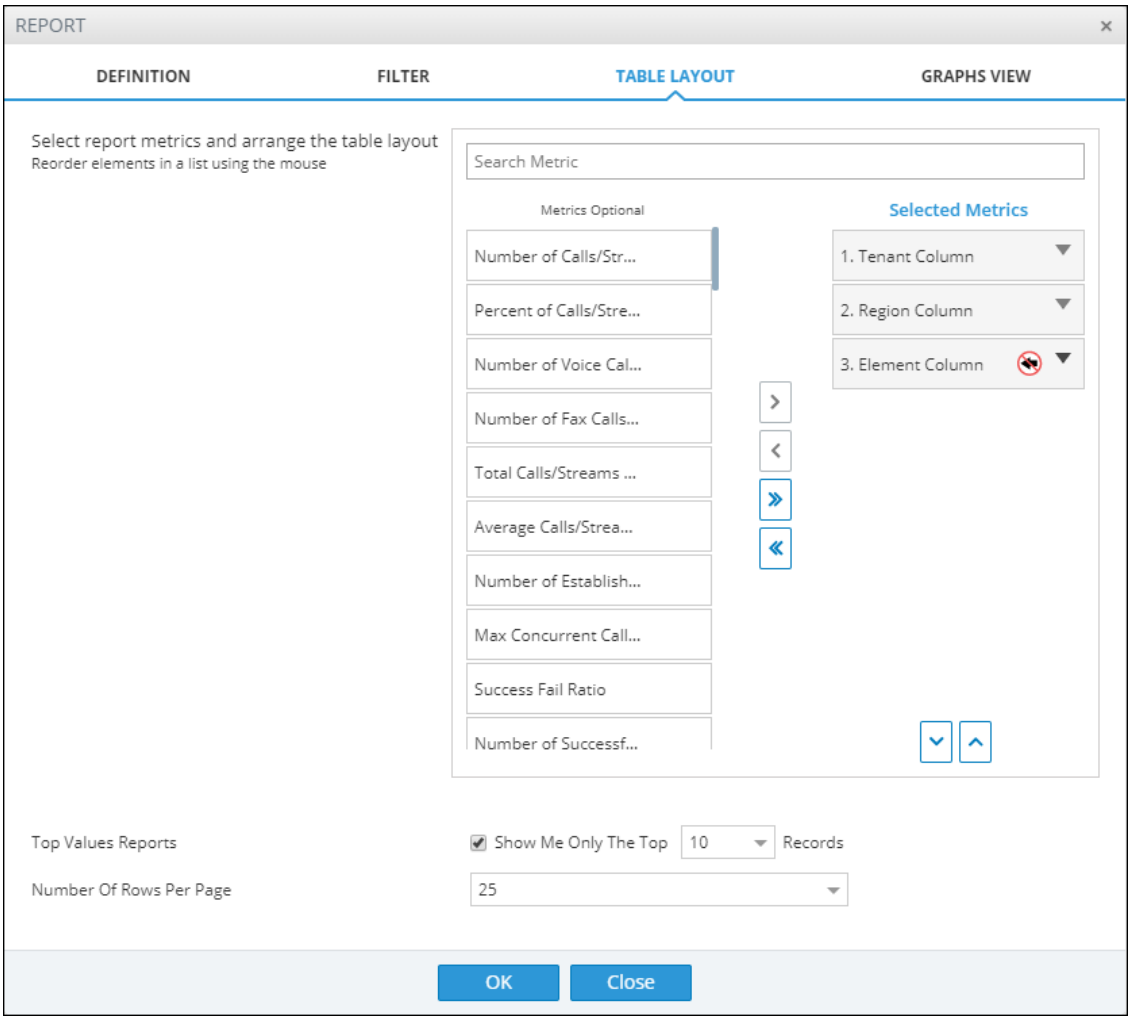
8. Under the 'Search by Name, IP or Serial Number' field, select from the topology tree the specific element (elements) on which to produce the report. The previous parameter 'Report Element Type' functions as a filter, making it easier to find in the tree the element (elements) on which to product the report.
   - If for example you selected **URI** for parameter 'Report Element Type', you'll only view tenants in the tree; you won't be able to navigate down to any lower-level element than tenant because enterprise users are located directly under tenant.
   - If for example you selected **Device** for parameter 'Report Element Type', only tenants, regions and devices will be links will be displayed in the tree making it easy to navigate to and select devices or a specific device on which to produce the report.
   - If for example you selected **Link** for parameter 'Report Element Type', devices will be filtered out from the tree; navigate to and select links or a specific link on which to produce the report.
9. If under 'Topology' you select **Select All Entities**, all tenants in the tree and all lower level entities under those tenants will be included in the report. You can then *deselect* elements until only those you want included the report remain selected.



Combined with parameter 'Report Element Type' and the **Select All Entities** option, the topology tree facilitates an easy operator experience when selecting elements on which to produce reports.

10. [Only displayed if **User** or **URI** is selected from the 'Report Element Type' drop-down] In the 'RegEx' field, enter a URI (or multiple URIs) or a user name (or multiple user names); the report results will display statistics only for those URI/URIs or user/users you defined. If the field is left undefined, reports results will be displayed for all URIs and users listed in the Active Directory.
11. Click the **Table Layout** tab.

Figure 10-5: Table Layout tab



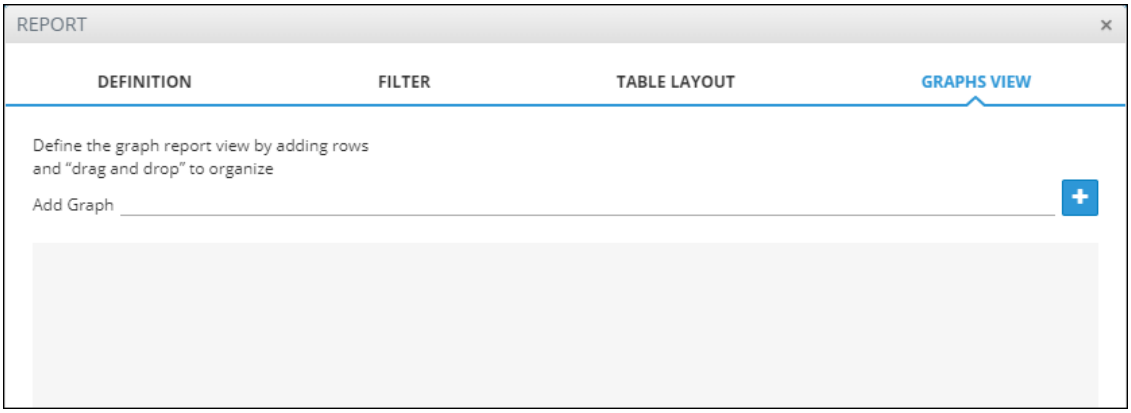
12. For the report types 'Element (Entity) Statistics' and 'Aggregated Statistics Trends':
    - Click > to include an 'Optional Metric' in the report.
    - Click < to exclude a metric from the report.
    - Click << and >> to add / remove ALL metrics to / from the report.
    - Up to four columns of metrics in a report can be sorted.
        - Click the arrow ▼▲ to make a column sortable in a direction of your choice
        - To perform a multiple-sort, press CTRL and then click a drop-down arrow; a number indicates the sort order (for two and three columns sort).
        - Use the number displayed on the arrows of the sort to determine the order of the sort.
13. For the 'Top Values Reports' parameter, select the **Show Me Only The Top** option if it's not selected (the default is selected); the 'Records' drop-down is activated. Select 10, 20, 30, 50, 100, 1000 or 10000.

When reports are on element type 'User', 'URI' or 'Endpoint', they can include multiple rows. Reports on element type 'User' can potentially include tens of thousands of rows (users). Reports on element type 'URI' can include tens of millions of calls. Reports on these element types are therefore limited to the first 10,000 users to keep them within reasonable proportions.

- The **Show Me Only The Top** option is by default selected when 'Element (Entity) Statistics' report type is selected and when the element type selected is 'User', 'URI' or 'Endpoint'; reports are limited to the first 10000 users.
- The **Show Me Only The Top** option is by default cleared when 'Aggregated Statistics Trends' report type is selected.
- The **Show Me Only The Top** option is by default cleared when 'Trends Statistics Comparison' report type is selected.

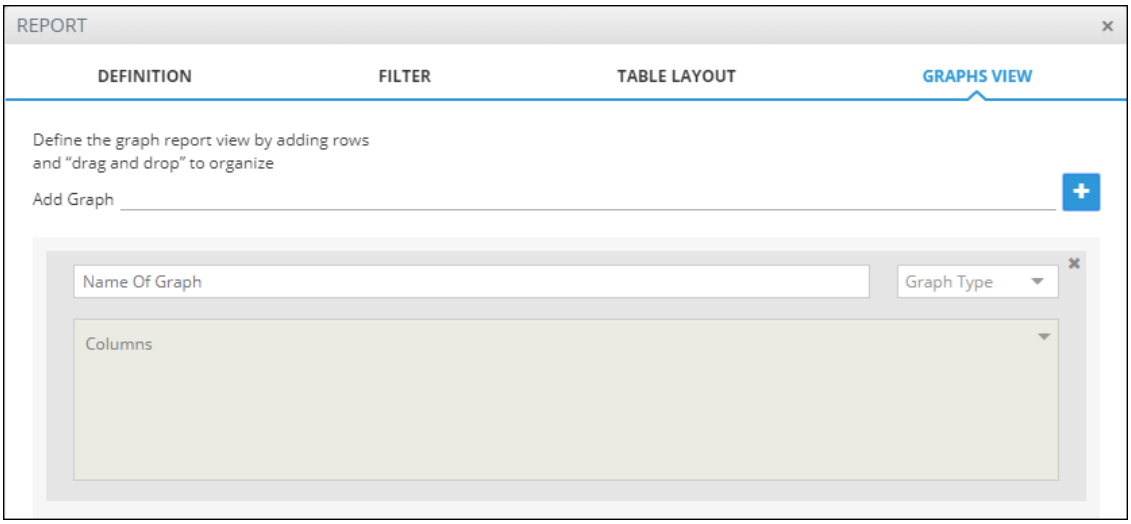
14. From the 'Number Of Rows Per Page', select 25, 50, 100 or 500.
15. Click **OK** or click the **Graphs View** tab.

