

One Voice Operations Center

Version 8.2



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: January-03-2024

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes



Related Documentation

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

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

LTRT	Description
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.
92007	Stack Manager. Voice.AI Gateway. RXV80. User Management Pack (UMP). Maximum Storage Period. VoiceAI Connect. # of calls with and / or without Call Flow (SIP Ladder) to store. Packet Capture (PCAP) file. Operator Authentication with SAML. Customizing Max Storage Period. WebSocket tunnel. Changed GUI for floating usage.
92008	(8.0.3000) Calls Call Details pages. Statistics Graphs. Label customer / create OVOC link using Domain. Call Flow page's message info windows can be resized. Dashboard: New Features, content, UI changes and sync with portal. Merge calls into a single call. Privacy Mode: Number of concealed digits. Filter by Call ID. New look and feel. SBC/GW full backup.
92009	(8.0.3000 Fix 1) Note to Adding a Teams device. New 'Trends Statistics Comparison' report metrics.
92010	(8.2) SBA via RDP. Login screen. Topology report file download. Adding MS Teams device - xref to IOM.
92012	(8.2.1000) SSO to Device Manager. Alarm forwarding to REST API. Vulnerability findings in OVOC 8.0.3106. Increased # of counter value from 10000 to 25000 while fetching PM reports.
92013	[8.2.2000 and 8.2.3000] Management Scope - Global vs Operator. Migrating private data. Tenant Privacy Management (Tenant Details > Privacy Mode). UX app. 'Monitoring Links' operator - new capabilities. Analytics Report Module. Auto-Positioning Nodes in Network Topology. Customizing Dashboard per Operator Type Security Level. Operator Security Permissions. Log Levels. CLM note re. Floating License if WebRTC or SIPREC≠0. Links Monitor.

LTRT	Description
	[8.2.3000] SIP Ladder. Changed screens: Replaced login, main and filters. Additional SBC information. Operator login from IPs, support subnets. New filters in Alarms page. Forward Journal Events. Alarm forwarding during specific hours. Failed call labeling. Support SIP ladder pcap multipart format. UI new columns selection per table. New UI design.
92014	[8.2.3000 fixes] Determining if Reason for Call Termination is SBC-GW or 3rd Party. Restarting a Device. Resetting Redundant.

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
	Saving your Workspace	9
	Getting Acquainted with the Dashboard	10
	Getting Acquainted with the Network Topology Page	16
	Hovering Over a Cluster to Display Information	31
	Hovering Over a Device to Display Information	32
	Hovering over a Link to Display Information	33
	Returning to 'Home' Page by Clicking the OVOC Logo	33
	Auto-Positioning Nodes in the Network Topology Page	33
	Getting Acquainted with the Network Map Page	35
	Configuring Operator Authentication	40
	Configuring Operator Authentication Centrally using an LDAP Server	41
	Configuring Operator Authentication Centrally with a RADIUS Server	44
	Viewing Operator Authentication in the 'Welcome' Window	45
	Testing Connectivity with the LDAP / RADIUS Server	46
	Configuring Operator Authentication Centrally with Azure Active Directory	46
	Logging in as an Azure User with Multi Factor Authentication	49
	Configuring Operator Authentication with SAML	51
	Configuring Operator Authentication Locally, in OVOC	53
	Global vs. Tenant Scope	55
	Selecting a Scope: Global vs. Tenant	55
	Operator Security Permissions	57
	Adding a 'System' Operator	58
	Editing a 'System' Operator	63
	Deleting a 'System' Operator	63
	Deleting Multiple Operators	63
	Suspending a 'System' Operator	63
	Releasing a Suspended 'System' Operator	63
	Forcing a Password Change	64
	Forcing an Operator Logout	64
	Adding a 'Tenant' Operator	65

Editing a 'Tenant' Operator	70
Deleting a 'Tenant' Operator	71
Deleting Multiple Operators	71
Suspending a 'Tenant' Operator	71
Releasing a Suspended 'Tenant' Operator	72
Forcing a Password Change	72
Forcing an Operator Logout	72
3 Configuring System Settings	74
License Management	76
Loading the OVOC Server License	77
System License Allocations	78
Security Management	78
OVOC Server Management	79
Determining OVOC Server Status	79
OVOC Server Info	80
Securing Connections with FQDN or IP Address	81
Configuring Device Manager FQDN	82
Perform Auto-Detection using Devices FQDN Hostname	83
Configuring Privacy Mode, Concealing Users Calls Details	84
Determining Operator Behavior with OVOC's UX App	85
Uploading a Global Logo to Display in Report Results	86
Providing a Description to be Forwarded in Alarm Info	86
Viewing Calls Status	88
Viewing Log Levels	89
Configuring Templates	90
Configuring SNMP Connectivity	90
Configuring HTTP Connectivity	92
Configuring QoE Thresholds	92
Configuring QoE Status and Alarms	97
Enabling Automatic Device Backup Periodically	99
Customizing Default Dashboard per Operator Type Security Level	100
Customizing Calls Storage	101
Customizing Maximum Storage Period	106
Configuring Maximum Calls	107
Determining if Reason for Call Termination is SBC-GW or 3rd Party	108
Configuring Profiles	111
Configuring Alarms Settings	112
Adding Configuration Files to OVOC Software Manager	114
Adding a Configuration Package (ZIP) File	116
Adding the ini File	118
Adding a cmp File	119
Viewing cmp File Details in Software Manager	121
Adding a cli File	122
Adding Auxiliary Files	123

Adding X509 Certificate Files	125
Connecting Directly to External Applications	126
Device Manager	127
ARM	127
Data Layer Manager	129
Tasks tab	130
Displaying the Status of Tasks Currently Under Execution	131
4 Defining your Network Topology	133
Adding a Tenant	133
Editing a Tenant - Defining a Logo	144
Defining a Tenant Logo - Example	147
Adding a Region	151
Adding AudioCodes Devices	152
Adding AudioCodes Devices Automatically	152
Adding AudioCodes Devices Manually	157
Enabling Initial Connection Provisioning	163
Before Enabling the Feature	164
Enabling the Feature	165
Making Sure First Time Provisioning was Successful	165
Adding a Generic Device Manually	168
Adding a Microsoft Teams Device Manually	169
Adding a Microsoft Skype for Business Device Manually	172
Backing up a Device's Configuration using Backup Manager	176
Manually Backing up a Device's Configuration	176
Saving the Last Backed-up Configuration to your PC	178
Restoring the Last Backed-up Configuration to the Device	179
Adding Links	179
Adding Sites	184
Managing Endpoints	185
Dynamic Allocation of Endpoint Licenses	185
Configuring Endpoints	186
Monitoring Endpoints Status	187
Removing Endpoints from QoE Support	187
Adding an Endpoints Group	187
Adding a Topology Group	191
5 Managing SBC Licenses	193
Adding an SBC to the Floating License	195
Performing Floating License Actions	199
Unmanage	199
Update	200
Reset	200
Register	201
Configuring OVOC-Floating License Service Communications	201

Cloud License	202
Configuring a Cloud License	204
Viewing Floating License Summaries	206
Saving a Usage Data Report to your PC	208
Flex Pool License	209
Configuring an Alarm Threshold Percentage for Flex Pool Mode	209
Configuring SBC Priority - Which to Take out of Service First	210
Determining License Status from Alarms	211
Determining License Status from the Network Summary	211
Migrating from Cloud Mode to FlexPool Mode	214
Fixed License Pool	215
Performing License Pool Actions	218
Applying a License to a Device from the Pool	218
Saving Fixed License Pool Data to CSV File	218
Before Performing 'Manage Device' / 'Update Device'	219
License Pool Alarms	222
6 Assessing Network Health	223
Assessing Health from the Network Summary	223
Assessing Health from the Network Topology Page	227
Filtering to Access Specific Information	231
Filtering by 'Time Range'	232
Filtering by 'Topology'	243
Filtering the Device Floating License Page	246
Filtering by 'Status'	250
Filtering by 'More Filters'	252
Filtering by 'Groups'	252
Determining Network Health from Alarms	254
Configuring Alarm Settings	254
Monitoring Active Alarms to Determine Network Health	254
Performing Management Actions on Active Alarms	254
Filtering by 'Severity'	256
Filtering by 'Source Type'	259
Filtering by 'More Filters'	260
Filtering by 'Type'	262
Filtering by 'Alarm Names'	264
Viewing Journal Alarms to Determine Operator Responsibility	264
Filtering the Alarms Journal by 'More Filters'	265
Viewing History Alarms	268
Filtering by 'Type'	270
Filtering by 'Alarm Names'	271
Forwarding Alarms	272
Configuring when Forwarding will be Active	278
Forwarding Alarms whose Destination Type is 'SNMP'	281
Forwarding Alarms whose Destination Type is 'Mail'	284

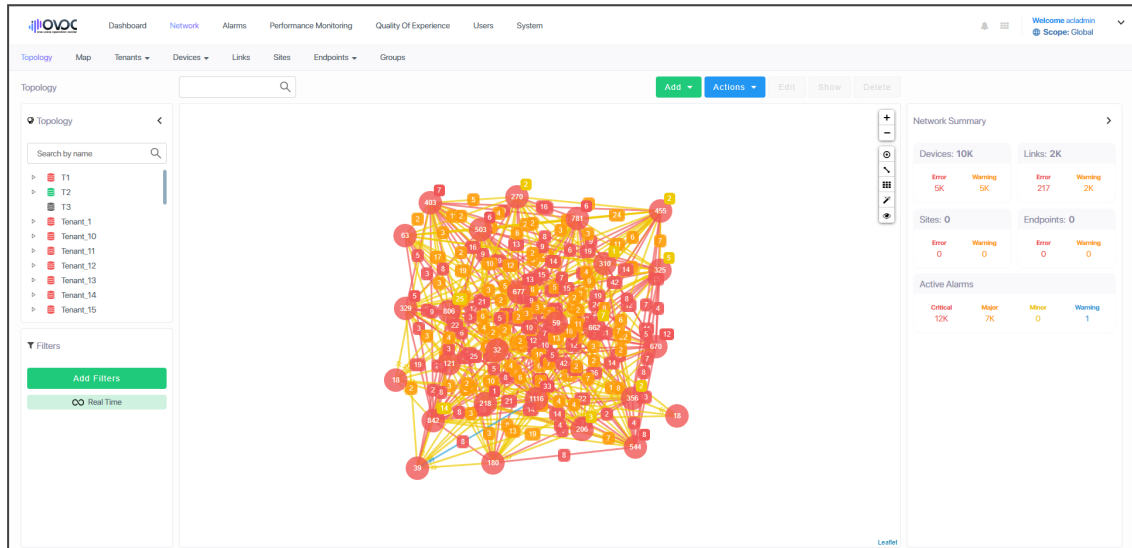
Forwarding Alarms whose Destination Type is 'Syslog'	286
Forwarding Alarms whose Destination Type is 'Notification'	289
Forwarding Alarms whose Destination Type is 'REST'	292
Viewing the New Rules in the Alarms Forwarding Page	295
Forwarding Journal Activity	295
Assessing Network Health in the Statistics Pages	300
Viewing Statistics on Calls over Devices	300
Metrics Bar Charts	302
Statistics Summary	305
Viewing Statistics on Streams over Links	305
Viewing Statistics on Calls over Sites	306
Viewing Statistics on Calls over Endpoints	306
Monitoring Performance	306
Adding a PM Template	307
Adding a PM Profile	312
Starting and Stopping PM Polling	317
Viewing PM Data Resulting from Polling	318
Displaying Analytics	327
7 Managing your Network	334
Performing Management Actions	334
Updating Firmware	335
Updating Firmware on Multiple Devices	338
Updating Firmware on a Component in a Media Cluster	338
Restarting a Device	341
Locking or Unlocking a Device	342
Populating Links	343
Moving a Device	345
Backing Up	345
Restoring the Last Backup	346
Setting Configuration Factory Defaults	348
Saving a Device's Configuration File to Flash Memory	348
Saving a Device's Configuration File to the PC	348
Resetting Redundant	349
Performing Switchover	350
Changing Profile	350
Showing Device Information	352
Showing Link Information	355
Showing User Information	356
Editing a Device	358
Deleting a Device	358
Taking a Device Inventory	358
Resetting a Device	361
Refreshing a Device's Pool License	362
Connecting via RDP to Windows-based AudioCodes Products	362

Connecting to UMP via RDP	362
Connecting to SBA via RDP	364
Managing VoiceAI Connect	366
Managing Stack Manager	367
Monitoring Device-Level Backup and Performing Rollback	370
8 Obtaining Quality Statistics on Calls	371
Accessing the Calls List	371
Filtering by 'Active Directory'	374
Filtering by 'Quality'	376
Filtering by 'More Filters'	378
Showing Call Details	382
Details of a Call across Multiple Devices with Same Correlated ID	382
Details of a Call Made over an AudioCodes SBC	384
Media	385
Signaling	388
Trends	390
SIP Call Flow	391
Details of a Test Call Made over an SBC	395
Call Details Page – Debug File Button	397
Call Details Page - PCAP File	397
Details of a Call Made over Microsoft Skype for Business	399
Media	401
Signaling	404
Details of a Call Made over Microsoft Teams	405
Quality	407
Media tab	409
Network	411
Device	413
Details of a Call Made over an Endpoint Using SIP Publish	415
Media	418
Managing QoE Thresholds Profiles	421
Understanding the 3 Sensitivity-Level Profiles	421
Understanding How Call Color is Determined	422
Link Profile as Determinant	422
MOS Metric as Determinant	423
Adding a QoE Thresholds Profile per Tenant	424
Editing a QoE Thresholds Profile	428
Deleting a QoE Thresholds Profile	429
Managing QoE Status and Alarms	430
Adding a QoE Alarm Rule per Tenant	430
Editing a QoE Alarm Rule per Tenant	433
Deleting a QoE Alarm Rule	433
9 Getting Information on Users Experience	435
Adding an Active Directory to OVOC	435

Editing an Active Directory	439
Deleting an Active Directory	441
Synchronizing AD Users with the Server	441
Assessing Overall End Users Experience	441
Assessing a Specific End User's Experience	443
Filtering the Users Experience Page	444
Managing End Users	446
Filtering the User Details Page	447
10 Managing Reports	449
Using a Predefined Report	453
Defining # of Administrator-Defined Reports Produced at System Level	462
Defining a Report	463
Selecting a Metric	470
Viewing a Defined Report	479
Editing a Report	480
Performing Actions on Reports	480
Displaying Report Results	481
'Element (Entity) Statistics' Report Type	482
'Aggregated Statistics Trends' Report Type	484
Viewing a Snapshot of all Reports Statistics	485
Viewing Schedulers and Reports Executed by them	486
Adding a Report Scheduler	488
Editing a Defined Scheduler	491
Showing a Scheduled Report's Results	491
11 AudioCodes IP Network Telephony Equipment	493
12 Adding an Unprivileged User to MSSQL Server	502

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.



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.

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.

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

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, 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.

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, 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 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.

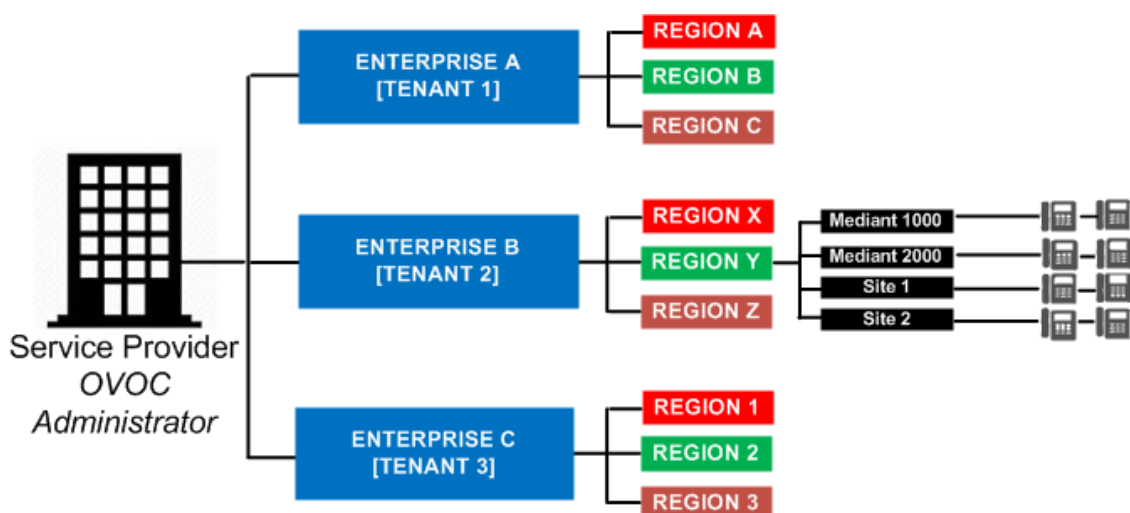
Network Architecture

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 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).

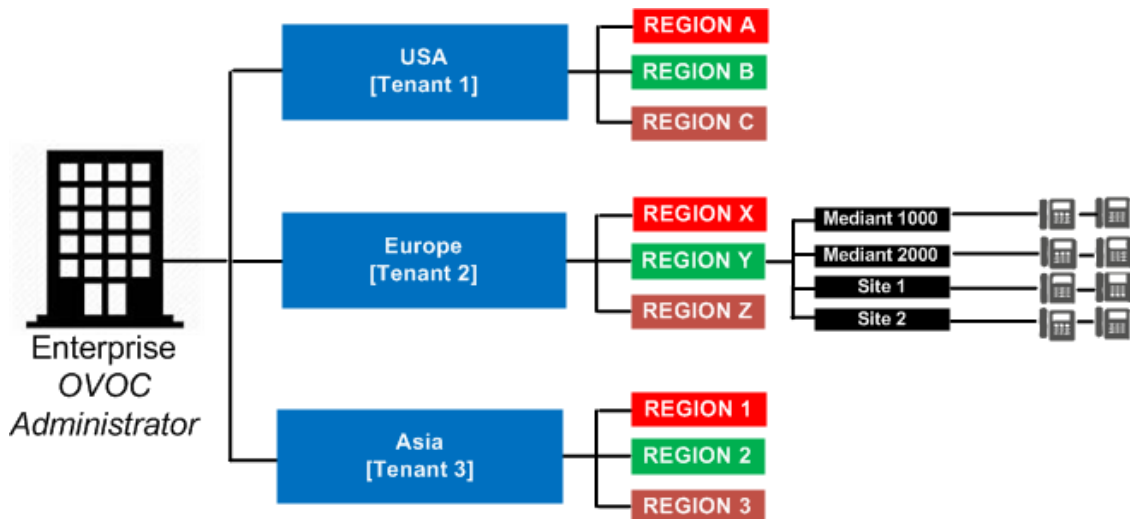


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

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 1-1: Enterprise Multi-Tenancy Architecture

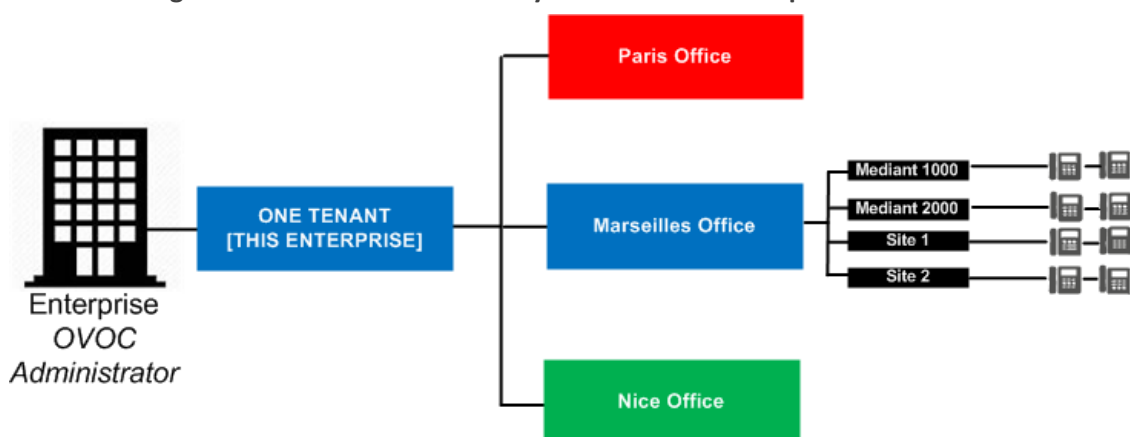


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

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 1-2: Non Multi-Tenancy Architecture - Enterprise



Elements in Multi-Tenancy Architecture

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

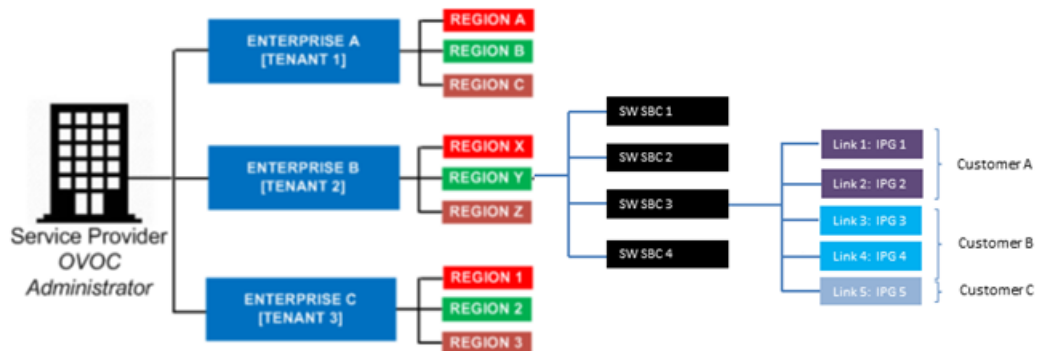
Element	Description
System	An ITSP managing multiple enterprises using a cloud-based or hosted 'global' OVOC application.
Tenant	<ul style="list-style-type: none"> ■ An ITSP's enterprise customer, using only a portion of the OVOC resources and only some of the OVOC entities. Other tenants (the ITSP's 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	<p>Any element which can be managed or used as a whole:</p> <ul style="list-style-type: none"> ■ 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	<p>Any element that can be partly managed/assigned:</p> <ul style="list-style-type: none"> ■ 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 1-3: 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.



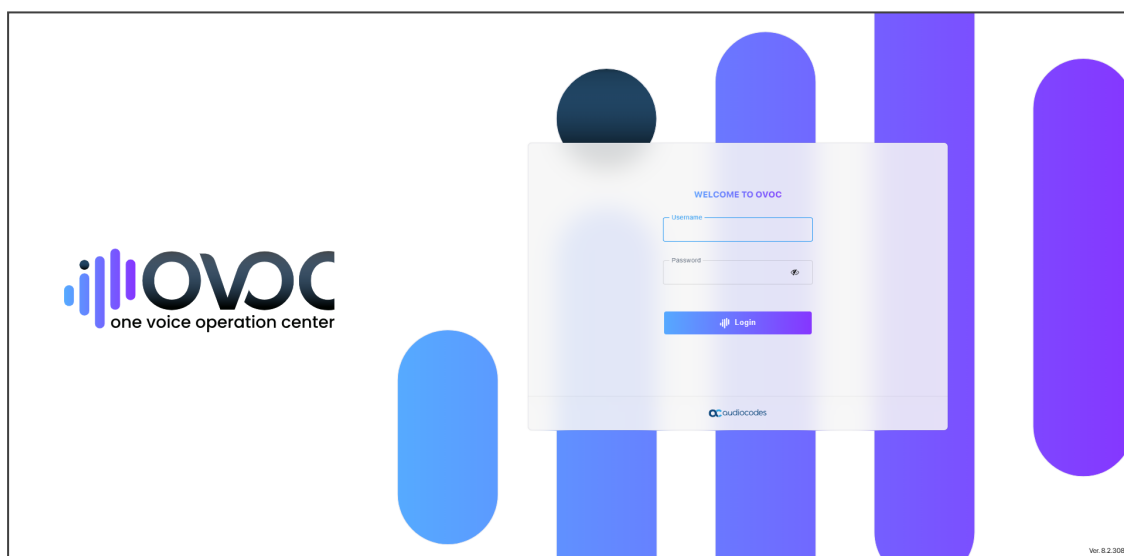
- Before getting started, make sure you have a correct OVOC license.
- For detailed information about the OVOC Server License, see [Loading the OVOC Server License](#) on page 77.

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.



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.



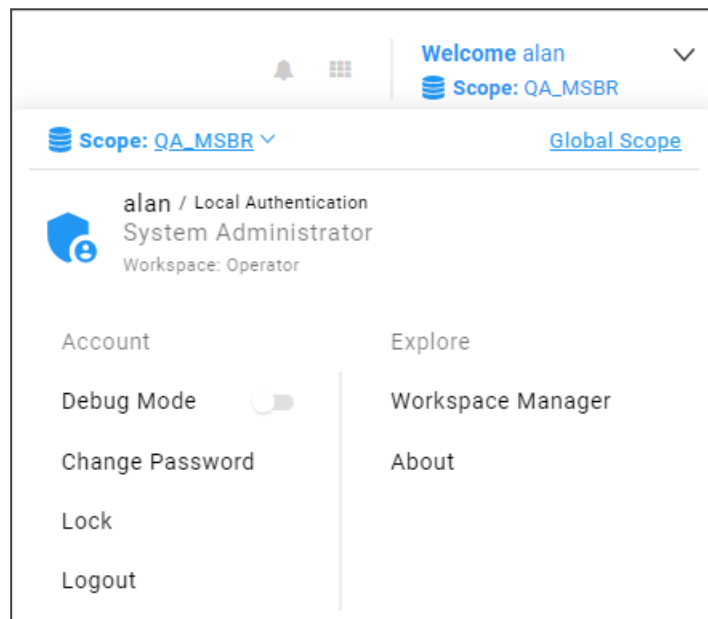
- It's recommended to change the password after initial login.
- If the operator attempting to log in is an Azure operator and if Multi Factor Authentication is enabled in the Azure configuration for this operator, see [here](#) and [here](#).

Saving your Workspace

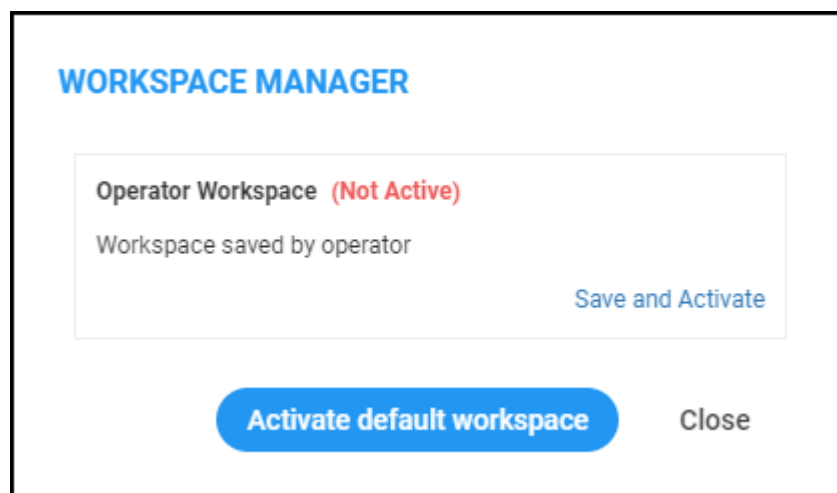
Operators can save their workspace, i.e., they can save their GUI contexts such as filters, Network Map zoom positions, column widths, etc. The feature can be enabled manually or automatically. After logging out or after the browser is closed, all saved GUI contexts are retrieved the next time the operator logs in. Best practice is to save the workspace you're currently performing operations in, so re-accessing it is quick and effortless.

➤ **To save a workspace:**

1. In the page (workspace) you're currently working in, click the **Welcome <user-name>** dropdown menu in the upper right corner.

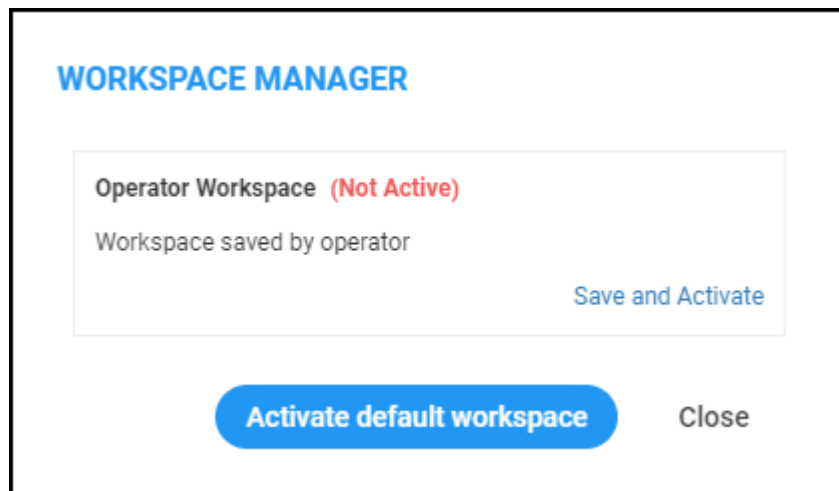


2. Click the **Workspace Manager** option.



3. Click **Save** and then click **Activate**.

4. If the Workspace has never been saved before it's your first use of this feature, **Save and Activate** will be displayed:

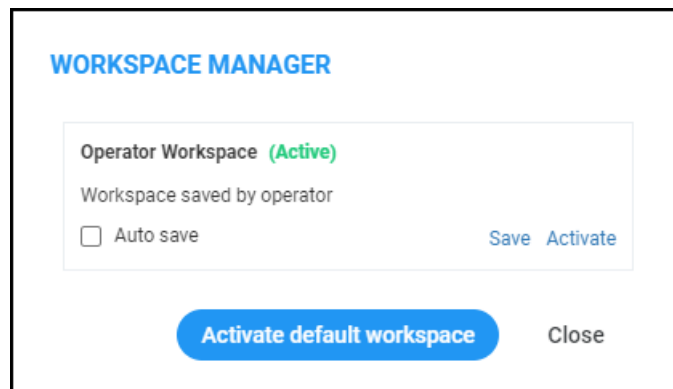


5. Click **Save and Activate**.
6. In the 'Confirmation' prompt, click **OK**.



You can use the **Activate default workspace** button to disable an active Workspace and to activate a clean Workspace.

7. Click again the **Welcome <user-name>** dropdown menu and click again the **Workspace Manager** option.



8. Verify that you've successfully saved the Workspace (**Active**).



Selecting the **Auto save** option gives you an easy way to keep your Workspace up to date; your workspace is automatically saved every time you make a change.

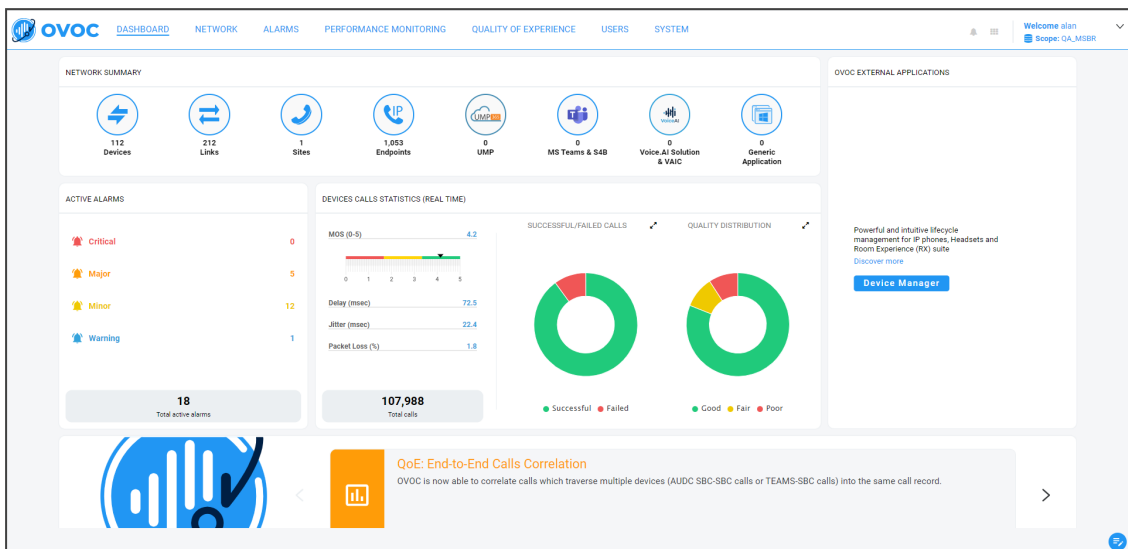
Getting Acquainted with the Dashboard

The Dashboard opens by default after logging in to 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

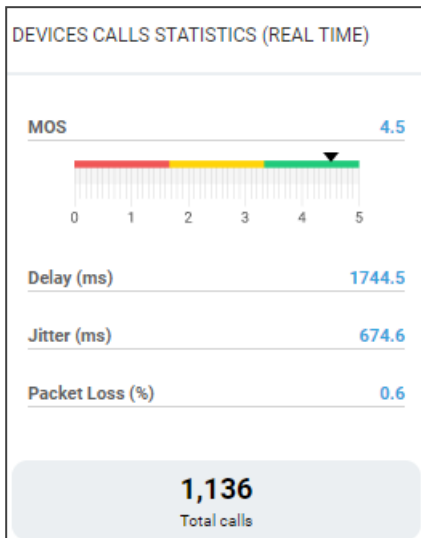
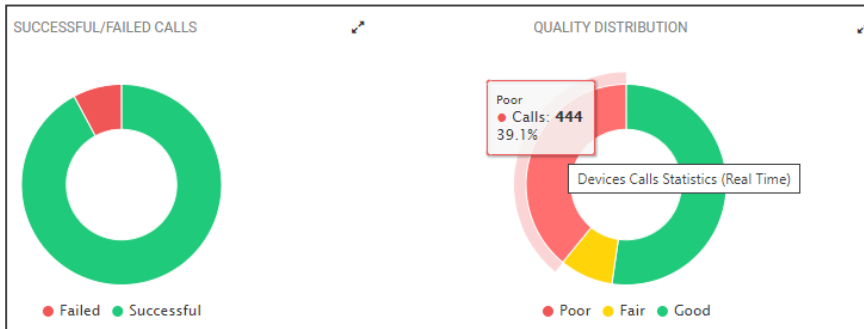
It may be helpful to get familiar with the page before getting started.



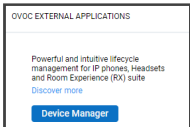
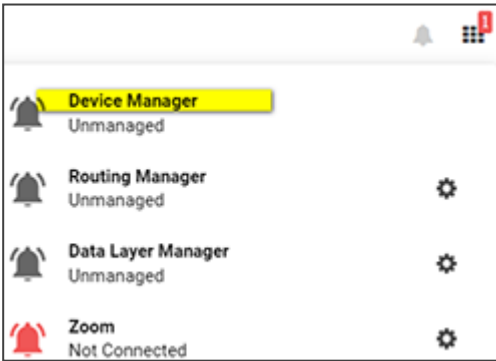






Use the following table as reference:

Cluster Icon	Description
	[Devices] Indicates the number of AudioCodes SBC / MSBR / Gateway devices currently managed by 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 OVOC. Click to access the Links page. See Adding Links on page 179.
	[Sites] Indicates the number of sites currently managed by OVOC. Click to open the Sites page. See Adding Sites on page 184
	[Endpoints] Indicates the number of endpoints currently managed by OVOC. Click to open the Endpoints page. See Monitoring Endpoints Status on page 187.
	[UMP] Indicates the number of User Management Packs (UMPs) 365 currently managed by OVOC. For more information about the AudioCodes UMP 365, see under AudioCodes IP Network Telephony Equipment on page 493.
	[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 OVOC. Click to access the Device

Cluster Icon	Description												
	Management page.												
<div> 0 Voice.AI Solution & VAIC</div>	[VoiceAI Solution and VAIC]. Indicates the number of AudioCodes VoiceAI solution entities and Voice AI Connect entities currently managed by OVOC. Click to directly access the Device Management page. The page will also display AudioCodes' SmartTAP Application server. SmartTap 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.												
<div> 0 Generic Application</div>	[Generic Application] Indicates the number of Generic Application entities, for example, AudioCodes' Survivable Branch Appliances (SBAs) for Microsoft Teams, currently managed by OVOC. Click to access the Device Management page.												
Active Alarms	<div>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.</div> <div><div>ACTIVE ALARMS</div><table><tr><td></td><td>Critical</td><td>120416</td></tr><tr><td></td><td>Major</td><td>16</td></tr><tr><td></td><td>Minor</td><td>0</td></tr><tr><td></td><td>Warning</td><td>0</td></tr></table><div><div>120,432</div><div>Total active alarms</div></div></div> <div><div>Clicking the total number of active alarms in the network opens the Active Alarms page.</div><div>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</div></div>		Critical	120416		Major	16		Minor	0		Warning	0
	Critical	120416											
	Major	16											
	Minor	0											
	Warning	0											

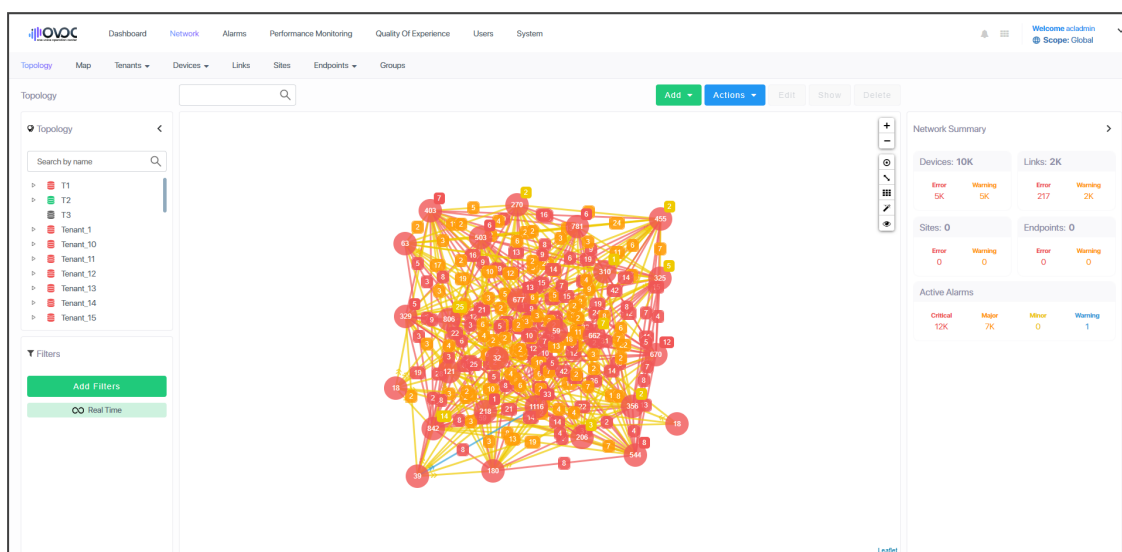
Cluster Icon	Description
	details.
Devices Calls Statistics (Real Time)	<p>■ Indicates (1) the total number of calls, in real time and (2) the average MOS, Jitter, Delay and Packet Loss (%) scores:</p> <div data-bbox="528 427 951 963"> <p>DEVICES CALLS STATISTICS (REAL TIME)</p>  </div> <p>✓ Click 'Total calls' to access the Statistics-Aggregated QoE page, displaying QoE statistics on all calls.</p> <p>■ Below left: Successful / Failed Calls</p> <p>■ Below right: Quality Distribution (Good, Fair, Poor)</p> <div data-bbox="520 1207 1388 1534">  </div> <p>✓ Position your mouse above a pie segment to view QoE details.</p> <p>✓ [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.</p> <p>✓ [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</p>

Cluster Icon	Description
	<p>tab that opens.</p> <p>Constantly provides operators new updates and features from the OVOC server. To view each new update feature, click the > icon displayed on the right. To go back, click the < icon then displayed on the left. To access an update feature, click the Discover More link.</p> <p>To receive dynamic updates, the OVOC Web client must have access to AudioCodes' portal.</p> <p>URL: https://ovoc.blob.core.windows.net/default/ovoc.json</p> <p>If this is not possible, customers are presented with the latest features released in the version they currently have.</p>
 External Applications	<p>Each external application described next opens in a separate browser tab or browser window depending on the operator's browser settings. As described next, the Device Manager is directly accessed via SSO.</p>
	<p>Click the button for the OVOC to perform a Single Sign-On (SSO) to the Device Manager and directly access IP phones and meeting room devices. The Device Manager is the AudioCodes lifecycle management tool for AudioCodes IP phones and EPOS and Jabra headsets and speakers.</p> <p>Opening the Device Manager from the External Applications menu (see previous description) is also performed via SSO.</p> 
Routing Manager	<p>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 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</p>

Cluster Icon	Description
	<p>simply and rapidly.</p> <p>Note that the icon is never disabled even when the ARM is disconnected; if the ARM is disconnected, the AudioCodes website page related to the ARM opens instead.</p>
Data Layer Manager	<p>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.</p>
Notifications 	<p>Notifications can be configured to pop up in the uppermost right corner when a task is performed or when an alarm is received. The bell icon indicates the number of notifications that have not yet been viewed; the color indicates highest alarm severity level. Clicking the bell opens the notifications list. In the list, operators can delete a notification, delete all notifications or click a notification to open the Tasks page or Alarms History page. The display time can be changed. The feature can be switched off.</p>
	<p>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.</p> <div data-bbox="529 1205 1050 1305">  <p>OVOC Advanced Quality Package license is missing.</p> </div> <p>Clicking the icon opens details about how to troubleshoot the issue.</p> <div data-bbox="529 1370 1402 1682"> <div>ADVANCED QUALITY PACKAGE MISSING ×</div> <p>You are using Quality Monitoring without OVOC Advanced Quality Package license. Please contact your local distributor to purchase the OVOC Advanced Quality Package license.</p> <div>OK</div> </div>
	<p>Located in the lowermost right corner of the Dashboard, this icon allows operators to customize the Dashboard and rearrange elements to suite preferences by clicking-and-dragging.</p>

Getting Acquainted with the Network Topology Page

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







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.







Entity	Icon	Explanation
Tenant	<div><div>▶  OVOC-QA-TEAMS</div><div>▶  Simulator-TEAMS</div><div>▶  Tring</div></div>	<p>For detailed information about multi-tenancy architecture, see ITSP Multi-Tenancy Architecture on page 3.</p> <p> = Tenant status is Error when one or more of the following exists:</p> <ul style="list-style-type: none">✓ management status of at least one region is Error✓ voice quality status of at least one region is Error

Entity	Icon	Explanation
		<ul style="list-style-type: none"> ✓ 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. <p> = Tenant status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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 <p> = Tenant status is OK when all of the following exist:</p> <ul style="list-style-type: none"> ✓ 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 <p> = Tenant status is Unmonitored when all of the following exist:</p> <ul style="list-style-type: none"> ✓ management status of all regions is Unmonitored ✓ voice quality status of all regions is Unmonitored



Entity	Icon	Explanation
		<ul style="list-style-type: none"> ✓ license status of all regions is Unmonitored
Region		<p> = Region status is Error when one or more of the following exist:</p> <ul style="list-style-type: none"> ✓ 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 <p> = Region status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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 <p> = Region status is OK when all of the following exist:</p> <ul style="list-style-type: none"> ✓ 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 <p> = Region status is Unmonitored when all of the following exist:</p> <ul style="list-style-type: none"> ✓ management status of all devices and sites is Unmonitored ✓ voice quality status of all devices and sites is Unmonitored ✓ license status of all devices and sites is Unmonitored

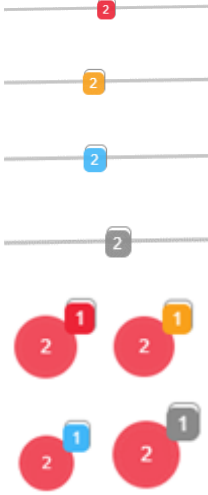

Entity	Icon	Explanation
Device	  	<p>Indicates an SBC belonging to AudioCodes communicating with OVOC.</p> <p>Red = Device status is Error when one or more of the following exist:</p> <ul style="list-style-type: none"> ✓ management status is Error (if device alarms status or connection status is disconnected) ✓ 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 <p>Orange = Device status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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) <p>Blue = Device status is OK when all of the following exists:</p> <ul style="list-style-type: none"> ✓ 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) ✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) <p>Strikethrough = locked No strikethrough = unlocked</p>

Entity	Icon	Explanation
UMP	  	<p>Indicates the AudioCodes User Management Pack 365 communicating with OVOC.</p> <p>Red = UMP status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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 <p>Orange = UMP status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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) <p>Blue = UMP status is OK when all of the following exist:</p> <ul style="list-style-type: none"> ✓ 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) ✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) <p>Strikethrough = locked No strikethrough = unlocked</p>

Entity	Icon	Explanation
Microsoft Skype for Business Device		 = Microsoft Skype for Business Mediation Server  = Microsoft Skype for Business Edge Server  = Microsoft Skype for Business Front End Server
Generic Device		<p>Indicates a non-AudioCodes device or entity that is also part of the OVOC network topology: IP PBX (shown on left), SIP trunk, other vendors' SBC / gateway. These devices participate in processing OVOC network calls and are connected to devices.</p>
Site		<p>Color and status are propagated from the endpoints under the site.</p> <p>Red = Site status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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 <p>Orange = Site status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 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 is no voice quality license) <p>Blue = Site status is OK when all of the following exist:</p> <ul style="list-style-type: none"> ✓ management status is OK - Clear or Undetermined (if site alarms status or connection status is OK - Clear or Undetermined)

Entity	Icon	Explanation
		<ul style="list-style-type: none"> ✓ 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) <p>Gray = Site status is Unmonitored when all of the following exist:</p> <ul style="list-style-type: none"> ✓ management status of all endpoints is Unmonitored ✓ voice quality status of all endpoints is Unmonitored ✓ license status of all endpoints is Unmonitored
Link		<p>A link joins two devices:</p> <p>Red = Voice quality status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 'Critical' Control Status ✓ 'Critical' Media Status <p>Orange = Voice quality status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ✓ 'Major' Control Status ✓ 'Major' Media Status <p>Blue = Voice quality status is OK/Clear when all of the following exists:</p> <ul style="list-style-type: none"> ✓ Control Status is OK/Clear ✓ Media Status is OK/Clear ✓ Control Status or Media Status is Unmonitored <p>Gray = Voice quality status is Unmonitored when both of these exist:</p> <ul style="list-style-type: none"> ✓ Control Status is Unmonitored ✓ Media Status is Unmonitored <p>Note:</p> <ul style="list-style-type: none"> ✓ If no voice quality license exists, status will be







Entity	Icon	Explanation
		<p>Unmonitored.</p> <ul style="list-style-type: none"> ✓ Link status does not impact device / region ✓ When the number of links exceeds 1000, only links whose <i>source and destination are within the visible bounds of the map</i> 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		<p>Indicate aggregated clusters of devices (AudioCodes devices as well as non-AudioCodes devices). The numbers indicate how many devices are in the cluster.</p> <ul style="list-style-type: none"> ■ Red = at least one entity in this cluster has a status of Error – see above in this table for the one or more conditions that need to exist for status to be Error ■ 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

Entity	Icon	Explanation
		<ul style="list-style-type: none"> 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		<p>Square icons indicate aggregated clusters of links. The link indication can be on a line representing a link (left upper) or adjoined to a device cluster (left lower). The number in each square indicates how many links are in the cluster.</p> <ul style="list-style-type: none"> 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		<p>Indicates the AudioCodes SmartTAP communicating with OVOC.</p> <ul style="list-style-type: none"> Red = SmartTAP status is Error when management status is Error (if SmartTAP alarms status or connection status is disconnected) 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:

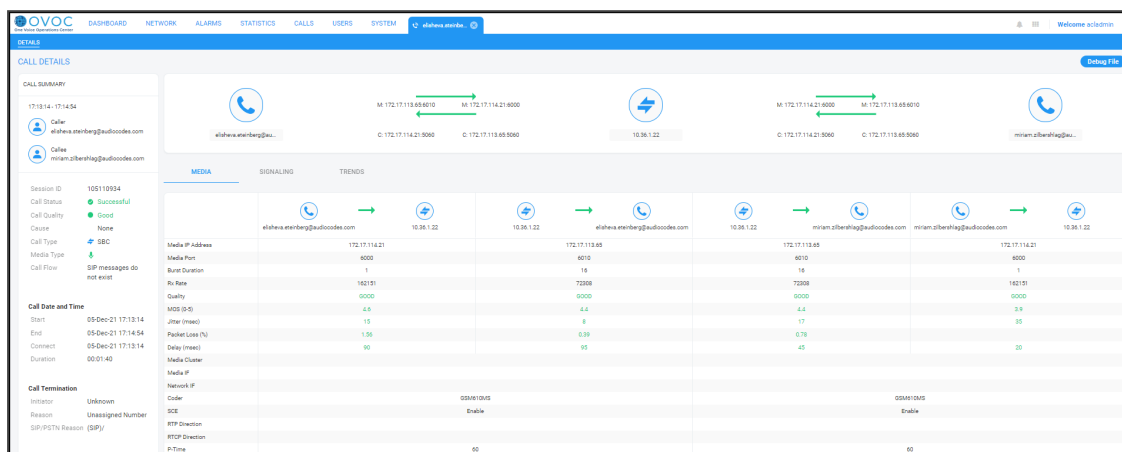
- Click + or - to zoom in or out of the map.
- Click  to center the map in the page - useful if the previous operator dragged it off center.
- Click  to create a link.
- Click  to display gridlines; the background of the page is by default white.
- Click  to determine the proximity of nodes to one another in the page. See also [here](#).
- Click  to show the labels of the links in the page; click it again to hide them; this reduces clutter for more effective management, especially in networks with many devices and links.
- Click  to not show clusters; click it again to 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 31).

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 2-1: Dynamic Tab for Fast Access to Specific Information

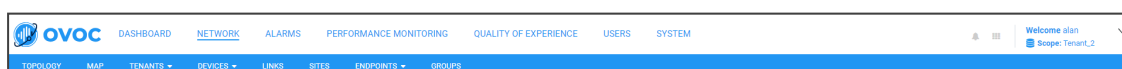


For more information about the dynamic tab that is created for call details, see [Showing Call Details](#) on page 382.

For more information about the dynamic tab that is created for user details, see [Assessing a Specific End User's Experience](#) on page 443.

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.



Use the table as reference to the figure. See also [Getting Acquainted with the Dashboard](#) on page 10.

Menu	Tab	Description
Network	Topology	<p>The tab's page lets you:</p> <ul style="list-style-type: none"> Assess at a glance the topology of the network Perform multiple configuration and maintenance actions Select multiple devices (Ctrl+) and perform multiple

Menu	Tab	Description
		<p>actions simultaneously (Ctrl+ to deselect)</p> <ul style="list-style-type: none"> ■ Select multiple links (Ctrl+) and perform multiple actions simultaneously (Shift+ to deselect) ■ Filter out unwanted information to facilitate quick access to specific information <p>The page features two 'modes':</p> <ul style="list-style-type: none"> ■ 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 231 for information about time filters.
	Map	<p>The tab's page lets you:</p> <ul style="list-style-type: none"> ■ Assess at a glance the enterprise network's global distribution ■ Filter <p>The page features two 'modes':</p> <ul style="list-style-type: none"> ■ 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 231 for information about time filters.
	Tenants	The tab lets you:
	Devices	<p>The tab lets you:</p> <ul style="list-style-type: none"> ■ Add a network component: ■ Perform a device action ■ Show device
	Links	Lets you add, edit or delete links.
	Sites	<p>Lets you:</p> <ul style="list-style-type: none"> ■ add a set of endpoints based on a network subnet

Menu	Tab	Description
		<ul style="list-style-type: none"> ■ edit or delete the SIP clients (phones)
	Endpoints	<p>From the tab's drop-down you can select:</p> <ul style="list-style-type: none"> ■ 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.
	Groups	
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 271.
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	<p>Displays the Links Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> ■ 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) <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>
	Sites	<p>Displays the Sites Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> ■ which call quality metrics to display (Successful/Failed Streams, Max Concurrent

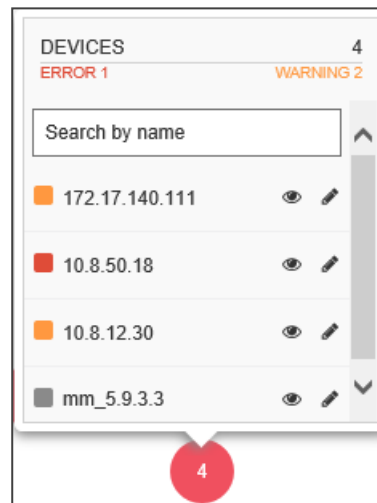
Menu	Tab	Description
		<p>Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo)</p> <ul style="list-style-type: none"> ■ which sites to display (per Topology or Time Range) <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>
	Endpoints	<p>Displays the Endpoints Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> ■ 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) <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>
	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 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.

Menu	Tab	Description
	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	<p>Calls Count, Total Duration, Success / Failed, Call Quality, MOS, Jitter, Delay, and Packet Loss.</p> <p>Gives operators network health monitoring capability, including alarms and diagnostics. Used to maximize the quality of experience (QoE) of end users in the network.</p>
	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	<p>Allows performing administration:</p> <ul style="list-style-type: none"> ■ License <ul style="list-style-type: none"> ✓ Configuration ✓ System Allocations ✓ Tenants Allocations ✓ Floating License ■ Security <ul style="list-style-type: none"> ✓ Authentication ✓ Operators ■ OVOC Server
	Configuration	<p>Allows performing OVOC administration:</p> <ul style="list-style-type: none"> ■ Templates (SNMP Connectivity, HTTP Connectivity, QoE Thresholds, QoE Status & Alarms, Perf Monitoring) ■ Alarms

Menu	Tab	Description
		<ul style="list-style-type: none"> File Manager (Software Manager) OVOC Server Device Backup
	Tasks	Only displays asynchronous actions performed by the OVOC operator.

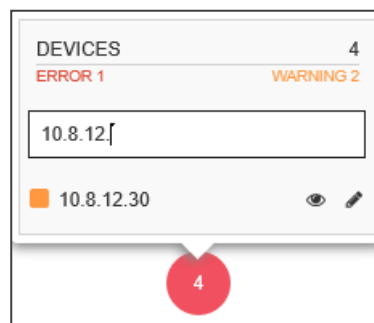
Hovering Over a Cluster to Display Information

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:



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.



The screenshot displays a network map with various devices represented by colored circles and labels. A pop-up window titled 'DEVICES' is open, showing a search bar and a list of devices. The device 'dd_10.36.41.102' is selected. To the right, the 'DEVICE DETAILS' panel is visible, showing information for the device '10.8.50.15'.

DEVICES

ERROR 0 WARNING 2

Search by name

- dd_10.36.41.102
- 10.8.50.15

DEVICE DETAILS

NAME 10.8.50.15

STATUS Warning

IP ADDRESS 10.8.50.15

SERIAL NUMBER 3074943

PRODUCT TYPE MEDIANT 1000 MSBR

HA No

QOE STATUS Unmonitored

MANAGEMENT STATUS Warning

LICENSE Ok

REGION Region1_Eva

TENANT Eva

ACTIVE ALARMS

CRITICAL	MAJOR	MINOR	INDETERMINATE
1	4	1	12

TOTAL CALLS 0 **MAX CONCURRENT CALLS** 0

MOS	JITTER	DELAY	PLOS
0	0	0	0

SUCCESSFUL/FAILED CALLS QUALITY DISTRIBUTION

Hovering Over a Device to Display Information

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

The screenshot shows a pop-up window for the device '10.36.41.15'. It displays a summary of device information and statuses. The lower bar contains icons for actions that can be performed on the device.

10.36.41.15

FQDN My.BS.LAB.QA-EMS.LOCAL

IP ADDRESS 10.36.41.15

VERSION 7.20A.251.178

SERIAL NUMBERS 10015, 9034617

PRODUCT TYPE MEDIANT 500 E-SBC

HA Yes

TENANT Zipora2

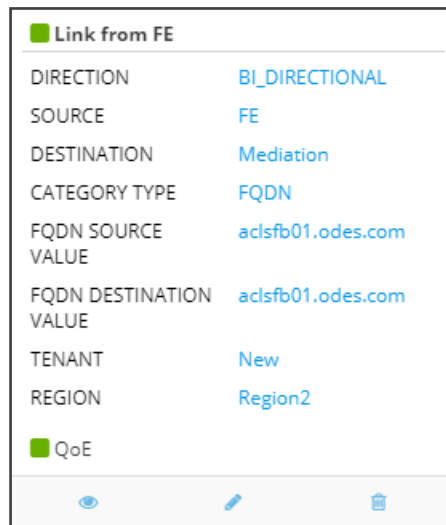
REGION Region2

Management QoE License

- 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 OVOC Logo

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



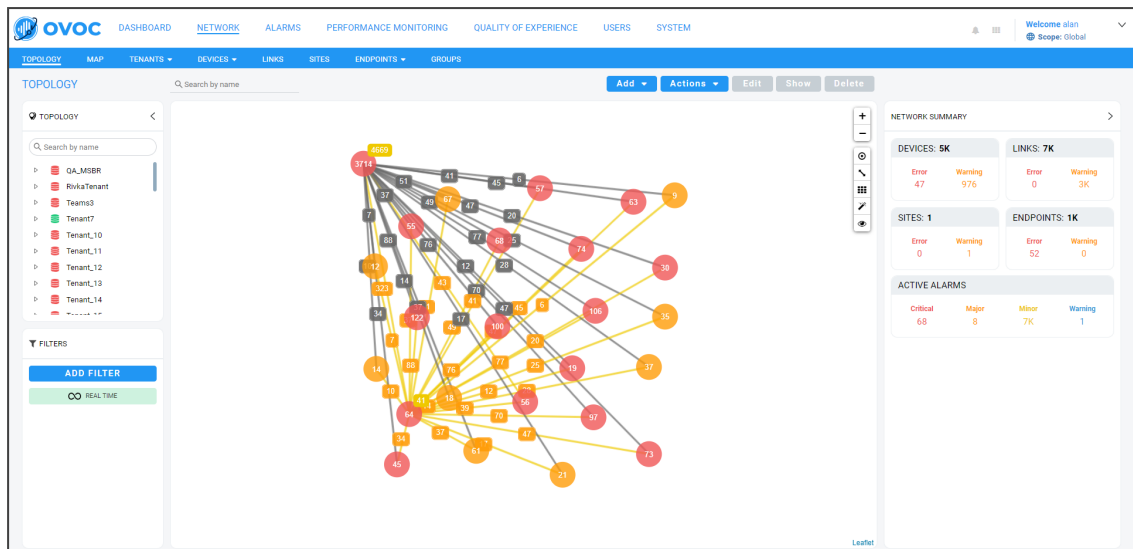
- The logo functions as a 'Home' page button.
- Click it to return to the Network Topology page from any page.
- The feature enhances quick and operator-friendly navigation in OVOC.

Auto-Positioning Nodes in the Network Topology Page

An auto-positioning feature enables operators to determine the proximity of nodes to one another in the Network Topology page. The feature can reduce congestion of displayed nodes and facilitate a more operator-friendly view.

➤ To auto-position nodes in the page:

1. In the Topology page (**Network > Topology**), click the **Auto Position** button .



2. View the Auto Generate Map dialog.

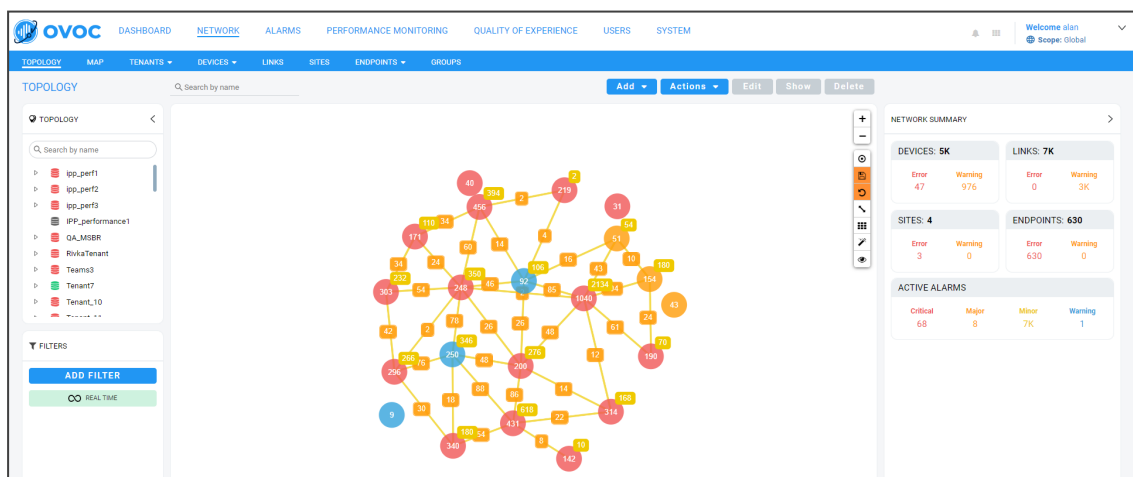
AUTO GENERATE MAP

Site/Device Proximity Value: (1)

*Please note, for large number of links/devices/sites this process may take a while.

Cancel
Generate

3. Slide the gauge to a proximity value that matches your requirements and then click **Generate**; proximity is adjusted accordingly; the higher the value set, the more space between nodes (i.e., the less proximity of nodes to one another).

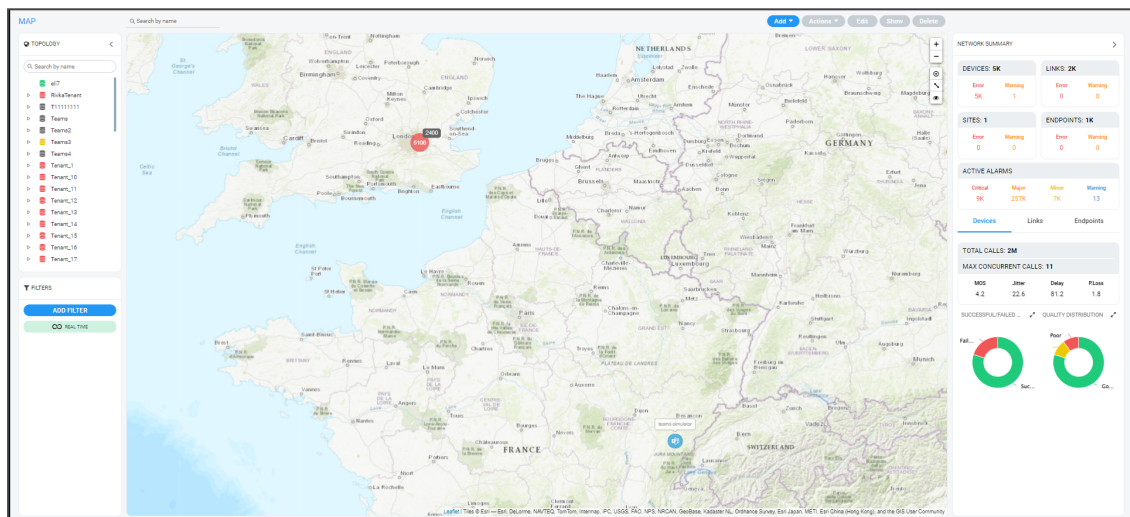




- Click the **Save Local Changes to Server** button after making a change to the network topology, for example, after dragging a device to a different location. The button is only displayed if a change is made. It's highlighted orange. After saving the change, the button disappears.
- Click the **Revert 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.

Getting Acquainted with the Network Map Page

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

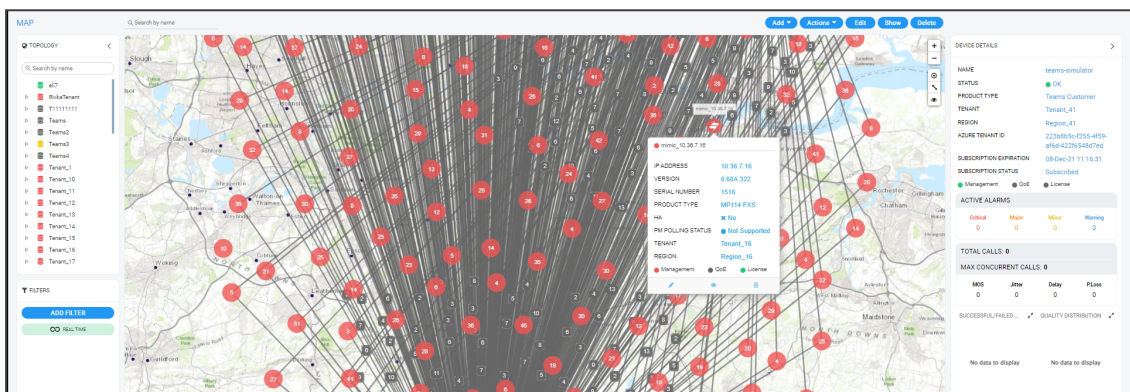


With the exception of cluster icons, entity icons in the Network Map page are identical to those in the Network Topology page described in the table [Getting Acquainted with the Network Topology Page](#) on page 16. A cluster is based on geographical locations of devices in the Network Map page. Clusters 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.

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

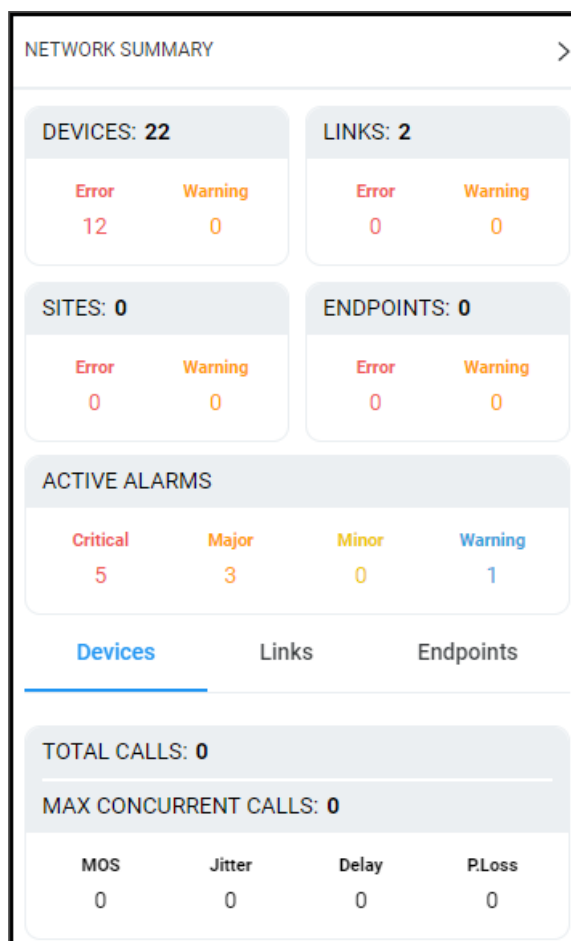
Cluster Icon	Description
	or Unmonitored. Click a cluster to zoom in and view the entities under it.
●	Cluster status is Unmonitored when the management status of all devices and sites is Unmonitored. Click a cluster to zoom in and view the entities under it.

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:



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

DEVICE MANAGEMENT													
NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	STATUS	QoS STATUS	CALLS	MAX CONCURRENT CALLS	QUALITY	SUCCESSFUL/FAILED	VERSION	MANAGEMENT	DEVICE DETAILS	
13.80.146.92-984119...	13.80.146.92	Voice AI Solution	✗	●	●					5.4.0	●	NAME	13.92.243.52
13.92.243.52	13.92.243.52	SW SBC	✗	●	●					7.40A.190.698	●	STATUS	● Error
13.95.15.193	13.95.15.193	Voice AI Solution	✗	●	●					5.4.0	●	IP ADDRESS	13.92.243.52
20.101.116.40-97603...	20.101.116.40	Voice AI Solution	✗	●	●					5.3.1	●	VERSION	7.40A.190.698
20.56.17.78-1955297...	20.56.17.78	User Manage...	✗	●	●					8.0.200.347	●	OS VERSION	OS8
20.72.207.115-74511...	20.72.207.113	SW SBC	✗	●	●					7.40A.190.320	●	SERIAL NUMBER	942270433
20.76.73.144-ca731f...	20.76.73.144	VAC	✗	●	●					3.0.001	●	PRODUCT TYPE	SW SBC
20.83.72.141-914554...	20.83.72.141	SW SBC	✗	●	●					7.40A.090.755	●	HA	✗ No
51.136.7.31	51.136.7.31	User Manage...	✗	●	●					8.0.000.237	●	PM POLLING STATUS	● Not Supported
FrontEnd		Skyline Front End...	✗	●	●						●	TENANT	OVOC-QA-TEAMS
Mediation		Skyline Mediation...	✗	●	●						●	REGION	Teams
mimic	1.1.1.1	Mediant 500 E-S...	✗	●	●					7.20A.256.808	●		

Filters: ADD FILTER, REAL TIME, STATUS: Error

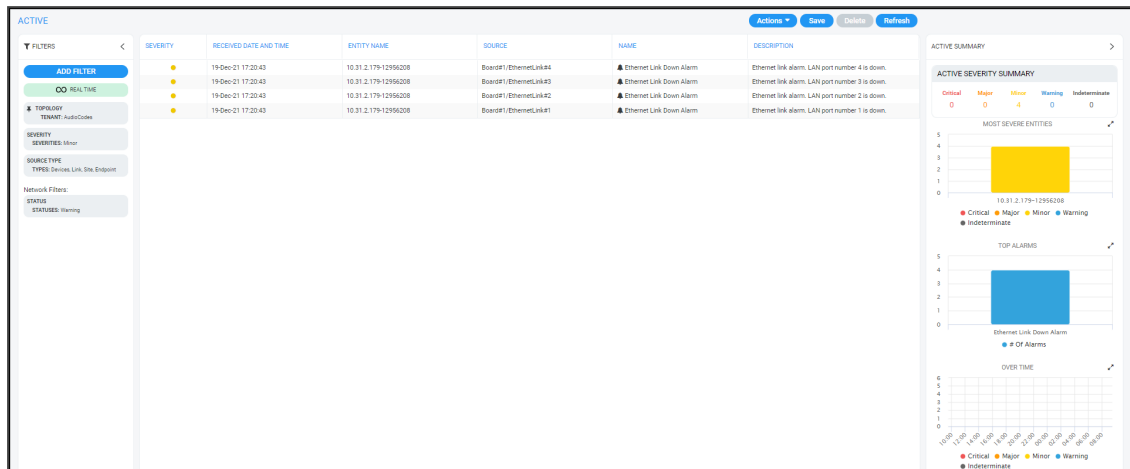
ACTIVE ALARMS: Critical 1, Major 0, Minor 0, Warning 0

TOTAL CALLS: 0, MAX CONCURRENT CALLS: 0

MOS 0, Jitter 0, Delay 0, P.Loss 0

SUCCESSFUL/FAILED ... QUALITY DISTRIBUTION ...

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, click **3**:

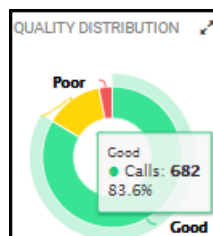


You can select an alarm to view detailed information about it then displayed in the Active Details window on the right side of the page.

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.

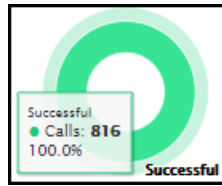
The Quality Distribution pie chart in the Network Summary window allows you to point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose quality was measured to be good, fair or poor respectively:



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:



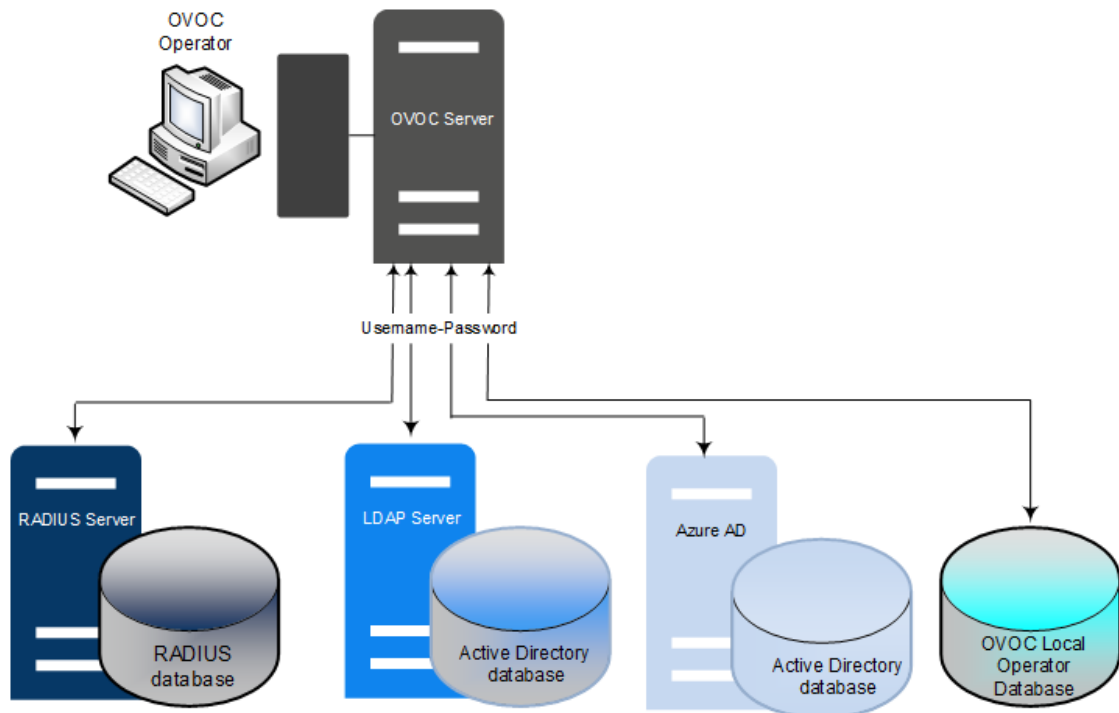
Click any color-coded segment to open the Calls List filtered by that call performance evaluation (Successful or Failed).

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 [here](#))
- Centrally, using a RADIUS server (see [here](#))
- Locally, in the OVOC (see [here](#))

The following figure shows the three different 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. 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**.

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. 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 OVOC Software Manager](#) on page 114.

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 133).

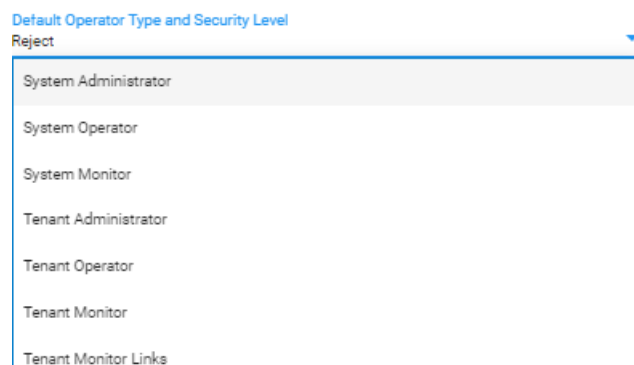
If the LDAP validates OVOC's query, the operator is authenticated and allowed access. Operators who are both 'System' and 'Tenant' type are checked in this way. See also [Adding a 'System' Operator](#) on page 58 and [Adding a 'Tenant' Operator](#) on page 65.

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. A 'Tenant' type operator with 'Monitoring Links' permissions can:

- Monitor multiple links representing different SBC devices; the links Source and Destination devices must be in the operator's tenant
- Monitor QoE information (Calls, Statistics and Link alarms)
- View the SIP Ladder (SIP Call Flow)

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 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 187.

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**.

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 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.

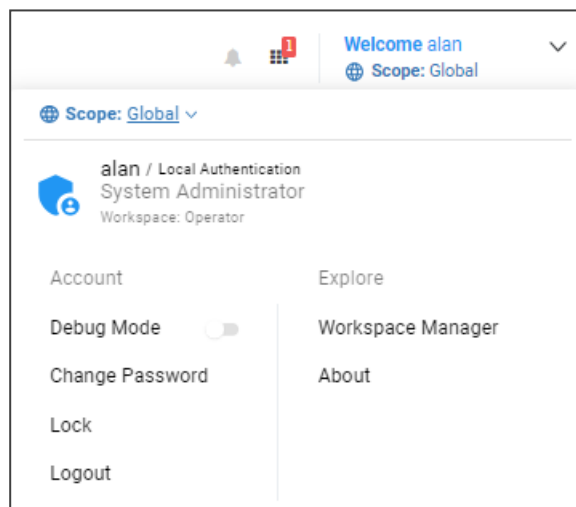
If **Enable combined authentication** is selected and an operator attempts to log in to the RADIUS server but it's unavailable, the OVOC connects to the *local* database with the same operator credentials.

- **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 'Welcome' 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 'Welcome' window displays the operator's authentication type.



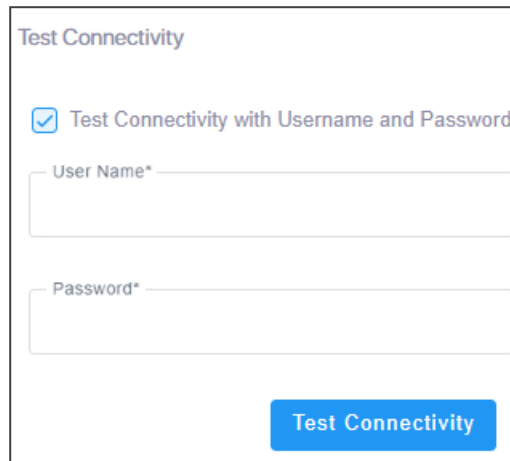
The 'Welcome' window always displays operator security level irrespective of how authentication is performed.

Testing Connectivity with the LDAP / RADIUS Server

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.



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**.

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. 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 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.

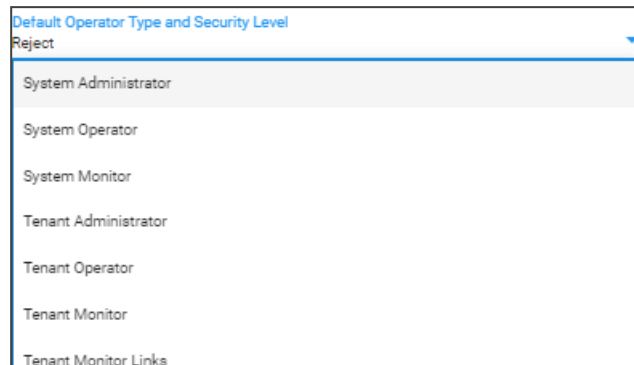
- The parameters below are used to define a User Group in the Azure AD.
- In the Tenant Details screen under the **Multitenancy** tab, the parameter 'AD Authentication: Group Name' is used to define a User Group in the OVOC when a tenant level is provisioned (see under [Adding a Tenant](#) on page 133).

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 58 and [Adding a 'Tenant' Operator](#) on page 65.

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. Only 'System' type operators can configure this group; 'Tenant' type operators can only view it. A 'Tenant' type operator with 'Monitoring Links' permissions can:
 - Monitor multiple links representing different SBC devices; the links Source and Destination devices must be in the operator's tenant

- Monitor QoE information (Calls, Statistics and Link alarms)
- View the SIP Ladder (SIP Call Flow)

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 187.

18. Click **Submit**.



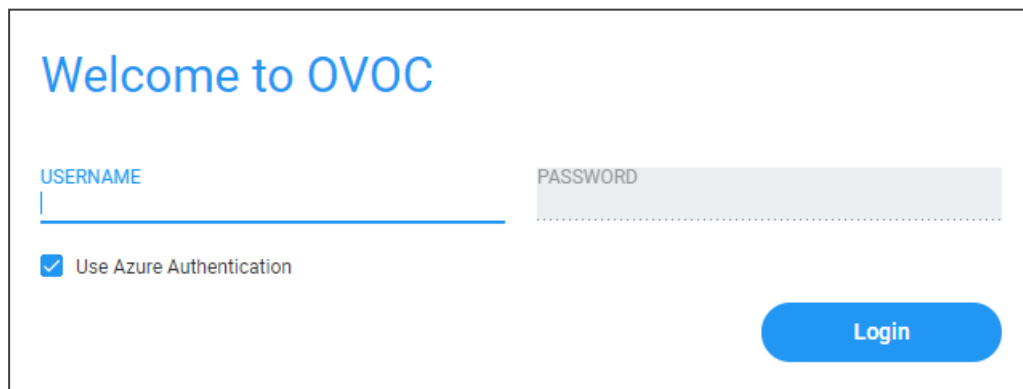
To configure Active Directory on Microsoft Azure, see the *OVOC Integration with Northbound Interfaces Guide*.

