OVOC

Product Description

Version 8.2

One Voice Operations Center

audiocodes

Notice

Date Published: June-10-2024

WEEE EU Directive

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

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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
OVOC Documents
Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center
One Voice Operations Center IOM Manual
One Voice Operations Center Product Description
One Voice Operations Center User's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Deployment Guide
Device Manager Pro Administrator's Manual
ARM User's Manual
Documents for Managed Devices
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500Li MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800 MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual

Document Name
Mediant 2600 E-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
Microsoft Teams Direct Routing SBA Installation and Maintenance Manual
Mediant 800B/1000B/2600B SBA for Skype for Business Installation and Maintenance Manual
Fax Server and Auto Attendant IVR Administrator's Guide
Voca Administrator's Guide
VoiceAI Connect Installation and Configuration Manual

Document Revision Record

LTRT	Description
94036	Initial Version for this release. ■ Added Sections: Added OVOC Capacities and Requirements; Managed VoIP Equipment;; Management Scope; Customize Dashboard; RDP Support for Additional Windows-Based Devices; Call Storage Settings per Tenant; Journal Event Forwarding; Forwarding Alarms and Journal Alerts for Specific Time Ranges; REST API Host Alarm Forwarding Destination; BULK Android APK Upgrade; Upgrade AudioCodes AppSuite; IP Phones Certificate Status Reporting; REST API Host Alarm Forwarding Destination; Single Sign-on to Device Manager; Microsoft's SIP Gateway Integration; Converting C448HD and C450HD Teams Phones to SIP Gateway; Meeting Room Bundle Device Statuses; Peripheral Device Management; Bundling Icon; Calls Correlation (SBC – Teams and SBC – SBC); Analytics Report Module; Device Manager Communication and Optimization ■ Updated Sections: OVOC Server; Voice Quality Management-Key Features; OVOC Cloud Architecture Mode; Mass Operations; Jabra Device Management; OVOC Capacities and Requirements ■ Removed Sections: Service Provider Cluster

Table of Contents

This page is intentionally left blank.

1 One Voice Operations Center - Overview

AudioCodes One Voice Operations Center (OVOC) is a 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.

In light of OVOC's clear GUI design, system administrators can manage the full life-cycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks which 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 performed with speed and simplicity.

OVOC uses standards-compliant distributed SNMP-based management software that is optimized to support day-to-day Network Operation Center (NOC) activities with a feature-rich management framework. It supports fault management, voice quality management and security for devices, endpoints, links and sites. The OVOC simultaneously manages AudioCodes' full line of SBCs, VoIP Media Gateways, Customer Premises Equipment (CPE), Multi-Service Business Routers (MSBR), Microsoft SBAs, CloudBond 365s, CCEs and devices.

The OVOC suite is perfectly tailored for medium to large enterprises as well as for Service Providers with its high security features, high availability and multi-tenancy.

OVOC features sophisticated Web architecture, enabling customer access from multiple, remotely located work centers and workstations over HTTPS.

OVOC can run on a dedicated HP server provided by AudioCodes, either VMware or HyperV platforms. OVOC server runs on Linux CentOS 64-bit platform. All management data is stored on the server using Oracle relational database software. OVOC server High Availability is supported on Virtualization platforms.

OVOC includes a tenant and region/site hierarchy in which devices can be defined. The combination of OVOC tenants and regions/sites and user configuration can be used to define multi tenancy where each user can be defined to operate or monitor in specific tenants or regions/sites.

OVOC can simultaneously manage multiple AudioCodes devices and endpoints. For a full listing of supported managed products and versions, refer to the OVOC Release Notes.

OVOC has an integration point with the AudioCodes Routing Manager (ARM). Managing the dial plan and call routing rules for multi-site, multi-vendor enterprise VoIP networks can be an extremely complicated activity. AudioCodes Routing Manager (ARM) delivers a powerful, innovative solution to this problem by enabling centralized control of all session routing decisions.

Key Elements of the OVOC Suite

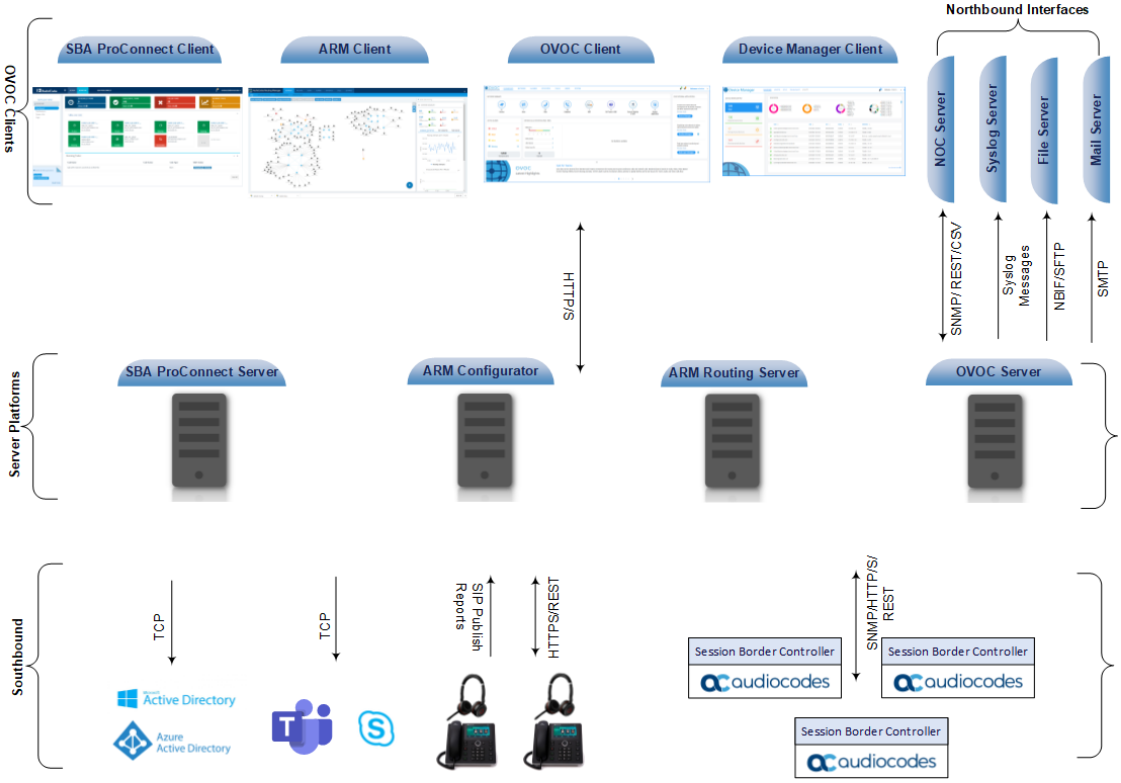
This section describes the key elements of the OVOC suite.

- **Remote Management of Entities:** Remote standards-based management of AudioCodes products within VoIP networks, covering all areas vital for their efficient operation, administration, management and security. A single user interface provides real time information including network and device component status, activity logs and alarms. Complete End-to-End network control includes data on all devices, all locations, all sizes, all network functions and services and full control over the network, including services, updates, upgrades, and operations.
- **Voice Quality Management:** Real-time Voice Quality statistics analysis enables the rapid identification of the metrics responsible for degradation in the quality of any VoIP call made over the network nodes including managed endpoints. It provides an accurate diagnostic and troubleshooting tool for analyzing quality problems in response to VoIP user criticism. It proactively prevents VoIP quality degradation and optimizes quality of experience for VoIP users.
  - Integration with Microsoft Teams Subscription Notifications service with Microsoft Graph API for retrieval of Calls data (subscriptions notifications) for users managed by a specific tenant including Teams peer-to-peer or Conference calls and network calls.
  - Integration with Skype for Business server SQL monitoring server to provide end-to-end VoIP quality monitoring of Skype for Business deployments. The OVOC server enables you to synchronize with the Enterprise network Active Directory user databases and monitor call quality for the Active Directory users.
  - Integrates and monitors with endpoints reporting RFC 6035 SIP PUBLISH packets.
- **Device Management:** AudioCodes' Device Manager Pro interface enables enterprise network administrators to effortlessly and effectively set up, configure and update up to 30000 400HD Series IP phones in globally distributed corporations. Remote management and configuration can be performed with no additional installation in case the devices are located on a remote site where an AudioCodes device may be installed on the remote site and used as an HTTP Proxy to traverse NAT and firewalls. AudioCodes' Device Manager Pro run using standard web browser supporting HTML5 such as Internet Explorer, Chrome or Firefox. REST (Representational State Transfer) based architecture enables statuses, commands and alarms to be communicated between the devices and the OVOC server. The device send their status to the server according to configured interval (e.g. one hour) for display. Management of devices through Cloud Services (SaaS) as a centralized hosting business or through Internet Telephony Service Providers (ITSPs). When devices are deployed behind a firewall or NAT, communication is facilitated through an agent application "Device Management Agent". This agent enables the OVOC server to initiate actions toward devices such as uploading firmware and configuration files.
- **Performance Monitoring:** Performance Monitoring analysis enables OVOC operators with network planning and administration in the OVOC topology through the collection of high-level historic data polled from the managed entities.

- **Simplified Routing:** Call routing configuration, previously handled by multiple SBC/Media Gateway devices, each requiring separate routing configurations, can be handled centrally by the ARM server. If an enterprise has an SBC in every branch, a single ARM, deployed in HQ, can route all calls in the globally distributed corporate network to PSTN, the local provider, enterprise headquarters, or to the IP network (Skype for Business/ Lync). Consequently, this saves considerable IT resources, by significantly reducing the configuration time. ARM can also synchronize with the Active Directory for user-based routing.
- **SBA ProConnect:** The SBA Pro Connect is a Web Management tool designed for servicing the installation base for large SBA deployments. This tool enables you to perform the following actions:
  - Upgrade from Microsoft Lync 2010/13 to Skype for Business.
  - Mass Microsoft Cumulative Updates (CU)
  - Upgrade process monitoring and notifications
  - Task scheduling
  - Segmentation of SBAs into groups for selective upgrade
- **Tool for AudioCodes Professional Services:** Prior to the deployment of AudioCodes products, AudioCodes professional services team are often contracted to conduct a readiness analysis of the customer's VoIP network. This analysis includes the voice quality analysis of existing network, network capacity limits assessment for voice traffic (e.g. peak hours) and voice quality analysis across LAN and WAN (multiple sites and remote users). Once the analysis is complete, recommendations are made on the best-fit deployment of AudioCodes products.

The figure below illustrates the OVOC products' suite architecture:

Figure 1-1: OVOC Architecture



Key Interface Elements

The figures below display examples of the OVOC Map view which represents the OVOC topology transposed over a map indicating the location of managed entities. Clicking a specific tenant or region node opens a magnified view of the site installations for the selected tenant or region.