Figure 10-6: Graphs View tab



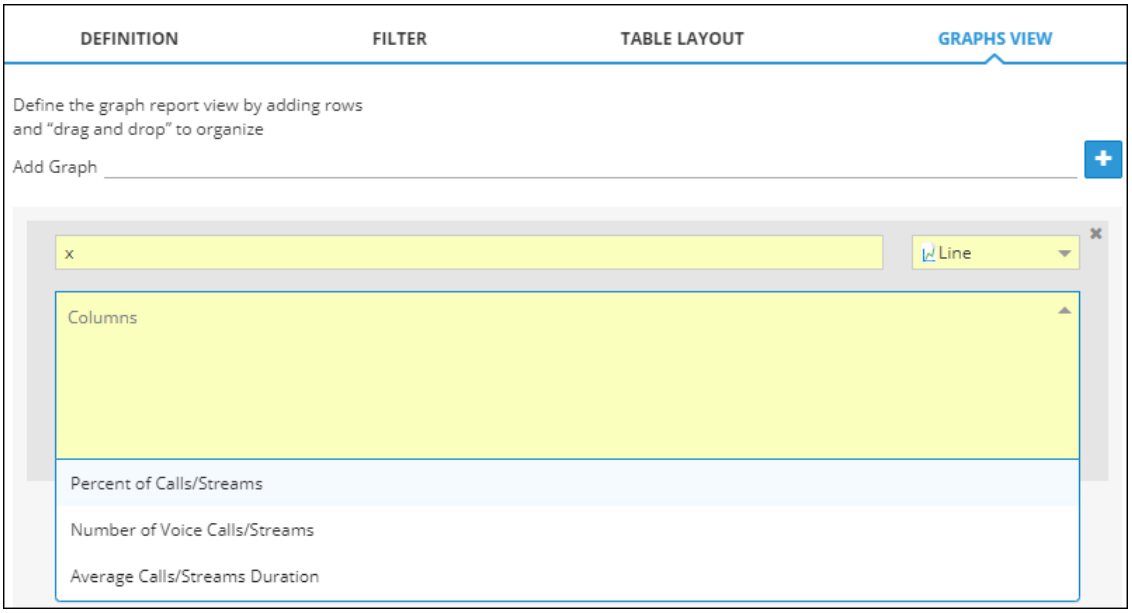
16. Click the + icon to add a graph.

Figure 10-7: Add Graph



17. Click the 'Name of Graph' field and enter an intuitive name to facilitate effective management later; the field turns yellow.
18. From the 'Graph Type' drop-down, select the type of graph to display: **Bar**, **Line**, **Pie** or **Stack Bar**; the field turns yellow; the 'Columns' pane below it also turns yellow.
19. From the 'Columns' drop-down in the 'Columns' pane, select graph columns (available columns depend on graph type and on the metrics you previously selected in the **Graphs View** tab).

Figure 10-8: Add Columns



The size of a column definition can be minimized to thumbnail by dragging the lowermost right corner inward. Multiple columns can be defined. Thumbnails can be dragged and dropped. Up to four can fit across the pane.

20. Click **OK**.

Selecting a Metric

Use the table below as reference when defining a 'Trends Statistics Comparison' report as described under Defining a Report on page 385.

Any metric listed in the table below can intuitively be understood from its *name*. If the first metric *Number of Calls / Streams* is selected to be included in a 'Trends Statistics Comparison' report, a bar, linear or pie chart will display the total sum of calls (if the element on which the report is produced is defined as *Device*) or streams (if the element on which the report is produced is defined as *Link*), made in a defined time period, as a number. Any metric listed can be understood in this way.

Metric	REST Metric Name	# % :	Type of	Total as

			Chart	a...
Number of Calls/Streams	callsCounter	Number	Bar, Line, Pie	Sum
Percent of Calls/Streams	callsPercent	Percent	Bar, Line, Pie	Sum
Number of Voice Calls/Streams	voiceCallsCounter	Number	Bar, Line, Pie	Sum
Number of Fax Calls/Streams	faxCallsCounter	Number	Bar, Line, Pie	Sum
Total Calls/Streams Duration	totalCallsDuration	Number	Bar, Line, Pie	Sum
Average Calls/Streams Duration	averageCallDuration	Number	Bar, Line, Pie	Average
Number of Established Calls/Streams	averageCallDurationCount	Number	Bar, Line, Pie	Sum
Max Concurrent Calls/Streams	maxConcurrentCalls	Number	Bar, Line, Pie	Max
Success Fail Ratio	successFail	Ratio	Stack bar	Percent
Number of Successful Calls/Streams	successfulCounter	Number	Bar, Line, Pie	Sum
Number of Failed Calls/Streams	failedCallsCounter	Number	Bar, Line, Pie	Sum
Success	successfulCallsPercent	Number	Bar,	Percent

Calls/Streams Ratio			Line	
Failed Calls/Streams Ratio	failedCallsPercent	Number	Bar, Line	Percent
Calls/Streams Quality Ratio	callsQuality	Ratio	Stack bar	Percent
Calls/Streams Quality Ratio Without Unknown	callsQualityWithoutUnknown	Ratio	Stack bar	Percent
Number of Good Calls/Streams	goodCallsCounter	Number	Bar, Line, Pie	Sum
Number of Fair Calls/Streams	fairCallsCounter	Number	Bar, Line, Pie	Sum
Number of Bad Calls/Streams	poorCallsCounter	Number	Bar, Line, Pie	Sum
Number of Unknown Calls/Streams	unknownCallsCounter	Number	Bar, Line, Pie	Sum
Good Quality Ratio	goodCallsPercent	Number	Bar, Line	Percent
Fair Quality Ratio	fairCallsPercent	Number	Bar, Line	Percent
Bad Quality Ratio	poorCallsPercent	Number	Bar, Line	Percent
Unknown Quality Ratio	unknownCallsPercent	Number	Bar, Line	Percent
MOS Ratio	mosQuality	Ratio	Stack bar	Percent
MOS Ratio	mosQualityWithoutUnknown	Ratio	Stack	Percent

Without Unknown			bar	
MOS Unknown Ratio	mosUnknownCallsPercent	Number	Bar, Line	Percent
MOS Good Ratio	mosGoodCallsPercent	Number	Bar, Line	Percent
MOS Fair Ratio	mosFairCallsPercent	Number	Bar, Line	Percent
MOS Bad Ratio	mosPoorCallsPercent	Number	Bar, Line	Percent
Jitter Ratio	jitterQuality	Ratio	Stack bar	Percent
Jitter Ratio Without Unknown	jitterQualityWithoutUnknown	Ratio	Stack bar	Percent
Jitter Unknown Ratio	jitterUnknownCallsPercent	Number	Bar, Line	Percent
Jitter Good Ratio	jitterGoodCallsPercent	Number	Bar, Line	Percent
Jitter Fair Ratio	jitterFairCallsPercent	Number	Bar, Line	Percent
Jitter Bad Ratio	jitterPoorCallsPercent	Number	Bar, Line	Percent
Delay Ratio	delayQuality	Ratio	Stack bar	Percent
Delay Ratio Without Unknown	delayQualityWithoutUnknown	Ratio	Stack bar	Percent
Delay Unknown Ratio	delayUnknownCallsPercent	Number	Bar, Line	Percent
Delay Good Ratio	delayGoodCallsPercent	Number	Bar, Line	Percent

Delay Fair Ratio	delayFairCallsPercent	Number	Bar, Line	Percent
Delay Bad Ratio	delayPoorCallsPercent	Number	Bar, Line	Percent
PLoss Ratio	plossQuality	Ratio	Stack bar	Percent
PLoss Ratio Without Unknown	plossQualityWithoutUnknown	Ratio	Stack bar	Percent
PLoss Unknown Ratio	plossUnknownCallsPercent	Number	Bar, Line	Percent
PLoss Good Ratio	plossGoodCallsPercent	Number	Bar, Line	Percent
PLoss Fair Ratio	plossFairCallsPercent	Number	Bar, Line	Percent
PLoss Bad Ratio	plossPoorCallsPercent	Number	Bar, Line	Percent
Echo Ratio	rerlQuality	Ratio	Stack bar	Percent
Echo Ratio Without Unknown	rerlQualityWithoutUnknown	Ratio	Stack bar	Percent
Echo Unknown Ratio	rerlUnknownCallsPercent	Number	Bar, Line	Percent
Echo Good Ratio	rerlGoodCallsPercent	Number	Bar, Line	Percent
Echo Fair Ratio	rerlFairCallsPercent	Number	Bar, Line	Percent
Echo Bad Ratio	rerlPoorCallsPercent	Number	Bar, Line	Percent
Avg MOS	avgMos	Number	Bar, Line	Average

Max MOS	maxMos	Number	Bar, Line, Pie	Max
Min MOS	minMos	Number	Bar, Line, Pie	Min
Avg Jitter	avgJITTER	Number	Bar, Line	Average
Max Jitter	maxJITTER	Number	Bar, Line, Pie	Max
Min Jitter	minJITTER	Number	Bar, Line, Pie	Min
Avg PLoss	avgPacketLoss	Number	Bar, Line	Average
Max Ploss	maxPacketLoss	Number	Bar, Line, Pie	Max
Min Ploss	minPacketLoss	Number	Bar, Line, Pie	Min
Avg Delay	avgDELAY	Number	Bar, Line	Average
Max Delay	maxDELAY	Number	Bar, Line, Pie	Max
Min Delay	minDELAY	Number	Bar, Line, Pie	Min
Avg Echo	avgRERL	Number	Bar, Line	Average
Max Echo	maxRERL	Number	Bar, Line,	Max