Logging in as an Azure User with Multi Factor Authentication

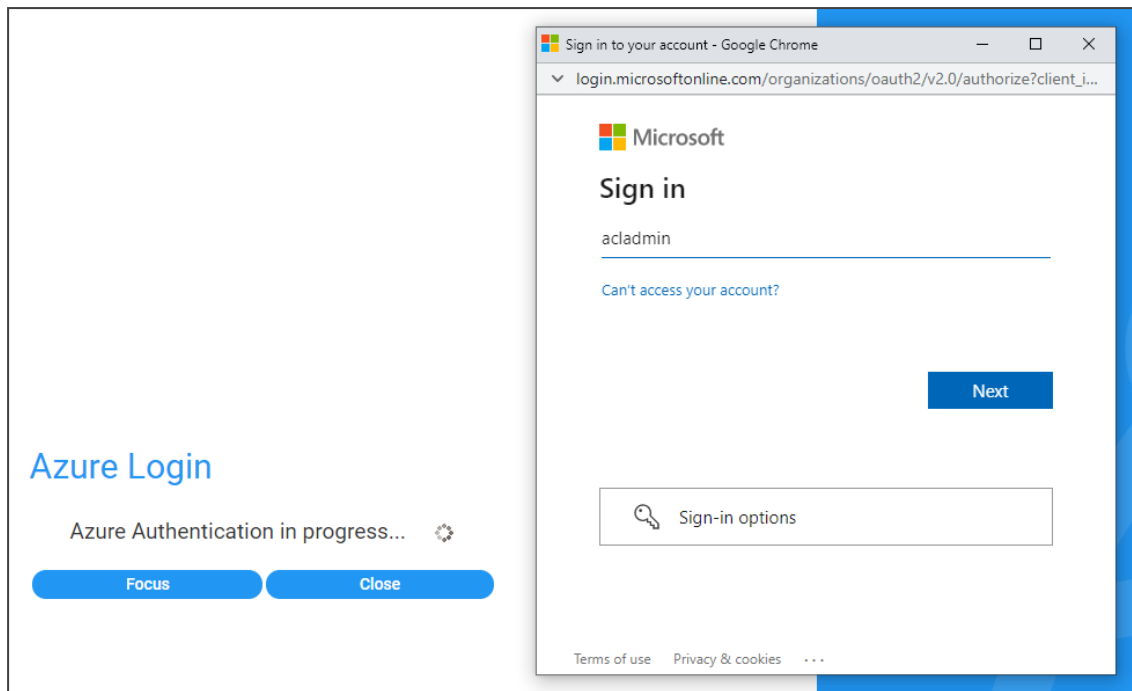
When logging in to the OVOC, the login process is slightly different if the operator attempting to log in is an Azure operator and if Multi Factor Authentication is enabled for this operator in the Azure configuration, as shown [here](#).

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

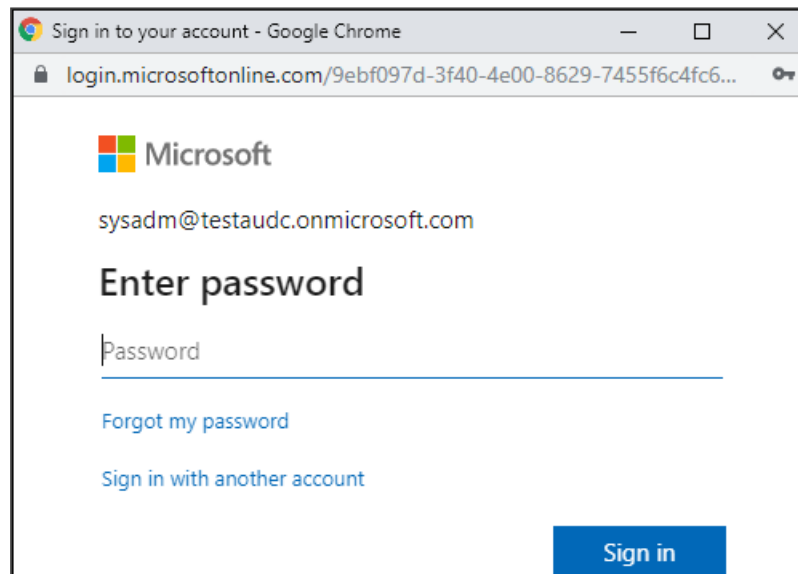
1. Point your browser to the OVOC server's IP address: **https://<IP Address>**. You only need to enter its IP address; the rest of the URL is automatically added. Logging in can optionally be performed using FQDN rather than IP address.



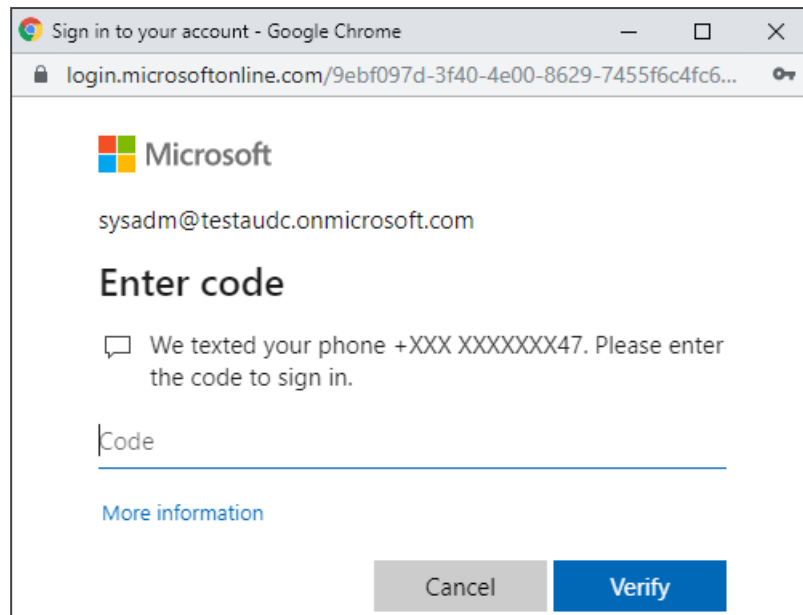
2. Enter your Username and Password and then click **Login**.



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. Under **Sign in**, enter your Microsoft username, e.g., johnb@enterprise.com, and click **Next**.



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.



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 with SAML

OVOC supports Security Assertion Markup Language (SAML) based authentication of a carrier's operators who are managing an enterprise customer using Azure AD and who need to get a consolidated view of the quality statistics of that enterprise customer's users calls.

SAML is an XML-based open-standard allowing operator identity data to pass between an identity provider (IdP) and a service provider (SP). The IdP performs operator authentication and passes the operator's identity and authorization level to the SP; the SP trusts the IdP and authorizes operator access.

➤ To configure authentication of OVOC operators with SAML:

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

SAML CONFIGURATION

Identity Provider Name*

Description

☐ Identity Provider Enabled

Identity Provider URL*

Identity Provider Certificate File*

ATTRIBUTES

Operator Type*

operatorType

Operator Security Level*

securityLevel

Tenants List*

tenantsList

Tenants Links List*

tenantsLinksList

Endpoint Group User*

endpointGroupUser

Endpoint Group List*

endpointGroupsList

Default Security Level*

Reject

Submit

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

SAML Parameter	Description
Identity Provider Name	Enter the name of the IdP.
Description	Enter a description of the IdP.
Is Identity Provider Enabled	Select the check box to enable IdP.
Identity Provider URL	Enter the URL of the IdP.
Identity Provider Certificate File ID	From the drop-down list, select the ID of the IdP's Certificate File.
Operator Type	Enter the Operator Type.
Operator Security Level	Enter the Security Level of the operator.
Tenants List	List the tenants allocated to the operator.
Tenants Links List	List the links of the tenants allocated to the operator.
Endpoint Group User	Enter the TBD
Default Security Level	Enter the default Security Level configured for the operator.

3. Click **Submit**.

Configuring Operator Authentication Locally, in OVOC

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

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

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

The screenshot shows the 'AUTHENTICATION' configuration page in the OVOC interface. On the left, there is a sidebar with 'ADMINISTRATION' and 'SECURITY' sections. Under 'SECURITY', 'Authentication' is selected. The main area shows 'Authentication Type' set to 'OVOC'. Below this, the 'OVOC AUTHENTICATION SETTINGS' are displayed in a grid. The settings include: 'Number of login attempts before blocking' (3), 'Max number of simultaneous login sessions' (5), 'Notifications display time (sec)' (3), 'Minimum password length' (8), 'Non repetitive characters from previous password' (0), 'Number of last passwords that can't be reused' (5), 'Password complexity' (No Complexity), 'Check dictionary for sufficient password complexity' (unchecked), 'Enable password expiration extension' (unchecked), 'Number of additional logins (after password reset)' (1), 'Additional logins time period (days)' (1), and 'Auto Suspend (days)' (0). A 'Submit' button is located at the bottom right of the settings area.

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

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 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
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

Parameter	Description
	cleared from the OVOC server after twenty minutes. See also here .
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	<p>From the drop-down, select either:</p> <ul style="list-style-type: none"> ■ 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	<p>Select this option for the OVOC server to perform a password weakness check on the OVOC operator's password.</p> <p>Default: Disabled (unselected).</p>
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.

Global vs. Tenant Scope

A 'System' operator's scope can be 'Global' or 'Tenant'. Management operations that the 'System' operator can perform in 'Global' scope are different to the operations that the 'System' operator can perform in 'Tenant' scope.



- Scope does not apply to 'Tenant' operator.
- 'System' operator in 'Global' scope can view all data *excluding private tenant data*; the 'System' operator in 'Global' scope *cannot view private data about tenants*, including QoE.
- 'System' operator in 'Tenant' scope can view *only that selected tenant's data*, including their *private data*.

For details on the actions that can be performed for each scope, see [here](#).

For details on the operations that can be performed for each security level, see [Operator Security Permissions](#) on page 57.

Selecting a Scope: Global vs. Tenant

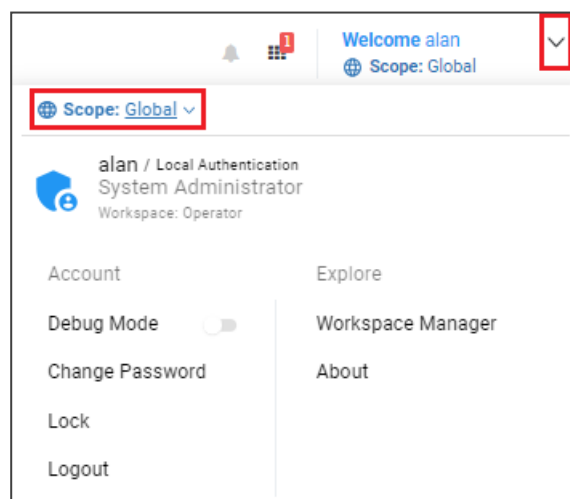


Applies only to the 'System' operator.

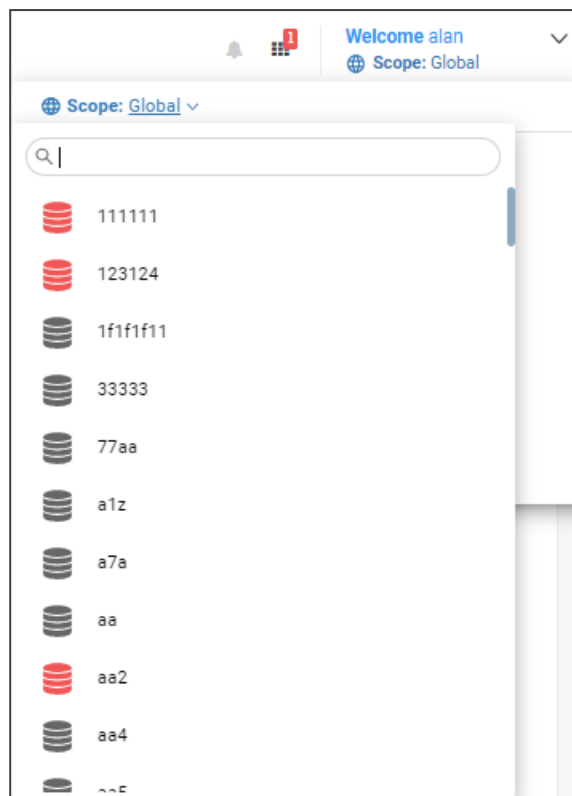
Scope can be 'Global' or 'Tenant'. If 'Tenant' is selected, data is filtered according to the selected Tenant. For more details of scope management, see [Global vs. Tenant Scope](#) above.

➤ To select a scope:

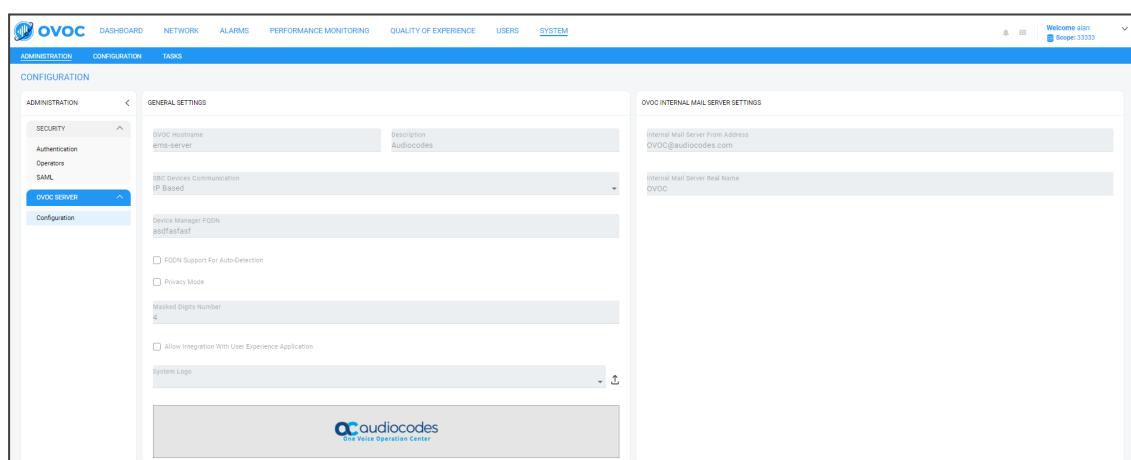
1. Click the 'Welcome' drop-down in the upper-right corner of any OVOC page.



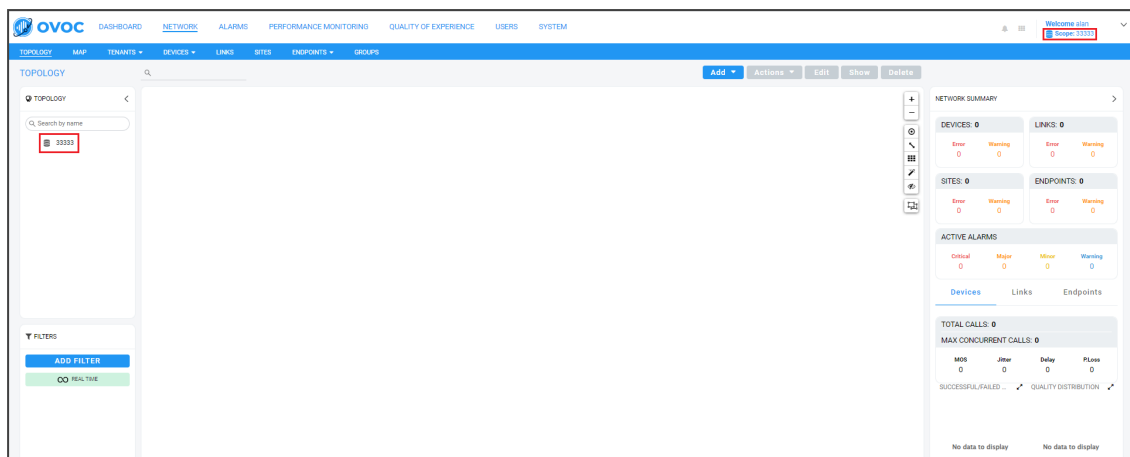
2. Click the 'Scope' drop-down indicated in the figure above.



3. Scroll down if necessary and select a tenant; the grayed out (disabled) Configuration page is displayed; this 'Tenant' cannot change these settings.



4. Click the Network menu and view the 'Tenant' scope as indicated in the figure below.



Operator Security Permissions

OVOC 'System' operators and 'Tenant' operators are allocated one of the following security levels:

- Admin
- Operator
- Monitoring
- Monitoring Links

The following table describes the capabilities allowed for each Operator Type / Security Level.

Op Type	Security Level	Define ops	Man- age ten- ants	Manage system resource- s	Manage tenant resource- s	Monitor system resource- s	Monitor tenant resource- s
System	Admin	Yes, all operator types & security levels	Yes	Yes	Yes	Yes	Yes
	Operator	No	Yes	Yes	Yes	Yes	Yes
	Monitor	No	Yes	No	No	Yes	Yes
Tenant	Admin	Yes, in their own 'tenant'	Yes, but only their own	No	Yes, in their own 'tenant'	No	Yes, in their own

Op Type	Security Level	Define ops	Manage tenants	Manage system resources	Manage tenant resources	Monitor system resources	Monitor tenant resources
	Operator	No	Yes, but only their own	No	Yes, in their own 'tenant'	No	Yes, in their own
	Monitor	No	Yes, but only their own	No	No	No	Yes, in their own
	Monitoring Links	No	No	No	No	No	Links only



- System in 'Global' scope cannot view private data about tenants including QoE.
- System in 'Tenant' scope views the data the same as the 'Tenant' operator.

Adding a 'System' Operator

You need to add a 'system' operator to 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 OVOC, open the Operators page (**System > Administration > Security > Operators**).
2. Click **Add** and then from the drop-down menu, select **System Operator**.



- When 'Scope' is defined as Tenant, only **Tenant Operator** is available as 'Operator Type'.
- When 'Scope' is defined as Global, both **Tenant Operator** and **System Operator** are available as 'Operator Type'.

SYSTEM OPERATOR DETAILS

Basic info
Advanced info

Operator Type

System

Operator Name*

Password*

Confirm Password*

☐ Change Password on Next Login

Security Level

Monitoring

Valid IPs to Login From

Full Name

Phone

Email

Description

Close

OK

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

Parameter	Description
User Name	Enter the operator's name. Must be unique.
Password	Enter the operator's password.
Confirm Password	Confirm the operator's password.
User Type	[Read-only] System or Tenant depending on what you selected in step 2.
Security Level	From the drop-down select: <div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; background-color: #0056b3; margin-right: 5px;"></div> Monitoring (lowest security level) </div>

Parameter	Description
	<ul style="list-style-type: none"> ■ 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 here. When adding this operator to multiple links, the links can be from different source SBCs but 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. The field not only supports IP addresses but also subnets (for customers that provide subnets).
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**.

SYSTEM OPERATOR DETAILS

Basic info
Advanced info

Suspension
▼

Not Suspended

Account Inactivity Period (Days)

0

Session Leasing Period (Hours)

0

Password Validity Max Period (Days)

90

Allowed Login Attempts

3

Notifications display time (sec)

3

Session Timeout Period (Minutes)

0

Password Update Min Period (Hours)

24

Password Warning Max Period (Days)

7

Max Simultaneous Login Sessions

5

Close
OK

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

Parameter	Description
Suspend User	<p>Select this option to suspend the 'system' operator. If you choose Future Suspension from the drop-down, the 'Choose suspension date' field is displayed:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <div style="border: 1px solid #ccc; padding: 2px 5px; display: flex; justify-content: space-between;"> Suspension ▼ </div> <div style="background-color: #f0f0f0; padding: 2px 5px;">Future Suspension</div> <div style="margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px; display: flex; justify-content: space-between;"> Choose suspension date:* </div> <div style="background-color: #f0f0f0; padding: 2px 5px;"> </div> </div> </div> <p>Click the calendar icon to define on what date to suspend the operator.</p>
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is suspended.
Account Inactivity Period	If the operator does not log into OVOC for the number of days specified, their account will be suspended. Maximum: 10 days.

Parameter	Description
(Days)	Default: 0 (The operator can log into 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.

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

➤ To release an operator who was previously suspended from 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 [Global vs. Tenant Scope](#) on page 55 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).

	OPERATOR NAME	OPERATOR TYPE	SECURITY LEVEL	STATUS	LAST SUCCESSFUL LOGIN	LAST FAILED LOGIN
<input type="checkbox"/>	dev	System	Admin	NOT ACTIVE	02-Oct-23 09:48:02	02-Sep-19 11:06:57
<input checked="" type="checkbox"/>	alan	System	Admin	ACTIVE	01-Jan-20 02:00:00	06-Aug-19 16:29:11
<input type="checkbox"/>	mike	System	Admin	NOT ACTIVE	13-Nov-18 14:49:37	
<input type="checkbox"/>	stef	System	Admin	NOT ACTIVE	25-Oct-17 14:10:55	19-Nov-17 13:43:51
<input type="checkbox"/>	daniel	System	Operator	NOT ACTIVE	01-Dec-23 10:34:26	28-Aug-23 21:08:38
<input type="checkbox"/>	daniel2	System	Monitoring	NOT ACTIVE	08-Dec-23 22:05:44	01-Oct-23 09:20:06
<input type="checkbox"/>	daniel3	System	Monitoring	NOT ACTIVE	09-Nov-23 15:36:42	30-Nov-23 01:10:29
<input type="checkbox"/>	daniel5	System	Monitoring	NOT ACTIVE	08-Dec-23 17:38:49	30-Nov-23 01:10:13
<input type="checkbox"/>	adminidm1	System	Monitoring	NOT ACTIVE	28-Dec-23 17:26:18	08-Dec-23 17:30:16
<input type="checkbox"/>	adminidm2	System	Monitoring	NOT ACTIVE	14-Dec-23 18:41:13	01-Dec-23 23:32:07
<input type="checkbox"/>	Alan	System	Admin	NOT ACTIVE	19-Feb-18 15:25:22	21-Feb-19 11:36:38
<input type="checkbox"/>	oran	System	Admin	NOT ACTIVE	17-Apr-18 15:09:23	02-Sep-21 18:07:06
<input type="checkbox"/>	gina	System	Admin	NOT ACTIVE	19-Apr-20 17:35:54	23-Nov-21 16:55:30

3. Select the active operator to log out; their 'Active' status is indicated in the Status column.

4. From the 'Actions' drop-down, select **Force Logout**.
5. Click the prompt **Force Operator Logout** to implement the action.

Adding a 'Tenant' Operator

You can add a 'tenant' operator to 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Click **Add** and then select **Tenant Operator** from the 'Operator Type' drop-down menu.



- When 'Scope' is defined as Tenant, only **Tenant Operator** is available for 'Operator Type'.
- When 'Scope' is defined as Global, both **Tenant Operator** and **System Operator** are available for 'Operator Type'.

TENANT OPERATOR DETAILS

Basic info
Advanced info
Topology

Operator Type
Tenant

Operator Name*

Password*

Confirm Password*

☐ Change Password on Next Login

Security Level
Monitoring ▼

Valid IPs to Login From
_____ ▼

Full Name

Phone

Email

Description

Close
OK

4. Configure 'tenant' operator's basic info using the table as reference.

Parameter	Description
Operator Type	[Read-only] System or Tenant depending on what you selected in step 2.
Operator Name	Enter the operator's name. Must be unique.
Password	Enter the operator's password.
Confirm Password	Confirm the operator's password.
Change Password on Next Login	Optionally select this option for the password to be changed the next time the operator logs in.
Security Level	From the drop-down select: <ul style="list-style-type: none"> ■ Admin (highest security level) ■ Operator (medium security level) ■ Monitoring (lowest security level)

Parameter	Description
	<ul style="list-style-type: none"> ■ Monitoring Links (Applicable only when adding a 'Tenant' type operator in a deployment whose architecture is ITSP customer multi-tenant architecture - see here. When adding this operator to multiple links, the links can be from different source SBCs but 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. The field not only supports IP addresses but also subnets (for customers that provide subnets).
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.

5. Click **Advanced Info**.

TENANT OPERATOR DETAILS

Basic info
Advanced info
Topology

Suspension
 Not Suspended ▼

Account Inactivity Period (Da...
 0

Session Timeout Period (Min...
 0

Session Leasing Period (Hour...
 0

Password Update Min Period ...
 24

Password Validity Max Period...
 90

Password Warning Max Perio...
 7

Allowed Login Attempts
 3

Max Simultaneous Login Ses...
 5

Notifications display time (sec)
 3

Close
OK

6. Configure using the table as reference. The screen displays advanced account and password settings.

Parameter	Description
Suspend User	<p>Select this option to suspend the 'tenant' operator. If you choose Future Suspension from the drop-down, the 'Choose suspension date' field is displayed:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <div style="display: flex; justify-content: space-between;"> Suspension ▼ </div> <div style="border-bottom: 1px solid #ccc; padding: 2px 0;">Future Suspension</div> <div style="margin-top: 5px;"> Choose suspension date:* <div style="display: flex; align-items: center;"> <div style="width: 20px; height: 20px; background-color: #f0f0f0; border: 1px solid #ccc; margin-right: 5px;"></div> <div style="flex-grow: 1; border-bottom: 1px solid #ccc;"></div> ▼ </div> </div> </div> <p>Click the calendar icon to define on what future date to suspend the operator.</p>
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is being suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is being suspended.
Account Inactivity Period (Days)	If the operator does not log into OVOC for the number of days specified, their account will be suspended. Maximum: 10 days.

Parameter	Description
	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.

7. Click **Topology.**

TENANT OPERATOR DETAILS

Basic info Advanced info **Topology**

Assigned Tenants: ▼

Assigned Links for a Specific Device: -----

Close **OK**

8. [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.
9. [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).

10. 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Select the 'tenant' operator whose details you need to edit and then click **Edit**; the Operator Settings screen opens.
4. 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 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Select the operators to remove and then click **Delete**.

Suspending a 'Tenant' Operator

You can suspend a 'tenant' operator from OVOC.

➤ **To suspend a 'tenant' operator:**

1. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Select the 'tenant' operator to suspend and then click **Actions**. Multiple operators can be selected for release from suspension.

4. 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 OVOC.

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

1. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Select the suspended operator to release and then click **Actions**.
4. 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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).
3. Select the operator whose password to change and then click **Actions**. Multiple operators can be selected.
4. 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

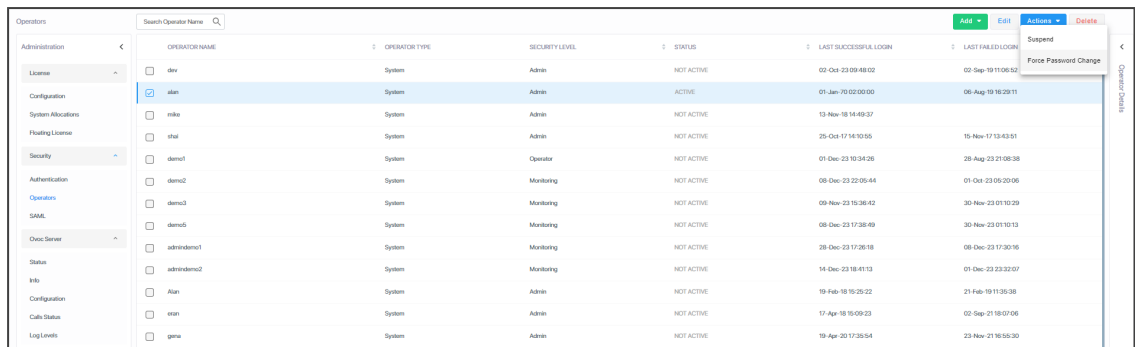


Applies only to OVOC operators with 'Admin' security level. See [Global vs. Tenant Scope](#) on page 55 for an explanation of the different security levels.

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. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Operators page (**System > Administration > Security > Operators**).

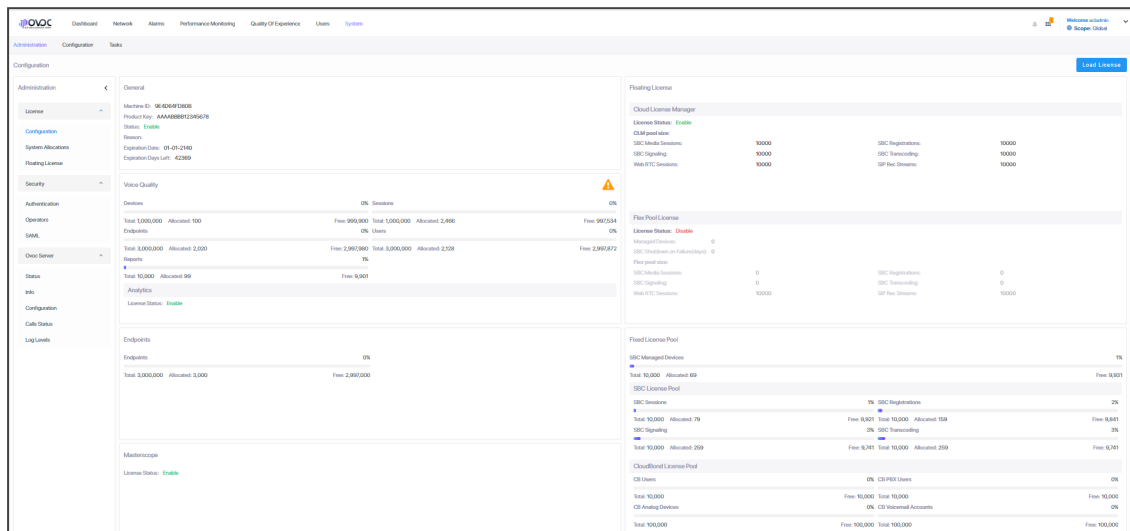


OPERATOR NAME	OPERATOR TYPE	SECURITY LEVEL	STATUS	LAST SUCCESSFUL LOGIN	LAST FAILED LOGIN
<input type="checkbox"/> dev	System	Admin	NOT ACTIVE	02-Oct-23 09:48:02	02-Sep-19 11:06:52
<input checked="" type="checkbox"/> alan	System	Admin	ACTIVE	01-Jan-20 02:00:00	06-Aug-19 16:28:11
<input type="checkbox"/> mike	System	Admin	NOT ACTIVE	13-Nov-18 14:49:37	
<input type="checkbox"/> shai	System	Admin	NOT ACTIVE	25-Oct-17 14:30:55	15-Nov-17 13:43:51
<input type="checkbox"/> demc1	System	Operator	NOT ACTIVE	01-Dec-23 10:34:26	28-Aug-23 21:05:38
<input type="checkbox"/> demc2	System	Monitoring	NOT ACTIVE	06-Dec-23 22:05:44	01-Oct-23 05:20:06
<input type="checkbox"/> demc3	System	Monitoring	NOT ACTIVE	09-Nov-23 15:36:42	30-Nov-23 01:10:29
<input type="checkbox"/> demc5	System	Monitoring	NOT ACTIVE	06-Dec-23 17:38:49	30-Nov-23 01:10:13
<input type="checkbox"/> admin@demc1	System	Monitoring	NOT ACTIVE	28-Dec-23 17:26:18	06-Dec-23 17:30:16
<input type="checkbox"/> admin@demc2	System	Monitoring	NOT ACTIVE	14-Dec-23 18:41:13	01-Dec-23 22:22:07
<input type="checkbox"/> Alan	System	Admin	NOT ACTIVE	19-Feb-18 15:25:22	21-Feb-19 11:35:38
<input type="checkbox"/> erin	System	Admin	NOT ACTIVE	17-Apr-18 15:09:23	02-Sep-21 18:07:06
<input type="checkbox"/> gema	System	Admin	NOT ACTIVE	19-Apr-20 17:35:54	23-Nov-21 16:55:35

3. Select the active operator to log out; their 'Active' status is indicated in the Status column.
4. From the 'Actions' drop-down, select **Force Logout**.
5. Click the prompt **Force Operator Logout** to implement the action.

3 Configuring System Settings

After logging in to OVOC, configuring operator authentication and then adding an operator, you can configure settings under the System menu. This menu is context-sensitive according to the managed scope ('Global' or 'Tenant' scope) - see [here](#) for more information.



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.
		Tenants Allocation	See Allocating Licenses to Tenants.
		System Allocation	See Defining # of Administrator-Defined Reports Produced at System Level on page 462 .
		Floating License	See under Managing SBC Licenses on page 193 .
	Security	Authentication	Lets you configure Operator authentication using OVOC/LDAP and Azure. See Configuring Operator Authentication on page 40.

Tab	Folder	Item	Description
		Operators	Lets you add operators to OVOC. See Global vs. Tenant Scope on page 55.
		SAML	Lets you configure Operator authentication using SAML. See Configuring Operator Authentication with SAML on page 51.
	OVOC Server	Status	Lets you view information about the status of the OVOC server. See Determining OVOC Server Status on page 79.
		Info	Lets you view information about the OVOC server. See OVOC Server Info on page 80.
		Configuration	Lets you configure the general OVOC server settings. See Securing Connections with FQDN or IP Address on page 81.
		Calls Status	Lets you view Calls Status statistics. See Viewing Calls Status on page 88.
		Log Levels	Lets you view log levels configured for OVOC processes. See Viewing Log Levels on page 89.
Configuration	Templates	SNMP Connectivity	Lets you configure SNMP templates. See Configuring SNMP Connectivity on page 90.
		HTTP Connectivity	Lets you configure HTTP templates. See Configuring HTTP Connectivity on page 92.
		QoE Thresholds	Lets you configure QoE Threshold templates. See

Tab	Folder	Item	Description
			Configuring QoE Thresholds on page 92.
		QoE Status & Alarms	Lets you configure QoE Status & Alarms templates. See Configuring QoE Status and Alarms on page 97.
		Performance Monitoring	Lets you configure PM Profiles. See Adding a PM Profile on page 312 .
		Device Backup	Lets you configure Device Backup settings. See Enabling Automatic Device Backup Periodically on page 99 .
		Dashboard	Lets you configure the layout for Dashboard elements. See Customizing Default Dashboard per Operator Type Security Level on page 100 for details.
		Calls Storage	Lets you configure Call Storage Settings. See Customizing Calls Storage on page 101 for details.
	Alarms		See Configuring Alarms Settings on page 112 for details.
	File Manager	Software Manager	See Adding Configuration Files to OVOC Software Manager on page 114 for details.
	External Applications		See Connecting Directly to External Applications on page 126 for details.
	Tasks		See Tasks tab on page 130 for details.

License Management

Global License configuration includes the following:

- The **Configuration** item lets you load the OVOC server license. See [Loading the OVOC Server License](#) below.
- The **System Allocation** item lets you manage Global scope licenses for Analytics and Reports. See [System License Allocations](#) on the next page.
- The **Floating License** item lets you configure OVOC Floating License Service Communications. See [Configuring OVOC-Floating License Service Communications](#) on page 201.

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 [Global vs. Tenant Scope](#) on page 55 for more information.

➤ To load the license:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the License Configuration page (**System > Administration > License > Configuration**).

The screenshot displays the OVOC License Configuration page. The left sidebar shows the navigation menu with 'License' selected under 'Administration'. The main content area is divided into several sections:

- General:** Shows system information like 'Master ID: SE-004F0008', 'Product Key: AAM68881245678', 'Status: Enable', 'Release: 7.6.1000', 'Expiration Date: 01-01-2140', and 'Expiration Days Left: 42389'.
- Security:** Includes 'Value Quality' and 'Authentication' sections.
- Floating License:** Contains a 'Cloud License Manager' table with columns for 'License Status', 'License Type', 'License Count', and 'License Description'. It also includes a 'Fixed License Pool' section.
- Fixed License Pool:** Shows a table with 'License Status', 'License Type', 'License Count', and 'License Description'.

A 'Load License' button is located in the top right corner of the page.

3. Click the **Load License** button and in the browser window that opens, navigate to the txt file containing the license on your machine.
4. 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.
- The License Configuration page displays only the parameters that exist in the License Key provided by AudioCodes. Make sure the license you purchased provides the capabilities you ordered.

System License Allocations

The System Allocations page lets the System admin (Global scope) enable the Analytics feature (see [Displaying Analytics](#) on page 327) and to configure license for report generation.

➤ Do the following:

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

The screenshot shows the OVOC web interface. The top navigation bar includes 'DASHBOARD', 'NETWORK', 'ALARMS', 'PERFORMANCE MONITORING', 'QUALITY OF EXPERIENCE', 'USERS', and 'SYSTEM'. The left sidebar shows the 'ADMINISTRATION' tab selected, with sub-items like 'License', 'Configuration', 'System Allocations', 'Floating License', 'SECURITY', 'Authentication', 'Operators', 'SAML', and 'OVOC SERVER'. The main content area is titled 'SYSTEM ALLOCATIONS' and contains the 'ANALYTICS' section. In this section, there is a checkbox labeled 'Analytics Status' which is currently unchecked. Below it is a slider for 'Reports' with a value of 0, a 'Total' of 10,000, and a 'From 10,000' label. A 'Submit' button is located at the bottom right of the analytics section.

2. Select the **Analytics Status** check box to enable the Analytics feature.
3. Adjust the value slider to configure the number of Reports required by the Global scope admin to generate.
4. Click **Submit** to confirm changes.

Security Management

- The 'Security' folder's **Authentication** item lets you configure LDAP and RADIUS authentication. See [Configuring Operator Authentication](#) on page 40 .
- The 'Security' folder's **Operators** item lets you add OVOC operators. See [Global vs. Tenant Scope](#) on page 55.
- The 'Security' folder's **SAML** item lets you configure OVOC to operate with SAML. See [Configuring Operator Authentication with SAML](#) on page 51.

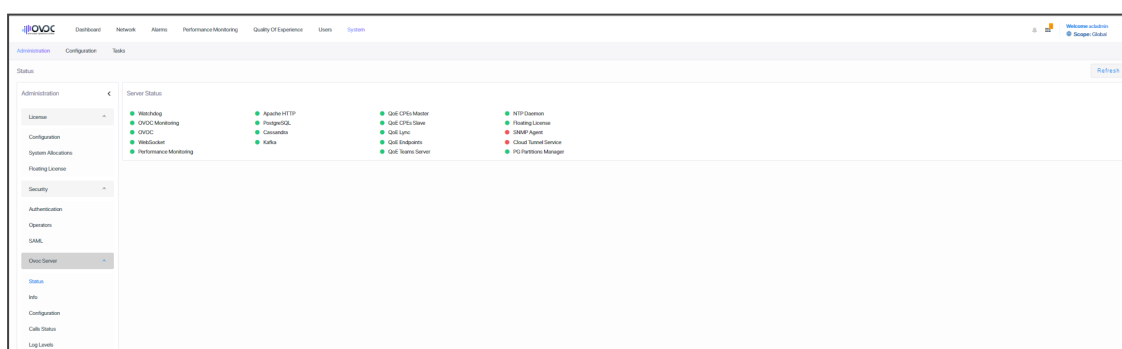
OVOC Server Management

OVOC Server management includes the following:

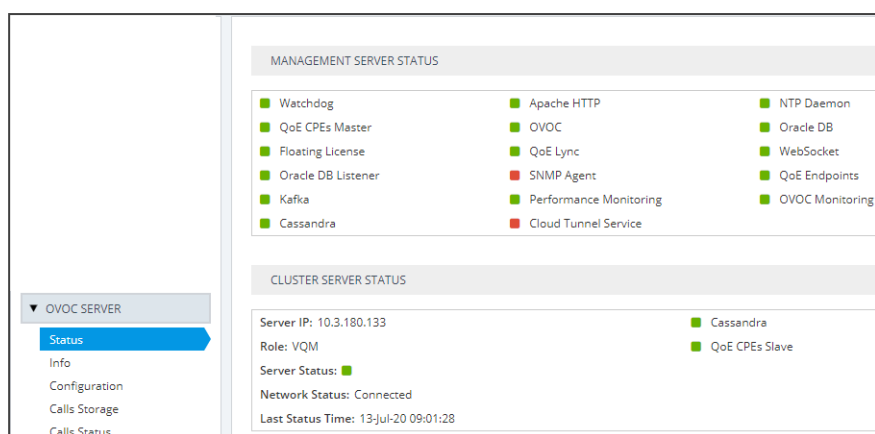
- Lets you view the status of OVOC server components ([Determining OVOC Server Status](#) below).
- Lets you view information on the OVOC server Operating System and networking elements ([OVOC Server Info](#) on the next page).
- Lets you secure the connection between managed devices and OVOC ([Securing Connections with FQDN or IP Address](#) on page 81).
- Lets you perform initial connection of SBC devices with auto detection using SBC FQDN ([Perform Auto-Detection using Devices FQDN Hostname](#) on page 83).
- Lets you configure Privacy mode for concealing digits in Call details ([Configuring Privacy Mode, Concealing Users Calls Details](#) on page 84).
- Lets you integrate with the User Experience application ([Determining Operator Behavior with OVOC's UX App](#) on page 85).
- Lets you upload a Global logo to display in Report results ([Uploading a Global Logo to Display in Report Results](#) on page 86).
- Lets you enter a description that appears in the alarms that are forwarded to SNMP destinations ([Providing a Description to be Forwarded in Alarm Info](#) on page 86).
- Lets you view Calls Status statistics ([Viewing Calls Status](#) on page 88).
- Lets you view configured Server Log Levels ([Viewing Log Levels](#) on page 89)

Determining OVOC Server Status

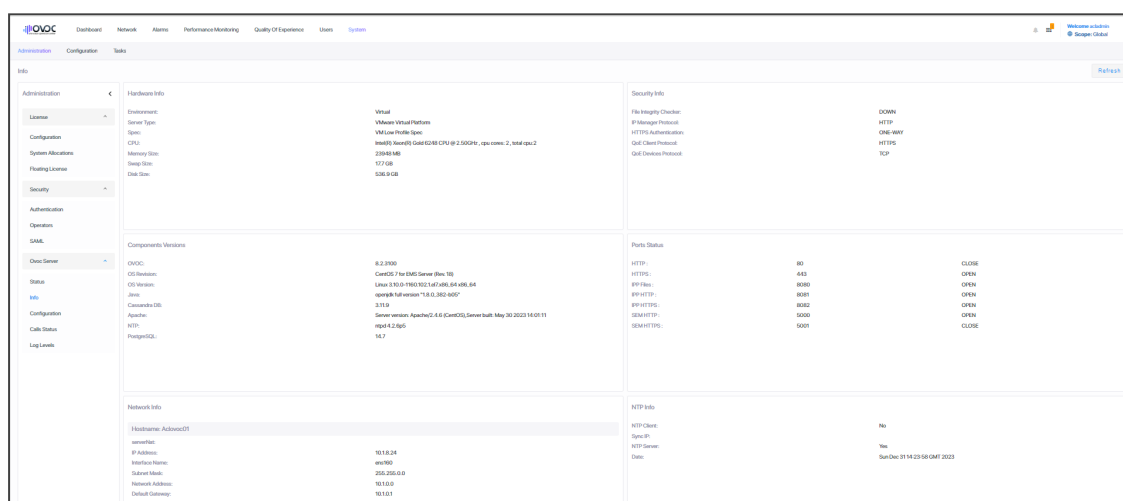
The Server Status page (**System > Administration > OVOC Server > Status**) lets you determine at-a-glance status information about the OVOC server. The feature saves operators from having to log in to the EMS Server Manager. The same information is presented, only in friendlier format.



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.



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.



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

OVOC Server Info

The Server Info page (**System menu > Administration tab > OVOC Server folder > Info**) lets you determine at-a-glance information about the OVOC server Operating System specifications and Networking information. The feature saves operators from having to log in to the OVOC Server Manager. The same information is presented, only in a friendlier format.

HARDWARE INFO		SECURITY INFO	
Environment:	Hardware	File Integrity Checker:	DOWN
Server Type:	Virtual Machine	IP Manager Protocol:	HTTP
Spec:	VM Low Profile Spec	HTTPS Authentication:	ONE-WAY
CPU:	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz, cpu cores: 2, total cpu: 2	OoE Client Protocol:	HTTPS
Memory Size:	31247 MB	OoE Devices Protocol:	BOTH
Swap Size:	20.1 GB		
Disk Size:	536.9 GB		
COMPONENTS VERSIONS		PORTS STATUS	
OVOC:	8.2.2350	HTTP :	80 OPEN
OS Revision:	CentOS 7 for EMS Server (Rev. 20)	HTTPS :	443 OPEN
OS Version:	Linux 3.10.0-1160.95.1.el7.x86_64 x86_64	IPP Files :	8080 OPEN
Java:	openjdk full version "1.8.0_362-b08"	IPP HTTP :	8081 OPEN
Cassandra DB:	3.11.9	IPP HTTPS :	8082 OPEN
Apache:	Server version: Apache/2.4.6 (CentOS) Server built: May 30 2023 14:01:11	SEM HTTP :	5000 OPEN
NTP:	ntpd 4.2.6p5	SEM HTTPS :	5001 OPEN
PostgreSQL:	14.7		
NETWORK INFO		NTP INFO	
HOSTNAME: IPPQA		NTP Client:	Yes
serverNat:		Sync IP:	*51.16.77.36
IP Address:	172.17.123.100	NTP Server:	Yes
Interface Name:	eth0	Date:	Wed Sep 6 10:53:06 BST 2023
Subnet Mask:	255.255.255.0		
Network Address:	172.17.123.0		
Default Gateway:	172.17.123.1		

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



For OVOC to access Teams, an FQDN (e.g., qa-ovoc-tlc.trunkpack.com) rather than a hostname (e.g., qa-ovoc-tlc) must be used.

➤ To secure connections with FQDN or IP Address:

- Open the Server Configuration page (**System > Administration > OVOC Server > Configuration**) and then from the 'SBC Devices Communication' drop-down list, select either **IP Based** (default) or **Hostname Based**.

The screenshot displays the OVOC configuration interface, divided into two main sections: General Settings and OVOC Internal Mail Server Settings.

General Settings:

- OVOC Hostname:** aclovc01
- Description:** Audiocodes
- SEC Devices Communication:** A dropdown menu is open, showing options: IP Based (selected), Hostname Based, and IP Based.
- Masked Digits Number:** 5
- Device Manager FQDN:** (Empty field)
- Allow Integration With User Experience Application:** (Unchecked checkbox)
- System Logo:** globalLogo.png

OVOC Internal Mail Server Settings:

- Internal Mail Server From Address:** OVOC@audiocodes.com
- Internal Mail Server Real Name:** OVOC

At the bottom of the General Settings section, there is a blue **Submit** button.

Configuring Device Manager FQDN

Operators can enter the Device Manager FQDN. This is the base URL of the customer URL used by customers for web access to OVOC. The customer URL is created when the customer is created.

For example: `https://<DeviceManager_OVOC_Management_System>/ltcfordevice/<Customer_Tenant_Id>/`

where `<DeviceManager_OVOC_Management_System>` is the interface system platform where keep-alive messages are aggregated from the endpoints.

The platform may be either:

- OVOC server
- Imperva Incapsula WAF

➤ To configure Device Manager FQDN:

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

The screenshot shows the 'Configuration' page for the OVOC system. On the left is a navigation menu with options: Administration, License, Configuration, System Allocations, Floating License, Security, Authentication, Operators, SAML, OVOC Server, Status, Info, Configuration (highlighted), Calls Status, and Log Levels. The main content area is titled 'General Settings' and contains the following fields:

- OVOC Hostname:** aclovoc01
- Description:** Audiocodes
- SBC Devices Communication:** IP Based
- ☐ FQDN Support For Auto-Detection
- ☐ Privacy Mode
- Masked Digits Number:** 5
- Device Manager FQDN:** (This field is highlighted with a blue border)
- ☐ Allow Integration With User Experience Application
- System Logo:** globalLogo.png

At the bottom right of the form is a blue 'Submit' button. The Audiocodes logo and 'One Voice Operation Center' text are visible at the bottom of the main content area.

2. Enter the URL and then click **Submit**.

Perform Auto-Detection using Devices FQDN Hostname

You can perform auto-detection with managed devices to OVOC using the SBC devices' Host Name FQDN instead of its IP address.

➤ To configure auto-detection using FQDN:

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

This screenshot is identical to the one above, showing the 'Configuration' page for the OVOC system. The main difference is that the ☒ FQDN Support For Auto-Detection checkbox is now checked. The 'Device Manager FQDN' field remains empty and is no longer highlighted.

2. Select the **FQDN Support for Auto-Detection** option as shown in the preceding figure.

Configuring Privacy Mode, Concealing Users Calls Details

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**).

The screenshot shows the 'Configuration' page for the 'OVOC Server'. The left sidebar contains a navigation menu with options: Administration, License, Configuration, System Allocations, Floating License, Security, Authentication, Operators, SAML, Ovoc Server, Status, Info, Configuration (highlighted), Calls Status, and Log Levels. The main content area is titled 'General Settings' and includes the following fields:

- OVOC Hostname:** alovoc01
- Description:** Audiocodes
- SBC Devices Communication:** IP Based
- ☐ FQDN Support For Auto-Detection
- ☒ **Privacy Mode**
- Masked Digits Number:** 5
- Device Manager FQDN:** (empty field)
- ☐ Allow Integration With User Experience Application
- System Logo:** globalLogo.png

At the bottom of the form is the Audiocodes logo and a 'Submit' button.

2. Under General Settings, select the 'Privacy Mode' option as shown in the preceding figure 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

3. In the 'Masked Digits Number' field, enter the number of digits that will be masked from the phone number when in 'Privacy Mode' (described in the previous step). This setting defines the *global* number of digits that will be masked from the phone number. For information about configuring 'Masked Digits Number' *per tenant*, see [Adding a Tenant](#) on page 133.

By default, the OVOC conceals the *last four digits* from users' phone numbers. The configuration can be changed on-the-fly if necessary.

Between the globally-defined configuration and the per-tenant configuration, the one with the higher number of masked digits configured takes priority.

If you're operating with multiple tenants, take the highest number of masked digits configured and apply it to your tenants calls. Example: Tenant A is configured with four masked digits while Tenant B is configured with six; the operator assigned to both tenants will see six digits masked in both tenants' users' calls.

Masking rules apply to both Calls List page and to the Call Details screen (see [Accessing the Calls List](#) on page 371 and [Showing Call Details](#) on page 382).

Determining Operator Behavior with OVOC's UX App

OVOC includes an integrated UX app for learning how OVOC is used, which pages are visited, for how long pages are visited, and what the common operator flows are. Data is collected and analyzed based on customer reports sent to the app server located in the cloud. The following data is monitored:

- Page title
- Page URL
- Buttons pressed and options selected from drop-downs
- Filter(s) set with which fields
- Control changes (for example, in the Alarms page, if table columns were resized, filter / summary panels closed, graphs opened in large view)
- Forms opening and editing



Important to note: When this feature is enabled, permission is given for the browser to send all user interactions to the UX server in the cloud.

➤ To enable the UX app:

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

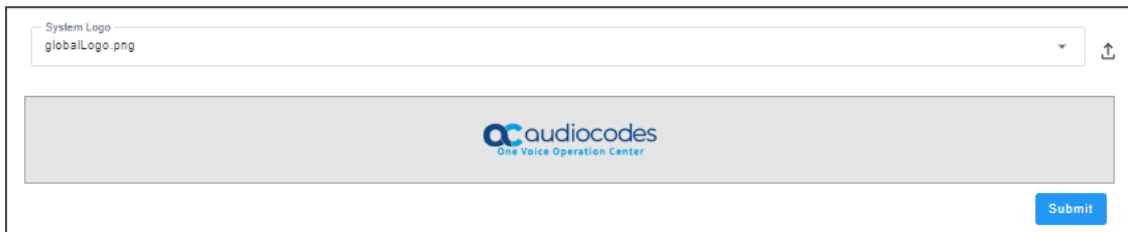
2. Select the option **Allow Integration With User Experience Application** and click **Submit**. Default: disabled.


Uploading a Global Logo to Display in Report Results

Admins can upload a global logo to be displayed 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 admins.

➤ To upload a global logo:

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



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.



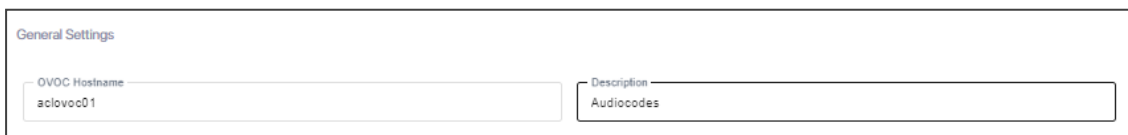
- If the logo image file has already been uploaded to the OVOC server and is displayed in the Software Manager, you can select it from the drop-down list.
- See also [Defining a Report](#) on page 463 for related information.
- See also [Adding Configuration Files to OVOC Software Manager](#) on page 114 for related information.
- See also [Editing a Tenant - Defining a Logo](#) on page 144 to define a logo to be displayed in report results related to a specific tenant.
- See also [Configuring Privacy Mode, Concealing Users Calls Details](#) on page 84 for information about the parameter 'Masked Digits Number'.

Providing a Description to be Forwarded in Alarm Info

OVOC allows operators to provide a 'Description' to be forwarded in 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**).



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 *OVOC Northbound Integration Guide*.



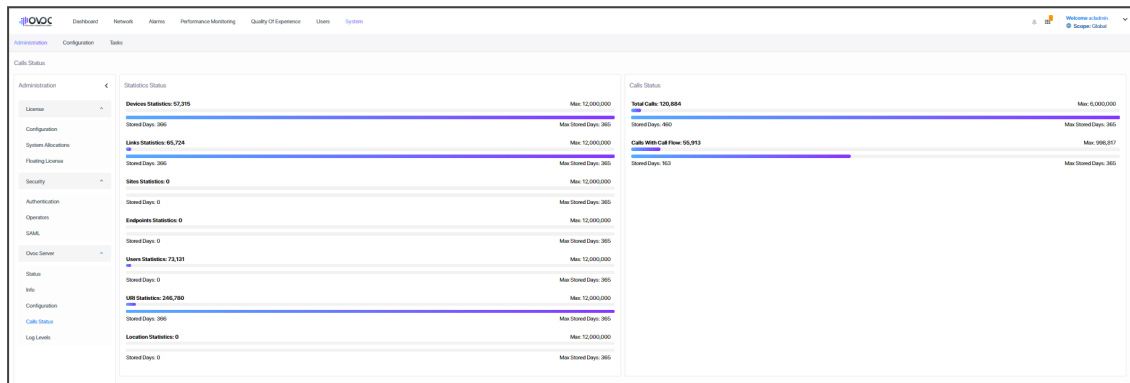
The configuration in the 'Description' field should be mirrored in the Alarm Forwarding rule - see under [Forwarding Alarms](#) on page 272 for more information. AudioCodes FAEs then use these as *Customer #s*. Each alarm from the OVOC server opens a ticket to AudioCodes or to the customer, depending on with whom the OVOC is deployed.

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. Admins can use the page as reference to determine OVOC server database status.

➤ To view statuses:

1. Open the Statistics Status page (**System > Administration > OVOC 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 Calls Storage](#) on page 101); 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.



80 million calls can be stored for a year (for example) but when operating in an Azure or AWS environment and disk space is empty for most of the year because it can take months to fill up, customers are provided with an option to decrease disk size and number of stored entities. See the *OVOC IOM* for the minimum disk space required for each platform.

- 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 Calls Storage](#) on page 101.

Viewing Log Levels

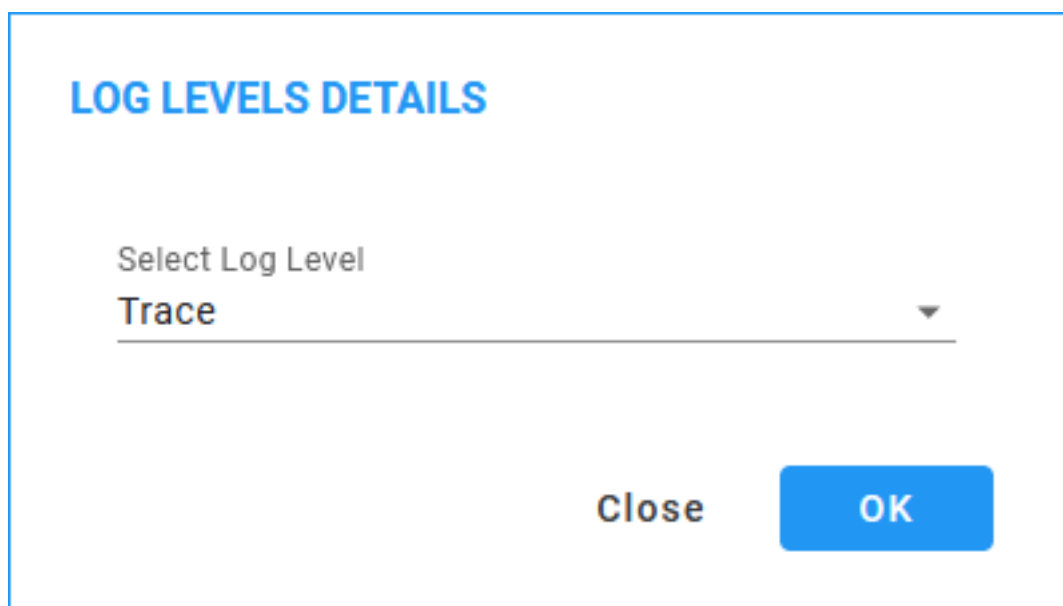
The Log Levels screen lets you view the that are configured for each OVOC process in the OVOC Server Manager.

➤ To view log levels:

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



2. Select a log and then click **Edit** to filter the view by Log Level.



- From the drop-down, select the relevant Log Level to filter by and then click **OK**.

Configuring Templates

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

- SNMP Connectivity ([Configuring SNMP Connectivity](#) below)
- HTTP Connectivity ([Configuring HTTP Connectivity](#) on page 92)
- QoE Thresholds ([Configuring QoE Thresholds](#) on page 92)
- QoE Status & Alarms ([Configuring QoE Status and Alarms](#) on page 97)
- Backup managed devices ([Enabling Automatic Device Backup Periodically](#) on page 99)
- Performance Monitoring Template ([Adding a PM Template](#) on page 307)
- Dashboard elements ([Customizing Default Dashboard per Operator Type | Security Level](#) on page 100)
- Calls Storage ([Customizing Calls Storage](#) on page 101)

Configuring SNMP Connectivity

OVOC enables you to configure an SNMP connectivity template whose parameter values can then be applied system-wide (globally). SNMP/HTTP templates are the default profile values for each defined tenant. Tenant SNMP/HTTP profiles are used as default for the devices under them.

➤ To configure an SNMP connectivity template:

- Open the SNMP Connectivity screen (**System > Configuration > Profiles > SNMP Connectivity**).

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

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: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Authentication and Privacy (default) <input type="checkbox"/> No Security <input type="checkbox"/> Authentication
Authentication Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> SHA (default) <input type="checkbox"/> MDS <input type="checkbox"/> No Protocol
Authentication Key	Enter an Authentication Key. Default: 123456789.
Privacy Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> AES 128 (default) <input type="checkbox"/> DES
Privacy Key	Enter a Privacy Key. Default: 123456789.

3. Click **Submit**.

Configuring HTTP Connectivity

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

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

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

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

Parameter	Description
Device Admin User	Enter the device Web server user name. Example: Admin . Password - "Admin".
Change Device Admin Password	Enter the Web server password. Example: Admin .
Communication Protocol	From the drop-down, select either: <ul style="list-style-type: none"> ■ HTTP (default) ■ HTTPS <p>Note: You must configure OVOC to use HTTPS to connect to an SBC / Gateway if you configured the device's parameter 'Secured Web Connection (HTTPS)' to HTTPS Redirect for Single-Sign On (SSO) from OVOC to the device.</p>

3. Click **Submit**.

Configuring QoE Thresholds

OVOC enables admins to configure QoE Thresholds which determine *global* (system-wide) voice quality thresholds templates.



For information on how to configure QoE Thresholds profiles *per tenant*, see [Managing QoE Thresholds Profiles](#) on page 421.

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 configure global QoE thresholds templates:**

1. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. From the System menu, open the QoE Thresholds page (**System > Configuration > Templates > QoE Thresholds**).

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.

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

Template	Description
	Profile per Tenant on page 424.

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

QOE THRESHOLDS DETAILS

Threshold Name

Medium Sensitivity Threshold

Description

Tenant

AudioCodes

Attachments

7 Devices, 17 Links, 470 Endpoints

[View](#)

Defaults

☒ Device
 ☒ Link
 ☐ Endpoint

VOICE

VIDEO

☒ MOS (0-5)

→ 3.5

→

→ 2.8

→

☒ Delay (msec)

→ 180

→

→ 500

→

☒ Packet Loss (%)

→ 2

→

→ 5

→

☒ Jitter (msec)

→ 40

→

→ 80

→

☒ Echo (dB)

→ 25

→

→ 10

→

Close

OK

QOE THRESHOLDS DETAILS

Threshold Name: MS Teams Thresholds

Description:

Tenant: AudioCodes

Attachments
0 Devices, 0 Links, 0 Endpoints
[View](#)

Defaults
☐ Device ☐ Link ☐ Endpoint

VOICE

☒ MOS (0-5) → 4 →

☒ Delay (msec) → 500 →

☒ Packet Loss (%) → 10 →

☒ Jitter (msec) → 30 →

☐ Echo (dB)

VIDEO

→ 4 →

→ 500 →

→ 10 →

→ 30 →

[Close](#) [OK](#)

4. Provide an intuitive name for the profile. As a reference, use the names of the four QoE Threshold Templates displayed in the table above.
5. Enter a description of the profile to facilitate effective intuitive management later.
6. Select the **Device** option to set the profile as devices default.
7. Select the **Links** option to set the profile as links default.
8. Select the **Endpoints** option to set the profile as endpoints default.
9. By default, **All** metrics are included in the profile, except for Teams where the metric **Echo** is excluded. 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)**.
10. Do the same for the other metrics thresholds.
11. [Applies only to MS Teams] In the QoE Thresholds Details screen for the MS Teams profile, click the **Video** tab (the settings described in the preceding steps were related to the **Voice** tab).

QOE THRESHOLDS DETAILS

Threshold Name: MS Teams Thresholds Description:

Tenant: AudioCodes

Attachments: 0 Devices, 0 Links, 0 Endpoints [View](#)

Defaults

☐ Device ☐ Link ☐ Endpoint

VOICE VIDEO

Video

☒ Avg Video Frame Loss Percentage (%) 45 50

☒ Avg Video Frame Rate (fps) 7 7

☒ Post Forward Error Correction Packet Loss Rate 0.15 0.15

Screen Sharing

☒ Avg Video Frame Loss Percentage (%) 50 50

☒ Avg Video Frame Rate (fps) 2 2

[Close](#) [OK](#)



All default values in Teams QoE Thresholds are based on recommended Microsoft CQD (Call Quality Dashboard) values. Operators can customize them per Teams device (Teams Tenant).

Use the following table as reference to the preceding figure.

Table 3-2: QoE Thresholds Details - MS Teams Thresholds - Video

Setting	Description
Avg Video Frame Loss Percentage (%)	Threshold values representing recommended data for the 'Low' sensitivity level.
Avg Video Frame Rate (fps)	Threshold values representing recommended data for the 'Medium' sensitivity level.
Post Forward Error Correction Packet Loss Rate	Threshold values representing recommended data for the 'High' sensitivity level.

Setting	Description
Screen Sharing	
Avg Video Frame Loss Percentage (%)	Same as for video. Threshold values representing recommended data for the 'Low' sensitivity level.
Avg Video Frame Rate (fps)	Same as for video. Threshold values representing recommended data for the 'Medium' sensitivity level.
Post Forward Error Correction Packet Loss Rate	Same as for video. Threshold values representing recommended data for the 'High' sensitivity level.

12. Click **OK**; the profile is displayed in the QoE Thresholds screen.

Configuring 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](#) on page 430.


➤ To view the global QoE status:


1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the QoE Status and Alarms page (**System > Configuration > Templates > QoE Status & Alarms**).

Configuration	DETAILS	NAME	TENANT	LAST RUNTIME	MONITOR	MIN/MAX	FAILED CALLS PROFILE (%)	POOR QUALITY CALLS (%)	AVERAGE CALL DURATION (S)	BAWMETHODS (S)	MAX CONCURRENT CALLS	FAILED CALLS SERVICE (%)	FAILED CALLS SERVICE (%)	DESCRIPTION
Profile	<input type="checkbox"/>	ALARM RULE	AudioCodes	01-Jan-24 12:00	15	50	5	5	10	12	5	5	10	
QoS Profiles	<input checked="" type="checkbox"/>	G4B Inband calls	AudioCodes	01-Jan-24 12:00	15	50	5	5	10	12	5	5	10	
QoS Thresholds	<input type="checkbox"/>	test	AudioCodes	01-Jan-24 12:00	15	2	2	2	10	10	2	2	10	
QoS Status & Alarms	<input type="checkbox"/>	test	AudioCodes	01-Jan-24 12:00	15	1	2	2	10	10	2	2	10	
Failed Call Reasons	<input type="checkbox"/>	GET LOW	AudioCodes	01-Jan-24 12:00	15	1	2	2	10	10	2	2	10	
Alarms	<input checked="" type="checkbox"/>	test	AudioCodes	01-Jan-24 12:00	15	50	2	2	10	10	2	2	10	test
File Manager	<input type="checkbox"/>	test	AudioCodes	01-Jan-24 12:00	15	50	2	2	10	10	2	2	10	

3. Use the following table as reference.

Page Indications	Description
Defaults	<div> = displayed when the alarm rule applies to devices </div> <div> = displayed when the alarm rule applies to links </div> <div> = displayed when the alarm rule applies to sites </div>

Page Indications	Description
	 = displayed when the alarm rule applies to IP phones
Name	Indicates the name of the alarm rule.
Last Runtime	Indicates the last time the alarm rule was activated.
Monitoring Frequency Min	Indicates at least how often monitoring is performed. Default: 15
Minimum Calls per Entity to Analyze	Indicates the minimum number of calls to analyze, per entity. Default: 50
Failed Calls (%)	<p>➔ 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.</p> <p> 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 430).</p>
Poor Quality Calls (%)	<p>➔ x ➔ y ➔ indicates that green changes to orange ('Major' severity) when the x percentage of poor quality calls is exceeded and orange changes to red ('Critical' severity) when the y percentage of poor quality calls is exceeded.</p> <p> 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 430).</p>
Average Call Duration (seconds)	<p>➔ 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.</p> <p> 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 430).</p>
Bandwidth Rule (Kbps)	<p>➔ 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.</p> <p> indicates alarm issued – displayed if the Generate Alarm option is</p>

Page Indications	Description
	selected in the Alarm Rule Details screen (see Adding a QoE Alarm Rule per Tenant on page 430).
Maximum Concurrent Calls Rule (#)	<p>➔ 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.</p> <p> 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 430).</p>

Enabling Automatic Device Backup Periodically

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.



- All devices that are version 7.4.200 and later are backed up with a .zip file.
- Up to *five* different backup files are saved for each device (a backup file that has not been changed from a previous backup will not be saved)
- The number of backup files stored includes old and new file types. For example, if a device operates with an .ini file and already has three stored .ini files when the maximum that can be stored is five, two more .zip files are stored before deletion of old .ini files begins.
- For upgraded devices which operate with the old file type, in the next backup round after the upgrade, a .zip file is created (and the oldest backup is deleted if necessary).

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 3-1: Device Backup

DEVICE BACKUP

☒ Enable Periodic backup

Number of backup files per device: 5

Number of retries: 2

Submit

2. Select the 'Enable Periodic backup' option.

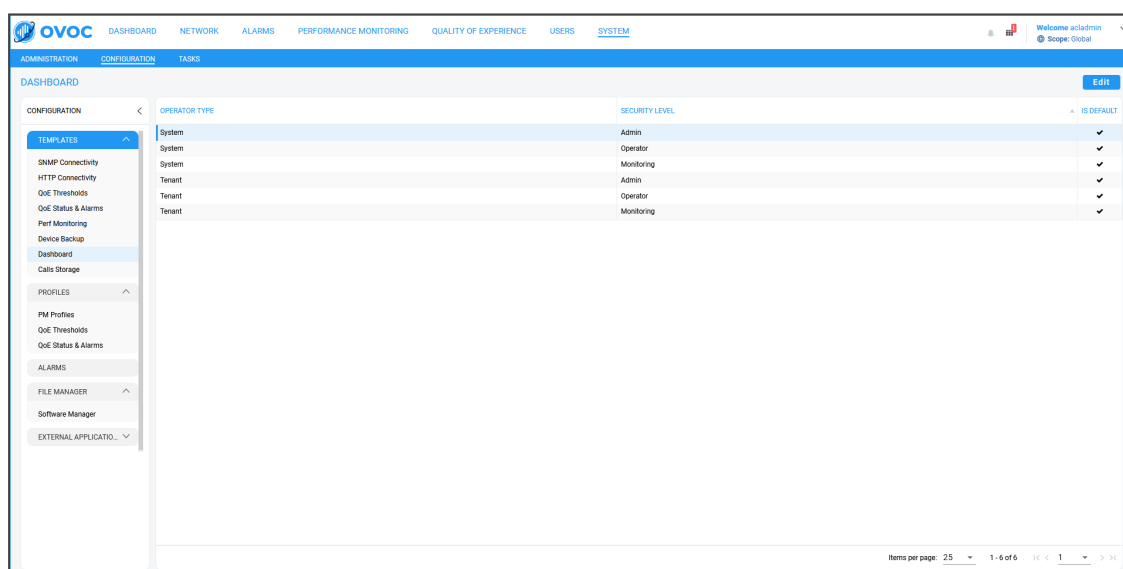
- When enabled (selected), backup is automatically performed daily; all device configuration files (ini, conf and cli) are backed up to the Backup Manager from all devices.
 - When disabled, you can perform manual backup after making changes to a device's configuration (see [Backing up a Device's Configuration using Backup Manager](#) on page 176 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**.

Customizing Default Dashboard per Operator Type | Security Level

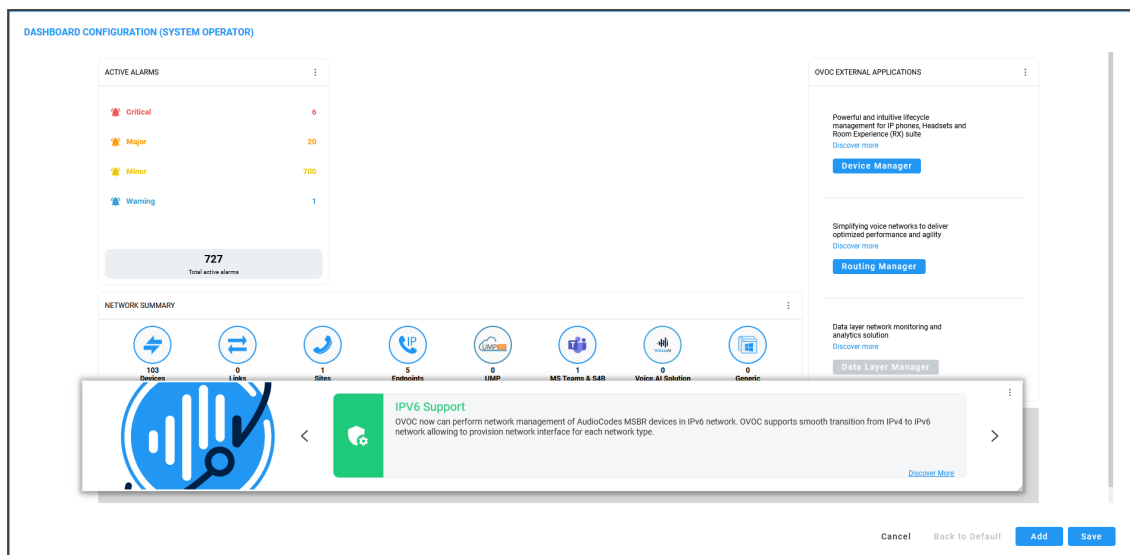
A default dashboard can be customized per Operator Type and Security Level. You can click and drag to rearrange screen elements.

➤ To customize the dashboard:

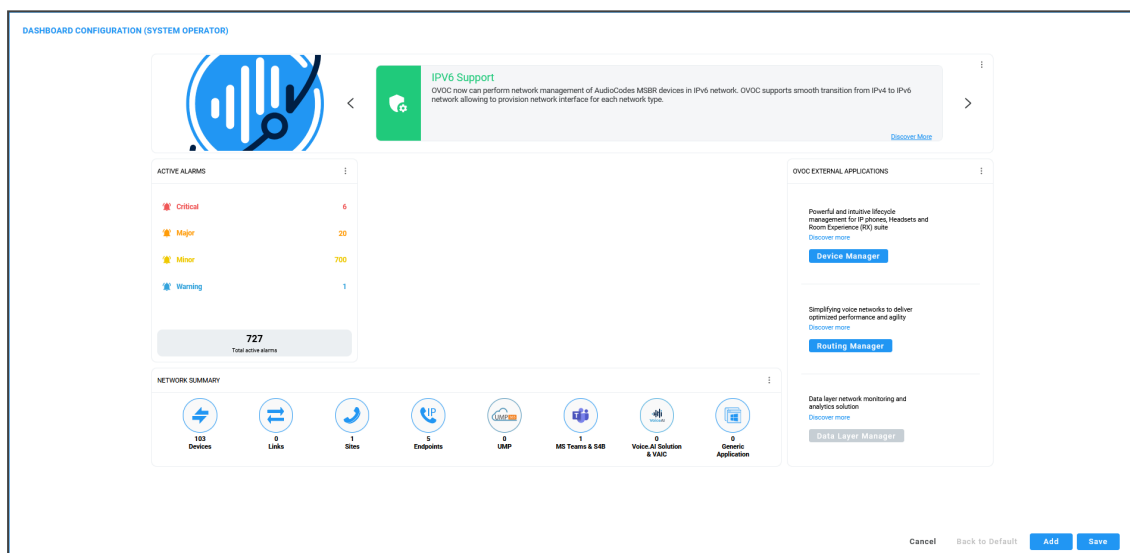
1. Open the Dashboard screen (**System > Configuration > Templates > Dashboard**).



2. Select the Operator Type for which to customize the default dashboard and then click **Edit**.



3. Click and drag screen elements into positions that match your preference and then click **Save**.



Customizing Calls Storage

The OVOC's Calls Storage page enables operators 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 calls storage:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Calls Storage page (**System > Administration > OVOC Server > Calls Storage**).

Figure 3-2: Calls Storage - Maximal

CALLS STORAGE

CALLS STORAGE SETTINGS

Calls Storage level: Maximal

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

3. 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 3-3: Calls Storage - Minimal

CALLS STORAGE

CALLS STORAGE SETTINGS

Calls Storage level: Minimal

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

Figure 3-4: Calls Storage - Recommended

CALLS STORAGE

CALLS STORAGE SETTINGS

Calls Storage level: Recommended

Successful Calls

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

Failed Calls

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

4. Use the matrices below as reference.

Table 3-3: 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 3-4: 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

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

Table 3-5: Recommended

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

Table 3-6: 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	Yes	Yes	Yes

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
	(fair/poor)			
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 enables 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Calls Storage page (**System** > **Administration** > **OVOC Server** > **Calls Storage**) and locate the 'Max Storage Period (Days)' section of the page.

MAX STORAGE PERIOD (DAYS)

Total Calls

1 Day 6 Months 1 Year 365

Calls with Call Flow

1 Day 6 Months 1 Year 365

Statistics

1 Day 6 Months 1 Year 365

☒ URI Statistics

1 Day 6 Months 1 Year 365

☒ Locations Statistics

1 Day 6 Months 1 Year 365



- 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

3. 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.
4. 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.
5. 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.

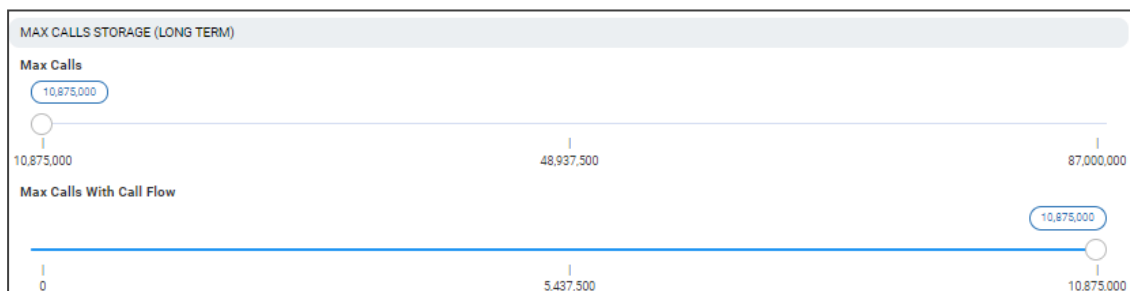
6. Select or clear the **URI Statistics** option for URI statistics to be stored on the OVOC server or not. If you select the option, drag and drop the slider to the maximum number of days you require *URI statistics* to be stored on the OVOC server before they're cleared.
7. Select or clear the **Locations Statistics** option for locations statistics to be stored on the OVOC server or not. If you select the option, drag and drop the slider to the maximum number of days you require *locations statistics* to be stored on the OVOC server before they're cleared.

Configuring Maximum Calls

OVOC allows you to set how many calls with and / or without Call Flow (SIP Ladder) to store.

➤ **To configure how many calls with and / or without Call Flow (SIP Ladder) to store:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Calls Storage page (**System > Administration > OVOC Server > Calls Storage**) and locate the Maximum Calls Storage (Long Term) section.



3. View two sliders:
 - **Max Calls**
 - **Max Calls with Call Flow**
4. Drag to set the **Max Calls** slider. Range depends on the OVOC platform. See the *OVOC IOM* for more information.
5. Drag to set the **Max Calls With Call Flow** slider. Range depends on the OVOC platform. See the *OVOC IOM* for more information.



OVOC server has a defined amount of disk storage space for calls QoE data. OVOC can save calls *with* or *without* call flow (SIP data); calls *without* call flow consume less disk space, calls *with* call flow consume more disk space. To save more calls *with* call flow (which consume more disk space), save fewer *overall* calls.

Max Calls and **Max Calls With Call Flow** are subsets of the overall call total. When you increase calls *with* call flow, the *overall* call total is decreased, and vice versa. Calls *with* call flow cannot exceed the overall call total.

Determining if Reason for Call Termination is SBC-GW or 3rd Party

OVOC enables admins to determine whether AudioCodes SBCs | Media Gateways are the reason for a reported call termination or whether a third-party proprietary device is the reason.

Admin can configure separate lists of reasons for call terminations originated by AudioCodes devices and originated by third-party proprietary devices, for Global and Tenant templates.

OVOC then shows in the Calls List page under the TERMINATION REASON column whether the call was terminated because of a reason related to SBC-GW or third-party device.

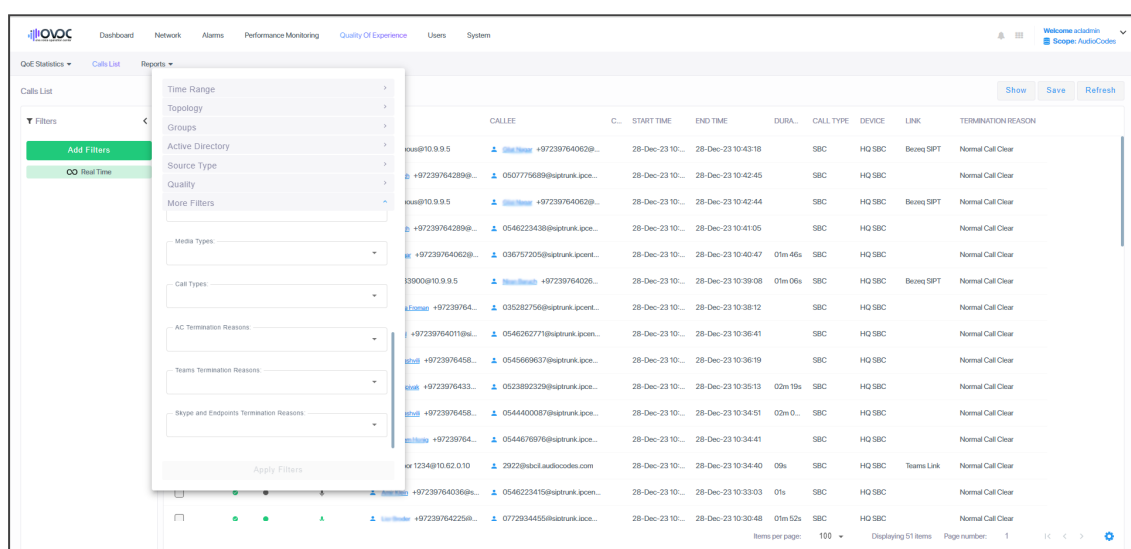
➤ To configure reasons for call terminations originated by SBC/GW or by third-party device:

1. Open the Failed Call Reasons page (**System > Configuration > Templates > Failed Call Reasons**).

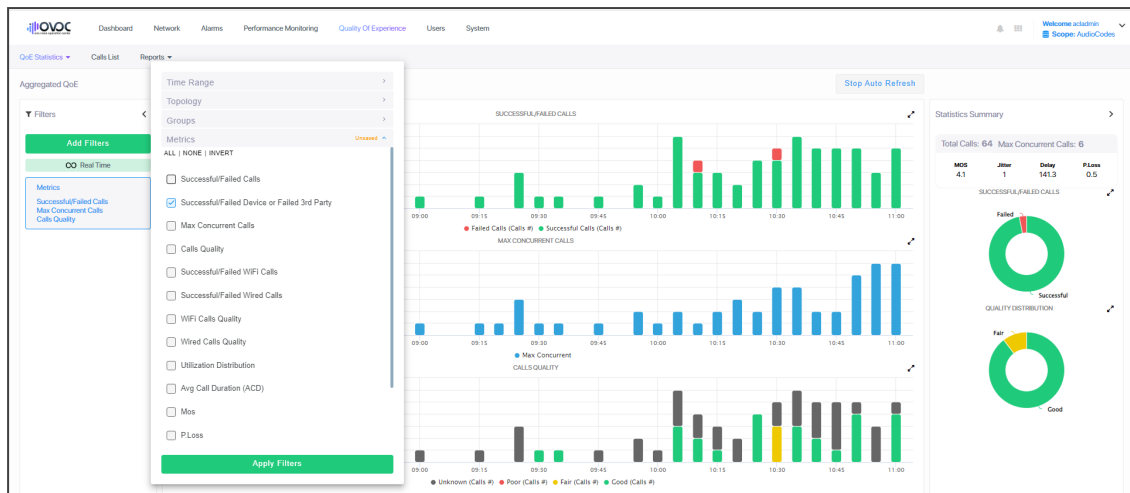
The screenshot shows the OVOC web interface. The top navigation bar includes 'Dashboard', 'Network', 'Alarms', 'Performance Monitoring', 'Quality Of Experience', 'Users', and 'System' (selected). The left sidebar has 'Administration', 'Configuration' (selected), and 'Tasks'. Under 'Configuration', there is a 'Failed Call Reasons' section. The main content area is titled 'Failed Call Reasons' and has a 'Refresh' button. It contains two columns of reasons for call termination. The left column is 'Reasons originated by the device' and the right column is 'Reasons originated by 3rd party'. Both columns have a search bar and a list of reasons. Navigation arrows are between the columns.