Figure 1-2: OVOC Dashboard

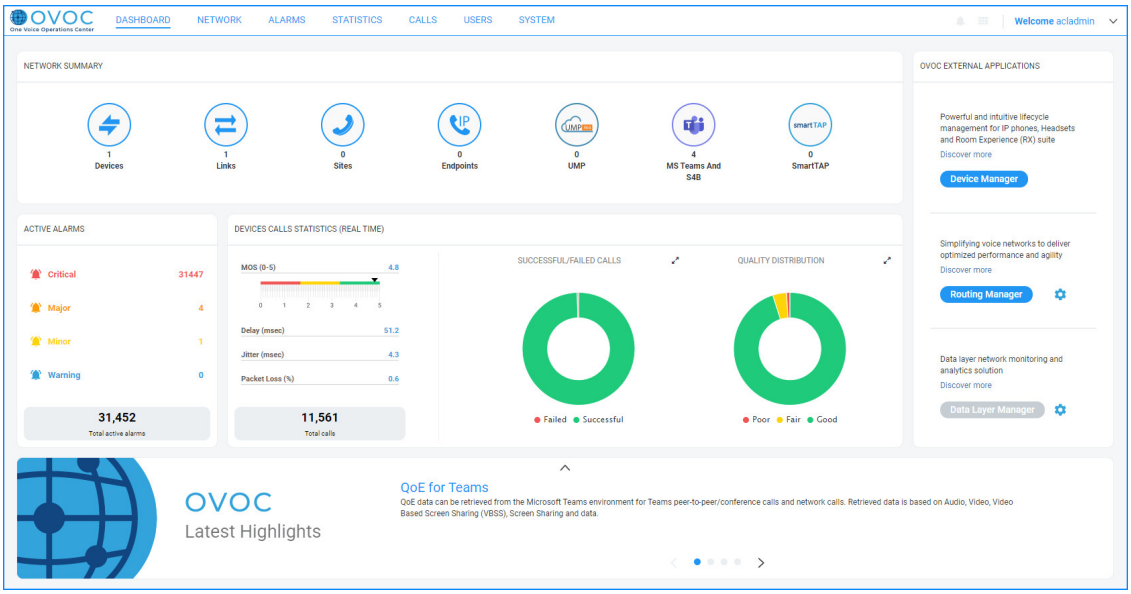
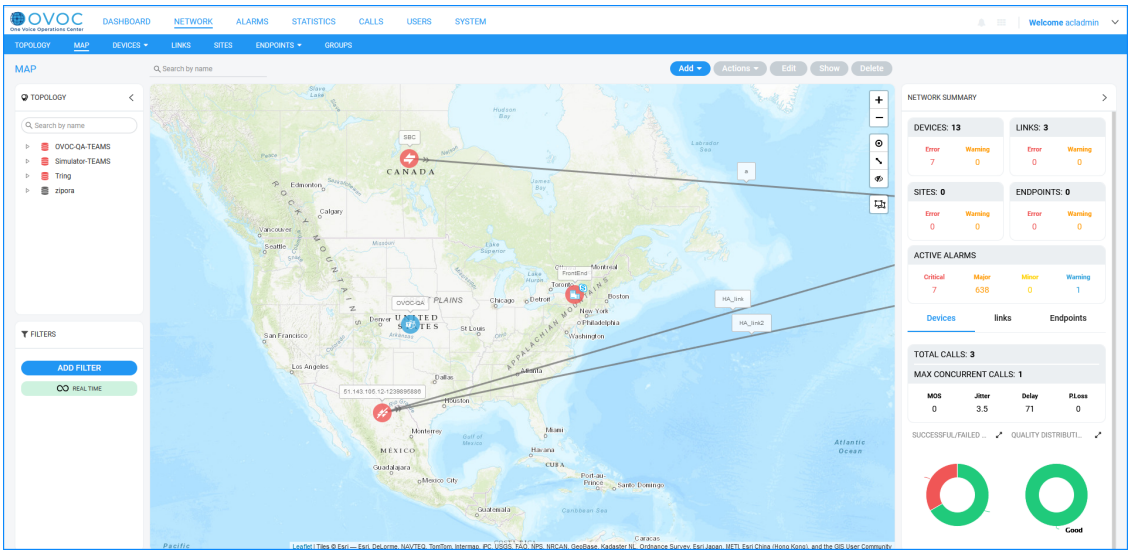


Figure 1-3: OVOC Network Maps



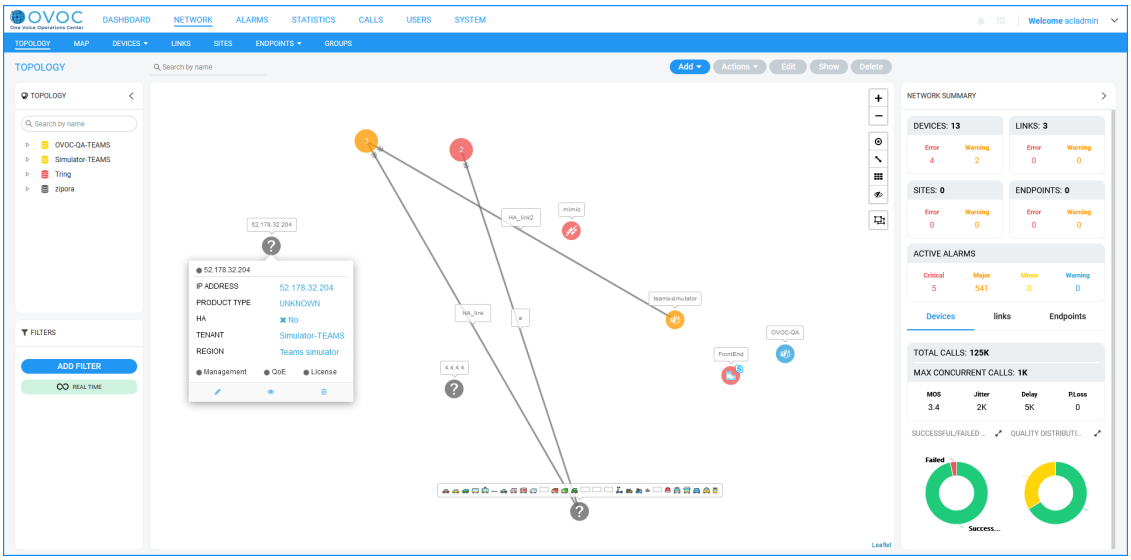
The Geo Map/Topology view consists of the following elements:

- **OVOC Dashboard:** The OVOC dashboard provides a snapshot view of the state of the OVOC network for all managed entities and external applications including the following:

- Aggregation of the number of managed entities for each managed device type. For example, 29 Devices indicates that OVOC currently manages a total of 29 SBC / MSBR / gateway devices.
- Links to the corresponding entity status page. For example, clicking the Devices icon opens the Devices page for all managed AudioCodes devices.
- Aggregation of the active alarms for all managed entities and link to the Active Alarms page.
- Aggregation of call statistics and link to the Device Statistics page
- Links to the login page for each of the supported external application management interfaces

- **Regions pane:** This pane allows you to manage and check the health of the Topology tree which consists of of Tenants, Regions and Sites.
- **Topology/Map:** This is the main view which shows all of the managed devices and links.
- **Network Summary pane:** This pane shows the following:
  - A summary of all devices, links, sites and endpoints, listing the number of errors and warnings for each of these entities.
  - A list of active alarms including a division for critical, major and minor alarms.
  - QoE statistics for all devices, links and endpoints.
- **Real-Time Color-Coded operative statuses for all nodes associated with the tenant:** Color-Coded indications of the operative states of all tenants and their associated nodes. The indications include operative and health state of all nodes under this tenant.
- **Filters:** Filtering is a powerful feature of the interface that allows you to display only information that is relevant to the current monitoring activity or analysis. For example, you can filter based on a time range, or based on the Topology i.e. you can display information that is only associated to a specific tenant.
- **Context-Sensitive Entity Actions:** Context-sensitive action button options differ according to the configured entity and relevant view. For example, on the device's page, you can perform Upload and Download of files or Reset. On the License Manager page, available actions include Apply License or Refresh License.
- **Smart Devices and Links Aggregation in Network Map View:** Support for viewing aggregating of device statuses (Network Topology view). Devices and links are aggregated into clusters where the number of devices and links in each cluster are indicated. Clicking the parent cluster node, opens the sub-nodes or sub-clusters according to the next aggregation level. In addition, you can select shift and click (make area selection) and drag to select specific devices. For links, an indication is also provided whether the link is configured to show only incoming or outgoing calls with an arrow showing the link direction. You can zoom in and out to display different aggregated clusters of devices and links i.e. when you zoom out to the maximum, you see the total aggregated devices and links for the installation.

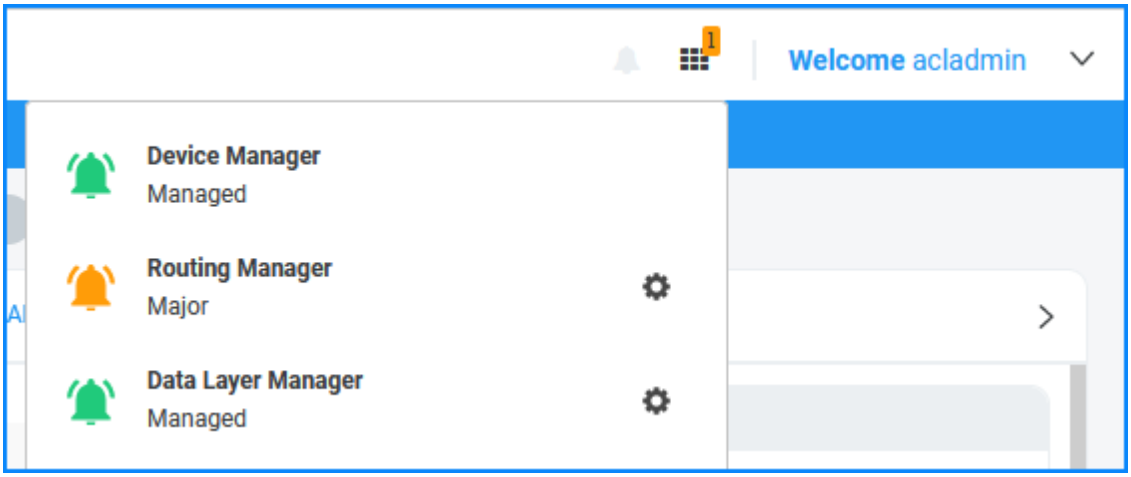
Figure 1-4: Device and Link Aggregation



External Application Integration

The OVOC platform enables you to connect to external applications. The status window keeps track of these applications and enables you to access them from the Status screen.

Figure 1-5: External Application Integration



OVOC License Management for Enterprise Devices

Licenses for AudioCodes Gateway and SBC devices can be managed using the following methods:

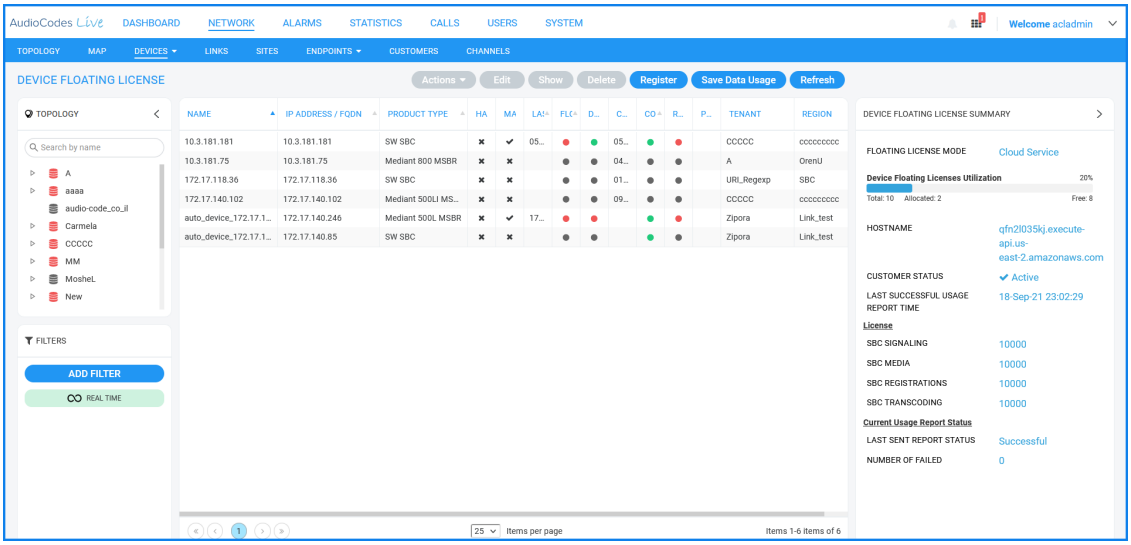
- Local license installed on the device
- Fixed License Pool on page 11
- Floating License below

Floating License

The Floating License service, managed as an AudioCodes Cloud service provides a network-wide license intended for customer deployments with multiple SBCs sharing a dynamic pool of SBC resources. The Floating License simplifies network capacity planning, and provides cost benefits related to aggregated calls statistics, follow-the-sun scenarios and on disaster recovery setups which involve two or more data centers. The Floating license operates in the following modes:

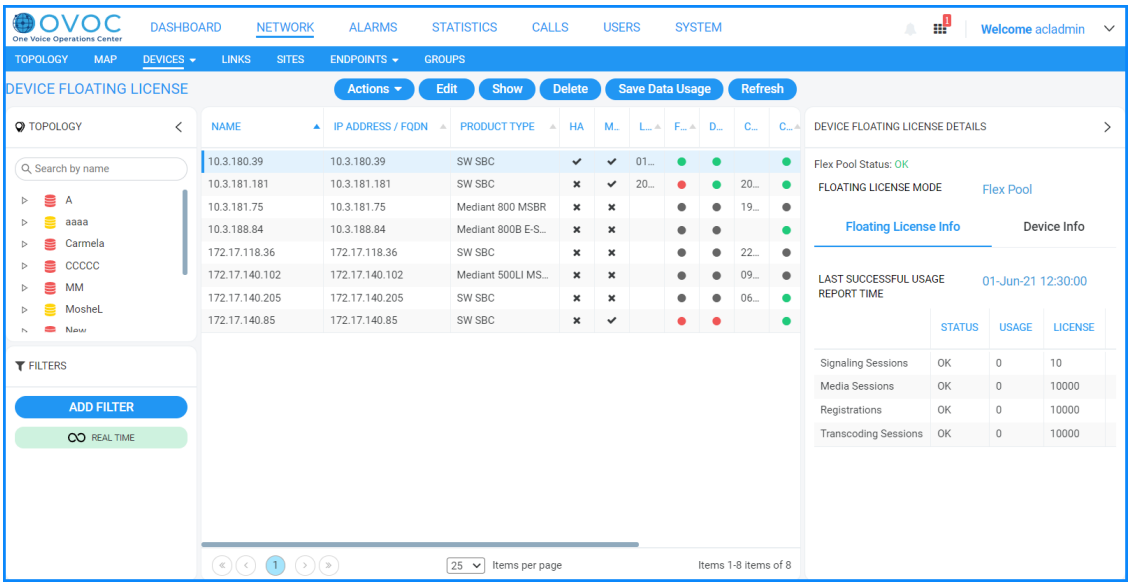
- **Cloud Mode:** This mode manages the license per tenant in the Cloud using the AudioCodes Floating License Service. This model implements 'pay as you grow' model. If the license limits are exceeded, incremental billing is automatically enforced, thereby eliminating the need to manually purchase additional SBC licenses when capacity requirements are increased.