			Pie	
Min Echo	minRERL	Number	Bar, Line, Pie	Min
Avg SNR	avgSNR	Number	Bar, Line	Average
Avg Total Kbps	avgTotalPackets	Number	Bar, Line, Pie	Average
Avg Rx Kbps	avgRxPackets	Number	Bar, Line, Pie	Average
Avg Tx Kbps	avgTxPackets	Number	Bar, Line, Pie	Average
Number of MOS Calls/Streams	mosCounter	Number	Bar, Line, Pie	Sum
Number of Jitter Calls/Streams	jitterCounter	Number	Bar, Line, Pie	Sum
Number of Delay Calls/Streams	delayCounter	Number	Bar, Line, Pie	Sum
Number of PLoss Calls/Streams	packetLossCounter	Number	Bar, Line, Pie	Sum
Number of Echo Calls/Streams	rerlCounter	Number	Bar, Line, Pie	Sum
Number of SNR Calls/Streams	snrCounter	Number	Bar, Line, Pie	Sum
Number of	outgoingCounter	Number	Bar,	Sum

Outgoing Calls/Streams			Line, Pie	
Number of Incoming Calls/Streams	incomingCounter	Number	Bar, Line, Pie	Sum

Viewing a Defined Report

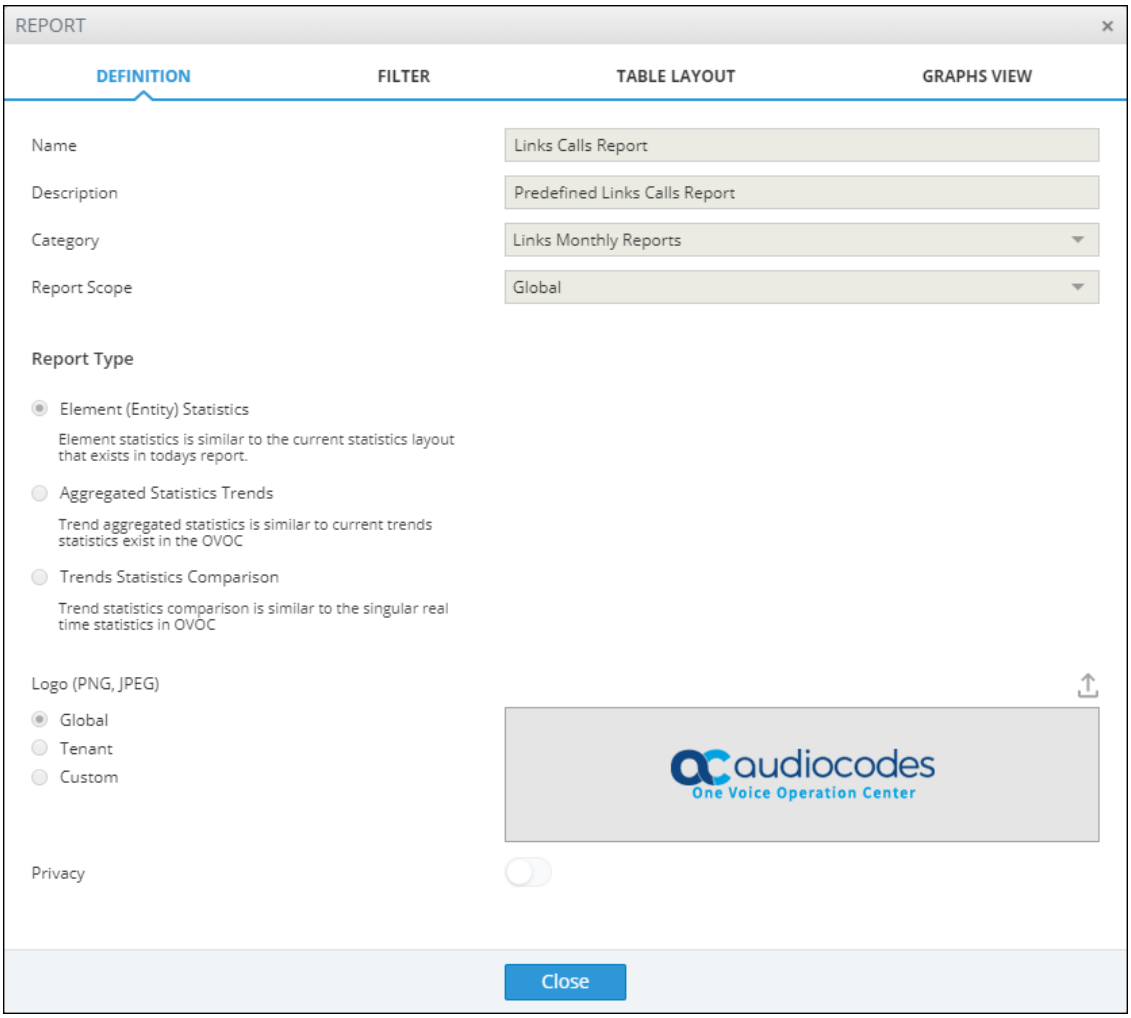
Network administrators who do *not* have permission to *edit* report definitions can nonetheless *view* them. The **View** button in the Reports page gives these administrators this capability. The **Edit** button is available to administrators who *do* have permission to edit report definitions.

After defining a report as shown in Defining a Report on page 385, you can view its definition to make sure it conforms to what you want and if it doesn't, then you can edit it as shown in Editing a Report on the next page.

➢ **To view a defined report:**

1. In the Reports page (**Statistics** > **Reports** > **Reports**), select the report whose definition you want to view and then click the **View** button.

Figure 10-9: Report



2. View the read-only parameter definitions under the tabs **Definition**, **Filter**, **Table Layout** and **Graphs View**. Make a note of definitions that do not conform to your requirements. Click **Close** and then optionally edit the definitions as shown in Editing a Report below.

Editing a Report

Reports can be edited and tweaked to conform with network administrator requirements.

The 'Privacy' parameter under the **Definition** tab in the Report screen determines who is allowed to edit a report and who isn't.

- When the 'Privacy' parameter is set to private, the report can:
  - ✔ be edited only by the owner operator
  - ✔ be deleted only by System / Tenant Admin
  - ✔ be deleted by a Tenant operator if the report is defined under that operator's tenant
- When the 'Privacy' parameter is set to public, the report can:
  - ✔ be modified by any operator whose security level is higher than Monitor

➢ To edit a report:

- In the Reports page, select a report and click the **Edit** button. The button will only be activated *depending on editing permission*. Network administrators who do *not* have permission to *edit* report definitions can nonetheless *view* them. The **View** button in the Reports page gives these administrators this capability. See Viewing a Defined Report on page 399 for more information.

> When editing a report, use the information in Defining a Report on page 385 as reference. The screens displayed when editing a report are identical to those displayed when defining one.

Performing Actions on Reports

The OVOC lets network administrators perform actions such as running a report, exporting a report definition, importing a report definition and duplicating a report definition.

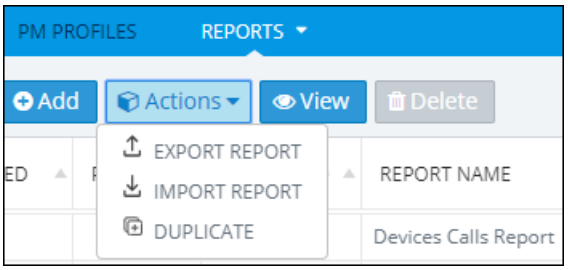
➢ To run a report:

- In the Reports page, select a report and then click the activated **Run** button; a notification is displayed indicating *Report Executed*. *Execute Report Succeeded* and the report is displayed. If a report is not selected, the **Run** button will not be activated.

➢ To export a report definition:

- Click the **Actions** button and from the drop-down menu select **Export Report**. All operators can view except the operator whose security level is 'Monitor'. The exported report definition - in JSON format - is indicated in the lowermost left corner of the Reports page.

Figure 10-10: Export Report Definition



➢ To import a report definition:

- Click the **Actions** button and from the drop-down menu select **Import Report**. If a report with the same 'unique fields' already exists, choose to overwrite when prompted *Do you want to overwrite?* Only operators who have permission to add / edit reports can import.

➢ To duplicate a report definition:

- Click the **Actions** button and from the drop-down menu select **Duplicate**. Only operators who have permission to add / edit reports can duplicate.