Reasons originated by the device	Reasons originated by 3rd party
Release Because Gw Locked	Channel Unacceptable
Release Because Fail	User Congestion
Release Because ACD Threshold Crossed	Release Because Reg Max Threshold Cros...
Release Because CID CMD Failure	Number Changed
Release Because NER Threshold Crossed	Release Because Nortel Xfer Success
Release Because Internal Route	No Route To Destination
Release Because ASR Threshold Crossed	Release Because In Media Limits Exceeded
Release Because Featurekey Changed	Release Because Rtp Conn Broken
	Bc Not Implemented
	Release Because out Admission Failed
	Cug Non Existent
	Release Because User Blocked
	Suspended Call But Call Id Not Exist
	Release Because Unmatched Credentials
	Release Because Transcoding Full
	Perm Fr Mode Conn Operational
	Release Because Voice Device Not Found

2. Select a single termination reason and then click > or < to configure it.
3. Select multiple termination reasons and then click >> or << to configure them simultaneously.
4. Use the feature in OVOC:
 - In the Calls List page, view a call's termination reason under column TERMINATION REASON.
 - [Optionally] Filter the Calls List page by
 - ◆ AC Termination Reasons -or-
 - ◆ Teams Termination Reasons -or-
 - ◆ Skype and Endpoints Termination Reasons



- In the Call Details page (select the call in the Calls List page and click **Show**), view the call's termination reason under Call Termination > REASON displayed in the page's left side pane.
- Filter the QoE Statistics page (**Quality of Experience** > **QoE Statistics** > **Devices | Links**) by 'Successful/Failed Device or Failed 3rd Party' (under 'Metrics') (applies to devices and links only).



- Forward an alarm, including **Failed Calls Device** termination reason and **Failed Calls 3rd Party** termination reason, from the QoE Status & Alarms page (**System > Configuration > Profiles > QoE Status & Alarms**) (add a new alarm or edit an existing listed alarm).

QOE STATUS & ALARMS DETAILS

15

50

Attachments

0 Devices, 0 Links, 0 Sites, 0 Endpoints
[View](#)

Defaults

☐ device
 ☐ link
 ☐ Site
 ☐ Endpoint

THRESHOLD VALUES

	Status Threshold Values		Generate Alarm
Failed Calls Alarm (Calls %)	→ 2 →	→ 10 →	<input checked="" type="checkbox"/>
Poor Quality Calls Alarm (Calls %)	→ 2 →	→ 10 →	<input checked="" type="checkbox"/>
Avg Call Duration Alarm (sec)	→ 5 →	→ 3 →	<input checked="" type="checkbox"/>
Bandwidth Alarm (Kb/sec)	→ 5 →	→ 10 →	<input type="checkbox"/>
Max Concurrent Calls Alarm (Calls #)	→ 5 →	→ 10 →	<input type="checkbox"/>
Failed Calls Device (Calls %)	→ 2 →	→ 10 →	<input type="checkbox"/>
Failed Calls 3rd Party (Calls %)	→ 2 →	→ 10 →	<input type="checkbox"/>

Close

OK

Configuring Profiles

Profiles can be configured by Tenant operators (Tenant scope) who can optionally use the existing default templates configured by the Global scope Admin or create new ones for the following entities:

- [Adding a PM Template](#) on page 307
- [Configuring QoE Thresholds](#) on page 92
- [Configuring QoE Status and Alarms](#) on page 97

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 Configuration page (**System > Configuration > Alarms**).

Figure 3-5: Alarms Settings

The screenshot shows the 'ALARMS CONFIGURATION' page with the following sections:

- ALARMS AUTOMATIC CLEARING**:
 - ☐ Alarms Automatic Clearing
 - Alarms Automatic Clearing Period (days): 30
- EVENTS AUTOMATIC CLEARING**:
 - ☒ Events Automatic Clearing
 - Events Automatic Clearing Period (days): 3
- ALARMS FORWARDING**:
 - Max number of alarms to aggregate in single Email: 10
 - Email alarms aggregation time interval (seconds): 60
- ALARMS SUPPRESSION**:
 - ☐ Alarms Suppression
 - Alarms Suppression Counter Threshold: 20
 - Alarms Suppression Interval (seconds): 2
 - Note: These configurations apply to alarms of the same type and source
- OVOC KEEP-ALIVE**:
 - ☐ OVOC keep-alive
 - OVOC keep-alive trap interval (seconds): 60
 - Important: Alarm forwarding rule containing OVOC Keep-Alive event must be configured

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

Table 3-7: 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. 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.

Setting	Description
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 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.

Setting	Description
OVOC Keep-Alive	Select this option for the OVOC to generate SNMP Keep-alive traps to 3rd-party applications, such as a Syslog server. This trap can be sent to either the SNMP, Syslog or Mail server destination. You can send the Keep-Alive trap to the target destination, according to an existing configured forwarding destination rule.
OVOC Keep-Alive trap interval (seconds)	[Only applicable if 'OVOC Keep-Alive' is selected] Determines how frequently the trap is sent from the OVOC to the configured destination. Default: Every 60 seconds. You can configure a different interval to suit your requirements.
Internal Mail Server From Address	<p>If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'From Address'.</p> <p>For example, if you configure 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:</p> <p>john.brown@enterprisename.com < John Brown ></p> <p>See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under Forwarding Alarms on page 272.</p>
Internal Mail Server Real Name	<p>If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'Real Name'.</p> <p>For example, if you configure 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:</p> <p>john.brown@enterprisename.com < John Brown ></p> <p>See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under Forwarding Alarms on page 272.</p>

Adding Configuration Files to OVOC Software Manager

You can add cmp firmware files, ini files, cli files, conf files and other auxiliary files to 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 OVOC, 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)
- 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 86)
- 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 144)

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

Table 3-8: OVOC Software File Management per Operator Type

Operator Type	Permitted to Perform this File Management
System (except operators with 'Monitoring' security level)	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ 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.

Operator Type	Permitted to Perform this File Management
	<input type="checkbox"/> 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 page 119 for 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 a Configuration Package (ZIP) File

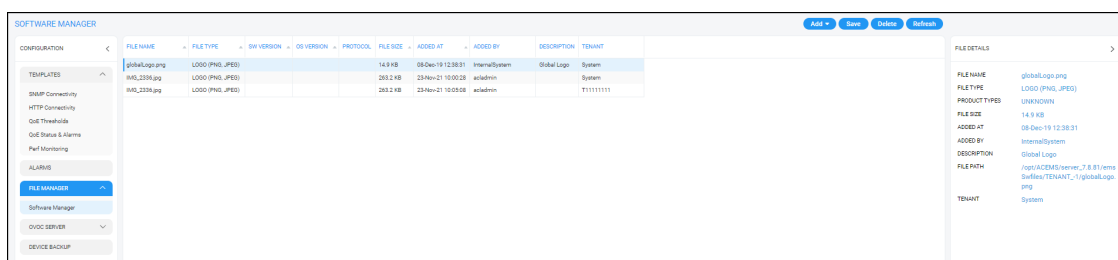
OVOC allows network operators to back up an SBC/Gateway's entire configuration package with a Configuration Package (.zip) file.



- Supported by all SBCs (all devices that support ini or cli files)
- File type name: SBC_ZIP_TYPE
- SBC version 7.4.200 and later is supported

➤ To add a Configuration Package (ZIP) file to OVOC's Software Manager:

- Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
- Open OVOC's Software Manager page (**System > Configuration > File Manager > Software Manager**).



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

ADD AUXILIARY FILE

Tenant*
miryam

File Type
Configuration Package (ZIP)

File Name*
 Choose File

File Description

Close **OK**

4. [Refer to the figure above] From the 'Tenant' drop-down, select the tenant under which to add the auxiliary file.
5. [Refer to the figure above] From the 'File Type' drop-down list, select the auxiliary file to be added, in this case, **Configuration Package (ZIP)**. Other selectable configuration file types are (for example):
 - cli script file for AudioCodes' MSBRs
 - conf file for AudioCodes' MP-202 or MP-204
 - zip file for AudioCodes' VoiceAI Connect
 - JSON file for AudioCodes' Stack Manager
 - ini file for all other AudioCodes devices (except CloudBond, UMP and SmartTAP)
6. Enter a description of the file in the 'File Description' pane for intuitive future file management.
7. Next to the 'File Name' field, click **Choose File** and browse to the file's location.

8. 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.

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 OVOC. When loading the ini file to the device, operators can select one of the following options according to requirements:

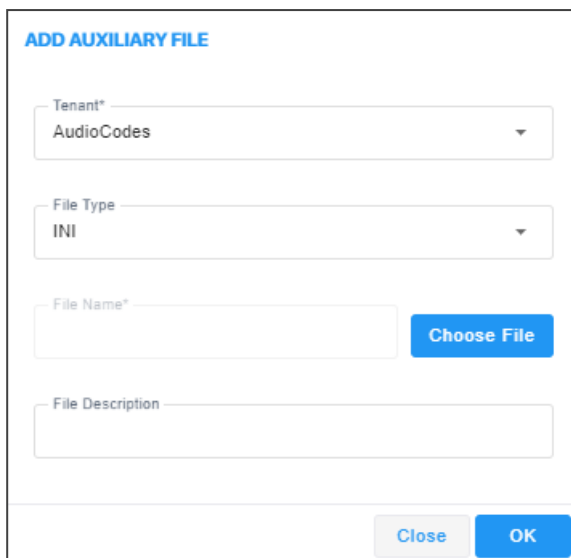
- Full Configuration ini file download – with validation. The device checks the validity of the ini file before the file is loaded to the device, and then the file is loaded to the device.
- Full Configuration ini file download – without validation and apply (for software upgrade). The device does not check the validity of the ini file and the loaded file does not take effect unless the device is restarted.
- Incremental ini file download (the previous configuration remains) Enables loading a subset of certain parameters rather than loading the device's entire configuration. Only those parameters you want to configure are loaded.

➤ To add the ini file to the OVOC:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Software Manager page (**System > Configuration > File Manager > Software Manager**).

FILE NAME	FILE TYPE	FILE SIZE	ADDED AT	ADDED BY	DESCRIBE
<input type="checkbox"/> logo-prade-01.png	LOGO (PNG, JPEG)	131 KB	21-Sep-23 12:2...	Manoap	
<input type="checkbox"/> aadbaadbaad-new-logo-transparent-1.png	LOGO (PNG, JPEG)	43.7 KB	31-Aug-20 11:3...	adadadn	
<input type="checkbox"/> Private-Logo.png	LOGO (PNG, JPEG)	13.5 KB	21-Sep-23 12:3...	Manoap	
<input type="checkbox"/> EXT_Verify_Transfered.cti	CTI	0.0 KB	07-Aug-17 23:3...	ding	
<input type="checkbox"/> m2k.h	INI	6.6 KB	25-Jul-22 12:55...	adadadn	
<input type="checkbox"/> m2k2.h	INI	1.7 KB	31-Aug-23 14:0...	adadadn	
<input type="checkbox"/> SW58C_SF_P720A_20220301.png	CMP	144454.9...	06-Nov-18 23:2...	luth	sw-58c-h
<input type="checkbox"/> HoloTP_CENTOS_SF_P720C0206-070.png	CMP	72000256.0...	23-Nov-20 10:4...	adadadn	

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



4. From the 'Tenant' drop-down, select the tenant under which the ini file will be added.
5. From the 'File Type' drop-down, select **INI** (default) if it isn't selected already.
6. Next to the 'File Name' field, click **Choose File** and browse to the ini 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 ini file is added to the Software Manager.

Adding a cmp File

You can add a firmware (cmp) file to 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 OVOC in order (for example) to change the software version.

➤ To add a cmp file to OVOC:

1. Access either Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open OVOC's Software Manager page (**System > Configuration > File Manager > Software Manager**).
3. Click **Add** and select **Add Software File** from the drop-down menu.

ADD SOFTWARE FILE

Tenant*

miryam

Description

CMP/RMS/RMT*

Choose File

Select Product*

NO GROUP

Close

OK

4. From the 'Tenant' drop-down, select the tenant under which the cmp file will be added.
5. Next to the 'CMP' field, click **Choose File** to navigate to the cmp file's location.
6. Enter a description of the file in the 'Description' pane for intuitive future file management.
7. 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.
8. In the read-only 'OS Version' field, view the CentOS version for Software SBC (6 or 8).
9. From the 'Select Product' drop-down list, select the relevant product corresponding to the cmp or rmt/rms file.
10. From the 'Select Protocol' drop-down, select the protocol. Default: SIP. MGCP and MEGACO are also available.
11. 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 page 119, 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 3-6: File Details

The screenshot shows the 'SOFTWARE MANAGER' interface. On the left is a sidebar with navigation options: CONFIGURATION, TEMPLATES, SNMP Connectivity, HTTP Connectivity, QoS Thresholds, QoS Status & Alarms, Perf Monitoring, ALARMS, FILE MANAGER (selected), Software Manager, OVOC SERVER, and DEVICE BACKUP. The main area displays a table of files. The selected file is 'M3100_SIP_F7.40M3.002.103.cmp'. On the right, a 'FILE DETAILS' pane shows the following information:

Column / File Detail	Description
File Name	M3100_SIP_F7.40M3.002.103.cmp
File Type	CMP
SW Version	7.40M3.002.103
Protocol	SIP
Product Types	Mediant 3000 8410
File Size	23416.5 KB
Added At	02-May-21 12:05:12
Added By	aciadmin
File Path	/opt/ACEMS/server_8.0.1097/e-mswifiles/TENANT_9/M3100_SIP_F7.40M3.002.103.cmp
Tenant	Simulator-TEAMS

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 3-9: CMP Columns / File Details

Column / File Detail	Description
File name	The name of the file. See also Adding a cmp File on page 119.
File Type	CMP
SW Version	The CMP file version
OS Version	The CentOS version for the Software SBC: <ul style="list-style-type: none"> ■ 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

Column / File Detail	Description
Description	A description of the CMP file. See also Adding a cmp File on page 119.
Tenant	The name of the tenant under which the SBC is located.

Adding a cli File

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

➤ To add a cli file to OVOC:

1. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open OVOC's Software Manager page (**System > Configuration > File Manager > Software Manager**).
3. Click **Add** and select **Add Auxiliary File** from the drop-down menu.

ADD AUXILIARY FILE

☐ System File

Tenant*

miryam

File Type

INI

File Name*

Choose File

File Description

Close

OK

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

Adding Auxiliary Files

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

➤ **To add an auxiliary file to the Software Manager:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Software Manager page (**System > Configuration > File Manager > Software Manager**).
3. Click **Add** and select **Add Auxiliary File** from the drop-down menu.

4. From the 'Tenant' drop-down, select the tenant under which to add the auxiliary file.
5. From the 'File Type' drop-down list, select the auxiliary file to be added.



- See the device's *User's Manual* for more information about device-related files.
- The CERTIFICATE file secures the following connections:
 - ✓ Active Directory server (domain controller)
 - ✓ MSSQL Front End server
 - ✓ LDAP User Authentication
- The X.509 PRIVATE KEY, X.509 CERTIFICATE and X.509 TRUSTED ROOT CERTIFICATE files are AudioCodes certificate files that secure the connection between OVOC and the devices.
 - ✓ The X.509 files are for all the security files, including LDAP.
- These files may be default AudioCodes certificate files or files generated by an external CA. For more information about certification implementation, see the *One Voice Operations Center Security Guidelines*.
- A logo image file, to be displayed in report results, can also be added in this screen. See also [Defining a Report](#) on page 463

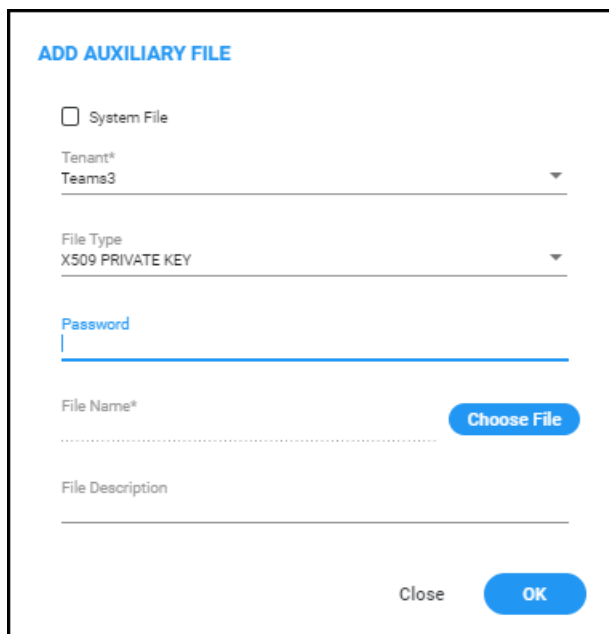
6. Next to the 'File Name' field, click **Choose File** and browse to the file's location.
7. Enter a description of the file in the 'File Description' pane for intuitive future file management and then click **OK**; the file is added to the Software Manager.

Adding X509 Certificate Files

You can download SBC certificate files in a specific transport layer security (TLS) context.

➤ **To download SBC certificate files in a specific TLS context:**

1. In the OVOC's Software Manager (**System > Configuration > File Manager > Software Manager**), click the **Add** button and then select the **Add Auxiliary File** option.



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

- A checkbox labeled "System File" which is currently unchecked.
- A dropdown menu labeled "Tenant*" with "Teams3" selected.
- A dropdown menu labeled "File Type" with "X509 PRIVATE KEY" selected.
- A text input field labeled "Password" with a blue underline.
- A text input field labeled "File Name*" with a blue underline and a "Choose File" button to its right.
- A text input field labeled "File Description" with a blue underline.
- At the bottom right, there are two buttons: "Close" and "OK".

2. From the 'Tenant' dropdown, select the tenant and from the 'File Type' dropdown, select **X509 PRIVATE KEY**.
3. If the X509 Private Key is encrypted, in the 'Password' field then displayed enter the password of the Private Key file.
4. In the Device Management page (**Network > Devices**), select the SBC, click the **Actions** button and from the **Maintenance** submenu, select **Update Auxiliary File**.

UPDATE AUXILIARY FILE

TYPE	S...	NAME	P...	OWNER
INI		2461627...		Tenant: T1
INI		VaicCapt...		Tenant: T1
INI		10.4.220....		Tenant: T1
X509 TRUSTED ROOT CERTIFICATE		root.crt		System
X509 PRIVATE KEY		server.key		System

1 - 5 of 5
|< < 1 > >|

Device TLS Context
Default (Index: 0)

Close
Update

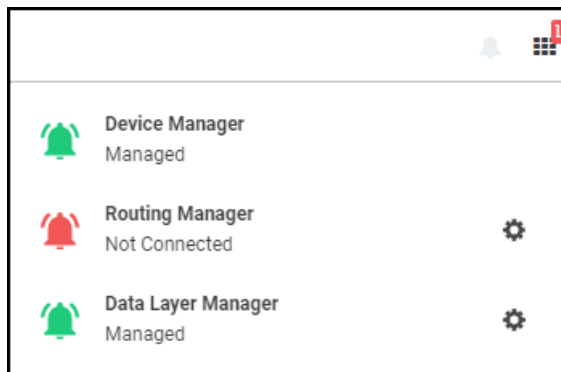
- Select **X509 Private Key**, **X509 Certificate** or **X509 Root Certificate** from the list of auxiliary files displayed in the Update Auxiliary File screen then displayed (shown in the preceding figure); the common available TLS contexts from the selected devices are presented in the Device TLS Context combo box.
- From the Device TLS Context combo box, select a TLS context for the device/s to which the X509 file will be applied and then click **Update**.

Connecting Directly to External Applications

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 (SSO) to:
 - ◆ Device Manager (see [Device Manager](#) below for more information)
 - ◆ Routing Manager (see [ARM](#) below for more information)
 - ◆ Data Layer Manager (see [Data Layer Manager](#) on page 129 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. (Check this, I don't think it is an external app).

➤ 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 3-7: 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 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.
5. Under the OVOC-ARM Communication section, you can select the Secure Communication option for HTTPS secured communications between OVOC-ARM. Specify an ARM operator and their password to allow communication from OVOC to ARM. If an OVOC-ARM connection has already been established, you can opt to configure the 'Change ARM Password' parameter value.
6. Under the ARM-OVOC Communication section, specify a valid OVOC operator. This operator must be a 'System' operator (see [Adding a 'System' Operator](#) on page 58) with a security level of 'Operator'. This operator will then be defined in the ARM to be used by the ARM with REST communication toward OVOC.
7. Click **Submit**.
8. 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.

9. In the external applications menu that opens, click the **Routing Manager** link.
10. 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 Server**) and then click the **Data Layer Manager** option.

Figure 3-8: 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 126 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).
- 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.

Log In to MasterScope

Username

Password

LOG IN

The application opens in a new browser tab.

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. OVOC continues to display them 20 minutes after they're completed. They are then removed from the page.



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

Displaying the Status of Tasks Currently Under Execution

Multiple AudioCodes devices can be added to OVOC. 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 3-9: Task - Add Multiple AudioCodes Devices

MULTIPLE AC DEVICES DETAILS

General SNMP HTTP First Connection

Name Prefix*
NY

Description
Adding new branch

Tenant
Tring

Region*
AutoDetection

Configured Device By
IP Address Range

From*
10.1.1.1

To*
10.1.1.10

Address

Close OK

- [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.



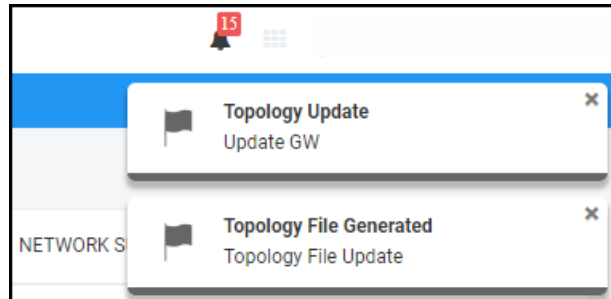
To configure the *timeout* of the notification pop-up, see [Configuring Operator Authentication Locally, in OVOC](#) on page 53 and refer to the parameter 'Notifications display time (sec)'. The default is 3 seconds. Configuring the parameter to 0 disables the notification pop-up feature.

- 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.

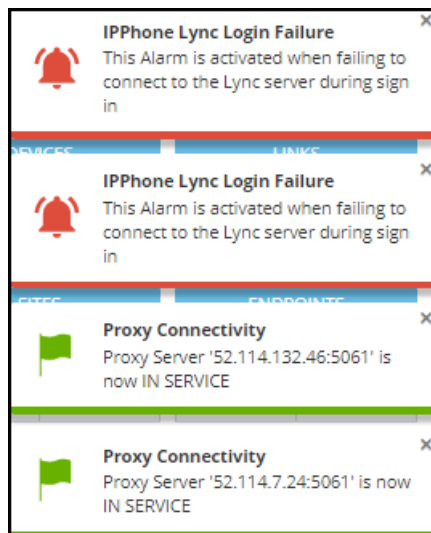
➤ **To view the notifications history:**

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

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 *

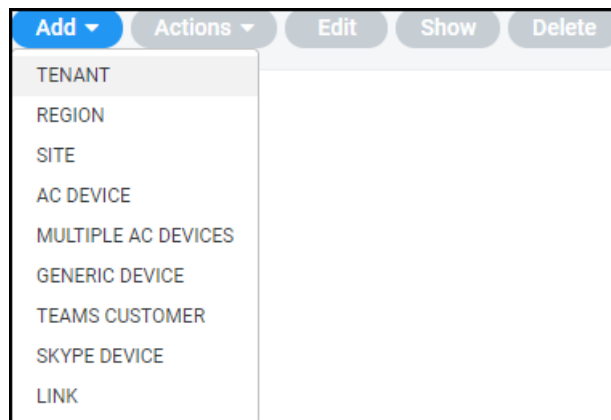
Adding a Tenant



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**.



2. Select **Tenant**.

TENANT DETAILS

General
SNMP
HTTP
Operators
License
ZOOM
Operator Connect

Tenant Name
audio-code_co_il

Description

Is Default
False

HTTP Operator (License Pool)

Users URI Regexp
*

Azure Tenant ID
bb8950c6-9262-4757-92eb-212e113ec24c

Subnet (CIDR Notation)

None

Masked Digits Number
4

Close
OK

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

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 215). After selecting a 'tenant' operator, the association cannot be removed (see also Adding a 'Tenant' Operator on

Parameter	Description
	page 65) and they're automatically displayed under the Operators tab (see following).
Description	Enter a tenant description to facilitate effective management later.
Users URI Regexp	<p>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 <i>on calls made exclusively from URIs in a specific tenant</i>. Operators can run a regional expression to find the URIs associated with the specific tenant and then generate statistics exclusively on them.</p> <ul style="list-style-type: none"> ■ 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. <p>Note: If in a five minute interval there are more than 2000 different URIs, the URI statistics for this five minute interval <i>will not</i> be saved.</p>
Subnet (CIDR Notation)	Enter the tenant's subnet mask. Must be in prefix format x.x.x.x/y. For example: 255.255.0.0/16. For any <i>region</i> under the tenant, subnet mask is not mandatory, but if it is configured, its subnet mask must be within the tenant's, for example, 255.255.0.0/1.
Masked Digits Number	<p>Enter the number of digits that will be masked from the phone number when in 'Privacy Mode'. The parameter defines the number of digits that will be masked from the phone number for the tenant. For information about configuring a <i>global</i> 'Masked Digits Number', see under Configuring Privacy Mode, Concealing Users Calls Details on page 84.</p> <p>By default, OVOC conceals the <i>last four digits</i> from users' phone numbers. The configuration can be changed on-the-fly if necessary.</p> <p>Masking rules apply to both Calls List page and to the Call Details screen (see Accessing the Calls List on page 371 and Showing Call Details on page 382).</p>

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

TENANT DETAILS

General
SNMP
HTTP
Operators
License

☒ Use System SNMP Profile

SNMP V2

SNMP Read Community

Trap Community

SNMP Write Community

SNMP V3

Security Name
OVOCUser

Authentication Protocol
SHA

Privacy Protocol
AES_128

Security Level
Authentication and Privacy

Authentication Key

Privacy Key

Close
OK

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

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.

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

TENANT DETAILS

General
SNMP
HTTP
Operators
License

☒
Use System HTTP Profile

Device Admin User
Admin

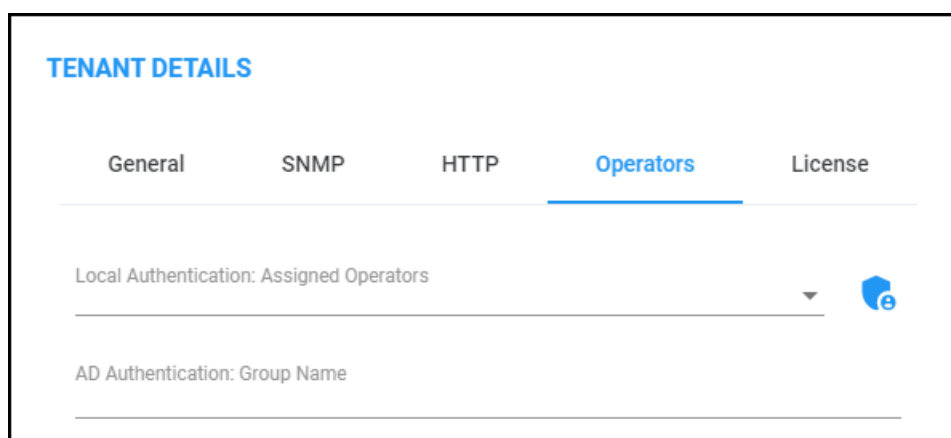
Device Admin Password

Communication Protocol
HTTP

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



Parameter	Description
Use System HTTP Profile	This option is selected by default. Only available when adding a tenant. The option enables customers to use an HTTP profile of the system, eliminating the need for the HTTP password to be resent as plain text between the server and OVOC GUI. The option tightens customer security.
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.
Communication Protocol	From the drop-down, select either: <ul style="list-style-type: none"> ■ HTTP (default) ■ HTTPS The default is taken from main HTTP template. Note: Configure OVOC to use HTTPS to connect to an SBC / Gateway if you configured the device's parameter 'Secured Web Connection (HTTPS)' to HTTPS Redirect for Single-Sign On (SSO) from OVOC to the device.

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




TENANT DETAILS

General SNMP HTTP **Operators** License

Local Authentication: Assigned Operators  

AD Authentication: Group Name

10. Use the following table as reference.

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 65 for more information about configuring 'tenant' type operators.
	Operator authentication can be configured locally, in OVOC (see Configuring Operator Authentication Locally, in OVOC on page 53). Click the icon to add a new 'tenant' type operator; the 'Tenant Operator Details' screen opens (see Adding a 'Tenant' Operator on page 65). 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 OVOC, 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 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: <ul style="list-style-type: none"> • Configuring Operator Authentication Centrally with Azure Active Directory on page 46 • Configuring Operator Authentication Centrally using an LDAP Server on page 41

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

TENANT DETAILS

General

SNMP

HTTP

Operators

License

Calls Storage Entities

ANALYTICS

☒ Analytics Status

VOICE QUALITY

Devices

105

Total: 1,000

Allocated: 215

Free: 785

22%

Sessions

1000

Total: 20,000

Allocated: 1,110

Free: 18,890

6%

Endpoints

10

Total: 100

Allocated: 30

Free: 70

30%

Users

15

Total: 4,000

Allocated: 125

Free: 3,875

3%

Reports

100

Total: 5,000

Allocated: 1,110

Free: 3,890

22%

ENDPOINTS MANAGEMENT

Endpoints

6

Total: 3,000

Allocated: 1,016

Free: 1,984

34%

LICENSE POOL

SBC Managed Devices

10%

Close

OK

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

License Pool	Description
Analytics Status	Enables the Analytics license for viewing snapshots of Tenant's SBC and Teams device data (see Displaying Analytics on page 327).
Voice Quality	
Devices	Enter the number of SBCs, gateways and MSBRs that can be monitored in this tenant.

License Pool	Description
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	<div data-bbox="566 555 1385 647"> </div> <p>Click the field and from the arrow that is then displayed select the number of reports to allocate to the tenant. In the example here, 0 can be allocated; if you select 1, the indication bar turns red alerting you that the total has been exceeded.</p>
Endpoints Management	
Endpoints	Enter the number of endpoints the Device Manager application supports for this tenant.
License Pool	
SBC Managed 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 Media Sessions	Enter the number of concurrent call sessions supported by the SBCs in your deployment.
SBC Registrations	Enter the number of SIP endpoints that can register with the SBCs allowed by your license.
SBC Signaling	Enter the number of SBC signaling sessions supported by the SBCs in your deployment.
SBC Transcoding	Enter the number of SBC transcoding sessions supported by the SBCs in your deployment.
CB 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

License Pool	Description
	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 PBX Users	Support pending. Currently unsupported.
CB Analog Devices	Support pending. Currently unsupported.
CB Voicemail Accounts	Support pending. Currently unsupported.

13. Click **OK** and then click **Call Storage Entities**.

For each of the statistics categories below, the Tenant allocation is displayed as a percentage of the Total allocation for the OVOC instance. The allocation is displayed using a slider bar and absolute units.

TENANT DETAILS

General
SNMP
HTTP
Operators
License
Calls Storage Entities

Total Calls

80000

Total: 6,000,000
Allocated: 81,000
Free: 5,919,000

Calls with Call Flow

9332

Total: 466,600
Allocated: 10,332
Free: 456,268

devices Statistics

1200000

Total: 12,000,000
Allocated: 1,201,000
Free: 10,799,000

links Statistics

100000

Total: 12,000,000
Allocated: 100,111
Free: 11,899,889

Sites Statistics

6000000

Total: 12,000,000
Allocated: 6,001,000
Free: 5,999,000

Endpoints Statistics

3

Total: 12,000,000
Allocated: 10,003
Free: 11,989,997

Users Statistics

0

Total: 12,000,000
Allocated: 1,000
Free: 11,999,000

URI Statistics

240000

Total: 12,000,000
Allocated: 241,000
Free: 11,759,000

Location Statistics

240000

Total: 12,000,000
Allocated: 241,000
Free: 11,759,000

Close
OK

Parameter	Description
Total Calls	Enter the number of storage units for SBC and Teams calls.
Calls with Call Flow	Enter the number of storage units for Call Details including SIP Ladder (SIP Call Flow).
devices Statistics	Enter the number of storage units for statistics from managed devices.
links Statistics	Enter the number of storage units for statistics from managed links.

- 143 -

Parameter	Description
Sites Statistics	Enter the number of storage units for statistics from site locations.
Endpoints Statistics	Enter the number of storage units for statistics from managed endpoints.
Users Statistics	Enter the number of storage units for statistics from managed users.
URI Statistics	Enter the number of storage units for Calls URI statistics.
Location Statistics	Enter the number of storage units for statistics from managed AD locations.

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.

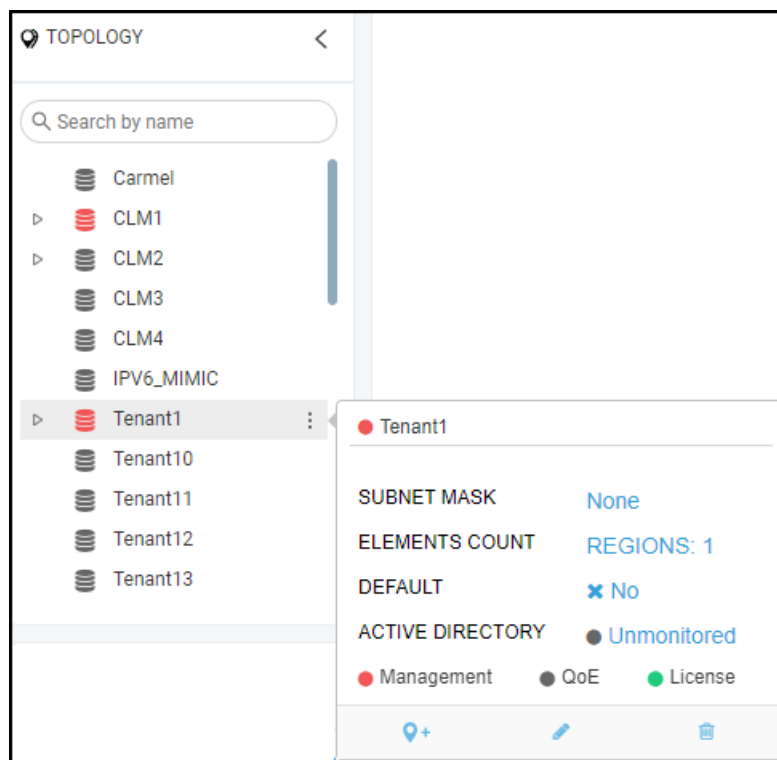


The behavior of the tenant logo is subject to the following circumstances:

- 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, the AudioCodes logo will be displayed when that operator logs in to OVOC.
- If a system operator logs in to the OVOC, the AudioCodes logo will always be displayed.

➤ To add a logo image:

1. In the Network Topology page, hover your mouse over the tenant and then click the vertical ellipsis : displayed next to the tenant.

Figure 4-1: Edit Tenant



2. Click the edit icon ; in the Tenant Details screen that opens (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 4-2: Tenant Details

TENANT DETAILS

General

SNMP

HTTP

Operators

License

Tenant Name
Tenant1

Description

Is Default
False

HTTP Operator (License Pool)

Users URI Regexp
*

Azure Tenant ID

Subnet (CIDR Notation)

None

Masked Digits Number
4

Close

OK

- 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 463].
- 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 123 from the 'File Type' drop-down in the Add Auxiliary File screen.
- See also [Adding Configuration Files to OVOC Software Manager](#) on page 114 for related information.
- See also [Defining a Report](#) on page 463 for related information.
- For information about the other parameters in the Tenant Details screen, use the tables in [Adding a Tenant](#) on page 133 for reference.

Defining a Tenant Logo - Example

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

Figure 4-3: Edit Tenant


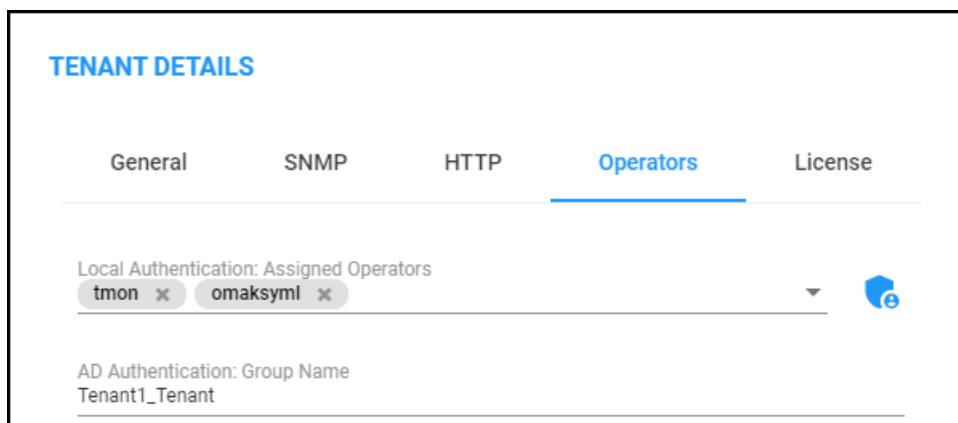
2. In the Tenant Details screen that opens, navigate to and select the tenant's logo image from the 'Tenant Logo' drop-down or click the upload icon  to upload it if necessary.

Figure 4-4: Tenant Details - General - Tenant Logo

3. Click the **Operators** tab.

Figure 4-5: Tenant Details - Operators



The screenshot shows the 'TENANT DETAILS' configuration page with the 'Operators' tab selected. The 'Local Authentication: Assigned Operators' section displays two operators: 'tmon' and 'omaksym', each with a close icon. The 'AD Authentication: Group Name' is set to 'Tenant1_Tenant'. A blue shield icon with a plus sign is visible on the right side of the assigned operators list.

TENANT DETAILS

General SNMP HTTP **Operators** License

Local Authentication: Assigned Operators

tmon x omaksym x

AD Authentication: Group Name

Tenant1_Tenant


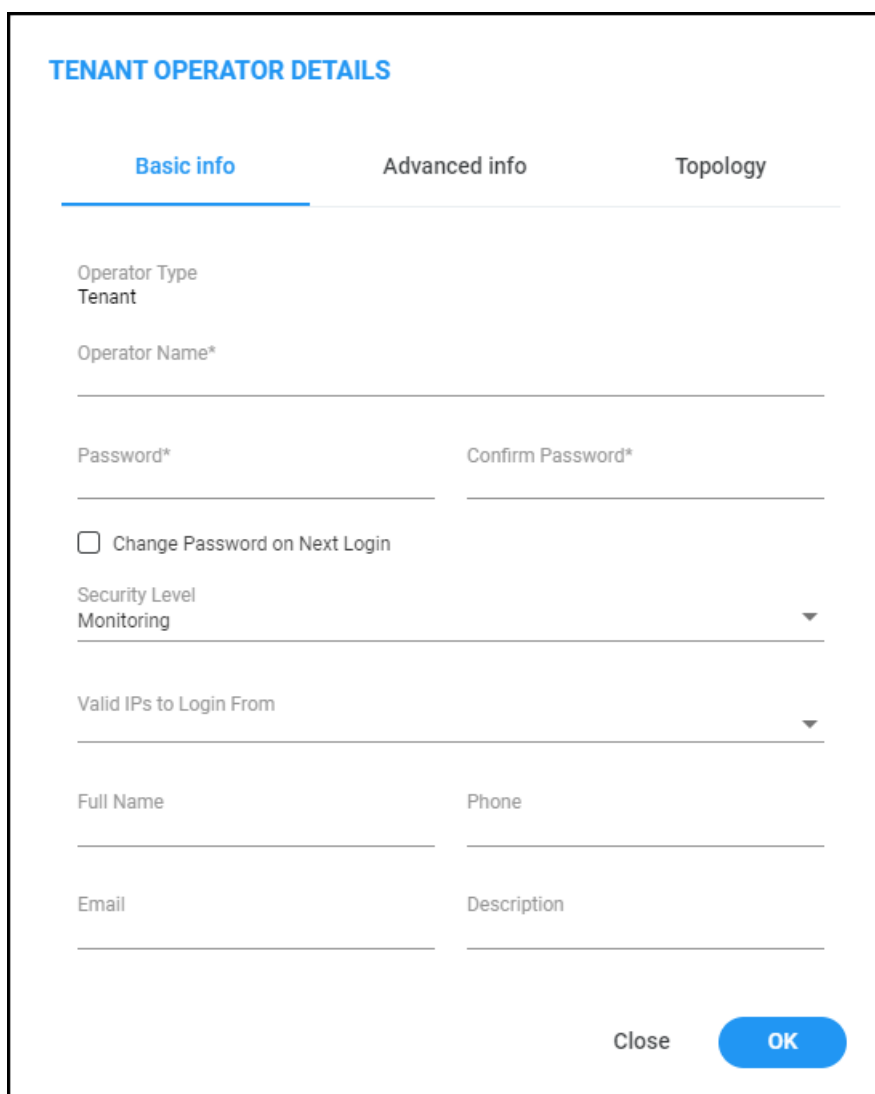
4. Click the  icon and then in the Tenant Operator Details screen that opens, add a new operator.

Figure 4-6: Tenant Operator Details



The screenshot shows the 'TENANT OPERATOR DETAILS' configuration page with the 'Basic info' tab selected. The page contains several input fields for operator information, including Operator Type, Operator Name, Password, Confirm Password, Security Level, Valid IPs to Login From, Full Name, Phone, Email, and Description. There is also a checkbox for 'Change Password on Next Login'. The 'Close' and 'OK' buttons are at the bottom right.

TENANT OPERATOR DETAILS

Basic info Advanced info Topology

Operator Type

Tenant

Operator Name*

Password* Confirm Password*

☐ Change Password on Next Login

Security Level

Monitoring

Valid IPs to Login From

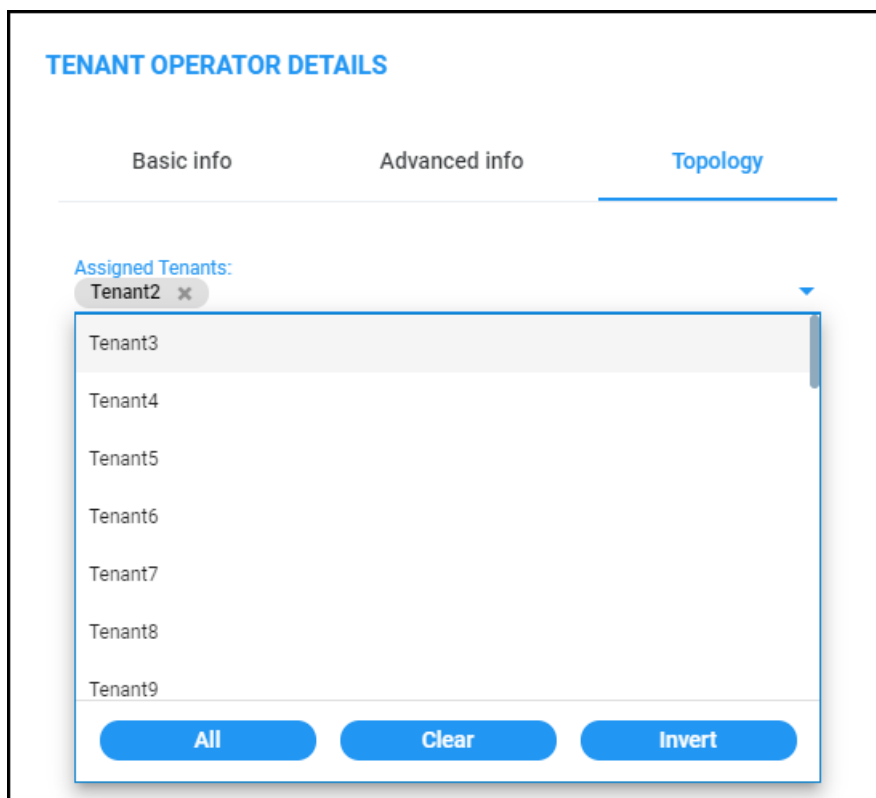
Full Name Phone

Email Description

Close OK

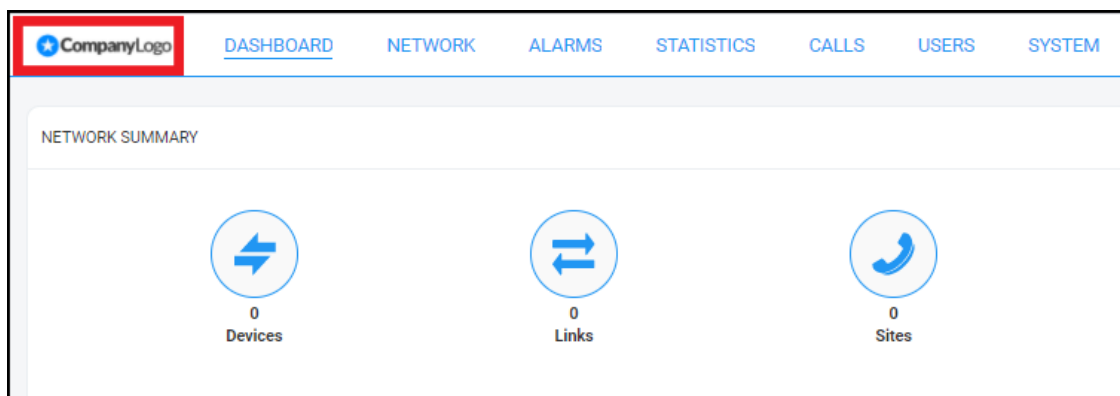
5. Under the **Basic Info** tab, enter the operator's name and credentials and configure the parameters as described in [Adding a 'System' Operator](#) on page 58.
6. Under the **Advanced info** tab, configure the parameters as described in [Adding a 'System' Operator](#) on page 58.
7. Under the **Topology** tab, navigate to and select the tenant to assign to the operator.

Figure 4-7: Tenant Operator Details - Topology



8. Click **OK** 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 4-8: Tenant logo displayed in OVOC GUI





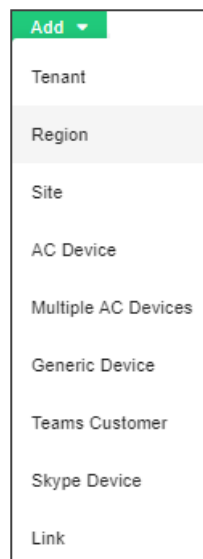
- Multiple tenants can be chosen.
- If you choose a single tenant and that tenant has a logo, you'll view the tenant logo when you log in with that tenant operator.

Adding a Region

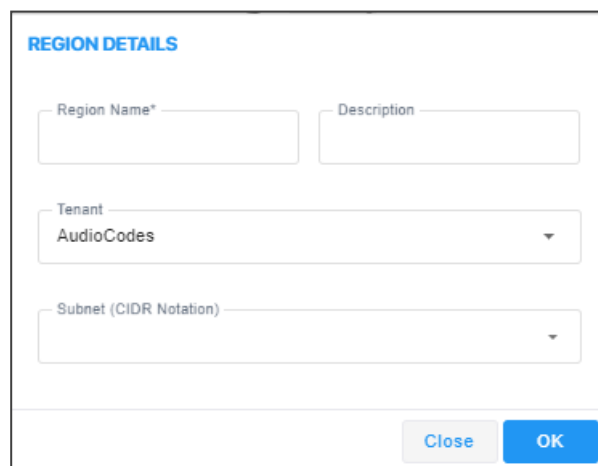
ITSPs or enterprises manage devices in regions. A region typically represents a geographical area for the ITSP or the enterprise. Devices are added to OVOC under a tenant, after defining one.

➤ **To add a region:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Network Topology page (**Network > Topology**).
3. Click **Add** and select Region.



4. View the Region Details screen.

A screenshot of a form titled 'REGION DETAILS'. It contains several input fields: 'Region Name*' (a text box), 'Description' (a text box), 'Tenant' (a dropdown menu with 'AudioCodes' selected), and 'Subnet (CIDR Notation)' (a dropdown menu). At the bottom right, there are two buttons: 'Close' and 'OK'.

5. From the 'Tenant' drop-down, select a tenant that you configured previously.
6. Define the region's name and type in a description to facilitate operator-friendly management later.

7. [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.
8. Click **OK**; the region is added to OVOC.

Adding AudioCodes Devices

AudioCodes devices can be added to 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 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
 - ◆ When a WebSocket tunnel is used for communication between the OVOC server and certain devices (clients), these devices first initiate the HTTPS tunnel connection to OVOC. For more information, see Section 'Configure OVOC Cloud Architecture Mode' in the *OVOC IOM Manual*.
- **Adding Devices Manually** from OVOC (OVOC-initiated connection) (see Section [Adding AudioCodes Devices Manually](#) on page 157)
 - **Predefined by IP address:** Devices are manually added to OVOC by IP address, under the correct entity
 - **Predefined by Serial Number:** Devices are manually added to OVOC by serial number, under the correct entity
- **Adding Devices with First Time Provisioning** (semi-automatic) (see Section [Enabling Initial Connection Provisioning](#) on page 163)
 - 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 OVOC's Network Topology. Devices can be added after acquiring them from AudioCodes, or, as the case may be, after acquiring OVOC from AudioCodes and adding OVOC to an existing deployment of devices.

OVOC's Automatic Detection feature enables devices to be *automatically connected and added* to 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 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

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 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 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 OVOC but OVOC does not detect the device, the device sends an event to OVOC; OVOC takes the information from the event and automatically connects the device.

Figure 4-9: Web interface: SNMP Community Strings

The screenshot shows the 'SNMP Community Settings' page in the OVOC web interface. The left sidebar contains navigation options: TIME & DATE, WEB & CLI (with sub-items: Local Users (2), Authentication Server, Web Settings, CLI Settings, Access List, Additional Management Interfaces (0)), SNMP (with sub-items: SNMP Community Settings (highlighted), SNMP Trap Destinations, SNMP Trusted Managers, SNMP V3 Users (1)), LICENSE, and MAINTENANCE. The main content area is titled 'SNMP Community Settings' and is divided into two sections: GENERAL SETTINGS and MISC. SETTINGS. In GENERAL SETTINGS, 'Disable SNMP' is set to 'No'. Below this are two sections: READ-ONLY COMMUNITY STRINGS and READ-WRITE COMMUNITY STRINGS, each with five input fields. In MISC. SETTINGS, 'Trap Community String' is 'trapuser', 'Trap Manager Host Name' is empty, and 'Activity Trap' is set to 'Disable'. At the bottom right are 'Cancel' and 'APPLY' buttons.

Figure 4-10: Web interface: SNMP Trap Destinations

The screenshot shows the 'SNMP Trap Destinations' page in the OVOC web interface. The left sidebar is identical to Figure 4-9, but 'SNMP Trap Destinations' is highlighted under the SNMP section. The main content area is titled 'SNMP Trap Destinations' and contains a table with the following data:

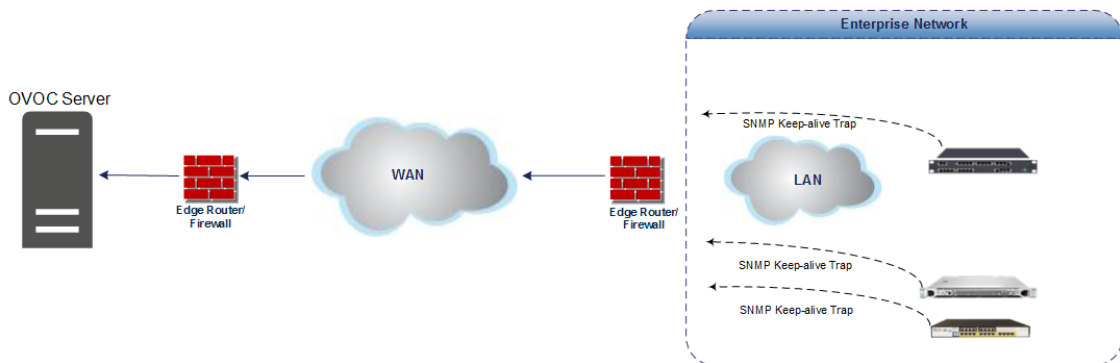
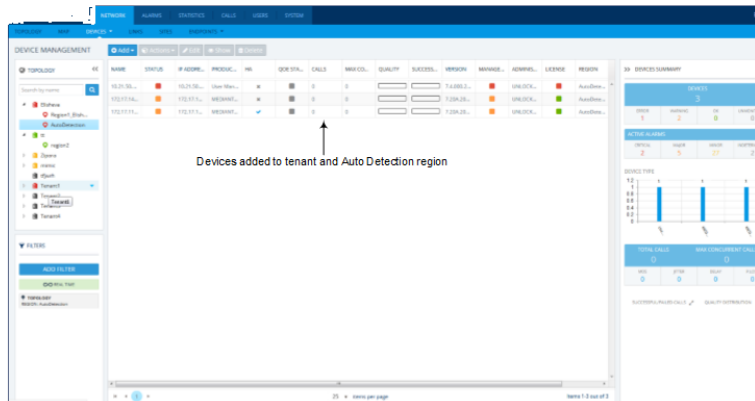
	NAME	IP ADDRESS	TRAP PORT	TRAP USER	TRAP ENABLE
<input checked="" type="checkbox"/>	SNMP Manager 1	172.17.140.203	162	v2cParams	Enable
<input type="checkbox"/>	SNMP Manager 2	0.0.0.0	162	v2cParams	Enable
<input checked="" type="checkbox"/>	SNMP Manager 3	10.3.180.235	162	v2cParams	Enable
<input checked=""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

At the bottom right are 'Cancel' and 'APPLY' buttons.

When devices are deployed in a private network using Network Address Translation (NAT), they can connect to the internet so long as their connection with 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 OVOC server. This allows OVOC to perform SNMP SET and GET commands at any time. When devices are added to OVOC, OVOC recognizes them according to their field 'sysDesc' and their serial number, and according to the entries in OVOC's 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. OVOC recognizes these changes after devices are reset.

Figure 4-11: AudioCodes Devices Added to OVOC



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

```
SNMPPort_0 = 161
SNMPManagerTrapPort_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
```

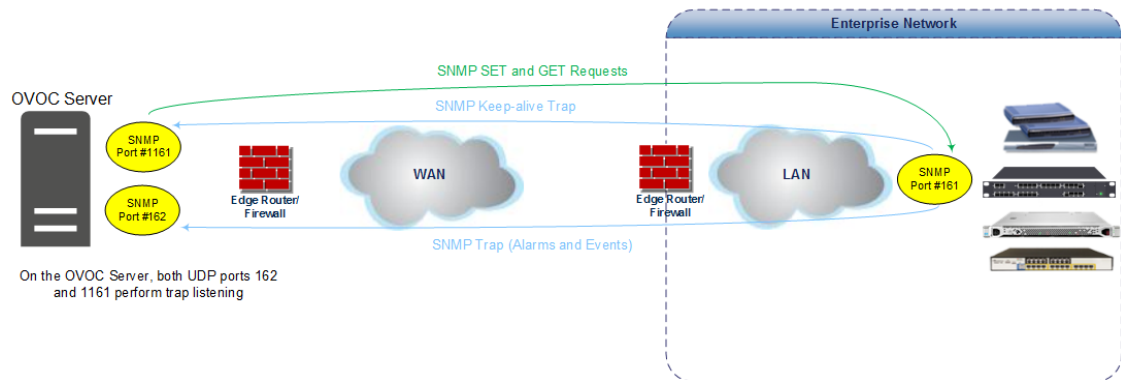
After devices are connected to the power supply and network, they reboot, initialize and send a coldStart trap to the OVOC server. When the coldStart trap (or keep-alive trap, if

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

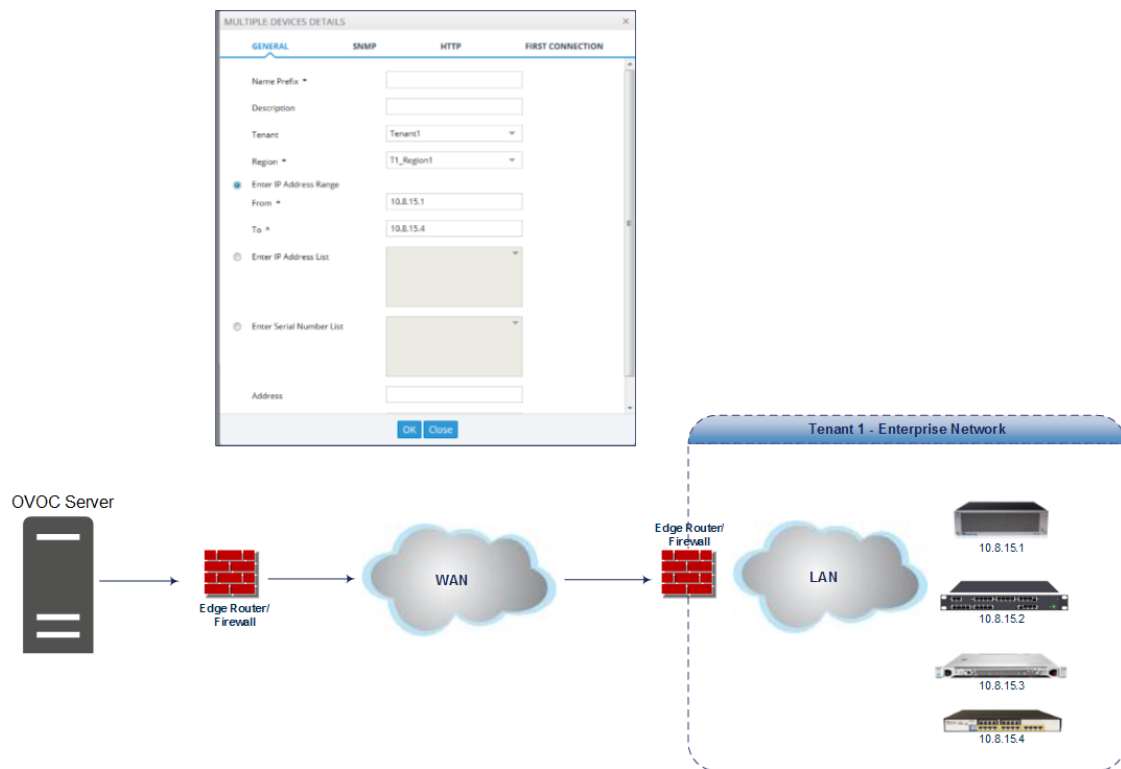
Figure 4-12: OVOC Server and Devices SNMP Connections



Adding AudioCodes Devices Manually

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

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



➤ To manually add the devices:

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

Figure 4-14: AC Device | Multiple AC Devices



The Multiple AC Devices Details screen opens:

MULTIPLE AC DEVICES DETAILS

General SNMP HTTP First Connection

Name Prefix* _____ Description _____

Tenant Carmel ▼ Region* _____ ▼

Configured Device By IP Address Range _____ ▼

From* _____ To* _____

Address _____

Close **OK**

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 133.
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 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 OVOC cannot resolve the IP address, 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 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:

AC DEVICE DETAILS

General
SNMP
HTTP
SBA
First Connection

☒ SNMP v2
☐ SNMP v3

SNMP Read Community

SNMP Write Community

Close



Before connecting a device to OVOC, an SNMP connection between the device and 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 OVOC and agents, as well as user-based access control.

The SNMP connection must be configured on both 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 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 OVOC. If different values are configured on the device, it's added to OVOC as 'Unknown' until updated in 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:

MULTIPLE AC DEVICES DETAILS

General
SNMP
HTTP
First Connection

☐ SNMP v2
☒ SNMP v3

☒ Use Tenant SNMP Profile

Security Name <div style="border: 1px solid #ccc; padding: 2px;">OVOCUser</div>	Security Level <div style="border: 1px solid #ccc; padding: 2px;">Authentication and Privacy</div>
Authentication Protocol <div style="border: 1px solid #ccc; padding: 2px;">SHA</div>	Authentication Key <div style="border: 1px solid #ccc; padding: 2px;"></div>
Privacy Protocol <div style="border: 1px solid #ccc; padding: 2px;">AES_128</div>	Privacy Key <div style="border: 1px solid #ccc; padding: 2px;"></div>



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.

MULTIPLE AC DEVICES DETAILS

General SNMP **HTTP** First Connection

☒ Use Tenant HTTP Profile

Device Admin User
Admin

Device Admin Password

Communication Protocol
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. From the 'Communications Protocol' dropdown, select **HTTPS** to secure the connection with the device. 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 must configure OVOC to use **HTTPS** to connect to an SBC / Gateway if you configured the device's parameter 'Secured Web Connection (HTTPS)' to **HTTPS Redirect** for Single-Sign On (SSO) from OVOC to the device.
- 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.

AC DEVICE DETAILS

General
SNMP
HTTP
SBA
First Connection

☐ Enable SBA

SBA Configured By
IP Address

IP Address

SNMP Read Community

SNMP Write Community

Description

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 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 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 OVOC.

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

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. 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.

3. From the now-activated 'Configuration File' drop-down, select the applicable file.
4. 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.

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



A Media Gateway device housing two blades can be added to the 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 Media Gateway device housing two blades that was added to the OVOC using two IP addresses in OVOC versions earlier than Version 7.4.3000, and then add them again using a single IP address. After this action, the Alarms History and QoE calls & statistics history is cleared.

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

Before Enabling the Feature

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

➤ To validate the ini file:

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



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

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 when adding a single AudioCodes device and 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 OVOC Software Manager](#) on page 114 for details.

Figure 4-15: First Connection

MULTIPLE AC DEVICES DETAILS

General SNMP HTTP **First Connection**

☐ Enable Initial Connection Provisioning

Configuration File (INI/CLI/CONF)

Firmware File (CMP/RMS/RMT)

➤ 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 152 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 4-16: Alarms Journal

JOURNAL								
FILTERS <<		SEV...	DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	TENANT
ADD FILTER								
REAL TIME								
MORE FILTERS								
			30-Jul-17 11:48:12	AutoDetection		CONFIGURATION_ADD	Add Region: AutoDetection in tenant Singapore	Singapore
			30-Jul-17 11:45:53	System		CONFIGURATION_RE...	Endpoint name 0008P3FF6BA.192.168.3.124 was deleted	AudioCodes
			30-Jul-17 11:35:04	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.Tenants subnet masks was changed fro...	Singapore
			30-Jul-17 11:34:43	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.	Singapore
			30-Jul-17 11:31:11	Singapore		CONFIGURATION_ADD	New Tenant Singapore was added.	Singapore
			30-Jul-17 11:30:53	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.38.2.9 with Administration security lev...	System
			30-Jul-17 11:29:23	System	EMS Server	SECURITY_EDIT_OPE...	Update amil user details: password was changed to "*****"	System
			30-Jul-17 11:29:23	System	EMS Server	SECURITY_EDIT_OPE...	Changing user password: amil	System
			30-Jul-17 11:27:42	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.16.2.10 with Administration security lev...	System
			30-Jul-17 11:27:06	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.1.11.1.1 with Administration security lev...	System

2. Optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 231), Topology (see [Filtering by 'Topology'](#) on page 243), Source Type (see [Filtering by 'Severity'](#) on page 256) or More Filters (see [Filtering the Alarms Journal by 'More Filters'](#) on page 265).
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 4-17: Alarms Journal – Entity Info

JOURNAL								
FILTERS <<		SEV...	DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	TENANT
ADD FILTER								
REAL TIME								
MORE FILTERS								
			30-Jul-17 11:58:22	0008P3FF6BA...		CONFIGURATION_UP...	Endpoint null, update fields: Tenant ID = 79117	Singapore
			30-Jul-17 11:55:59	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.1.1.117 with Administration security lev...	System
			30-Jul-17 11:48:12	AutoDetection		CONFIGURATION_ADD	Add Region: AutoDetection in tenant Singapore	Singapore
			30-Jul-17 11:45:53	System		CONFIGURATION_RE...	Endpoint name 0008P3FF6BA.192.168.3.124 was deleted	AudioCodes
			30-Jul-17 11:35:04	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.Tenants subnet masks was changed fro...	Singapore
			30-Jul-17 11:34:43	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.	Singapore

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

Figure 4-18: Critical Alarm – Initial Connection Provisioning Failed

SEVERITY	RECEIVED DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION
	24-Jul-17 16:47:04	11.200.1.2	EMS Server/11.200.1.2	Pre-Provisioning	Pre-Provisioning Process Failed.Device Name: 11.200.1.2, Device IP: 11.200.1.2, Device ...
	24-Jul-17 16:46:58	11.200.1.2	EMS Server	Topology Update	Update GW
	24-Jul-17 16:46:58	11.200.1.2	EMS Server	GW Connection Alarm	Connection established



If Initial Connection Provisioning was unsuccessful, download the configuration or firmware file to the device as shown in [Backing Up](#) on page 345.

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.



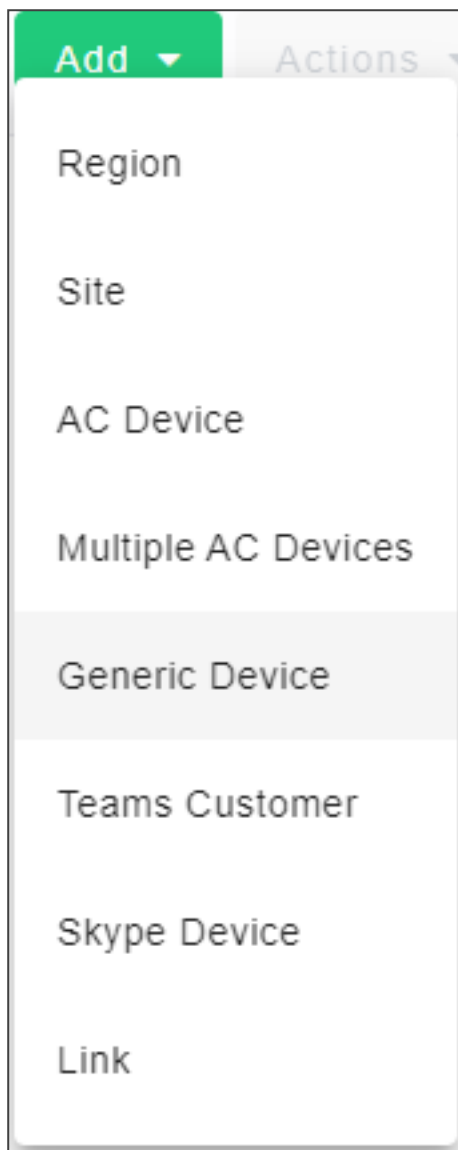
AudioCodes recommends that you consult with AudioCodes Customer Support or Professional Services about special configuration issues.

Adding a Generic Device Manually

Generic (non-AudioCodes) devices can manually be added to OVOC.

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

1. Access Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Network Topology page (**Network > Topology**).
3. Click **Add** and select **Generic Device**.



4. View the Generic Device Details screen.

GENERIC DEVICE DETAILS

Name*	IP
Tenant	Region*
miryam	miryam
Address	

CloseOK

5. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
6. Enter the device's IP address.
7. From the 'Tenant' drop-down, select the device's tenant.
8. From the 'Region' drop-down, select the device's region and then click **OK**; the device is added and displayed in 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. Microsoft 365 tenant must be configured to allow call records permissions (see *OVOC IOM* for more information). OVOC will receive call records notifications and accumulate statistics of the Teams tenant.

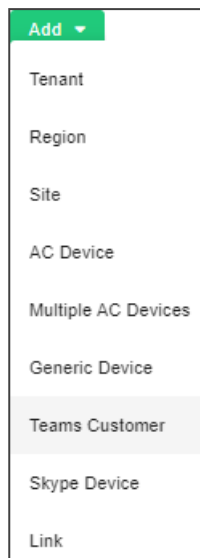


For the required prerequisites (certificates, public FQDN, IP address, etc.), see section 'Setting Up Microsoft Teams Subscriber Notifications Services Connection' in the *OVOC IOM*.

➤ To add a device:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).

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

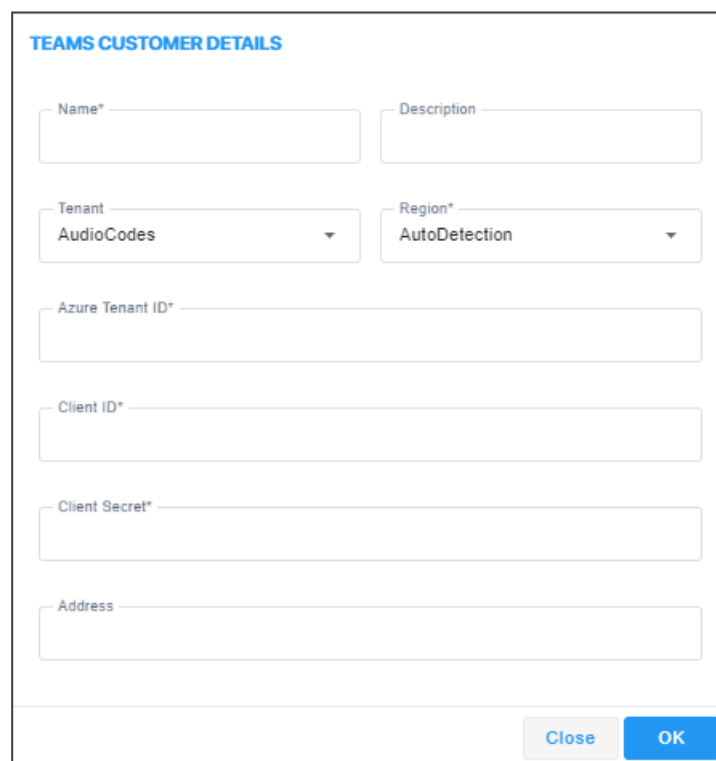


A dropdown menu with a green 'Add' button at the top. The menu lists the following options: Tenant, Region, Site, AC Device, Multiple AC Devices, Generic Device, Teams Customer (highlighted with a grey background), Skype Device, and Link.



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

4. View the Teams Customer Details screen.



The 'TEAMS CUSTOMER DETAILS' form contains the following fields:

- Name* (text input)
- Description (text input)
- Tenant (dropdown menu, currently showing 'AudioCodes')
- Region* (dropdown menu, currently showing 'AutoDetection')
- Azure Tenant ID* (text input)
- Client ID* (text input)
- Client Secret* (text input)
- Address (text input)

At the bottom right, there are two buttons: 'Close' and 'OK'.

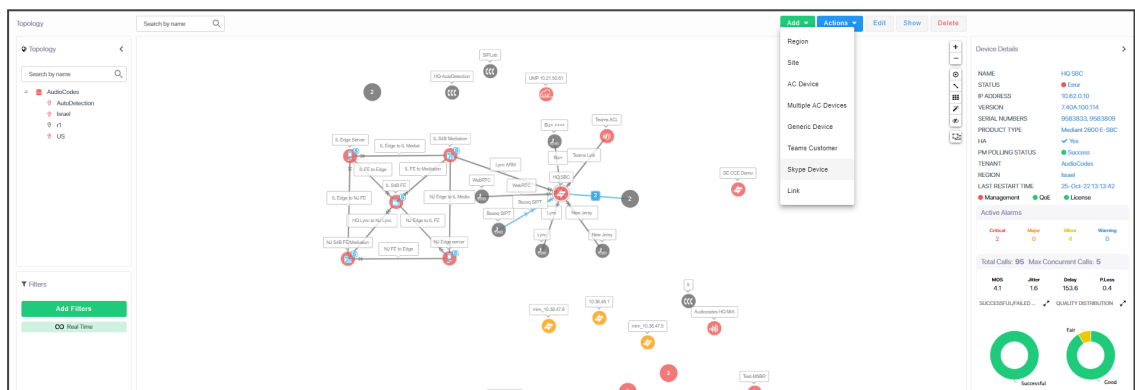
5. Define an intuitive name to facilitate operator-friendly management later. Don't use underscores.
6. Enter a Description to facilitate operator-friendly management later.
7. From the 'Tenant' drop-down, select the tenant with which to associate the device.
8. From the 'Region' drop-down, select a region you configured when [Adding a Region](#) on page 151.
9. 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.
10. Microsoft generates a Client ID for a specific application - 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'.
11. Microsoft generates a Client ID for a specific application - 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. OVOC will then be capable of accessing Office 365 / Microsoft 365 / Azure.
12. [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.
13. 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. 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 502.

➤ To add a Microsoft Skype for Business device:

1. Select Global or Tenant scope (see [here](#) for more information).
2. Open the Network Topology page (**Network > Topology**).
3. Click **Add** and select **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.

4. View the Skype Details screen.

SKYPE DETAILS

Name* FQDN*

Tenant AudioCodes Region* AutoDetection

Address

Device Type Skype Front End Server

SQL SERVER DB

IP Address*

SQL Mode SQL Port Port* 1433

Connection Mode SQL Server Authentication Domain

Username* Password*

Close OK

5. Define an intuitive name to facilitate operator-friendly management later. Don't use underscores.
6. From the 'Region' drop-down, select a region you configured when [Adding a Region](#) on page 151.
7. 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.
 - ◆ 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
8. In the 'FQDN' field, enter the device's Fully Qualified Domain Name.
9. 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 OVOC functions as the monitoring SQL database. After connecting, OVOC presents all Call Details from the Skype for Business network in the Calls List and Call Details pages. When functioning with Skype for Business pools, FE, Edge and Mediation servers cannot be defined in OVOC, so the entire Skype for Business network is presented in OVOC only as a single object, namely, the monitoring SQL database.
10. 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)
11. [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
12. In the 'User Name' field, enter the user of the SQL Server or Windows Server. Applies to the centralized Skype for Business database.
13. In the 'Password' field, enter the Password of the SQL Server or Windows Server. Applies to the centralized Skype for Business database.
14. In the 'Domain' field (relevant only when 'Connection Mode' is configured to **Windows Authentication**), enter the Windows Server user's domain.

15. From the 'SSL' drop-down, secure the connection between OVOC and the SQL server over SSL by selecting either:
 - **Trusted:** An SSL connection between OVOC server and the SQL server is opened, though it's not authenticated using a certificate.
 - **Using Certificate:** An SSL connection between OVOC and the SQL server is opened. 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 OVOC Software Manager](#) on page 114.

Default: **Disabled**. The SSL connection with the SQL server is by default non-secured.

16. [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.
17. 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 99.

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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Backup Manager page (**Network > Devices > Backup Manager**).

The screenshot shows the Backup Manager interface. On the left is a sidebar with a 'Topology' section containing a search bar and a list of nodes: 'AutoCoders', 'AutoDetection', 'Inet', 'H', and 'US'. Below this is a 'Filters' section with an 'Add Filters' button. The main area is divided into two panels. The left panel, titled 'Backup summary', contains a table with columns: 'DEVICE NAME', 'PRODUCT TYPE', 'NUMBER OF FILES', 'LAST SUCCESSFUL BACKUP TIME', 'LAST BACKUP TIME', 'LAST BACKUP STATUS', and 'TEN'. The right panel, titled 'Backup Files', contains a table with columns: 'BACKUP TYPE', 'UPLOAD TIME', 'FILE TYPE', 'FILE SIZE', and 'FILE NAME'. Both tables list various devices and their backup details.

3. View the following in the Backup Manager page:

- **Backup Summary** window: Displays all devices for whom files have been backed up on the OVOC server. Click a device to view those files under the **Backup Files** window to the right.
- **Backup Files** window: Displays backup files for each device that have been saved to the Backup Manager; ini and cli script files (MSBRs), zip file (Configuration Package) (SBCs / Gateways), zip file (VoiceAI Connect) and JSON file (Stack Manager).



- All SBCs / Gateways whose version is 7.4.200 and later are backed up with the zip file.
- The number of backup files stored includes old and new file types. For example, if a device operates with an ini file and already has three stored ini files when the maximum that can be stored is five, two more zip files are stored before deletion of old ini files begins (see also [Enabling Automatic Device Backup Periodically](#) on page 99).
- For upgraded devices which operate with the old file type, in the next backup round after the upgrade, a zip file is created (and the oldest backup is deleted if necessary) (see also [Enabling Automatic Device Backup Periodically](#) on page 99).

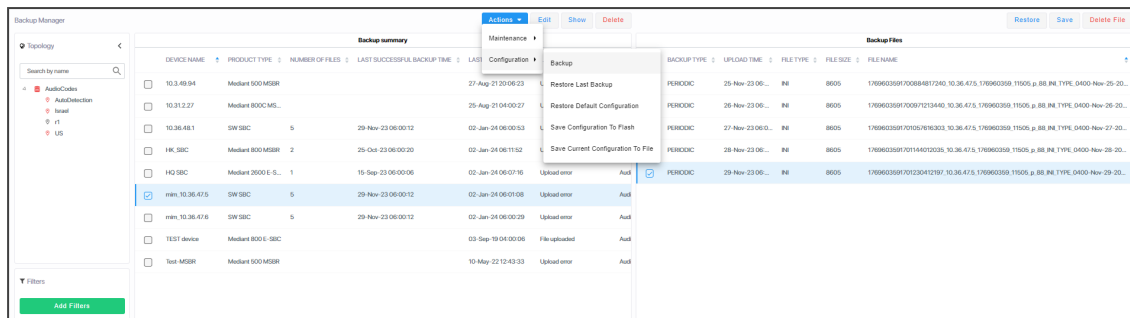
4. View under **Backup Summary** the following columns for each entry:

- Device Name and Product Type
 - Number of Files [the number of files backed up from the device to the OVOC]
 - Last Successful Backup Time
 - Last Backup Time
 - Last Backup Status
 - Tenant [the tenant under which the device is located]
 - Region [the region under which the device is located]
5. Optionally filter displayed files for more effective access to the specific files you need:
 - Click a column header; files are displayed accordingly.
 6. View under **Backup Files** the backed-up file names. They're in the following 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
 7. Use the following table as reference to the preceding example.

Table 4-1: Explanation of Backed Up File Name Format

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

8. 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.



9. From the **Actions** drop-down, select **Configuration** and then select the **Backup** option; you're prompted with a message 'Are you sure you want to upload configuration from this device?'
10. Click **OK**; the configuration is uploaded from the device to the OVOC server.



The backup action automatically stores .ini or .cli file according to device type. The action also automatically backs up SBCs / Gateways whose version is 7.4.200 and later, with a .zip (configuration package) file, and stores it.

11. Optionally, select **Restore Last Backup** or **Restore Default Configuration** from the **Actions > Configuration** drop-down.



- The restore procedure for devices whose version is 7.4.200 and later supports two file types: .zip and .ini / .cli (from previous versions).
- All newly added SBCs whose version is 7.4.200 and later are added with the .zip backup file.

12. Optionally, select **Save Current Configuration to File**; this action downloads to your pc the configuration file for:
 - **MSBR**; the ini file appears at the lowermost left corner of your pc screen; select **Keep** (for downloading the file to the device) or **Discard**.
 - **SBC**; the ini file appears at the lowermost left corner of your pc screen; select **Keep** (for downloading the file to the device) or **Discard**.

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?'
3. Click **Download**; the configuration is downloaded from the PC to the device.

Adding Links

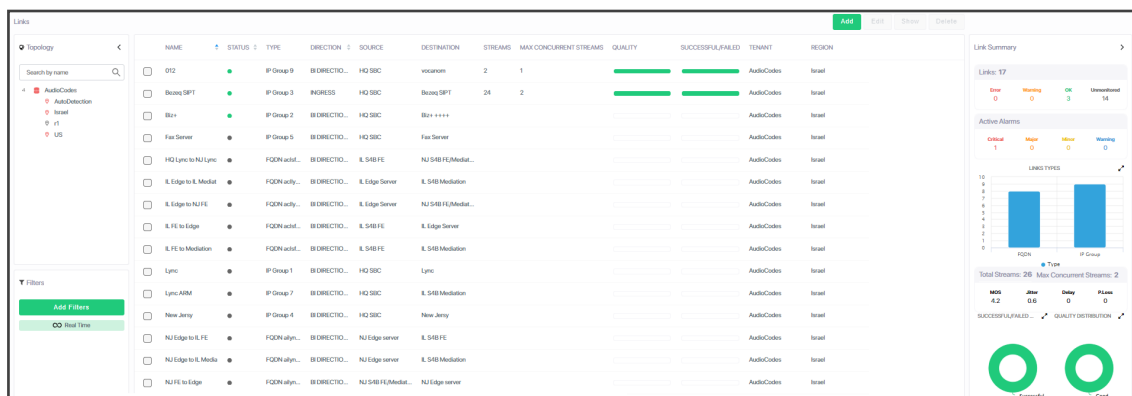
Links are logical VoIP communication paths between devices that measure and display key metrics on calls made on them. Links are defined according to IP Group (IP network entity such as a server, e.g., IP PBX, or a group of users, e.g., LAN IP phones, with which the E-SBC communicates), Trunk Group (logical 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 371.