Figure 1-6: Cloud Service



- **FlexPool Mode:** This mode supports a Floating License across a network without the need to connect to a public cloud. If the license limits are exceeded, service is disrupted for a percentage of managed devices and for the remainder of devices allowed to continue uninterrupted for a grace period . Once the grace period has expired, services are disrupted for all managed devices. Priorities can be assigned in the Devices page per device ("Low", "Normal" and "High") to determine the order of devices to which service is disrupted. The license limit mechanism is managed per parameter feature e.g. SBC Sessions.

Figure 1-7: FlexPool



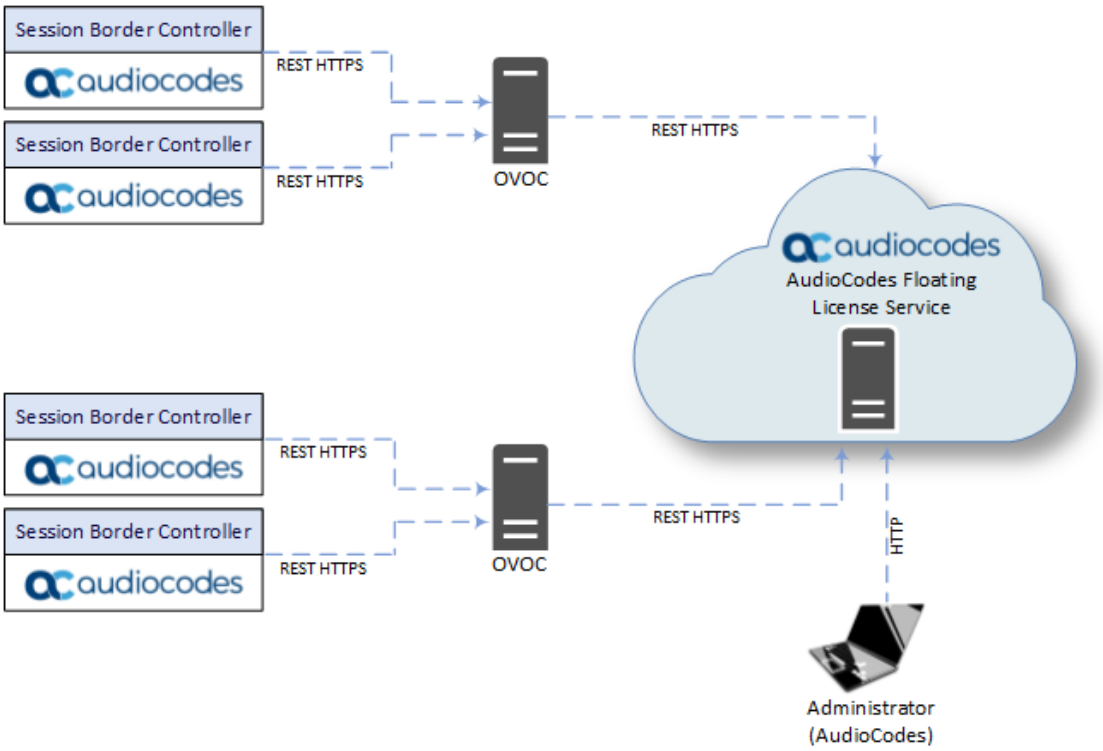
The SBCs deployed in the network are "open" to utilize the maximum hardware capacity of the device based on pre-defined profiles or can be configured by users with customized session capacity profiles. The Floating License includes the following parameters:

- **SBC Sessions:** the number of concurrent SBC call sessions (media and signaling)
- **SBC Signaling Sessions**: the number of concurrent SIP messages (signaling only)
- **Registrations:** The number of SIP endpoints that can register on the SBC devices.
- **Transcoding Sessions:** The number of concurrent codec types
- **SBC Sessions:** The number of SBC devices that can be managed (FlexPool mode only)

The managed SBC devices report their capacity consumption to OVOC every five minutes. For the Cloud mode, OVOC sends this information to the AudioCodes Floating License cloud service.

If the SBC device does not receive acknowledgment from the OVOC server that Usage reports have been received (by default within 90 days) , then service is shutdown for this SBC device. The SBC must then reestablish connection with the OVOC server. The figure below illustrates an example topology with two OVOC managed customer sites connected to AudioCodes Cloud License Manager Web service.

Figure 1-8: Floating License Service



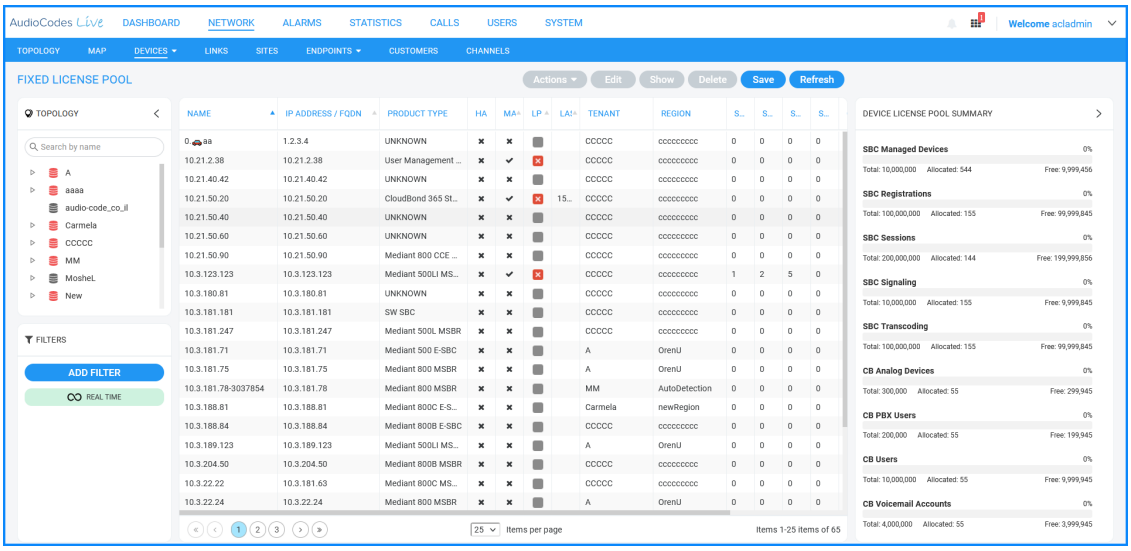
Fixed License Pool

The OVOC License Pool Manager enables operators to centrally manage and distribute session licenses for multiple devices using a flexible license pool. The operator can allocate and de-allocate the licenses for the devices in the pool according to their capacity requirements. This tool enables the following:

- License management between devices without changing the devices' local license key.
- Adding and removing licenses for devices according to site requirements without the need to contact AudioCodes. The License Pool feature does not require a new License key file per device from AudioCodes each time the user wishes to apply different settings to each device.
- Enables service providers to manage licenses for multiple customers by using the license pool to allocate licenses between them.

The operator can manage the various license parameters such as SBC session or SBC registrations using the License Pool Manager.

Figure 1-9: OVOC License Pool Manager



2 OVOC Requirements and Capacities

This chapter describes the OVOC requirements and capacities.

OVOC Requirements

Table 2-1: OVOC Server Minimum Requirements

Resources	Virtual Platform	Memory	Recommended Disk Space	Minimum Disk Space (OS + Data)	Processors
Low Profile					
VMWare	■ VMware: ESXi 8.0 ■ VMware HA cluster: VMware ESXi 6.0	24 GiB RAM	500 GB	320 GiB	■ 1 core with at least 2.5 GHz ■ 2 cores with at least 2.0 GHz
HyperV	■ Microsoft Hyper-V Server 2016 ■ Microsoft Hyper-V Server 2016 HA Cluster	24 GiB RAM	500 GB	320 GiB	■ 1 core with at least 2.5 GHz ■ 2 cores with at least 2.0 GHz
Azure	Size: D8ds_v4	32 GiB	500 GB SSD Premium	320 GiB	8 vCPUs
AWS	InstanceSize: m5.2xlarge	32 GiB	AWS EBS: General Purpose SSD (GP2) 500 GB	320 GiB	8 vCPUs
High Profile					
VMWare	■ VMware: ESXi 8.0 ■ VMware HA cluster: VMware ESXi 6.0	40 GiB RAM	1.2 TB	520 GiB	6 cores with at least 2 GHz
HyperV	■ Microsoft Hyper-V Server 2016 ■ Microsoft Hyper-V Server 2016 HA Cluster	40 GiB RAM	1.2 TB	520 GiB)	6 cores with at least 2 GHz
Azure	Size: D16ds_v4	64 GiB	2 TB SSD Premium	520 GiB	16 vCPUs
AWS	InstanceSize: m5.4xlarge	64 GiB	AWS EBS: General Purpose SSD (GP2) 2TB	520 GiB	16 vCPUs
Bare Metal (HP DL360p Gen10)					
	-	64 GiB	Disk: 2x 1.92 TB SSD configured in RAID 0		■ Intel ®Xeon ®Cascade Gold 6226R (16 cores 2.6 GHz each) ■ Intel ®Xeon ® Gold 6126 (12 cores 2.60 GHz each)
SP Single					
	VMware: ESXi 8.0 and VMware HA cluster: VMware ESXi 6.0	256 GB	Standalone mode: SSD 6TB with Ethernet ports: 10GB ports	~1.25T SSD	24 cores at 2.60 GHz

Table 2-2: OVOC Client Minimum Requirements

Resource	OVOC Client
Hardware	Screen resolution: 1280 x 1024
Operating System	Windows 10 or later
Memory	8 GB RAM
Disk Space	-
Processor	-
Web Browsers	■ Mozilla Firefox version 120 and higher ■ Google Chrome version 119 and higher ■ Microsoft Edge Browser version 119 and higher
Scripts	■ PHP Version 7.4 ■ Angular 10.0

OVOC Capacities

The following table shows the performance and data storage capabilities for the OVOC managed devices and endpoints.

Table 2-3: OVOC Capacities

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server
OVOC Management Capacity				
Managed devices	100	5,000	5,000	10,000
Links	200	10,000	10,000	10,000
Operators	25			
Device Manager Pro				
Managed devices (see Device Manager Communication and Optimization on page 16) for further details).	1,000	■ 30,000 Microsoft Lync/Skype for Business and third-party vendor devices ■ 20,000 Microsoft Teams devices	■ 10,000 Microsoft Lync/Skype for Business and third-party vendor devices Including phones, headsets and Conference Suite devices. ■ 20,000 Microsoft Teams devices	■ 30,000 Skype for Business devices and third-party vendor devices Including phones, headsets and Conference Suite devices. ■ 20,000 Teams device
Disk space allocated for firmware files	5 GB	10 GB		
Alarm and Journal Capacity				
History alarms	Up to 12 months or 10,000,000 million alarms			
Journal logs	Up to 12 months			
Steady state	20 alarms per second			50 alarms per second
Performance Monitoring				
Polled parameters per polling interval per OVOC-managed device	50,000	100,000	100,000	500,000

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server
Polled parameters per polling interval per OVOC instance	50,000	500,000	500,000	1,000,000
Storage time	One year			
QoE Call Flow (for SBC calls only)				
Maximum managed devices with QoE call flows	10	100	100	300
CAPS per OVOC instance	6	25	100	300
Maximum number of calls	1,000,000	1,000,000	1,000,000	10,000,000
OVOC QoE for Devices				
QoE for managed devices	100	1,200	3,000	10,000
CAPS (calls attempts per second) per device	30	120	300	1,000
CAPS per OVOC instance (SBC and SFB/Teams and RFC SIP Publish 6035)	30 Teams CAPS=30[1]	120 Teams CAPS=120[2]	300	1,000 Teams CAPS=[3]
QoE concurrent sessions	3,000	12,000	30,000	100,000
Call Details Storage - detailed information per call	Up to one year or 6,000,000	Up to one year or 80,000,000	Up to one year or 80,000,000	Up to one year or 200,000,000
Calls Statistics Storage - statistics information storage	Up to one year or 12,000,000	Up to one year or 150,000,000	Up to one year or 150,000,000	Up to one year or 500,000,000
QoE Capacity with SBC Floating License Capability				
CAPS (calls attempts per second) per OVOC instance with SIP call flow.	5	22	90	-
CAPS (calls attempts per second) per OVOC instance without SIP call flow.	27	108	270	-
Managed devices with floating license.	100	500	1,000	-
Lync and AD Servers– applicable for QoE license only				
MS Lync servers	Up to 2			
AD Servers for Users sync	Up to 2			
Users sync	Up to 150,000			
TEAMS Customer	up to 7[4]			

[1]The TEAMS CAPS estimation is based on round trip delay of 500 milliseconds to Microsoft Azure.