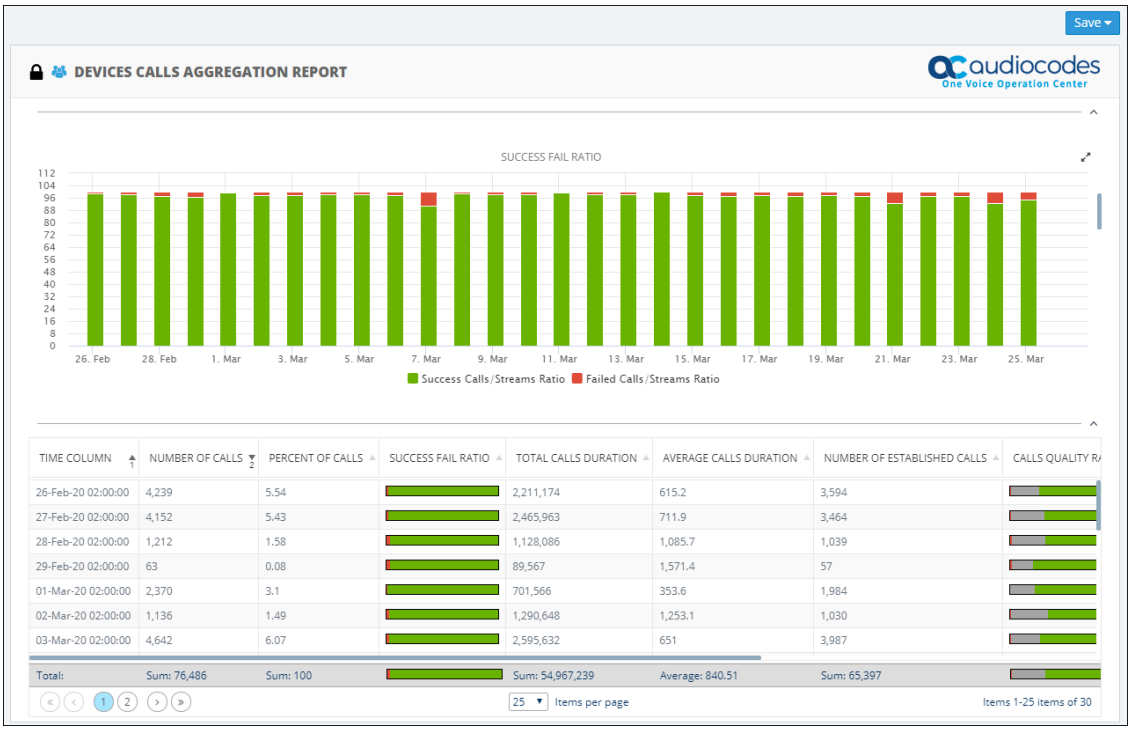
Displaying Report Results

After defining a report, the report can be run and displayed on your browser, and / or saved.

➢ To run and display a report:

1. Open the Reports page (**Statistics** > **Reports** > **Reports**), select the report you want to run and display and then click the **Run** button; the Report Result is dynamically tabbed and displayed and an 'Execute Report Succeeded' message is momentarily displayed.

Figure 10-11: Report Result



- The maximum number of bars in each chart is 100.
- The PDF file will display only the table's first columns (approximately 8-10 columns).

2. Use the 'Report Details' pane on the right of the page for quick reference. You can see in the preceding figure that this report is of type 'Aggregation'.
3. [Optionally] Click the **x** in the dynamic tab to remove the Report Result; you're returned to the Reports page.
4. In the Reports page, optionally select another report and click **Run**; as with the previous run, the Report Result is dynamically tabbed and displayed and an 'Execute Report Succeeded' message is momentarily displayed. Multiple Report Results can be dynamically tabbed facilitating comparative analysis.
5. [Optionally] Click the **Save** button located above the Report Details pane and select CSV or PDF from the drop-down to save the result as a file for distribution purposes.

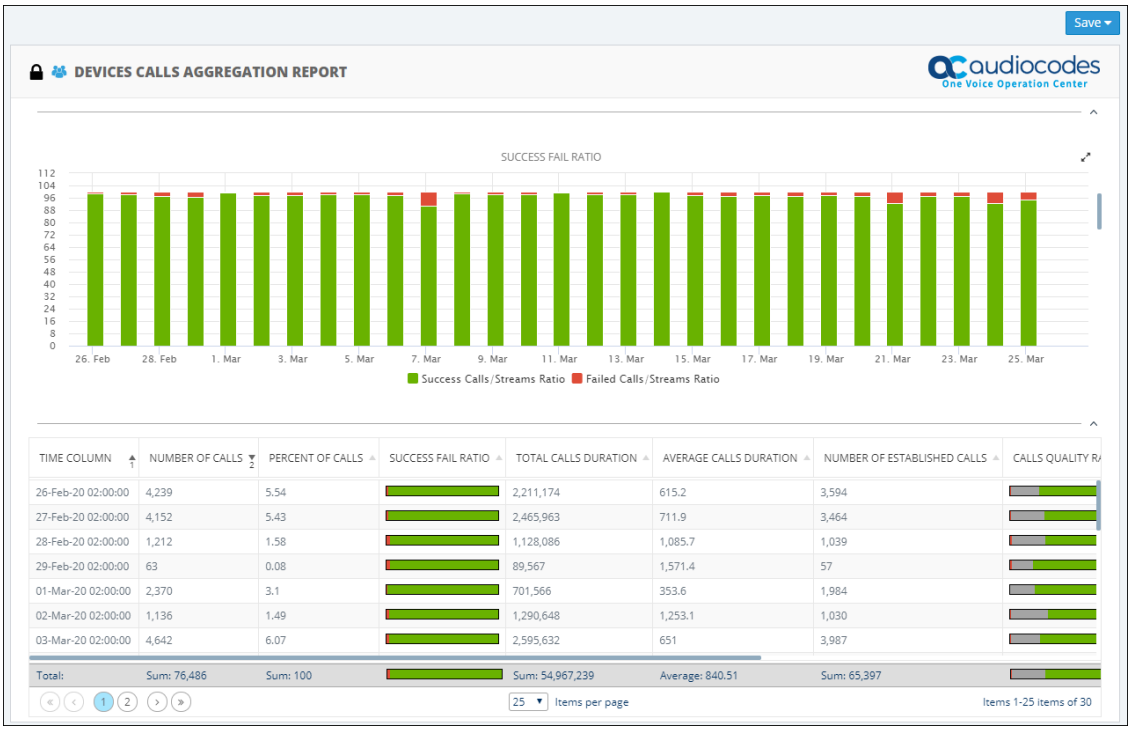
For more information about results of reports of type 'Element', see 'Element (Entity) Statistics' Report Type below

For more information about results of reports of type 'Aggregation', see 'Aggregated Statistics Trends' Report Type on the next page

'Element (Entity) Statistics' Report Type

After defining a report of type 'Element (Entity) Statistics', it can be run and displayed in your browser as shown in the figure below.

Figure 10-12: 'Element (Entity) Statistics' Report



Use the following to get acquainted:

- indicates a predefined report integrated with OVOC; cannot be deleted or edited
- indicates a public report; anyone can view, edit and delete it
- 'Devices Calls Report' indicates the defined name of the report
- Each bar in the chart shows the value (values, if it's a stack chart) of the metric, according to the chart legend:
  - Red = Failed calls / streams (as shown in the preceding figure)
  - Green = Successful calls / streams (as shown in the preceding figure)
- The y axis shows number of calls
- The x axis shows each device's name
- The Report Details pane on the right displays among other details

- the report category
- the defined time period
- the date and time the report was executed
- the number of entities in the topology

- The lowermost table columns show
  - tenant name
  - region name
  - element name
  - # of calls
  - % of calls
  - success|fail ratio
  - total calls duration
  - average calls duration
  - # of established calls
  - calls / streams quality ratio
  - maximum concurrent calls
  - # of voice calls
  - # of fax calls

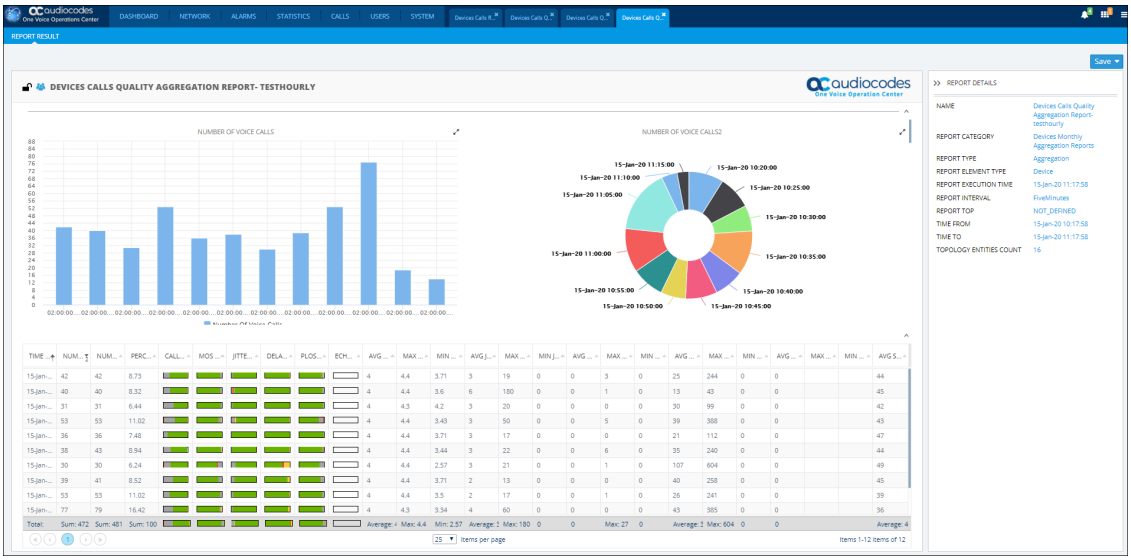
Colors of bars in a stack chart depend on *metric name*. In the preceding figure, for example, the metric name 'Success Calls / Streams Ratio' contains 'Success', so the stack chart is green.

- If the name of the metric contains 'Good' or 'Success', the stack chart will be green
- If the name of the metric contains 'Fail', 'Bad' or 'Poor', the stack chart will be red
- If the name of the metric contains 'fair', the stack chart will be yellow
- If the name of the metric contains 'Unknown', the stack chart will be gray

'Aggregated Statistics Trends' Report Type

After defining a report of type 'Aggregated Statistics Trends', it can be run and displayed in your browser as shown in the figure below.