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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. After configuring devices, open the Links page (**Network > Links**).



3. Click **Add**.

LINK DETAILS

Name*

Direction
BI DIRECTIONAL

Source Device*
HQ SBC

Destination Device*

Category Type*
Tenant

Category Value*

AD Group
Only for Monitor Links Operators

Close OK

4. Use the table as reference.

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 <i>from which</i> to link to the destination device. You can alternatively search for it.
Destination Device	From the drop-down list, select the destination device <i>to which</i> to link from the source device. You can alternatively search for it.
The link counts and computes statistics on all calls that originate in the source device, based on one of the following Category Types (selected from the 'Category Type' drop-down:	
Category Type	From the drop-down select one of the following Category Types. Based on your selection, the link will count and compute statistics on all calls originating in the source device.

Parameter	Description
	<div>LINK DETAILS<div><div>Name*</div><div>Direction</div><div>BI DIRECTIONAL</div></div><div><div>Source Device*</div><div>NJ SBC</div></div><div><div>Destination Device*</div></div><div><div>Category Type*</div><div>Tenant</div><div>Control IP</div><div>IP Group</div><div>Media IP</div><div>Media Realm</div><div>Phone Prefix</div></div></div>

Parameter	Description
	Tenant - Defines a Tenant. This parameter must be configured on the SBC as well . The value is obtained from the SIP message (header data) using Message Manipulation rules with the call variable Var.Call.Src Dst.TenantId. It can be included in the CDR by CDR customization using the SBC CDR Format table. The field is applicable only to SBC signaling ("CALL_CONNECT" and "CALL_END" CDR Report Types). The maximum number of characters for Syslog tabular alignment is 71.
	Control IP - Defines a valid IP address on which SIP control messages are originated.
	IP Group - Defines the source device IP-Group index (a list of options may be available).
	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).
	Phone Prefix - Defines the prefix text of a phone number or SIP URI string. See the Note following for more information.
	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.
	Trunk Group - Defines a Trunk Group, i.e., a logical group of physical trunks and channels each of which can include multiple trunks and ranges of channels. A Trunk Group needs to be configured and assigned with telephone numbers to enable and activate the channels of the device. After configuring a Trunk Group, you can use it 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

5. 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/>

6. Configure parameter 'AD Group'.



Only displayed when you select SBC as 'Source Device'. It isn't displayed if you select Lync device as 'Source Device'.

This parameter is only for Monitor Links Operators. It's used when OVOC authentication is LDAP or Azure single tenant authentication. The group must also be configured as a group in the LDAP/Azure server for the logged-in operator.

7. Click **Apply**; the link is added and displayed in 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. After configuring the region under which to locate the site, open the Sites page (**Network > Sites**).

NAME	STATUS	ENDPOINTS	QOS STATUS	CALLS	QUALITY	SUCCESSFUL/FAILED	MANAGEMENT STATUS	TENANT	REGION
<input type="checkbox"/> AutoDetection	●	0	●			●	●	AudioCodes	Israel
<input type="checkbox"/> AutoDetection	●	470	●			●	●	AudioCodes	AutoDetection
<input type="checkbox"/> CloudPSTN to AC Demo	●	0	●			●	●	AudioCodes	Israel
<input type="checkbox"/> course	●	0	●			●	●	AudioCodes	Israel
<input type="checkbox"/> HQ-AutoDetection	●	0	●			●	●	AudioCodes	AutoDetection
<input type="checkbox"/> OverP SIP	●	0	●			●	●	AudioCodes	Israel
<input type="checkbox"/> SIP-Lite	●	0	●			●	●	AudioCodes	Israel
<input type="checkbox"/> R	●	0	●			●	●	AudioCodes	r1

3. Click **Add**.

SITE DETAILS

Site Name* Description

Tenant Region*

Address

Subnet (CIDR Notation)

Close OK

4. From the 'Region' drop-down, select the region under which to locate the site.
5. Provide an intuitive name for the site to facilitate effective, intuitive management later.
6. Enter a description of the site to facilitate effective, intuitive management later.
7. 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.
8. [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.
9. Click **OK**; the site is added.

Managing Endpoints

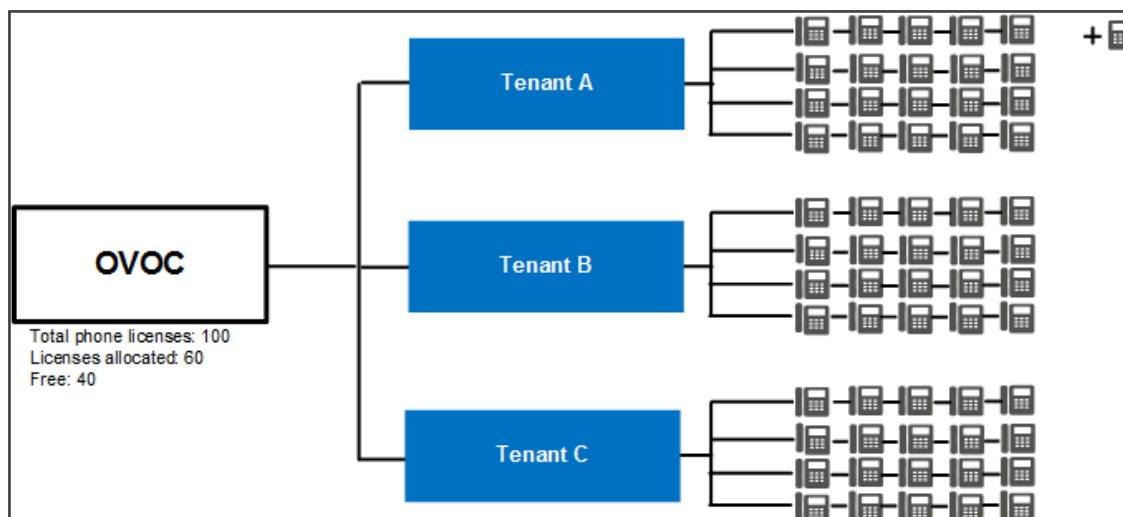
OVOC supports endpoints management through the directly accessible Device Manager application.

Dynamic Allocation of Endpoint Licenses

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. 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 4-19: 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
- 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
- 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

OVOC enables you to directly access AudioCodes' Device Manager management application with a single-sign on (SSO), to configure endpoints (phones and meeting room devices).

➤ **To access the Device Manager:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. From **Network > Endpoints**, select **Configurations**.



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

Monitoring Endpoints Status

OVOC enables you to monitor phones statuses.

➤ **To monitor phones statuses:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Endpoints page (**Network > Endpoints > Configurations**).



See the *Device Manager Administrator's Guide* 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 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

OVOC enables you to add an endpoints group. After adding a group, use Device Manager to add endpoints to that group and configure that endpoints group. OVOC allows viewing added groups; it doesn't allow *adding endpoints*. See the *Device Manager Administrator's Guide* 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Endpoint Groups page (**Network > Endpoints > Endpoint Groups**) and click the **Add** button.

3. 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.
4. [Applies only when operator authentication is by Azure AD / LDAP] When an operator logs in to OVOC, 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 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 46
 - [Configuring Operator Authentication Centrally using an LDAP Server](#) on page 41

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

5. In the Endpoint Groups page shown in the preceding figure, 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**. 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 252.
6. 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**; the Tenant Operator Details screen opens. See [Adding a 'Tenant' Operator](#) on page 65 .

7. From the 'Security Level' drop-down in the Tenant Operator Details screen, 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:

The screenshot shows the 'TENANT OPERATOR DETAILS' window with the 'Topology' tab selected. It features three tabs: 'Basic info', 'Advanced info', and 'Topology'. Below the tabs is a section for 'Assigned Tenants' with a dropdown arrow. At the bottom, there is a checkbox labeled 'Restrict Endpoints Actions Except For These Groups' which is currently unchecked.

8. 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.

This screenshot shows a detailed view of the configuration. The 'Assigned Tenants' section at the top shows 'x_tenant' and 'y_tenant' selected in a dropdown menu. Below this, the checkbox 'Restrict Endpoints Actions Except For These Groups' is checked. The 'Assigned Endpoints groups' section shows a list of groups: 'x_group' under 'Tenant: x_tenant' and 'y_group' under 'Tenant: y_tenant'. The 'y_group' entry is highlighted. An 'All' button is located at the bottom right of the groups list.

9. Click **OK**.

Assigned Tenants:

x_tenant x_ytenant

Restrict Endpoints Actions Except For These Groups ☒

Assigned Endpoints groups:

x_group y_group

No items found

Clear



- 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).

Assigned Tenants:

x_tenant x_ytenant

Restrict Endpoints Actions Except For These Groups ☐

10. 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.

OPERATOR NAME	OPERATOR TYPE	SECURITY LEVEL	STATUS	LAST SUCCESSFUL LOGIN	LAST FAILED LOGIN	OPERATOR DETAILS
mikiAdmin	System	Admin	NOT ACTIVE	29-Jul-19 17:08:04		OPERATOR NAME xy_operator
miki	System	Admin	NOT ACTIVE	18-Mar-20 09:23:30		OPERATOR TYPE Tenant
acldadmin	System	Admin	ACTIVE	24-Mar-20 16:49:37	22-Mar-20 18:09:04	TENANTS 2
xy_operator	Tenant	Admin	NOT ACTIVE			IS GROUP OPERATOR ✓
						GROUPS 2
						SECURITY LEVEL Admin
						VALID IPS TO LOGIN FROM None
						IS SUSPENDED ✗
						ACCOUNT INACTIVITY PERIOD 0
						SESSION TIMEOUT PERIOD 0
						SESSION LEASING PERIOD 0
						PASSWORD UPDATE MIN PERIOD 24
						PASSWORD VALIDITY MAX PERIOD 90
						PASSWORD WARNING MAX PERIOD 7
						CHANGE PASSWORD ON NEXT LOGIN ✗



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). 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

OVOC enables 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Topology Groups page (**Network > Groups**).

NAME	DESCRIPTION	TENANT	ATTACHED TOPOLOGY ENTITIES
group		AudioCodes	1
testDev		AudioCodes	1

3. Click **Add**.

GROUP DETAILS

Group Name* Description

Tenant* AudioCodes

Attachments

0 Devices, 0 Links, 0 Sites [View](#)

Close OK

4. 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.
5. Click the **View** link.

GROUP DETAILS

Group Name* Description

Tenant*
 AudioCodes

Attachments

0 Devices, 0 Links, 0 Sites
 [View](#)

Search by Name, IP or Serial Number

- ☐ AudioCodes
- ☐ AutoDetection
- ☐ Israel
 - ☐ devices
 - ☐ links
 - ☐ 012
 - ☐ Bezeq SIPT
 - ☐ Biz+
 - ☐ Fax Server
 - ☐ HQ Lync to NJ ...

6. Navigate to and select the entities to attach and click **OK**.
7. 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 252.

5 Managing SBC Licenses

OVOC enables network administrators to manage SBC calling capacity licenses, including management of features such as SBC sessions, SBC devices, SBC registrations, SBC transcoding and signaling sessions. Customers must sign the AudioCodes [EULA](#) when purchasing a license. Network administrators can implement different license modes.

■ Two Floating License modes:

- *Cloud License Manager 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 License](#) on page 202 for more information.
- OR-
- *Flex Pool License 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 [Flex Pool License](#) on page 209 for more information.



- A Flex Pool License cannot be applied at the same time as a Floating License.
- To use a Flex Pool License or a Floating License on the SBC, an OVOC Management License must first be installed (for SBC - OVOC communications).
- If you remove the Floating License, the SBC will not use the local Device License; a local Device License must be ordered *per device* for this.
- The Cloud License Manager (CLM) must be ready and declared on AudioCodes' side.
- **Benefits of pool-based licenses (Floating License | Flex Pool License | Fixed Pool License) are:**
 - ✓ Licenses can be implemented globally for an OVOC instance or can be adapted to different multi-tenancy architecture
 - ✓ When a single instance of OVOC is deployed for an ITSP, licenses can be allocated between multiple enterprise customers
 - ✓ When a single instance of OVOC is deployed in a large enterprise network, licenses can be allocated between sites
 - ✓ Licenses can be allocated between devices on the fly, without changing the devices' local license key
 - ✓ Licenses for devices can be added | removed according to site requirements without needing to contact AudioCodes
- **Benefits of Floating Pool License are:**
 - ✓ Dynamically exceed license capacity without service interruption
 - ✓ Globally configure license pool in OVOC for all devices in the pool
- **Benefits of a Flex Pool License are:**
 - ✓ All devices share the license pool capacity without need for individual device licenses.
 - ✓ Globally configure license pool in OVOC.
 - ✓ No need for external connection to AudioCodes License Manager.

■ **Fixed License Pool** (see [Fixed License Pool](#) on page 215)

- Recommended when multiple SBCs are deployed and *centrally managed*
- Allows a 'tenant' operator to update licenses from a central pool in a simple process



- A Fixed License Pool can be applied with a Floating License or a Flex Pool License.
- A Device License can only be added when you have a Fixed License Pool (a Floating License and a Flex Pool License overwrite the Device License).
- An SBC operates with one of the following: a Device License, Fixed License Pool, Flex Pool License or a Floating License.
- Local Device License sessions are added to a Fixed License Pool only when using an SBC with a Fixed License Pool.
- **Fixed Pool License benefits:**
 - ✓ All devices share the license pool capacity.
 - ✓ Each device receives a unique allocation unaffected by the other devices.

■ **Locally** by loading an ini file to the device using the Web interface, without requiring OVOC. See the device's *User Manual* for more information.

The table below shows supported license features.

Table 5-1: Supported License Features

License Feature	Description
SBC Signaling Sessions	The maximum number of concurrent SBC call sessions.
SBC Media Sessions	The maximum number of concurrent SBC call sessions.
SBC Registrations (also referred to as Far End Users)	The maximum number of SIP endpoints that can register with the SBC devices.
SBC Transcoding	The maximum number of SBC transcoding sessions.
Managed Devices	The maximum number of SBC devices that can be managed. For Flex License.
WebRTC	The maximum number of concurrent WebRTC sessions.
SIP Rec	The maximum number of concurrent SIP Rec streams.

Adding an SBC to the Floating License



Applies to both Floating License modes: Cloud License Manager mode *and* Flex Pool License mode.

Before adding an SBC to a Floating License, add an SBC to 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 163 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 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 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 > Administration > License > Floating License**).
2. From the 'Floating License' drop-down list, select **Enable**.

GENERAL	
Floating License	Enable
Connection with OVOC	Connected to OVOC
OVOC IP Address	172.17.140.203
OVOC Product Key	3F1927F8DF64

3. Reset the device with a burn-to-flash for your settings to take effect. After the device resets, it connects with OVOC and the following read-only fields display OVOC-related information:
 - 'Connection with OVOC': Displays the device's connectivity status with OVOC:
 - ◆ "Connected to OVOC": The device is connected to OVOC.
 - ◆ "Disconnected from OVOC" The device is temporarily disconnected from OVOC due to problems with the network (HTTPS TCP connection).
 - ◆ "Not Connected to OVOC": The device is not connected to OVOC.
 - 'OVOC IP Address': Displays the IP address of OVOC.

- 'OVOC Product Key': Displays the **Product Key of the OVOC tool that is providing the Floating License.**
4. From the 'Allocation Profile' drop-down list, select an SBC license Allocation Profile. The Allocation Profile determines the capacity of each SBC license type that you want allocated to your device by OVOC. You can choose from factory default profiles, which may suit your deployment requirements or you can configure your own customized profile. The optional factory default profiles include:
 - **SIP Trunking:** This profile is suited for SIP Trunking applications (i.e., where user registration is typically not required)
 - **Registered Users:** This profile is suited for applications where user registration is required.

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

Allocation Profile	Custom	
	Allocation	Limit
Far End Users	1600	
SBC Media Sessions	400	
SBC Signaling Sessions	400	
Transcoding Sessions	60	

Range: 0-400



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

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

- Open 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 OVOC). As reports are sent every 5 minutes, this may take up to 5 minutes to show.

Figure 5-1: Device Floating License Page – Newly Added SBC Appears in the List

NAME	PRODUCT TYPE	ADDRESS	HA	MANAGED	LAST REPORT TIME	FLOATING LICENSE S.	DEVICE STATUS	CONFIG STATUS	REPORT STATUS	REGION	TENANT
HQ SBC	MEDANT 2600 S SBC	10.62.0.10	✓	✓	13 Jun-18 11:20:00	■	■	■	■	US	A
NY SBC	MEDANT 1000 PRO	172.28.1.3	✗	✓	13 Jun-18 11:20:00	■	■	■	■	US	A

>> FLOATING LICENSE SUMMARY
 Device Floating Licenses Utilization 13%
 Total 10 Allocated 2 Free 8
 ADDRESS Cn-A.Com
 CUSTOMER STATUS Active
 LAST SUCCESSFUL USAGE 13 Jun-18 10:04:58
 REPORT TIME
 Current Usage Report Status
 LAST SENT Successful
 SUCCESSFUL/FAILED
 NUMBER OF FAILED 0

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

Table 5-2: Floating License Page Column Descriptions (applies to Cloud License Manager mode *and* Flex Pool mode 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 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).
Device Status	Grey	Unmanaged: Device is unmanaged by OVOC Unmonitored: Device is unmonitored by OVOC
	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

Column	Description	
		<p>as a result the device's CAC is reset to 0.</p> <p>Not Connected: Device is unable to establish a connection with the Floating License OVOC service (CAC 0)</p> <p>Temporarily Disconnected: Device is temporarily disconnected from the Floating License OVOC service due to problems with the HTTPS TCP connection.</p>
	Grey	<p>Unmanaged: The device is currently not managed by the OVOC Floating License service.</p> <p>Unmonitored: The device is currently unmonitored by OVOC Floating License service.</p> <p>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.</p>
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	<p>Not applicable: Indicates that the device was added to OVOC but is not yet managed.</p> <p>Unmonitored: Indicates that the device is currently unmonitored by OVOC.</p>
Report Status	Green	OK: Indicates that a report was successfully sent from the device to 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.

Column	Description	
	Red	<p>Failed: Indicates there's a problem with reports sent from the device to OVOC (missing / failed).</p> <p>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 OVOC and since then there has been a problem with reports from this device (missing / failed).</p> <p>Not Registered. Indicates that the device has not yet successfully registered to the OVOC Floating License service.</p>
	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 210 for more information.	
Region	Indicates the device's region.	
Tenant	Indicates the device's tenant.	

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

Performing Floating License Actions



Applies to both Floating License modes, i.e., to Cloud License Manager mode and to Flex Pool License mode, unless otherwise stated.

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

- Unmanage (see [here](#))
- Update (see [here](#))
- Reset (see [Reset](#) on the next page)
- Register (see [Register](#) on page 201) [only applies to Cloud License Manager 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 5-2: Device Floating License Page – Unmanage Action

MAINTENANCE ▶												
LICENSE ▶	UNMANAGE	DR...	HA	MANAGED	LAST REPORT TIME	FLOATIN...	DEVICE ST...	CONNECT...	CONFIG ...	REPORT S...	PRIORITY	
172.17.125.67	UPDATE	7.125...	✖	✓	06-Feb-20 16:00:00	■	■	27-Jan-20 1...	■	■	Normal	
172.17.118.235	UPDATE PRIORITY LEVEL	7.118...	✖	✓	06-Feb-20 15:30:00	■	■		■	■	Normal	
172.17.118.236	SW SBC	172.17.118...	✖	✓	23-Jan-20 16:30:00	■	■	31-Jan-20 1...	■	■	Normal	

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 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 5-3: Register

DEVICE FLOATING LICENSE

TOPOLOGY

Search by name

AudioCodes

BigBlueTenant

Devices_Agents

SRPaaS

SRPaaS-TEST-Tenant

OVIR

Singapore

Training

USA

Viva

Whisperer

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	MANAGED	LAST REPO...	FLOATING L...	DEVICE STAT...	CONNECTIO...	CONFIG STA...	REPORT STA...	PRIORITY	TENANT	REGION
HQ SBC	10.62.0.10	Mediant 2600 E-SBC	✓	✓	20-Dec-21 13...	●	●		●	●		AudioCodes	Israel
MyDevice	10.15.17.1	Mediant 800 E-SBC	✗	✓	17-Nov-21 14...	●	●		●	●		Training	MyRegion
MyDevice15	10.15.15.1	Mediant 1000 E-SBC	✗	✓	19-Sep-21 12...	●	●		●	●		Training	MyRegion
MyDevice16	10.15.16.1	Mediant 800 E-SBC	✗	✓		●	●		●	●		Training	MyRegion
NJ SBC	172.28.1.3	Mediant 1000 E-SBC	✗	✓	20-Dec-21 13...	●	●		●	●		USA	NewJersey

DEVICE FLOATING LICENSE DETAILS

FLOATING LICENSE MODE

Cloud Service

Device Info

LAST SUCCESSFUL USAGE REPORT TIME

19-Sep-21 12:30:00

	CURRENT	MAX CONFIGURED	MAX ACTUAL
Signaling Sessions	0	150	150
Media Sessions	0	150	150
Registrations	0	0	0
Transcoding Sessions	0	120	120

Configuring OVOC-Floating License Service Communications



Applies to both Floating License modes, i.e., to Cloud License Manager mode *and* to Flex Pool License mode, unless otherwise stated.

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**).

FLOATING LICENSE ADMINISTRATION LICENSE Configuration Tenants Allocations System Allocations Floating License SECURITY OVOC SERVER	GENERAL LICENSE CONFIGURATION Floating License OVOC Operator CLM_operator Submit	CLOUD LICENSE CONFIGURATION (DISABLED) Floating License Server Address s3luc2m1w7.enroute.ap-us-east-2.amazonaws.com Change Floating License Key*
	FLEX POOL CONFIGURATION Alarm Threshold Percentage 85 Submit	

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

Table 5-3: Floating License 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).

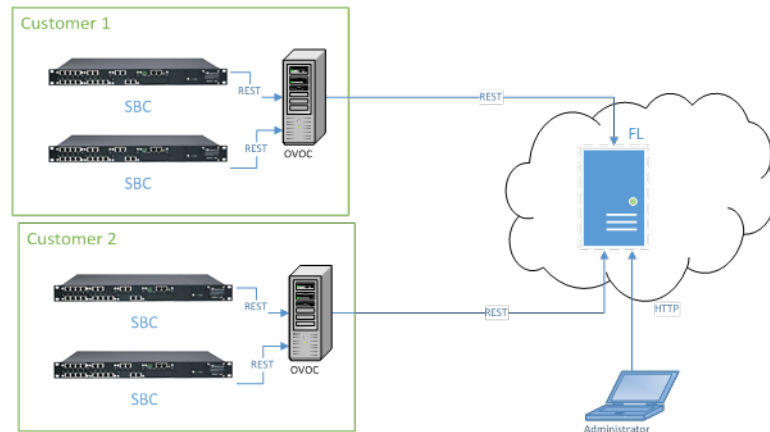


- The Cloud License Manager (CLM) must be ready and declared on AudioCodes' side.
- A Flex Pool License cannot be applied at the same time as a Floating License but you *can* apply a Fixed License Pool with a Floating License -OR- a Flex Pool License.
- A Device License can only be added when you have a Fixed License Pool (a Floating License and a Flex Pool License overwrite the Device License).
- An SBC operates with one of the following: a Device License, Fixed License Pool, Flex Pool License or a Floating License.
- Local Device License sessions are added to a Fixed License Pool only when using an SBC with a Fixed License Pool.
- If you remove a Floating License, the SBC will not use the local Device License; a local Device License must be ordered *per device* for this.
- To use a Flex Pool License or a Floating License on the SBC, an OVOC Management License must first be installed (for SBC - OVOC communications).

Cloud License

A Cloud License can be configured on AudioCodes SBCs and OVOC. The Cloud License replaced the legacy method of using the OVOC Advanced Monitoring package. A Cloud License 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 5-4: Cloud License



A Cloud License functions as follows:

- SBCs report their usage statistics at short intervals (typically every 5 minutes) to OVOC.
- 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 a Cloud License 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.
- See the *SBC User's Manual* if WebRTC or SIPREC has a non-zero value and you want to enable a Floating License on the SBC; the behavior differs to the behavior with the other licenses. WebRTC and SIPREC capabilities are not seamless applications compared to SBC Sessions and Registrations (for example). See [here](#) for links to the *SBC User's Manuals* (scroll down to 'Related Documentation').

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 a Cloud License

Configuring a Cloud License should only be done 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**.

3. Open the Floating License page (**System > Administration > License > 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 5-5: Product Key

GENERAL	
Machine ID:	8F203C19C4C
Product Key:	73BD884379F
Status:	Enable
Reason:	
Expiration Date:	01-01-2027
Expiration Days Left:	1977

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

DEVICE FLOATING LICENSE

TOPLOGY

Search by name

AutoCodes

BiFuYaTenant

Devices_Agents

IPFIND

IPFIND-TEST-Tenant

OVH

Singapore

t1

Training

USA

NAME

172.17.118.54-13066...

HQ SBC

15.82.0.10

MyDevice

MyDevice15

NJ SBC

IP ADDRESS / FQDN

abc544

10.15.15.1

172.28.1.3

PRODUCT TYPE

Mediant 500L MSBR

Mediant 2000 E-SBC

Mediant 800 E-SBC

Mediant 1000 E-SBC

Mediant 1000 E-SBC

HA

✓

✓

✓

✓

✓

MANAGED

✓

✓

✓

✓

✓

LAST REPORT TIME

26-Jul-22 14:50:00

09-May-22 20:00:00

18-May-22 19:30:00

02-May-22 08:00:00

FLOATING LICENSE STATUS

DEVICE STATUS

CONNECTION LOST

25-May-22 14:41:49

05-Aug-22 15:26:00

CONFIG STATUS

REPORT STATUS

PRIORITY

TENANT

AutoCodes

AutoCodes

Training

Training

USA

FLOATING LICENSE MODE

Cloud Service

Floating License Info

Device Info

LAST SUCCESSFUL USAGE REPORT TIME

26-Jul-22 14:50:00

Current

Max Configured

Max Actual

Signaling Sessions

0

600

600

Media Sessions

0

600

600

Registrations

6

100

100

Transcoding Sessions

0

150

150

- Make sure in the page that the OVOC successfully registered with the Floating License. Make sure that 'Customer Status' in the device's Floating License Details under the **Device Info** tab, displays **Active**.

Figure 5-6: Customer Status

HOSTNAME	clm.ac.com
CUSTOMER STATUS	✓ Active
LAST SUCCESSFUL USAGE REPORT TIME	
STATUS	Enable
SBC SESSIONS	0
SBC REGISTRATIONS	0
SBC TRANSCODING	0
SBC SIGNALING	0
Current Usage Report Status	
LAST SENT REPORT STATUS	Never Reported
NUMBER OF FAILED	0



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

Viewing Floating License Summaries

The OVOC's Device Floating License page (**Network > Devices > Floating License**) 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 the next page)
- Device Info pane (see [Viewing Device Info](#) on page 208)

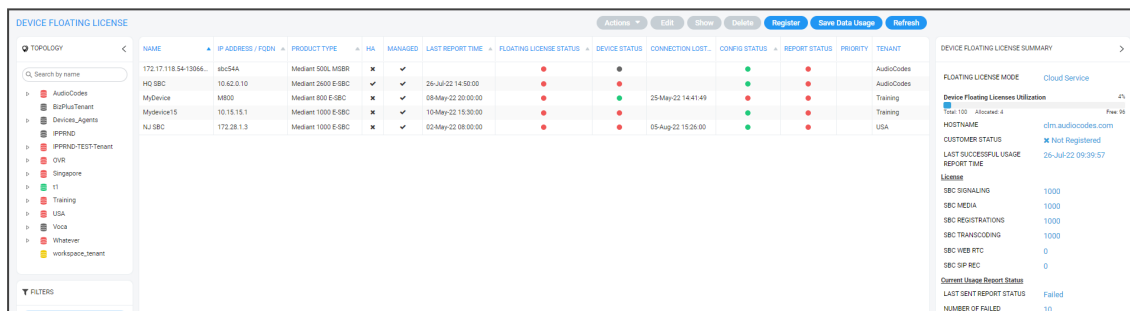
Device Floating License Utilization

The 'Device Floating License Utilization' pane is only displayed when no device is selected in the Device Floating License page (**Network > Devices > Floating License**).

➤ To view the pane if a device is selected:

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

Figure 5-7: Device Floating License Summary



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

Table 5-4: Device Floating License Utilization

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.

License Utilization	Description
	<p>Unknown - Status is undetermined by the OVOC</p> <p>Not Registered - OVOC has not registered successfully to the Floating License Cloud mode service</p>
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 Media, SBC Registrations, SBC Transcoding, SBC WEB RTC, SBC SIP REC.
Last Sent Report Status	Indicates whether the last attempt to send a usage report to the Floating License Cloud service was successful.
Number of Failed	Indicates the number of failed attempts to send usage reports to the Floating License Cloud service

Viewing Floating License Info

The OVOC's Device Floating License page (**Network > Devices > Floating License**) displays the 'Floating License Info' pane only when a device is selected in the page.

➤ To view the pane:

1. Select an entry in the page.

Figure 5-8: Device Floating License - Floating License Info

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	MANAGED	LAST REPORT TIME	FLOATING LICENSE STATUS	DEVICE STATUS	CONNECTION LOST	CONFIG STATUS	REPORT STATUS	PRIORITY	TENANT
HQ SBC	172.17.118.54-13066	Mediant 500L MSBR	✗	✓	26-Jul-22 14:50:00	●	●		●	●		AudioCodes
MyDevice	10.62.0.10	Mediant 2000 E-SBC	✗	✓	09-May-22 20:00:00	●	●	25-May-22 14:41:49	●	●		Training
MyDevice15	10.15.15.1	Mediant 1000 E-SBC	✗	✓	10-May-22 15:30:00	●	●		●	●		Training
NJ SBC	172.28.1.3	Mediant 1000 E-SBC	✗	✓	02-May-22 08:00:00	●	●	05-Aug-22 15:28:00	●	●		USA

LAST SUCCESSFUL USAGE REPORT TIME			
	Current	Max Configured	Max Actual
Signaling Sessions	0	600	600
Media Sessions	0	600	600
Registrations	6	100	100
Transcoding Sessions	0	180	180

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

Table 5-5: Device Floating License - Floating License Info

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

Session Capacity	Description
Configuration	device.
Maximum Actual	Indicates the maximum physical session capacity of the SBC device.

Viewing Device Info

The OVOC's Device Floating License page (**Network > Devices > Floating License**) displays the 'Floating License Info' pane only when a device is selected in the page.

➤ To view the pane:

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

Figure 5-9: Device Floating License Details - Device Info

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	MANAGED	LAST REPORT TIME	FLOATING LICENSE STATUS	DEVICE STATUS	CONNECTION LOST	CONFIG STATUS	REPORT STATUS	PRIORITY	TENANT
H3 SBC	10.62.0.10	Mediant 2600 E-SBC	✗	✓	26-Jul-22 14:50:00	●	●	●	●	●	●	AudioCodes
MyDevice	10.15.15.1	Mediant 800 E-SBC	✗	✓	08-May-22 20:00:00	●	●	●	●	●	●	Training
MyDevice15	10.15.15.1	Mediant 1000 E-SBC	✗	✓	10-May-22 19:30:00	●	●	●	●	●	●	Training
NJ SBC	172.28.1.3	Mediant 1000 E-SBC	✗	✓	02-May-22 08:00:00	●	●	●	●	●	●	USA

DEVICE FLOATING LICENSE DETAILS

FLOATING LICENSE MODE: Cloud Service

Floating License Info | **Device Info**

NAME: H3 SBC

STATUS: ● Error

IP ADDRESS: 10.62.0.10

VERSION: 7.40A.100.114

PRODUCT TYPE: Mediant 2600 E-SBC

HA: ✓ Yes

MANAGED: ✓ Yes

FLOATING LICENSE STATUS: ● Error

DEVICE STATUS: ● Temporary Disconnect...

CONFIG STATUS: ● Successful

REPORT STATUS: ● Failed

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

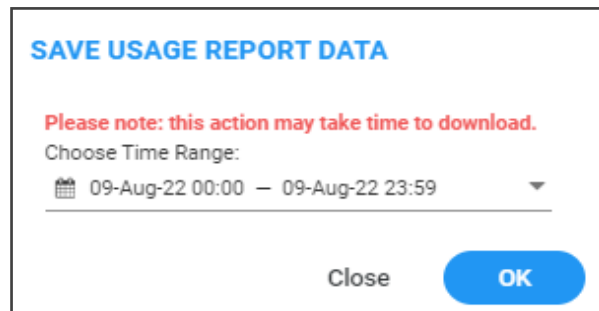
This feature allows customers to save reports to CSV file. Each report includes the currently configured license session values and the device's HA state.



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 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**.



SAVE USAGE REPORT DATA

Please note: this action may take time to download.

Choose Time Range:

09-Aug-22 00:00 — 09-Aug-22 23:59

Close OK

2. Define the period on which to produce the usage report data and then click **OK**.

Flex Pool License

After adding an SBC to the Floating License as shown in [Adding an SBC to the Floating License](#) on page 195 and configuring OVOC-Floating License service communications as shown in [Configuring OVOC-Floating License Service Communications](#) on page 201, Flex Pool License mode can be configured on SBCs and the OVOC. Flex Pool 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. Flex Pool License mode is supported from SBC version 7.2.256.300 or later.



Flex Pool is a system-level feature; it's not applicable per tenant.

Flex Pool License mode is different to Cloud License Manager 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 Flex Pool License mode.

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

Configuring an Alarm Threshold Percentage for Flex Pool Mode

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

➤ To configure an alarm threshold percentage for Flex Pool mode:

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

Figure 5-10: Flex Pool Configuration



FLEX POOL CONFIGURATION

Alarm Threshold Percentage

85

Submit

- 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

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:

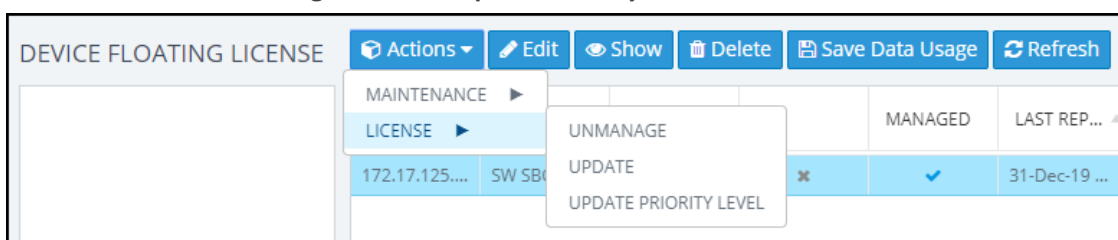
- Open the Device Floating License page (**Network > Devices > Floating License**).

Figure 5-11: Device Floating License

NAME	PRODUCT	IP ADDRESS	HA	MANAGED	LAST REP.	FLOATING	DEVICE ST.	CONNECT	CONFIG S.	REPORT S.	PRIORITY	REGION	TENANT
172.17.125...	SW SBC	172.17.125...	x	✓	31-Dec-19...	■	■	■	■	■	Normal	floating_lic...	floating_lic...

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

Figure 5-12: Update Priority Level



- 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 5-13: Device Floating License Page

DEVICE FLOATING LICENSE

Actions

Edit

Show

Delete

Save Data Usage

Refresh

TOPOLOGY

Search by name

floating_license

NAME	PRODUC...	IP ADDR...	HA	MANAGED	LAST REP...	FLOATIN...	DEVICE ST...	CONNECT...	CONFIG ...	REPORT S...	PRIORITY	REGION	TENANT
172.17.125...	SW SBC	172.17.125...	X	X	11-Feb-20...						Normal	floating_ic...	floating_lic...
172.17.118...	SW SBC	172.17.118...	X	X	29-Jan-20 1...						Normal	floating_ic...	floating_lic...
172.17.118...	SW SBC	172.17.118...	X	X	29-Jan-20 1...						Normal	floating_ic...	floating_lic...

Flex Pool Status: OK

FLOATING LICENSE SUMMARY

FLOATING LICENSE MODEFlex Pool

Device Floating Licenses Utilization2%

Total: 1000Allowed: 2Free: 998

Flex Pool Status Summary

	STATUS	USAGE	LICENSE
Signaling Sessions	OK	0	1000
Media Sessions	OK	0	1000
Registrations	OK	0	1000
Transcoding Sessions	OK	0	1000

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:

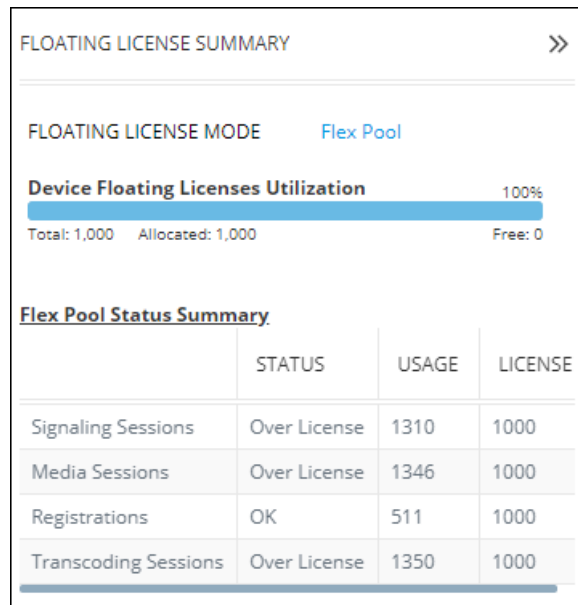
- **OK** [The statuses of all features in the **FlexPool Status Summary** table are 'OK']
- **Warning** [The status of at least one feature in the **FlexPool Status Summary** table is 'Warning' and the status of none is 'Over License']

- **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 5-14: 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 210.



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

Figure 5-15: FlexPool Mode Status

FLOATING LICENSE			
Cloud Mode Status:	Enable		
SBC Sessions:	0	SBC Transcoding:	0
SBC Registrations:	0	SBC Signaling:	0
Flex Pool Mode Status:	Disable		
SBC Sessions:	0	SBC Transcoding:	0
SBC Registrations:	0	SBC Signaling:	0
SBC Devices:	0	SBC Shutdown on Failure(days):	0

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.

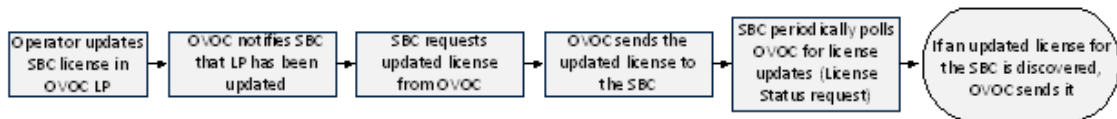
Fixed License Pool

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 134 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 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**).

FIXED LICENSE POOL

Actions

Edit

Show

Delete

Save

Refresh

Q TOPOLOGY

Q Search by name

102_102_115

default

miryam

New

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	MANAGED	LP STATUS	LAST REQUEST TIME	TENANT	REGION
10.21.50.70-1047004831	10.21.50.70	UNKNOWN	x	x	●		New	AutoDetection
10.3.181.70-10177698	10.3.181.70	Mediant 500L MSBR	x	x	●		New	AutoDetection
10.3.181.92	10.3.181.92	SW SBC	x	x	●		miryam	miryam
10.3.59.153-10407293	10.3.59.153	UNKNOWN	x	x	●		New	AutoDetection
169.254.0.2-1043508897	10.3.181.55	SW SBC	x	x	●		default	AutoDetection
172.17.141.97-9229094	172.17.141.97	UNKNOWN	x	x	●		New	AutoDetection
msbr247.0A-EMS.LOCAL	msbr247.0A-EMS.LO...	Mediant 500L MSBR	x	x	●		miryam	miryam

DEVICE LICENSE POOL DETAILS

License Summary

License Info

Device Info









Summary Of Tenant: default



Managed Devices

Total: 0

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

Table 5-6: LP Status

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

Icon	Description
	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 from the Fixed License Pool.



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. Open the Fixed License Pool page (**Network > Devices > Fixed License Pool**) and select the device to which to apply a license.

FIXED LICENSE POOL									
NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	MANAGED	LP STATUS	LAST REQ	MAINTENANCE	REGION	DEVICE LICENSE POOL DETAILS
10.21.50.70-1247004831	10.21.50.70	UNKNOWN	x	x	o			AutoDetection	
10.3.181.70-13177698	10.3.181.70	Mediant 500L MSBR	x	x	o			AutoDetection	
10.3.181.92	10.3.181.92	SW SBC	x	x	o			miryam	
10.3.59.153-13407293	10.3.59.153	UNKNOWN	x	x	o			New	
169.254.0.2-1043508897	10.3.181.55	SW SBC	x	x	o			default	
172.17.141.97-9225094	172.17.141.97	UNKNOWN	x	x	o			AutoDetection	
msb247-DA-EMS LOCAL	msb247-DA-EMS LO...	Mediant 500L MSBR	x	x	o			miryam	

2. Click the **Actions** button and select **License > Edit**.

LICENSE POOL DETAILS

☒ Enable License Pool

SBC

☒ SBC Sessions
0

☒ SBC Registrations
0

☒ SBC Transcoding
0

☒ SBC Signaling
0

3. Select the **Enable License Pool** option; select and configure other features.

4. Click **OK**.

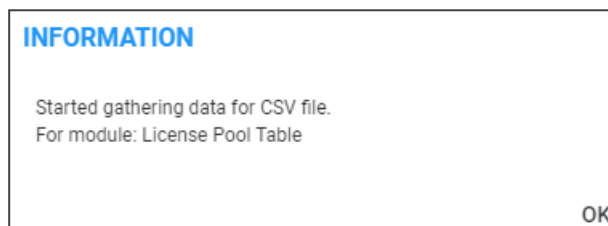
Saving Fixed License Pool Data to CSV File

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.

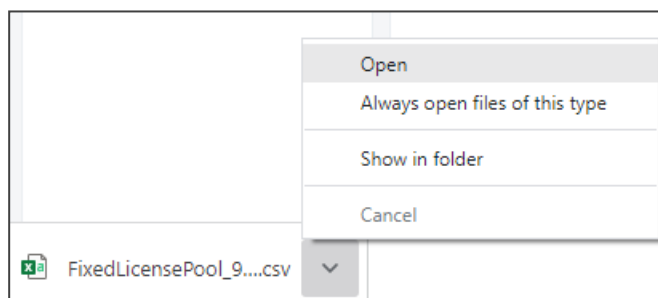
➤ To export Fixed License Pool data to a CSV file:

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

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



3. Click **OK**; locate the icon of the saved CSV file 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

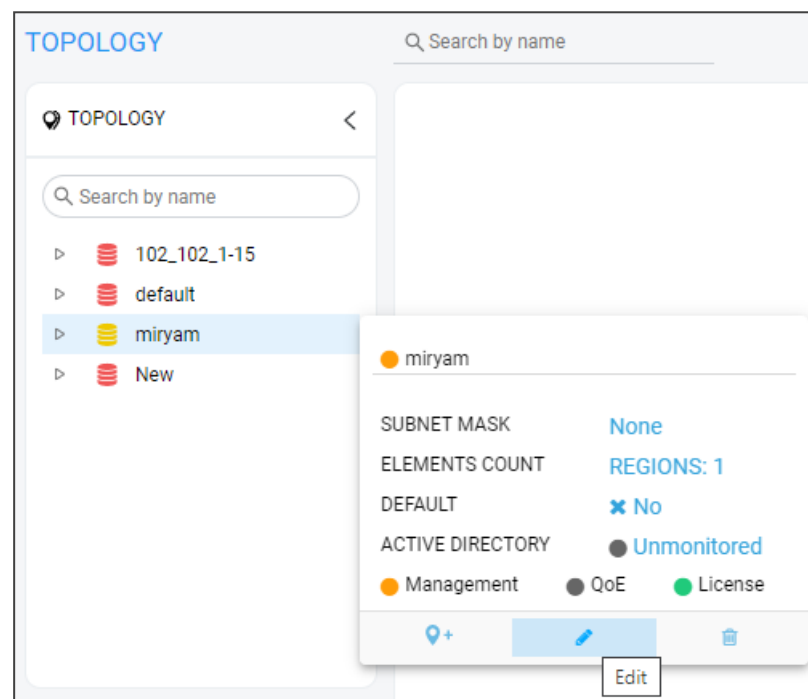
Before Performing 'Manage Device' / 'Update Device'

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

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

TENANT	SBC MANAGE.	SBC SESSIONS	SBC REGISTRA.	SBC TRANSCOD.	SBC SIGNALING	CB USERS	CB PER USERS	CB ANALOG D.	CB VOICEMAIL	QOE DEVICES	QOE ENERPONL.	QOE SESSIONS	QOE USERS	REPORTS	MANAGED ENDP.
AutoCodes	10	20	100	200	200	0	0	0	0	50	1,000	2,000	2,008	15	1,400
OVR	0	0	0	0	0	0	0	0	0	0	0	500	0	10	950
Singapore	0	0	0	0	0	0	0	0	0	10	0	50	0	10	100
Voca	0	0	0	0	0	0	0	0	0	0	0	0	0	10	173
USA	0	0	0	0	0	0	0	0	0	10	50	100	100	10	150
Devices/Agents	0	0	0	0	0	0	0	0	0	0	0	0	0	10	150
IPSPND-TEST-Tenant	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50
BiUPiaTenant	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Whatever	55	55	55	55	55	0	0	0	0	25	970	0	0	0	0
IPSPND	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Training	4	4	4	4	4	0	0	0	0	4	20	20	20	5	0
workspace_tenant	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2. 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 and click .



3. Click the edit option.

TENANT DETAILS

General	SNMP	HTTP	Operators	License
Tenant Name miryam	Description			
Is Default	HTTP Operator (License Pool)			
Users URI Regexp *	Azure Tenant ID			
Subnet (CIDR Notation)				
Tenant Logo None				
Masked Digits Number 4				

4. Make Sure 'HTTP Operator (License Pool)' is valid.
5. Make sure the device is connected to the OVOC (**Network > Devices > Manage** > select the device > **Show**).

Figure 5-16: Make Sure the Device is Connected to the OVOC

DEVICE INFORMATION

172.17.133.102-232... NAME	AutoDetection REGION	OK STATUS	UNLOCKED ADMIN STATE	No SAVE NEEDED?
172.17.133.102 ADDRESS	7.20A.156.009 FIRMWARE	SW SBC TYPE	232685563 S/N	No RESET NEEDED?

Management: OK

- Clear**
DEVICE ALARMS STATUS
- Unlocked**
ADMINISTRATION STATUS
- Connected**
CONNECTION STATUS

Voice Quality: Unmonitored

- Unmonitored**
CONTROL STATUS
- Unmonitored**
MEDIA STATUS
- Not Defined**
CONNECTION STATUS

License: OK

- License in Use**
MANAGEMENT STATUS
- Not Requested**
VOICE QUALITY STATUS
- OK**
LICENSE POOL STATUS

License Pool Alarms

Devices can issue the following License Pool alarms:

- acLicensePoolInfraAlarm
- acLicensePoolApplicationAlarm
- acLicensePoolOverAllocationAlarm
- acLicenseKeyHitlessUpgradeAlarm

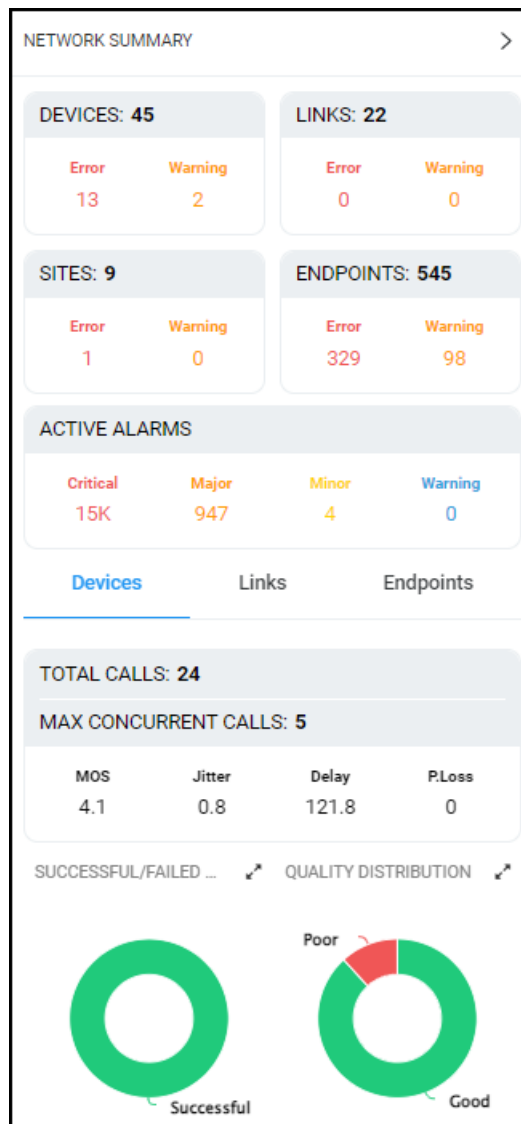
For more information about alarms related to the License Pool, see the *OVOC Alarms Guide*.

6 Assessing Network Health

OVOC enables you to determine the health of your IP telephony network. 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.



■ 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

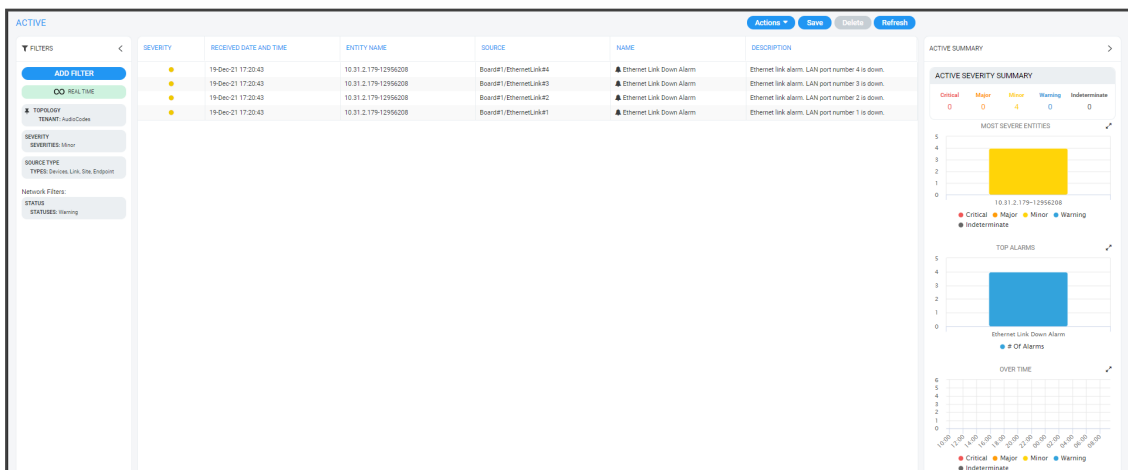
Figure 6-1: Example: Two Devices Whose Status is 'Warning'



■ The Active Alarms pane displays:

- The total number of Critical, Major, Minor and Warning active alarms (color-coded) currently active in the network.
- Click any severity level's total to display only alarms of that severity level in the Alarms page. Example: Under **Minor** in the Active Alarms pane above, click 4:

Figure 6-2: Alarms Filtered by 'Minor' Severity Level



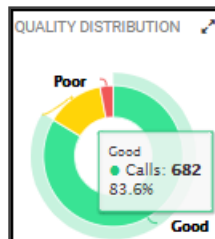
Select an alarm in the page to view detailed information about it in the Active Details pane then displayed on the right side of the page.

■ 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

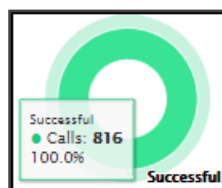
- Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of streams over links in the network whose quality was measured to be good, fair or poor respectively. For example:



- 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

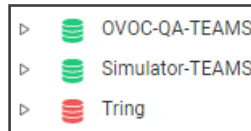
- Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over endpoints in the network whose quality was measured to be good, fair or poor respectively.

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:



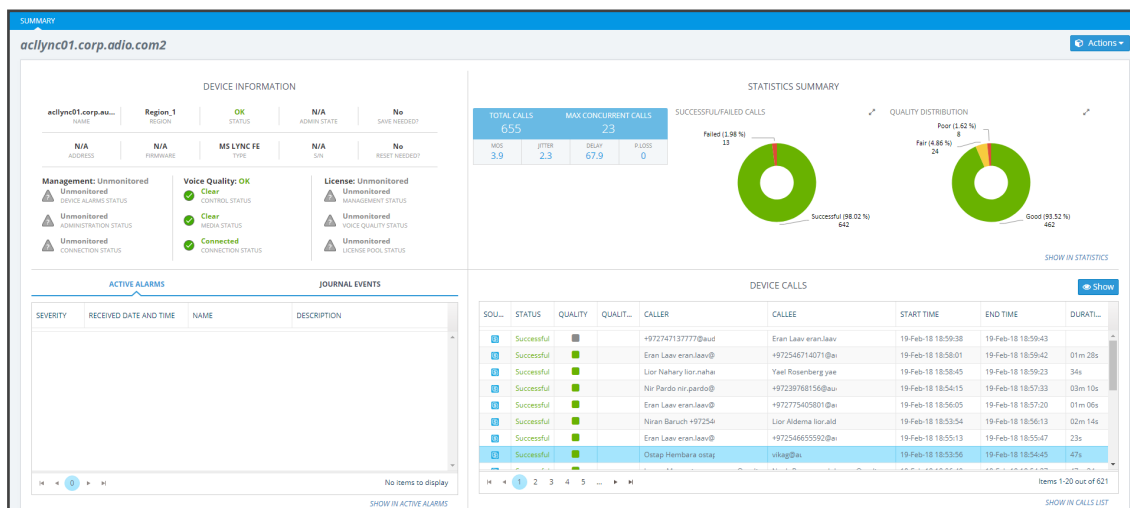
A red-coded tenant icon indicates that there is an alarm in the tenant, or that an OVOC threshold for voice quality has been exceeded in the tenant. This is the first-level navigation level.

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 6-3: Dynamic Tab for Quick Future Access to Device Information



Use the following table as reference to the page section 'Device Information' shown in the preceding figure.

Table 6-1: Device Information

Info About	Status Type	Description	Values
Management	Device Alarm Status	Indicates the severity status of the device's alarm, reported by the device; usually this is the maximum severity of the device's active alarm.	<ul style="list-style-type: none"> ■ Critical ■ Major ■ Minor ■ Warning ■ Indeterminate ■ Clear
	Administration Status	Indicates the status of the device's administration	<ul style="list-style-type: none"> ■ Locked ■ Unlocked
	Connection Status	Indicates the status of the device's SNMP connectivity	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Unmonitored ■ Clear ■ Major ■ Critical
	Connection Status	Indicates the status of the QoE connection	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Unmanaged ■ If License Pool is configured (same status as the status in the Fixed License Pool table)

Info About	Status Type	Description	Values
			<ul style="list-style-type: none">■ 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 371. 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 300 and specifically [Statistics Summary](#) on page 305. 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 254 and [Viewing Journal Alarms to Determine Operator Responsibility](#) on page 264. The page section 'Active Alarms | Journal Events' mirrors the Active Alarms page and the Journal Alarms page.

Filtering to Access Specific Information

Filter OVOC pages to quickly access specific information. Filters let you exclude unwanted information so that only the 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.

The screenshot shows the OVOC 'Calls List' page. On the left, there is a 'Filters' sidebar with an 'Add Filters' button and a 'Time Range' filter set from '26-Dec-23 17:53' to '27-Dec-23 17:53'. The main table displays call records with columns: SOU., STA., QUALITY, MEDIA TYPE, CALLER, CALLEE, CORRELATION ID, START TIME, END TIME, DURA., CALL T., DEVICE, LINK, and TERMINATION REAS.. The table contains five rows of call data.

SOU.	STA.	QUALITY	MEDIA TYPE	CALLER	CALLEE	CORRELATION ID	START TIME	END TIME	DURA.	CALL T.	DEVICE	LINK	TERMINATION REAS..
0547751968@10.9.9.5				0547751968@10.9.9.5	0547751968@10.9.9.5		27-Dec-23 17:...	27-Dec-23 17:40:15	02m 22s	SBC	HQ SBC	Beacon SPT	Normal Call Clear
0546262785@hunk.ipc...				0546262785@hunk.ipc...	0546262785@hunk.ipc...		27-Dec-23 17:...	27-Dec-23 17:17:31	12m 15s	SBC	HQ SBC		Normal Call Clear
0547751968@hunk.ipc...				0547751968@hunk.ipc...	0547751968@hunk.ipc...		27-Dec-23 17:...	27-Dec-23 17:17:15	02m 17s	SBC	HQ SBC		Normal Call Clear
052560483@hunk.ipc...				052560483@hunk.ipc...	052560483@hunk.ipc...		27-Dec-23 17:...	27-Dec-23 17:15:22		SBC	HQ SBC		Normal Call Clear
0547751968@10.9.9.5				0547751968@10.9.9.5	0547751968@10.9.9.5		27-Dec-23 17:...	27-Dec-23 17:10:37	33s	SBC	HQ SBC	Beacon SPT	Normal Call Clear

- **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'

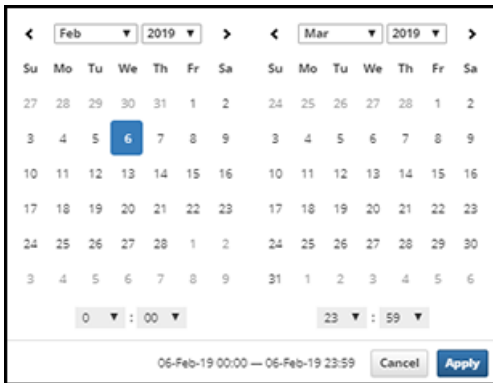
You can filter the Network Topology page and other pages by 'Time Range'. The 'Time Range' filter allows you to display *time range specific* information on the page.

Figure 6-4: Time Range Filter

Use the following table as reference.

Table 6-2: Time Range Filter

Filter Feature	Description
Pin all selected	Select this option (default) to 'preserve' the filter; the filter will remain displayed <i>in every page</i> whose tab you click. If you clear the option, the filter will only apply <i>locally</i> - to the page in which you apply the filter. The feature facilitates troubleshooting.
Back to real time	The link is enabled when you select a filter. Clicking the link removes the filter; the OVOC returns to real time.
Last 3 6 12 24 hours	Select one of these 'quick' filters in order to present only network data collected over the last 3 6 12 24 hours, to the exclusion of all other times.

Filter Feature	Description
Custom	<p>You can customize dates and times by which to filter. Select Custom and then click the drop-down field below it.</p>  <p>In the calendar on the left, select from when to filter: Choose a month and a day and optionally enter a time – the hour and the minutes past the hour. In the calendar on the right, select until when to filter: Choose a month and day and optionally enter the time – the hour and the minutes past the hour. Click Apply.</p>
Apply	<p>Click to implement the filter. To remove the filter if necessary, click the Back to real time link – see above.</p>



- 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.

Clock Filters

You can filter hours and minutes for specific days.

➤ **To filter hours and minutes:**

1. In the Calendar click a specific day.

TIME RANGE

Unsaved

☒ Pin all selected

[Back to real time](#)

Last 3 hours

Last 6 hours

Last 12 hours

Last 24 hoursCustom24-Jul-23 00:00 – 24-Jul-23 23:59

<<<>>>

JUL 2023

SMTWTFSS

JUL

1

23

24

25

26

27

28

29

30

31

start

00:00

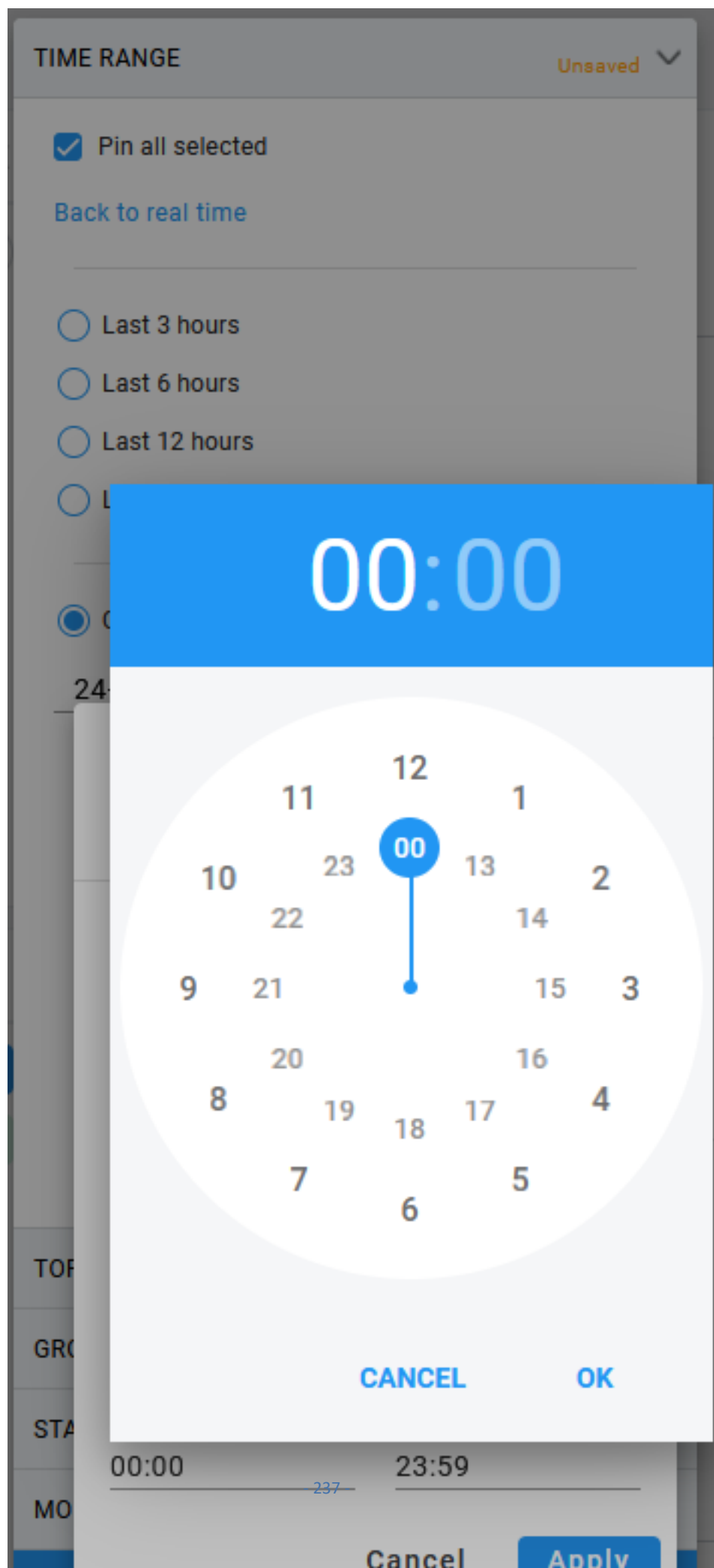
end

23:59

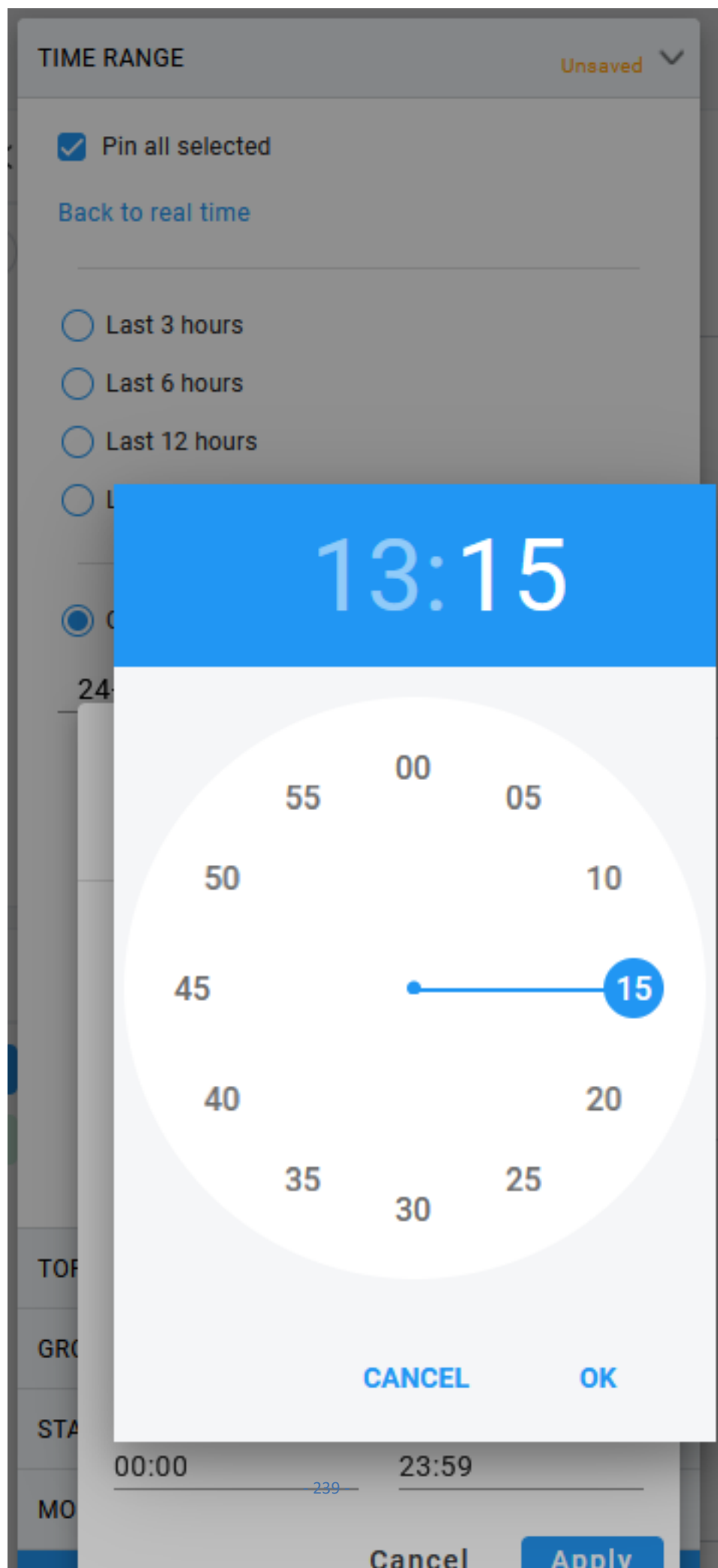
Cancel

Apply

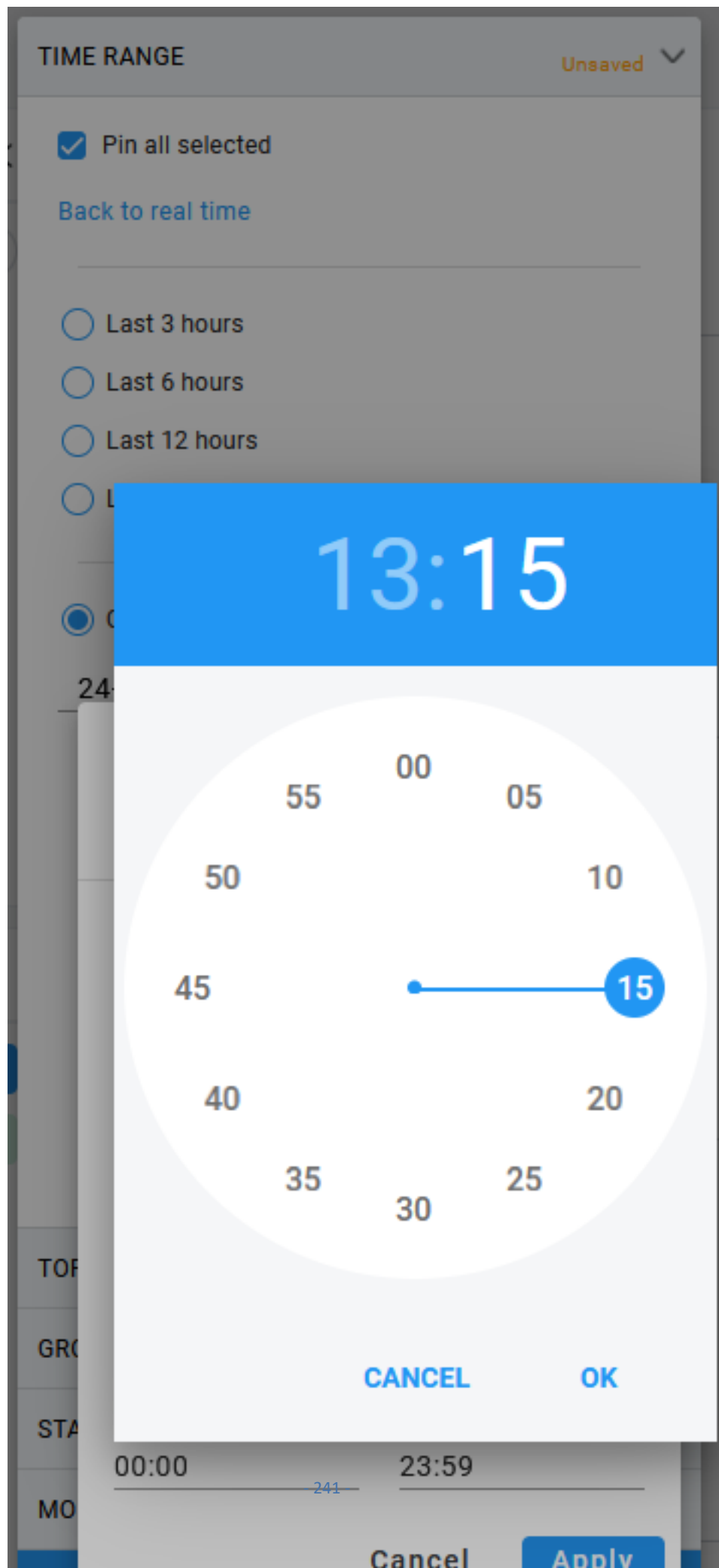
2. Click in the **start** field. The clock opens.



3. Move the clock arm to the desired hour and then click on it to open the Minutes clock view.



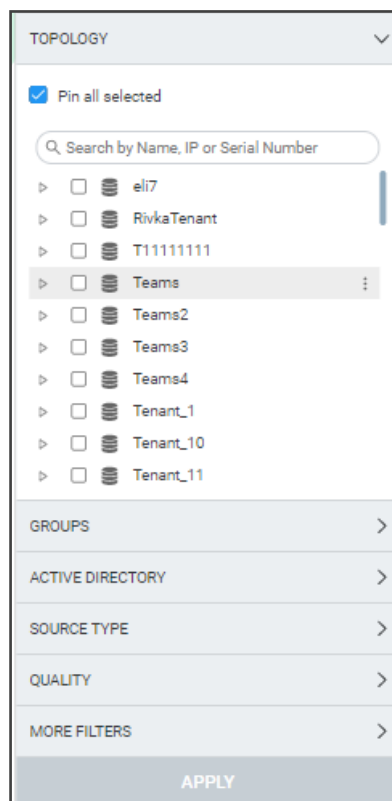
4. Set the desired minutes and then click **OK**.



5. Repeat the above steps to configure the time range for the ending time.
6. Click **Apply** to confirm changes.

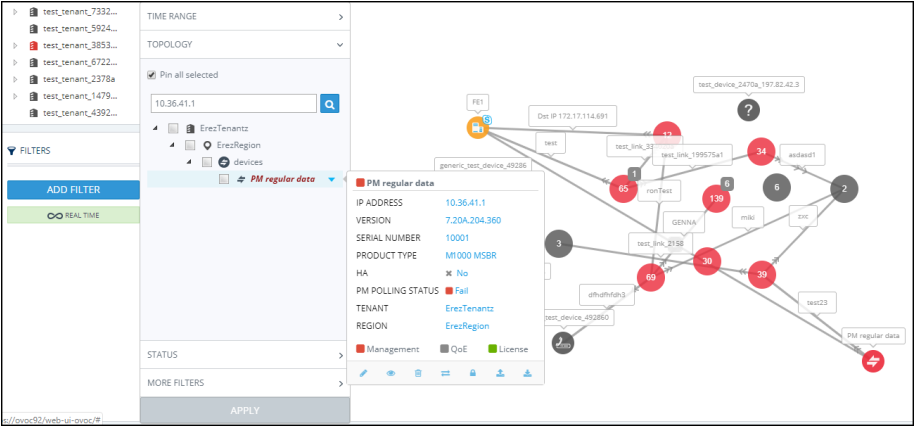
Filtering by 'Topology'

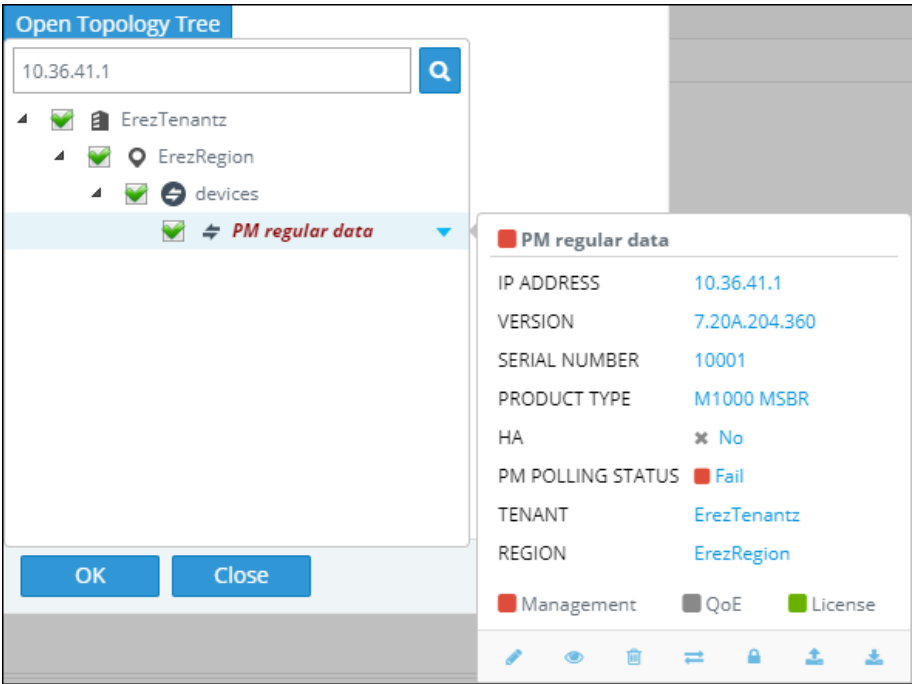
Filtering can be performed according to 'Topology'.



Use the table as reference.

Filter Feature	Description
Pin all selected	Select this option (default) in order to 'preserve' the filter; the filter will remain displayed in every screen whose tab you click. If you clear the option, the filter will only apply to the screen in which you apply the filter. The feature facilitates troubleshooting. After the filter is applied, the OVOC becomes non real time.
Search	<ul style="list-style-type: none"> ■ 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. <ul style="list-style-type: none"> ● 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

Filter Feature	Description
	<p>perform management actions from the row of action icons displayed lowermost.</p> <div></div> <p>■ Enter the Serial Number of the entity to search for; the entity whose SN you entered is displayed. Click the arrow adjacent to the entity to view information about the entity in a pop-up window and to decide if this entity is the one you are looking for. In the pop-up window, you can also choose to perform management actions from the row of action icons displayed lowermost.</p> <p>Note that the option to search per IP address and Serial Number is available in all pages / windows in which there is a Topology tree. In the Alarms Forwarding Rules Details screen, for example, the Open Topology Tree button opens a window whose search field can be searched per IP address and SN.</p>

Filter Feature	Description
	
'Tenant'	<p>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.</p>

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.

TIME RANGE >

TOPOLOGY >

GROUPS >

FLOATING LICENSE ▾

Floating License Status:

ALL | NONE | INVERT

☒ OK

☒ Error

☒ Config Error

☒ Unmanaged

☒ Unmonitored

Device Status:

ALL | NONE | INVERT

☒ Connected

☒ Rejected

☒ Not Connected

☒ Not Applicable

☒ Temporary Disconnected

MORE FILTERS >

APPLY



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.

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	Select to display entities that are temporarily disconnected from the

Filter	Description
Disconnected (red)	Floating License OVOC service due to problems with the HTTPS TCP connection.
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 OVOC.
Unmonitored (grey)	Select to display entities that are currently unmonitored by 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.

Filter	Description
No (red)	Select to display entities that are not managed by the Floating License service server.
Unmonitored (grey)	Select to display entities that are currently unmonitored by 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.

The screenshot shows a vertical filter menu with a light gray background. At the top, there are four filter categories: 'TIME RANGE', 'TOPOLOGY', 'GROUPS', and 'STATUS'. Each category has a right-pointing chevron (>) except for 'STATUS', which has a downward-pointing chevron (v). Below the 'STATUS' category, there are four status options, each with a blue checkmark in a box and a colored circle: 'OK' (green), 'Warning' (yellow), 'Error' (red), and 'Unmonitored' (gray). Above these options is the text 'ALL | NONE | INVERT'. At the bottom of the menu is a 'MORE FILTERS' link with a right-pointing chevron (>). Below the menu is a gray bar with the word 'APPLY' in white capital letters.

TIME RANGE	>
TOPOLOGY	>
GROUPS	>
STATUS	v
ALL NONE INVERT	
<input checked="" type="checkbox"/> ● OK	
<input checked="" type="checkbox"/> ● Warning	
<input checked="" type="checkbox"/> ● Error	
<input checked="" type="checkbox"/> ● Unmonitored	
MORE FILTERS	>
APPLY	

Use the following table as reference.

Status 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'.

The screenshot shows a 'MORE FILTERS' dialog box with a close button (v) in the top right corner. It contains three filter sections:

- Managed By License Pool:** A dropdown menu with 'Both' selected.
- Device Family Type:** A search box and a dropdown arrow.
- Product Type:** A search box and a dropdown arrow.

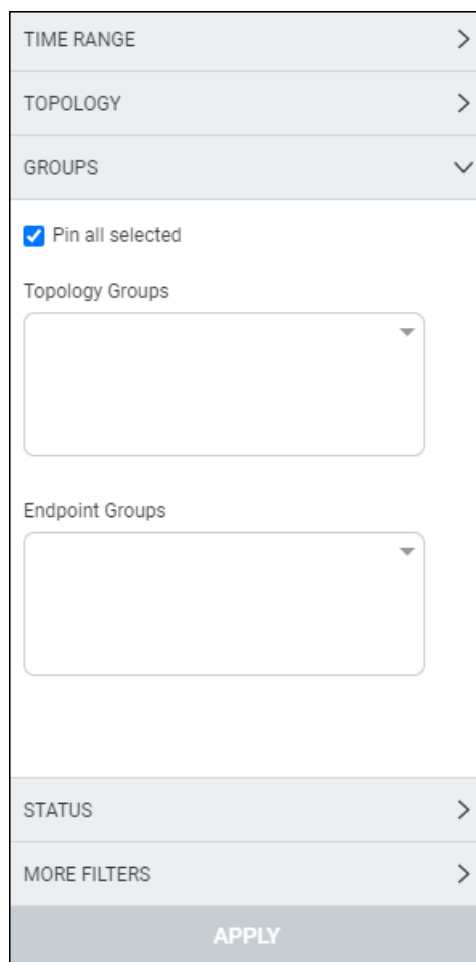
An **APPLY** button is located at the bottom of the dialog.

Use the following table as reference.

More 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'

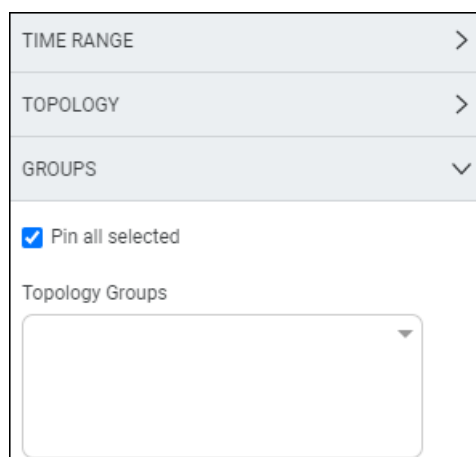
The OVOC's Endpoints Groups page (**Network > Endpoints > Groups**) allows the operator to filter OVOC pages according to Endpoints Groups.



The screenshot shows a vertical sidebar with several filter categories: TIME RANGE, TOPOLOGY, GROUPS, STATUS, and MORE FILTERS. Each category has a right-pointing chevron. The GROUPS category is expanded, showing a checked checkbox for 'Pin all selected' and two empty drop-down menus labeled 'Topology Groups' and 'Endpoint Groups'. At the bottom of the sidebar is a grey button labeled 'APPLY'.

- 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 187 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.