[2]As above

[3]Please contact AudioCodes OVOC Product Manager

[4]For additional support, contact AudioCodes Product Manager

Device Manager Communication and Optimization

All devices operate behind Network Address Translation (NAT) and utilize keep-alive messages to maintain connectivity. The system is designed to support up to 30,000 devices, with a default keep-alive interval of 10 minutes. To optimize the response time for actions performed on the devices, it is possible to reduce the keep-alive interval. The recommended keep-alive interval depends on the number of devices in the system: For deployments with up to 5,000 devices, a keep-alive interval of one minute is recommended. For every additional 5,000 devices, add two minutes to the keep-alive interval. The maximum recommended keep-alive interval is 10 minutes for deployments with 30,000 devices.

By adjusting the keep-alive interval based on the number of devices in the system, it is possible to optimize the response time for device actions. However, it is crucial to consider the trade-offs between response time and network overhead. Regular monitoring and performance tuning should be conducted to ensure the system operates efficiently and meets the desired performance goals.

3 Managed VoIP Equipment

Table 3-1: Managed VoIP Equipment

Product	Supported Software Version
Gateway, SBC and MSBR Devices	
Mediant 9000 SBC	Versions 7.0, 6.8
Mediant 9030 SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2
Mediant 9080 SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2
Mediant 4000 SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2, 7.0, 6.8
Mediant 4000B SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2, 7.0
Mediant 2600 E-SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2, 7.0, 6.8
Mediant 2600B E-SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2 and 7.0
Mediant Software SBC (Virtual Edition)	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2.2x, 7.2, 7.0, 6.8
Mediant Software SBC (Cloud Edition)	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2 (including support for MTC), 7.0, 6.8
Mediant Software SBC (Server Edition)	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2 (including support for MTC), 7.0, 6.8
Mediant3000 (TP-8410 and TP-6310)	7.0 (SIP), 6.8 (SIP), 6.6 (SIP)
Mediant 3100 SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.0
Mediant 2000 Media Gateways	Version 6.6
Mediant 1000 Gateway[1]	Version 6.6 (SIP)
Mediant 1000B Gateway and E-SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2., 7.0, 6.8, 6.6
Mediant 800B Gateway and E-SBC	Versions 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2, 7.0, 6.8, 6.6
Mediant 800C	Version 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2

[1] This product does not support Voice Quality Management.

Product	Supported Software Version
Mediant 600[1]	Version 6.6
Mediant 500 E-SBC	Version 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2
Mediant 500L E-SBC	Version 7.60A.xxx.xxx, **7.4.600**, 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2
Mediant 1000B MSBR	Version 6.6
Mediant800 MSBR	Versions 7.26.xx, 7.24.xx, 7.2, 6.8, 6.6
Mediant500 MSBR	Version 7.26.xx, 7.24.xx, 7.2, 6.8
Mediant 500L MSBR	Versions 7.26.xx, 7.24.xx , 7.2, 6.8
Mediant 500Li MSBR	Version 7.26.xx, 7.24.xx, 7.20.x.x
Mediant 800Ci MSBR	Version 7.26.xx, 7.24.xx
MP-504	Version 7.26.xx
MP-508	Version 7.26.xx
MP-532	Version 7.26.xx
MediaPack MP-11x series	Version 6.6 (SIP)
MediaPack MP-124	Version 6.6 (SIP) Rev. D and E
MP-1288	Version 7.4.500, 7.4.400, 7.4.300, 7.4.200, 7.4.100, 7.4, 7.2.2x, 7.2
MP-202	Version 4.4.9 Rev. B, D and R
MP-204	Version 4.4.9 Rev. B, D and R
SBA[2]	Product
Microsoft Lync	■ Mediant 800B SBA-Version 1.1.12.x and later and gateway Version 6.8 ■ Mediant 1000B SBA-Version 1.1.12.x and later and gateway Version 6.8 ■ Mediant 2000B SBA-Version 1.1.12.x and later and gateway Version 6.8
Microsoft Skype for Business	■ Mediant 800B SBA-Version 1.1.12.x and later and gateway Version 7.2 ■ Mediant 800C SBA-Version 1.1.12.x and later and gateway Version 7.2 ■ Mediant 1000B SBA-Version 1.1.12.x and later and gateway Version 7.2 ■ Mediant 2600B SBA-Version 1.1.12.x and later and gateway Version 7.0
CloudBond[3]	
CloudBond 365	Version 7.6 (with MediantVersion 7.2.100 and later)

[1] As above

[2] As above

[3] To support Voice Quality Management for these devices, customers should add the SBC/Media Gateway platform of the CloudBond 365 /CCE Appliances as standalone devices to the OVOC. Once this is done, the SBC/Gateway calls passing through the CloudBond 365 /CCE Appliances can be monitored.

Product	Supported Software Version
Pro Edition	
CloudBond 365 Enterprise Edition	Version 7.6 (with MediantVersion 7.2.100 and later)
CloudBond 365 Standard + Edition	Version 7.6 (with Mediant800B Version 7.2.100 and later)
CloudBond 365 Standard	Version 7.6 (with Mediant 800B Version 7.2.100 and later)
CloudBond 365	Version 8.0.0 (Skype for Business 2019 and Microsoft Teams
User Management Pack 365	
User Management Pack 365	Version 7.8.100
User Management Pack 365 ENT	Version 8.0.0
User Management Pack 365 SP Version	8.0.450, 8.0.400, 8.0.300, 8.0.220, 8.0.200, 8.0.100
Meetings and Recordings	
SmartTAP 360° Live Recording	Version 5.6, 5.5, 5.4, Ver. 5.3, Ver. 5.2, Ver. 5.1, Ver. 5.0, Version 4.3
Meeting Insights	Version 2.0.44.27
Voca Conversational Interaction Center	Version 8.4
Voice AI Connect	Version 3.12
Generic Applications	
Fax and Auto-Attendant (IVR)	Version 2.6.200
Microsoft Teams Direct Routing SBA	
Mediant 800B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 800C DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 1000B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 2600B DR-SBA	SBA Version 1.0.1xx and later with SBC certified by Microsoft.
Mediant DR-SBA Virtual Appliance	SBA Version 1.0.1x.x and later with SBC certified by Microsoft.
AudioCodes Routing Manager (ARM)	Version 9.8
Device Management	
400HD Series Lync server	From Version 2.0.13: 420HD, 430HD 440HD

Product	Supported Software Version
Generic SIP server	From Version 2.2.2: 420HD, 430HD 440HD, 405HD and 405 From Version 3.4.3: C450HD, 450HD, 445HD and RX50
400HD Series Skype for Business-Teams-compatible devices	■ From Version 3.0.0: 420HD, 430HD 440HD and 405HD. ■ From Version 3.0.1: 420HD, 430HD 440HD, 405HD and 450HD. ■ From Version 3.0.2: HRS 457 (with Jabra firmware support). ■ From Version 3.1.0: 445HD, 430HD 440HD, 405HD, 450HD and HRS. ■ From Version 3.2.0 C450HD. ■ From Version 3.2.1: C450HD, 445HD, 430HD 440HD, 405HD,450HD, HRS 457D and HRS 458. ■ From Version 3.4.2: RX50 Conference Phone ■ From Version 1.5: C448HD and C450HD ■ From Version 1.12.33: C435HD ■ From Version 1.8: C470HD ■ From Version 1.9: RXV80 Video Collaboration Bar ■ From Version 1.15: C455HD ■ From Version 2.0: MTRfA for Meeting Room Solution ■ From Version 1.18: MTRfWA/RXV81 Meeting RoomSolution ■ From AudioCodes AppSuite Version 1.0.0.0: MTRfW/RXV100 Meeting Room Solution ■ From Version 2.2: RX-PANEL ■ From Version 2.2: RXV200
Device Management - Third-party Vendor Products	
Spectralink	Spectralink 8440
Polycom	
Polycom Trio 8800	Polycom Trio 8800
Polycom VVX	Polycom VVX
CCX 500/600 phones	CCX 500/600 phones
Jabra Headset Support*	Jabra BIZ, Jabra Coach, Jabra DIAL, Jabra Eclipse, Jabra Elite, Jabra Engage, Jabra Evolve, Jabra Handset, Jabra LINK, Jabra Motion, Jabra Pro, Jabra Pulse, Jabra SPEAK, Jabra Sport, Jabra STEALTH, Jabra Steel, Jabra SUPREME. For a complete list of supported Jabra phones, see document Device Manager for Third-Party Vendor Products Administrator's Manual.
EPOS	For a list of supported devices, see: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/epos/fact-sheet-epos-manager-en.pdf

- All Versions VoIP equipment work with the SIP control protocol.
- Bold refers to new product support and Version support.
- *Supported Jabra models interwork with the Jabra Integration Service.

4 OVOC Server

This chapter describes the key features of the OVOC server platform.

- **Installation platform:**
  - On dedicated hardware
  - On a virtual machine: VMware or HyperV
  - On the cloud: Amazon AWS or Microsoft Azure
- **High Availability:** OVOC supports HA on the VMware or HyperV platforms by using the existing virtualization high availability features (e.g. VMware vSphere).

High Availability is not supported for OVOC servers on a Bare Metal platform.

- **Database:** PostgreSQL. This streamlined database is installed as part of the clean installation and upgrade process.The data migration process does not include calls, statistics, and alarms. Upgrade is only possible from OVOC version 8.0 and later.
- **Backup and Restore:**

  OVOC can automatically periodically back up device configurations (ini or MSBR CLI script) files according to OVOC server application time.

  Device ini and CLI script files are saved on the OVOC server machine in the /data/NBIF/mgBackup/ folder. These files can be accessed and transferred using SSH, and SFTP.

  Backup files are managed by the MG Backup Manager tool. This tool displays a summary for all files that have been backed up to OVOC for each device and a full listing of all backup files that have been saved to the MG Backup Manager for all devices.

  The user may rollback to former backup configuration in case of a disaster recovery handling in a single click.

  A lightweight mode enables partial backup of the OVOC database including OVOC topology and OVOC Web configuration. This prevents excessive downtime and reduces system utilization in the restore operation.
- **Networking:** Support for both IPv4 and IPv6 ethernet interfaces. SBC devices can connect to OVOC from different subnets to the respective interfaces on OVOC. Each IPv4 interface can be configured for NAT and one of the IPv4 interfaces can be configured to work in the Cloud Architecture mode. IPv6 support includes Alarm forwarding rules (SNMP and Syslog), PM Polling and configuration of IPv6 Ethernet Interfaces and IPv6 Static Routes on the OVOC server.
- **Storage:** OVOC provides recommended minimum disk sizes for all specifications and in addition supports disk downsizing for economizing disk storage costs.

- **Security Management:**
  - Initial access to the OVOC application is secured via the Login screen, where access control consists of authentication and authorization with a user name and password. An OVOC operator is authenticated and authorized using either the local OVOC user management tools or a centralized RADIUS, LDAP server or Microsoft Azure. These credentials can also be used to login to the AudioCodes devices via a Single Sign-on mechanism. By default, OVOC manages its users in the local OVOC server database.
  - OVOC supports Security Assertion Markup Language (SAML) based authentication for managing operator authentication between an identity provider (IdP) and a service provider (SP). This authentication method can be applied at system and tenant level for all operator types.
  - The OVOC server supports the implementation of X.509 user-defined certificates on OVOC server components and on AudioCodes devices for customer deployments requiring mutual SSL authentication using their own SSL certificate implementation.
  - "Privacy" mode can been enabled to to prevent specific operators from viewing sensitive data for their managed elements (regions, sites, devices and links). This includes the masking of gateway and SBC phone numbers, and hiding of calls data.
  - **For devices:**
    - OVOC server and device communication is secured over SNMPv3 for maintenance actions and fault management.
    - HTTPS is used for upgrading software and loading regional files and REST communication.
  - **For endpoints:**
    - Used for downloading firmware and configuration files
    - Used for sending REST updates

All user names and passwords used by the OVOC application to access devices (including SNMP, HTTP and SSH) are stored encrypted in the OVOC database. All actions performed in OVOC are recorded in an Actions Journal.