Figure 10-13: 'Aggregated Statistics Trends' Report



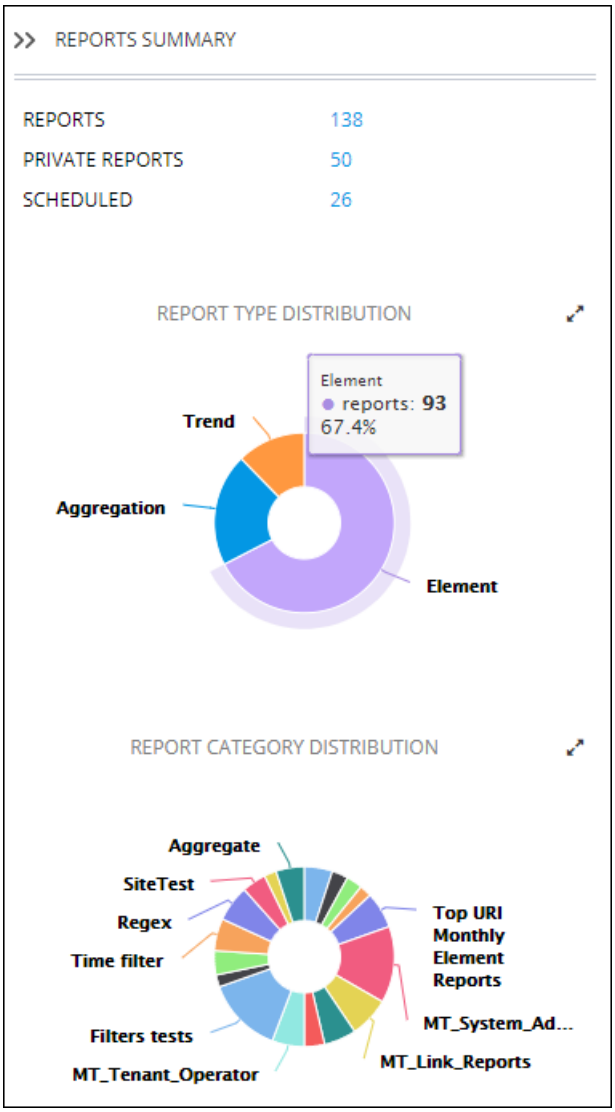
Use the following to get acquainted:

- indicates an administrator-defined report
- indicates the report is public; anyone can view, edit and delete it
- 'Devices Calls Quality Aggregation Report' indicates the defined name of the report
- The bar chart indicates the number of voice calls made per time period
- The pie chart presents the same information differently; a glance reveals during which time interval (segment) most calls were made; tooltips provide details
- The Report Details pane on the right displays among other details
  - the report category
  - the report interval
  - the date and time the report was executed
  - the number of entities in the topology
- The lowermost table columns show among other details the time, # of calls, call quality metrics, etc.

Viewing a Snapshot of all Reports Statistics

The Reports Summary page provides network administrators with a snapshot view of all statistics related to reports. The pane gives operators quick and deep insight into management accountability status. Open the Reports page (**Statistics** > **Reports** > **Reports**) and locate the Reports Summary pane on the right.

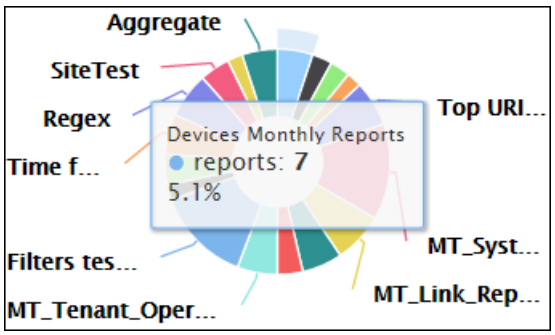
Figure 10-14: Reports Summary



- The *uppermost* section of the pane displays
  - the number of reports
  - the number of private reports
  - the number of scheduled reports
- The *middle* section of the pane shows a pie chart depicting how report types (Trend, Aggregation and Element) are distributed. Optionally, magnify the chart by clicking ⤢; a full-screen view of the pie chart is then displayed; in the full-screen view, click ⤡ to return to the pie chart in Summary Pane view. Hover your mouse over a segment of the pie. Use the preceding figure as reference; a popup indicates report type, # of reports of this type and the % of reports of this type. You can immediately determine for example for which report type most reports were run and for which least.
- The *lowermost* section of the pane shows a pie chart depicting how report categories are distributed. Optionally magnify the chart by clicking ⤢; a full-screen view of the pie chart is then displayed; in the full-screen view, click ⤡ to return to the pie chart in Summary Pane

view. Hover your mouse over a segment of the pie; a popup indicates report category, e.g., Devices Monthly Reports, # of reports in this category and the % of reports in this category. You can immediately determine for example in which report category most reports were run and in which least.

Figure 10-15: Pie Chart Depicting Distribution per Report Category



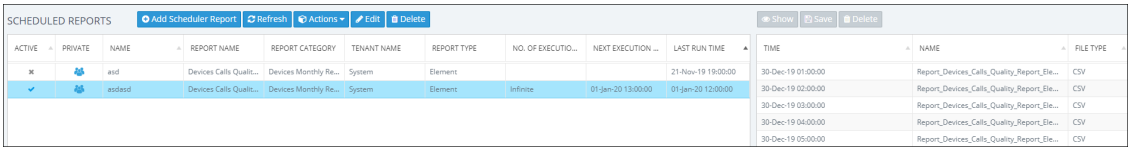
Viewing Schedulers and Reports Executed by them

The OVOC's Scheduled Reports page allows you to view report schedulers that have been configured and the reports that have been executed by them.

➢ To view Report Schedulers:

1. Open the Scheduled Reports page (**Statistics** > **Reports** > **Scheduled Reports**).

Figure 10-16: Scheduled Reports Page Displaying Configured Report Schedulers



2. On the left side of the page, view the configured Report Schedulers. The table following explains the columns on the left side of the page in which the Report Schedulers are listed.

Table 10-3: Viewing the Listed Report Schedulers

Column	Description
Active	Indicates whether the scheduled report is active or inactive. A scheduled report is activated or deactivated when it's added, by toggling the 'Active' switch in the Scheduler Report dialog.
Private / Public	indicates that the scheduled report is a *public* report; anyone can view, edit and delete it and indicate that the scheduled report is a *private* report indicates that *I am the owner* of this scheduled private report

Column	Description
	and that I can view, edit and delete it; the operator defined as Administrator can view and delete this scheduled report (but not edit it). indicates that *I am not the owner* of this scheduled private report; the icon is available only for the operator defined as Administrator; only the operator defined as Administrator can view and delete this scheduled report. The column can be sorted according to these classifications.
Name	The name of the Scheduler. Defined when a scheduled report is added, in the 'Scheduler Name' field (mandatory parameter) in the Scheduler Report dialog.
Report Name	The name of the scheduled report. Selected when a scheduled report is added from the 'Scheduler Name' drop-down list (mandatory parameter) in the Scheduler Report dialog.
Report Category	The category under which the scheduled report is categorized, corresponding to the previous column 'Report Name'. When a scheduled report is added, the 'Category' is displayed as a read-only indication under 'Report Info' in the Scheduler Report dialog.
Tenant Name	Corresponds to the option selected from the 'Scheduler Scope' drop-down list (mandatory parameter) in the Scheduler Report dialog, when adding the scheduled report.
Report Type	For example, 'Element'. When a scheduled report is added, the 'Type' is displayed under 'Report Info' as a read-only indication in the Scheduler Report dialog.
No. of Executions Left	Indicates the number of executions remaining. For example, 'Infinite'. Corresponds to the option selected from the 'Scheduler Scope' drop-down list (mandatory parameter) in the Scheduler Report dialog, when adding the scheduled report.
Next Execution Run	Indicates the day, date and time the next report is scheduled for. Corresponds to the day, date and time configured in the Scheduler Report dialog when adding a scheduled report.
Last Run Time	Indicates the day, date and time the last report scheduled was run. Corresponds to the day, date and time configured in the Scheduler Report dialog when adding a scheduled report. The column is sortable.

3. In the pane on the right side of the page, view a list of generated reports. The table following explains the columns in the pane on the right side of the page in which the generated reports are listed

Table 10-4: Viewing the Listed Generated Reports

Column	Description
Time	Indicates the time of the day and the day of the month on which the report was generated, in the following format: DD-Month-YY HH:MM:SS
Name	Indicates the name of the report. Tallies with the 'Report Name' column displayed in the left side of the Scheduled Reports page. The name is selected from the 'Scheduler Name' drop-down list (mandatory parameter) in the Scheduler Report dialog when a scheduled report is added. The column also displays the 'Report Type' (Element, in the figure below), Tenant / System, and the year / month / day / time.  TIME | NAME | FILE 30-Dec-19 04:00:00 | Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0200 | CSV 30-Dec-19 05:00:00 | Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0300 | CSV 30-Dec-19 06:00:00 | Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0400 | CSV
File Type	Indicates the type of file in which the report is formatted. CSV or PDF format. The column is sortable. Note that the PDF file will display only the table's first columns (approximately 8-10 columns).

4. In the left side of the Scheduled Reports page, select a Report Scheduler; the pane on the right side of the page displays a list of reports executed by that scheduler.