This screenshot is similar to the previous one, but it focuses on the 'Topology Groups' pane. It shows the same sidebar structure, but the 'Endpoint Groups' pane is not visible. The 'Topology Groups' drop-down menu is present and empty.

- 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 191 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

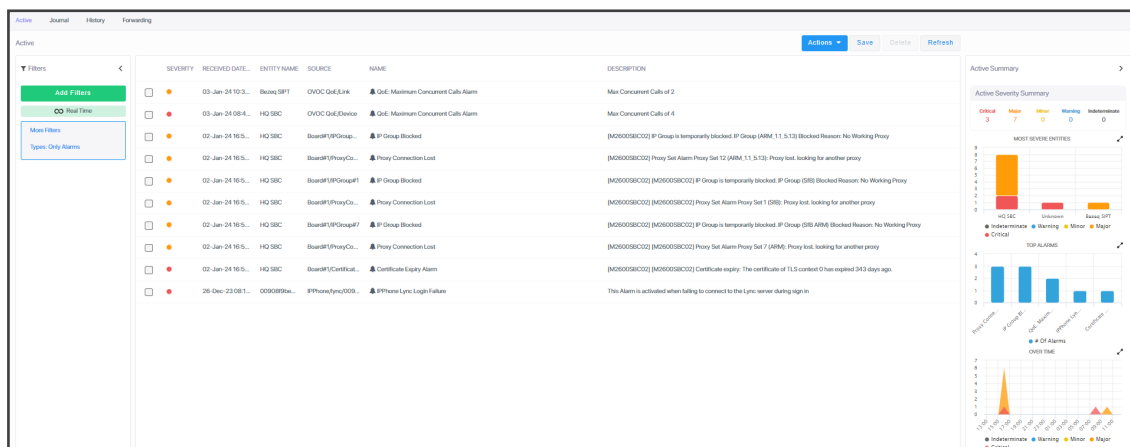
For information on how to configure the way alarms and events are displayed in the Alarms pages, see [Configuring Alarms Settings](#) on page 112.

Monitoring Active Alarms to Determine Network Health

The Active Alarms page's Active Alarm Summary pane enables admins to effectively monitor all active alarms of all severity levels in the IP telephony network.

➤ To monitor active alarms:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Active Alarms page (**Alarms > Active**) and locate the Active Summary pane on the right side of the page.

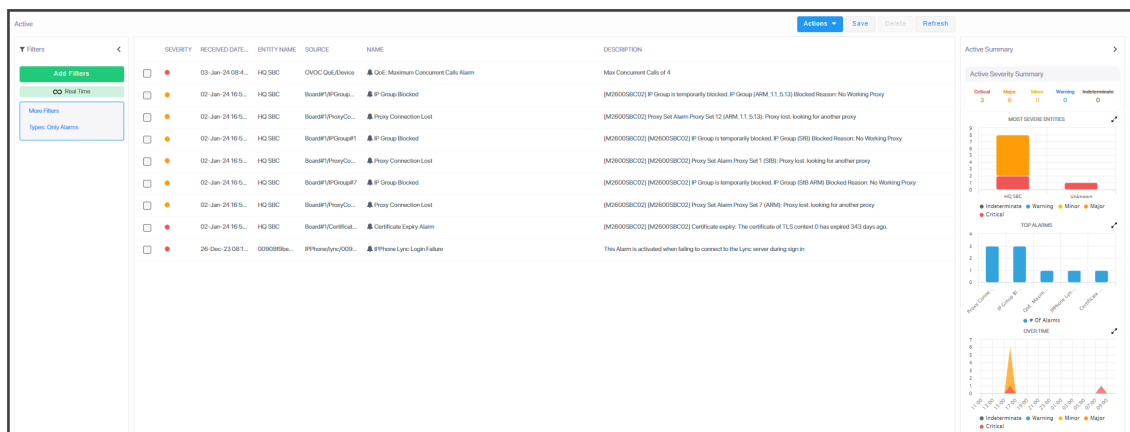


Performing Management Actions on Active Alarms

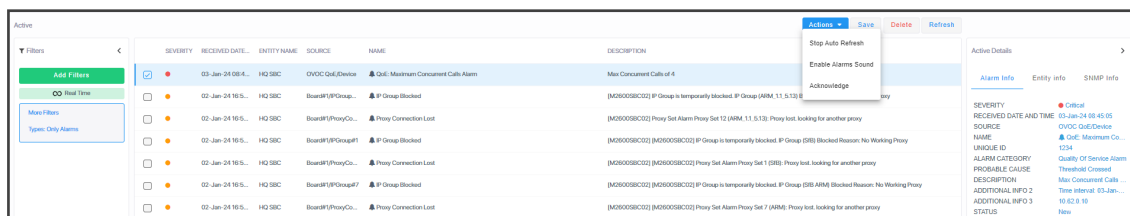
The Active Alarms page enables you perform management actions on all alarms currently active in the network, including deleting, acknowledging, and saving alarms to file.

➤ To perform management actions on active alarms:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Active Alarms page (**Alarms > Active**).



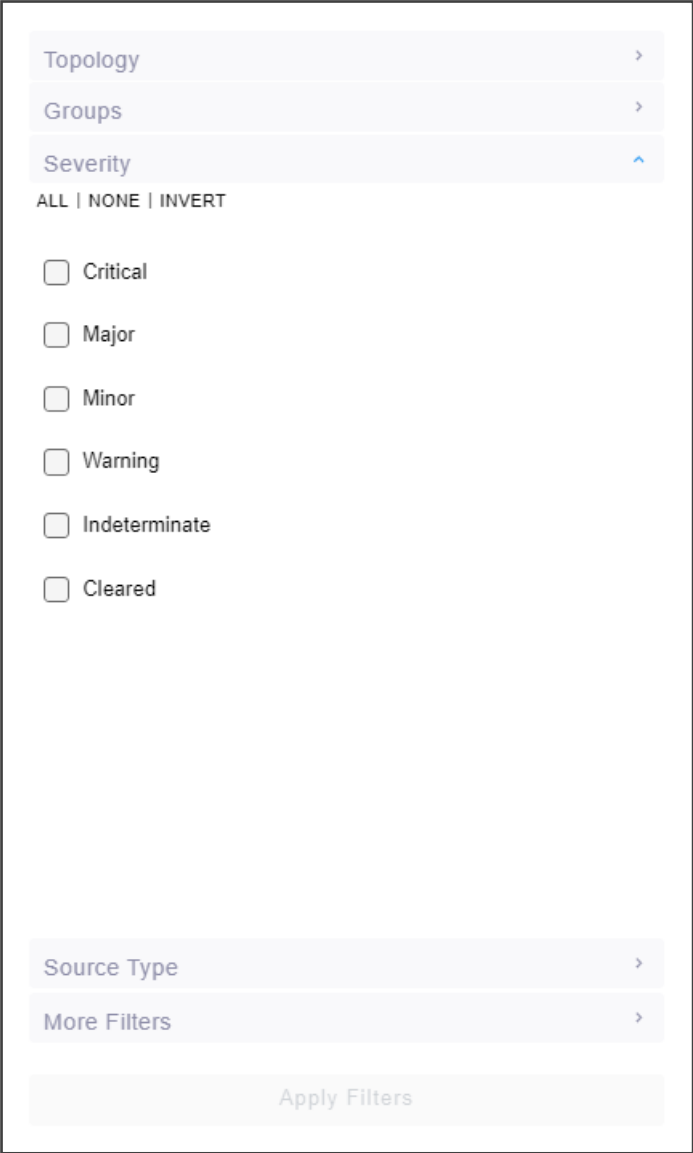
- Optionally filter the page by Topology (see [Filtering by 'Topology'](#) on page 243), Severity (see [Filtering by 'Status'](#) on page 250), Source Type (see [Filtering by 'Severity'](#) on the next page), or More Filters (see [Filtering by 'More Filters'](#) on page 260), and then select an alarm or multiple alarms and click **Actions**.



- [Optionally] Select **Stop Auto Refresh**, **Enable Alarms Sound** or **Acknowledge**.
- [Optionally] Click the **Save** button to save alarms to file for future reference.
- [Optionally] Select an alarm or multiple alarms and then click the **Delete** button.
- [Optionally] Click the **Refresh** button.

Filtering by 'Severity'

The 'Severity' filter applies to the pages under the **Alarms** menu: Active, Journal, History and Forwarding pages.



The screenshot shows a filter panel with the following elements:

- Three filter categories: 'Topology', 'Groups', and 'Severity'. Each has a right-pointing chevron. The 'Severity' category is expanded, showing a blue upward-pointing chevron.
- Below the 'Severity' category, there are three options: 'ALL', 'NONE', and 'INVERT', separated by vertical bars.
- A list of severity levels, each with an unchecked checkbox:
 - Critical
 - Major
 - Minor
 - Warning
 - Indeterminate
 - Cleared
- At the bottom of the panel, there are three more filter categories: 'Source Type', 'More Filters', and 'Apply Filters', each with a right-pointing chevron.

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 6-3: 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.
Cleared	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 OVOC. The figure below left shows the 'Source Type' filter in the Calls List page. The figure below right shows the 'Source Type' filter in the Alarms pages.

Time Range >

Topology >

Groups >

Active Directory >

Source Type ^

ALL | NONE | INVERT

☐ Devices

☐ Site

☐ Link

☐ Endpoint

☐ Location

Quality >

More Filters >

Apply Filters

Topology >

Groups >

Severity >

Source Type ^

ALL | NONE | INVERT

☐ Devices

☐ Site

☐ Link

☐ Endpoint

☐ ARM

☐ ZOOM

More Filters >

Apply Filters

Use the following table as reference.

Filter	Description
Devices	Displays only calls whose report was sent to the OVOC <i>from devices</i> .
Site	Displays only calls whose SIP Publish report was sent by endpoints to the OVOC <i>from sites</i> .
Links	Displays only calls transmitted <i>through links</i> .
Endpoint	Displays only calls whose SIP Publish report was sent to the OVOC <i>from endpoints</i> .
Location	Applies only to the Calls List page. Filters calls by the statistics that were calculated for Active Directory users locations.
ARM	Applies only to the Alarms pages (Active Alarms, Journal, History and

Filter	Description
	Forwarding). Only alarms that arrived from the ARM will be displayed.
ZOOM	Applies only to the Alarms pages (Active Alarms, Journal, History and Forwarding). Only alarms that arrived from Zoom will be displayed.

Filtering by 'More Filters'

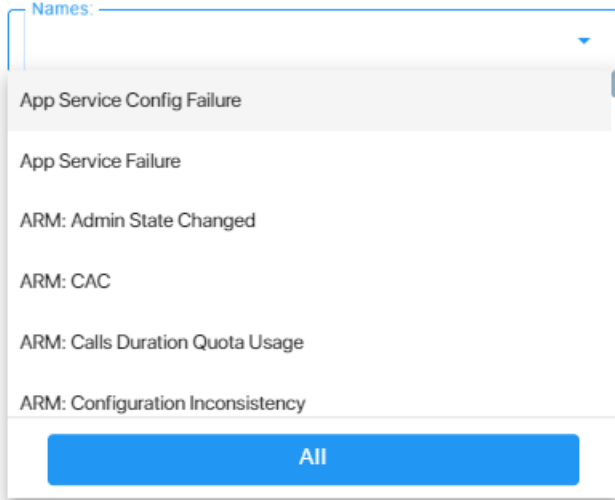
The Alarms > Active page can be filtered by **More Filters**.

The screenshot shows a 'More Filters' panel with the following elements:

- A list of filter categories: Topology, Groups, Severity, Source Type, and More Filters (indicated by a blue upward arrow).
- Three dropdown menus:
 - Alarm Types:** Set to 'Only Alarms'.
 - Names:** Empty.
 - Sources:** Empty.
- An 'Apply Filters' button at the bottom.

Use the following table as reference.

Filter	Description
Alarm Types	From the dropdown, select the 'Only Events' option for the page to display only alarms that are of type events.

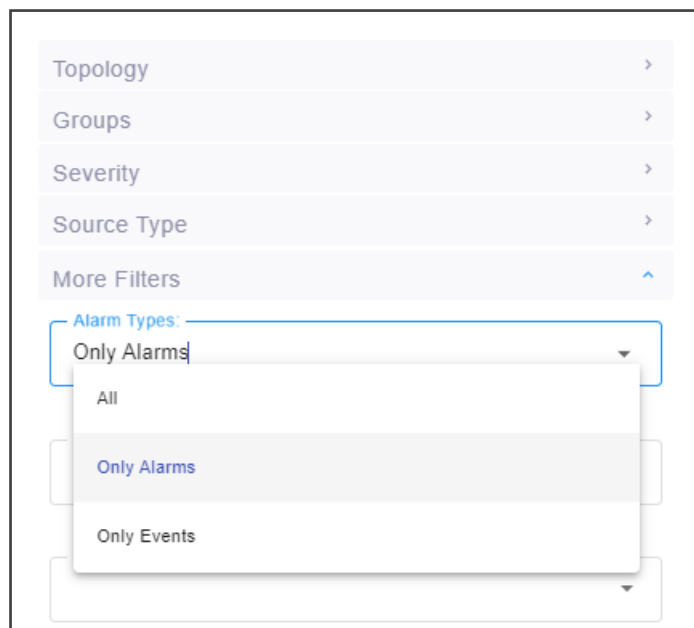
Filter	Description
	Select 'Only Alarms' for the page to display only alarms. 'All' includes 'Events' as well as 'Alarms'.
Names	<p>From the dropdown, select the name of the alarm to filter by.</p> 
Sources	Click the field and enter the source of the alarm to filter by. Other sources can in addition be specified. Click Apply Filters ; the page displays only those alarms that originated from the specified source(s).

Filtering by 'Type'

The 'Alarm Types' filter augments existing filtering capability in the Active page; you can filter the page for 'Only Alarms' or 'Only Events'.

➤ To filter for 'Alarm Types':

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



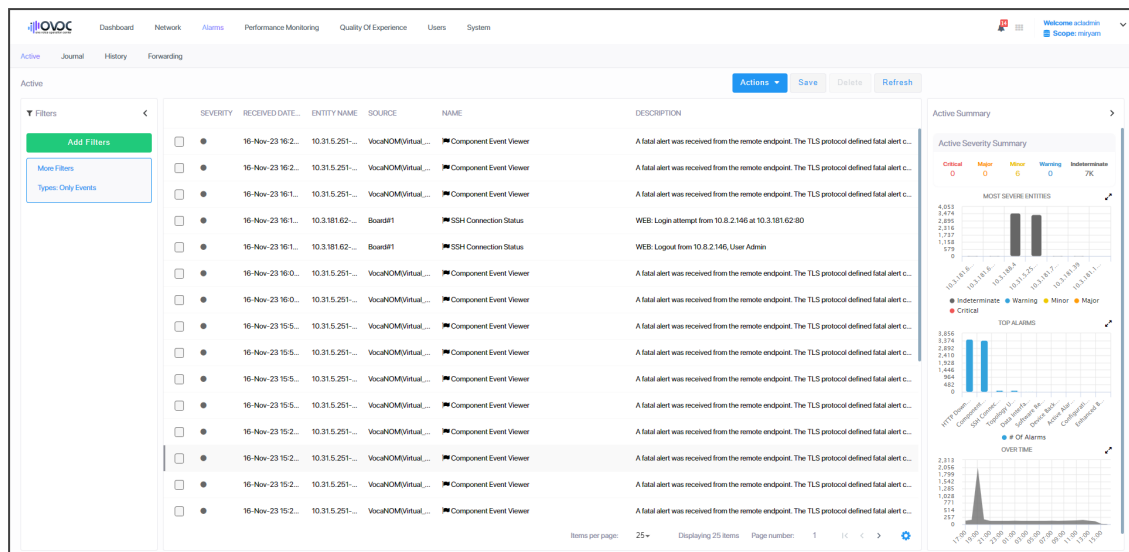
2. Click **Apply Filters** and view in the Active page, in the 'Name' column:

- Bell icons, if you filtered for 'Only Alarms'
- Flag icons, if you filtered for 'Only Events'

Figure 6-5: Filtering by Type - Alarms (bells icons in 'Name' column)

<div> <div>OVOC</div> <div>Dashboard Network Alarms Performance Monitoring Quality Of Experience Users System</div> <div>Welcome aadrian Scope: myyam</div> </div>									
Active Journal History Forwarding									
<div> <div>Filters</div> <div> <div>Add Filters</div> <div>More Filters</div> <div>Types: Only Alarms</div> </div> </div>									
	SEVERITY	RECEIVED DATE...	ENTITY NAME	SOURCE	NAME	DESCRIPTION			
<input checked="" type="checkbox"/>	●	16-Nov-23 16:2...	10.315.291-...	VocaNOM/VocaN...	▲ Connection Failure	Error when getting a Token from cloud manager using the TokenManager			
<input type="checkbox"/>	●	16-Nov-23 12:4...	10.3.181.62-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.			
<input type="checkbox"/>	●	16-Nov-23 12:4...	10.3.181.62-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.			
<input type="checkbox"/>	●	16-Nov-23 12:4...	10.3.181.62-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.			
<input type="checkbox"/>	●	16-Nov-23 09:5...	10.3.181.71-...	Board1	▲ Restart Needed Alarm	Configuration was changed. Reset the device for the new settings to take effect.			
<input type="checkbox"/>	●	15-Nov-23 09:2...	10.3.188.4	Board1(IPGroup#0	▲ IP Group Blocked	IP Group is temporarily blocked. IPGroup(Default, IPG) Blocked Reason: No Working Proxy			
<input type="checkbox"/>	●	14-Nov-23 17:5...	10.3.181.63-...	OVOC Mgmt	▲ Connection Alarm	Connection Lost			
<input type="checkbox"/>	●	14-Nov-23 17:3...	10.3.181.63-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.			
<input type="checkbox"/>	●	14-Nov-23 17:3...	10.3.181.63-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.			
<input type="checkbox"/>	●	14-Nov-23 17:3...	10.3.181.63-...	Board1(Ethernet...	▲ Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.			
<input type="checkbox"/>	●	14-Nov-23 17:3...	10.3.181.63-...	Board1(IPGroup#3	▲ IP Group Blocked	IP Group is temporarily blocked. IPGroup(CRP Gateway) Blocked Reason: No Working Pro...			
							Active Details		
							<div>Alarm Info Entity Info SNMP Info</div> <div> <div>SEVERITY</div> <div>CRITICAL</div> </div> <div> <div>OCCURRED DATE AND TIME</div> <div>16-Nov-23 16:23:27</div> </div> <div> <div>SOURCE</div> <div>VocaNOM/VocaNOM...</div> </div> <div> <div>NAME</div> <div>Connection Failure</div> </div> <div> <div>UNIQUE ID</div> <div>111291</div> </div> <div> <div>ALARM CATEGORY</div> <div>Other</div> </div> <div> <div>PROBABLE CAUSE</div> <div>Error when getting a T...</div> </div> <div> <div>DESCRIPTION</div> <div></div> </div> <div> <div>STATUS</div> <div>New</div> </div>		

Figure 6-6: Filtering by Type - Events (flags icons in 'Name' column)



Filtering by 'Alarm Names'

The 'Names' filter enables filtering the Alarms > Active page by alarm name.

➤ To filter by 'Names':

- In the Active page, click **Add Filter**, choose **More Filters** and then from the 'Names' drop-down, select the filter.

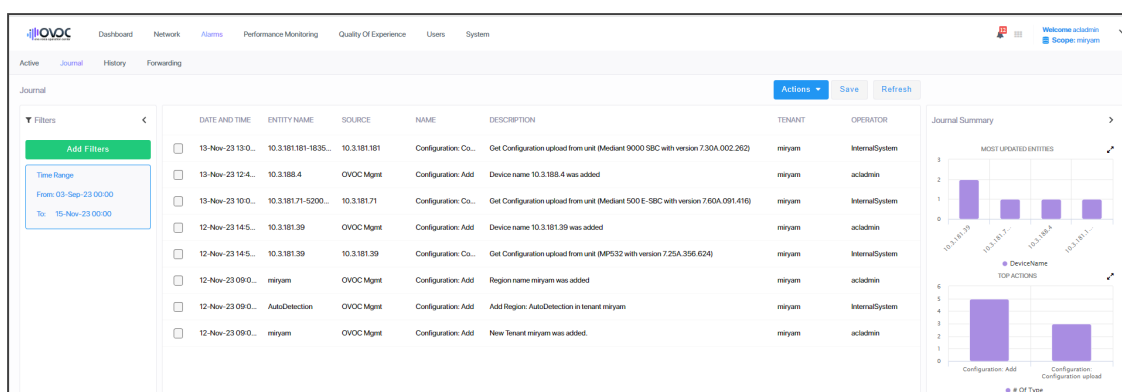
The screenshot shows the 'More Filters' dropdown menu in the OVOC interface. The menu is open, displaying a list of alarm names: 'App Service Config Failure', 'App Service Failure', 'ARM: Admin State Changed', 'ARM: CAC', 'ARM: Calls Duration Quota Usage', and 'ARM: Configuration Inconsistency'. The 'All' option is highlighted at the bottom of the list. The background shows the 'Topology', 'Groups', 'Severity', and 'Source Type' filters, and the 'Alarm Types' dropdown set to 'All'. An 'Apply Filters' button is visible at the bottom of the screen.

- 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 268).



- The Journal Alarms page reflects *all actions* performed by network administrators in AudioCodes's *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's *Device Manager Administrator's Manual*.
- Any activity performed on the OVOC is captured and displayed in the Journals Alarms page, including the source IP of the user. This applies to all actions performed by OVOC administrators like login, password change, creating new users, etc.
 - ✓ In the Journal Alarms page shown in the preceding figure, you can see that a new user has been added by acladmin.
 - ✓ Also displayed is the 'Operator IP Address' (source IP) from where acladmin added the new user.
- New Journal actions are logged when operators access private information:
 - ✓ When they access the Calls screen
 - ✓ When they access Call Details
 - ✓ When they access Users
 - ✓ When they access URI / User Reports

Filtering the Alarms Journal by 'More Filters'

The Alarms Journal page can be filtered by 'More Filters' to reduce unwanted information in the page and facilitate easier access to required information.

Time Range >

Topology >

Groups >

Source Type >

More Filters ^

Journal Names:

Sources:

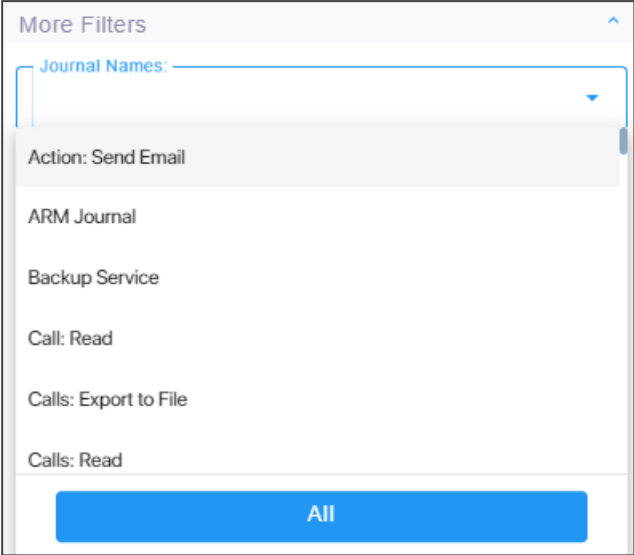
Description:

Operator:

Apply Filters

Use the table as reference.

Filter	Description
Journal Names	From the drop-down, select a journal name.

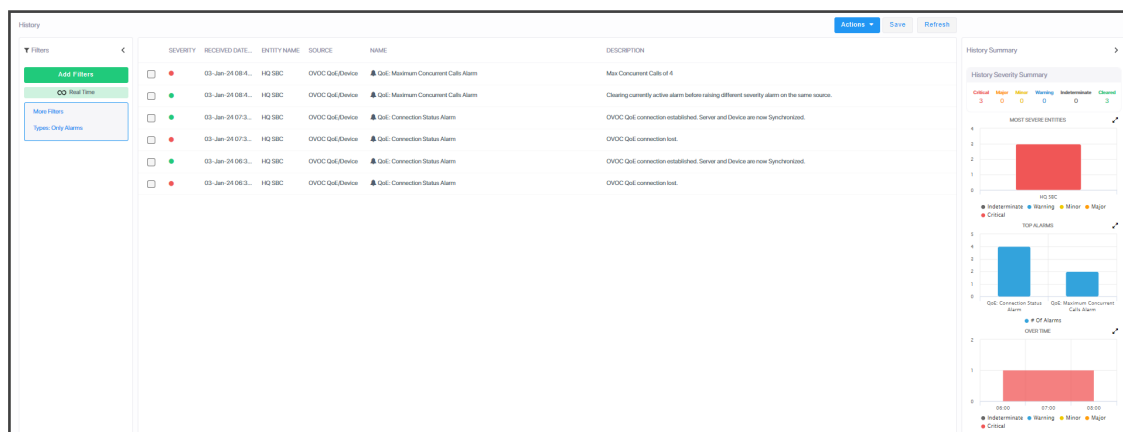
Filter	Description
	
Sources	From the drop-down, select the name of the entity from which the alarm originated.
Description	Enter a word or string recalled from the description by which to filter.
Operator	Enter the name of the operator by whom to filter.

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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the History page (**Alarms > History**).



3. 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 231.

Time Range

☒ Pin all selected

Real Time

☐ Last 3 hours

☐ Last 6 hours

☐ Last 12 hours

☐ Last 24 hours

☐ Custom

03-Jan-24 00:00 – 03-Jan-24 23:59

Topology

Groups

Severity

Source Type

More Filters

Apply Filters

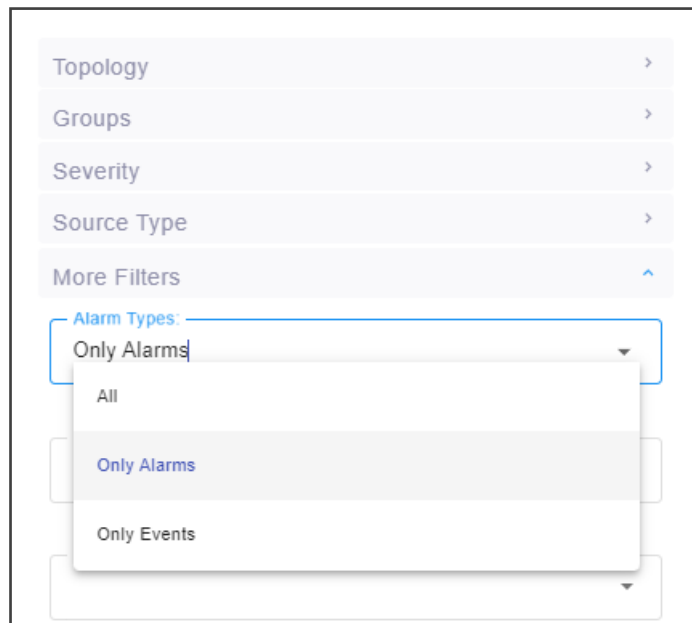
Filtering by 'Type'

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 6-7: 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 6-8: History Alarms - Type Filter

HISTORY						
FILTERS		Actions	Refresh			
ADD FILTER						
REAL TIME						
MORE FILTERS						
TYPE: ONLY ALARMS						
SEVERITY	RECEIVED DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	
03-May-18 14:53:04	10.3.181.83-9331606	Board#1/CertificateExpiry#0	Certificate Expiry Alarm	Certificate expiry: The certificate of TLS context 0 has expired 17654 days ago.		
03-May-18 14:53:04	10.3.181.83-9331606	Board#1/CertificateExpiry#0	Certificate Expiry Alarm	Alarm cleared: Certificate expiry: The certificate of TLS context 0 has expired 17653 days ago.		
03-May-18 13:36:25	CLM_10.36.50.244	OVOC Mgmt	GW Connection Alarm	Connection established		
03-May-18 13:36:25	CLM_10.36.49.178	OVOC Mgmt	GW Connection Alarm	Connection established		
03-May-18 13:36:25	10.36.12.154	OVOC Mgmt	GW Connection Alarm	Connection established		
03-May-18 13:36:25	mimic_10.36.12.192	OVOC Mgmt	GW Connection Alarm	Connection established		
03-May-18 13:35:34	CLM_10.36.50.244	OVOC Mgmt	GW Connection Alarm	Connection Lost		
03-May-18 13:35:34	CLM_10.36.49.178	OVOC Mgmt	GW Connection Alarm	Connection Lost		
03-May-18 13:35:34	10.36.12.154	OVOC Mgmt	GW Connection Alarm	Connection Lost		
03-May-18 13:35:34	mimic_10.36.12.192	OVOC Mgmt	GW Connection Alarm	Connection Lost		
03-May-18 12:51:47	mimic_10.36.1.69	OVOC QoS/mimic_10.36.1.69	Poor Voice Quality	Poor Quality 7% of calls, 14 of 215 calls.		
03-May-18 12:51:47	mimic_10.36.1.69	OVOC QoS/mimic_10.36.1.69	Poor Voice Quality	Clearing currently active alarm before raising different severity alarm on the same source		

Filtering by 'Alarm Names'

The 'Alarm Names' filter augments already existing filtering capability in the History Alarms page; you can filter the page by alarm name.

➤ **To filter by 'Alarm Names':**

1. In the Alarms History page, click **Add Filter**, choose **More Filters** and then from the 'Alarm Names' drop-down, select the filter.

Figure 6-9: 'Alarm Names' Filter

Topology >

Groups >

Severity >

Source Type >

More Filters ^

Alarm Types: All

Names:

- App Service Config Failure
- App Service Failure
- ARM: Admin State Changed
- ARM: CAC
- ARM: Calls Duration Quota Usage
- ARM: Configuration Inconsistency

All

Apply Filters

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. See also [Forwarding Alarms](#) on the next page following.

Forwarding Alarms

The Forwarding page enables operators to add an alarm forwarding rule.

➤ **To configure alarm forwarding:**

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Forwarding page (**Alarms > Forwarding**).

The screenshot shows the OVOC interface with the 'Forwarding' page selected. The table lists the following rules:

RULE NAME	ACTIVE	RULE TYPE	DESTINATION TYPE	DESTINATION	TENANT
<input checked="" type="checkbox"/> email	✓	Alarm	MAIL	miyam.brand@audiocodes.com	System
<input type="checkbox"/> not	✓	Alarm	NOTIFICATION	All Selected	System
<input type="checkbox"/> test	✓	Journal	MAIL	test@microsoft.com	System
<input type="checkbox"/> test1	✓	Journal	MAIL	110@110.com	System
<input type="checkbox"/> test222	✓	Alarm	SNMP	8.8.8.8	miyam

The sidebar on the right shows details for the 'email' rule:

- RULE NAME:** email
- ACTIVE:** ✓
- DESTINATION TYPE:** MAIL
- DESTINATION:** miyam.brand@audioco...
- Rule Conditions:**
- ALARM NAMES:** 4/41 Selected

3. Click **Add Alarm Rule**.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions

Rule Conditions

Destination

Active Time

Rule Owner*

System - all tenants

Attachments

Tenants:	all Tenant/s,	All / None	Open Topology Tree
Regions:	all Region/s,	All / None	
Devices:	all Device/s,	All / None	
Links:	0 Link/s,	All / None	
Sites:	0 Site/s,	All / None	

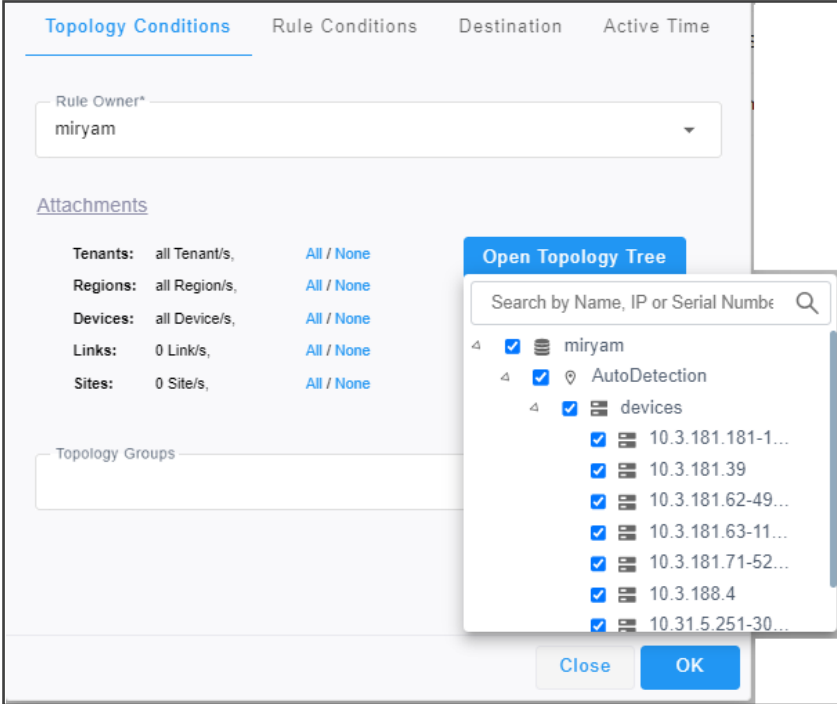
Topology Groups

Close

OK

- Configure the Topology Conditions using the following table as reference:

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select 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.</p> <p>See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 254</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under Rule Conditions and Destinations are met.</p> <p>See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 254</p>
Rule Owner	<p>From the drop-down, select System – all tenants; the rule will then apply to <i>all tenants</i> and to all regions/links/devices/sites under all tenants.</p> <p>Here's what you'll then view next to 'Attachments': all Tenant/s, all Region/s, all Device/s, all Link/s, all Site/s</p> <p>If you select <i>a specific tenant</i> from the drop-down, the rule will apply by default to <i>all entities under that specified tenant</i>.</p> <p>Click the Open Topology Tree button.</p>

Parameter	Description
	 <p>Only the operator assigned to that tenant can view and change. The All/None filters under 'Attachments' allow you to specify to which entities rule forwarding will apply, if not to all.</p>
Topology Groups	<p>In the Topology Groups page, entities can be added to a logical group as shown here. When adding an alarm forwarding rule, optionally select one of these groups (instead of selecting each individual entity in the Topology tree); alarms will be forwarded from all entities in that group.</p>

5. Click the **Rule Conditions** tab.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions

☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions

Rule Conditions

Destination

Active Time

Alarm Origin

All Selected

☐ none

Event Origin

All Selected

☐ none

Severities

All Selected

Alarm Names

All Selected

Alarm Types

All Selected

Source

Close

OK

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

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select 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.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 254</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under Rule Conditions and Destinations are met.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarm Settings on page 254</p>
Alarm Origin	<p>Select the origin from which alarms will be forwarded:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Management <input type="checkbox"/> QoE <input type="checkbox"/> Devices <input type="checkbox"/> Endpoints <input type="checkbox"/> ARM <input type="checkbox"/> VIP Endpoints Users
Event Origin	<p>Select the origin from which events will be forwarded:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Management <input type="checkbox"/> QoE <input type="checkbox"/> Devices <input type="checkbox"/> Endpoints <input type="checkbox"/> ARM <input type="checkbox"/> VIP Endpoints Users
Severities	From the 'Severities' drop-down, select the severity level of the alarms you want to receive:

Parameter	Description
	<ul style="list-style-type: none"> <input type="checkbox"/> Warning <input type="checkbox"/> Minor <input type="checkbox"/> Major <input type="checkbox"/> Critical <input type="checkbox"/> Indeterminate <p>Default: All Selected.</p>
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).

7. Click the **Destination** tab.

OVOC can forward alarms to multiple destinations, in these formats:

- SNMP Notifications (SNMP 1 / SNMP 2) - see [here](#)
- External Mail / Internal Mail - see [here](#)
- Syslog - see [here](#)
- Notification - see [here](#)
- REST - see [here](#)

8. Click the **Active Time** tab - see [here](#) for more information.

Configuring when Forwarding will be Active

The alarms forwarding feature can be configured to be active on specific days of the week and at specific times of the day.



If the forwarding feature is configured to be active on specific hours, OVOC does not consider alarms raised/cleared behavior, so a cleared alarm can be forwarded even if the corresponding raised alarm, raised outside the configured active time, was not forwarded.

➤ **To determine when the feature will be active:**

1. In the Alarms Forwarding Rule Details screen, click the **Active Time** tab.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions Destination **Active Time**

All / None

<input checked="" type="checkbox"/> Monday	Active all day	
<input checked="" type="checkbox"/> Tuesday	Active all day	
<input checked="" type="checkbox"/> Wednesday	Active all day	
<input checked="" type="checkbox"/> Thursday	Active all day	
<input checked="" type="checkbox"/> Friday	Active all day	
<input checked="" type="checkbox"/> Saturday	Active all day	
<input checked="" type="checkbox"/> Sunday	Active all day	

Close **OK**

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

Parameter	Description
All / None	Select a day days in the week on which the alarms forwarding feature will be active.

Forwarding Alarms whose Destination Type is 'SNMP'

The SNMP forwarding option (**Alarms > Forwarding > Add**) 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 6-10: SNMP v2

The screenshot shows a web-based configuration window titled "ALARMS FORWARDING RULE DETAILS". It contains several input fields and options for setting up an alarm forwarding rule. The "Destination" tab is selected, showing fields for "Destination Type" (set to "SNMP"), "Destination Host IP Address", "Destination Host Port" (set to "162"), and "Trap Community". There are also radio buttons for "SNMP v2" (selected) and "SNMP v3". At the bottom, there are "Close" and "OK" buttons.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions **Destination** Active Time

Destination Type*
SNMP

Destination Details

Destination Host IP Address*

Destination Host Port
162

☒ SNMP v2 ☐ SNMP v3

Trap Community

Close OK

Figure 6-11: SNMP v3

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions **Destination** Active Time

Destination Type*

SNMP

Destination Details

Destination Host IP Address*

Destination Host Port

162

☐ SNMP v2 ☒ SNMP v3

Security Name*

Security Level*

No Security

Authentication Protocol

Authentication Key

Close OK

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

Table 6-4: Forwarding Alarms – Destination

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select 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.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under Rule Conditions and Destinations are met.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
Destination Type	<p>Determines the format in which the alarm or event will be forwarded. From the drop-down, select</p> <ul style="list-style-type: none"> <input type="checkbox"/> SNMP (default) <ul style="list-style-type: none"> <input checked="" type="checkbox"/> SNMP v2 <input checked="" type="checkbox"/> SNMP v3 <input type="checkbox"/> MAIL <input type="checkbox"/> SYSLOG

Forwarding Alarms whose Destination Type is 'Mail'



This 'Destination Type' description also applies to Journal forwarding 'Destination Type' shown [here](#).

➤ To forward alarms whose destination is 'Mail':

1. In the Alarms Forwarding Rule Details screen (**Alarms > Forwarding > Add**), select **MAIL** from the 'Destination Type' drop-down.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions Destination Active Time

Destination Type*

Mail

Destination Details

☐ Use Internal Mail Server

Mail Host*

Mail Host Username

Mail Host Password

From*

Close OK

2. Select the **Use Internal Mail Server** option.
3. Configure the parameters using the following table as reference.

Parameter	Description
Use Internal Mail Server	<p>If this option is selected, all the fields in this table following will be deactivated, except the 'To' field. If selected, it'll only be necessary to configure the internal mail server as the destination to which to forward alarms; it'll be unnecessary to configure a mail host. If the option is cleared, all the fields in the table following will be activated.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
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	<p>Enter the e-mail address the recipient will see when the mail arrives.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
To	<p>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.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>

- 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 (**Alarms > Forwarding > Add**), select **SYSLOG** from the 'Destination Type' drop-down.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions **Destination** Active Time

Destination Type*
Syslog

Destination Details

Syslog Host IP Address*

Syslog Host Port
514

Close OK

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

Table 6-5: 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 112
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 112
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':

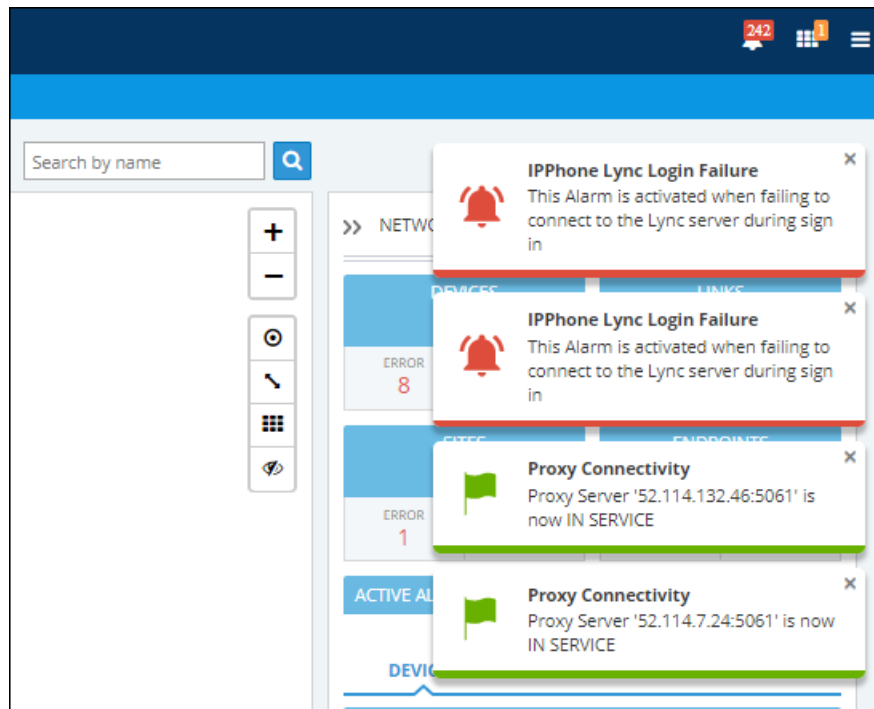
1. In the Alarms Forwarding Rule Details screen (**Alarms > Forwarding > Add**) under the **Destination** tab, select **Notification** from the 'Destination Type' drop-down.

The screenshot shows the 'ALARMS FORWARDING RULE DETAILS' screen. At the top, there is a title bar. Below it, there is a 'Rule Name*' text input field. Underneath, there are two radio buttons: 'Forward Alarms matching Topology and Rule conditions' (selected) and 'Prevent Forwarding of Alarms matching Topology and Rule conditions'. Below the radio buttons, there is a checkbox labeled 'Enable/Disable Rule' which is checked. At the bottom of the form, there are four tabs: 'Topology Conditions', 'Rule Conditions', 'Destination' (selected), and 'Active Time'. Under the 'Destination' tab, there is a 'Destination Type*' dropdown menu with 'Notification' selected. Below this, there is a section titled 'Destination Details' containing an 'Assigned Operators' dropdown menu with 'All Selected' selected. At the bottom right of the screen, there are two buttons: 'Close' and 'OK'.

2. Configure the parameters using the table as reference.

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select 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.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under Rule Conditions and Destinations are met.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in Configuring Alarms Settings on page 112</p>
Assigned Operators	<p>Under 'Destination Details', configure the operator (or operators) to whom you want the alarm notifications to be forwarded.</p> <p>Note:</p> <ul style="list-style-type: none"> ■ 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.

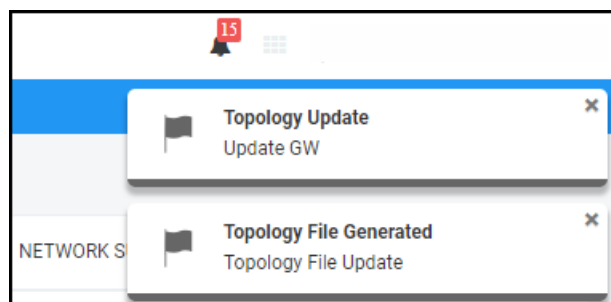
3. Click **OK**; notifications will automatically pop up in the uppermost right corner in the GUIs of all assigned operators, when alarms are received.



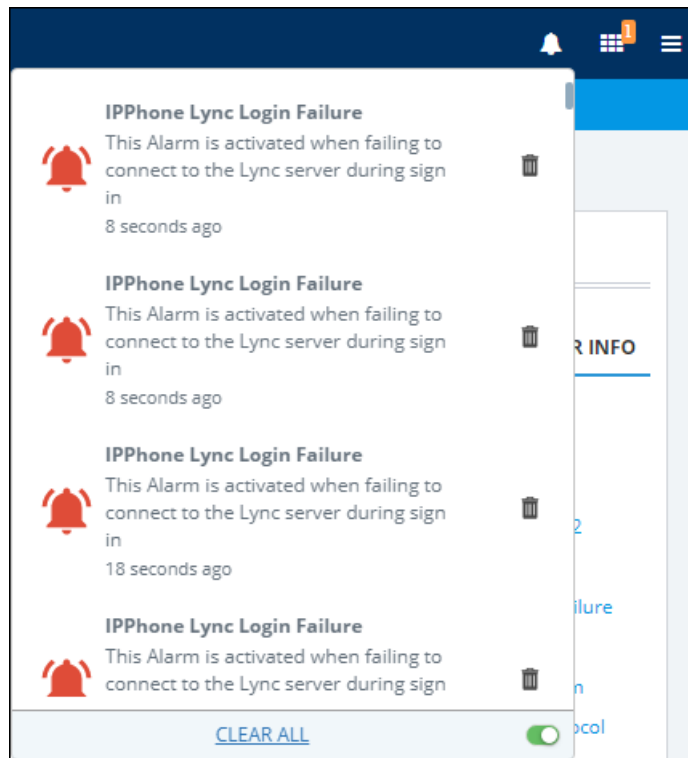
To configure the *timeout* of notification pop-ups, see [Configuring Operator Authentication Locally, in OVOC](#) on page 53 and refer to the parameter 'Notifications display time (sec)'. The default is 3 seconds. Configuring the parameter to 0 disables the feature.

➤ **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**.

Forwarding Alarms whose Destination Type is 'REST'

Alarms can be forwarded to the 'REST' destination type.



This 'Destination Type' description also applies to Journal forwarding 'Destination Type' shown [here](#).

This option allows forwarding alarms to the REST API.



- Both a 'System' operator with a security level of 'Admin' or 'Operator' *and* a 'Tenant' operator with a security level of 'Admin' or 'Operator' have permission to configure / edit an Alarm Forwarding rule.
- A 'System' operator with a security level of 'Monitoring' can only *view* rules.
- All alarms filters are available for the REST destination (see under [Performing Management Actions on Active Alarms](#) on page 254).

➤ To forward alarms whose Destination Type is 'REST':

1. In the Alarms Forwarding Rule Details screen (**Alarms > Forwarding > Add**) under the **Destination** tab, select **REST** from the 'Destination Type' drop-down.

ALARMS FORWARDING RULE DETAILS

Rule Name*

☒ Forward Alarms matching Topology and Rule conditions
☐ Prevent Forwarding of Alarms matching Topology and Rule conditions

☒ Enable/Disable Rule

Topology Conditions Rule Conditions **Destination** Active Time

Destination Type*

REST

Destination Details

Host*

Path

Authorization Header Key

Authorization

Authorization Header Value

Close

OK

- Configure the parameters using the table as reference.

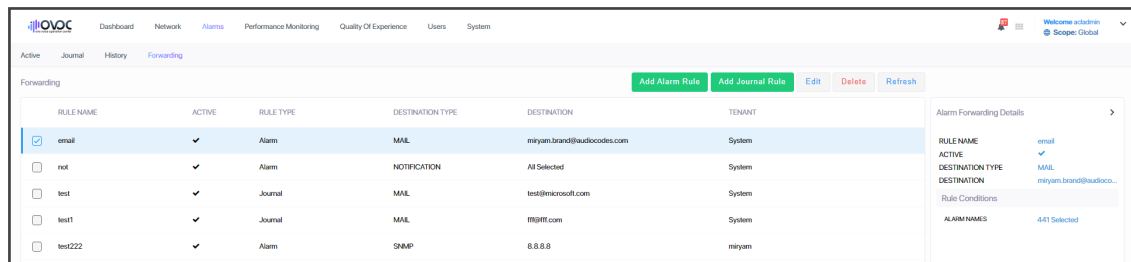
Table 6-6: Forwarding Alarms - Destination – REST

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or- Prevent forwarding matching	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
alarms/events	
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.
Destination Details	<p>Configure the following:</p> <ul style="list-style-type: none"> ■ Host (IP or FQDN of the destination REST server) ■ Path (The URL path of the REST server) ■ Authorization Header Key (Optional. String. Default: 'Authorization') ■ Authorization Header Value (Optional) <p>Note: OVOC uses the authorization header and value provided by the operator. If an authorization header is not provided, OVOC will use the default 'Authorization' used for basic authorization.</p> <p>If an authorization value is not provided, OVOC will not use send authorization at all (for REST servers that do not require authentication).</p>
Secured	Optional. Select the check box for a secured REST communication. Secured HTTPS does not support certificates. Clear the check box for an unsecured REST communication.

Viewing the New Rules in the Alarms Forwarding Page

The new rules are displayed in the Alarms Forwarding page (**Alarms > Forwarding**)



RULE NAME	ACTIVE	RULE TYPE	DESTINATION TYPE	DESTINATION	TENANT
<input checked="" type="checkbox"/> email	✓	Alarm	MAIL	miyam.brand@audiocodes.com	System
<input type="checkbox"/> not	✓	Alarm	NOTIFICATION	All Selected	System
<input type="checkbox"/> test	✓	Journal	MAIL	test@microsoft.com	System
<input type="checkbox"/> test1	✓	Journal	MAIL	ff@ff.com	System
<input type="checkbox"/> test222	✓	Alarm	SNMP	8.8.8.8	miyam

Alarm Forwarding Details

RULE NAME: email

ACTIVE: ✓

DESTINATION TYPE: MAIL

DESTINATION: miyam.brand@audioco...

Rule Conditions

ALARM NAMES: 4/41 Selected

Forwarding Journal Activity

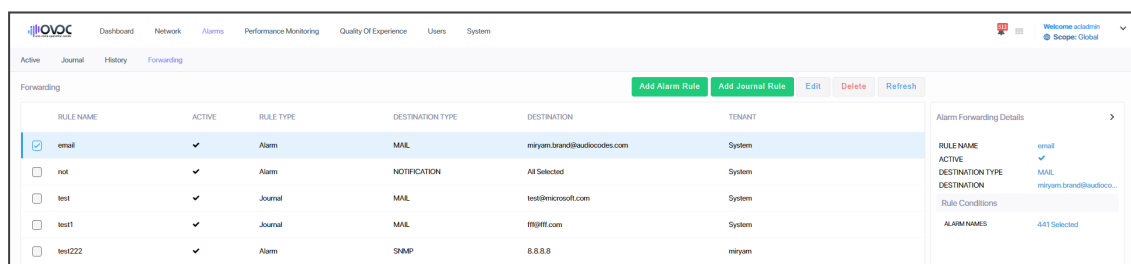
The Forwarding page enables operators to add a Journal forwarding rule.



Journal forwarding is available only to the 'System' type operator (only in 'Global' scope).

➤ To configure Journal forwarding:

1. Access the 'Global' scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Forwarding page (**Alarms > Forwarding**).



RULE NAME	ACTIVE	RULE TYPE	DESTINATION TYPE	DESTINATION	TENANT
<input checked="" type="checkbox"/> email	✓	Alarm	MAIL	miyam.brand@audiocodes.com	System
<input type="checkbox"/> not	✓	Alarm	NOTIFICATION	All Selected	System
<input type="checkbox"/> test	✓	Journal	MAIL	test@microsoft.com	System
<input type="checkbox"/> test1	✓	Journal	MAIL	ff@ff.com	System
<input type="checkbox"/> test222	✓	Alarm	SNMP	8.8.8.8	miyam

Alarm Forwarding Details

RULE NAME: email

ACTIVE: ✓

DESTINATION TYPE: MAIL

DESTINATION: miyam.brand@audioco...

Rule Conditions

ALARM NAMES: 4/41 Selected

3. Click **Add Journal Rule**.

JOURNAL FORWARDING RULE DETAILS

Rule Name*

☒ Enable/Disable Rule

Rule Conditions

Destination

Active Time

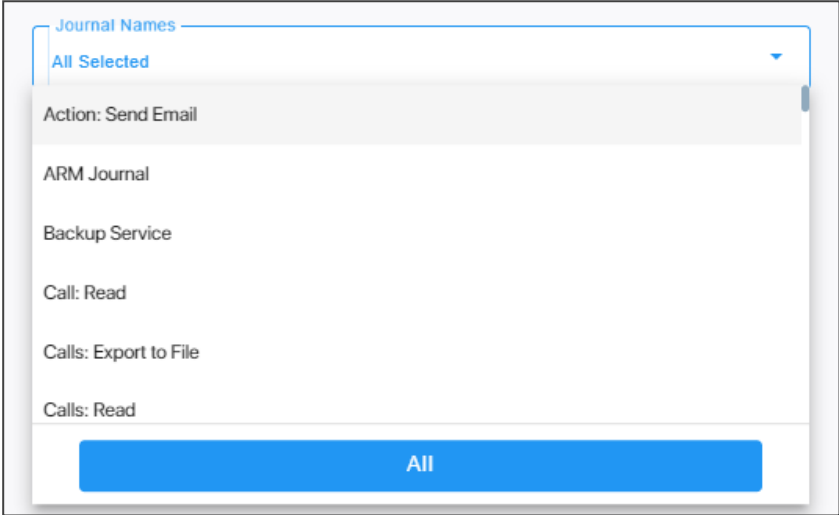
Journal Names

All Selected

Close

OK

4. Configure the rule using the following table as reference:

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under Rule Conditions and Destination and Active Time are met.
Journal Name	From the drop-down, select the name of the Journal activity. 

5. Click the **Destination** tab.

JOURNAL FORWARDING RULE DETAILS

Rule Name*

☒ Enable/Disable Rule

Rule Conditions **Destination** Active Time

Destination Type*
Mail

Destination Details

☐ Use Internal Mail Server

Mail Host*

Mail Host Username

Mail Host Password

From*

Close OK

OVOC can forward Journal activity to two destinations, in these formats:

- External Mail / Internal Mail - see [here](#) for a description of this 'Destination Type'
- REST - see [here](#) for a description of this 'Destination Type'

6. Click the **Active Time** tab.

JOURNAL FORWARDING RULE DETAILS

Rule Name*

☒ Enable/Disable Rule

Rule Conditions	Destination	Active Time
All / None		
<input checked="" type="checkbox"/> Monday	Active all day	
<input checked="" type="checkbox"/> Tuesday	Active all day	
<input checked="" type="checkbox"/> Wednesday	Active all day	
<input checked="" type="checkbox"/> Thursday	Active all day	
<input checked="" type="checkbox"/> Friday	Active all day	
<input checked="" type="checkbox"/> Saturday	Active all day	
<input checked="" type="checkbox"/> Sunday	Active all day	

Close
OK

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

Parameter	Description
All / None	<p>Select a day days in the week on which the Journal forwarding feature will be active.</p> <ul style="list-style-type: none"> Click All for the Journal forwarding feature to be active on all days in the week. Click None for the Journal forwarding feature to be active on no days in the week.
	<p>Click this icon adjacent to a day to define the start and end time the Journal forwarding feature will be active on that day; optionally use the clock icon to define the times.</p>

Parameter	Description
	<div> <div>Topology Conditions</div> <div>Rule Conditions</div> <div>Destination</div> <div>Active Time</div> </div> <div>All / None</div> <div> <div> <input checked="" type="checkbox"/> Monday <div>00:00 - 24:00</div> <div> <div>start</div> <div>00:00</div> <div>end</div> <div>24:00</div> </div> </div> <div> <div>+</div> <div>^</div> <div>🗑️</div> </div> </div> <div> <div> <input checked="" type="checkbox"/> Tuesday <div>Active all day</div> <div>+</div> </div> <div> <input checked="" type="checkbox"/> Wednesday <div>Active all day</div> <div>+</div> </div> <div> <input checked="" type="checkbox"/> Thursday <div>Active all day</div> <div>+</div> </div> <div> <input checked="" type="checkbox"/> Friday <div>Active all day</div> <div>+</div> </div> <div> <input checked="" type="checkbox"/> Saturday <div>Active all day</div> <div>+</div> </div> <div> <input checked="" type="checkbox"/> Sunday <div>Active all day</div> <div>+</div> </div> </div>

Assessing Network Health in the Statistics Pages

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.

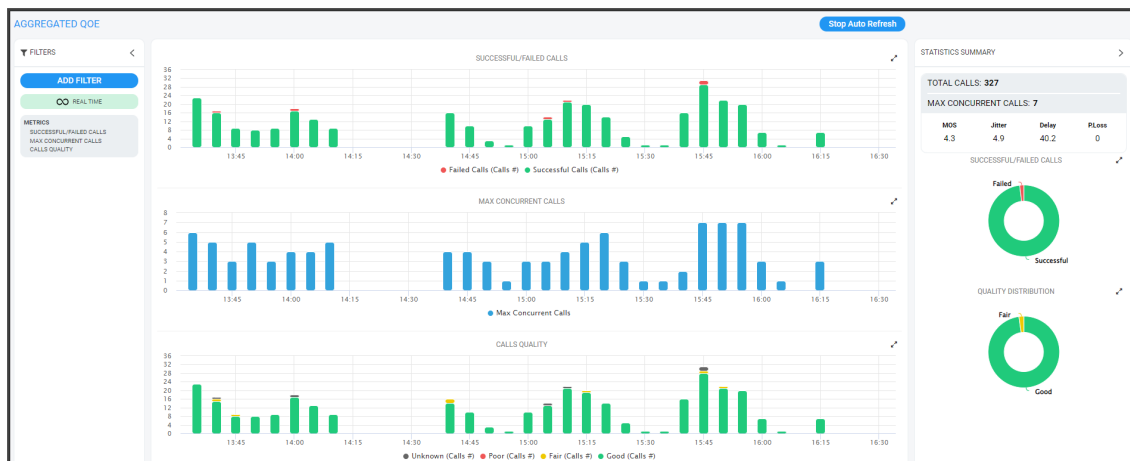
Viewing Statistics on Calls over Devices

Under the Statistics menu, the **Devices** tab enables 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:

1. Access the Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Aggregated QoE page (**Statistics > Devices**).

Figure 6-12: Devices Statistics



You can optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 231) and Topology (see [Filtering by 'Topology'](#) on page 243).

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 305)

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 231 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 6-13: Bar Charts

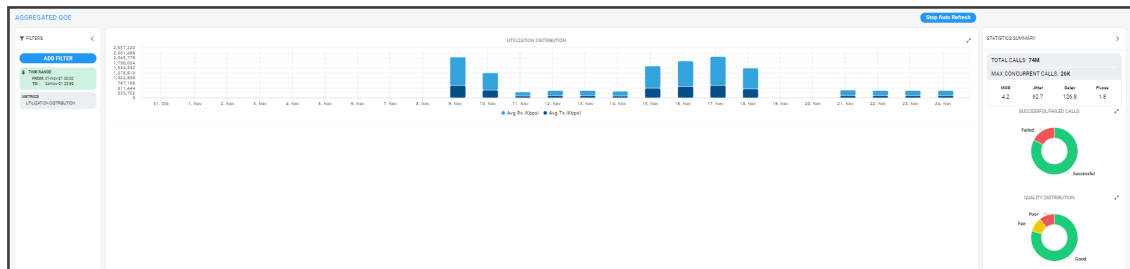


Compare charts. If, for example, you identify a correlation over time between 'Poor' voice quality and Jitter, then Jitter is the reason for the poor voice quality.

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:

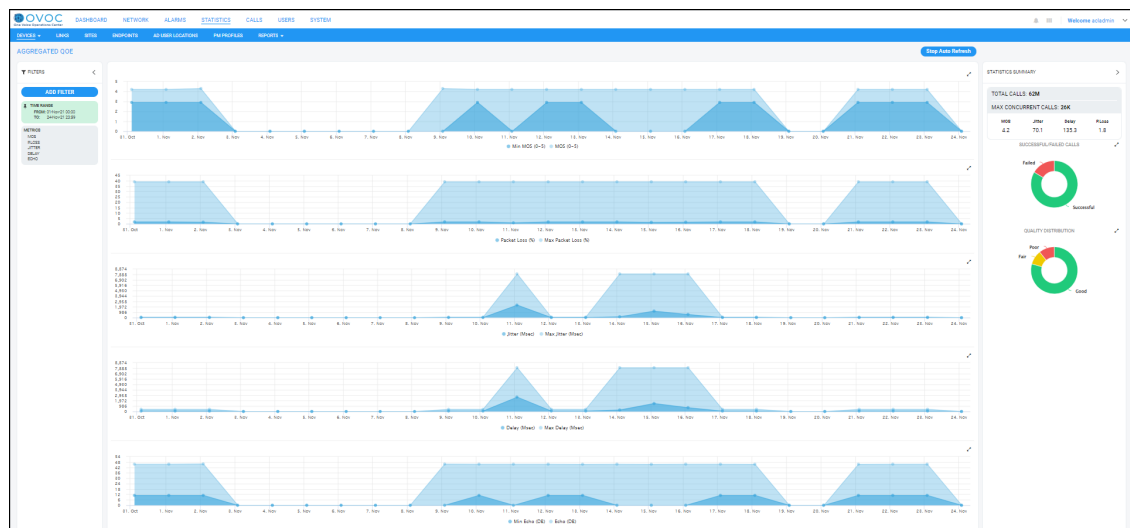
Figure 6-14: Utilization Distribution Bar Chart



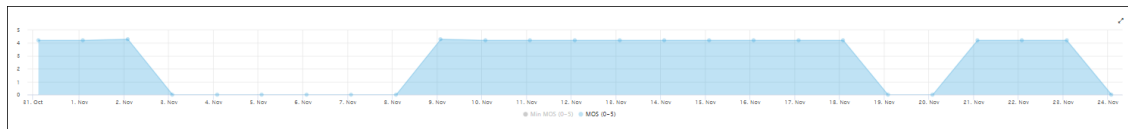
- Average Call Duration (ACD) chart shows distribution of ACD in the network over time. Point your mouse over a bar to determine average call duration in that time interval.
- MOS chart. Point your mouse over a bar to determine the average MOS scored in that time interval.
- Packet Loss chart. Point 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.

The figure below shows the Aggregated QoE page (**Statistics > Devices**) filtered to display five metrics charts: MOS, Packet Loss, Jitter, Delay and Echo.

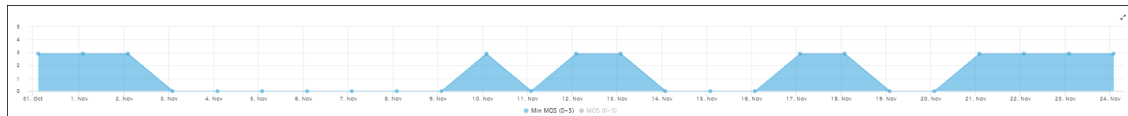
Figure 6-15: Aggregated QoE page Filtered to Display Charts for MOS, Packet Loss, Jitter, Delay and Echo



Under the MOS chart (for example), toggle between **Min MOS (0-5)** and **MOS (0-5)** as shown in the figures below; click **Min MOS (0-5)**.

Figure 6-16: Min MOS (0-5)

Click it again and then click **MOS (0-5)**.

Figure 6-17: MOS (0-5)

The feature enables you to easily compare the lowest MOS score that was scored in the time period, with the average MOS score that was scored in the time period. The same toggle feature applies to all bar charts besides the Packet Loss, Jitter, Delay and Echo charts shown here.

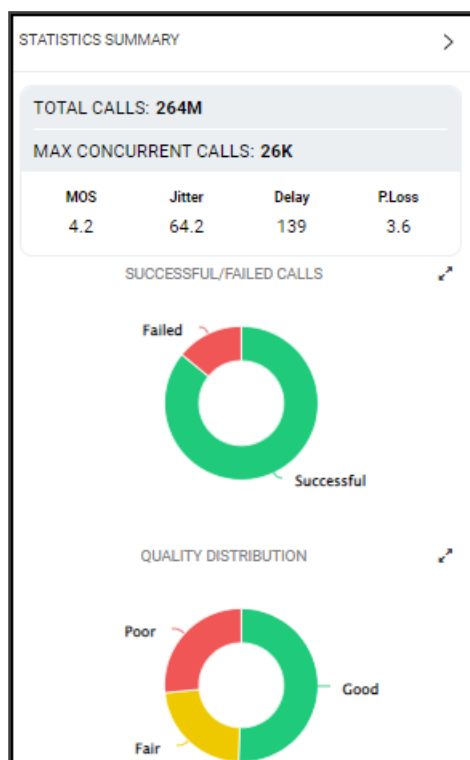


Values displayed in the charts are reported by devices for representation in OVOC. Sometimes, when reported values are higher than expected, for example, packet loss might be higher than 100%. In this case, contact AudioCodes Support for clarification.

Statistics Summary

On the right side of the Devices Statistics page, you can view the Statistics Summary pane.

Figure 6-18: 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 300). You can optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 231) and Topology (see [Filtering by 'Topology'](#) on page 243).

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 300. 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 231) and Topology (see [Filtering by 'Topology'](#) on page 243).

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 300). 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 231) and Topology (see [Filtering by 'Topology'](#) on page 243).

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 312.

➤ To set up PM using the *default PM template*:

1. Access the Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**) and make sure it displays a *default* Performance Monitoring (PM) template provided by AudioCodes.

3. 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. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. 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.
3. 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:**

1. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. 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

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. OVOC displays the default PM template in the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**).

Figure 6-19: Perf Monitoring

PERF MONITORING						Add Edit <small>Configuration</small> Refresh	
CONFIGURATION	DEFAULT	NAME	DESCRIPTION	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL	
<div>TEMPLATES</div> <ul style="list-style-type: none"> SNMP Connectivity HTTP Connectivity QoS Thresholds QoS Status & Alarms Perf Monitoring 	✓	PM Profile		38	✗	✗	

PERF MONITORING DETAILS	
DEFAULT	✓
NAME	PM Profile
PARAMETERS #	38
CREATE DATA FILE	✗
SEND EVENT PER INTERVAL	✗



- 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 6-20: PM Profiles

PM PROFILES							Add Edit Delete Refresh	
DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL		
✓	PM Profile	Factory PM Profile	T1	38	✗	✗		
✓	PM Profile	Factory PM Profile	T2	38	✗	✗		
✓	PM Profile	Factory PM Profile	mriyam	38	✗	✗		
✓	PM Profile		T4	38	✗	✗		
✓	PM Profile		leah	38	✗	✗		
✓	PM Profile		A	38	✓	✗		
✓	PM Profile		carrie22	38	✗	✗		
✓	PM Profile		carrieTenant	38	✗	✗		
✗	Test		T2	1279	✗	✗		
✓	PM Profile		Eran	38	✗	✗		
✓	PM Profile		a	38	✗	✗		

PERF MONITORING DETAILS

DEFAULT ✓
NAME PM Profile
TENANT T1
DESCRIPTION Factory PM Profile
PARAMETERS # 38
CREATE DATA FILE ✗
SEND EVENT PER INTERVAL ✗
MANUAL ATTACHMENTS 0
DEFAULT ATTACHMENTS 8

➤ **To add a PM template:**

1. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**) and click **Add**.

Figure 6-21: Performance Monitoring Template

PERFORMANCE MONITORING TEMPLATE

Name*

Description

☐ Default
☐ Create Data File
☐ Send Event Per Interval

☐ Parameters (0) All

☐ Name

MinMaxAvgVal

CPU (SW 7.4 & above) (0)
Gateway (0)
Gateway (SW 7.4 & above) (0)
IP Group (0)
IP Group (SW 7.4 & above) (0)
Media (SW 7.4 & above) (0)
Media Realm (SW 7.4 & above) (0)
Network (SW 7.4 & above) (0)
Partition (SW 7.4 & above) (0)
Port (SW 7.4 & above) (0)
SBC (0)

☐ Call Stats

Tel to IP Call Attempts
IP to Tel Call Attempts
Tel to IP Call Duration [sec]
IP to Tel Call Duration [sec]
Tel to IP Established Calls
IP to Tel Established Calls
Tel to IP Fax Call Attempts
IP to Tel Fax Call Attempts
Tel to IP Successful Fax Calls
IP to Tel Successful Fax Calls
Tel to IP Calls Terminated due to Forward
IP to Tel Calls Terminated due to Forward

☐
☐
☐
☐
☐
☐
☐
☐
☐
☐
☐
☐

☐ Call Failures

Tel to IP Failed Calls due to No Matched Capabilities
IP to Tel Failed Calls due to No Matched

☐
☐

Close

OK


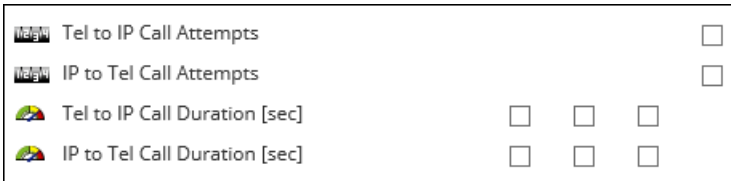
- Configure the PM template using the table below as reference.

Table 6-7: PM Template Parameter Descriptions

Parameter	Description
Name	Enter a name for the template. Choose an intuitive name to facilitate an operator-friendly network management experience later.
Description	Enter a free-text description of the template to help facilitate an operator-friendly network management experience. Example: "This template is for all tenants of Meteor Bank". This can help orient operators when managing complex networks.
Default	The PM Templates page <i>always displays one default</i> PM template. If you select this 'Default' option, the earlier default PM template will lose its default configuration and you'll be able to delete it from the Perf Monitoring page. There will always be a default PM template in the page, be it the AudioCodes-provided default PM template or a newly added operator-configured default PM tem-

- 309 -

Parameter	Description
	plate. The PM template configured as the default cannot be deleted. Every time you add a tenant, all PM templates listed in the Perf Monitoring page are <i>duplicated as PM profiles</i> in the PM Profiles page (Statistics > PM Monitoring) and all PM profiles listed in the PM Profiles page are <i>automatically allocated to that newly added tenant</i> .
Create Data File	OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. Select this option to save the PM metrics (data) <i>as a file</i> in operator-friendly JSON format. All PM information resulting from the poll is conveniently located in this file. An event is sent when the file is created (see the next parameter).
Send Event per Interval	Select this option for an event to be sent every 15 minutes, indicating that all parameters per device were successfully polled. If 10 devices were selected for polling, the event is sent indicating that all parameters on all 10 devices were successfully polled.
Parameters (0)	<p>Indicates how many PM metrics (check boxes) you selected to be polled. (0) indicates that none have been selected (yet). When you select parameters (metrics), the indication changes accordingly. The following tabs are displayed under 'Parameters':</p> <ul style="list-style-type: none"> ■ 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

Parameter	Description
	<p>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.</p> <p>■ SRD (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge ASR.</p> <p>See the <i>SNMP Reference Guide</i> for detailed information about each PM parameter.</p> <div>  <p>For SBC devices, you can also configure Performance Monitoring parameters for counting the number of call failures for specific SIP responses. These are configured in the SBC device's Web interface's User Defined Failure PM table. For more information, see the SBC device's <i>User's Manual</i>.</p> </div>
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include <i>most but not all</i> PM metrics in your template, select 'Name' (all check boxes will be selected) and then clear those to exclude.
Min Max Avg Value [Minimum value, Maximum value and Average value (Avg)],	<p>In the Call Stats pane shown in the next figure, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are <i>counters</i>. A single value (Val) is displayed after they're measured, i.e., # of counted call attempts.</p> <div>  </div> <p>In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are <i>gauges</i>. If all three adjacent check boxes are selected, the # of calls of minimum duration, the # of calls of maximum duration and the # of average-length calls will be monitored.</p>



Thresholds are configured at the SBC level in the device's Web interface, in the Open Device page. See the device's *User's Manual* for more information. Thresholds can alternatively be configured in an ini file and loaded to the device in 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 OVOC.

- 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 6-22: Performance Monitoring Templates

DEFAULT	NAME	DESCRIPTION	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL
<input checked="" type="checkbox"/>	PM Profile	Factory PM Profile	33	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

➤ **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. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).

2. Open the PM Profiles page (Statistics > PM Profiles).

Figure 6-23: PM Profiles

PM PROFILES							Add Edit Delete Refresh	
DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL		
✓	PM Profile	Factory PM Profile	T1	38	✗	✗		
✓	PM Profile	Factory PM Profile	T2	38	✗	✗		
✓	PM Profile	Factory PM Profile	mayam	38	✗	✗		
✓	PM Profile		T4	38	✗	✗		
✓	PM Profile		leah	38	✗	✗		
✓	PM Profile		A	38	✓	✗		
✓	PM Profile		came022	38	✗	✗		
✓	PM Profile		cameTenant	38	✗	✗		
✗	Test		T2	1279	✗	✗		
✓	PM Profile		Eran	38	✗	✗		
✓	PM Profile		a	38	✗	✗		

PERF MONITORING DETAILS

- DEFAULT: ✓
- NAME: PM Profile
- TENANT: T1
- DESCRIPTION: Factory PM Profile
- PARAMETERS #: 38
- CREATE DATA FILE: ✗
- SEND EVENT PER INTERVAL: ✗
- MANUAL ATTACHMENTS: 0
- DEFAULT ATTACHMENTS: 8

3. Click Add.

Figure 6-24: PM Profile

PERFORMANCE MONITORING PROFILE

Name*
Description

☐ Default
☐ Create Data File
☐ Send Event Per Interval

Tenant*
eli7
ATTACHMENTS
Select Devices
Manual 0

☐ Parameters (0) All

☐ Name Min Max Avg Val

☐ Call Stats

- Tel to IP Call Attempts
- IP to Tel Call Attempts
- Tel to IP Call Duration [sec]
- IP to Tel Call Duration [sec]
- Tel to IP Established Calls
- IP to Tel Established Calls
- Tel to IP Fax Call Attempts
- IP to Tel Fax Call Attempts
- Tel to IP Successful Fax Calls
- IP to Tel Successful Fax Calls
- Tel to IP Calls Terminated due to Forward
- IP to Tel Calls Terminated due to Forward

☐ Call Failures

Filter
Filters are not available for a singular topic

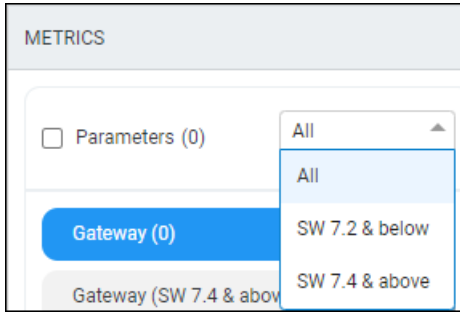
Close OK

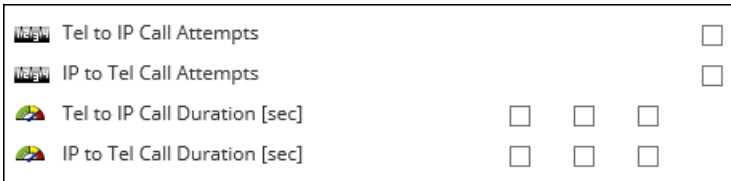
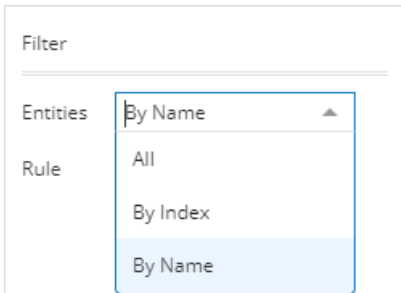
4. Configure a profile using the following table as reference.

Table 6-8: 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.

Parameter	Description
Default	The PM Profiles page <i>always displays one default</i> PM profile. If you select this 'Default' option, the previously configured default PM profile - be it the AudioCodes-provided default or a new operator-configured default - will lose its default configuration and you'll be able to delete it from the page. Every time you add a new tenant, the default profile together with all other profiles (if you configured other profiles) are automatically allocated to that tenant.
Create Data File	OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. Select the option to save the PM metrics (data) as a file in operator-friendly JSON format. All PM information resulting from the poll is conveniently located in this file. An event is sent when the file is created (see the next parameter).
Send Event per Interval	Select this option for an event to be sent every 15 minutes, indicating that all parameters per device were successfully polled. If 10 devices were selected for polling, the event is sent indicating that all parameters on all 10 devices were successfully polled.
Tenant	Select from the drop-down list the tenant to allocate this PM profile to.
Attachments	The Devices link gives operators the option to <i>manually select a specific device</i> to which to attach this PM profile.
Parameters (0)	<p>Indicates how many PM metrics (check boxes) you selected to be polled. (0) indicates that none have been selected (yet). When you select parameters (metrics), the indication changes accordingly. The following parameter categories are displayed:</p> <ul style="list-style-type: none"> ■ 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

Parameter	Description
	<p>counter Incoming Discarded Pkts.</p> <ul style="list-style-type: none"> ■ 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 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. <p>Note you can configure OVOC to sample by either:</p> <ul style="list-style-type: none"> ■ 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) <p>To configure this, click the 'Parameters (0)' field drop-down and select:</p> 
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include <i>most but not all</i> PM metrics in your profile, select 'Name' (all check boxes will be selected) and then clear those to exclude.
Min Max Av Value	In the Call Stats pane shown in the figure below, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are <i>counters</i> . A single value (Val) is displayed after they're measured, i.e., the #

Parameter	Description
	<p>of counted call attempts.</p>  <p>In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are <i>gauges</i>. If all three adjacent check boxes are selected, the # of calls of minimum duration, the # of calls of maximum duration and the # of average-length calls will be monitored.</p>
Filter	<p>Only applies to tabs 'IP Group', 'Trunk Group' and 'SRD'. Enables filtering for specific entities per index or per name. 'Trunk Group' can be filtered only by index.</p>  <p>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.</p>



Thresholds are configured at the SBC level in the device's Web interface, in the Open Device page. See the device's *User's Manual* for more information. Thresholds can alternatively be configured in an ini file and loaded to the device in 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 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 6-25: PM Profiles

DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL		>> PERF MONITORING DETAILS
✖	PM Profile	Factory PM Profile	MeteorBank	41	✖	✖		DEFAULT <input checked="" type="checkbox"/> NAME MeteorBank DESCRIPTION PM profile for the SBC located at Meteor Bank, Skyscape City TENANT MeteorBank PARAMETERS # 31 CREATE DATA FILE ✖ SEND EVENT PER INTERVAL ✖ MANUAL ATTACHMENTS 0 DEFAULT ATTACHMENTS 1
✔	MeteorBank	PM profile for the SBC located at Meteor Bank, Skyscape City	MeteorBank	31	✖	✖		

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.

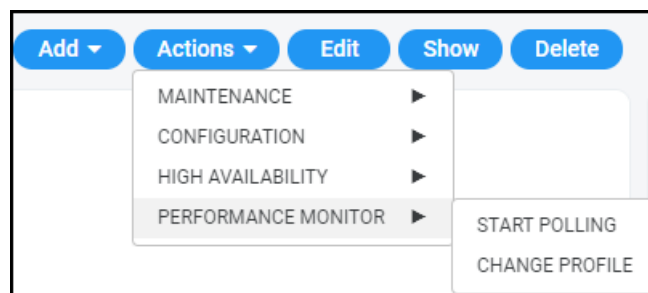
Starting and Stopping PM Polling

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. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Network Topology page (**Network > Topology**) or the **Device Management** page (**Network > Devices > Manage**).
3. 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.

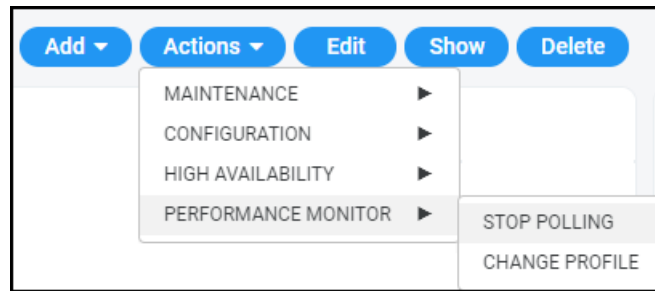
Figure 6-26: Start Polling



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.

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

Figure 6-27: Stop Polling



5. View the results of the poll.
 - See [Viewing PM Data Resulting from Polling](#) below

Viewing PM Data Resulting from Polling

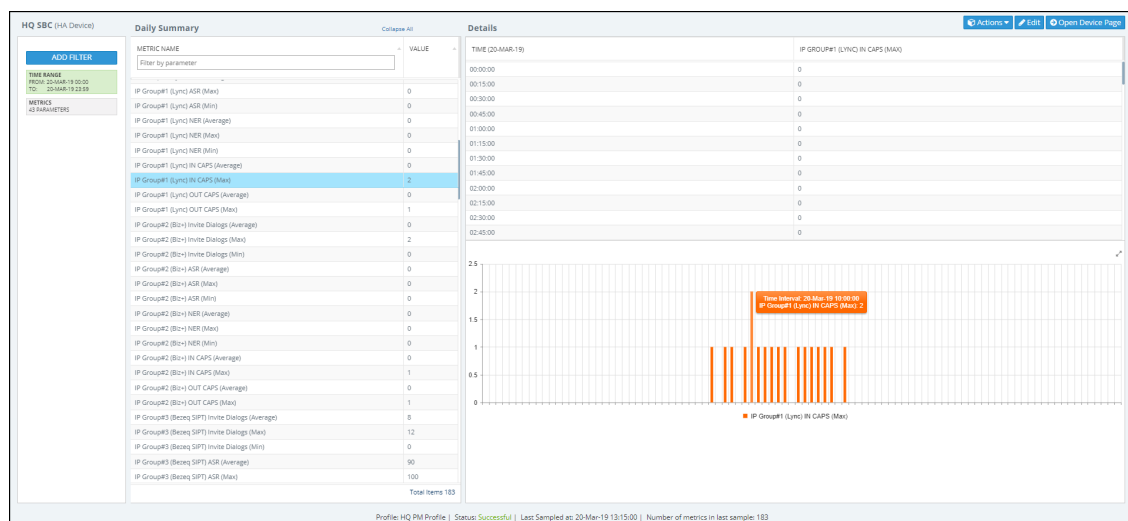
After polling a device (see [Starting and Stopping PM Polling](#) on the previous page), operators can view PM data resulting from polling in:

- 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. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Device Management page (**Network > Devices > Manage**), select the device whose PM data you want to view, and then click the **Show** button.
3. In the device's dynamic tab's Summary page, click the **Statistics** tab.