5 Multi-Tenancy

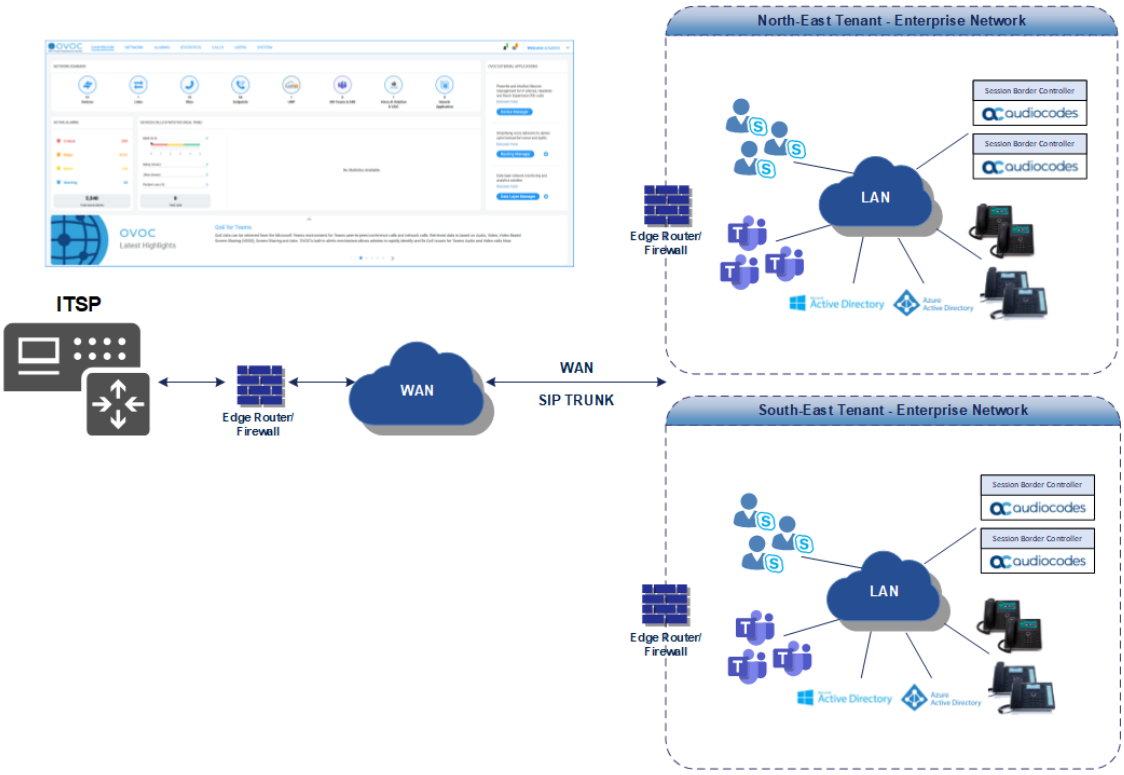
Multi-tenancy architecture enables large enterprises and service providers to install the One Voice Operations Center application in a Data Center and to remotely manage VoIP topology in multiple diverse locations. This may comprise of one of the following topologies:

- **ITSP Multi-Tenancy:** an ITSP can purchase a single instance of the OVOC application with a license to manage multiple tenants, where each tenant may represent an Enterprise customer.
- **Enterprise Multi-Tenancy:** an Enterprise can purchase a single instance of the OVOC application with a license to manage multiple tenants, where each tenant may represent a separate Enterprise entity.
- You can configure regions and sites under each tenant. For example, under the Europe tenant, you can configure the region Holland with sites Amsterdam and Rotterdam and the region Belgium with sites for Brussels and Antwerp.

ITSP Multi-Tenancy Architecture

ITSP multi- tenancy architecture allows an Internet Telephony Service Provider (ITSP) administrator to deploy a single instance of the OVOC application to provide a telephony network management service to multiple enterprise customers (tenants). Remote SNMP Management of devices over a WAN connection through a firewall is enabled through the Auto-detection mechanism.

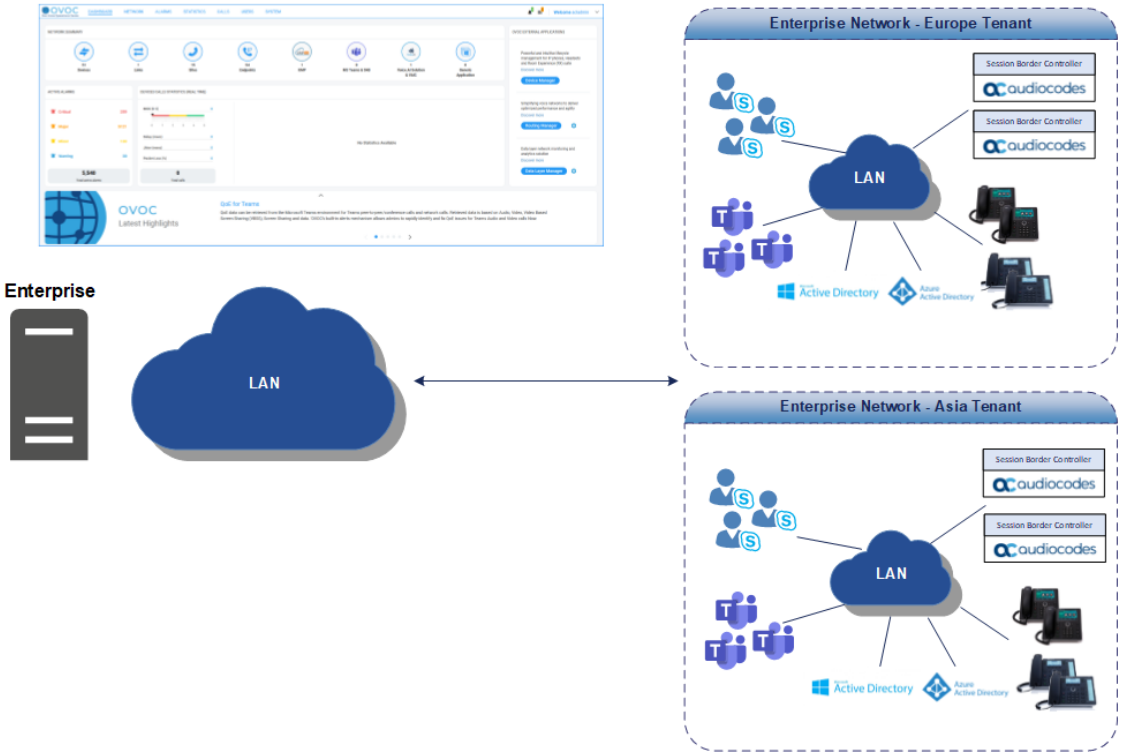
Figure 5-1: ITSP Multi-Tenancy Architecture



Enterprise Multi-Tenancy Architecture

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

Figure 5-2: Enterprise Multi-Tenancy Architecture



What is Managed Globally by OVOC?

The following elements are managed globally by OVOC:

- **Global resources:** OVOC server-related management including the OVOC server License, File Storage, Operating System, Server Backup and Restore and HA configuration.
- **Global entities:** security policy for operators, CA certificate assignment, storage policy, global alarm settings and device backup policy settings.
- **System entities:** system alarms, forwarding rules for system alarms and statistics reports.

What is Managed by the Tenant in the OVOC ?

The following elements are managed specifically by each tenant:

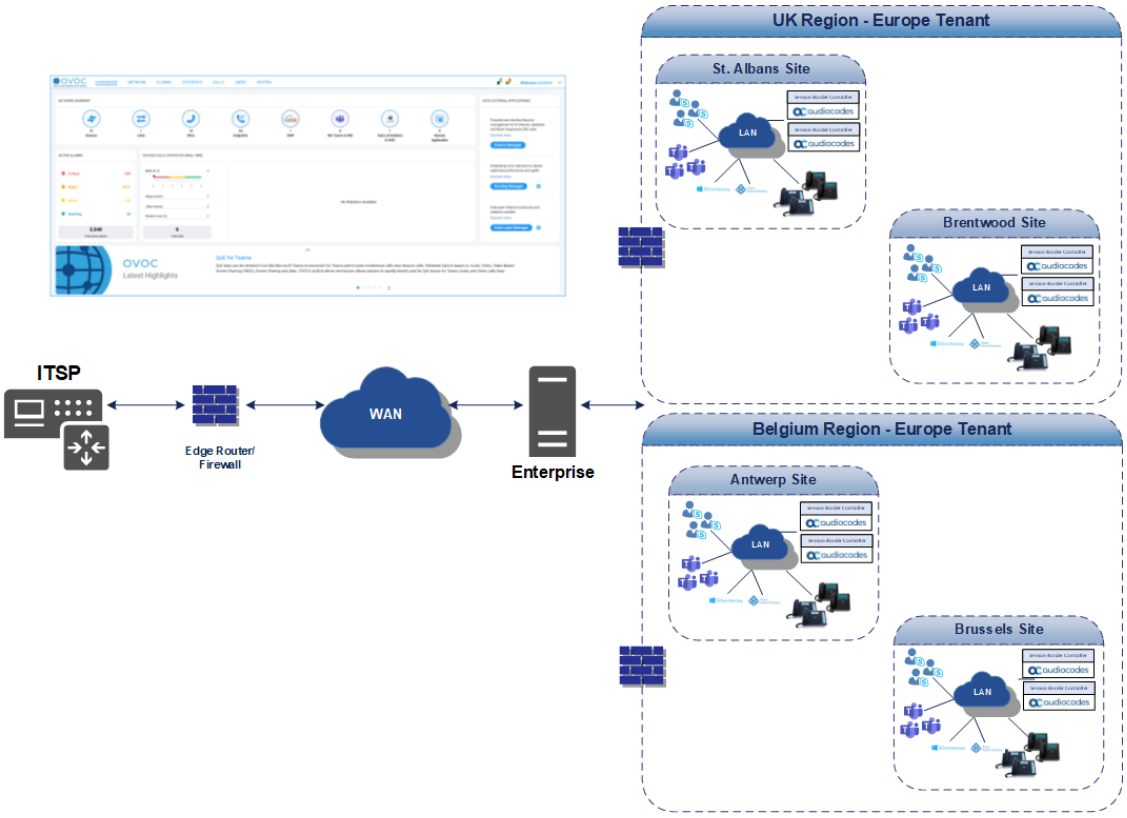
- **Tenant resources:** the portion of the OVOC server License that is allocated to the tenant.
- **Tenant entities:** all entities that are accessible for a specific tenant such as all regions, sites, devices, links, call hierarchies and summaries, journal records and alarms. In addition to statistics reports, alarm forwarding rules and threshold and alert rules.

For details of which actions can be performed according to Operator Security level, refer to the documentation of each specific feature in the OVOC User's Manual.

Monitoring Links

The Monitoring Links security profile allows multiple operators assigned to the same tenant to monitor a sub-set of links. For example, separate dedicated operators may be defined to manage links for Broadworks and Microsoft deployments;. Microsoft deployment between the Microsoft Edge Server IP Group and the Skype for Business Front End IP Group and for the Broadworks deployment between defined trunk groups and the BroadWorks Softswitch.The monitoring capabilities include viewing all call data for the managed link entities such as alarms and events and call statistics. This feature complements OVOC's existing ITSP multi-tenancy architecture that allows Service providers to deploy a single instance of the OVOC application to provide a telephony network management service to multiple enterprise tenants. The Monitoring Links operator's tenant is assigned to an LDAP Authentication Group, which is defined globally for all Monitoring Links operators for the OVOC server instance.

Figure 5-3: Monitoring Links



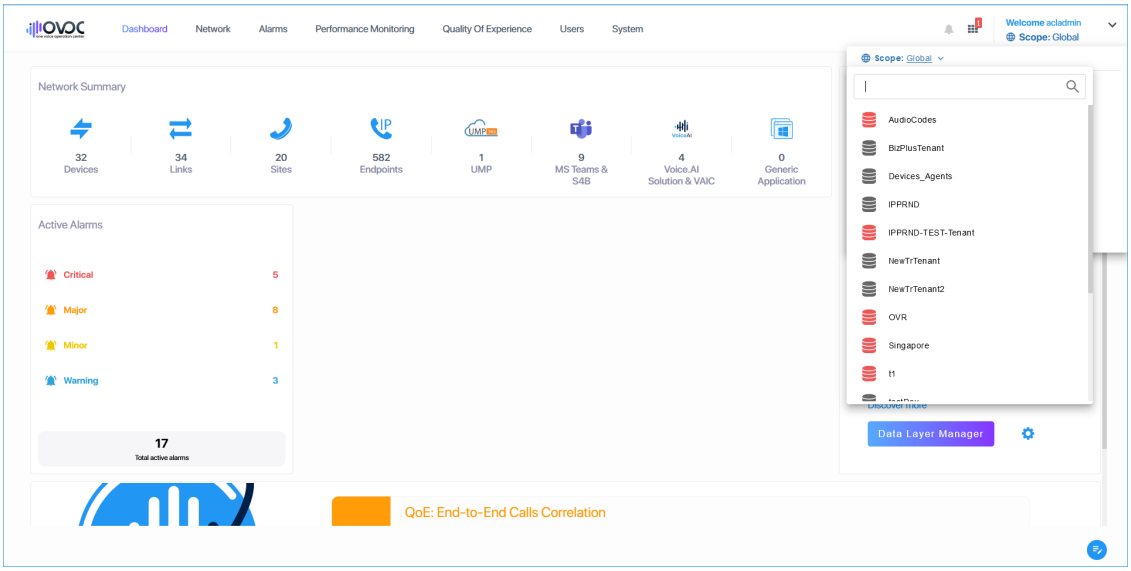
Groups

The "Group" entity provides a logical entity which contains devices, links and sites with the ability to filter all application topics, topology, calls, statistics and alarms.