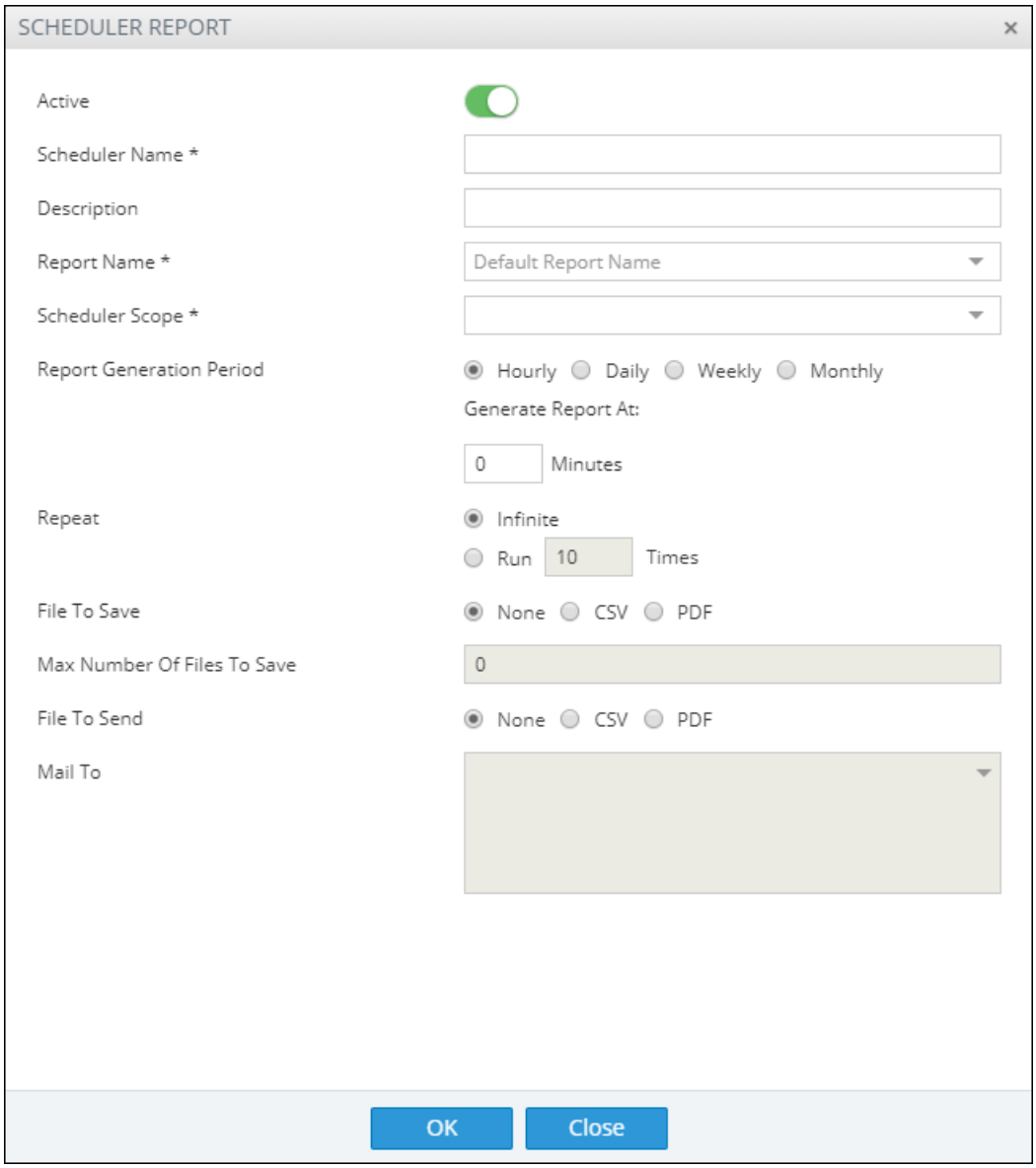
Adding a Report Scheduler

The 'Report Scheduler' feature allows administrators to schedule OVOC reports. A report can be scheduled for every hour, day, week or month, infinitely or for a specified number of times. The feature automates report generation, reducing administrator workload and providing built-in accountability. By presenting information about IP network telephony performance and quality of experience *over time*, the feature facilitates longitudinal comparative analysis.

➢ To add a report scheduler:

1. In the Scheduled Reports page (**Statistics** > **Reports** > **Scheduled Reports**), click the **Add Scheduler** button.

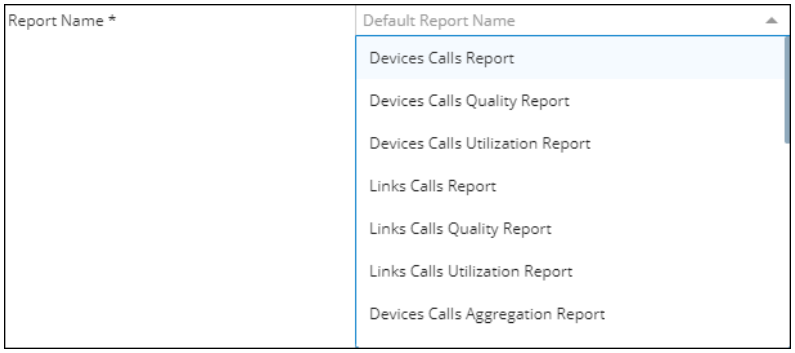
Figure 10-17: Report Scheduler



2. Configure a schedule using the table as reference.

Table 10-5: Report Scheduler

Column	Description
Active	Toggle the 'Active' switch to activate or deactivate the scheduler.
Scheduler Name	Enter an intuitive, management friendly name for the scheduler.
Description	Enter a description for the scheduler to facilitate management for other operators.
Report Name	From the drop-down, select a report name. Scroll down to view the full list of options. Auto complete is also supported.

Column	Description
	
Scheduler Scope	From the drop-down, select ■ **System** for the scope of the scheduler to be *per system*, irrespective of tenant ■ per specified tenant for the scope of the scheduler to be *for that specified tenant*
Report Generation Period	Select either **Hourly** (default), **Daily**, **Weekly** or **Monthly**. Determines how frequently reports will be generated. If you select ■ **Hourly** then 'Minutes' will also be configurable. ■ **Daily** then 'Hours' and 'Minutes' will also become configurable. [Note that a daily report for Microsoft Teams should be configured for after 01:30/02:00]. ■ **Weekly** then 'Days', 'Hours' and 'Minutes' will also become configurable. ■ **Monthly** then 'Days', 'Hours' and 'Minutes' will also become configurable.
Repeat	Select **Infinite** for the scheduler to run reports endlessly, without limitation; or **Run**, in which case the scheduler will by default generate the report 10 times. This value can be changed to suit individual requirements. After the nth time, the scheduler stops running and transitions to 'Disabled' state.
File to Save	Select either **None**, **CSV** or **PDF**.
Max Number Of Files To Save	Defines the number of historical reports. Default: 60. If **CSV** or **PDF** is selected for the preceding parameter, the field is activated and the default can be modified.
File To Send	Select either **None**, **CSV** or **PDF**.

Column	Description
Mail To	If **CSV** or **PDF** is selected for the preceding parameter, the 'Mail To' field is activated and a destination email address or multiple destination email addresses can be entered.

3. Click **OK**.

Editing a Defined Scheduler

IP network administrators can edit a defined 'Report Scheduler'.

➢ To edit a defined report scheduler:

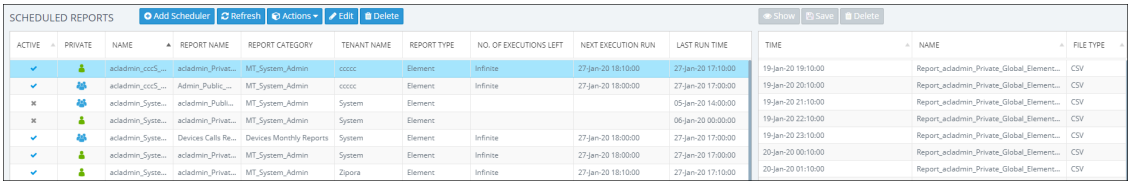
- In the Scheduled Reports page (**Statistics** > **Reports** > **Scheduled Reports**), select the scheduler to edit and then click the **Edit** button; the same screen opens as that when adding a scheduler. See Adding a Report Scheduler on page 409 for more information. Edit the scheduler definitions using the same table for reference as that in Adding a Report Scheduler on page 409.

Showing a Scheduled Report's Results

A scheduled report's results can be displayed (shown), saved and / or deleted.

➢ To show a scheduled report's results:

1. In the Scheduled Reports page (**Statistics** > **Reports** > **Scheduled Reports**), select a Report Scheduler from the list of configured Report Schedulers listed in the left side of the page.



2. In the pane on the right side of the Scheduled Reports page, select a report from the list of generated reports and click the **Show** button; the Report Result is dynamically tabbed and displayed and a 'Load Scheduler Result Succeeded' message is momentarily displayed. See the figure in Displaying Report Results on page 402 for reference.
3. Use the 'Report Details' pane on the right of the report for quick reference.
4. [Optionally] Click the **x** in the dynamic tab to remove the Report Result; you're returned to the Scheduled Reports page.
5. In the Scheduled Reports page, optionally select another scheduler and report, and click **Show**; as previously, the Report Result is dynamically tabbed and displayed and a 'Load Scheduler Result Succeeded' message is momentarily displayed. Multiple scheduled report results can be dynamically tabbed facilitating longitudinal comparative analysis.

6. [Optionally] Click the **Save** button located above the pane to save a result as a file for distribution.

11 AudioCodes IP Network Telephony Equipment

The following table shows the supported AudioCodes IP network telephony equipment.