Figure 6-28: 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 6-29: Filter by parameter

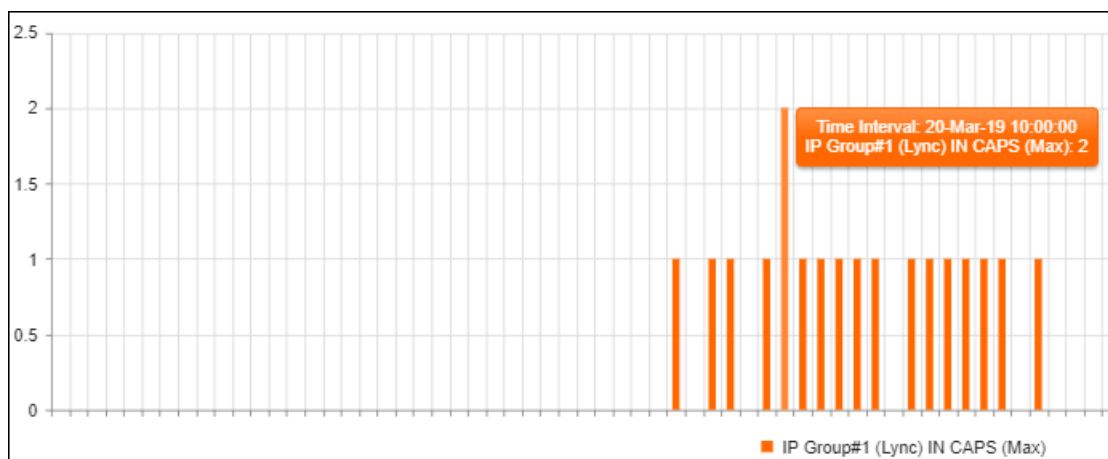
METRIC NAME	VALUE
tel to ip	
▼ Gateway: 20-Mar-19 (5 items)	
Tel to IP Call Attempts (Value)	0
Tel to IP Established Calls (Value)	0
Tel to IP Failed Calls due to No Matched Capabilities (Value)	0
Tel to IP Calls Terminated due to a Busy Line (Value)	0
Tel to IP Failed Calls due to Other Reasons (Value)	0

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



Multiple metrics can be selected using the Ctrl key on the keyboard. Operators can select multiple metrics for tabular and graphical comparisons of the metrics.

- Details [right side of page]:
 - after a metric is selected in the Daily Summary list, a table and a bar chart display the distribution details of that metric's values over each 15 minute interval in the Time Range (the default Time Range is 24 hours, from 00:00 to 23:59)
 - pointing the cursor over a bar in the chart opens a tool tip summarizing that bar; the tool tip in the figure indicates that the maximum incoming calls per second (CAPS) was measured on IP Group#1 (Lync) in the interval beginning 10:00 on March 20, 2019 to be 2



■ Status bar (lowermost in page):

- displays the name of the PM profile assigned to the device, the Status of the last polling interval (Successful), the date and time at which the device was last polled, and the number of metrics (parameters) polled in the last interval



















➤ To view PM data in a data file:

- Make sure the 'Create Data File' option in the PM Profile is selected. The OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. If this option is selected, the PM metrics (data) are saved as a file in operator-friendly XML format. All PM information resulting from the poll will conveniently be located in this file. An event is sent when the file is created.

➤ To access the data file:













1. In your browser, enter URL **http://172.17.140.84/nbif** and in the prompt, enter user name **nbif** and password **pass_1234**.

Figure 6-30: 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 6-31: 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 6-32: Data File Displayed in XML Editor