6 Management Scope

Scope management determines access to OVOC according to operator role. The Global scope represents System operator permissions and the Tenant scope represents Tenant operator permissions. The Tenant scope has privileged access to Privacy data for GDPR compliance including: Analytics; QoE Statistics (Devices, Links Sites, Endpoints, PMs and AD user Locations); Calls and Reports. Phone numbers displayed in the Call Details can be masked for privacy GDPR by System operators. Privacy data (QoE Statistics) can optionally be migrated per tenant as part of the Upgrade scripts for compliance with GDPR regulations.

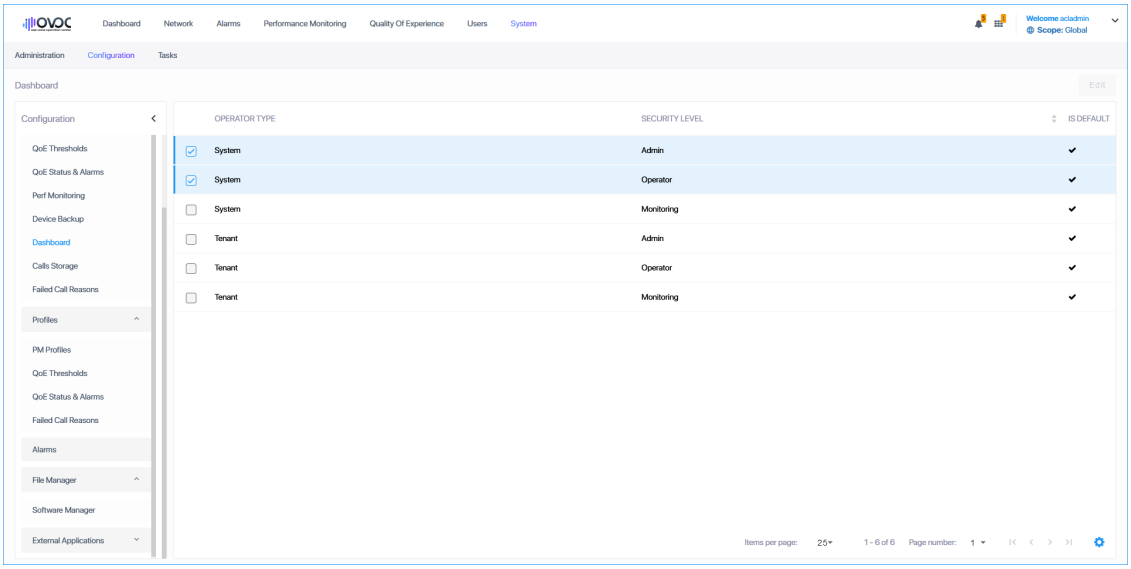
Scope is chosen from the 'Welcome' drop-down. Once a tenant is selected, data is filtered according to this tenant.



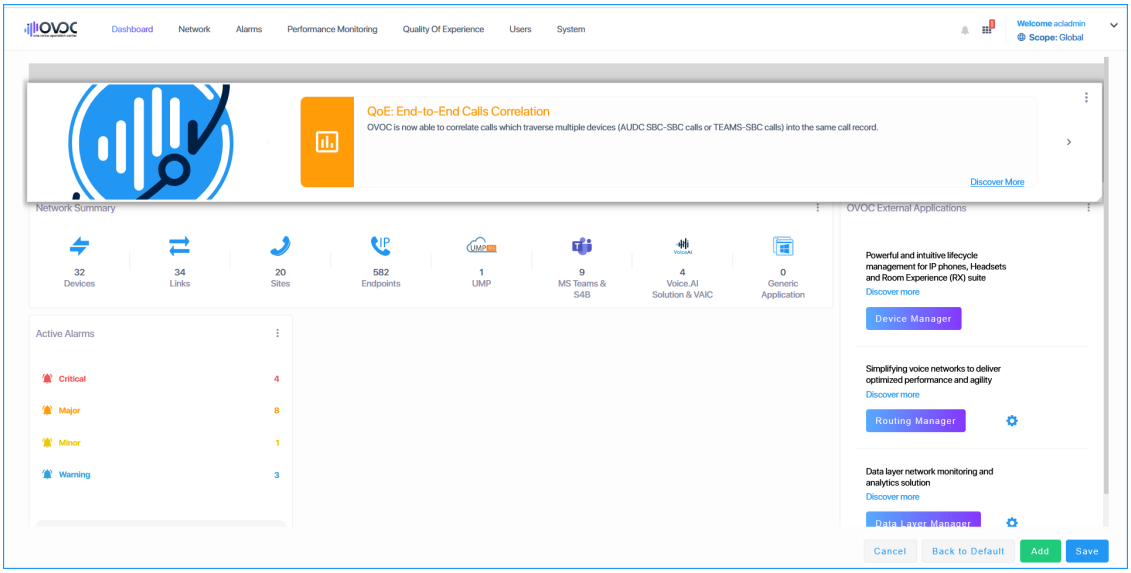
7 Customize Dashboard

OVOC Dashboard defaults can be customized per Operator Type and Security Level, in the Dashboard screen (**System** > **Configuration** > **Templates** > **Dashboard**).

The dashboard can be saved as part of the operator workspace.



In the OVOC Dashboard, icon allows rearranging elements by clicking-and-dragging, and then saving changes.



8 Provisioning and Commissioning

- **Automatic Device Detection:** Automatic detection enables devices to be added to OVOC automatically (without adding them manually in the OVOC). As soon as a device is configured with the OVOC server IP address and to send keep-alive messages, OVOC connects to the device or endpoint and automatically determines its firmware version and its subnet. The devices are then added to the appropriate tenant/region/site according to the best match to its subnet address. Devices that cannot be successfully matched are added to the Auto-Detection region under the default tenant. This feature is used also for NAT traversal, and allows SNMP communication with the devices when they are located behind NAT and are managed over a remote WAN connection.
- **Interoperability Automatic Provisioning for Devices:** The Interoperability Automatic Provisioning feature enables the mass deployment of multiple devices in your network. This is achieved by providing an automated mechanism for loading template configuration files and firmware files to new devices. This feature enables a quick-and-easy initial deployment of multiple devices in the customer network, with only minimal pre-configuration. Once the new device and OVOC connection is configured, the template configuration and firmware files can automatically be loaded to the device upon power up.
- **Device Manager Pro zero touch**: Enables the automatic download of configuration and firmware to the devices when they are initially connected to the network. A Configuration Profile Wizard enables the quick setup for connecting and initial provisioning of the Skype for Business devices to the OVOC server. The wizard lets you define initial settings, associate templates and configure the DHCP server. The configuration file templates lets network administrators customize configuration files per phone model, tenant, site, device and user. You can also apply template configurations for specific features, for example, Daylight Savings Time. Once the phones have been loaded with their initial configuration, you can provision specific phones with updates for groups of users or for individual users as shown in the example figure below. Phones can be provisioned with their template file either by defining a tenant in the URL in DHCP Option 160 or according to their subnet. If the network administrator does not define a tenant in the URL in DHCP Option 160, the phone is allocated a tenant/site according to best match i.e. according to either a tenant Subnet Mask or site Subnet Mask that is configured in Site/Tenant details in the OVOC Web. You can import (.csv files) and export (.zip files) containing configuration and phone firmware files. You can also import and export lists of users and devices. Both Skype for Business and non-Skype for Business users can be associated with devices upon user login (with user and password authentication) to the phone and therefore only users need to be imported to the IP Phone Manager in the pre-staging deployment stage.

9 RDP Support for Additional Windows-Based Devices

Support for opening an RDP session from Web via the Apache Guacamole VPN gateway to the Windows server residing the application. This feature supports 10 simultaneous Remote access sessions where the Administrator can view the list of active sessions and close (stop) sessions manually. This feature in OVOC 8.2 version supports the following applications:

- Voice.AI applications:
  - SmartTAP (support for RDP added in Version 8.2)
  - Meeting Insights (support for RDP added in Version 8.2)
  - Vocanom
- Generic Applications:
  - DR-SBA (support for RDP added in Version 8.2)
- UMP-365 Devices

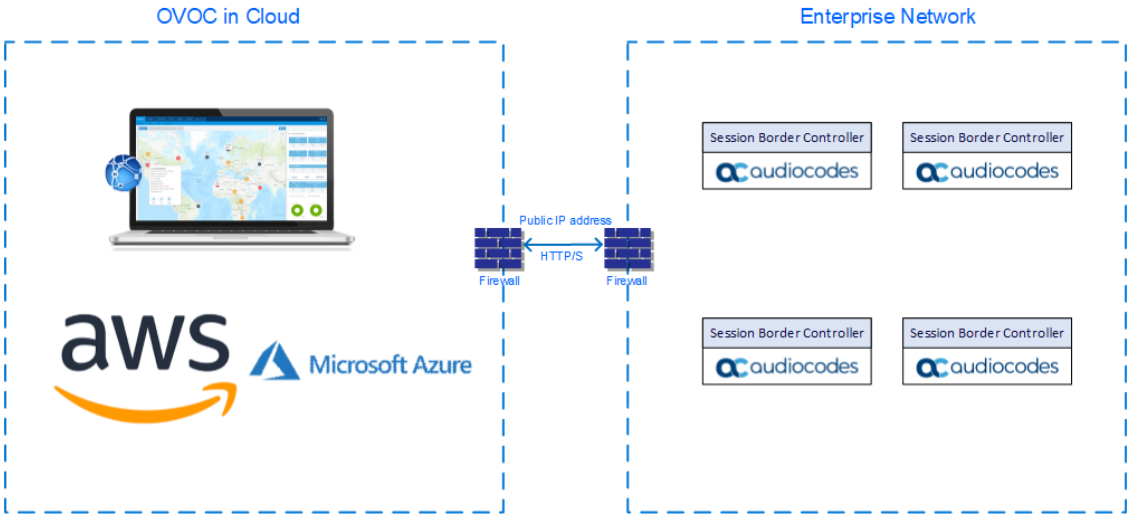
10 OVOC Cloud Architecture Mode

When OVOC is deployed in a Cloud environment, an automatic mechanism can be enabled to secure OVOC server and Device communication including SNMP, HTTP, syslog and debug recording through binding to a single dedicated HTTP/S tunnel through a generic WebSocket server connection. This mechanism provides the following benefits:

- Enables Single Sign-on to managed devices that are deployed behind a NAT
- Eliminates the need for administrators to manually manage firewall rules
- Eliminates the need to lease third-party VPN services

This deployment is illustrated in the figure below:

Figure 10-1: OVOC Cloud Deployment



This mode is supported for both Microsoft Azure and Amazon AWS deployments.

11 Call Storage Settings per Tenant

The following Call Storage settings can be configured per tenant:

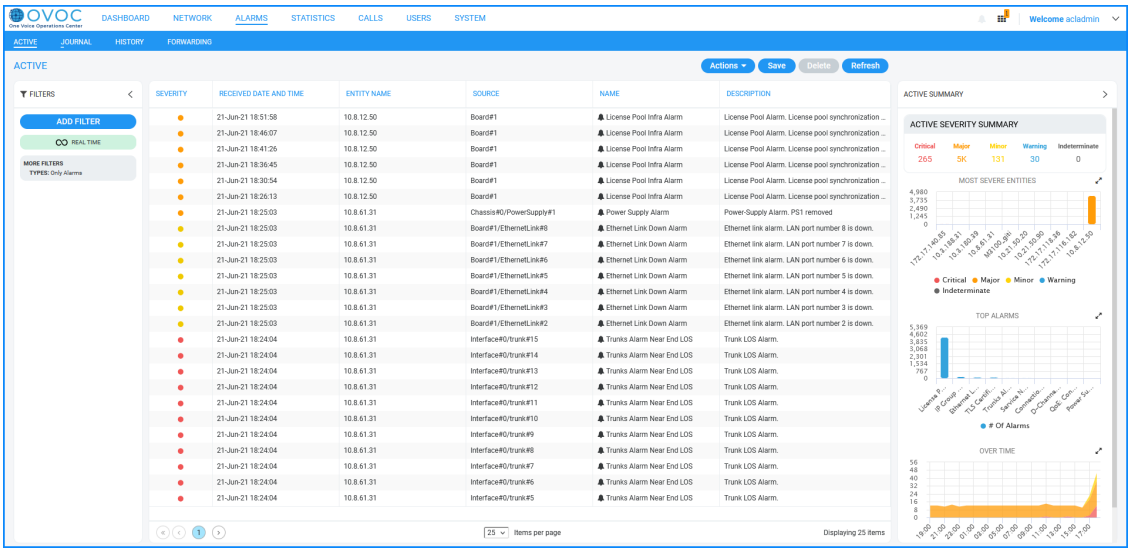
- Manage Call storage data according to the Call Quality category where you also can determine whether to save Call Flow and Call Trend data for each respective category.
- Set the storage periods that Calls-related data is kept on the OVOC server before its cleared.
- Determine whether to store URI and Location statistics.