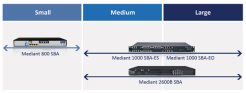
Table 11-1: Supported AudioCodes IP Network Telephony Equipment

Supported IP Network Telephony Equipment	Description
  MediaPack	**MP-1xx:** 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. **MP-20x:** 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. (See product documentation for detailed information)
 Mediant 500 E-SBC  Mediant 500L E-SBC	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.
 Mediant 500 MSBR  Mediant 500L MSBR  Mediant 800 MSBR  Mediant 1000 MSBR	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. 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. 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. (See the specific product documentation for detailed information)
Mediant 500Li	Part of the the AudioCodes Mediant i-Series, this device offers service providers a range of all-in-one SOHO, SMB and SME routers

Supported IP Network Telephony Equipment	Description
	combining access, data, voice and security into a single device. The device is suited for managed data, SIP trunking, hosted PBX and cloud-based services, and enable service providers to deploy flexible and cost-effective solutions. In addition to their powerful integrated routing and security software, the device also features a unique multi-core architecture that ensures consistent high performance, allowing end customers to maximize their broadband connections for both data and voice applications. (See the specific product documentation for detailed information)
 Mediant 500 Enterprise Session Border Controller (E-SBC)	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.
 Mediant 2600 E-SBC	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.
 AudioCodes Mediant Software Enterprise Session Border Controllers	Mediant Software E-SBCs are pure-software products, enabling connectivity and security between enterprises' and service providers' VoIP networks. Includes the following product variants: **Mediant Server Edition SBC:** x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements. **Mediant Virtual Edition SBC:** Installed and hosted in a virtual machine environment that complies to specified requirements.
Mediant Cloud	The OVOC supports the AudioCodes Mediant Cloud Edition. The

Supported IP Network Telephony Equipment	Description
Edition	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.
 MP-1288	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. 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.
 Mediant 3000 Media Gateway	Medium-sized member of the family of market-ready, standards-compliant Media Gateway systems. 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 Applications: VoP Trunking devices, IP-Centrex devices, VoP Access devices 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)

Supported IP Network Telephony Equipment	Description
 Mediant 4000 E-SBC	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.
 Media Transcoder [Mediant 4000B]	Delivers high capacity DSP-based transcoding in conjunction with AudioCodes' field-proven hardware-based SBC product family. Aimed at service providers and large enterprises, AudioCodes MT offloads media transcoding from AudioCodes SBCs handling large call volumes. This ensures high quality and reliability in heterogeneous environments where simultaneous support for multiple codecs is needed.
 AudioCodes Mediant Cloud Edition (CE) software session border controller (SBC)	The AudioCodes Mediant Cloud Edition (CE) software session border controller (SBC) leverages the advantages of cloud agility to allow enterprises and service providers to fully realize the potential of virtual environments by offering full cloud elasticity that rapidly adjusts to changing needs. The Mediant CE automatically provides extra capacity when required and scales back when demand drops. Its microservices architecture, combined with a scalable media cluster, enables new revenue-generating communications services to be introduced simply and cost-effectively.
 Mediant 9000 SBC	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. 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.
Survivable Branch	Designed for Microsoft Skype for Business Server, the Survivable

Supported IP Network Telephony Equipment	Description
Appliance (SBA) 	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. 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.
	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.
	■ 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. ■ 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. ■ UMP Quick Connect gives service providers a simple and fast way to add new customers. It also enables the configuration of AudioCodes SBCs and the Microsoft Office 365 tenant in just a few minutes, without entering CLI commands or resorting to PowerShell.
SmartTAP	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

Supported IP Network Telephony Equipment	Description
	SmartTAP, enterprises can capture and index any customer or organizational interaction across external and internal communication channels seamlessly.
	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. 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.
	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. 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.
	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.

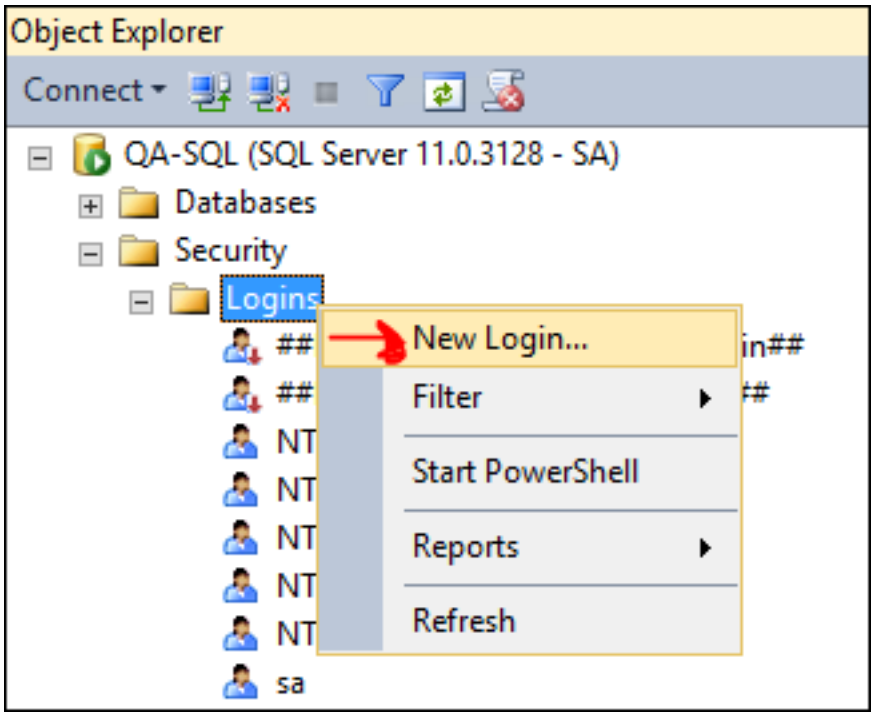
12 Adding an Unprivileged User to MSSQL Server

An unprivileged user can be added to the MSSQL server with SQL Server Management Studio.

➢ **To add an unprivileged user to the MSSQL server:**

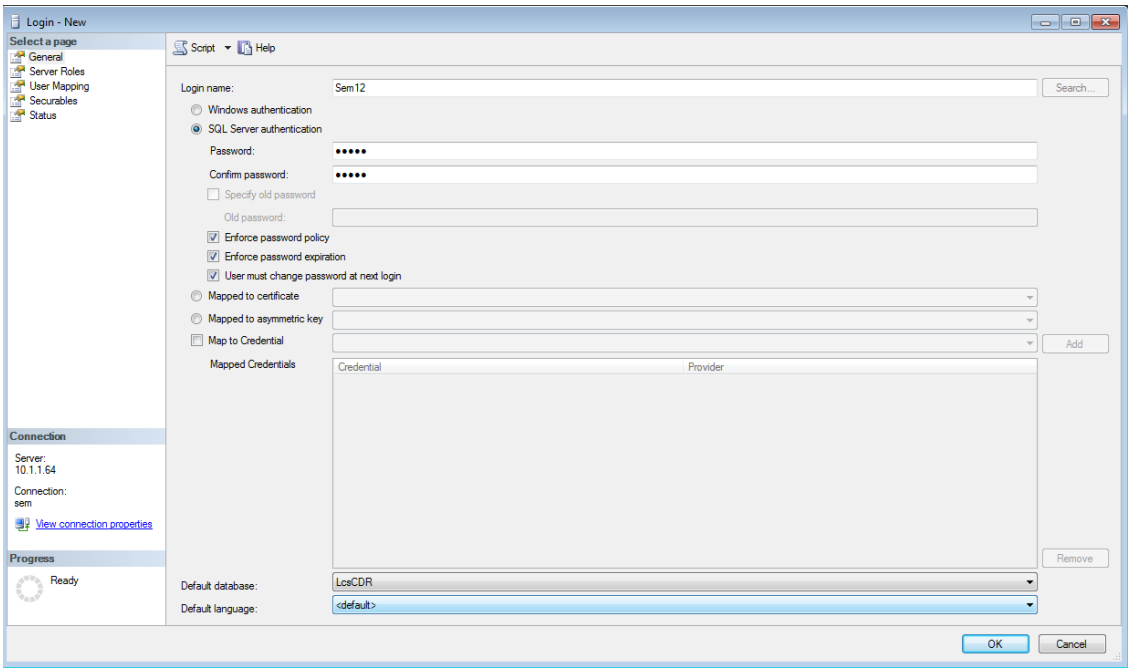
1. In the 'Security' folder, right-click **Logins** and select **New Login**.

Figure 12-1: New Login



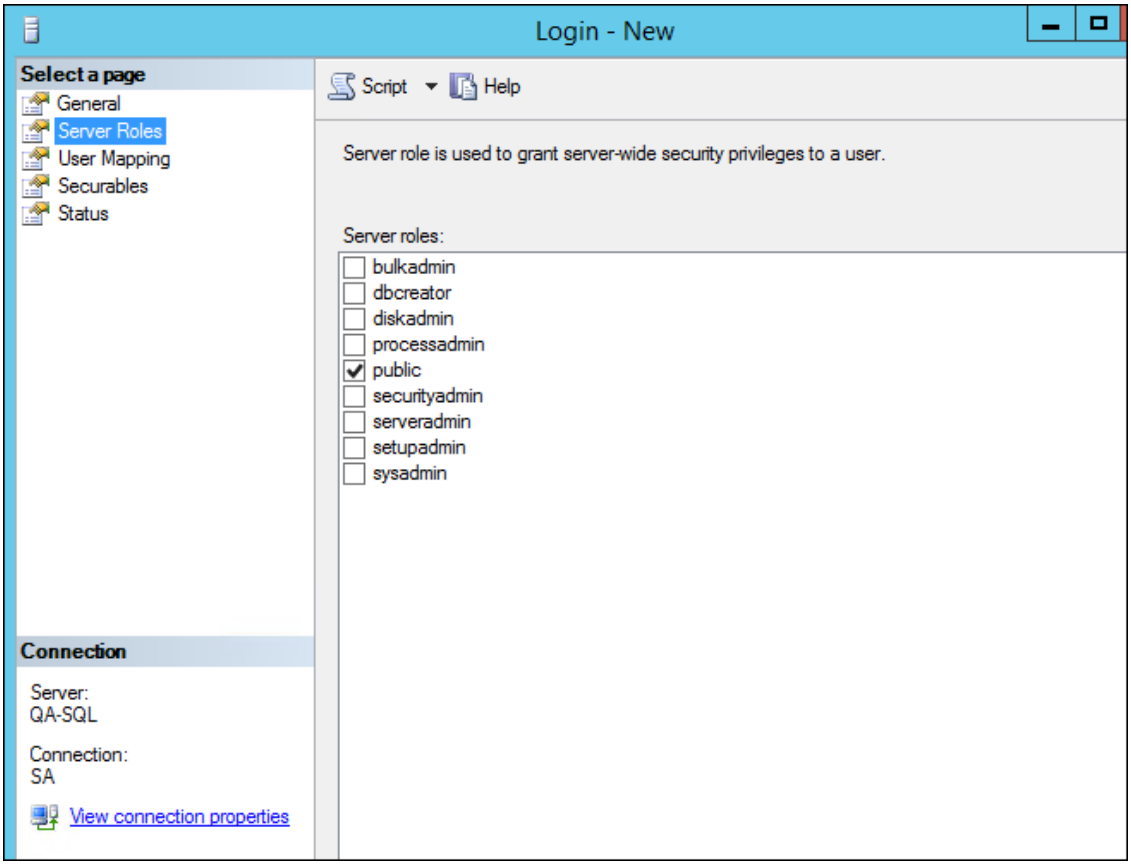
2. Under 'General', enter the Login name, select the **SQL server authentication** option, enter and confirm the password, from the 'Default database' drop-down select the default database to log in with, and then click **OK**.