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
  <deviceInfo>
    <devicenName>10.3.181.71</devicenName>
    <ip>10.3.181.71</ip>
    <productType>92</productType>
    <sn>5200544</sn>
    <swVersion>7.20A.251.155</swVersion>
    <tenant>
      <tenantName>Zipora</tenantName>
      <region>
        <regionName>Region1</regionName>
      </region>
    </tenant>
  </deviceInfo>
  <timeInterval>
    <from>2019-01-10T06:15:00.000+0000</from>
    <to>2019-01-10T06:30:00.000+0000</to>
  </timeInterval>
  <profile>
    <dictionaryId>1</dictionaryId>
    <id>21</id>
    <name>PM Profile</name>
  </profile>
  <data>
    <topics>
      <topic>
        <parameters>
          <parameter>
            <paramName>
acPMSIPSBAttemptedCallsVal</paramName>
            <parameterData>
              <element>
                <value>0</value>
              </element>
            </parameterData>
          </parameter>
          <parameter>
            <paramName>acPMSBCAsrAverage</paramName>
            <parameterData>
              <element>
                <value>0</value>
              </element>
            </parameterData>
          </parameter>
        </parameters>
        <topicName>SBC</topicName>
      </topic>
    </topics>
  </data>

```

- 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

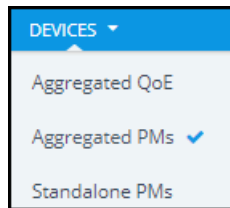
➤ To view aggregated PM metrics from the OVOC's Statistics page:



- **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.

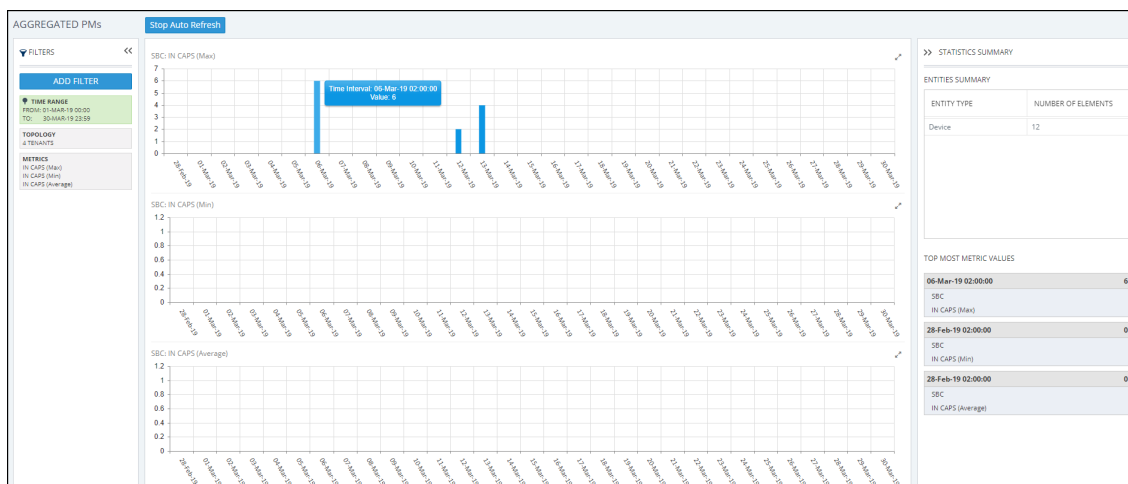
1. Open the Statistics page and from the **Devices** drop-down, select **Aggregated PMs**.

Figure 6-33: 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 312 as reference.
3. View the aggregated PMs then displayed.

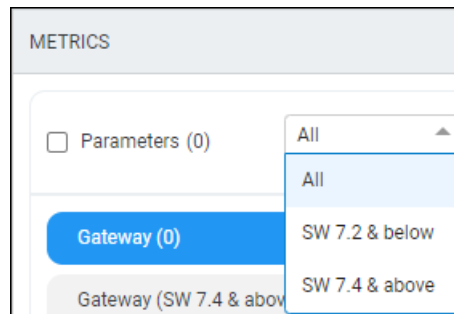
Figure 6-34: Aggregated PMs



[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)

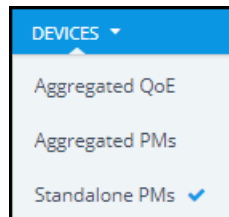
- 'Entities Summary' displays the entity type | types polled and how many of each type was polled
- Top Most Metric Values indicates the interval in which the highest value was measured for a metric, for example, on 06-Mar-2019 the metric 'IN CAPS (Max)', i.e., the maximum aggregated incoming calls per 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 6-35: Selecting 'Standalone PMs'

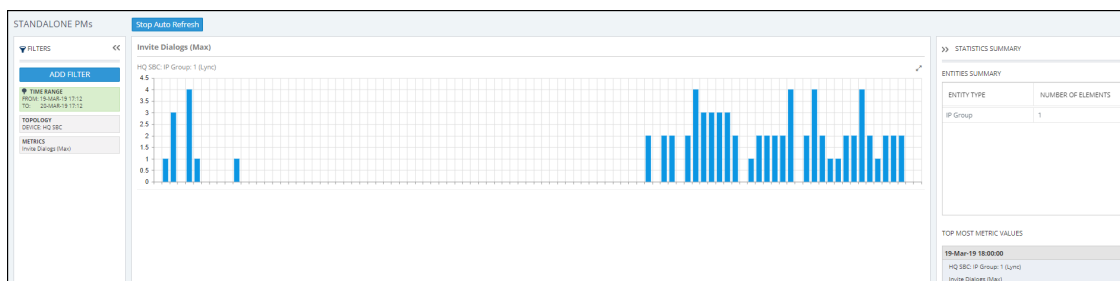
2. In the Standalone PMs page that opens, you're prompted 'Missing Topology and Metrics Filter'. Click **Add Filter**.
 - a. Change the 'Time Range' or leave it unchanged at the default (the preceding 24 hours, i.e., 00:00 to 23:59). Click **Apply**.
 - b. Click **Topology** and select a tenant or multiple 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 6-36: 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 'Entities' drop-down, select if necessary (and if available) the specific IP Group (for example) to poll. In this case, select its index. You can then select another. Optionally, select **All**.
3. View the standalone PMs metrics then displayed.

Figure 6-37: 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

Displaying Analytics

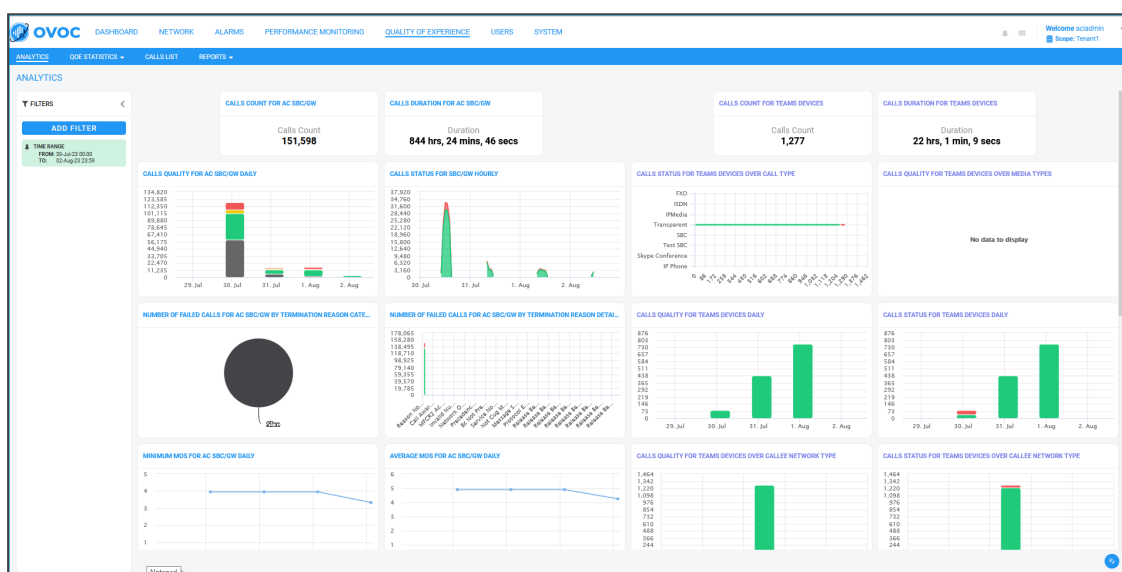
The Analytics page allows operators to view their enterprise IP network telephony analytics.




- Analytics data for the last seven days is available.
- The feature is only available when:
 - ✓ It's included in the OVOC license.
 - ✓ It's enabled in the EMS Server Manager under Main Menu > Application Maintenance > Analytics API (see the *IOM Manual* for more information).
 - ✓ The 'Analytics Status' option is selected in the OVOC's Tenant Details screen under the **License** tab as shown [here](#).

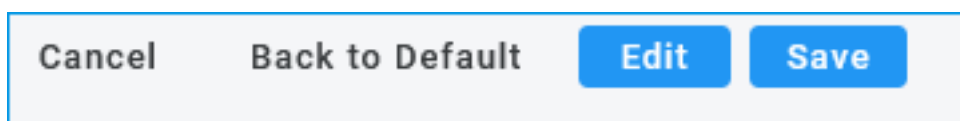
➤ To display analytics:

1. Open the Analytics page (Quality of Experience > Analytics).

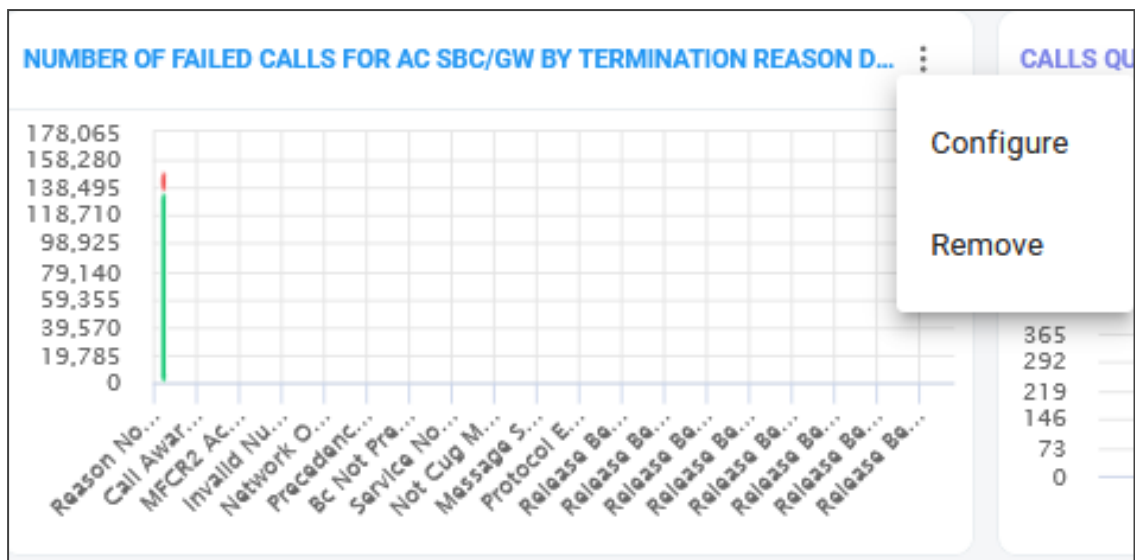


2. Optionally, customize the page:

- a. In the lowermost right corner of the page, click the  icon; the charts in the page display vertical ellipsis menus; the following is also displayed:



- b. Click the vertical ellipsis menu of a chart.



- c. Select **Configure**. (Alternatively, select **Remove** to remove the chart from the page).

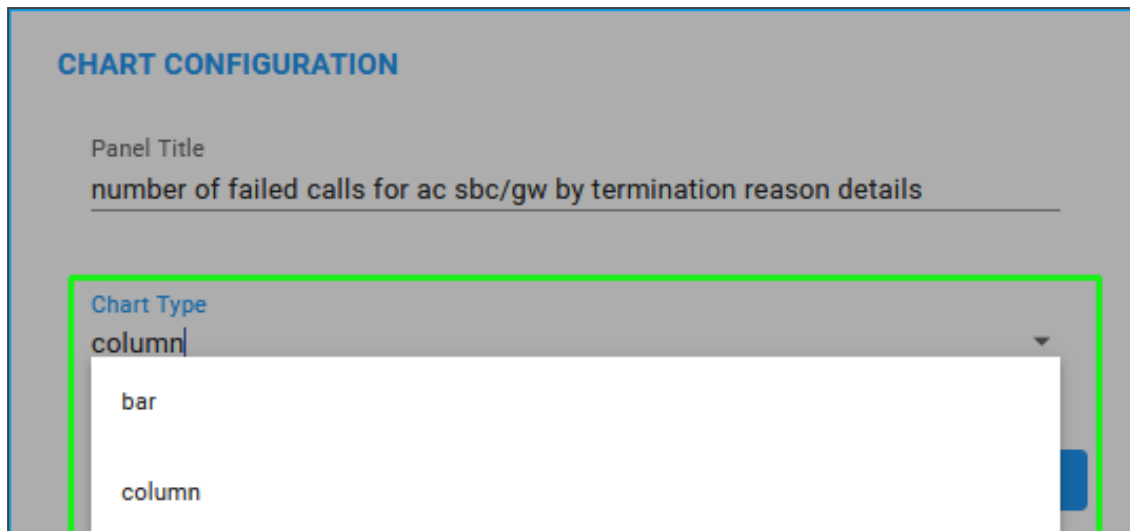
CHART CONFIGURATION

Panel Title

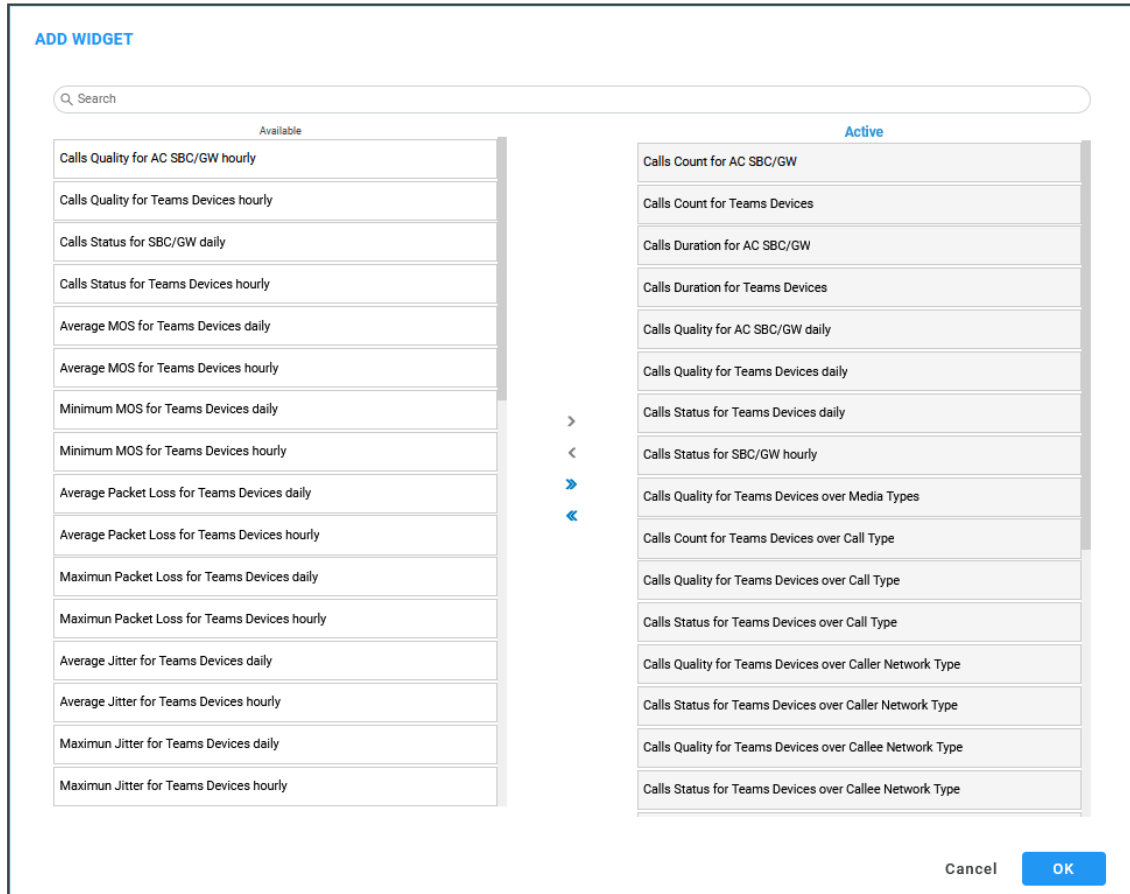
Chart Type

Cancel **OK**

- d. Configure | reconfigure the Panel Title and the Chart Type as required. See the table below for supported chart types.



- e. Click **OK**.
- f. Optionally, resize a chart by dragging out its corner.
- g. Optionally, relocate a chart on the page by dragging it from its title and then dropping it in the preferred location.
- h. Click the **Edit** option and then select the analytics charts from the 'Available' charts to activate using the > key for a single chart and >> for multiple charts. To deactivate a chart, select the chart from the 'Active' charts and then click <. To deactivate multiple charts, click <<.



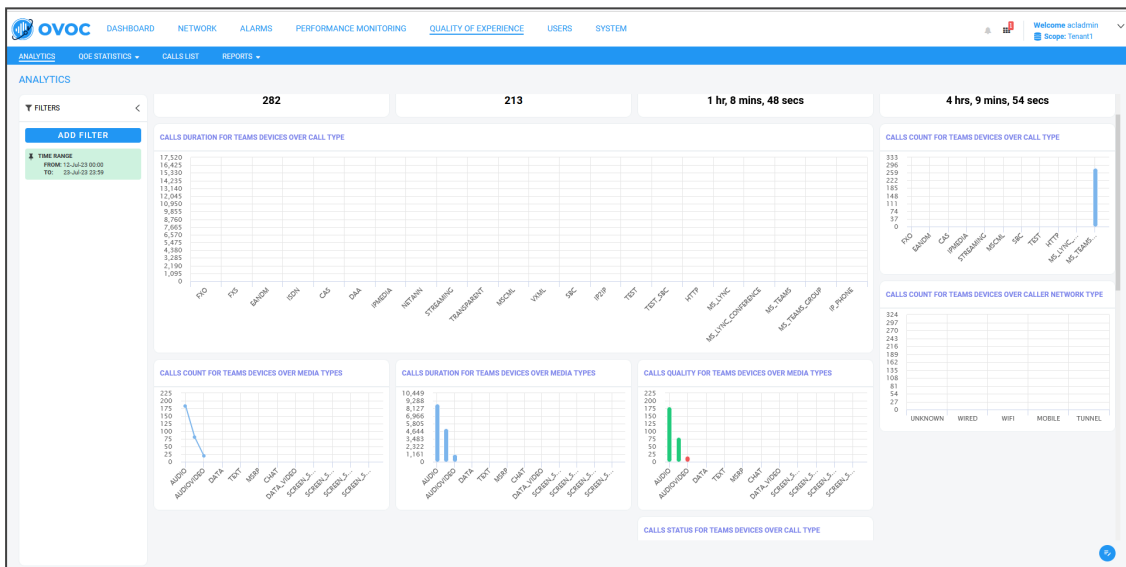
3. Use the table as reference to the preceding parameters.

Data Category	Supported Graph Types	Description
SBC		
Calls Count for AC SBC/GW	Absolute Number	The aggregated number of calls connected through AudioCodes SBC devices.
Calls Duration for AC SBC/GW	Absolute Number	The aggregated call time for calls connected through AudioCodes SBC devices.
Calls Quality for AC SBC/GW Daily	Bar, Column, Line, Area	The aggregated Daily Calls Quality breakdown for calls connected through AudioCodes SBC devices.
Calls Status for SBC/GW Hourly	Bar, Column, Line, Area	The aggregated Hourly Calls Status breakdown for calls connected through AudioCodes SBC devices.
Number of Failed Calls for AC SBC/GW By Termination Reason Category	Bar, Column	The aggregated number of Failed Calls connected through AudioCodes SBC devices By Termination Reason Category.
Number of Failed Calls for AC SBC/GW By Termination Reason Details	Bar, Column	The aggregated number of failed calls connected through AudioCodes SBC devices by Termination Reason Details.
Minimum MOS for AC SBC/GW Daily	Bar, Column, Line, Area	The Minimum MOS value reported daily for calls connected through AudioCodes SBC devices.
Maximum Packet Loss For AC SBC/GW Daily	Bar, Column, Line, Area	The Maximum Packet Loss value reported daily for calls connected through AudioCodes SBC devices.
Maximum Jitter For AC SBC/GW Daily	Bar, Column, Line, Area	The Maximum Jitter value reported daily for calls connected through AudioCodes SBC devices.
Maximum Delay For AC SBC/GW Daily	Bar, Column, Line, Area	The Maximum Delay value reported daily for calls connected through AudioCodes SBC devices.
Average MOS For AC SBC/GW Daily	Bar, Column,	The Average MOS value reported daily for calls connected through AudioCodes SBC devices.

Data Category	Supported Graph Types	Description
	Line, Area	
Average Packet Loss For AC SBC/GW Daily	Bar, Column, Line, Area	The Average Packet Loss value reported daily for calls connected through AudioCodes SBC devices.
Average Jitter For AC SBC/GW Daily	Bar, Column, Line, Area	The Average Jitter value reported daily for calls connected through AudioCodes SBC devices.
Teams		
Calls Count For Teams Devices	Absolute Number	The aggregated number of calls connected through Teams devices.
Calls Duration For Teams Devices	Absolute Number	The aggregated call time for calls connected through Teams devices.
Calls Status For Teams Devices Over Call Type	Bar, Column	The aggregated status breakdown of Teams calls according to Call type: FXO, ISDN; IPMedia; Transparent; SBC; Skype Conference; IP Phone
Calls Quality For Teams Devices Over Media Types	Bar, Column	The aggregated status breakdown of Teams calls according to Media type.
Calls Quality For Teams Devices Daily	Bar, Column, Line, Area	The Daily Calls Quality breakdown for calls connected through Teams devices.
Calls Status For Teams Devices Daily	Bar, Column, Line, Area	The Daily Calls Status breakdown for calls connected through Teams devices.
Calls Quality For Teams Devices Over Callee Network Type	Bar, Column	The Calls Quality breakdown for calls connected through Teams devices according to network interface type : WiFi; Wired; Mobile and Tunnel
Calls Status For Teams Devices Over Callee Network Type	Bar, Column	The Call Status breakdown for calls connected through Teams devices according to network interface type : WiFi; Wired; Mobile and Tunnel

Data Category	Supported Graph Types	Description
Calls Quality For Teams Devices Over Call Type	Bar, Column	The Call Quality breakdown for calls connected through Teams devices according to Calls type: FXO, EANDM, CAS, IPMedia, Streaming, MSCML, SBC, Test, HTTP, Skype Conference and Teams Group Call
Calls Count For Teams Devices Over Call Type	Bar, Column	The Number of Calls breakdown according to Calls type: FXO, EANDM, CAS, IPMedia, Streaming, MSCML, SBC, Test, HTTP, Skype Conference and Teams Group Call.

4. Click **OK** and view your configuration.



5. Click **Save**.

7 Managing your Network

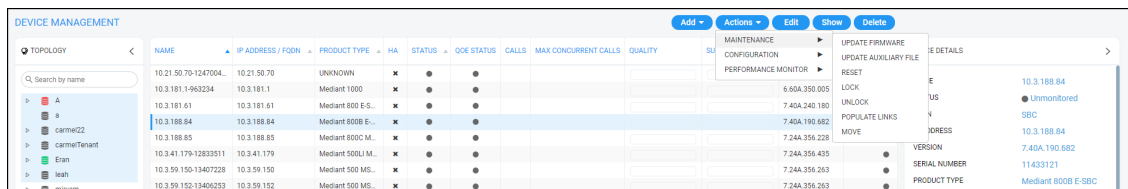
OVOC enables ITSPs and enterprises to independently manage their telephony networks.

Performing Management Actions

OVOC lets operators perform multiple 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.



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 338)
- ◆ Restart (see [Restarting a Device](#) on page 341)
- ◆ Lock or Unlock (see [Locking or Unlocking a Device](#) on page 342)
- ◆ Populate Links (see [Populating Links](#) on page 343)
- ◆ Move (see [Moving a Device](#) on page 345)

- **Configuration**

- ◆ Backup (see [Backing Up](#) on page 345)
- ◆ Restore Last Backup (restore a device's configuration) (see [Restoring the Last Backup](#) on page 346)
- ◆ Restore Default Configuration (see [Setting Configuration Factory Defaults](#) on page 348)

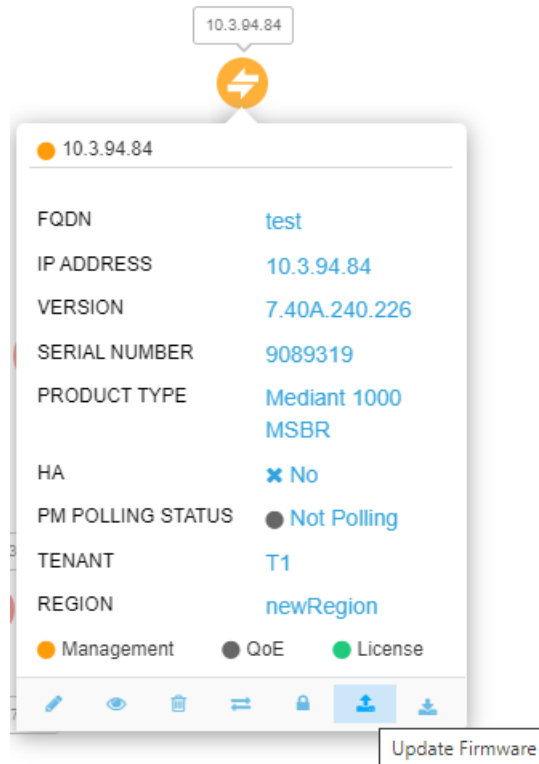
- ◆ Save Configuration to Flash (see [Saving a Device's Configuration File to Flash Memory](#) on page 348)
 - ◆ Save Current Configuration to File (see [Saving a Device's Configuration File to the PC](#) on page 348)
 - **Performance Monitor**
 - ◆ Start Polling (see [Starting and Stopping PM Polling](#) on page 317)
 - ◆ Change Profile (see [Changing Profile](#) on page 350)
 - **High Availability**
 - ◆ Reset Redundant (see [Resetting Redundant](#) on page 349)
 - ◆ Switchover (see [Performing Switchover](#) on page 350)
4. Use also the following dedicated buttons to perform management actions:
- **Show** device information (see [Showing Device Information](#) on page 352)
 - **Show** link information (see [Showing Link Information](#) on page 355)
 - **Show** user information (see [Showing User Information](#) on page 356)
 - **Edit** a device (see [Editing a Device](#) on page 358)
 - **Delete** a device (see [Deleting a Device](#) on page 358)

Updating Firmware

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 and locate in the popup the **Update Firmware** icon.

Figure 7-1: Update Firmware

2. Click the **Update Firmware** icon.

Figure 7-2: Update Firmware

UPDATE FIRMWARE

TYPE ▲	SW VE... ▲	NAME ▲	PROT... ▲	OWNER ▲
CMP	7.20A.25...	MP500_E...	SIP	System
CMP	7.20A.25...	MP500_E...	SIP	System
CMP	7.20A.25...	MP500_E...	SIP	System

1 - 3 of 3 |< < 1 ▾ > >|

Close Update

3. Select the firmware file you require and click **Update**.

Updating Firmware on Multiple Devices

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**.

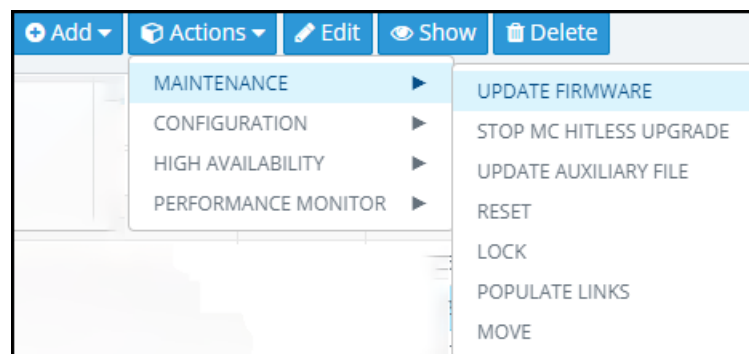
Updating Firmware on a Component in a Media Cluster

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

UPDATE FIRMWARE

☒ Cluster Manager ☐ Cluster Manager MTs

TYPE ▲	SW VER... ▲	NAME ▲	PROTOC... ▲	OWNER ▲
CMP	7.30A.001....	HostedTP_...	SIP	System
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.20A.256....	HostedTP_...	SIP	System
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111

◀ ◁ 1 ▷ ▶ Items 1-7 items of 7

Update Close

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



- **Cluster Manager** is AudioCodes's 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

UPDATE FIRMWARE

☐ Cluster Manager
 ☒ Cluster Manager MTs

TYPE ▲	SW VER... ▲	NAME ▲	PROTOC... ▲	OWNER ▲
CMP	7.30A.001....	HostedTP_...	SIP	System
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.20A.256....	HostedTP_...	SIP	System
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111
CMP	7.30A.001....	HostedTP_...	SIP	Tenant: a_66111

« < 1 > »
 Items 1-7 items of 7

Hitless ☒

Graceful Timeout (seconds)



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.

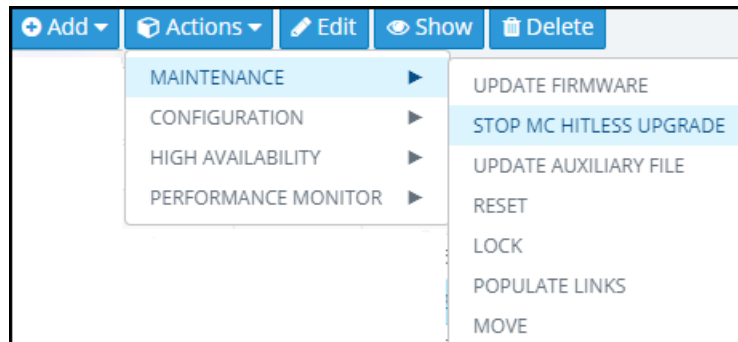
➤ **To stop the upgrade:**



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

TASKS					
TASKS					
<div> <div> <div>STOP MC UPGRADE</div> <div>1 entry admin</div> <div>100%</div> </div> </div>					
TASK DETAIL: STOP MC UPGRADE					
Stop MC Upgrade					
STATUS	UNIT NAME	UNIT TYPE	TASK TIME	STATUS DESCRIPTION	
●	10.4.212.182	Device	05-Jul-20 15:25:57	Action completed - Action completed - Stop M...	

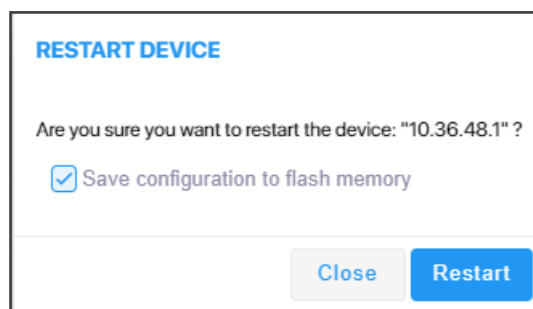
For more information about the Tasks page, see [Tasks tab](#) on page 130

Restarting a Device

For certain settings to take effect a device restart is required. Restarting a device may also be necessary for maintenance purposes.

➤ **To restart a device:**

1. Open the Device Management page (**Network > Devices > Manage**).
2. Select the device, click **Actions** and from the drop-down select **Restart** under the 'Maintenance' menu.



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 restarting.
 - If you do not select the option, the device restarts without saving the current configuration to flash and all configuration performed after the last configuration save will be discarded (lost) after restarting.
4. Click **Restart**.

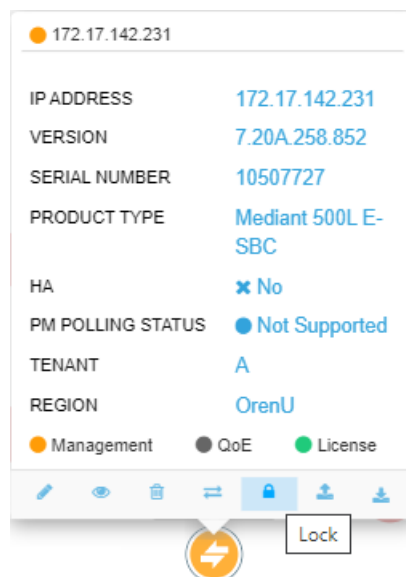
Locking or Unlocking a Device

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.

Figure 7-8: Lock



2. Click the **Lock** icon.

Figure 7-9: Lock Device

LOCK DEVICE

Are you sure you want to lock the device: "172.17.142.231" ?

☒ Immediate Lock

☐ Graceful Lock

☐ Graceful Lock (time)

Close Lock

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 **Lock**; a confirmation prompt is displayed.

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 179] 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.

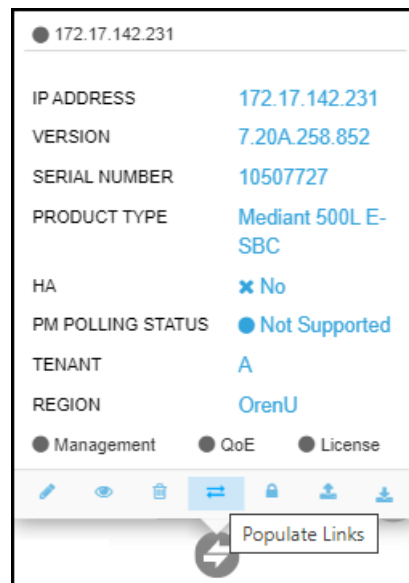
Example:

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:**

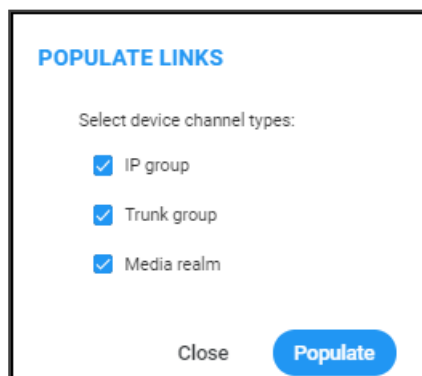
1. In the Network Topology page, position your cursor over the device.

Figure 7-10: Position cursor over device in Network Topology page



2. Click the **Populate Links** icon. [Alternatively, select the device in the Network Topology page and then from the **Actions** menu select **Maintenance > Populate Links**].

Figure 7-11: Populate Links



3. If necessary, clear an SNMP table option and then click **Populate**; 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, select the device and then from the **Actions** menu, select **Maintenance > Move**.

Figure 7-12: Move Device



MOVE DEVICE

Tenant
A

Region*
OrenU

Close Move

2. From the 'Tenant' drop-down, select from the list of tenants the tenant to move the device to (see [Adding a Tenant](#) on page 133 for information on how to add a tenant).
3. From the 'Region' drop-down, select from the list of regions the region to move the device to (see [Adding a Region](#) on page 151 for information on how to add a region).
4. Click **Move**.



If you move a device between tenants, some of its configuration might be changed, for example:

- its links will be deleted
- its profiles and alarm rules will be changed
- SBC license might be affected

Backing Up

You can back up a device's configuration file to the OVOC server. See also [Manually Backing up a Device's Configuration](#) on page 176 for information about how to view a device's backed-up configuration files in the Backup Manager page, and how to back up a device's configuration file from that page.

➤ **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 OVOC server.

2. Click **Actions** and from the drop-down choose the **Configuration** option.

3. Select the **Backup** option.

4. In the Confirmation prompt, click **OK**; the latest file is uploaded to the OVOC server from the device.



If the device selected is:

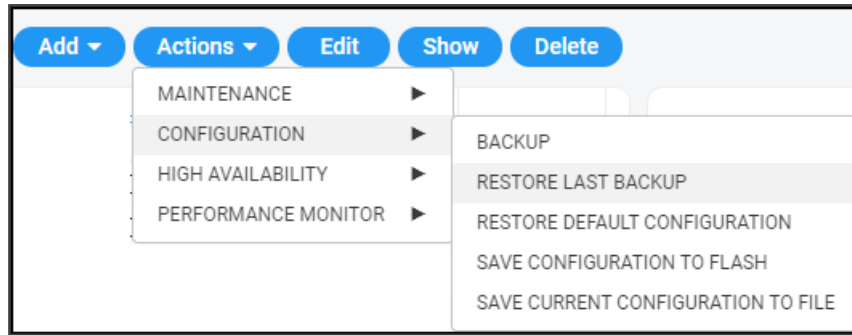
- AudioCodes SBC / Gateway whose version is 7.4.200 and later, the latest zip (Configuration Package) file is uploaded.
- MSBR, the latest cli file is uploaded.
- MP-202 or MP-204, the latest conf file is uploaded.
- VoiceAI Connect, the latest zip file is uploaded.
- Stack Manager, the latest JSON file is uploaded.
- 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 and in the confirmation prompt, click **Restore**; 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.

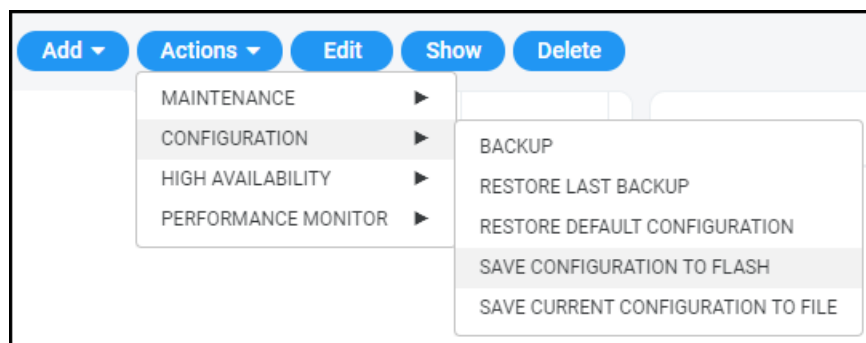
Saving a Device's Configuration File to Flash Memory

You should save (burn) the current configuration of a device to the device's flash memory (non-volatile) before performing a Reset action (see [Restarting a Device](#) on page 341) 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** and then in the confirmation prompt click **OK**.



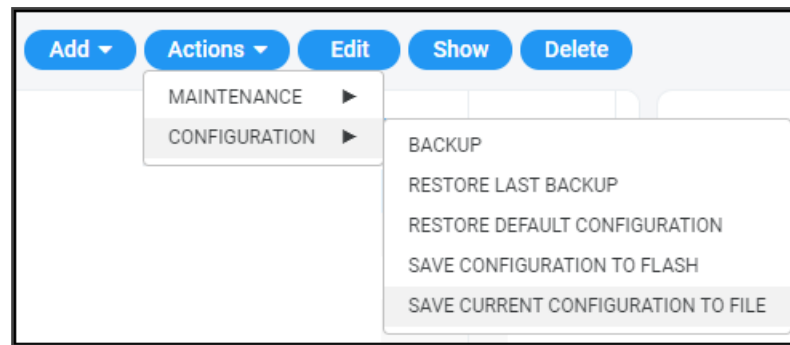
Saving configuration to flash may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see [Locking or Unlocking a Device](#) on page 342).

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. Select **Save Current Configuration to 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

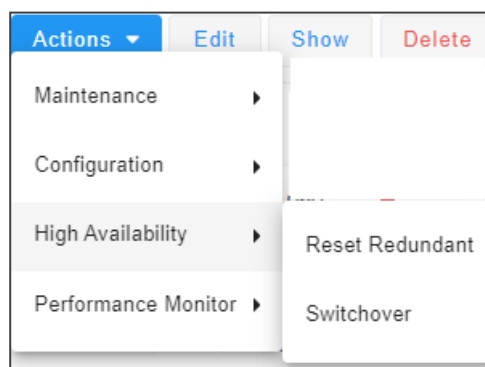
You can reset a device's redundant chassis.



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*.

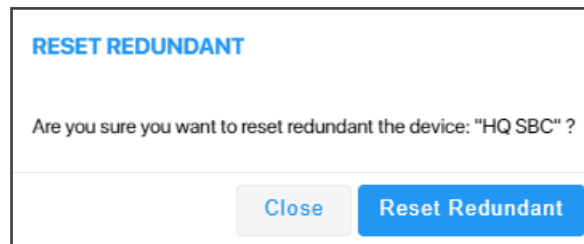
➤ To reset a device's redundant chassis:

1. In the Network page under either the **Topology** or **Devices** tab, select the device to reset and then click the activated **Actions** button.



If the menu option unavailable, the device selected does not support HA.

2. Navigate to **High Availability** and then select **Reset Redundant**.



3. In the prompt, click **Reset Redundant**.



Resetting a device's redundant chassis is identical to restarting an active device. See [Restarting a Device](#) on page 341 for more information.

Performing Switchover

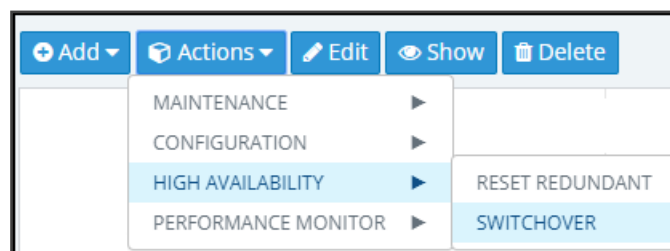
This only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

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 7-14: 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 312. A profile determines how the OVOC monitors network | device performance. A profile determines:

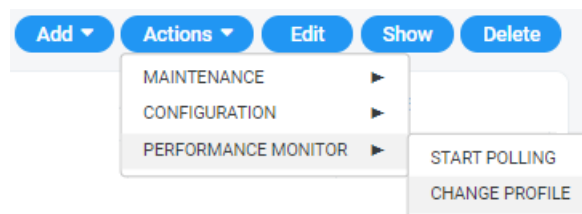
- What's monitored [which network | device parameters]
- How frequently [how often they're polled]

- When an alarm is issued [at what parameter threshold]
- Alarm severity [if a parameter threshold is exceeded]

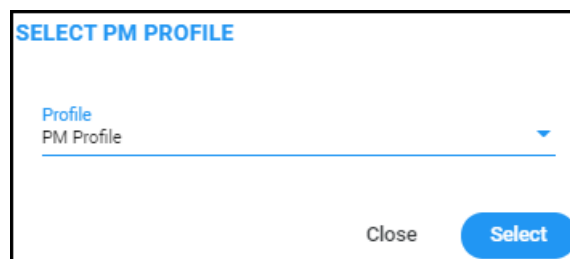
➤ **To change profile:**

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

Figure 7-15: 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**.



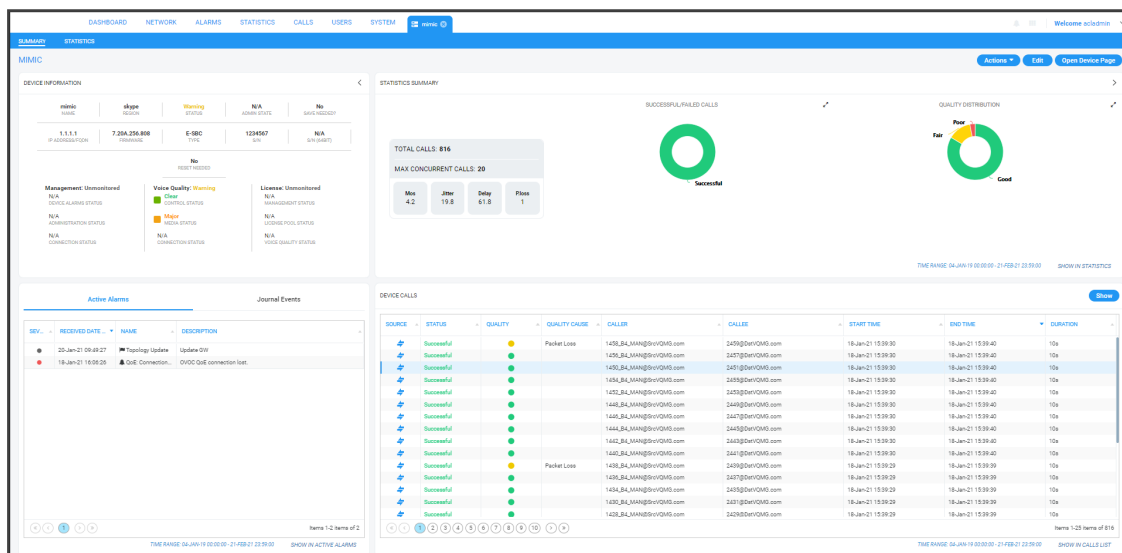
Showing Device Information

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.

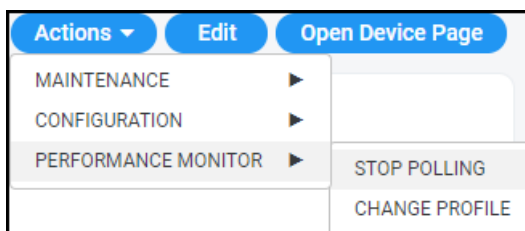
Figure 7-16: Show Device Information



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 317 and [Changing Profile](#) on page 350.



- OVOC can fetch up to 25000 metrics values in a single PM Statistics filter request.

Metric Name	Value
IP Group (SW 7.4 & above): 25-Oct-22 (12 Items)	
IP Group (SW 7.4 & above) (Default_IPG) Active Calls In (Average)	0
IP Group (SW 7.4 & above) (Default_IPG) Active Calls Out (Max)	0
IP Group (SW 7.4 & above) (Default_IPG) Active Calls Out (Average)	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate In (L...	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate In (A...	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate Out ...	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls In (Average)	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls Out (Max)	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls Out (Average)	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate In (Max)	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate In (Aver...	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate Out (Av...	0
CPU (SW 7.4 & above): 25-Oct-22 (4 Items)	
CPU (SW 7.4 & above) (SPM & RW) CPU Utilization (Average)	42.02
CPU (SW 7.4 & above) (SPM & RW) CPU Utilization (Max)	58
CPU (SW 7.4 & above) (SPLS) CPU Utilization (Max)	6
CPU (SW 7.4 & above) (SPLS) CPU Utilization (Average)	6

If for example an operator requests an entire month and has more than 25000 metrics values, the OVOC prompts the operator to refine the filter. OVOC *displays* up to 10000 metrics values and indicates that the operator can download the results as an XML file (the same XML file that the OVOC downloads after clicking **Save Device PM Data**).

Metric Name	Value
IP Group (SW 7.4 & above): 25-Oct-22 (12 Items)	
IP Group (SW 7.4 & above) (Default_IPG) Active Calls In (Average)	0
IP Group (SW 7.4 & above) (Default_IPG) Active Calls Out (Max)	0
IP Group (SW 7.4 & above) (Default_IPG) Active Calls Out (Average)	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate In (L...	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate In (A...	0
IP Group (SW 7.4 & above) (Default_IPG) Attempted Calls Rate Out ...	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls In (Average)	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls Out (Max)	0
IP Group (SW 7.4 & above) (IP-Users) Active Calls Out (Average)	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate In (Max)	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate In (Aver...	0
IP Group (SW 7.4 & above) (IP-Users) Attempted Calls Rate Out (Av...	0
CPU (SW 7.4 & above): 25-Oct-22 (4 Items)	
CPU (SW 7.4 & above) (SPM & RW) CPU Utilization (Average)	42.02
CPU (SW 7.4 & above) (SPM & RW) CPU Utilization (Max)	58
CPU (SW 7.4 & above) (SPLS) CPU Utilization (Max)	6
CPU (SW 7.4 & above) (SPLS) CPU Utilization (Average)	6

- ✓ In OVOC versions prior to 8.2.1000, the limitation was 10000 metrics values, so if for example an operator had 1000 IPGroups and 20 PM metrics values in a day, the OVOC returned $20 \times 1000 = 20000$ metrics values to the OVOC, which was not possible.

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 382 for more information).



- OVOC supports 25,000 counters values (via the OVOC GUI and the REST API) while fetching PM reports. As a result, it's possible to fetch a report for an SBC for all IP Groups. Prior to version 8.2.1000, 10,000 counters values were supported.
- If the number of filtered entities is between 10,000-25,000, an option to download the XML file is provided and data isn't loaded to the GUI.

Showing Link Information

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

➤ **To show link information:**


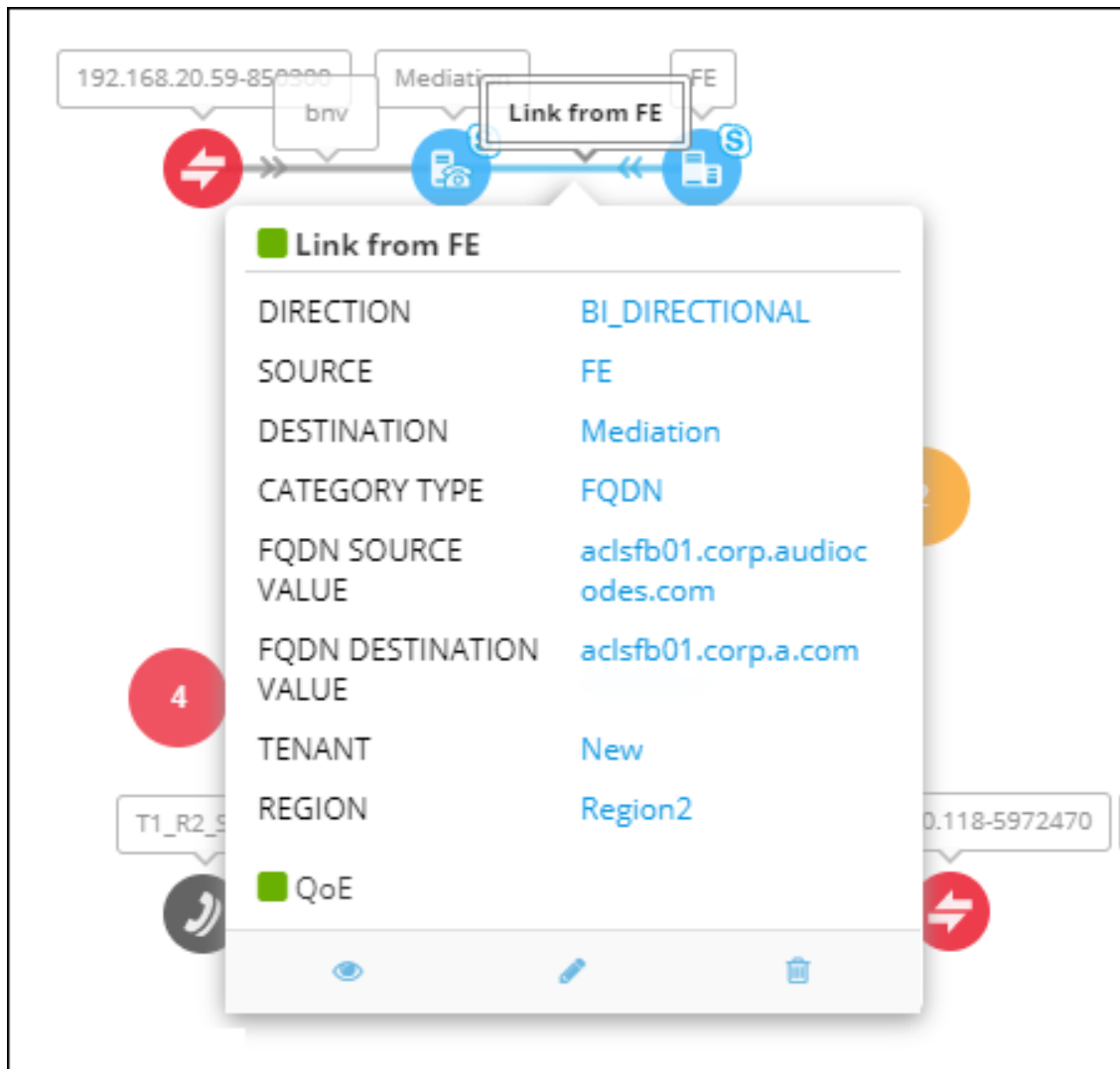
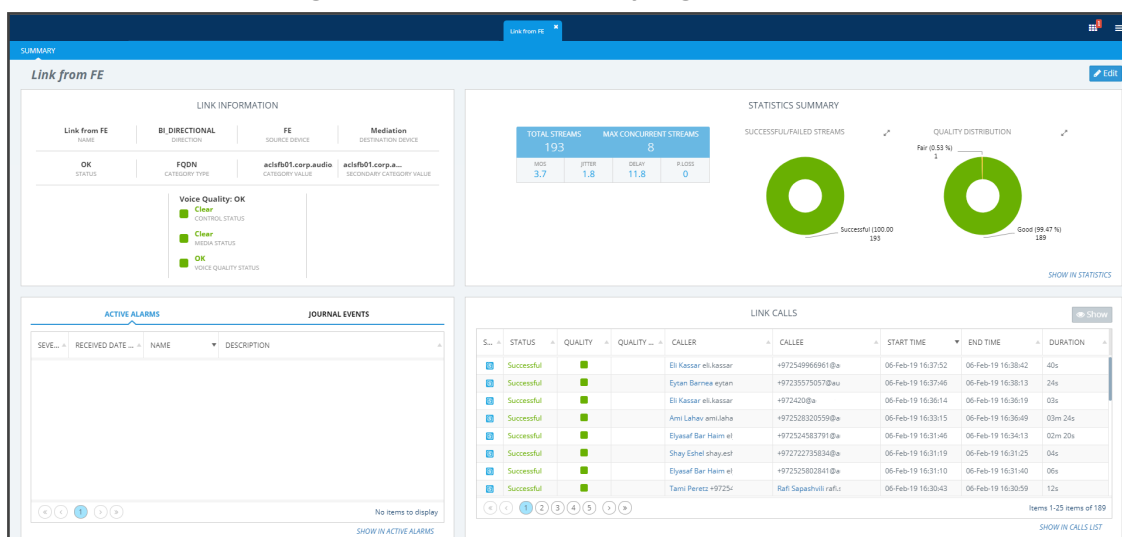
1. In the Network page under the **Topology** or **Links** tab, select the link and click the **Show** button. Alternatively, under the **Topology** tab, hover your mouse device over the link label and from the pop-up menu select the icon .

Figure 7-17: Show Link Information



The link's Summary page opens.

Figure 7-18: Link's Summary Page



- The page displays information about active alarms on the link, journal events, statistics summary and calls made over the link.
- The page is dynamically automatically tabbed on the menu bar: **Link from FE** in the figure above. Operators can delete the tab at any time. The tab facilitates quick future access to the page from other OVOC pages, for troubleshooting.
- Under the 'Statistics Summary' section of the page, the Successful / Failed Streams pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: Stream, Time, Successful / Failed or Quality Color.
- Under 'Link Calls' select any call made over the link and click **Show** to display that call's details; the Call Details page opens (see [Showing Call Details](#) on page 382 for more information).

Showing User Information

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

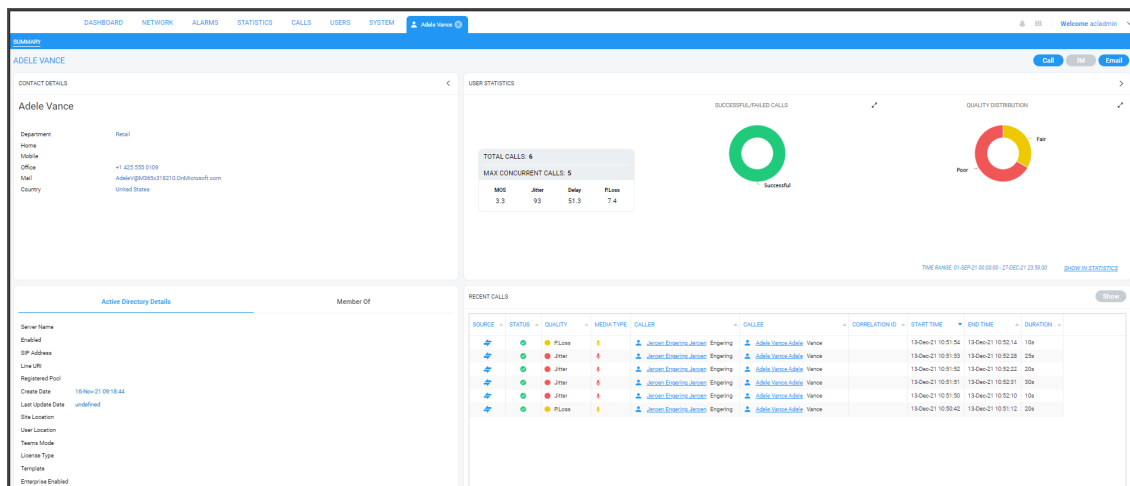


Information related to Teams users, which includes users' personal data as well as QoE reports, requires adding a Teams device to OVOC. See the *OVOC IOM* for more information.

➤ To show telephony information about a user:

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

Figure 7-19: Showing Information about a User



- The page displays contact details, Skype for Business details if any, user statistics and recent calls.

The page is dynamically automatically tabbed on the menu bar with the user's name. Operators can delete it at any time. The tab facilitates quick access to the page from other OVOC pages, for future reference.

- 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.
- 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 382 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 7-20: Device Details

The screenshot shows a web form titled "AC DEVICE DETAILS". It has five tabs: "General", "SNMP", "HTTP", "SBA", and "First Connection". The "General" tab is selected. The form contains the following fields:

Name	Description
10.3.181.61	

Tenant	Region
A	OrenU

Configured Device By
IP Address

IP Address
10.3.181.61

Address
The Severells Estate [Leith Hill], Noons Common Road, Broadmoor, Wotton, Abinger, Mole Vall

At the bottom right, there are two buttons: "Close" and "OK".

2. Edit the device's details. For more information, see [Adding AudioCodes Devices Automatically](#) on page 152.
3. Click **OK**.

Deleting a Device

The **Delete** button lets you delete a device from OVOC.

➤ **To delete a device:**

- Select the device to delete and then click the **Delete** button.

Taking a Device Inventory

OVOC enables customers to quickly and easily take an inventory of all AudioCodes devices managed in their network, in order to align (for example) OVOC's managed inventory with the support renewal contract.

With the feature, a customer who has globally deployed hundreds of AudioCodes devices can quickly and easily extract information and site locations from OVOC, facilitating effective management.



Only available for network administrators whose *permission level* is 'System Operator'.

The network administrator downloads a Topology report file (topology.csv) that also includes geographical location information obtained by the OVOC server accessing the location server; if the server is inaccessible and the address cannot be mapped (i.e., if there is no connection to the server), the field in the OVOC GUI displays LAT / LONG and LATITUDE and LONGITUDE is saved in the file.



The Topology report file (topology.csv) is not subject to multi-tenancy and contains all tenants' AudioCodes devices.

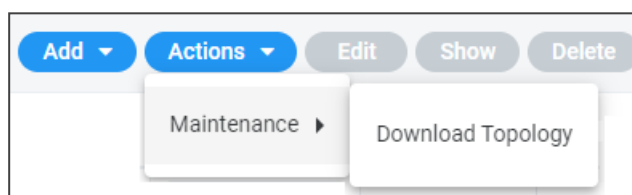
The Topology report file includes these fields:

- Serial Number
- IP Address
- Gateway Name
- Region Name
- Product Type
- Software Version
- Performance Polling Status
- Description
- SBA FQDN Name
- SBA IP Address
- SNMP Version
- SNMP Read
- SNMP Write
- SNMP User Profile
- Gateway User
- Gateway Password
- HTTPS Enabled
- FQDN
- Second Serial Number

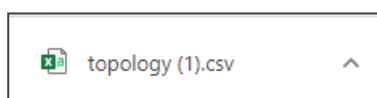
- Tenant Name
- Address
- Number of licensed signaling sessions
- Number of licensed SIP-REC sessions
- Number of provisioned E1 trunks
- Trunks Type (e.g., 2x E1 or SIP)
- Last restart time of the device
- Number of configured trunks

➤ **To take an inventory of the devices in your network:**

1. In the Device Management page (**Network > Devices > Manage**), click the **Actions** button.



2. Select the **Maintenance > Download Topology** option.
3. View the topology.csv file icon in the lowermost left corner of your screen.



4. Click the icon to open the file.

Serial Number	IP Address	GW Name	Region Name	Product Type	Software Version	Performance Polling Status	Description	SBA FQDN Name	SBA IP Address	SNMP Version	SNMP Read	SNMP Write	SNMP User Profile	Gateway User	Gateway Password	HTTPS Enabled	R
9796899	2010:0001:0000:000 10.3.181.247	region	Mediant 500L M7.24A.356.404			Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	16
188304493	172.17.118.88	172.17.118.88 AutoDetectIO	SW SBC		7.40A.100.330	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
2	10.36.1.2	10.36.1.2	SBC	MP114 FXS	6.60A.322	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
1	10.36.1.1	10.36.1.1	SBC	MP114 FXS	6.60A.322	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
5887475	172.17.118.58	172.17.118.58 Teams	Mediant 500 E-SI 7.40A.290.051			Not Polling	172.17.118.58			SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
8	0.0.4.210		1 aa	UNKNOWN		Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
12340184	10.3.181.7	12340184-10.3.aa	Mediant 1000 E-17.40A.290.085			Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
10	1.2.2.2	1.2.2.2	aa	UNKNOWN		Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
11	3.3.3.3	3.3.3.3	aa	UNKNOWN		Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
12	1.2.3.5	1.2.3.5	R1	UNKNOWN		Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
13 11599	10.36.47.99	10.36.47.99	bb	SW SBC	7.20A.201.375	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
14	10.21.2.38	10.21.2.38	AutoDetectIO UNKNOWN			Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
1640307502	10.3.181.88	10.3.181.88	AutoDetectIO SW SBC		7.40A.290.140	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
16	1.2.3.6	1.2.3.6	aler1(5)	AutoDetectIO UNKNOWN		Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
17 169856209	10.3.181.89	2010:3:181:89 AutoDetectIO	SW SBC		7.40A.290.130	Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	
18 11317393	172.17.140.246	172.17.140.246 AutoDetectIO	Mediant 500L M7.24A.356.685			Not Polling				SNMPv2	8ktrnBulPIT1/OBAMNtinsMVeryk4hfg==	Admin	fseUjPsaO6h4ugStOI	0		0	



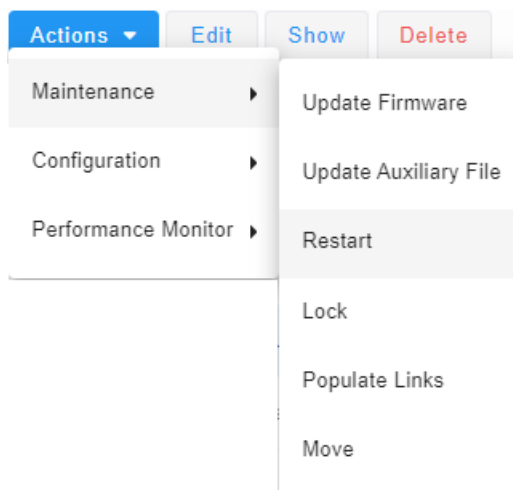
The file contains AudioCodes devices only.

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**.



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 348 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**.

Connecting via RDP to Windows-based AudioCodes Products

OVOC allows network administrators to access Windows-based AudioCodes products via Remote Desktop Protocol (RDP) when they're managed via WebSocket.

The Windows-based server products currently supported are:

- UMP (see [here](#))
- SBA for Teams (Generic) (see [here](#))

Connecting to UMP via RDP

Network administrators can connect to an AudioCodes User Management Pack (UMP) server via Remote Desktop Protocol (RDP) using Guacamole RDP Gateway.



If the UMP is operating under WebSocket Tunneling, Guacamole RDP can optionally go through WebSocket Tunneling.

➤ To connect to a UMP server via RDP:

1. Enable the Guacamole RDP Gateway (see the *IOM Manual* for detailed information, including user name / password).
2. In the OVOC's Dashboard page, locate the UMP server's icon.



3. Click the icon.

Figure 7-21: Device Management page filtered to display only UMP servers


NAME	IP ADDRESS / FQDN	PRODUCT TYPE	H.	STATUS	QOS ST.	CALLS	MAX CO.	QUALITY	SUCCESSFUL/F.	VERSION	MANAG.	ADMINIST.	LICENSE	PM POLL.	TENANT	REGION
10.21.2.142	10.21.2.142	User Management	✗	●	0	0			8.0.0.0.180	8.0.0.0.180	UNLOCKED	●	●		T2	R2
10.21.50.61	10.21.50.61	User Management	✗	●	0	0			8.0.0.0.345	8.0.0.0.345	UNLOCKED	●	●		T1	R1

- In the Device Management page filtered to display only UMP servers, select the UMP server to which to connect to via Remote Desktop, and then click **Actions**.

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	H.	STATUS	QOS ST.	CALLS	MAX CO.	QUALITY	SUCCESSFUL/F.	VERSION	MANAG.	ADMINIST.	LICENSE	PM POLL.	TENANT	REGION
10.21.2.142	10.21.2.142	User Management	✗	●	0	0			8.0.0.0.180	8.0.0.0.180	UNLOCKED	●	●		T2	R2
10.21.50.61	10.21.50.61	User Management	✗	●	0	0			8.0.0.0.345	8.0.0.0.345	UNLOCKED	●	●		T1	R1

- Select **Maintenance > Open RDP Session**.

Figure 7-22: Maintenance > Open RDP Session



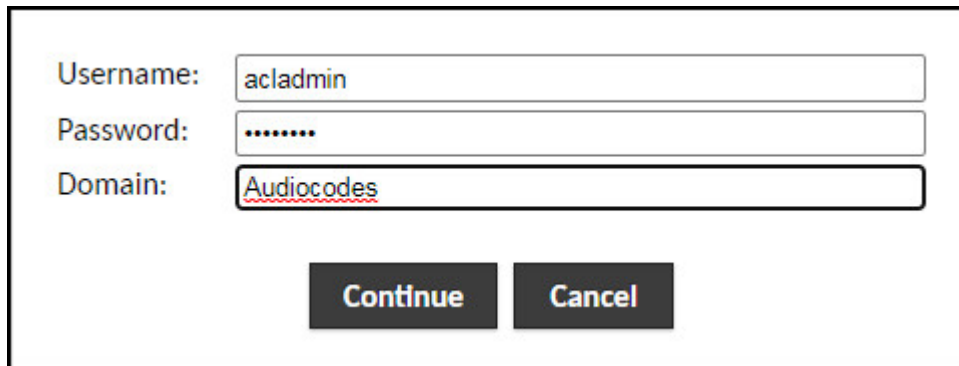
APACHE GUACAMOLE

Password

Login

- Enter the username and password of the Apache Guacamole Remote Desktop (RDP) Gateway. Defaults: umpman / umppass. The password can be changed; see the *IOM Manual* for more information.
- Click **Login**.

Figure 7-23: UMP Username | Password | Domain



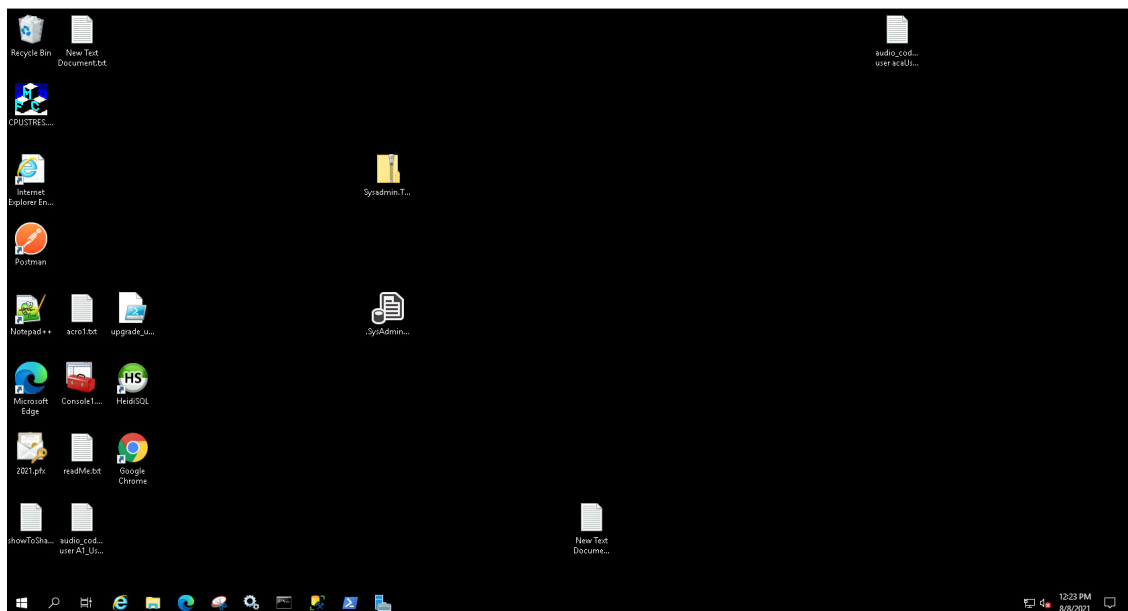
Username:

Password:

Domain:

8. Enter the username / password / domain for the UMP's Remote Desktop; the RDP connection is established.

Figure 7-24: UMP Remote Desktop



Connecting to SBA via RDP

Network administrators can connect to AudioCodes' Survivable Branch Appliances (SBAs) for Microsoft Teams, via RDP using Guacamole RDP Gateway. From the OVOC's Dashboard page, administrators can view AudioCodes' SBAs for Microsoft Teams deployed in their networks, in the Device Management page, by clicking this icon:





- If the SBA is operating under WebSocket Tunneling, Guacamole RDP can optionally go through WebSocket Tunneling.
- SSO is supported.

➤ **To connect to SBA via RDP:**

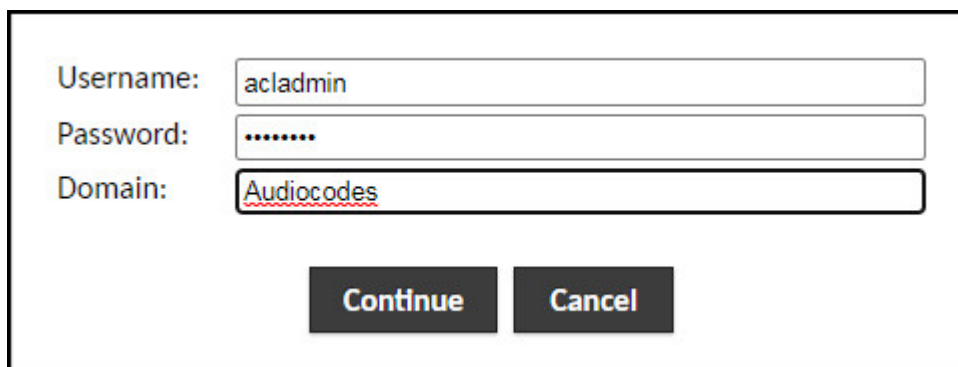
1. Enable the Guacamole RDP Gateway (see the *IOM Manual* for detailed information, including user name / password).
2. In the OVOC's Dashboard page, locate the SBA icon and click the icon; the Device Management page opens, filtered to display only SBAs for Microsoft Teams.
3. Select the SBA to which to connect to via Remote Desktop, and then click **Actions**.
4. Select **Maintenance > Open RDP Session**.

Figure 7-25: Maintenance > Open RDP Session

The screenshot shows the Apache Guacamole login interface. At the top is the Guacamole logo, which is a green mole head inside a black circle. Below the logo, the text "APACHE GUACAMOLE" is centered. Underneath, there are two input fields: the first is for the username, and the second is labeled "Password". Below these fields is a dark gray button with the word "Login" in white text.

5. Enter the username and password of the Apache Guacamole Remote Desktop (RDP) Gateway. Defaults: umpman / umpass. The password can be changed; see the *IOM Manual* for more information.
6. Click **Login**.

Figure 7-26: SBA Username | Password | Domain



Username:

Password:

Domain:

Continue **Cancel**

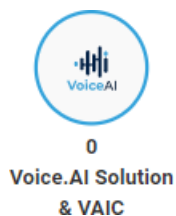
7. Enter the username / password / domain for the SBA's Remote Desktop; the RDP connection is established.

Managing VoiceAI Connect

OVOC enables network administrators to manage AudioCodes' VoiceAI Connect. Network administrators can perform **Add**, **Edit**, **Backup** and **Restore** actions. VoiceAI Connect enables connecting any contact center of SIP trunk to any bot framework. VoiceAI Connect creates a communication hub between any bot framework, any telephony system and any cognitive speech service to support virtually any voice-bot use case.

➤ To manage VoiceAI Connect:

1. In the OVOC's Dashboard page, locate the **Voice.AI Solution & VAIC** icon.



2. Click the icon; the Device Management page opens displaying Voice AI & Voice AI Connect entities.

Figure 7-27: Voice AI & Voice AI Connect entities

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	STATUS	QoS ST.	CALLS	MAX CO.	QUALITY	SUCCESSFUL	VERSION	MANAG.	ADMINIST.
10.11.2.8-bdc5000b...	10.11.2.8	Voice AI Solution	×	●	●					7.7.0	●	UNLOCKED
10.31.5.251-30918b...	10.31.5.251	Voice AI Solution	×	●	●					8.4.0.9	●	UNLOCKED
10.38.2.137-a744a1...	10.38.2.137	Voice AI Solution	×	●	●					4.0.2000	●	UNLOCKED

- In the filtered page, select the entity to manage and then click **Show**.

Figure 7-28: Voice AI Connect - Show

NAME	AutoDetection	Error	N/A	No	20.76.73.144	2.9.025	VAC	ca731f69-17b8-4849-8CE9-42FEC683B27A	N/A	No
20.76.73.144-ca731f69-17b8-4849-8CE9-42FEC683B27A	AutoDetection	Error	N/A	No	20.76.73.144	2.9.025	VAC	ca731f69-17b8-4849-8CE9-42FEC683B27A	N/A	No

- View the entity's statuses.
- In the Device Management page, you can also **Add** and/or **Edit** Voice AI & Voice AI Connect entities in the same way as with other managed entities (see [Adding AudioCodes Devices](#) on page 152 for more information).

Managing Stack Manager

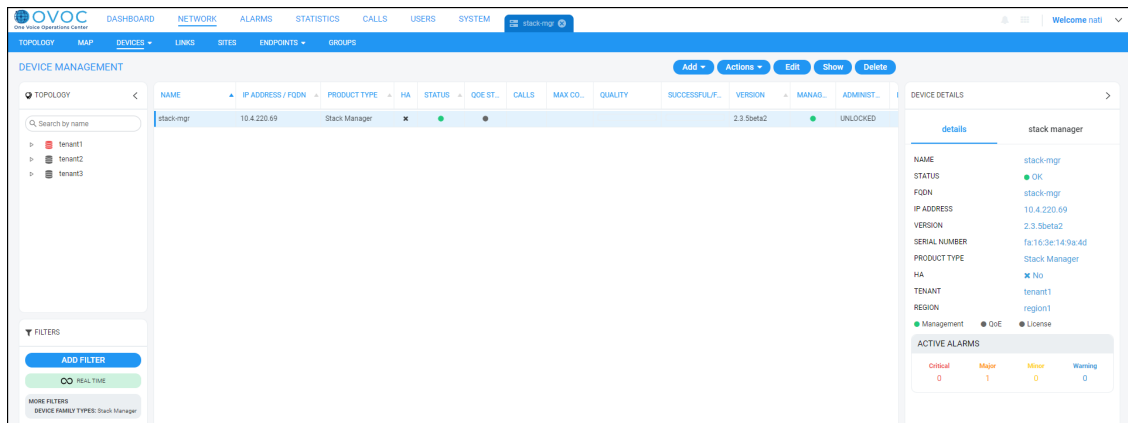
OVOC enables network administrators to manage AudioCodes' Stack Manager. Network administrators can use the OVOC to perform **Add**, **Edit**, **Backup** and **Restore** actions. The Stack Manager is used for managing 'software stacks' deployed in virtual environments. It implements the complete stack lifecycle, including Stack deployment, Stack termination, manual stack size adjustment – using user-initiated scale-in / scale-out, automatic stack size adjustment – using automatic scaling, and stack configuration update.

➤ To manage a Stack Manager:

- Open the Device Management page (**Network > Devices > Manage**) and if necessary, filter for Stack Manager (click **Add Filter** and then select **More Filters** and from the **Device**

Family Types dropdown select **Stack Manager Devices** -OR- from the **Product Types** dropdown select **Stack Manager**).

Figure 7-29: Stack Manager in Device Management page



2. In the filtered page, select the Stack Manager to manage and view in the Device Details pane on the right side of the page:
 - the name of the device, status, FQDN, IP address, version, SN, Product Type, HA, Tenant and Region
 - the management status, QoE status and License status
 - the alarms currently active on the device
3. In the Device Details pane, click the **stack manager** tab.

DEVICE DETAILS >	
details	stack manager
NAME	orenu-nqm
IP ADDRESS	52.149.62.135
SERIAL	43758731345474
STATE	stopped
NAME	yehoshua-loader-1
IP ADDRESS	20.190.5.50
SERIAL	65648303641803
STATE	running
NAME	timg-aws-ve-1
IP ADDRESS	18.159.88.30
STATE	stopped
NAME	AmritaMemory
IP ADDRESS	52.143.72.161
SERIAL	119720755870122
STATE	stopped
NAME	garyd-aws-ve-2
IP ADDRESS	18.198.20.49
STATE	stopped

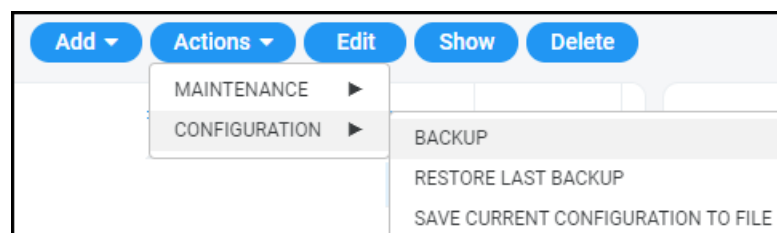
- In the Device Management page, click the **Show** button to view device information, more detailed management status, more detailed license status, more detailed active alarms and the same information but in a different format as the information shown in the Device Details pane > **stack manager** tab.

Figure 7-30: Stack Manager - Show

The screenshot shows the OVOC Stack Manager - Show page. The top navigation bar includes Dashboard, Network, Alarms, Statistics, Calls, Users, System, and Stack Mgr. The main content area is divided into several sections:

- DEVICE INFORMATION:** A table showing device details for 'stack-mgr' in 'region1'. It includes fields for NAME, REGION, STATUS (OK), N/A, DESCRIPTION, and SAVE NEEDED. Below this, there are sections for Management (OK) and License (Unmonitored) with corresponding status indicators.
- Active Alarms:** A table showing active alarms with columns for SEVE., RECEIVED DATE, NAME, and DESCRIPTION. It lists three events related to Topology Update and FQDN Resolve.
- Journal Events:** A table showing journal events with columns for SEVE., RECEIVED DATE, NAME, and DESCRIPTION. It lists three events related to Topology Update and FQDN Resolve.
- STACK MANAGER:** A table listing various stack managers with columns for NAME, TYPE, ENVIRONME., STATE, IP ADDRESS, SERIAL, # OF MCS, # CONNECTE., CE MEDIA US., and CE DSP USAGE. It lists several devices like 'orenu-nqm', 'yehoshua-load...', 'fmg-aws-ve-1', etc.

4. After selecting the device in the Device Management page, click the **Actions** button.



5. Perform the following optional actions: Backup, Restore Last Backup, Save Current Configuration to File, Move.
6. Click the **Edit** button to edit the device's settings or the **Add** button to add a new Stack Manager to the OVOC (see under [Adding AudioCodes Devices](#) on page 152 for more information).

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 176.

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 (**Quality of Experience > Calls List**) lists and shows quality information on calls made in the network over the past three hours (default) for a specific tenant.

Filters	SOURCE	STATUS	QUALITY	MEDIA TYPE	CALLER	CALLEE	CORRELATION ID	START TIME	END TIME	DURATION	CALL TYPE	DEVICE	LINK	TERMINATION REASON
<input type="checkbox"/>	0087145136375@10.9.9.5	●	●	↓	0087145136375@10.9.9.5	39764343 39764343 0018...		27-Dec-23 16:...	27-Dec-23 16:35:41		SBC	HQ SBC	Beceq SPT	No User Responding
<input type="checkbox"/>	0087145136375@10.9.9.5	●	●	↓	0087145136375@10.9.9.5	39764343 39764343 0018...		27-Dec-23 16:...	27-Dec-23 16:35:40		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0087145136375@10.9.9.5	●	●	↓	0087145136375@10.9.9.5	39764343 39764343 0018...		27-Dec-23 16:...	27-Dec-23 16:35:34		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0087143605197@10.9.9.5	●	●	↓	0087143605197@10.9.9.5	39764343 39764343 0018...		27-Dec-23 16:...	27-Dec-23 16:35:14		SBC	HQ SBC	Beceq SPT	No User Responding
<input type="checkbox"/>	0087143605197@10.9.9.5	●	●	↓	0087143605197@10.9.9.5	39764343 39764343 0018...		27-Dec-23 16:...	27-Dec-23 16:35:14		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	Mina Samir +97239764103@...	●	●	↓	Mina Samir +97239764103@...	0507056925@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:30:07		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0547751166@10.9.9.5	●	●	↓	0547751166@10.9.9.5	0547751166@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:29:17	01m 20s	SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	Mehdi Fakhri +9723976463...	●	●	↓	Mehdi Fakhri +9723976463...	0507056925@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:29:08	11s	SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0547751166@10.9.9.5	●	●	↓	0547751166@10.9.9.5	0547751166@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:27:38		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0547751166@10.9.9.5	●	●	↓	0547751166@10.9.9.5	0547751166@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:25:53		SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0775455028@iptrunk.ipc...	●	●	↓	0775455028@iptrunk.ipc...	0775455028@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:25:28	05s	SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	Daniel Shamoun +9723976410...	●	●	↓	Daniel Shamoun +9723976410...	0507056925@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:24:42	01m 57s	SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	Hanan Ghazal +9723976412...	●	●	↓	Hanan Ghazal +9723976412...	0544450864@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:22:16	01m 35s	SBC	HQ SBC	Beceq SPT	Normal Call Clear
<input type="checkbox"/>	0547751166@10.9.9.5	●	●	↓	0547751166@10.9.9.5	0547751166@iptrunk.ipc...		27-Dec-23 16:...	27-Dec-23 16:18:08	21s	SBC	HQ SBC	Beceq SPT	Normal Call Clear







Calls on AudioCodes High Availability devices during switchover are not supported. OVOC's QoE app 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:

- Time Range (see [Filtering to Access Specific Information](#) on page 231).
- Topology (see [Filtering by 'Topology'](#) on page 243)
- Groups (see [Filtering by 'Groups'](#) on page 252)
- Active Directory (see [Filtering by 'Active Directory'](#) on page 374)
- Source Type (see [Filtering by 'Severity'](#) on page 256)
- Quality (see [Filtering by 'Quality'](#) on page 376)
- More Filters (see [Filtering by 'More Filters'](#) on page 378).

Use the following table as reference to the columns in the Calls List.

Table 8-1: Calls List Columns

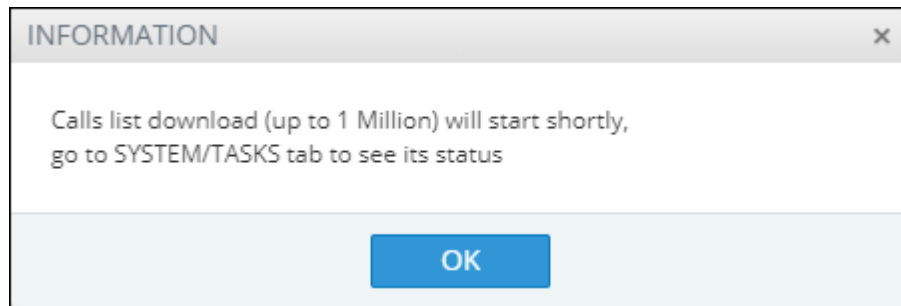
Column	Description	
Source	 indicates the call is from Microsoft Teams  indicates the call is from Microsoft Skype for Business  indicates the call is from an AudioCodes device.  indicates the call is from an AudioCodes IP phone.	
Status	Indicates call control status: Successful or Failed	
Quality	Indicates 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

Column	Description	
		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
Media Type	Indicates the media type: MSRP (Message Session Relay Protocol), Audio, Image, Application Sharing (a Skype for Business media type), Video, Data, Chat, Audio V150, Text, Unknown or All.	
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.	
Correlation ID	Calls sent across several devices (Microsoft Teams and AudioCodes SBCs) are detected and reported separately to OVOC, and are displayed as different calls. 'Correlation ID' indicates calls detected that are <i>united into a single call</i> ; these have the same Correlation ID. The Calls List page allows filtering according to Correlation ID. See also Filtering by 'More Filters' on page 378 Filtering by 'More Filters' on page 378 for information about how to filter the page by 'Correlation ID'.	
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was started.	
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Duration (sec)	The duration of the call, in seconds. See the note following.	
Call Type	Indicates the call type.	
Device	Indicates the device/s over which the call passed.	
Link	Indicates the link/s over which the call passed.	
Termination Reason	Indicates the reason why the call was terminated.	



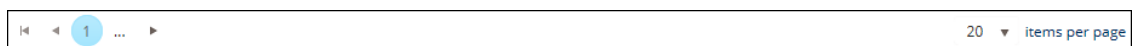
An SBC call (exclusively) whose duration is longer than three hours (e.g., the session of a participant in a Skype for Business conference call over an SBC) or an SBC call that is incompletely reported to the OVOC server won't be displayed in the Calls List.

The **Save** button allows operators to save up to one million calls to a zip file comprising 10 separate csv files, each including up to 100,000 calls.



A README file is also included in the save, with details of the Calls List filter settings, the number of exported entities, the time range and the tenant operator credentials.

The foot of the page features a pager.



The pager lets you (from left to right):

- Click the | **Go to the first page** to return to the first page from any page.
- Click the **Go to the previous page** arrow to return to the page before the presently displayed page.
- Click ... **[More pages]** to the left of the page number or ... **[More pages]** to the right of the page number to page backwards or forwards respectively.
- Click the **Go to the next page** arrow to browse to the page after the presently displayed page.
- From the 'Items per page' drop-down, select the number of calls to display per page: **20, 30 or 50.**

Filtering by 'Active Directory'

Filter a page by a 'Active Directory' filter. The 'Active Directory' filters applies to the Calls List page under the Calls menu and to the Users Experience and Users Details under the Users menu.

TIME RANGE

>

CUSTOMERS

>

ACTIVE DIRECTORY

▼

☒ Pin all selected

User Locations:

SOURCE TYPE

>

QUALITY

>

MORE FILTERS

>

Filter	Description
Pin all selected	<ul style="list-style-type: none">■ Check the option for the filter to 'follow' you when navigating between pages that feature the same filter.■ Clear the option for the filter to only apply to this page.
User Locations	From the Drop-down list, select the relevant User Location to filter. Calls statistics are displayed for all Active Directory users at the filtered location.

Filtering by 'Quality'

Filter a page by a 'Quality' filter. The 'Quality' filters apply to the Calls List page under the Calls menu. The filter displays only those calls whose Status is Failed | Success and/or whose Quality is Poor, Fair Good or Unknown.

Figure 8-1: Quality Filter

TIME RANGE >

TOPOLOGY >

SOURCE TYPE >

QUALITY ▼

Status:

☒ Failed

☒ Success

Quality:

☒ ■ Poor

☒ ■ Fair

☒ ■ Good

☒ ■ Unknown

Cause:

☒ None

☒ MOS

☒ Jitter

☒ Delay

☒ P. Loss

☒ Echo

MORE FILTERS >

APPLY

Use the following table as reference.

Table 8-2: 'Quality' Filter

Filter	Description
Failed Success	Filters calls according to their status. If you clear Success and select Failed, only calls whose status was Failed are displayed in the page.
Poor, Fair, Good or Unknown	Filters calls according to their quality. If you clear all except Poor, only calls whose quality was Poor will be displayed.
None, MOS, Jitter,	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

Filter	Description
Delay, P. Loss or Echo	display only calls <i>whose quality was poor/fair because there was a delay on the line.</i>

Filtering by 'More Filters'

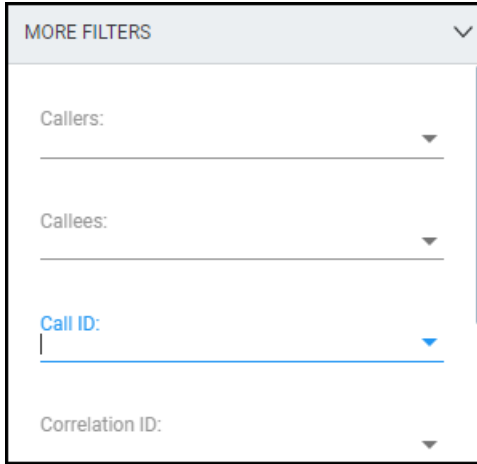
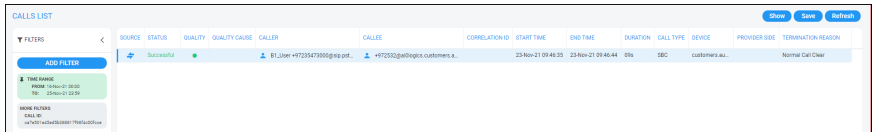

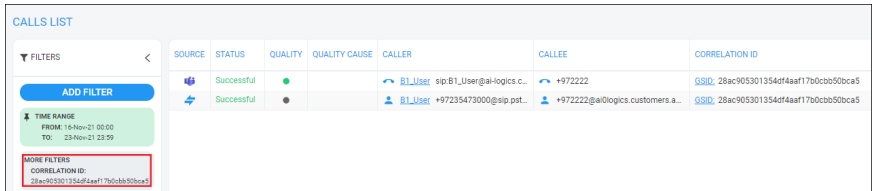
The Calls List page can be filtered using the 'More Filters' filter. This filter lets you display calls according to caller, callee, media type, etc.

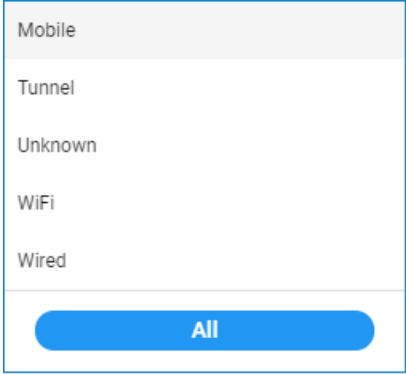
Figure 8-2: More Filters – Calls List Page

Use the following table as reference.

Table 8-3: More Filters – Calls List

Filter	Description
Filter either caller or callee	<p>Used in combination with the 'Callers' and 'Callees' filters below.</p> <ul style="list-style-type: none"> ■ Select this option for the page to be filtered by users who are 'Callers' or by users who are 'Callees'. ■ Clear the option for the page to be filtered by users who are 'Callers' and by users who are 'Callees' separately.
Callers	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.
Callees	Enter the name of a called party (or the names of called parties) whose calls you want to display in the page. The filter is case sensitive.

Filter	Description
Call ID	<p>Service Providers can use this filter to track calls in (for example) protocol verification scenarios with other Service Providers. The network operator obtains the Call ID from the SBC and then pastes it into the Call ID filter field in OVOC.</p>  <p>After clicking the Apply button, the Calls List page is filtered to display only that call ID.</p> 
Correlation ID	<p>See Accessing the Calls List on page 371 for more information about Correlation ID.</p> <p>To filter according to Correlation ID:</p> <ol style="list-style-type: none"> In the Calls List page, click the GSID of a unified call:  View the call displayed in the page together with the call with which it is unified. View also the Correlation ID displayed under the filter. 
Caller Connection Types	Click the dropdown arrow and select the type to filter by:

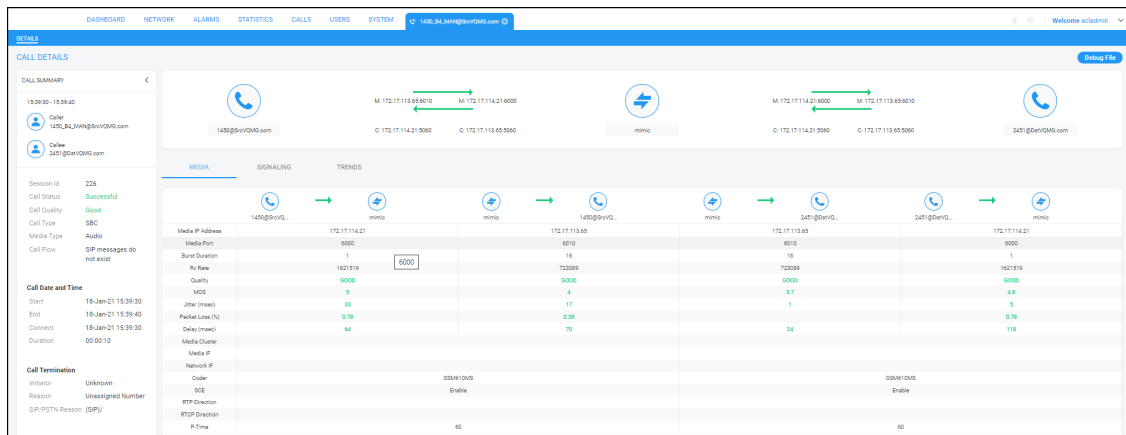
Filter	Description
	 <p>Caller Connection Types: ▼</p>
Callee Connection Types	Click the dropdown arrow and select the type to filter by (the options are identical to the options for Caller Connection Types described in the preceding field. The page by default displays all connection types for both caller and callee.
Media Types	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), Audio, Image, Application Sharing (a Skype for Business media type), Video, Data, 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.
AC Termination Reasons	<p>Click the dropdown arrow and select from the list the reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.</p> <p>Some AudioCodes termination reasons are:</p> <ul style="list-style-type: none"> ■ Reason Not Relevant ■ Unassigned Number ■ Invalid Information Element Content

Filter	Description
	<ul style="list-style-type: none"> ■ 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
Teams Termination Reasons	See the device's <i>User's Manual</i> for more information about Termination Reason.
Skype and Endpoints Termination Reasons	<p>Click the dropdown arrow and select from the list the reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.</p> <p>Some MS Skype for Business Termination Reasons are:</p> <ul style="list-style-type: none"> ■ 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

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 231), Topology (see [Filtering by 'Topology'](#) on page 243), Source Type (see [Filtering by 'Severity'](#) on page 256), Quality (see [Filtering by 'Quality'](#) on page 376) and / or More Filters (see [Filtering by 'More Filters'](#) on page 378), 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 8-3: Call Details – Details of a Call Made over an AudioCodes Device



Details of a Call across Multiple Devices with Same Correlated ID

The figure below shows how the 'Correlation ID' column in the Calls List page indicates a call that has been made across multiple devices and which has been *united into a single call* having the same Correlation ID.

Figure 8-4: Calls List - Correlation ID

CALLS LIST													
<div> <div> <div>SHOW FILTERS</div> <div> <div>ADD FILTER</div> <div> <div>TIME RANGE</div> <div>FROM: 16-Nov-21 00:00</div> <div>TO: 25-Nov-21 23:59</div> </div> </div> </div> </div>													
SOURCE	STATUS	QUALITY	QUALITY CAUSE	CALLER	CALLER	CALLER	CORRELATION ID	START TIME	END TIME	DURATION	CALL TYPE	DEVICE	PROVIDER SIDE
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:41:58	25-Nov-21 11:42:09	11s	Teams	ai-logics	Teams
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:41:24	25-Nov-21 11:42:08	10s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:40:53	25-Nov-21 11:41:02	09s	Teams	ai-logics	Teams
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:40:43	25-Nov-21 11:41:00	09s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:39:59	25-Nov-21 11:40:04	05s	Teams	ai-logics	Teams
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 11:39:57	25-Nov-21 11:40:02	04s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 10:48:18	25-Nov-21 10:48:18	0s	Teams	ai-logics	Teams
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 10:48:16	25-Nov-21 10:48:17	0s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	25-Nov-21 10:48:06	25-Nov-21 10:48:16	0s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	24-Nov-21 08:57:11	24-Nov-21 08:57:16	05s	Teams	ai-logics	Teams
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	24-Nov-21 08:57:11	24-Nov-21 08:57:16	04s	SBC	customers.ai...	ai-logics
123456789	Successful	Good		123456789	123456789	123456789	1a83e0d7f5a42818e45b0c24924800	23-Nov-21 09:46:36	23-Nov-21 09:46:45	09s	Teams	ai-logics	Teams

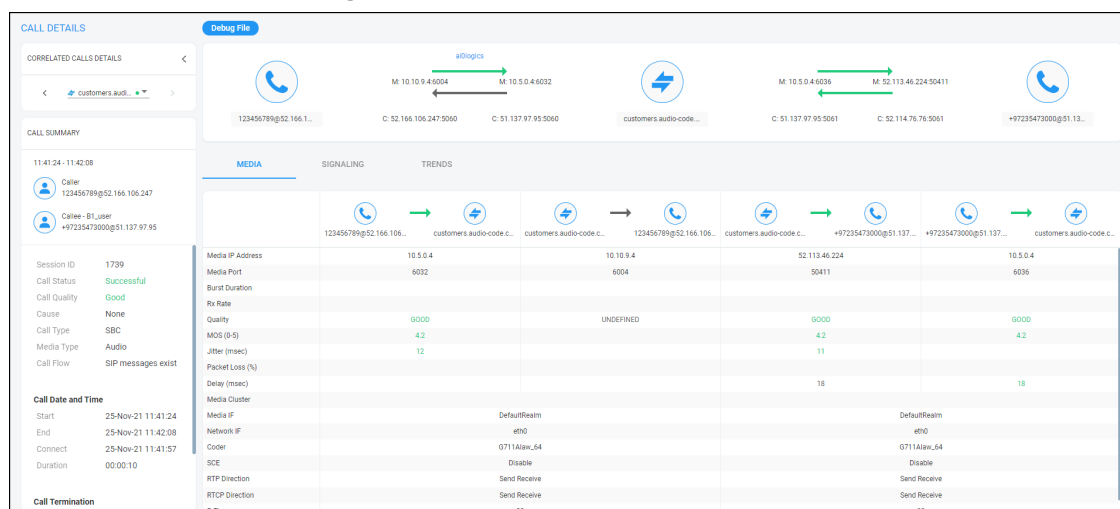


- The preceding figure shows the OVOC unifying a call sent across AudioCodes SBC - Microsoft Teams, under the same Correlation ID. OVOC also unifies SBC - SBC calls under the same Correlation ID. OVOC merges these calls into a single call and displays the details of all the legs of this call as shown next.
- The ini file parameter SendAcSessionIDHeader must be enabled on the SBC; it uses the Global Session ID (AC-Session-ID header) in SIP messages. See the device's *User's Manual* for more information.
- OVOC will correlate calls from SBC-SBC and Teams-SBC only when all devices reside in the same tenant.
- SBC-Teams failed calls will not be correlated if the Teams notification arrived less than five minutes after the call ends.
- SBC-Teams calls will not be correlated if the reported time difference between the SBC and Teams call is more than two seconds.
- SBC-Teams calls will not be correlated if Azure Active Directory was not defined as users sync source.

➤ To view the details of calls across multiple devices, united into a single call:

1. Select either of the calls as shown in the preceding figure, and then click the **Show** button.

Figure 8-5: Call Details



The screen is automatically dynamically tabbed on the menu bar of the Calls List page 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.

2. For detailed explanations about the parameter values displayed under the **Media**, **Signaling** and **Trends** tabs, see [Details of a Call Made over an AudioCodes SBC](#) on the next page and [Details of a Call Made over Microsoft Teams](#) on page 405.

- Each call reported by the SBC is color-coded using SBC quality thresholds as reported by the SBC. The color of the SBC and the color of the SBC links are affected.
- Each call reported by Microsoft Teams is color-coded using Teams quality thresholds. The Teams device and corresponding links are affected.
- A conference call can be also part of a correlated call. Its details are also displayed in the Call Details screen.
- The Call Details screen differentiates calls correlated with one another and unified under a common Correlation ID, by displaying *every leg of the unified call*. For example:
 Caller ↔ SBC ↔ Teams ↔ Callee -or-
 Caller ↔ SBC1 ↔ SBC2 ↔ IP phone ↔ Callee
- This provides operators an easy and convenient way to move to each specific leg based on the reporting device.
- The diagram in the Call Details screen displays the unified call's overall quality, i.e., worst leg quality.

Details of a Call Made over an AudioCodes SBC

The figure above shows the details of a call made over the AudioCodes SBC. You can also display the details of calls made/received over other entities. The page is automatically dynamically tabbed on the menu bar for quick and easy future access and troubleshooting. Operators can delete the tab at any time. The page displays detailed diagnostic information, in graphic and textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality. Use the following table as reference.

Table 8-4: Call Details Page

Page Sub-division	Description
(Uppermost) Call summary	Displays parameters and values identical to those displayed in the Calls List page.
(Middle) Graphic illustration	<p>Displays a graphical illustration of voice quality on each leg of the call, on both the caller and callee side. Each leg is:</p> <ul style="list-style-type: none"> ■ Connected via the VoIP cloud to the device ■ Color-coded to indicate quality (green = good, yellow = fair, red = poor, grey = unknown) ■ Tagged by C and M <p>C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)</p>

Page Sub-division	Description
(Lowermost) Three tabs	<p>Each opens a page displaying detailed information:</p> <ul style="list-style-type: none"> Media (see Media below) (includes Quality) Signaling (see Signaling on page 388) Trend (see Trends on page 390) (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 391)

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 8-6: Media

CALL DETAILS									
MEDIA					SIGNALING				
	+972397...	E-58C	E-58C	+972397...	E-58C	123@AC...	123@AC...	E-58C	
Media IP Address	10.1.1.158		10.62.0.10		10.10.10.2		10.9.9.130		
Media Port	51592		6920		8990		42582		
Signal Level									
Noise Level									
SNR									
Burst Duration									
Rx Rate	87		0		87		87		
Quality	GOOD		GOOD		GOOD		GOOD		
MOS			4.1		4.1				
Jitter	1		6		5		2		
Packet Loss									
Delay			3						
Echo									
Media IF		MRLAN				MRWAN			
Network IF		Voice				WANSP			
Coder		G711Mulaw				G711Alaw_64			
SCE		false				false			
RTP Direction		Send Receive				Send Receive			
RTCP Direction		Send Receive				Send Receive			
P-Time		20				20			

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

Table 8-5: Media Parameters

Parameter	Description
Media IP Address	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. Port of the destination host / media network.

Parameter	Description
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = $10 \log_{10}(\text{RMS talk spurt power (mW)})$. 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 = $10 \log_{10}(\text{Power Level (RMS), in mW, during periods of silence})$. A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). $\text{SNR} = \text{Signal level} - \text{Noise level}$.
Burst Duration	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
Rx Rate	Shows the call's reception rate, in Kbps.
Quality	Voice quality: Good (green), Fair (yellow) OR Red (poor).
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises: MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, for the caller and for the callee side. Packet Loss can be more than 100%.
Delay	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include

Parameter	Description
	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 8-7: 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. 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. 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 8-8: Signaling

CALL DETAILS				
<div> <div>← C: 10.1.1.158:64745 - C: 10.62.0.10:5069 →</div> <div>← C: 10.10.10.2:5060 - C: 10.9.9.5:5060 →</div> </div>				
MEDIA		SIGNALING		TRENDS
	<div> <div>+972397...</div> <div>→</div> <div>E-SBC</div> <div>→</div> <div>E-SBC</div> <div>→</div> <div>+972397...</div> </div>		<div> <div>E-SBC</div> <div>→</div> <div>123@AC...</div> <div>→</div> <div>123@AC...</div> <div>→</div> <div>E-SBC</div> </div>	
SIP IP	10.1.1.158	10.62.0.10	10.10.10.2	10.9.9.5
SIP Port	64745	5069	5060	5060
URI	+97239764491@a.com	+972123@edgw01.corp.a.com	39764491@a.com	123@edgw01.corp.com
Output URI Before Map	+97239764491@a.com	+972123@edgw01.corp.com	+97239764491@a.com	+972123@edgw01.corp.a.com
Endpoint Type	SBC		SBC	
SRD	SRDLAN: 1		SRDWAN: 2	
IP Group	Lync ARM: 7		Bezeq SIP: 3	
SIP IF				
Proxy Set	7		3	
IP Profile	1		3	
Transport Type	TLS		UDP	
Signaling diff server	40		40	

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

Table 8-6: Signaling Parameters

Parameter	Description
SIP IP	The call's caller/callee (source/destination) IP address.
SIP Port	The port number used for the SIP call.
URI	The URI (Uniform Resource Identifier) of the caller/callee (source/destination). The SIP URI is the user's SIP phone number (after manipulation, if any). The SIP URI resembles an e-mail address and is written in the following format: sip:x@y:Port, where x=Username and y=host (domain or IP).
Output URI Before Map	The SIP URI address of the caller/callee before manipulation (if any) was done on the URI.
Endpoint Type	Indicates the type of endpoint. For example, 'SBC'.
SRD	The unique name and index configured for the signaling routing domain (SRD). Example: someSRD (n) , where n following the displayed name is the number indicating the SRD's index used to facilitate network configuration.
IP Group	The ID of the IP Group with which the call is associated.
SIP IF	The ID of the SIP Interface with which the call is associated.
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

Parameter	Description
	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 8-9: 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.

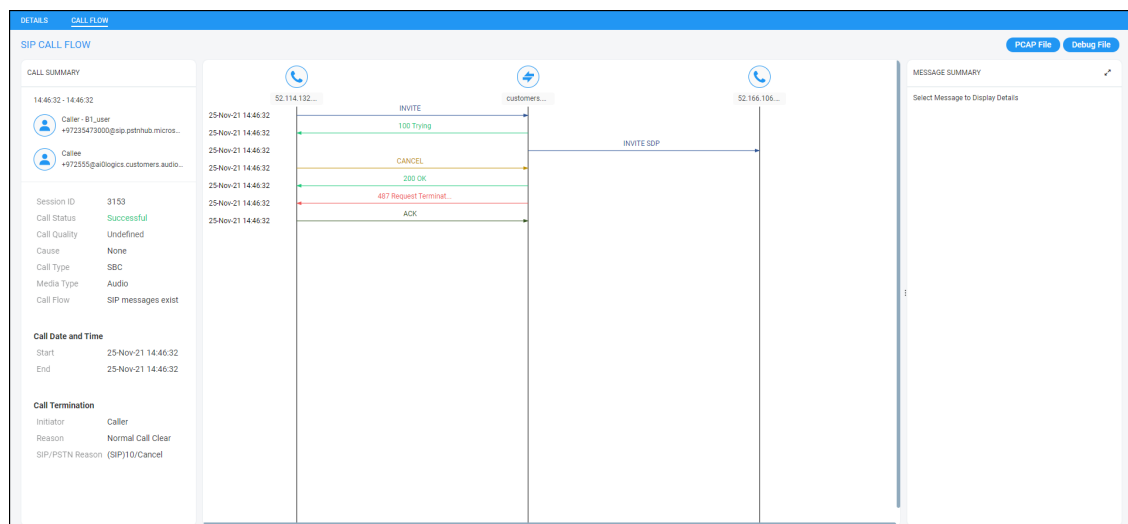
SIP Call Flow

The **SIP Call Flow** tab is displayed in the Call Details page when a SIP Ladder (Call Flow) is available or partially available and found for a specific call over an SBC.

➤ **To view the Call Flow screen:**

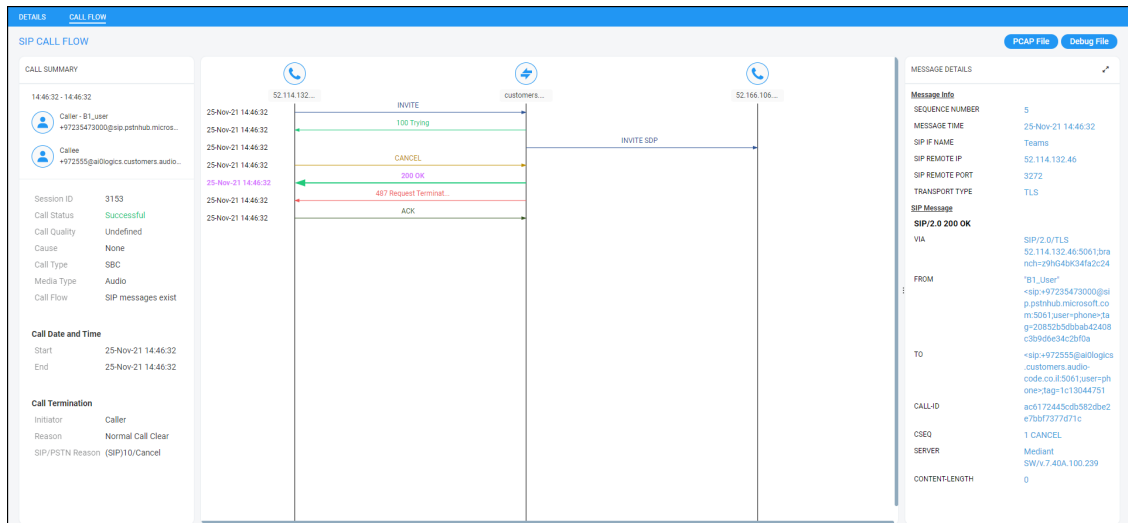
1. In the Calls List page (**Calls > Calls List**), select the call, click the **Show** button and then in the Call Details page that opens, click the **Call Flow** menu.

Figure 8-10: SIP Call Flow



2. Click the textual indication of a SIP message to display MESSAGE DETAILS in the right pane.

Figure 8-11: Message Details



- The text indication changes color to bold pink
- The call flow leg line is made bold
- See **200 OK** in the figure above as an example



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.

- Use the following table as a reference for error response color codes. Use the table following it as a reference for the 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

Color	SIP Message
Brown	CANCEL
Purple	BYE
Black (unbolded)	All other SIP messages and codes



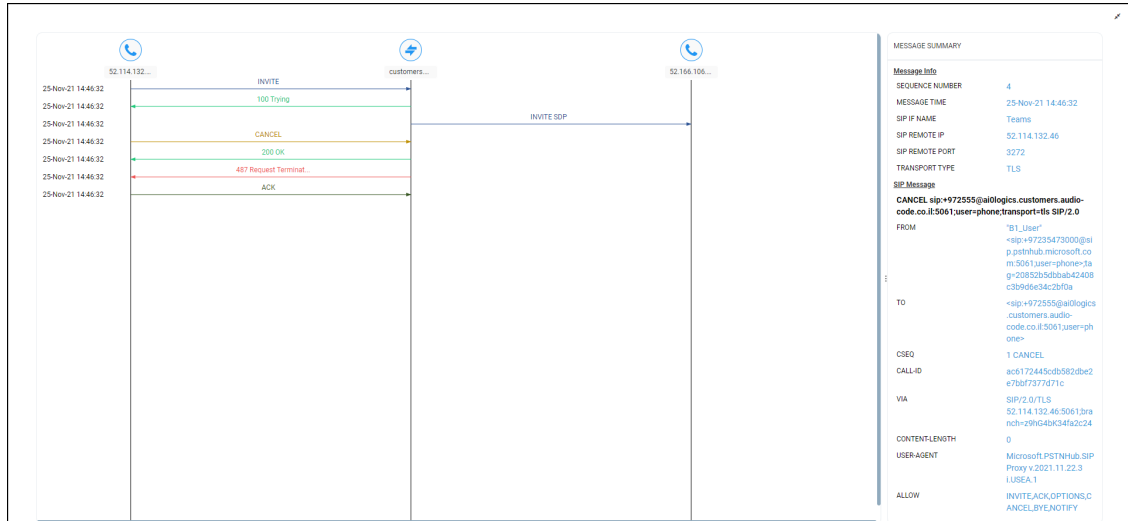
- Optionally click the  icon in the upper right corner of the MESSAGE DETAILS pane to expand the page maximally. [Optionally, widen the pane in which the details of the SIP message are presented by positioning your cursor over the vertical ellipsis  located on the left margin of the pane, and then dragging it left].

Figure 8-12: Message Details Maximized

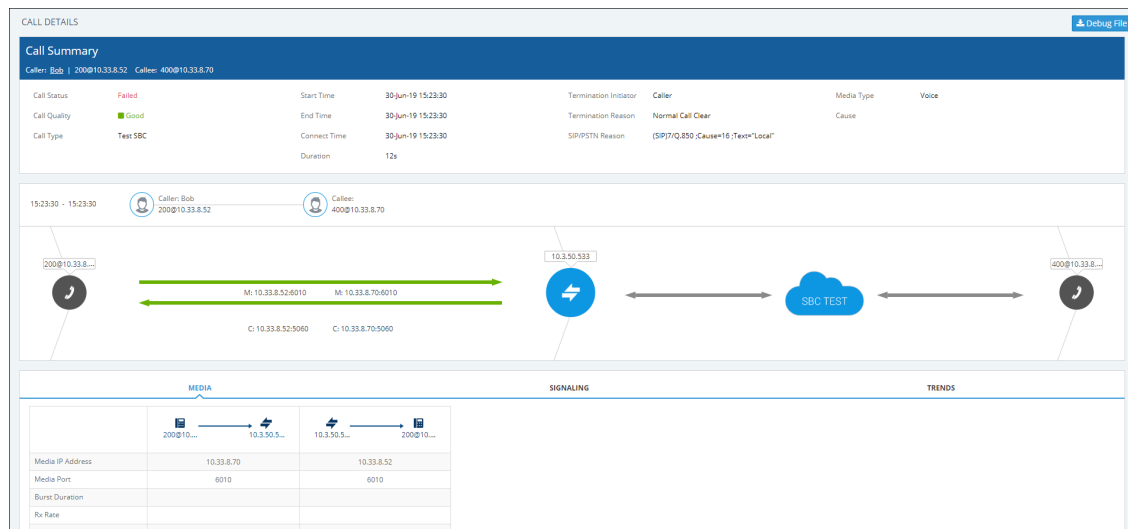


- Click the  icon to restore the page to its default display size.

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 378), 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 8-13: 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 and year) when the call was terminated.

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 <i>User's Manual</i> for more information about Termination Reason.	
SIP PSTN Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about the SIP/PSTN Reason.	
Media Type	Voice	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the 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	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ✓ Connected to a device ✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✓ Tagged by C and M <ul style="list-style-type: none"> C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip) 	
(Lowermost) Two tabs	<p>Each opens a page displaying detailed information:</p> <ul style="list-style-type: none"> ■ Media (see Media on page 418) ■ Signaling (see Signaling on page 388) 	

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, click the **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.

Call Details Page - PCAP File

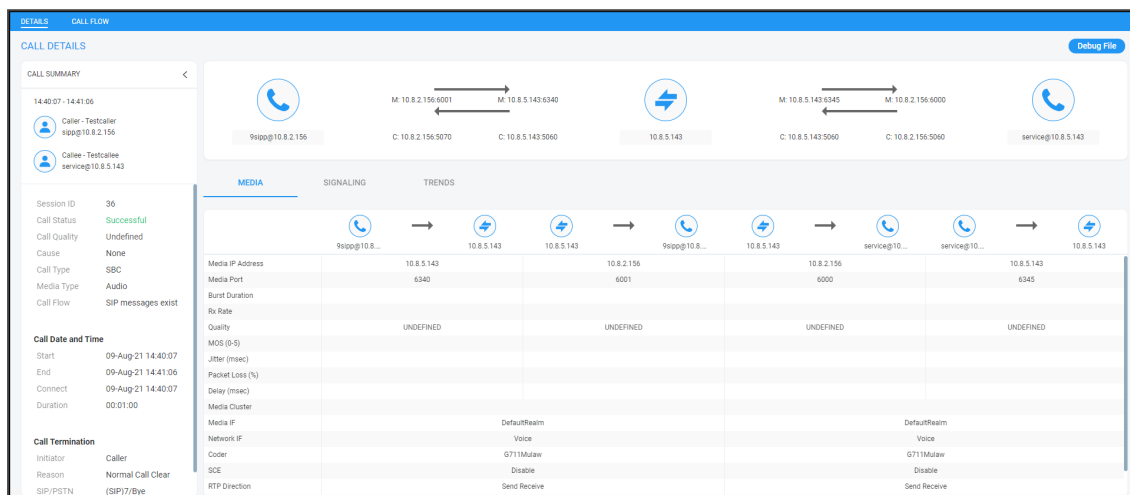
Details of calls made over AudioCodes devices and for which the OVOC displays a SIP Call Flow screen can be exported to a Packet Capture (PCAP) file. The PCAP file format specifically stores the SIP Ladder displayed in the SIP Call Flow screen.

➤ To export to PCAP file:

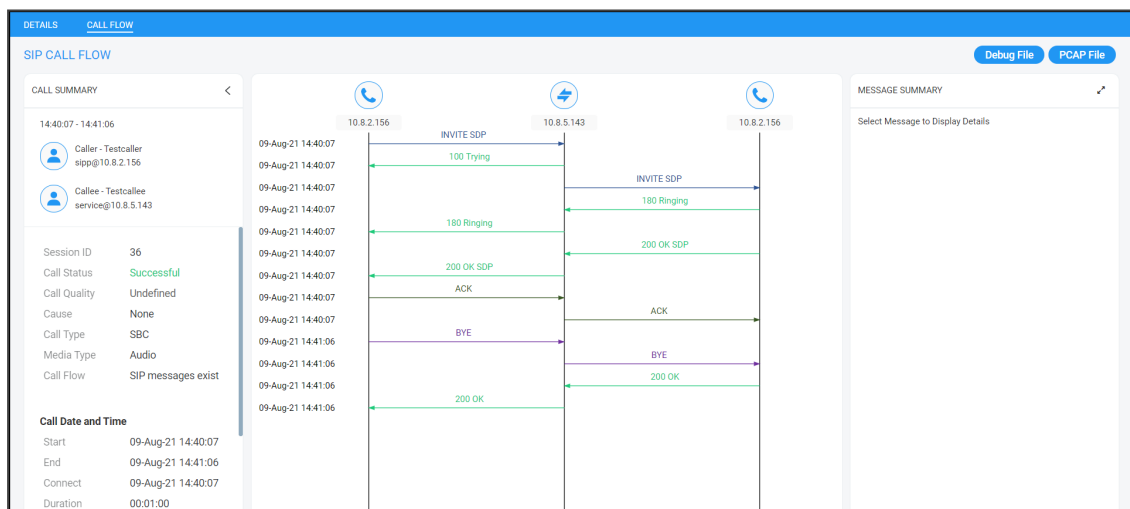
1. In the Calls List page (**Calls > Calls List**), select the call whose 'Call Type' is SBC:

CALLS LIST													Show	Save	Refresh
Filters	Source	Status	Quality	Quality CA.	Caller	Callee	Start Time	End Time	Duration	Call Type	Device	Link			
ADD FILTER		Successful			prebuil031@audio-codes.info	prebuil033@audio-codes.info	09-Aug-21 14:42:06	09-Aug-21 14:42:17	10s	Skype	carne@skype4...				
REAL TIME		Successful			prebuil031@audio-codes.info	prebuil033@audio-codes.info	09-Aug-21 14:42:06	09-Aug-21 14:42:17	10s	Skype	aaa12				
		Successful			prebuil021@audio-codes.info	prebuil025@audio-codes.info	09-Aug-21 14:41:55	09-Aug-21 14:42:09	07s	Skype	carne@skype4...				
		Successful			prebuil021@audio-codes.info	prebuil025@audio-codes.info	09-Aug-21 14:41:55	09-Aug-21 14:42:09	07s	Skype	aaa12				
		Successful			prebuil031@audio-codes.info	prebuil035@audio-codes.info	09-Aug-21 14:41:29	09-Aug-21 14:41:40	10s	Skype	carne@skype4...				
		Successful			prebuil031@audio-codes.info	prebuil035@audio-codes.info	09-Aug-21 14:41:29	09-Aug-21 14:41:40	10s	Skype	aaa12				
		Successful			prebuil04@audio-codes.info	prebuil06@audio-codes.info	09-Aug-21 14:40:56	09-Aug-21 14:41:12	15s	Skype	carne@skype4...				
		Successful			prebuil04@audio-codes.info	prebuil06@audio-codes.info	09-Aug-21 14:40:56	09-Aug-21 14:41:12	15s	Skype	aaa12				
		Successful			prebuil029@audio-codes.info	prebuil029@audio-codes.info	09-Aug-21 14:40:54	09-Aug-21 14:41:08	05s	Skype	carne@skype4...				
		Successful			prebuil033@audio-codes.info	prebuil033@audio-codes.info	09-Aug-21 14:40:54	09-Aug-21 14:41:08	05s	Skype	aaa12				
		Successful			TestCaller sipp@10.8.2.156	TestCallee service@10.8.5.143	09-Aug-21 14:40:07	09-Aug-21 14:41:06	01m	SBC	10.8.5.143				
		Successful			prebuil02@audio-codes.info	prebuil04@audio-codes.info	09-Aug-21 14:40:23	09-Aug-21 14:41:02	34s	Skype	carne@skype4...				
		Successful			prebuil02@audio-codes.info	prebuil04@audio-codes.info	09-Aug-21 14:40:23	09-Aug-21 14:41:02	34s	Skype	aaa12				
		Successful			prebuil031@audio-codes.info	prebuil033@audio-codes.info	09-Aug-21 14:40:48	09-Aug-21 14:40:59	06s	Skype	carne@skype4...				

2. Click the **Show** button; the Call Details screen is displayed.



3. Click the **Call Flow** tab; the SIP Call Flow screen is displayed.



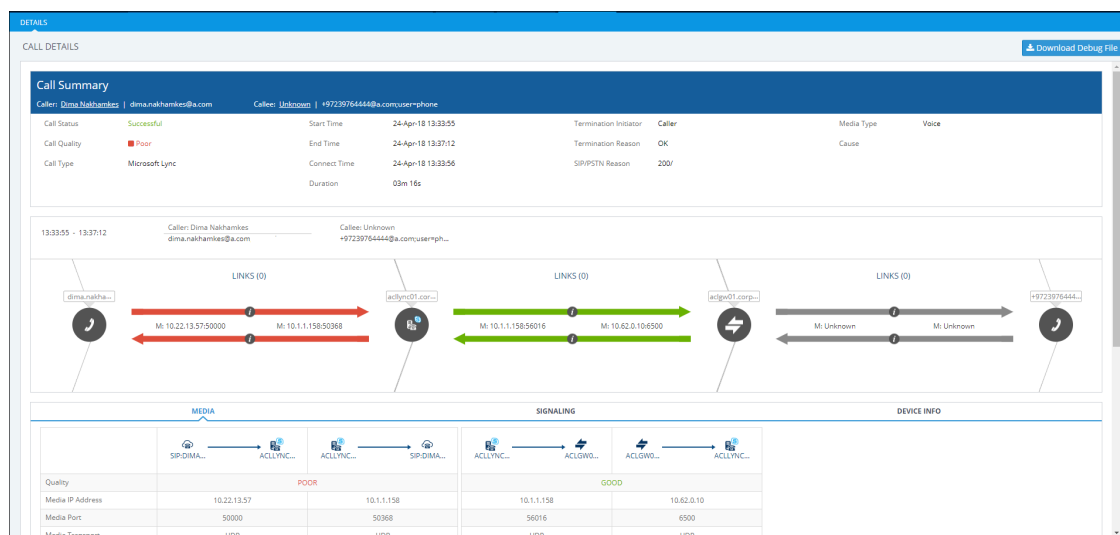
4. Click the **PCAP File** button and then view in the lowermost left corner of your PC screen the PCAP file.



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 8-14: 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.

Page Section	Description	
Duration	The duration of the call, in seconds.	
Termination Initiator	The network entity from which the call was terminated.	
Termination Reason	<p>The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.</p> <p>Some Skype for Business Termination Reasons are:</p> <ul style="list-style-type: none"> ■ 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 <i>User's Manual</i> 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

Page Section	Description	
		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
(Middle) Graphic illustration	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ✓ Connected to a device ✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✓ Tagged by C and M <ul style="list-style-type: none"> C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip) 	
(Lowermost) Two tabs	<p>Each opens a page displaying detailed information:</p> <ul style="list-style-type: none"> ■ Media (see Media below) ■ Signaling (see Signaling on page 388) 	

Media

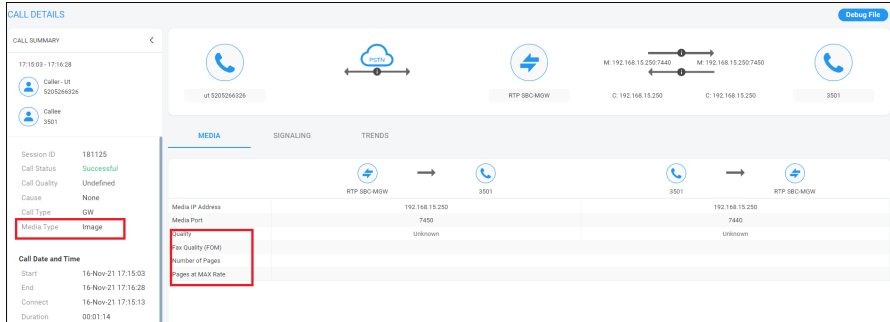
The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-15: Media

DETAILS		CALL DETAILS			
		MEDIA		SIGNALING	
		SIP-SHAL...	ACLLYNC...	ACLLYNC...	SIP-SHAL...
		ACLLYNC...	ACLLYNC...	ACLLYNC...	ACLLYNC...
Quality		GOOD		GOOD	
Media IP Address		10.11.2.8	10.1.1.158	10.1.1.158	10.62.0.10
Media Port		50008	55924	56198	6950
Media Transport		UDP	UDP	UDP	UDP
Coder		PCMU	PCMU		
MOS		3.71	4.2		3.7
Jitter					1
Packet Loss					
Delay		8	7	3	
Echo					
Signal Level		-10			
Noise Level		-71			
SNR		61			
Burst Duration					
BW Estimation					

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

Table 8-11: Media Parameters

Parameter	Description
Quality	Indicates the call's voice quality: Good Fair Poor
Media IP Address	<ul style="list-style-type: none"> The IP address of the device source in the operations, administration, and provisioning (OAMP) network. The IP address of the destination host / media network.
Quality Fax Quality Number of Pages Pages at MAX Rate	
Media Port	<ul style="list-style-type: none"> The device's source port in the operations, administration, 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.

Parameter	Description
MOS	<p>Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises:</p> <p>MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p> <p>MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p>
Jitter	<p>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.</p>
Packet Loss	<p>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%.</p>
Delay	<p>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.</p>
Echo	<p>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.</p>
Signal Level	<p>The ratio of the voice signal level to a 0 dBm0 reference. $\text{Signal level} = 10 \log_{10} (\text{RMS talk spurt power (mW)})$. A value of 127 indicates that this parameter is unavailable.</p>
Noise Level	<p>The ratio of the level of silent-period background noise level to a 0 dBm0 reference. $\text{Noise level} = 10 \log_{10} (\text{Power Level (RMS), in mW, during periods of silence})$. A value of 127 indicates that this parameter is unavailable.</p>
SNR	<p>The ratio of the signal level to the noise level (Signal-Noise Ratio). $\text{SNR} = \text{Signal level} - \text{Noise level}$.</p>

Parameter	Description
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 8-16: Signaling

MEDIA		SIGNALING
	Caller	Callee
Edge Server		
Gateway		
Mediation Server		
URI	4696@a.com	ami.lahav@a.com
Phone Number		
Is Internal	true	true
FrontEnd	adlync01.corp.a.com	
Pool	acpool2013.corp.a.com	
Call Priority	Normal	

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

Table 8-12: Signaling Parameters

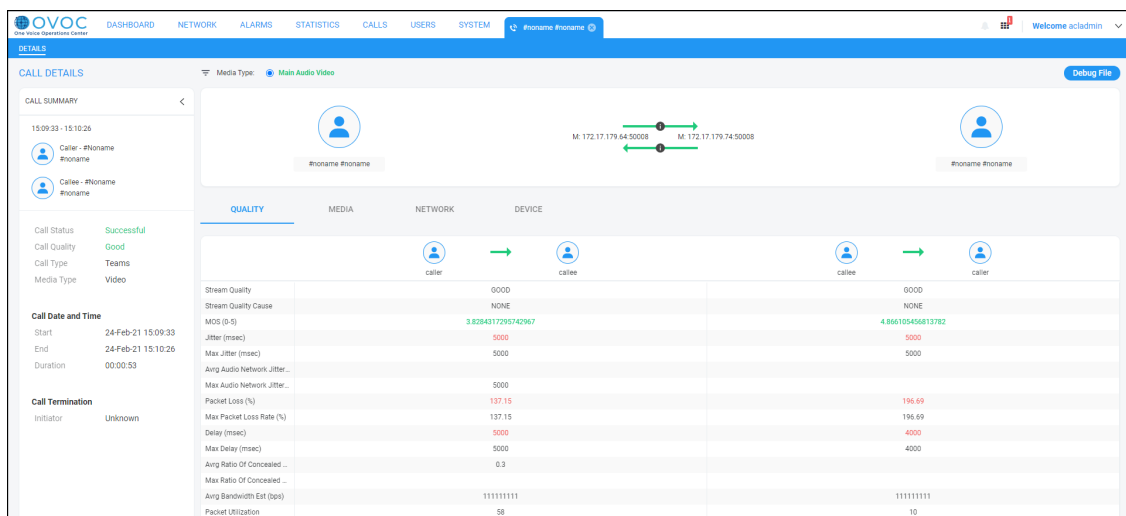
Parameter	Description
Edge Server	FQDN of the Edge server used by the user who started (caller) / joined (callee) the session.
Gateway	Gateway of the user who started (caller) / joined (callee) the session.
Mediation Server	Mediation Server of the user who started (caller) / joined (callee) the session.
URI	URI of the user who started (caller) / joined (callee) the session.
Phone Number	Phone URI of the user who started (caller) / joined (callee) the session.
Is Internal	Indicates whether the user who started (caller) / joined (callee) the session logged on from the internal network.
Front End	FQDN of the Front End server that captured the data for the session.
Pool	FQDN of the pool that captured the data for the session.

Parameter	Description
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 8-17: 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.

Page Section	Description	
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 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	<ul style="list-style-type: none"> ■ 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: 	

Page Section	Description
	<ul style="list-style-type: none"> ✓ 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)
(Lowermost) Three tabs	<p>Each tab opens a page displaying detailed information:</p> <ul style="list-style-type: none"> ■ Quality (see Quality below) ■ Media (Media tab on page 409) ■ Network (see Network on page 411) ■ Device (see Device on page 413)



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	<p>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.</p> <p>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.</p>
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

Parameter	Description
	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.
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	<p>Maximum packet loss rate for stream. Values grouped by range. 0.1 indicates 10% packet loss.</p> <p>Example value: 023: [0.09 - 0.1]</p> <p>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.</p>
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	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.

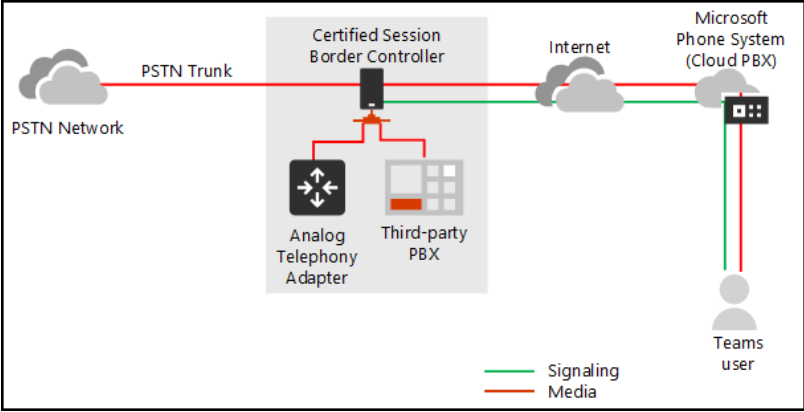
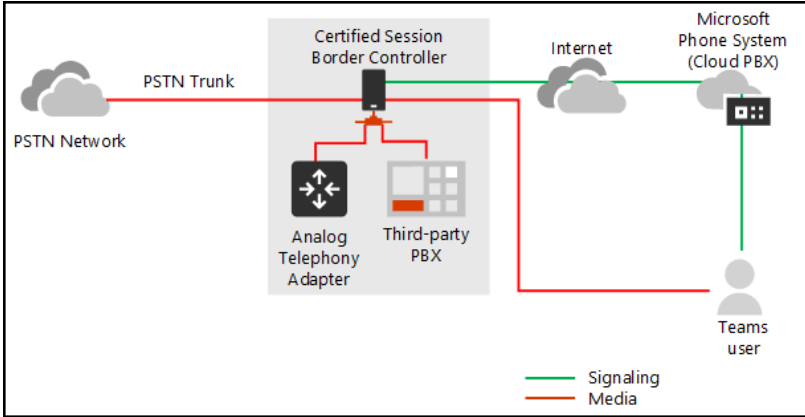
Parameter	Description
Samples	Example value: 015: [0.01 - 0.02] If the value is blank, possible reasons are (1) the value was not reported by the receiver of the stream (2) the stream was not an audio stream.
Max Ratio of Concealed Samples	The maximum seen number of audio frames with samples generated 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]
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

Parameter	Description
	<p>and the client must be in the same location or network.</p> <p>Without media bypass, when a client makes or receives a call, both signaling and media flow between the SBC, the Microsoft Phone System, and the Teams client, as shown in the following diagram:</p>  <p>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:</p> <ul style="list-style-type: none"> ■ <i>Without media bypass</i>, media will flow via either Amsterdam or Dublin (where Microsoft datacenters are deployed) and back to the SBC in Frankfurt. <p>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.</p> <ul style="list-style-type: none"> ■ <i>With media bypass</i>, the media is kept directly between the Teams user and the SBC as shown in the following diagram:  <p>Media bypass leverages protocols called Interactive Connectivity</p>

Parameter	Description
	Establishment (ICE) on the Teams client and ICE lite on the SBC. 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 Event Ratio	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.

Parameter	Description
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	<p>Wi-Fi band used as reported by the endpoint. Example value: 5.0 Ghz</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Battery Charge (%)	<p>Estimated remaining battery charge in percentage [0-99] reported by the endpoint. Values grouped by range. 0 indicates that the device was plugged in.</p> <p>Example value: 081: [90 - 100]</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Channel	<p>Wi-Fi channel used by the endpoint. Example value: 10</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ Wi-Fi was not used ■ The channel was not reported
Wi-Fi Microsoft Driver	<p>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</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported

Parameter	Description
Wi-Fi Microsoft Driver Version	<p>Version of Microsoft Wi-Fi driver reported by the endpoint. Example value: Microsoft:10.0.14393.0</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported
Wi-Fi Radio Type	<p>Type of Wi-Fi radio used by the endpoint. HRDSSS is equivalent to 802.11b.</p> <p>Example value: 802.11ac</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ Wi-Fi wasn't used ■ The driver information was not reported
Wi-Fi Signal Strength (%)	<p>Wi-Fi signal strength in percentage [0-100] reported by the endpoint. Example value: 081: [90 - 100]</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ The value was not computed by the endpoint ■ The value was not reported
Wi-Fi Vendor Driver	<p>Vendor and name of WiFi driver reported by the first endpoint. Example value: Contoso Dual Band Wireless-AC Driver.</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ Wi-Fi wasn't used by the endpoint ■ The driver information was not reported
Wi-Fi Vendor Driver Version	<p>Version of Microsoft WiFi driver reported by the first endpoint. Example value: Microsoft:10.0.14393.0</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ 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

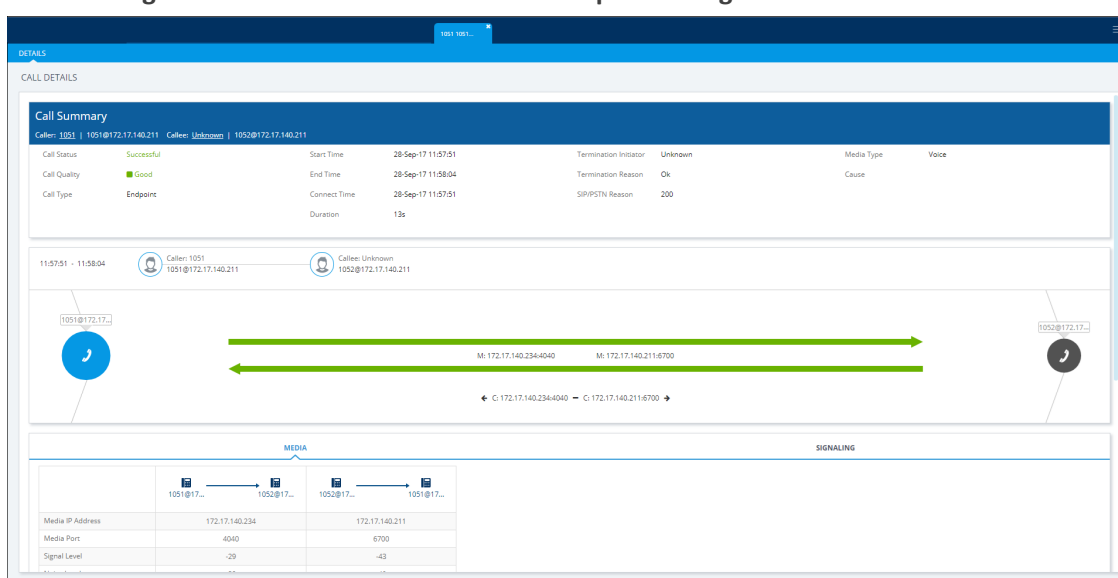
Parameter	Description
Capture Device Driver	<p>Name of the capture device driver used by the endpoint in the form of "manufacturer : version".</p> <p>For:</p> <p>Audio streams = driver used for the microphone</p> <p>Video streams = driver used for the camera</p> <p>Video-based-screen-sharing and app sharing streams = blank</p> <p>Example value: Microsoft: 10.0.14393.0</p> <p>Possible reasons for blank values:</p> <ul style="list-style-type: none"> ■ 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 Insufficient 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.
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.

Parameter	Description
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 interval 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 8-18: 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
Call Quality	Good Fair Poor voice quality
Call Type	Endpoint
Start Time	The precise time (hour, minutes and seconds) and date (month, day

Page Section	Description	
	and year) when the caller began dialing the number to call.	
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.	
Duration	The duration of the call, in seconds.	
Termination Initiator	The network entity from which the call was terminated.	
Termination Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.	
SIP PSTN Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about the SIP/PSTN Reason.	
Media Type	Voice	
[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.

Page Section	Description	
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
(Middle) Graphic illustration	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ✓ Connected to a device ✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✓ Tagged by C and M <ul style="list-style-type: none"> C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip) 	