12 Fault Management

The OVOC's high-level fault management functionality manages all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm view. Separate views are displayed for active and history alarms. OVOC can typically process 20 SNMP traps per second continuously. When an alarm is received, it is parsed, stored in the database and immediately displayed. The alarms are summarized in graphical reports according to key indicators such as distribution of alarm severities and alarm types. Operators can quickly isolate a problem's precise location i.e. Region, site or device and view all Journal records and Alarms History related to these contexts. You can also filter alarms according to specific criteria, such as time interval or device IP address. All traps received by the OVOC from managed entities and the ones that are issued by the OVOC itself can be forwarded to the NMS over SNMPv2c or SNMPv3. Active alarms can be synchronized to overcome network impairments. Device alarms and events can also be forwarded as Mail notifications or Syslog messages.

An aggregated list of alarm notifications can be forwarded from OVOC in a batch to a mail server in a single email according to the alarm filter settings in the Forwarding rule. Alarms can be forwarded to different destination types including SNMP, Syslog, REST and Mail Server.

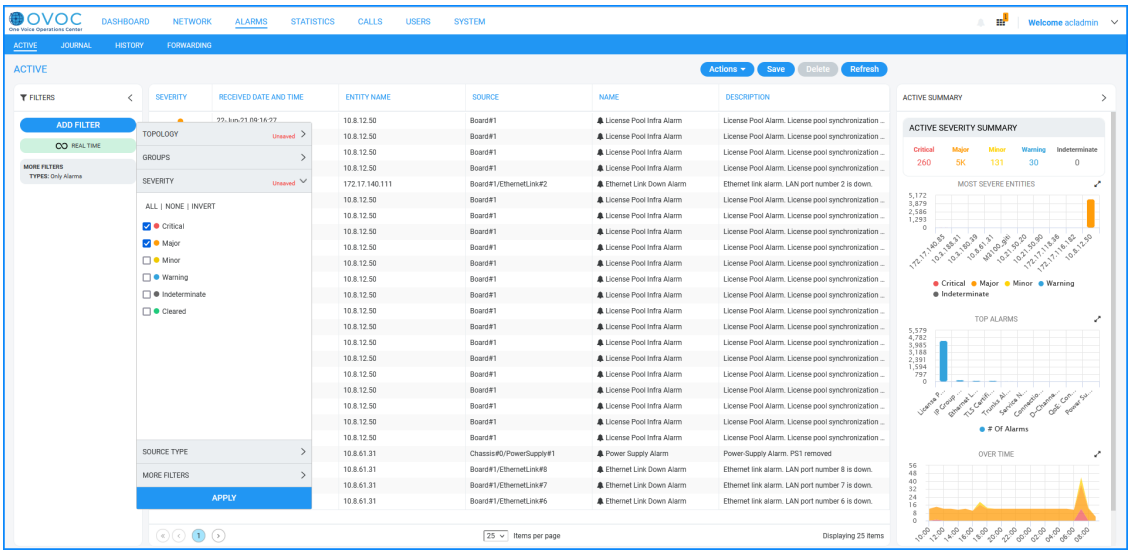
Figure 12-1: OVOC Alarms



Alarm Filtering

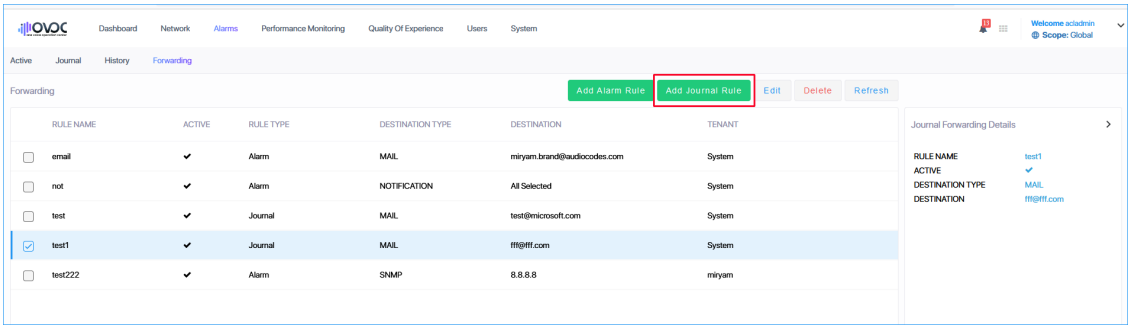
You can customize filters for alarms according to specific criteria, such as time interval,device IP address, severity or alarm name or type.The example below shows alarm filter criteria for a specific alarm 'GW Connection Alarm'.

Figure 12-2: Alarm Filtering



Journal Event Forwarding

Journal Rules can be forwarded as email or REST alerts like alarms. This feature is available for System operators only, for the purpose of Security Information and Event Management (SIEM) - System and Organization Controls (SOC) audits to enhance enterprise security and reduce risks.



Forwarding Alarms and Journal Alerts for Specific Time Ranges

Alarm and Journal rules can include time range criteria for determining when alarms and journal events are forwarded as alerts to their respective destinations. This prevents alerts from being sent during non-working hours or during times when operators do not wish to disturbed by alerts. Rule time ranges can easily be cloned to other days.

REST API Host Alarm Forwarding Destination

An alarm forwarding destination can be defined for a REST server host. This enables customers to categorize the alarms sent to the REST server through configuring Topology and Rule conditions according to their network logic. For example, enabling alarms forwarding for the default tenant and its sub-entities with rule conditions specified to retrieve only Quality of Service alarms with status "Critical".

13 Performance Monitoring

Performance Monitoring analysis is one of the tools that can be used by OVOC operators for network planning and administration in the OVOC topology. This monitoring involves the collection of high-level historic data polled from the managed entities. Examples of uses include:

- Set different subscriber plans according to traffic peaks based on PMs such as the number of attempted and established calls by comparing polling results for different time intervals during a 24-hour period.
- Determine transcoding requirements based on data such as the maximum number of G711 and G729 Active Calls for the filtered time period.
- Track the effective level of license utilization based on the number of media legs, transcoding sessions for the filtered time period.
- Performance Monitoring parameters can be managed using both SNMP and REST API

The data topology is based on a default tenant-level profile which is automatically allocated to a new tenant. Tenant Operators can later customize PM templates and easily assign them to all types of managed devices. Polling can be started and stopped for one or more devices. Threshold monitors raise alarms when a threshold is exceeded and clear them when the PMs value falls below the defined low threshold value. Polled Performance Monitoring data can be automatically saved to a data file according to PM template for each polling interval (saved to the NBIF folder). In addition, you can save the output of a PM filter query to a CSV file. For example, you can save output for several polling intervals.

Figure 13-1: Aggregated PM Report for Specific Metric

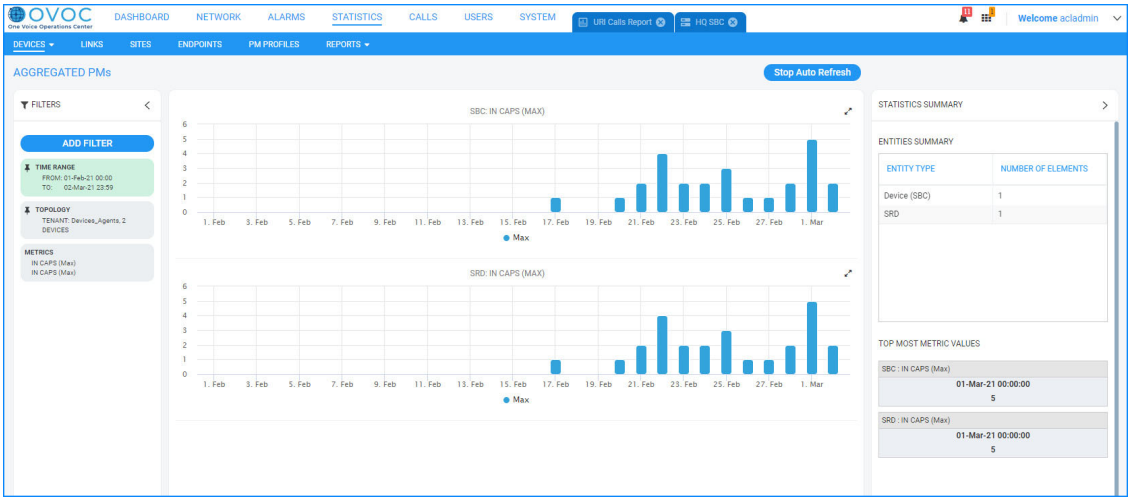
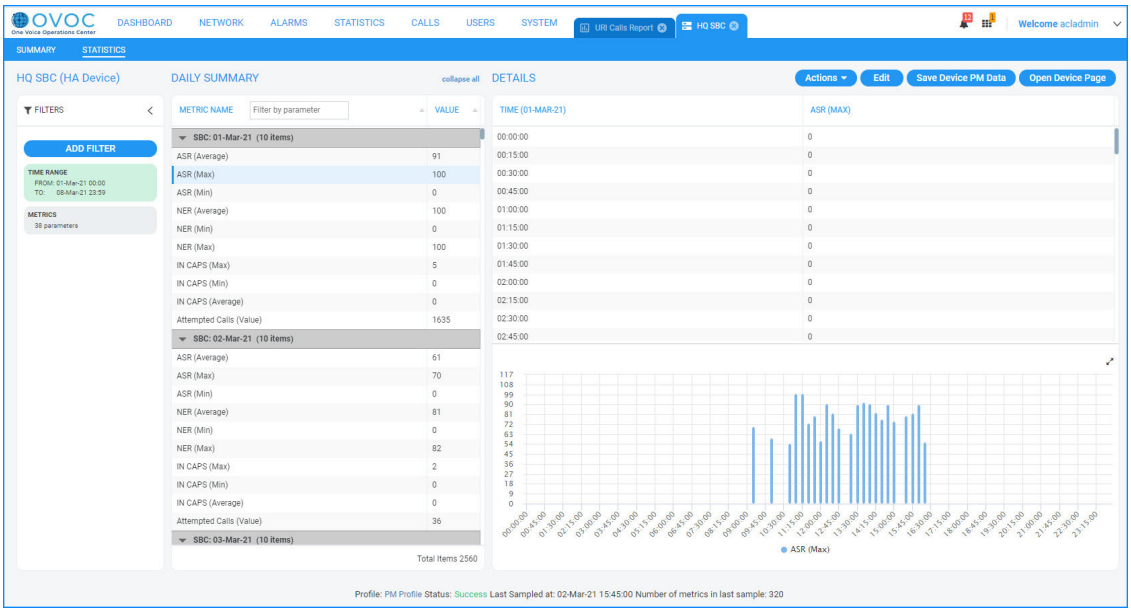


Figure 13-2: Stand Alone PM Report for Multiple Metrics



For a comprehensive list of PM parameters supported on each device, refer to the OVOC Performance Monitoring Guide.

14 Voice Quality Management

AudioCodes' Voice Quality Management delivers important technical and business statistics based on AudioCodes methodologies developed over many years of VoIP implementation and design . It provides real-time health and diagnostics monitoring of VoIP voice traffic network quality data that is generated by AudioCodes devices, endpoints and links. It includes modular views for analyzing network nodes, aggregated voice quality statistics, user data and alarms. In addition, sophisticated report modules enable the generation of tailored reports according to specific users and called telephone numbers. Managed entities are graphically represented in map, table and region, featuring popup summaries of critical metrics. VoIP network traffic health monitoring includes both history and real-time modules. The key focus of the Voice quality data processing is based on the call quality rating metrics (MOS, jitter, packet loss, delay/latency and echo).

AudioCodes' Voice Quality Management includes the monitoring of links which can be automatically created for calls between AudioCodes devices and Microsoft Skype for Business server components and third-party SIP trunks. You can also manage Active Directory users and their respective call statistics. Call trend statistics are collected based on key metrics, traffic load, and average call duration and call success. Alerts can be generated based on call success rate and quality thresholds defined by the network administrator.