Figure 12-2: SQL Server Authentication



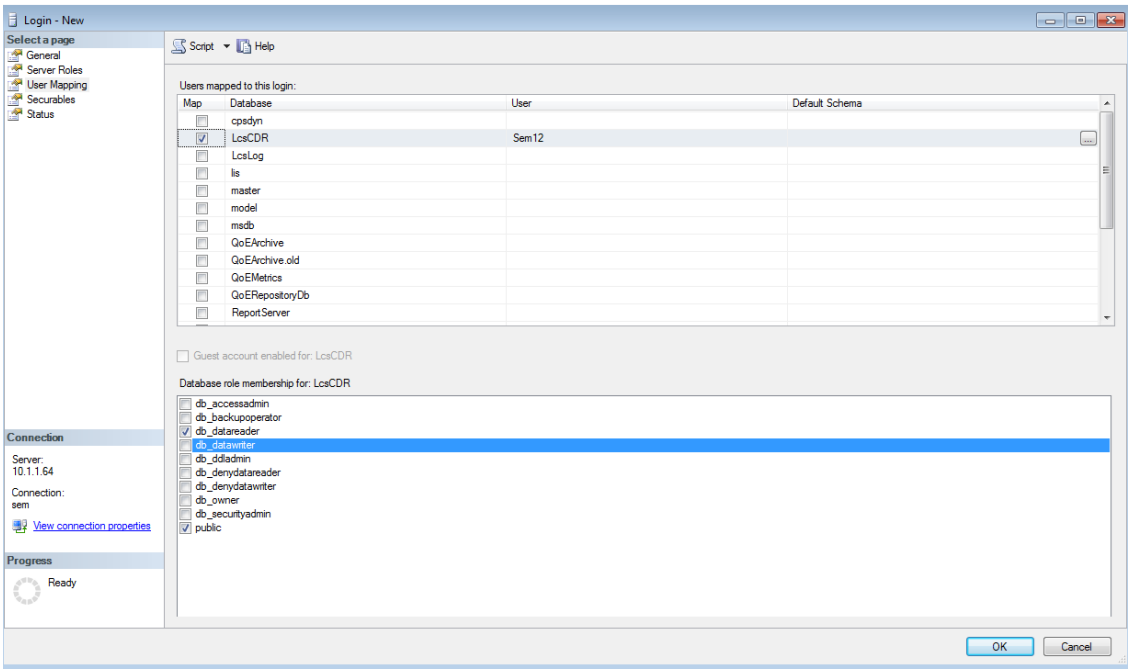
3. Under 'Server Roles' shown in the following figure, select **public**.

Figure 12-3: Login Properties – Servers Role - public



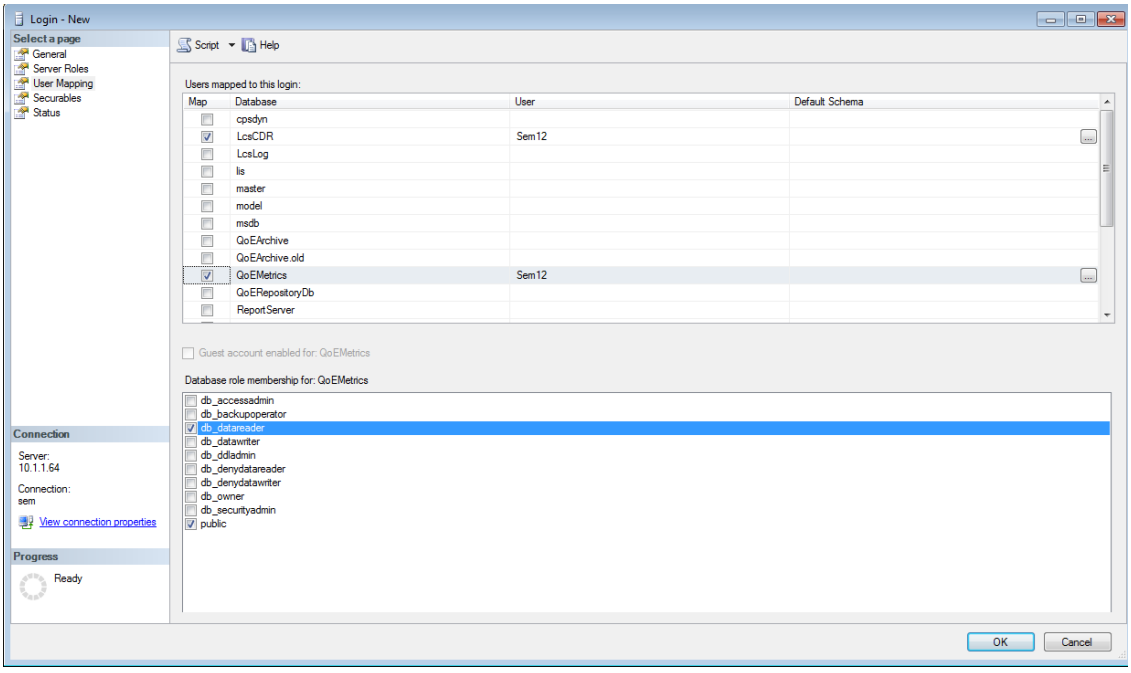
4. Under 'User Mapping' shown in the following figure, in the 'Users mapped to this login' pane, select **LcsCDR** and in the 'Database role membership for LcsCDR' pane, select **db_datareader** and **public**.

Figure 12-4: Login Properties – User Mapping – db_datareader | public



5. 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**.

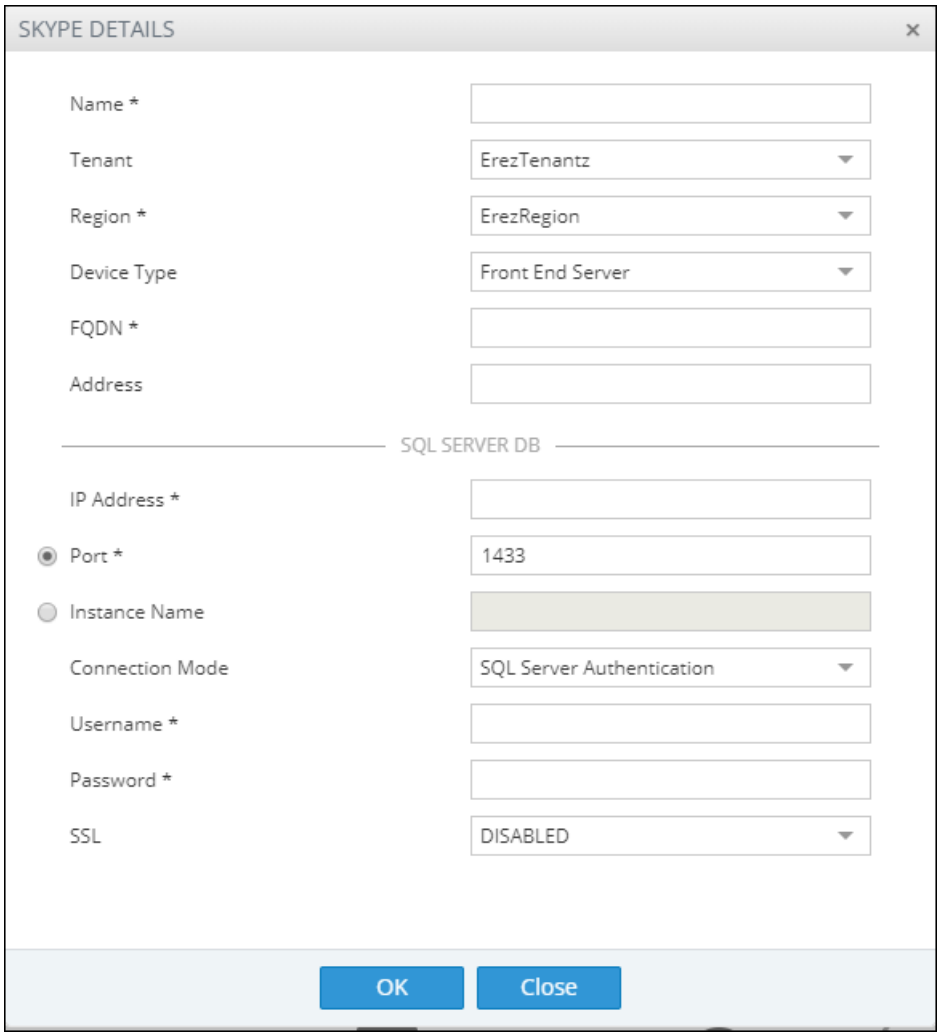
Figure 12-5: User Mapping – QoEMetrics - db_datareader | public



The SQL server side is now ready.

6. In the OVOC, under 'Network', click **Add** and then select **Skype Device**.

Figure 12-6: Skype Details



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/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

©2021 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, AudioCodes Meeting Insights, AudioCodes Room Experience 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-92005