(Lowermost) Two tabs	<p>Each opens a page displaying detailed information:</p> <ul style="list-style-type: none"> ■ Media (see Media on the next page) ■ Signaling (see Signaling on page 388) 	

Media

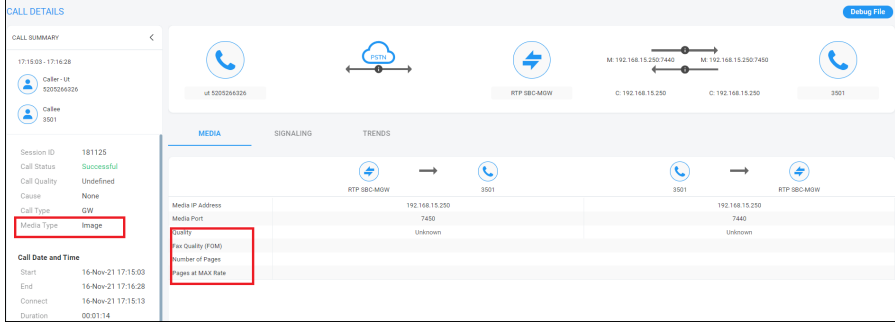
The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-19: Media

DETAILS		
CALL DETAILS		
MEDIA		
	1051@17...	1052@17...
	1052@17...	1051@17...
Media IP Address	172.17.140.234	172.17.140.211
Media Port	4040	6700
Signal Level	-29	-43
Noise Level	-38	-40
SNR	9	-3
Rx Rate	62	62
Quality	GOOD	GOOD
MOS	4.3	4.3
Jitter	10	10
Packet Loss		
Delay	10	8
Echo		
Coder	G727_32_16	
SCE	false	
RTP Direction	Send Receive	
RTCP Direction	Send Receive	
P-Time	20	

Use the following table as reference.

Table 8-19: Media Parameters

Parameter	Description
Media IP Address	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. Port of the destination host / media network.
Quality Fax Quality Number of Pages Pages at MAX Rate	
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference.

Parameter	Description
	Signal level = $10 \log_{10}$ (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 = $10 \log_{10}$ (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). $SNR = \text{Signal level} - \text{Noise level}$.
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

Parameter	Description
	of supported coders.
SCE	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).
RTP Direction	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Direction	RTCP Directional Control. Controlled internally by the device according to the selected coder.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.

Managing QoE Thresholds Profiles

The QoE Thresholds page lets you adding a profile of Quality of Experience threshold values, *per tenant scope*. For information about adding a *global* (system) QoE Thresholds template, see [Configuring QoE Thresholds](#) on page 92.

➤ **To view QoE thresholds profiles:**

1. Access the relevant Tenant or Global scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the QoE Thresholds page (**System** menu > **Configuration** tab > **Profiles** folder > **QoE Thresholds**).

Figure 8-20: QoE Thresholds Profiles

QOE THRESHOLDS											
DEFAULTS	NAME	TENANT	MOS (0-5)	DELAY (MSEC)	PLOSS (%)	JITTER (MSEC)	ECHO (DB)	DESCRIPTION		QOE THRESHOLDS DETAILS	
	MS Teams Thresholds	Tenant_30	4	500	10	30					
	MS Teams Thresholds	Zipora	4	500	10	30					
	MS Teams Thresholds	Tenant_31	4	500	10	30					
	MS Teams Thresholds	Tenant_2	4	500	10	30					
	MS Teams Thresholds	Tenant_32	4	500	10	30					
	MS Teams Thresholds	Tenant_33	4	500	10	30					
	MS Teams Thresholds	Tenant_34	4	500	10	30					
	MS Teams Thresholds	Tenant_35	4	500	10	30					
	Low Sensitivity Threshold	Teams	3.4	200	2.7	45	23				
	Medium Sensitivity Threshold	Teams	3.5	160	2	40	25				
	High Sensitivity Threshold	Teams	3.6	140	1.5	35	27				
	MS Teams Thresholds	Teams	4	500	10	30					
	Low Sensitivity Threshold	Teams2	3.4	200	2.7	45	23				
	Medium Sensitivity Threshold	Teams2	3.5	160	2	40	25				
	High Sensitivity Threshold	Teams2	3.6	140	1.5	35	27				
	MS Teams Thresholds	Teams2	4	500	10	30					
	Low Sensitivity Threshold	Teams3	3.4	200	2.7	45	23				
	Medium Sensitivity Threshold	Teams3	3.5	160	2	40	25				
	High Sensitivity Threshold	Teams3	3.6	140	1.5	35	27				
	MS Teams Thresholds	Teams3	4	500	10	30					
	Low Sensitivity Threshold	Teams4	3.4	200	2.7	45	23				
	Medium Sensitivity Threshold	Teams4	3.5	160	2	40	25				
	High Sensitivity Threshold	Teams4	3.6	140	1.5	35	27				
	MS Teams Thresholds	Teams4	4	500	10	30					

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 424)
- edit or delete an existing profile (see [Editing a QoE Thresholds Profile](#) on page 428 and [Deleting a QoE Thresholds Profile](#) on page 429)

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 to understand better how 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 (**System** menu > **Configuration** tab > **Profiles** folder > **QoE Thresholds**).
2. Click **Add**.

Figure 8-21: QoE Thresholds Details

QOE THRESHOLDS DETAILS

Threshold Name* _____ Description _____

Tenant*
A

ATTACHMENTS

0 Devices, 0 Links, 0 Endpoints
[View](#)

DEFAULTS

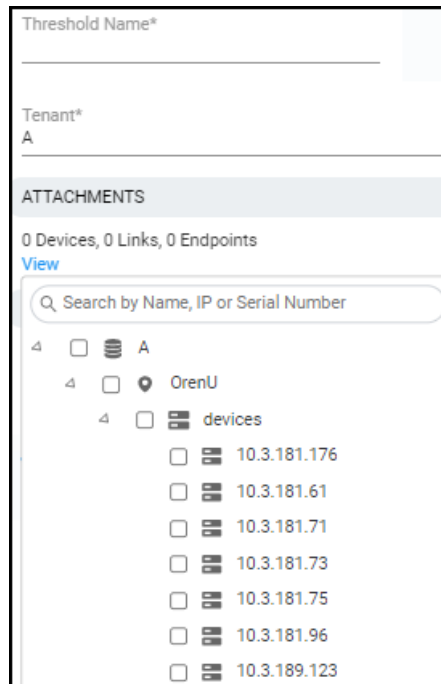
☐ Device ☐ Link ☐ Endpoint

VOICE **VIDEO**

<input checked="" type="checkbox"/> MOS (0-5)	→ 3.5 →	→ 2.5 →
<input checked="" type="checkbox"/> Delay (msec)	→ 160 →	→ 500 →
<input checked="" type="checkbox"/> Packet Loss (%)	→ 2 →	→ 5 →
<input checked="" type="checkbox"/> Jitter (msec)	→ 40 →	→ 80 →
<input checked="" type="checkbox"/> Echo (dB)	→ 25 →	→ 10 →

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. Under 'Attachments', click **View**.

Figure 8-22: 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 8-23: QoE Thresholds Settings - Medium Sensitivity Threshold

QOE THRESHOLDS DETAILS

Threshold Name	Description
Medium Sensitivity Threshold	

Tenant
MosheL

ATTACHMENTS

0 Devices, 0 Links, 0 Endpoints
[View](#)

DEFAULTS

☒ Device ☒ Link ☒ Endpoint

	VOICE	VIDEO
<input checked="" type="checkbox"/> MOS (0-5)	→ 3.5 →	→ 3 →
<input checked="" type="checkbox"/> Delay (msec)	→ 160 →	→ 500 →
<input checked="" type="checkbox"/> Packet Loss (%)	→ 2 →	→ 5 →
<input checked="" type="checkbox"/> Jitter (msec)	→ 40 →	→ 80 →
<input checked="" type="checkbox"/> Echo (dB)	→ 25 →	→ 10 →

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 8-24: QoE Thresholds Details

QOE THRESHOLDS DETAILS

DEFAULTS

NAME

TENANT

Voice

MOS (0-5)

DELAY (MSEC)

PACKET LOSS (%)

JITTER (MSEC)

ECHO (DB)

Attached Items

DEVICE

LINK

ENDPOINTS

DEFAULT DEVICE

DEFAULT LINK

DEFAULT ENDPOINTS

Medium Sensitivity Threshold

eli7

3.5

3

160

500

2

5

40

80

25

10

0

0

0

11

1

11

13. Shown in the preceding figure, view in the QoE Thresholds Details pane 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

14. In the QoE Thresholds Details pane for the MS Teams Thresholds profile, you'll also view **Video** details (in addition to **Voice**).

Figure 8-25: QoE Thresholds Details - Video

QOE THRESHOLDS DETAILS

DEFAULTS

NAMEMS Teams Thresholds

TENANTqwq

Voice

MOS (0-5)

4

4

DELAY (MSEC)

500

500

PACKET LOSS (%)

10

10

JITTER (MSEC)

30

30

Video

AVG VIDEO FRAME LOSS PERCENTAGE (%)

50

50

AVG VIDEO FRAME RATE (FPS)

7

7

POST FORWARD ERROR CORRECTION PACKET LOSS RATE

0.15

0.15

Screen Sharing

AVG VIDEO FRAME LOSS PERCENTAGE (%)

50

50

AVG VIDEO FRAME RATE (FPS)

2

2

POST FORWARD ERROR CORRECTION PACKET LOSS RATE

0.15

0.15

Attached Items

DEVICE0

LINK0

ENDPOINTS0

DEFAULT DEVICE0

DEFAULT LINK0

DEFAULT ENDPOINTS0

Editing a QoE Thresholds Profile

You can edit an existing QoE Thresholds profile for a specific Tenant.

➤ To edit a QoE Thresholds profile:

- In the QoE Thresholds page (**System** menu > **Configuration** tab > **Profiles** folder > **QoE Thresholds**), select the profile to edit and then click **Edit**; the screen shown under [Adding a QoE Thresholds Profile per Tenant](#) on page 424 opens. Refer to the instructions under the figure.

Deleting a QoE Thresholds Profile

You can delete a QoE Thresholds profile for a tenant.

➤ **To delete a QoE Thresholds profile:**

- In the QoE Thresholds page (**System** menu > **Configuration** tab > **Profiles** folder > **QoE Thresholds**), select the profile to delete and then click **Delete**. Note that default profiles cannot be deleted.

Managing QoE Status and Alarms

The QoE Status & Alarms page enables you manage QoE statuses and alarms *per tenant scope*. For information about managing *global (system-wide)* QoE statuses and alarms, see [Configuring QoE Status and Alarms](#) on page 97.

➤ To view QoE statuses and alarms:

1. Select Tenant or Global scope (see [here](#) for more information).
2. Open the QoE Status & Alarms page (**System > Configuration > Profiles > QoE Status & Alarms**).

QOE STATUS & ALARMS											Add Edit Delete	
DEFAULTS	NAME	TENANT	LAST RUNTIME	MONITO...	MINIMEL...	FAILED CALLS PRO...	POOR QUALITY CAL...	AVERAGE CALL DU...	BANDWIDTH RULE (...)	MAX CONCURRENT...	DESCRIPTION	QOE ALARMS DETAILS
ALARM RULE	Tenant_1	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_2	18-Mar-21 10:10:00	15	50	1	1	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_3	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_4	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_5	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_6	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_7	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_8	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_9	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_10	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_11	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_12	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_13	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_14	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_15	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_16	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_17	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_18	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_19	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_20	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_21	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_22	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_23	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS
ALARM RULE	Tenant_24	18-Mar-21 10:10:00	15	50	2	2	5	0	0	1		QOE ALARMS DETAILS

3. View the information displayed in the page. Information about QoE Status & Alarms *per tenant* is identical to information displayed in the *global (system-wide)* QoE Status & Alarms page. See [Configuring QoE Status and Alarms](#) on page 97 for a detailed description.

Adding a QoE Alarm Rule per Tenant

A rule for a QoE alarm can be added per tenant.

➤ To add a QoE alarm rule per tenant:

1. Open the QoE Status & Alarms Details screen (**System > Configuration > Profiles > QoE Status & Alarms**), and then click **Add**.

QOE STATUS & ALARMS DETAILS

Name*

Description

Tenant*

A

Monitoring Frequency Min

15

Minimum Call Per Entity To Analyze

50

ATTACHMENTS

0 Devices, 0 Links, 0 Sites, 0 Endpoints
[View](#)

DEFAULTS

☐ Device
☐ Link
☐ Site
☐ Endpoint

THRESHOLD VALUES

	Status Threshold Values		Generate Alarm	
Failed Calls Alarm (Calls %)	→ 2 →	→ 10 →	<input checked="" type="checkbox"/>	
Poor Quality Calls Alarm (Calls %)	→ 2 →	→ 10 →	<input checked="" type="checkbox"/>	
Avg Call Duration Alarm (sec)	→ 5 →	→ 3 →	<input checked="" type="checkbox"/>	
Bandwidth Alarm (Kb/sec)	→ 5 →	→ 10 →	<input type="checkbox"/>	
Max Concurrent Calls Alarm (Calls #)	→ 5 →	→ 10 →	<input type="checkbox"/>	

- Configure the parameters using the following table as reference.

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. <ul style="list-style-type: none"> 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 OVOC automatically performs data analysis. Defines every 15 (default), 30 or 60 minutes.

Parameter	Description
Minimum Calls to Analyze	<p>Defines the number of calls to analyze. Default = 50 calls. Up to 1000 calls can be defined.</p> <p>If the number of calls made doesn't exceed the defined # of calls to analyze, OVOC won't perform data analysis.</p>
Failed Calls Alarm	<p>Select the Generate Alarm option to activate the alarm. Clear the option to deactivate the alarm.</p> <p>Critical Threshold: 5% of calls (default); if this threshold is exceeded, the alarm is triggered.</p> <p>Major Threshold: 3% of calls (default); if this threshold is exceeded, the alarm is triggered.</p>
Poor Quality Calls Alarm	<p>Select the Poor Quality Calls Alarm option to activate the alarm. Clear the option to deactivate the alarm.</p> <p>Critical Threshold: 10% of calls (default); if this threshold is exceeded, the alarm is triggered.</p> <p>Major Threshold: 8% of calls (default); if this threshold is exceeded, the alarm is triggered.</p>
Avg Call Duration Alarm	<p>Select the Avg Call Duration Alarm option to activate the alarm. Clear the option to deactivate the alarm.</p> <p>Critical Threshold: 5 seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered.</p> <p>Major Threshold: 10 seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered.</p>
Bandwidth Alarm	<p>Select the Bandwidth Alarm option to activate the alarm. Clear the option to deactivate the alarm.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ■ You must configure a <i>higher</i> value for the <i>Critical</i> 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 <i>Critical</i> Threshold is higher than the value you configure for the Major Threshold.
Max Concurrent	Select the Max Concurrent Calls Alarm option to activate the alarm.

Parameter	Description
Calls Alarm	<p>Clear the option to deactivate the alarm.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ■ You must configure a <i>higher</i> value for the <i>Critical</i> 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 <i>Critical</i> Threshold is higher than the value you configure for the Major Threshold.
Failed Calls Device (Calls %)	<p>[Not shown in the preceding figure, you need to scroll down to it]</p> <p>Enables forwarding an alarm if the reason for a terminated call is related to an AudioCodes SBC or Media Gateway. See also here for more information.</p>
Failed Calls 3rd Party (Calls %)	<p>[Not shown in the preceding figure, you need to scroll down to it]</p> <p>Enables forwarding an alarm if the reason for a terminated call is related to a third-party device. See also here for more information.</p>

3. Click **OK**; the QoE alarm rule is now listed in the QoE Status & Alarms page.

Editing a QoE Alarm Rule per Tenant

A QoE alarm rule per tenant can be edited if necessary.

➤ To edit a QoE alarm rule per tenant:

- In the QoE Status & Alarms page (**System** menu > **Configuration** tab > **Profiles** folder > **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

A QoE alarm rule can be deleted if necessary.

➤ To delete a QoE alarm rule:

- In the QoE Status & Alarms page (**System** menu > **Configuration** tab > **Profiles** folder > **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

OVOC enables you to get information on how end users experience IP network telephony.



- Information related to Teams users, which includes users' personal data as well as QoE reports, requires adding a Teams device to OVOC. See the *OVOC IOM* for more information.
- 'End users' refers to an enterprise's employees. By contrast, 'operators' refers to administrators managing the enterprise's network using OVOC.

[Adding an Active Directory to OVOC](#) below shows how to add an Active Directory in the Active Directories page.

[Assessing Overall End Users Experience](#) on page 441 and [Assessing a Specific End User's Experience](#) on page 443 show how to get user experience info in the Users Experience page.

[Adding an Active Directory to OVOC](#) below shows how to manage end users in the User Details page.

Figure 9-1: Getting Information on Users

FILTERS	FULL NAME	USER NAME	DESCRIPTION	CALLS COUNT	TOTAL DURATION	SUCCESSFUL/FAILED	CALL QUALITY	MOS	JITTER	DELAY	PACKET LOSS	TENANT
ADD FILTER	newAdmin	newAdmin		20,058	07h 43m	<div><div></div></div>	4.3	4.3	2758.5	3566.6	5.7	Tenant_L41
	FAE1	FAE1		20,084	07h 47m 32s	<div><div></div></div>	4.3	4.3	2724.4	3592.5	5.7	Tenant_L41

Adding an Active Directory to OVOC

OVOC lets you connect to customer tenant Active Directories for managing the Quality of Experience of associated users.

➤ To add an Active Directory to OVOC:

1. Access the Global scope or relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Active Directory page (**Users > Active Directories**).

Figure 9-2: Active Directories

ACTIVE DIRECTORIES		ACTIVE DIRECTORY DETAILS	
<div> <div>EMS-AD-QA-EMS-LOCAL</div> <div>151863 users</div> </div>	<div> <div>ADD</div> <div>EDIT</div> <div>Sync Now</div> <div>Details</div> <div>Refresh</div> </div> <div> <div>Last update: 28-Dec-21 09:41:35</div> </div>	<div>NAME</div> <div>EMS-AD-QA-EMS-LOCAL</div>	<div>STATUS</div> <div>Connected</div>
		<div>IS ENABLED</div> <div>Yes</div>	<div>TENANT</div> <div>Tenant_L41</div>
		<div>USERS</div> <div>151863</div>	<div>HOST</div> <div>10.2.190.11</div>
		<div>PORT</div> <div>389</div>	<div>SSL ENABLED</div> <div>false</div>
		<div>DN</div> <div>Admin@QA-EMS-LOCAL</div>	<div>BASE OBJECT</div> <div>OU=QA,DC=QA-EMS,DC=LOCAL</div>
		<div>TIME</div> <div>1 hour</div>	<div>LAST</div> <div>28-Dec-21 09:41:35</div>
		<div>FULL SYNC</div> <div>0.0</div>	<div>AT</div> <div>0.0</div>
		<div>EVERY</div> <div>3 days</div>	<div>LAST</div> <div>28-Dec-21 02:13:18</div>

3. Click **Add**.

Figure 9-3: Active Directory Details

ACTIVE DIRECTORY DETAILS

General Synchronization

Name* _____ Description _____

Tenant*
Tenant_27 ▼

Active Directory Type
LDAP ▼

Host* _____ Port*
389

Base object* _____

Bind DN* _____ Password* _____

☐ Enable SSL

Certificate File _____

☐ Verify Certificate Subject Name

Test Connectivity

Figure 9-4: Active Directory Details - Azure

ACTIVE DIRECTORY DETAILS

General Synchronization

Name* _____ Description _____

Tenant*
dalia ▼

Active Directory Type
Azure ▼

Azure Tenant ID* _____ Client ID* _____ Client Secret* _____

4. Configure the **General** settings using the following table as reference.

Table 9-1: Active Directory Details - 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

Setting	Description
	Adding a Tenant on page 133.
Active Directory Type	From the drop-down, select LDAP or Azure depending on the infrastructure of the enterprise.
Host	[Applies only to LDAP] Consult with the IT manager responsible for the AD in your enterprise.
Port	[Applies only to LDAP] The default is typically 389 but consult with the IT manager responsible for the Active Directory in your enterprise.
Base object	[Applies only to LDAP] Enterprise employees are listed under branches/departments in a tree structure. Enter in the field the branch/department whose employees the AD manages. The AD will then access only to that (relevant) branch/department's employees. For more information, consult with the IT manager responsible for the Active Directory in your enterprise.
Bind DN	[Applies only to LDAP] For the 'DN' (Domain Name) field, consult with the IT manager responsible for the Active Directory in your enterprise.
Password	[Applies only to LDAP] Consult with the IT manager responsible for the AD in your enterprise.
Enable SSL	[Applies only to LDAP] Select the option to secure the connection with the AD server over SSL; an HTTPS connection between OVOC and the LDAP server is opened. Clear (default) the option for the connection with the LDAP server to be non-secured.
Certificate file	[Applies only to LDAP] 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. 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 OVOC Software Manager on page 114.
Test connectivity	[Applies only to LDAP] Click to test synchronization of OVOC and the Active Directory databases. You can alternatively click Sync Now in the Active Directories page.
Verify Certificate	[Applies only to LDAP] This option is only activated if the 'Enable

Setting	Description
Subject Name	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 OVOC server and the LDAP server.
Azure Tenant ID	[Applies only to Azure] For each enterprise that purchases Azure services or any other service, Microsoft defines a 'micro' enterprise cloud with an identifier – a Tenant ID. In the 'Azure Tenant ID' field, enter this ID. It represents the 'micro' enterprise cloud: Azure. Defining this environment is necessary for permissions. See also Adding a Microsoft Teams Device Manually on page 169.
Client ID	[Applies only to Azure] Microsoft generates a Client ID for a specific application - OVOC, in this case - to allow OVOC access with MS Graph API (subscription creation or call record retrieving). In the 'Client ID' field, enter the OVOC application's 'user name'. See also Adding a Microsoft Teams Device Manually on page 169.
Client Secret	[Applies only to Azure] Microsoft generates a Client ID for a specific application - OVOC, in this case - to allow the application access with a graph API. In the field, define the shared secret - the 'password' - to allow OVOC application access to the specific 'micro' enterprise cloud. Must be cryptically strong. OVOC will then be capable of accessing Azure. See also Adding a Microsoft Teams Device Manually on page 169.

- Click the **Synchronization** tab.

Figure 9-5: Active Directory Details - Synchronization

ACTIVE DIRECTORY DETAILS

General **Synchronization**

Check for updates every (hours)
1

PERFORM FULL UPDATE EVERY

Days 3 Hours 0 Minutes 0

- Configure the settings using the following table as reference.

Table 9-2: Active Directory Details - Synchronization

Setting	Description
Check for updates every (hours)	Lets you schedule how frequently synchronization of OVOC and the Active Directory databases takes place. After synchronization is performed, OVOC's User Details page is updated to reflect the Active Directory.
Perform full update every	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, OVOC's User Details page is updated to reflect the Active Directory.
Hours Minutes	Lets you schedule the time at which the full synchronization is performed. After it's performed, OVOC's User Details page is updated to reflect the Active Directory.

7. Click **OK**.

Editing an Active Directory

You can edit the settings for an existing Active Directory configuration.

➤ To edit an Active Directory:

1. Access the Global scope or relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Active Directory page (**Users > Active Directories**).

The screenshot displays the OVOC web interface for managing Active Directories. The top navigation bar includes links for DASHBOARD, NETWORK, ALARMS, PERFORMANCE MONITORING, QUALITY OF EXPERIENCE, USERS, and SYSTEM. The 'USERS' section is active, leading to the 'ACTIVE DIRECTORIES' page. This page features a table of configured Active Directories and a detailed sidebar for the selected 'audiocodes' directory.

NAME	STATUS	TENANT	USERS	HOST	PORT	SSL ENABLED	DN	BASE OBJECT
audiocodes	Connected	rest_example_tenant...	4266	10.1.1.6	389	false	ldap_bind@CORPAUDICODES...	dc=corp,dc=audiocodes,dc=com

ACTIVE DIRECTORY DETAILS

- NAME:** audiocodes
- STATUS:** Connected
- IS ENABLED:** Yes
- TENANT:** rest_example_tenant...
- USERS:** 4266
- HOST:** 10.1.1.6
- PORT:** 389
- SSL ENABLED:** false
- DN:** ldap_bind@CORPAUDICODES...
- BASE OBJECT:** dc=corp,dc=audiocodes,dc=com

Sync Settings:

- EVERY:** 1 hour
- LAST:** 24-Aug-23 10:31:36

Full Sync Settings:

- AT:** 00:00
- EVERY:** 3 days
- LAST:** 24-Aug-23 00:00:40

3. Select the Active Directory to edit and then click the activated **Edit** button.

Figure 9-6: Active Directory Details

ACTIVE DIRECTORY DETAILS

General

Synchronization

Name	Description
audiocodes	

Tenant
rest_example_tenant__

Active Directory Type
LDAP

Host
10.1.1.6

Port
389

Base object
dc=corp,dc=audiocodes,dc=com

Bind DN
ldap_bind@CORP.AUDIOCODES.COM

Password

☐ Enable SSL

Test Connectivity

Close

OK

4. Edit the parameters under **General** and/or under **Synchronization** using the tables in [Adding an Active Directory to OVOC](#) on page 435 as reference, and then click **OK**.

Deleting an Active Directory

You can delete an Active Directory if necessary.

➤ To delete an Active Directory:

1. Access the Global scope or relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Active Directory page (**Users > Active Directories**).
3. Select the Active Directory to delete and then click the activated **Delete** button.

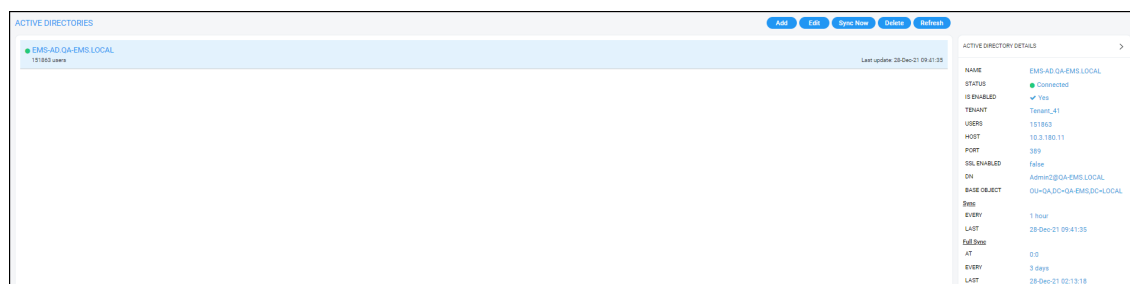
Synchronizing AD Users with the Server

You can manually synchronize with a specific AD to retrieve an updated list of associated users.

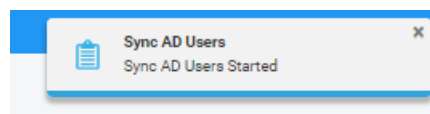
➤ To synchronize AD users with the server:

1. Access the Global scope or relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Active Directories page (**Users > Active Directories**).

Figure 9-7: Active Directories



3. Select the Active Directory to synchronize and then click the **Sync Now** button; view the 'Sync AD Users Started' prompt in the upper right corner of the screen.



Assessing Overall End Users Experience

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. Access the relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).

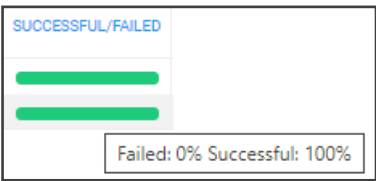
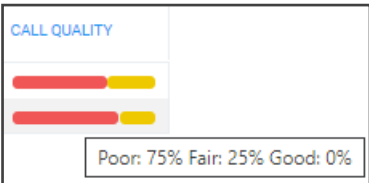
2. Open the Users Experience page (**Users** menu > **Users Experience** tab).

Figure 9-8: Users Experience

	FULL NAME	USER NAME	DESCRIPTION	CALLS COUNT	TOTAL DURATION	SUCCESSFUL/FAILED	CALL QUALITY	MOS	JITTER	DELAY	PACKET LOSS	TENANT
	Adele Vance	adev@G4505018210.onlinetech.com		0	01m 55s	<div><div></div></div>	<div><div></div></div>	3.3	69	51.3	7.4	T2
	Jeron Engering	jer.Engering@acthocommunications.eu		8	02m 19s	<div><div></div></div>	<div><div></div></div>	3.2	93.8	42	7.7	T2

3. [Optional] Filter the page to present only information you require. You can filter by Time Range (see [Filtering to Access Specific Information](#) on page 231) or by Users (see [Filtering the User Details Page](#) on page 447).
4. Use the following table as reference to the page.

Table 9-3: Users Experience

Column	Description
Full Name	The first name and the family name of the end user (the employee) in the enterprise.
User Name	The employee's user name, defined by the enterprise's network administrator.
Calls Count	The total number of calls made by the end user (employee).
Total Duration	The total length of time the end user (enterprise employee) spent on the phone.
Success/Failed	Color-coded bar lets you determine at glance the call success/failure rate (percentage) was for end users. Point your cursor over a specific end user's bar to see the rate of successful versus unsuccessful calls. 
Call Quality	Lets you determine at glance end users calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red). Point your cursor over a specific end user's bar to see that specific end user's % of calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red). 
MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800)

Column	Description
	- 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.

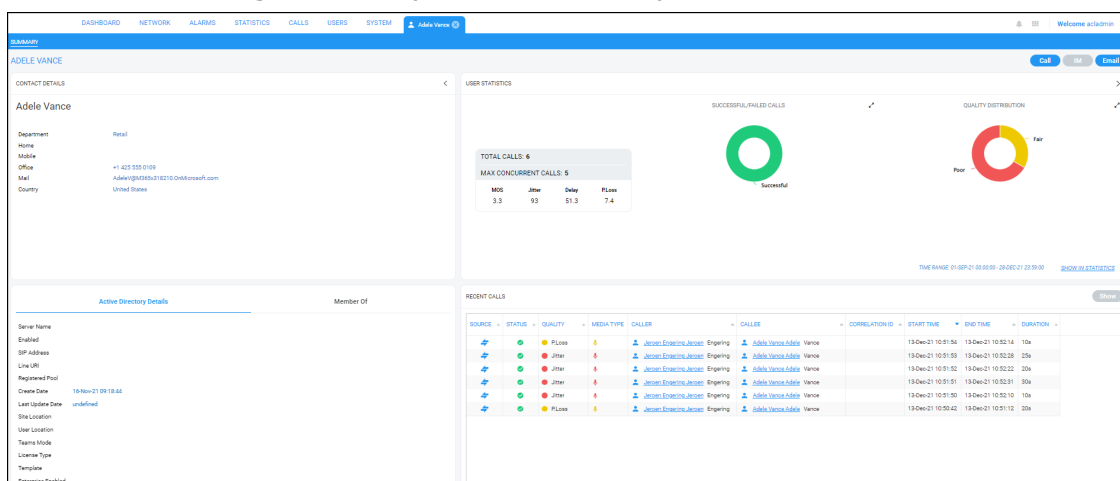
5. [Optional] Select an end user's row and then click **Show**; details about that specific user's experience are displayed.
6. [Optional] Click **Refresh** to manually synchronize the page with the Active Directory.

Assessing a Specific End User's Experience

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. Access the relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Users Experience page (**Users** menu > **Users Experience** tab).
3. 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 9-9: Specific End User's Experience

4. 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 **Adele Vance...** in the page shown above, facilitating quick and easy future access and troubleshooting management. The pin can be deleted from the menu bar at any time.

Filtering the Users Experience Page

Filter the User Details page using the following options:

Filter	Description
Filtering by Time Range	<ul style="list-style-type: none"> Filtering by 'Time Range' on page 232
Topology Groups	
Pin all selected	<ul style="list-style-type: none"> Check the option for the filter to 'follow' you when navigating between pages that feature the same filter. Clear the option for the filter to only apply to this page.
Topology Groups	From the drop-down, select a Topology Group to filter the page by; only the details of those users who are associated with the selected Topology Group are displayed in the page. See also Adding a Topology Group on page 191.
More Filters	
Tenants	From the drop-down, select a configured tenant. Only the details of users assigned to this tenant are displayed in the page.
Name	Enter the name of a user - or enter only part of a user's name; only the details of that user - or those users - whose name contains the value you entered are displayed in the page.

Filter	Description
Country	Enter the name of a country. Only the details of users in that country are displayed in the page.
Department	Enter the name of a department in the enterprise. Only the details of users in this department are displayed in the page.
Line URI	Enter a line URI - or enter only part of the line URI; only the details of that user - or those users - whose line URI contains the value you entered (i.e., part of whose line URI matches what you entered) are displayed in the page.
Active Directory	
Pin all selected	See above under 'Groups'.
Active Directories	From the drop-down, select an Active Directory; the details of users associated with this Active Directory are displayed.
User Locations	From the drop-down, select a User Location; the details of users associated with this user user location are displayed.

Managing End Users



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

Username and passwords of end users are by default locally stored in the OVOC application's database. The User Details page allows operators to locally manage end users. The page mirrors the Active Directory. Any change to the AD is reflected in the User Details page immediately after synchronization is performed.

➤ To manage end users:

1. Access the relevant Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the User Details page (**Users** menu > **User Details** tab).

Figure 9-10: User Details

USER DETAILS																
FULL NAME	USER NAME	DESCRIPTION	DEPARTMENT	OFFICE PHONE	MOBILE	LINE URI	EMAIL	SERVER	CUSTOMER	COUNTRY	SITE LOCATION	USER LOCATION	TEAMS MODE	LICENSE TYPE	TEMPLATE	ENTERPRISE ENABLED
AC user		some desc	AC				mail.com		2222221	US						
AC user		some desc 2	AC 2				mail.com		2222221	US	name	location	teams_mode	license_type	template	✓
Conf Room Adams	Adams@M0955-018210-DnMora...						Adams@M0955-018210-DnMora...		2222221	United Stat...						testOC
Adela Vance	AdelaV@M0955-018210-DnMora...		Retail	+1 425 555 5109			AdelaV@M0955-018210-DnMora...		2222221	United Stat...						T2
MOD Administrator	admin@M0955-018210-DnMora...			425-555-0100	425-555...		admin@M0955-018210-DnMora...		2222221	NL						testOC
Alex Wilbur	AlexW@M0955-018210-DnMora...		Marketing	+1 800 555 5110			AlexW@M0955-018210-DnMora...		2222221	United Stat...						testOC
Allen DeYoung	AllenD@M0955-018210-DnMora...		IT	+1 202 555 5109			AllenD@M0955-018210-DnMora...		2222221	United Stat...						testOC
Automate Bot	AutomateB@M0955-018210-DnMora...						AutomateB@M0955-018210-DnMora...		2222221	United Stat...						testOC
Conf Room Baker	Baker@M0955-018210-DnMora...						Baker@M0955-018210-DnMora...		2222221	United Stat...						testOC
Bianca Pizarri	BiancaP@M0955-018210-DnMora...		Sales	+1 425 555 5100			BiancaP@M0955-018210-DnMora...		2222221	United Stat...						testOC
Brian Johnson (THALPHE)	BrianJ@M0955-018210-DnMora...						BrianJ@M0955-018210-DnMora...		2222221	United Stat...						testOC

3. Optionally, use filters for quick access to specific users.
4. 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

Filter the User Details page using the following options:

The image displays three filter panels for the User Details page:

- GROUPS Panel:** Features a 'Pin all selected' checkbox (checked) and a 'Topology Groups' drop-down menu.
- MORE FILTERS Panel:** Includes a 'Tenants' drop-down menu, 'Full Name', 'Country', 'Department', and 'Line URI' text input fields.
- ACTIVE DIRECTORY Panel:** Includes a 'Pin all selected' checkbox (checked), an 'Active Directories' drop-down menu, and a 'User Locations' drop-down menu.

Table 9-4: User Details page filters

Filter	Description
Topology Groups	
Pin all selected	<ul style="list-style-type: none"> Check the option for the filter to 'follow' you when navigating between pages that feature the same filter. Clear the option for the filter to only apply to this page.
Topology Groups	From the drop-down, select a Topology Group to filter the page by; only the details of those users who are associated with the selected Topology Group are displayed in the page. See also Adding a Topology Group on page 191.
More Filters	
Tenants	From the drop-down, select a configured tenant. Only the details of users assigned to this tenant are displayed in the page.

Filter	Description
Name	Enter the name of a user - or enter only part of a user's name; only the details of that user - or those users - whose name contains the value you entered are displayed in the page.
Country	Enter the name of a country. Only the details of users in that country are displayed in the page.
Department	Enter the name of a department in the enterprise. Only the details of users in this department are displayed in the page.
Line URI	Enter a line URI - or enter only part of the line URI; only the details of this user - or those users - whose line URI contains the value you entered (i.e., part of whose line URI matches what you entered) are displayed in the page.
Active Directory	
Pin all selected	See above under 'Groups'
Active Directories	From the drop-down, select an Active Directory; the details of users associated with this Active Directory are displayed in the page.
User Locations	From the drop-down, select a User Location; the details of users associated with this user location are displayed.

10 Managing Reports

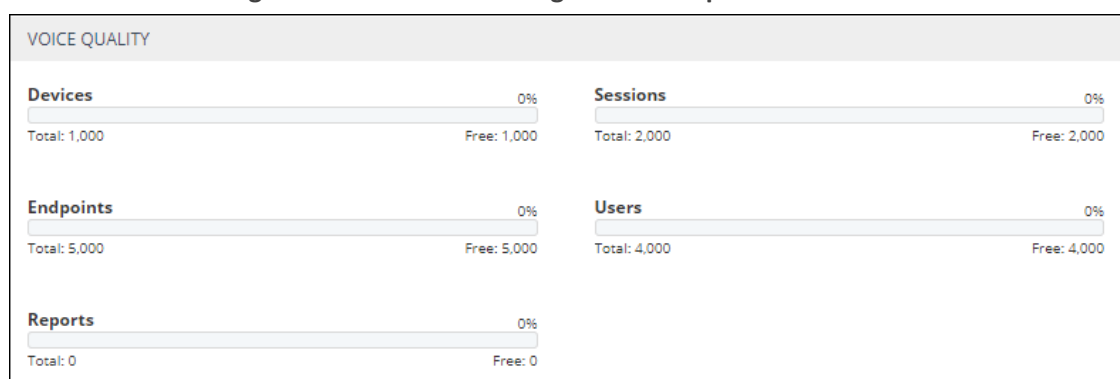
OVOC allows administrators to produce reports that can be used to distribute information about IP telephony performance and quality of experience across the enterprise and to external authorities, for accurate diagnosis, correction of issues and optimization.

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.

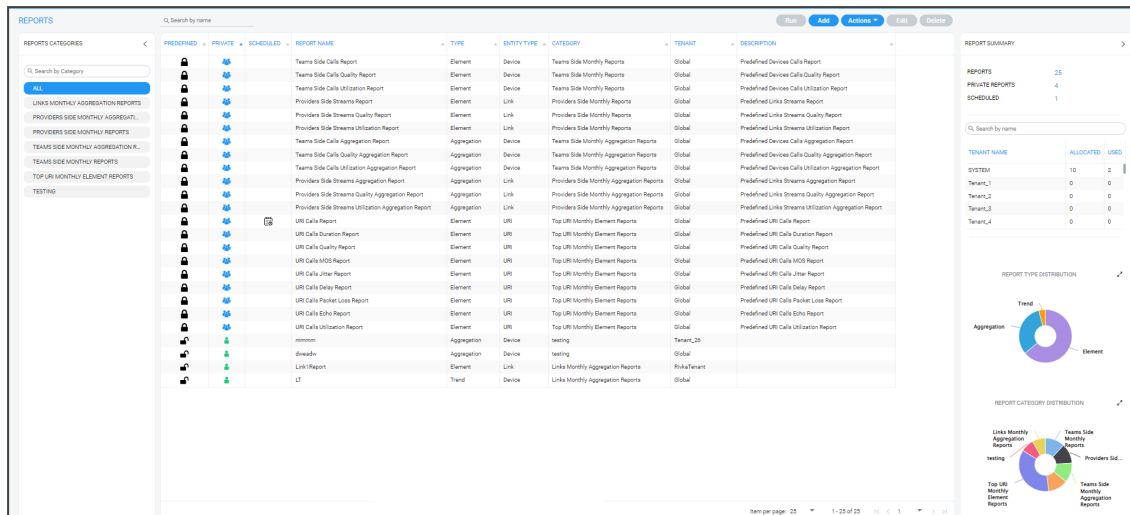
In the Reports page, you can

- manage reports - see below
- define a report - see [Defining a Report](#) on page 463
- view a defined report - see [Viewing a Defined Report](#) on page 479
- edit a report - see [Editing a Report](#) on page 480
- run, export, import, duplicate or delete a report - see [Performing Actions on Reports](#) on page 480

➤ **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	<p>Select a category according to which reports in the page will be filtered. The default reports categories are:</p> <ul style="list-style-type: none"> Devices Monthly Reports Links Monthly Reports Devices Monthly Aggregation Reports Links Monthly Aggregation Reports Top URI Monthly Element Reports <p>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.</p> <p>See also the description of the column 'Category' below, including under each category the names of the predefined reports.</p>
Predefined	<p> 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.</p> <p> indicates an administrator-defined report.</p>
Private / Public	indicates that the report is a <i>public</i> report; anyone can view,

Column	Description
	<p>edit and delete it</p> <p> and  indicate that the report is a <i>private</i> report</p> <p> indicates that <i>I am the owner</i> 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).</p> <p> indicates that <i>I am not the owner</i> 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.</p> <p>The column can be sorted according to these classifications.</p>
Scheduled	<p> indicates a report that is currently scheduled. The column can be sorted.</p>
Report name	<p>Indicates the name of the 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.</p> <p>See also the description of the column 'Category' below, including the names of the predefined reports under each category.</p>
Type	<p>Indicates the type of report. Either:</p> <ul style="list-style-type: none"> ■ Element [Entity] Statistics. Default. See 'Element (Entity) Statistics' Report Type on page 482 for more information. 'Aggregated Statistics Trends' Report Type on page 484 ■ Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ■ Trends Statistics Comparison. See Selecting a Metric on page 470 for more information.
Entity Type	<p>Indicates the type of entity on which the report was applied, for example, Device.</p>
Category	<p>Indicates the category under which each report is categorized. The column can be sorted.</p> <p>Available categories and the <i>names of the predefined reports</i> under each category are:</p> <ul style="list-style-type: none"> ■ Devices Monthly Aggregation Report <ul style="list-style-type: none"> ✓ <i>Monthly Aggregation Report</i> ✓ <i>Devices Calls Quality Aggregation Report</i>

Column	Description
	<ul style="list-style-type: none"> ✓ <i>Devices Calls Utilization Aggregation Report</i> ■ Devices Monthly Reports <ul style="list-style-type: none"> ✓ <i>Devices Calls Report</i> ✓ <i>Devices Calls Quality Report</i> ✓ <i>Devices Calls Utilization Report</i> ■ Links Monthly Aggregation Report <ul style="list-style-type: none"> ✓ <i>Links Streams Aggregation Report</i> ✓ <i>Links Streams Quality Aggregation Report</i> ✓ <i>Links Streams Utilization Aggregation Report</i> ■ Links Monthly Reports <ul style="list-style-type: none"> ✓ <i>Links Streams Report</i> ✓ <i>Links Streams Quality Report</i> ✓ <i>Links Streams Utilization Report</i> ■ Top URI Monthly Element Reports <ul style="list-style-type: none"> ✓ <i>URI Calls Report</i> ✓ <i>URI Calls Duration Report</i> ✓ <i>URI Calls Quality Report</i> ✓ <i>URI Calls MOS Report</i> ✓ <i>URI Calls Jitter Report</i> ✓ <i>URI Calls Delay Report</i> ✓ <i>URI Calls Packet Loss Report</i> ✓ <i>URI Calls Echo Report</i> ✓ <i>URI Calls Utilization Report</i>
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.

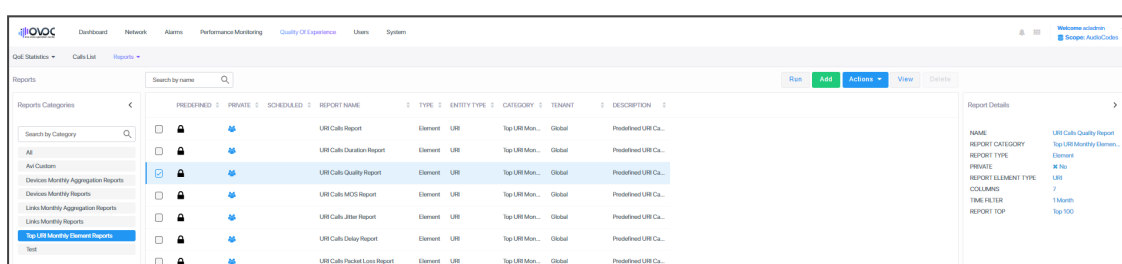
3. Optionally locate specific information quickly using the 'Search by name' field; the filter applies to all text columns in the page.

Using a Predefined Report

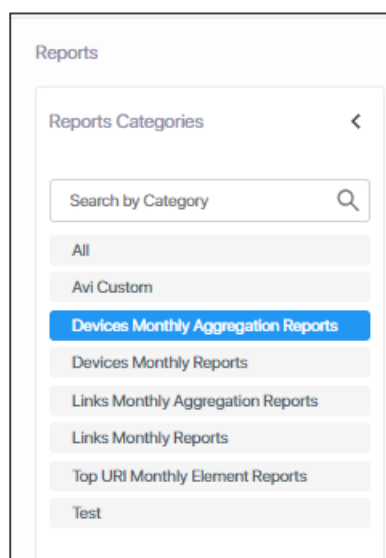
Network admins can use *predefined OVOC reports* instead of defining a Custom report as shown under [Defining a Report](#) on page 463. A Predefined report is sometimes enough for admins to quickly get the info they need; it provides a valuable glimpse into the IP network's functioning. But if a deeper analysis of network telephony performance is needed, an independently-defined report may be better practice.


➤ To use a predefined report:


1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Reports page (**Quality of Experience > Reports**).



3. View under the 'Search by Category' filter the categories of all predefined reports available.



4. Select a category; the names of the reports available under that category are displayed.  indicates predefined report integrated with the OVOC; it cannot be deleted or edited. Operators of every security level can view a predefined report but none can edit.
5. Use the table below as reference to running a predefined report.

Category	Report name	Parameters / Columns
Devices Monthly	 Devices Calls Report	Devices Calls Report

Category	Report name	Parameters / Columns
Reports	<ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Device ■ Devices Calls Quality Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Device ■ Devices Calls Utilization Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Device 	<ol style="list-style-type: none"> 1. Tenant Column 2. Region Column 3. Element Column 4. Number of Calls/Streams 5. Percent of Calls/Streams 6. Success Fail Ratio 7. Total Calls/Streams Duration 8. Average Calls/Streams Duration 9. Number of Established Calls/Streams 10. Calls/Streams Quality Ratio 11. Max Concurrent Calls/Streams 12. Number of Voice Calls/Streams 13. Number of Fax Calls/Streams <p>Devices Calls Quality Report</p> <ol style="list-style-type: none"> 1. Tenant Column 2. Region Column 3. Element Column 4. Number of Voice Calls/Streams 5. Number of Calls/Streams 6. Percent of Calls/Streams 7. Calls/Streams Quality Ratio 8. MOS Ratio 9. Jitter Ratio 10. Delay Ratio 11. PLoss Ratio

Category	Report name	Parameters / Columns
		12. Echo Ratio 13. Avg MOS 14. Max MOS 15. Min MOS 16. Avg Jitter 17. Max Jitter 18. Min Jitter 19. Avg PLoss 20. Max Ploss 21. Min Ploss 22. Avg Delay 23. Max Delay 24. Min Delay 25. Avg Echo 26. Max Echo 27. Min Echo 28. Avg SNR Devices Calls Utilization Report 1. Tenant Column 2. Region Column 3. Element Column 4. Avg Total Kbps 5. Avg Rx Kbps 6. Avg Tx Kbps 7. Avg PLoss 8. Number of Calls/Streams
Links Monthly Reports	<ul style="list-style-type: none"> ■ Links Streams Report <ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Link ■ Links Streams Quality Report 	Links Streams Report 1. Tenant Column 2. Region Column 3. Element Column 4. Number of Calls/Streams 5. Percent of Calls/Streams 6. Success Fail Ratio

Category	Report name	Parameters / Columns
	<ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Link ■ Links Streams Utilization Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: Link 	<p>7. Total Calls/Streams Duration</p> <p>8. Average Calls/Streams Duration</p> <p>9. Number of Established Calls/Streams</p> <p>10. Calls/Streams Quality Ratio</p> <p>11. Max Concurrent Calls/Streams</p> <p>12. Number of Voice Calls/Streams</p> <p>13. Number of Fax Calls/Streams</p> <p>Links Streams Quality Report</p> <p>1. Tenant Column</p> <p>2. Region Column</p> <p>3. Element Column</p> <p>4. Number of Voice Calls/Streams</p> <p>5. Number of Calls/Streams</p> <p>6. Percent of Calls/Streams</p> <p>7. Calls/Streams Quality Ratio</p> <p>8. MOS Ratio</p> <p>9. Jitter Ratio</p> <p>10. Delay Ratio</p> <p>11. PLoss Ratio</p> <p>12. Echo Ratio</p> <p>13. Avg MOS</p> <p>14. Max MOS</p> <p>15. Min MOS</p> <p>16. Avg Jitter</p> <p>17. Max Jitter</p> <p>18. Min Jitter</p> <p>19. Avg PLoss</p>

Category	Report name	Parameters / Columns
		20. Max Ploss 21. Min Ploss 22. Avg Delay 23. Max Delay 24. Min Delay 25. Avg Echo 26. Max Echo 27. Min Echo 28. Avg SNR Links Streams Utilization Report 1. Tenant Column 2. Region Column 3. Element Column 4. Avg Total Kbps 5. Avg Rx Kbps 6. Avg Tx Kbps 7. Avg PLoss 8. Number of Calls/Streams
Devices Monthly Aggregation Reports	<ul style="list-style-type: none"> ■ Devices Calls Aggregation Report <ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Device ■ Devices Calls Quality Aggregation Report <ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Device ■ Devices Calls Utilization Aggregation Report 	Devices Calls Aggregation Report 1. Time Column 2. Number of Calls/Streams 3. Percent of Calls/Streams 4. Success Fail Ratio 5. Total Calls/Streams Duration 6. Average Calls/Streams Duration 7. Number of Established Calls/Streams 8. Calls/Streams Quality Ratio 9. Max Concurrent Calls/Streams

Category	Report name	Parameters / Columns
	<ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Device 	<p>10. Number of Voice Calls/Streams</p> <p>11. Number of Fax Calls/Streams</p> <p>Devices Calls Quality Aggregation Report</p> <p>1. Time Column</p> <p>2. Number of Voice Calls/Streams</p> <p>3. Number of Calls/Streams</p> <p>4. Percent of Calls/Streams</p> <p>5. Calls/Streams Quality Ratio</p> <p>6. MOS Ratio</p> <p>7. Jitter Ratio</p> <p>8. Delay Ratio</p> <p>9. PLoss Ratio</p> <p>10. Echo Ratio</p> <p>11. Avg MOS</p> <p>12. Max MOS</p> <p>13. Min MOS</p> <p>14. Avg Jitter</p> <p>15. Max Jitter</p> <p>16. Min Jitter</p> <p>17. Avg PLoss</p> <p>18. Max Ploss</p> <p>19. Min Ploss</p> <p>20. Avg Delay</p> <p>21. Max Delay</p> <p>22. Min Delay</p> <p>23. Avg Echo</p> <p>24. Max Echo</p> <p>25. Min Echo</p> <p>26. Avg SNR</p> <p>Devices Calls Utilization Aggregation Report</p>

Category	Report name	Parameters / Columns
		<ol style="list-style-type: none"> 1. Time Column 2. Avg Total Kbps 3. Avg Rx Kbps 4. Avg Tx Kbps 5. Avg PLoss 6. Number of Calls/Streams
Links Monthly Aggregation Reports	<ul style="list-style-type: none"> ■ Links Streams Aggregation Report <ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Link ■ Links Streams Quality Aggregation Report <ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Link ■ Links Streams Utilization Aggregation Report <ul style="list-style-type: none"> ✓ Type: Aggregated Statistics Trends. See 'Aggregated Statistics Trends' Report Type on page 484 for more information. ✓ Entity: Link 	<p>Links Streams Aggregation Report</p> <ol style="list-style-type: none"> 1. Time Column 2. Number of Calls/Streams 3. Percent of Calls/Streams 4. Success Fail Ratio 5. Total Calls/Streams Duration 6. Average Calls/Streams Duration 7. Number of Established Calls/Streams 8. Calls/Streams Quality Ratio 9. Max Concurrent Calls/Streams 10. Number of Voice Calls/Streams 11. Number of Fax Calls/Streams <p>Links Streams Quality Aggregation Report</p> <ol style="list-style-type: none"> 1. Time Column 2. Number of Voice Calls/Streams 3. Number of Calls/Streams 4. Percent of Calls/Streams 5. Calls/Streams Quality

Category	Report name	Parameters / Columns
		Ratio 6. MOS Ratio 7. Jitter Ratio 8. Delay Ratio 9. PLoss Ratio 10. Echo Ratio 11. Avg MOS 12. Max MOS 13. Min MOS 14. Avg Jitter 15. Max Jitter 16. Min Jitter 17. Avg PLoss 18. Max PLoss 19. Min PLoss 20. Avg Delay 21. Max Delay 22. Min Delay 23. Avg Echo 24. Max Echo 25. Min Echo 26. Avg SNR Links Streams Utilization Aggregation Report 1. Time Column 2. Avg Total Kbps 3. Avg Rx Kbps 4. Avg Tx Kbps 5. Avg PLoss 6. Number of Calls/Streams
Top URI Monthly Element Reports	<div> <div></div> <div>URI Calls Report</div> </div> <div> <div>✓</div> <div> Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. </div> </div>	URI Calls Report 1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Average Calls/Streams Duration 6.

Category	Report name	Parameters / Columns
	<ul style="list-style-type: none"> ✓ Entity: URI ■ URI Calls Duration Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls Quality Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls MOS Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls Jitter Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls Delay Report ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI 	<p>Number of Incoming Calls/Streams 7. Number of Outgoing Calls/Streams 8. Number of Voice Calls/Streams 9. Number of Fax Calls/Streams</p> <p>URI Calls Duration Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Average Calls/Streams Duration 6. Number of Incoming Calls/Streams 7. Number of Outgoing Calls/Streams</p> <p>URI Calls Quality Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Calls/Streams Quality Ratio 5. Number of Good Calls/Streams 6. Number of Fair Calls/Streams 7. Number of Bad Calls/Streams</p> <p>URI Calls MOS Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Number of MOS Calls/Streams 6. Avg MOS</p> <p>URI Calls Jitter Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Number of Jitter Calls/Streams 6. Avg Jitter</p>

Category	Report name	Parameters / Columns
	<ul style="list-style-type: none"> ■ URI Calls Packet Loss Report <ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls Echo Report <ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI ■ URI Calls Utilization Report <ul style="list-style-type: none"> ✓ Type: Element [Entity] Statistics. See 'Element (Entity) Statistics' Report Type on page 482 for more information. ✓ Entity: URI 	<p>URI Calls Delay Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Number of Delay Calls/Streams 6. Avg Delay</p> <p>URI Calls Packet Loss Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Number of PLoss Calls/Streams 6. Avg PLoss</p> <p>URI Calls Echo Report</p> <p>1. Tenant Column 2. Element Column 3. Number of Calls/Streams 4. Total Calls/Streams Duration 5. Number of Echo Calls/Streams 6. Avg Echo</p> <p>URI Calls Utilization Report</p> <p>1. Tenant Column 2. Element Column 3. Avg Total Kbps 4. Avg Rx Kbps 5. Avg Tx Kbps</p>

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 the next page 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 (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 10-3: Defining # of administrator-defined reports produced at system level

VOICE QUALITY

Reports
10

Total: 1,000 Allocated: 122 12% Free: 878

Submit

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.

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. Access the relevant Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55).
2. Open the Reports page (**Quality of Experience** menu > **Reports** tab).
3. Click the **Add** button (disabled for operators whose security level is configured as 'Monitor').

Figure 10-4: Add Report - Definition tab

REPORT

Definition

Filter

Table Layout

Graphs View

Name*

Description

Category*

Links Monthly Aggregation Reports

Report Scope*

Global

Report Type


☒ **Element (Entity) Statistics**
 Element statistics is similar to the current statistics layout that exists in today's report.

☐ **Aggregated Statistics Trends**
 Trend aggregated statistics is similar to current trends statistics exist in the OVOC

☐ **Trends Statistics Comparison**
 Trend statistics comparison is similar to the singular real time statistics in OVOC

Logo (PNG, JPEG)

☒ Global
 ☐ Tenant
 ☐ Custom




☒ Privacy


Close
 OK

- Use the table as reference.

Table 10-2: Report Definition

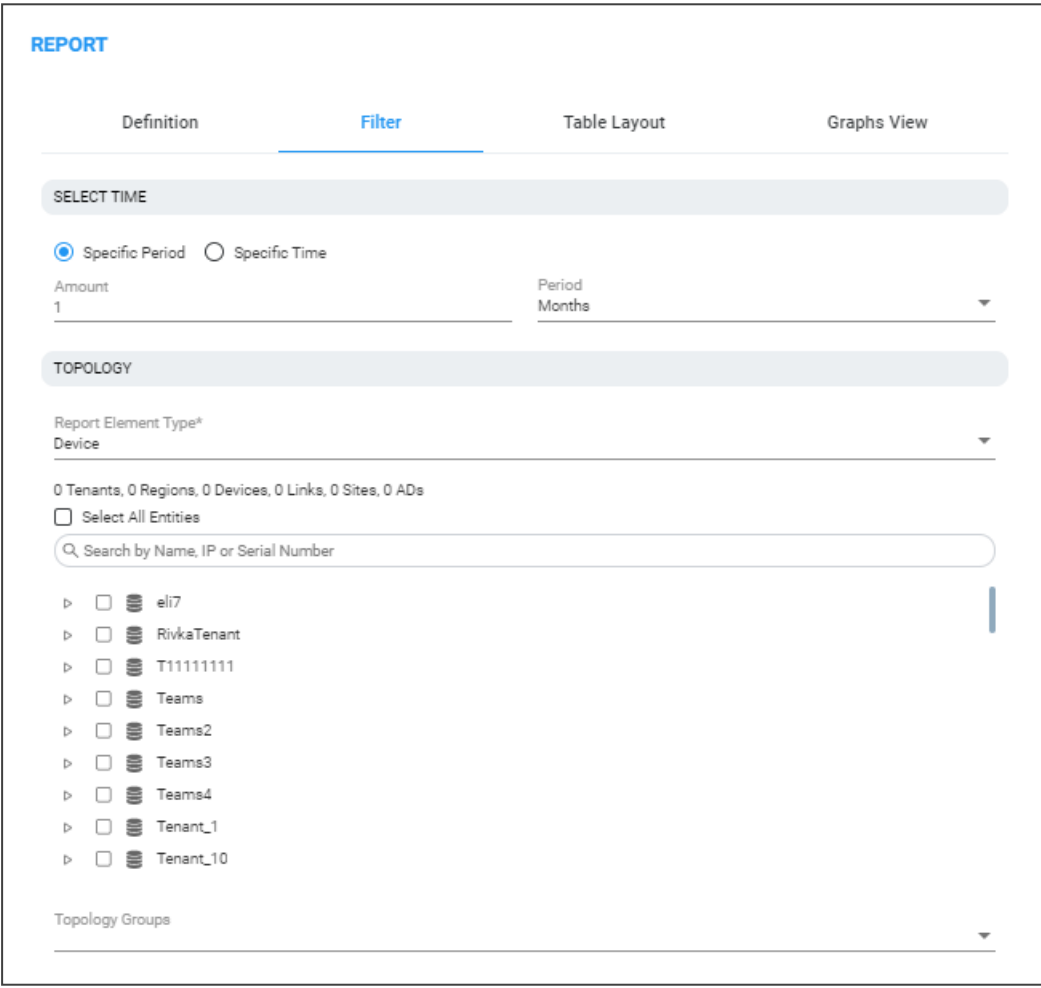
Column	Description
Name	Enter an intuitive name for the report. Enter a name that will facilitate management later.
Description	Enter a description of the report to facilitate management later.
Category	From the drop-down, select a category from the list of report categories or define a new category.
Report Type	Select the report type option you require. Use the following as reference:

Column	Description
	<ul style="list-style-type: none"> ■ 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 470 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)	<p>Enables logos to be displayed in report results thereby facilitating management of reports results later. The preferred logo size is 200X40 pixels.</p> <ul style="list-style-type: none"> ■ Default: Global. The logo image is displayed <i>globally</i> across <i>all report results</i>, 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 86; 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 added to the Software Manager. You can perform the same operation in the Software Manager; see Adding Auxiliary Files on page 123 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 144 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

Column	Description
	<p>definition.</p> <p>✓ 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.</p>
Privacy	Default: Private . Drag to change to Public ; the text in the screen changes correspondingly.

5. Click the **Filter** tab.

Figure 10-5: Filter tab



REPORT

Definition **Filter** Table Layout Graphs View

SELECT TIME

☒ Specific Period ☐ Specific Time

Amount: 1 Period: Months

TOPOLOGY

Report Element Type*: Device

0 Tenants, 0 Regions, 0 Devices, 0 Links, 0 Sites, 0 ADs

☐ Select All Entities

Search by Name, IP or Serial Number

- ☐ eli7
- ☐ RivkaTenant
- ☐ T11111111
- ☐ Teams
- ☐ Teams2
- ☐ Teams3
- ☐ Teams4
- ☐ Tenant_1
- ☐ Tenant_10

Topology Groups

6. 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.

7. [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.
8. 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
9. 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 produce 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 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.
10. 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 in 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.

11. [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.
12. Click the **Table Layout** tab.

Figure 10-6: Table Layout tab

REPORT

Definition Filter **Table Layout** Graphs View

Select report metrics and arrange the table layout
Reorder elements in a list using the mouse

Search Metric

Metrics Optional

- Number of Calls/Streams
- Percent of Calls/Streams
- Number of Voice Calls/Streams
- Number of Fax Calls/Streams
- Total Calls/Streams Duration
- Average Calls/Streams Duration
- Number of Established Calls/Streams
- Max Concurrent Calls/Streams
- Success Fail Ratio
- Number of Successful Calls/Streams

Selected Metrics

1. Tenant Column
2. Region Column
3. Element Column

☐ Enable Top Values

Number of top records

Number Of Rows Per Page
25

13. 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.

14. 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.

15. From the 'Number Of Rows Per Page', select 25, 50, 100 or 500.

16. Click **OK** or click the **Graphs View** tab.

Figure 10-7: Graphs View tab

17. Click the  icon to add a graph.

Figure 10-8: Add Graph

18. Click the 'Name of Graph' field and enter an intuitive name to facilitate effective management later; the field turns yellow.

19. 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.
20. From the 'Columns' drop-down, select graph columns (available columns depend on graph type and on the metrics you previously selected in the **Graphs View** tab).



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.

21. 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 463.



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 Chart	Total as 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,	Sum

			Pie	
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 Calls/Streams Ratio	successfulCallsPercent	Number	Bar, Line	Percent
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	poorCallsCounter	Number	Bar,	Sum

Calls/Streams			Line, Pie	
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 Without Unknown	mosQualityWithoutUnknown	Ratio	Stack bar	Percent
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,	Percent

			Line	
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, Pie	Max
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	delayCounter	Number	Bar,	Sum

Calls/Streams			Line, Pie	
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 Outgoing Calls/Streams	outgoingCounter	Number	Bar, Line, Pie	Sum
Number of Incoming Calls/Streams	incomingCounter	Number	Bar, Line, Pie	Sum
Number of WiFi Calls/Streams	wifiCallsCounter	Number	Bar, Line, Pie	Sum
Number of Wired Calls/Streams	wiredCallsCounter	Number	Bar, Line, Pie	Sum
WiFi Success/Fail Ratio	wifiSuccessFail	Ratio	Stack bar	Percent
WiFi Success Calls/Streams Ratio	wifiSuccessfulCallsPercent	Number	Bar, Line	Percent
WiFi Failed Calls/Streams Ratio	wifiFailedCallsPercent	Number	Bar, Line	Percent
Number of WiFi Successful Calls/Streams	wifiSuccessfulCounter	Number	Bar, Line, Pie	Sum
Number of WiFi Failed Calls/Streams	wifiFailedCounter	Number	Bar, Line,	Sum

			Pie	
Wired Success Fail Ratio	wiredSuccessFail	Ratio	Stack bar	Percent
Wired Success Calls/Streams Ratio	wiredSuccessfulCallsPercent	Number	Bar, Line	Percent
Wired Failed Calls/Streams Ratio	wiredFailedCallsPercent	Number	Bar, Line	Percent
Number of Wired Successful Calls/Streams	wiredSuccessfulCounter	Number	Bar, Line, Pie	Sum
Number of Wired Failed Calls/Streams	wiredFailedCounter	Number	Bar, Line, Pie	Sum
WiFi Calls/Streams Quality Ratio	wifiCallsQuality	Number	Bar, Line	Percent
WiFi Calls/Streams Quality Ratio Without Unknown	wifiCallsQualityWithoutUnknown	Ratio	Stack bar	Percent
Number of Good WiFi Calls/Streams	wifiGoodCallsCounter	Number	Bar, Line, Pie	Sum
Number of Fair WiFi Calls/Streams	wifiFairCallsCounter	Number	Bar, Line, Pie	Sum
Number of Bad WiFi Calls/Streams	wifiPoorCallsCounter	Number	Bar, Line, Pie	Sum
Number of WiFi Unknown Calls/Streams	wifiUnknownCallsCounter	Number	Bar, Line, Pie	Sum
WiFi Good Quality Ratio	wifiGoodCallsPercent	Number	Bar, Line	Percent
WiFi Fair Quality Ratio	wifiFairCallsPercent	Number	Bar, Line	Percent

WiFi Bad Quality Ratio	wifiPoorCallsPercent	Number	Bar, Line	Percent
WiFi Unknown Quality Ratio	wifiUnknownCallsPercent	Number	Bar, Line	Percent
Wired Calls/Streams Quality Ratio	wiredCallsQuality	Number	Bar, Line	Percent
Wired Calls/Streams Quality Ratio Without Unknown	wiredCallsQualityWithoutUnknown	Ratio	Stack bar	Percent
Number of Good Wired Calls/Streams	wiredGoodCallsCounter	Number	Bar, Line, Pie	Sum
Number of Fair Wired Calls/Streams	wiredFairCallsCounter	Number	Bar, Line, Pie	Sum
Number of Bad Wired Calls/Streams	wiredPoorCallsCounter	Number	Bar, Line, Pie	Sum
Number of Wired Unknown Calls/Streams	wiredUnknownCallsCounter	Number	Bar, Line, Pie	Sum
Wired Good Quality Ratio	wiredGoodCallsPercent	Number	Bar, Line	Percent
Wired Fair Quality Ratio	wiredFairCallsPercent	Number	Bar, Line	Percent
Wired Bad Quality Ratio	wiredPoorCallsPercent	Number	Bar, Line	Percent
Wired Unknown Quality Ratio	wiredUnknownCallsPercent	Number	Bar, Line	Percent

Viewing a Defined Report



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

After defining a report as shown in [Defining a Report](#) on page 463, 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Reports page (**Quality of Experience > Reports**).
3. Select the report whose definition you want to view and then click the **View** button.

REPORT

Definition
Filter
Table Layout
Graphs View

Name
Devices Calls Utilization Aggregation Report

Description
Predefined Devices Calls Utilization Aggregation Re

Category
Devices Monthly Aggregation Reports

Report Scope
Global

Report Type

☐ Element (Entity) Statistics
Element statistics is similar to the current statistics layout that exists in todays report.

☒ Aggregated Statistics Trends
Trend aggregated statistics is similar to current trends statistics exist in the OVOC

☐ Trends Statistics Comparison
Trend statistics comparison is similar to the singular real time statistics in OVOC

Logo (PNG, JPEG)

☒ Global
☐ Tenant
☐ Custom

Privacy

Close

4. 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 the previous page for more information.



When editing a report, use the information in [Defining a Report](#) on page 463 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:

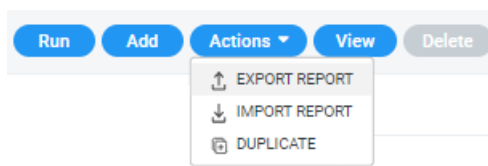
- In the Reports page, select a report and then click the activated **Run** button; a notification is displayed indicating *Report Executed. Execute Report Succeeded* and the report is displayed. If a report is not selected, the **Run** button will not be activated.

➤ To export a report definition:

- Select a report, 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 10-9: Export Report



➤ **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:**

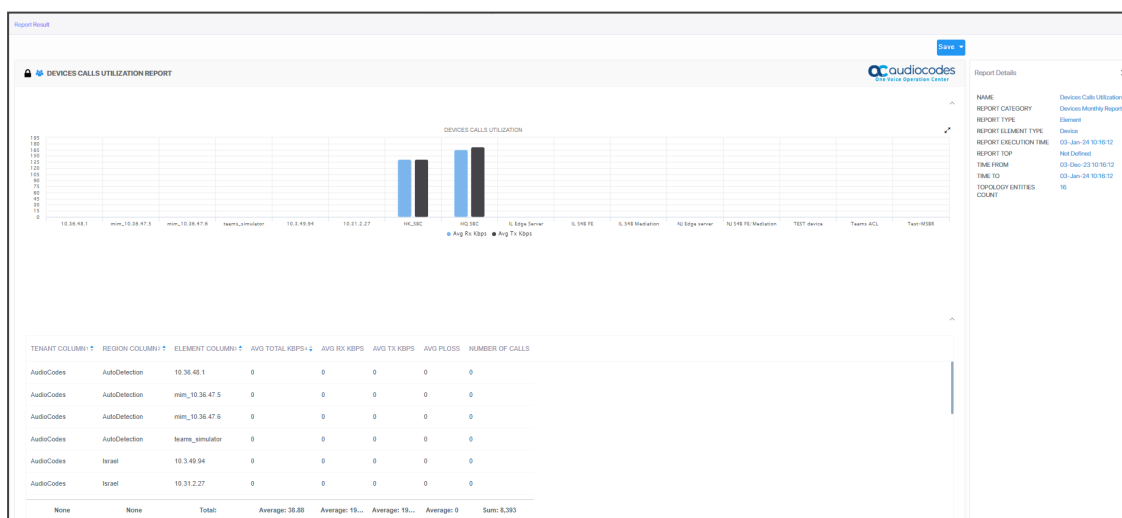
- Click the **Actions** button and then from the drop-down menu select **Duplicate**. Only operators who have permission to add / edit reports can duplicate.

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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Reports page (**Quality of Experience > Reports**).
3. Select the report you want to run and display and then click the **Run** button; the Report Result is dynamically tabbed and displayed.





- 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).

4. 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 'Element'.
5. [Optionally] Click the **x** in the dynamic tab to remove the Report Result; you're returned to the Reports page.
6. 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.
7. [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.



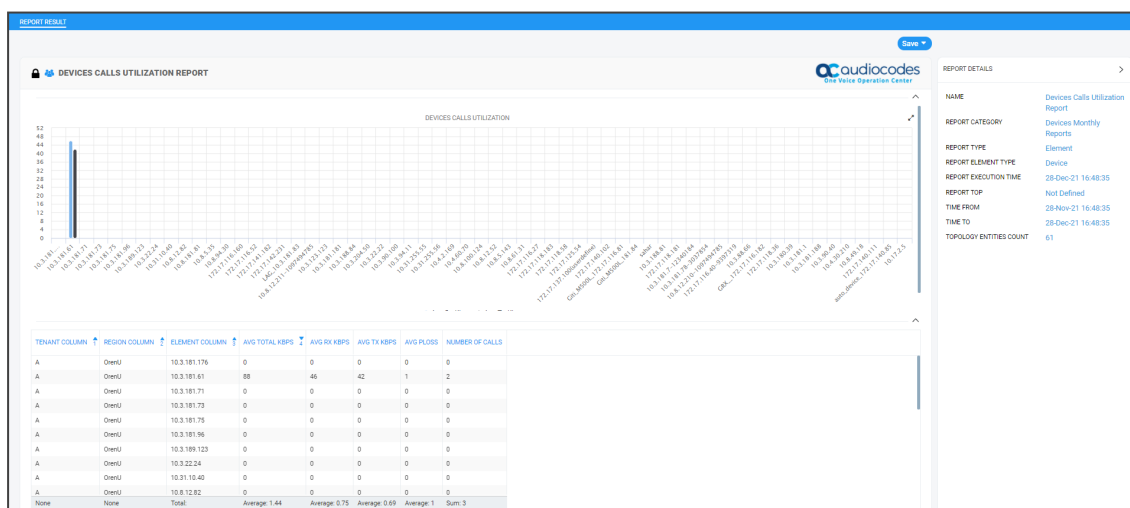
For more information about results of reports of type 'Element', see ['Element \(Entity\) Statistics' Report Type](#) below

For more information about results of reports of type 'Aggregation', see ['Aggregated Statistics Trends' Report Type](#) on page 484

'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 10-10: 'Element (Entity) Statistics' Report Type



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 Utilization 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:
 - Black = Unknown
 - Blue = Average
 - Red = Failed
 - Yellow = Fair
 - Green = Successful
- 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



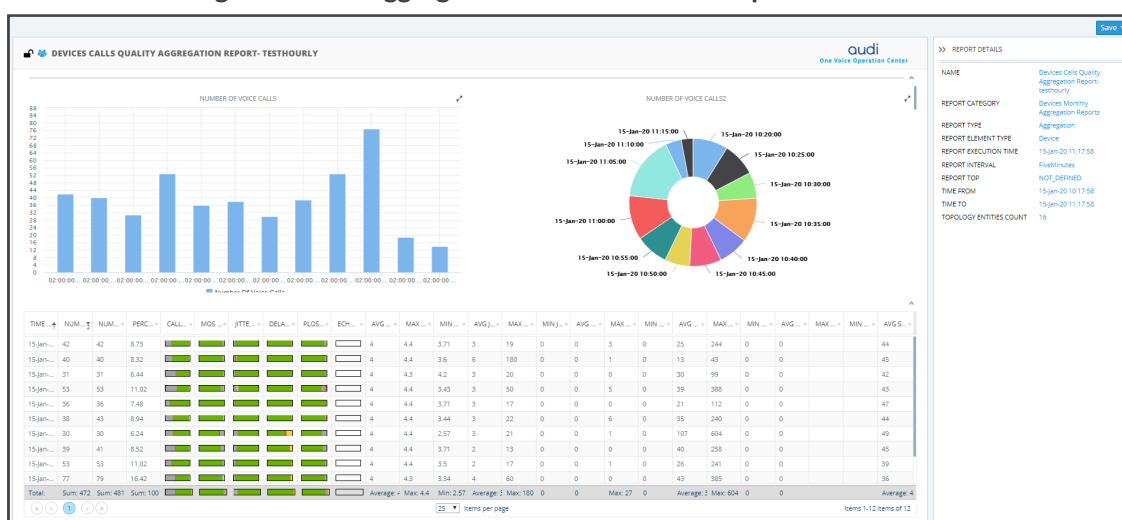
Colors of bars in a stack chart depend on *metric name*.

- 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 10-11: 'Aggregated Statistics Trends' Report



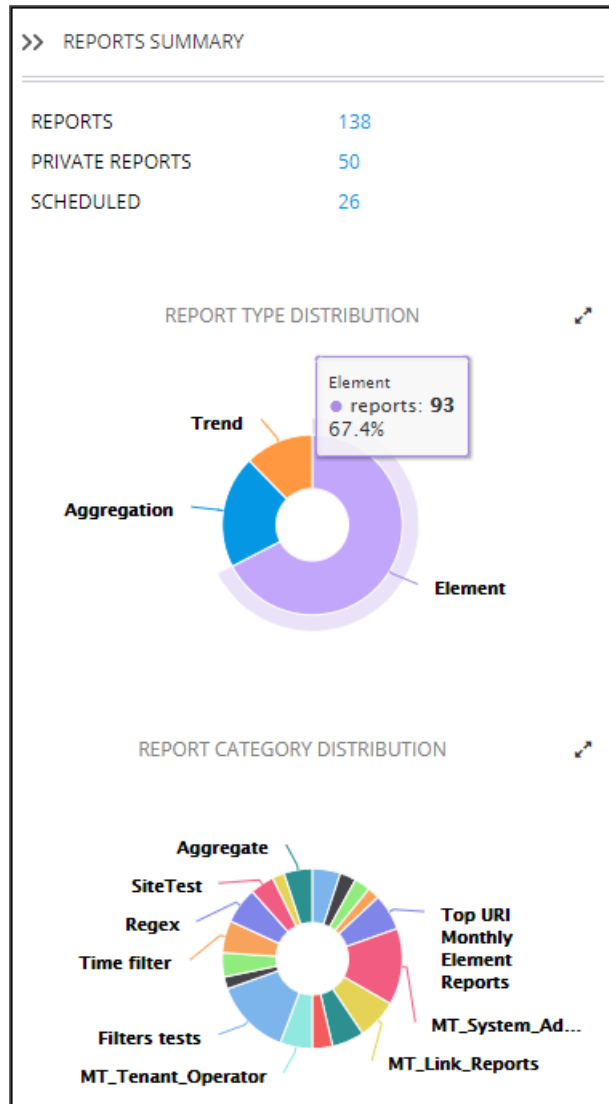
Use the following to get acquainted:

-  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 (**Quality of Experience** menu > **Reports** tab) and locate the Reports Summary pane on the right.

Figure 10-12: Reports Summary

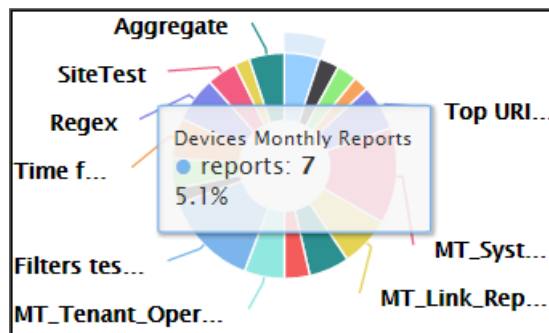


- The *uppermost* section of the pane displays
 - the number of reports
 - the number of private reports
 - the number of scheduled reports
- The *middle* section of the pane shows a pie chart depicting how report types (Trend, Aggregation and Element) are distributed. Optionally, magnify the chart by 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 10-13: Pie Chart Depicting Distribution per Report Category



Viewing Schedulers and Reports Executed by them

OVOC's Scheduled Reports page enables admins to view Report Schedulers that have been configured and the reports that have been executed by them.






➤ To view Report Schedulers:

1. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. Open the Scheduled Reports page (**Quality of Experience > Reports > Scheduled Reports**).

Scheduled Reports									
ACTIVE	PRIVATE	NAME	REPORT NAME	REPORT CATEGORY	TENANTS	REPORT TYPE	NO. OF EXECUTIONS LEFT	NEXT EXECUTION RUN	LAST RUN TIME
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Company Name Floating License	Devices Calls Utilization Report	Devices Monthly Reports		Element			23-Jul-2022:27:00
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dnsutil	Dnsutil Test	Links Monthly Aggregation Reports	AudioCodes	Element			15-Sep-2023:00:00
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IsoundTest	test	Avi Custom		Element			23-Feb-23:16:05:00
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Nat1	Devices Calls Report	Devices Monthly Reports		Element	Infinite	01-Feb-24 02:00:00	01-Jan-24 02:00:00
<input type="checkbox"/>	<input checked="" type="checkbox"/>	test	Devices Calls Report	Devices Monthly Reports	AudioCodes	Element			23-Jul-2022:30:00
<input type="checkbox"/>	<input checked="" type="checkbox"/>	VRXRM users	Run Test	Top URI Monthly Element Reports		Element	Infinite	01-Feb-24 02:01:00	01-Jan-24 02:01:00

3. On the left side of the page, view the configured Report Schedulers. The table below explains the columns on the left side of the page where the Report Schedulers are listed.

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.

Column	Description
Private / Public	<p> indicates that the scheduled report is a <i>public</i> report; anyone can view, edit and delete it</p> <p> and  indicate that the scheduled report is a <i>private</i> report</p> <p> indicates that <i>I am the owner</i> of this scheduled private report 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).</p> <p> indicates that <i>I am not the owner</i> 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.</p> <p>The column can be sorted according to these classifications.</p>
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

Column	Description
	run. Corresponds to the day, date and time configured in the Scheduler Report dialog when adding a scheduled report. The column is sortable.

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

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. <table><tr><th>TIME</th><th>NAME</th><th>FILE</th></tr><tr><td>30-Dec-19 04:00:00</td><td>Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0200</td><td>CSV</td></tr><tr><td>30-Dec-19 05:00:00</td><td>Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0300</td><td>CSV</td></tr><tr><td>30-Dec-19 06:00:00</td><td>Report_Devices_Calls_Quality_Report_Element_Tenant_2019-12-30_GMT_0400</td><td>CSV</td></tr></table>	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
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).												

5. 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 admins 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 admin 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. Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
2. In the Scheduled Reports page (**Quality of Experience > Reports > Scheduled Reports**), click the **Add Scheduler** button.

REPORT SCHEDULER

Details Scheduler

☒ Active

Scheduler Name*

Description

☒ Select All Tenants

Report Name*

Report Info

Type

Category

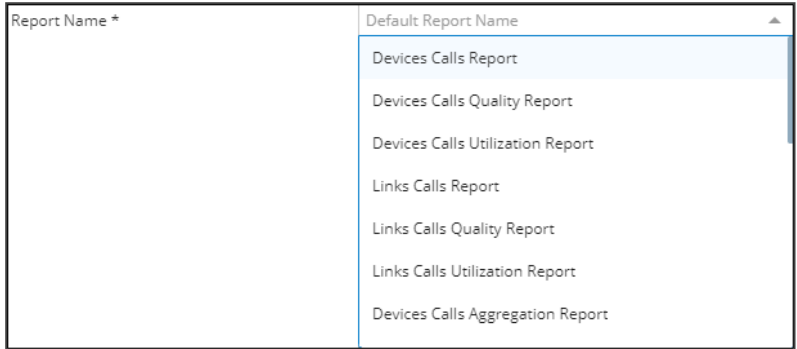
Entity Type

Time Filter

Close OK

3. Use the table as reference.

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 more effective management for other operators.
Select All Tenants	<input checked="" type="checkbox"/> Select this option to run this report on all tenants, including

Column	Description
	<p>new ones.</p> <ul style="list-style-type: none"> ■ Clear this option to run this report only on a specific tenant, and then select that specific tenant from the list.
Report Name	<p>From the drop-down, select a report name. Scroll down to view the full list of options. Auto complete is also supported.</p> 
Scheduler Scope	<p>[Only displayed if the 'Select All Tenants' option is selected] From the drop-down, select:</p> <ul style="list-style-type: none"> ■ System for the scope of the scheduler to be <i>per system</i>, irrespective of tenant ■ per specified tenant for the scope of the scheduler to be <i>for that specified tenant</i>
Report Generation Period	<p>Select either Hourly (default), Daily, Weekly or Monthly. Determines how frequently reports will be generated. If you select</p> <ul style="list-style-type: none"> ■ 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	<p>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.</p>

Column	Description
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 .
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.

- 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 (**Quality of Experience** menu > **Reports** tab > **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 488 for more information. Edit the scheduler definitions using the same table for reference as that in [Adding a Report Scheduler](#) on page 488.

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:

- Select Global or Tenant scope (see [Selecting a Scope: Global vs. Tenant](#) on page 55 for more information).
- In the Scheduled Reports page (**Quality of Experience** > **Reports** > **Scheduled Reports**), from the list of configured Report Schedulers listed in the left side of the page, select a Report Scheduler.

Scheduled Reports										Show Save Delete		
ACTIVE	PRIVATE	NAME	REPORT NAME	REPORT CATEGORY	TENANTS	REPORT TYPE	NO. OF EXECUTIONS LEFT	NEXT EXECUTION RUN	LAST RUN TIME	TIME	NAME	FILE TYPE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CompanyHome Phishing License	Device Calls Utilization Report	Device Monthly Reports		Element		23-Jul-20 22:27...		<input type="checkbox"/>	01-Oct-23 02:00...	Report Device... CSV
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dtmstest	Dtmstest Link Test	Links Monthly Aggregation Rep...	AudioCodes	Element		10-Sep-23 03:00...		<input type="checkbox"/>	01-Nov-23 02:00...	Report Device... CSV
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Isordtest	test	Ad Custom		Element		23-Feb-23 16:06...		<input checked="" type="checkbox"/>	01-Dec-23 02:00...	Report Device... CSV
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Nat1	Device Calls Report	Device Monthly Reports		Element	Initial	01-Feb-24 02:00:00	01-Jan-24 02:00...	<input type="checkbox"/>	01-Jan-24 02:00...	Report Device... CSV
<input type="checkbox"/>	<input checked="" type="checkbox"/>	test	Device Calls Report	Device Monthly Reports	AudioCodes	Element		23-Jul-20 22:30...				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	unique users	Run Test	Top 100 Monthly Element Reports		Element	Initial	01-Feb-24 02:01:00	01-Jan-24 02:01...			




3. 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. See the figure in [Displaying Report Results](#) on page 481 for reference.
4. Use the 'Report Details' pane on the right of the report for quick reference.
5. [Optionally] Click the **x** in the dynamic tab to remove the Report Result; you're returned to the Scheduled Reports page.
6. 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.
7. [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


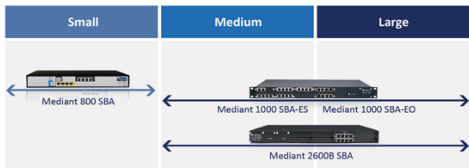

Supported IP Network Telephony Equipment	Description
 <p>MediaPack</p>	<p>MP-1xx: Analog VoIP devices featuring up to 24 analog ports connected directly to an enterprise PBX (FXO), to phones, or to fax (FXS). Support up to 24 simultaneous calls.</p> <p>MP-20x: VoIP Gateway. An all-in-one unit featuring (depending on model) a VoIP adapter, FXS lines, FXO interfaces, Ethernet LAN interfaces (with an internal Layer-2 switch), and Ethernet WAN interface.</p> <p>(See product documentation for detailed information)</p>
 <p>Mediant 500 E-SBC</p> <p>Mediant 500L E-SBC</p>	<p>Members of the AudioCodes family of Enterprise Session Border Controllers. Enable connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provide VoIP SBC functionality. Offer enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.</p>
 <p>Mediant 500 MSBR</p> <p>Mediant 500L MSBR</p> <p>Mediant 800 MSBR</p>	<p>These Multi-Service Business Routers are networking devices that combine multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server.</p> <p>Stand Alone Survivability (SAS) functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-</p>




Supported IP Network Telephony Equipment	Description
 <p>Mediant 1000 MSBR</p>	<p>Centrex server or IP-PBX.</p> <p>The devices also provide an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing. (See the specific product documentation for detailed information)</p>
<p>Mediant 500Li</p>	<p>Part of the the AudioCodes Mediant i-Series, this device offers service providers a range of all-in-one SOHO, SMB and SME routers 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)</p>
 <p>Mediant 500 Enterprise Session Border Controller (E-SBC)</p>	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provides VoIP SBC functionality. Offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.</p>
 <p>Mediant 2600 E-SBC</p>	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. 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)</p>




Supported IP Network Telephony Equipment	Description
	implementation. The SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.
 <p>Mediant Software Enterprise Session Border Controllers</p>	<p>Mediant Software E-SBCs are pure-software products, enabling connectivity and security between enterprises' and service providers' VoIP networks. Includes the following product variants:</p> <p>Mediant Server Edition SBC: x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements.</p> <p>Mediant Virtual Edition SBC: Installed and hosted in a virtual machine environment that complies to specified requirements.</p>
Stack Manager	Used for managing 'software stacks' deployed in virtual environments. It implements the complete stack lifecycle, including Stack deployment, Stack termination, manual stack size adjustment – using user-initiated scale-in / scale-out, automatic stack size adjustment – using automatic scaling, and stack configuration update.
Mediant Cloud Edition	OVOC supports the AudioCodes Mediant Cloud Edition. The feature is offered by the Mediant VE SBC in AWS-based environments. It provides similar functionality to the Media Transcoding Cluster feature but is in the cloud, and its Media Components handle transcoding as well as all media directly, without traversing the Mediant VE SBC.

Supported IP Network Telephony Equipment	Description
 <p>MP-1288</p>	<p>Cost-effective best-of-breed, high density analog media VoIP gateway. Provides superior voice technology for connecting legacy telephones, fax machines and modems with IP-based telephony networks, as well as for integration with IP PBX systems. Designed and tested to be fully interoperable with leading soft switches, unified communications (UC) servers and SIP proxies.</p> <p>Designed for carrier environments including 1+1 power supplies and 1+1 Ethernet redundancy, maintaining high voice quality to deliver reliable enterprise VoIP communications. Advanced call routing mechanisms, network voice quality monitoring and survivability capabilities (including PSTN fallback) result in minimum communications downtime.</p>
 <p>Mediant 3000 Media Gateway</p>	<p>Medium-sized member of the family of market-ready, standards-compliant Media Gateway systems.</p> <p>Main features: Redundant common equipment (Power, Controller, Ethernet Switch); Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SS7/SIGTRAN Interworking (SS7/PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant</p> <p>Applications: VoP Trunking devices, IP-Centrex devices, VoP Access devices</p> <p>Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; Voice Coders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fallback to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1,</p>

Supported IP Network Telephony Equipment	Description
	<p>SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP</p> <p>(See product documentation for detailed information)</p>
 <p>Mediant 4000 E-SBC</p>	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.</p>
 <p>Media Transcoder [Mediant 4000B]</p>	<p>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.</p>
 <p>AudioCodes Mediant Cloud Edition (CE) software session border controller (SBC)</p>	<p>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-</p>

Supported IP Network Telephony Equipment	Description
	generating communications services to be introduced simply and cost-effectively.
 <p>Mediant 9000 SBC</p>	<p>Highly scalable Session Border Controller designed for deployment in large enterprise and contact center locations and as an access SBC for service provider environments. High-capacity SBC supporting thousands of concurrent sessions and extensive SIP connectivity with wide-ranging interoperability, enhanced perimeter defense against cyber-attacks, and advanced voice quality monitoring.</p> <p>Also supports active/standby (1+1) redundancy (High Availability) by employing two devices in the network. Offers branch survivability during WAN failure, ensuring call service continuity.</p>
<p>Survivable Branch Appliance (SBA)</p> 	<p>Designed for Microsoft Skype for Business Server, the Survivable Branch Appliance (SBA) allows remote branch resiliency in a Microsoft Skype for Business Server network. The AudioCodes SBA resides on the OSN server platform of the Mediant 800B and the Mediant 1000B running on a Microsoft Windows 2008 Telco R2 operating system.</p> <p>Displayed in the OVOC as a module of the Mediant 800B and the Mediant 1000B devices. When you add either of these platforms to the OVOC, there is an option to enable the SBA module. The SBA module has a separate IP address and FQDN Name.</p>
	<p>405HD, 420HD, 430HD, 440HD, C435HD, 445HD, 450HD, C450HD and C470HD 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.</p>

Supported IP Network Telephony Equipment	Description
	Phone models support Microsoft Skype for Business environments as well as non-Microsoft environments.
	The RXV80 Video Collaboration Bar delivers an intuitive experience that supports collaboration in video-enabled meeting rooms, certified for Microsoft Teams.
	The RXV100 bundles act as Microsoft Teams Rooms on Windows devices to bring on-site meetings to life and deliver the optimal collaboration experience to a greater number of participants. Delivers effective video and audio collaboration in larger rooms, including factors such as voice pickup range, visual coverage, and integrated unified communications to ensure productive meetings.
	<ul style="list-style-type: none"> 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

Supported IP Network Telephony Equipment	Description
	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 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

Supported IP Network Telephony Equipment	Description
	can save up to 30% in support expenditure by automating simple and repetitive tasks.

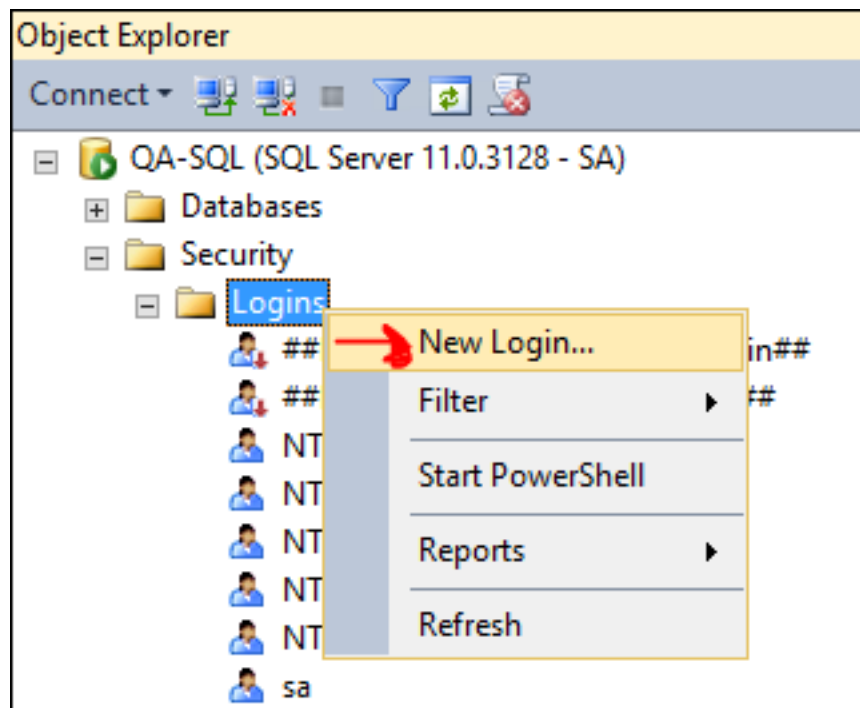
12 Adding an Unprivileged User to MSSQL Server

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

Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

Login name: Sem12

Windows authentication
☒ SQL Server authentication

Password:
 Confirm password:
☐ Specify old password
 Old password:

☒ Enforce password policy
☒ Enforce password expiration
☒ User must change password at next login

☐ Mapped to certificate
☐ Mapped to asymmetric key
☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Default database: LcsCDR
 Default language: <default>

Ready

OK Cancel

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

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

Login - New

Select a page: General, **Server Roles**, User Mapping, Securables, Status

Script Help

Server role is used to grant server-wide security privileges to a user.

Server roles:

- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☒ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☐ sysadmin

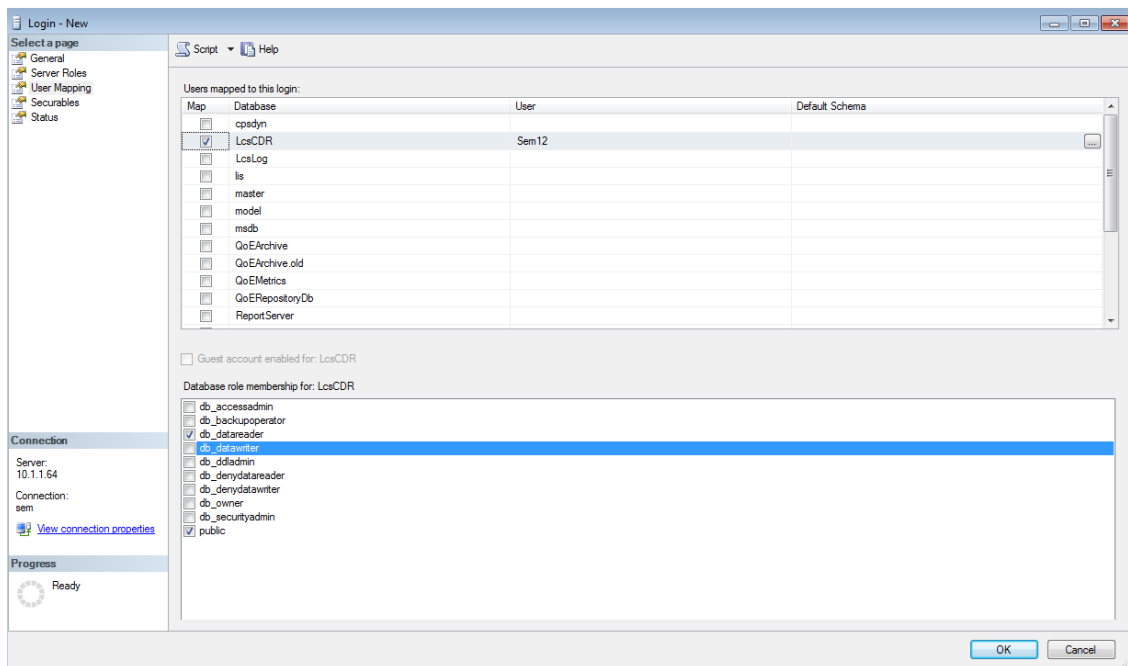
Connection

Server: QA-SQL
 Connection: SA

[View connection properties](#)

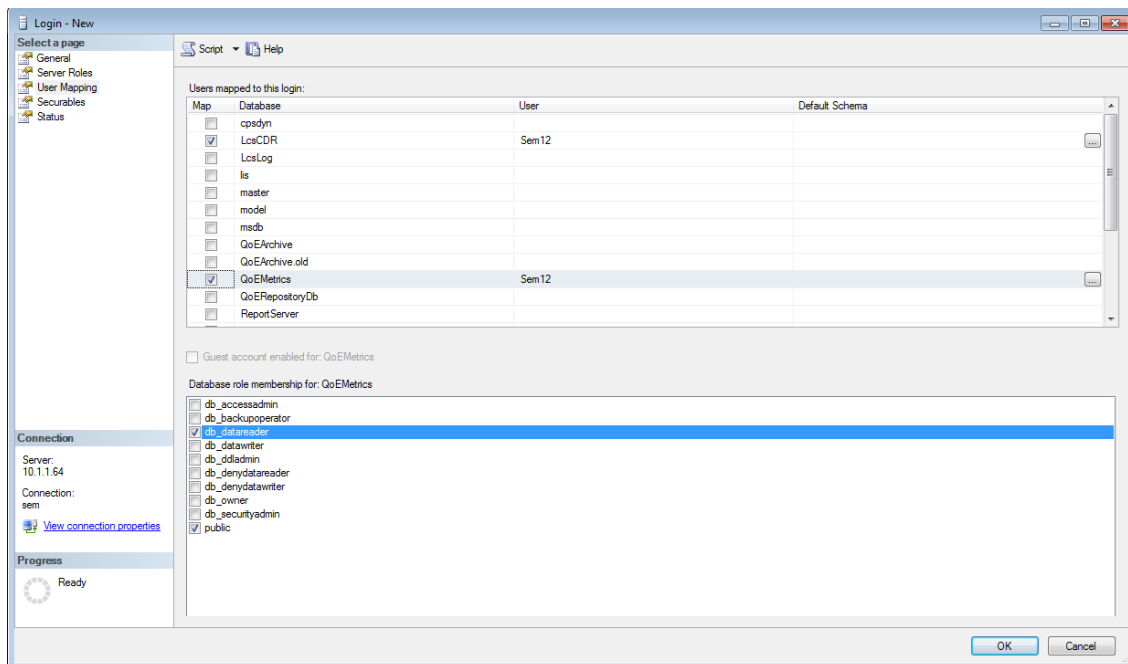
- Under 'User Mapping' shown in the following figure, in the 'Users mapped to this login' pane, select **LcsCDR** and in the 'Database role membership for LcsCDR' pane, select **db_datareader** and **public**.

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



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

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



The SQL server side is now ready.

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

Figure 12-6: Skype Details

The screenshot shows a 'SKYPE DETAILS' dialog box with the following fields and values:

Field	Value
Name *	
Tenant	ErezTenantz
Region *	ErezRegion
Device Type	Front End Server
FQDN *	
Address	
SQL SERVER DB	
IP Address *	
Port *	1433
Instance Name	
Connection Mode	SQL Server Authentication
Username *	
Password *	
SSL	DISABLED

Buttons: OK, Close

7. From the 'Device Type' drop-down, select **Front End Server**.
8. Enter the SQL Server IP address.
9. Select the **SQL Port** option and leave the default unchanged.
10. Click the 'Address' field, enter the first letter of the location, and from the list displayed, select it.
11. Enter the other details about your Microsoft SQL server - use the user credential defined previously in the SQL server.

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
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>

©2024 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, and AudioCodes Room Experience 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-92014