Figure 14-1: Statistics

Voice Quality Management-Key Features

- **Network Readiness Testing:** OVOC may be used by AudioCodes Professional services in order to test VoIP network quality readiness prior to actual deployment of the UC systems. This is done by setting active probes in the network which simulate calls in the VoIP network. This data is then collected and analyzed by AudioCodes Professional services teams using the OVOC quality monitoring capabilities.

- **Entity Analysis Scope:** Separate monitoring views and filtering for Devices, Links, Sites and Endpoints entities.
- **Calls List:** Listing of calls made in the network over the past three hours (default) for a specific tenant.
- **Triggering Quality Alerts:** Quality alerts optimize session experience management by providing VoIP network administrators with the ability to trigger alerts according to pre-defined quality of service alert rules. This help to avoid false alarms when defining the appropriate minimal number of calls and criteria thresholds.
- **QoE for Microsoft Teams:** OVOC can retrieve QoE data (Subscription Notifications service) from the Microsoft Teams environment (Office 365/Microsoft 365/Microsoft Azure). See QoE for Microsoft Teams below
- **Skype for Business Server Components Monitoring:** OVOC can synchronize with the Skype for Business server and retrieve call quality measures for all the major components (Front End, Edge, SBA and Mediation servers) and their connecting links.
- **Active Directory Users Management:** OVOC can synchronize with Active Directory organization user databases and retrieve all registered users. You can then manage the telephony experience from the retrieved list of the enterprise's Active Directory listed employees.
- **Endpoints Monitoring:** OVOC supports endpoint devices reporting call quality using SIP Publish messages according to compliance with RFC 6035. Endpoints are added to the OVOC application automatically after the first time that SIP Publish messages are sent to the OVOC server. This feature is supported for the following phone models:
  - Polycom Trio conference phones
  - Polycom VVX phones

  For more information, refer to the Device Manager for Third-Party Phones Administrator's Manual
- **OVOC-Defined QoE Threshold Profiles:** QoE Threshold profiles can be applied for voice quality metrics (MOS, Delay, Packet Loss, Echo and Jitter). The QoE Threshold profile consists of threshold values set for each of these metrics for the following different call quality categories: 'Poor', 'Fair' and 'Good'. This feature includes pre-defined profiles. In addition, the user can define their own custom profile with threshold definitions for specific metrics.
- **Voice Quality Reports:** Both template and custom reports can be generated for devices, links and URIs for managed entities (Tenants, Regions and Elements) (see Voice Quality Reports on page 39)

QoE for Microsoft Teams

OVOC can retrieve QoE data (Subscription Notifications service) from the Microsoft Teams environment (Microsoft Graph API database) on Office 365/Microsoft 365/Microsoft Azure. Permissions for data access is granted for the managed Microsoft Tenant. Calls data

(subscriptions notifications) can then be retrieved for users managed by this tenant including Teams peer-to-peer or Conference calls and network calls. Overall call quality and related legs are determined by both voice and video metrics. Threshold-based alarms are affected by both voice and video quality and all the default values in Teams Threshold sets are based on Microsoft CQD recommended values and can be customized by the operator per Teams device (Teams tenant).

Figure 14-2: Microsoft Teams Calls

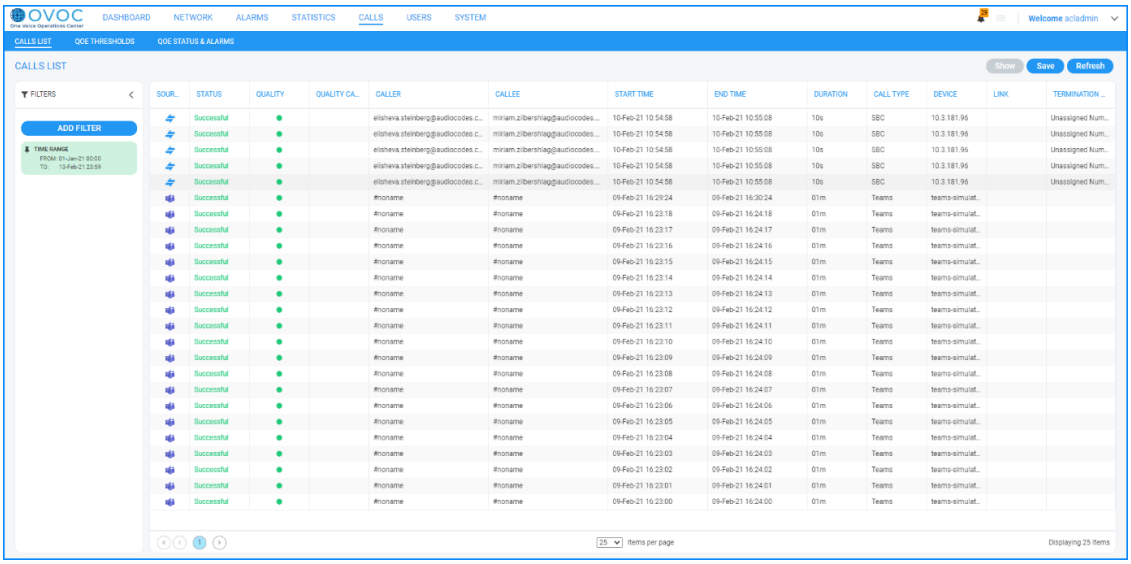
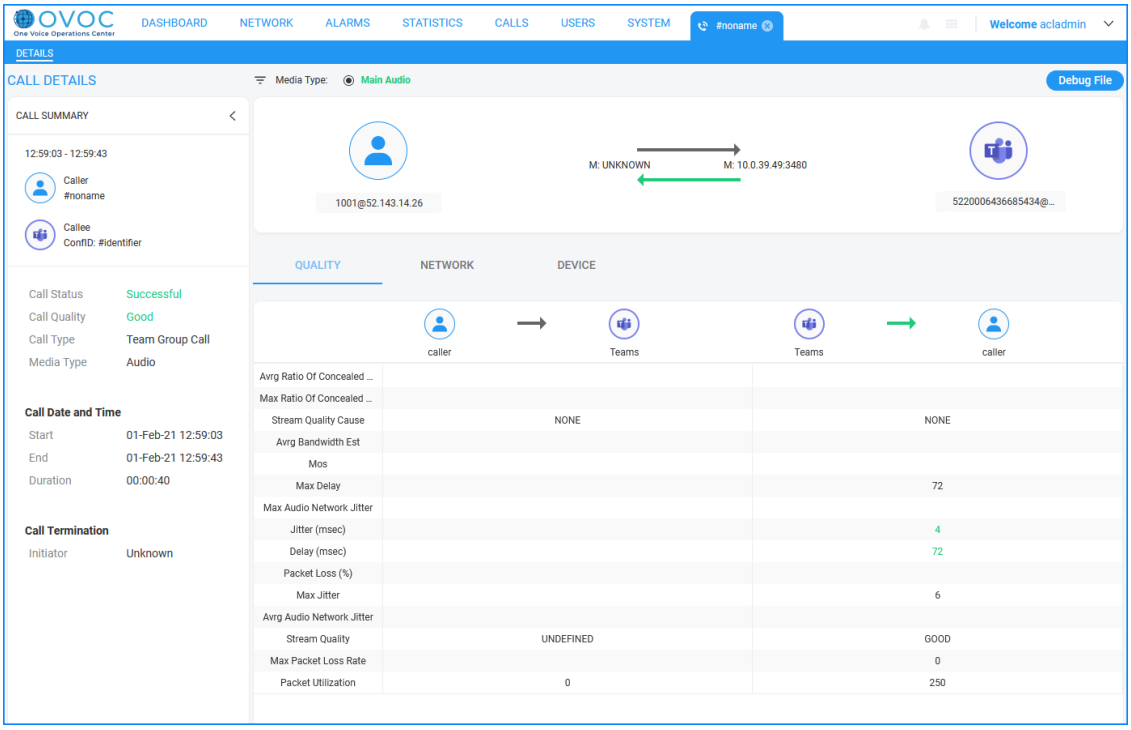


Figure 14-3: Teams Calls Details

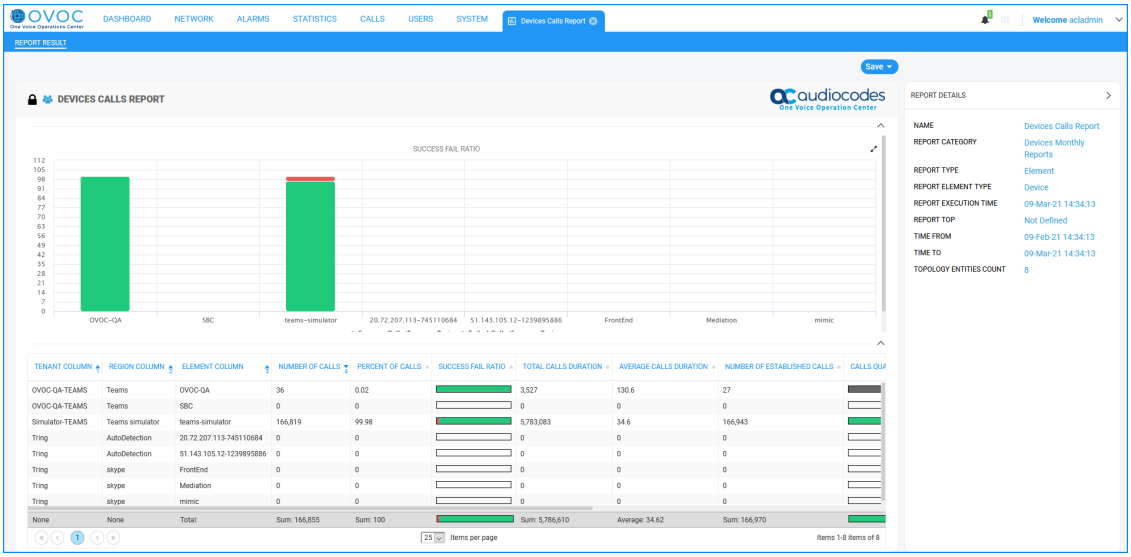


Voice Quality Reports

Both template and custom Voice Quality reports can be generated for devices, links and URIs for Tenants, Regions and Elements.

- Reports can be customized to different report types including Element Statistics, Aggregated Statistics Trends and Trends Statistics Comparison and for Top URI Monthly elements.
- Reports can be filtered for specific topology and tailored with a personal “look and feel” including the table columns and graph types and to include a tenant’s corporate logo.
- Reports can be scheduled to run hourly, daily, weekly or monthly.
- Report definitions can be exported to a JSON file and opened using Adobe Acrobat. Likewise, report definitions can be imported and replicated.
- Results of the Report output (see figure below) can be exported to a CSV file

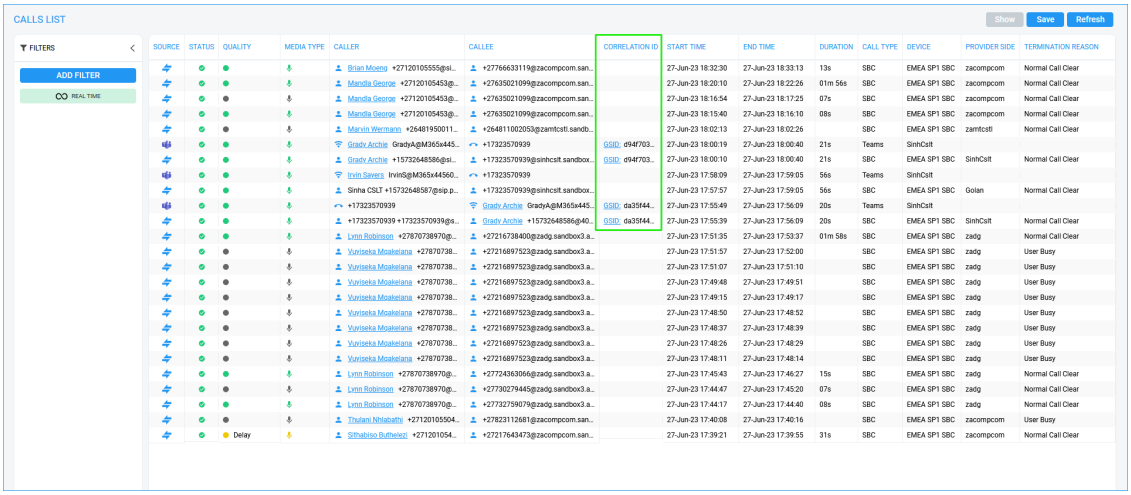
Figure 14-4: Voice Quality Reports



> Customers can generate template reports without purchasing licenses; however, to generate customized reports, customers must purchase licenses as part of the OVOC license (“Reports” Voice Quality feature). These licenses can be allocated to tenant or system operators in the OVOC Web interface.

Calls Correlation (SBC – Teams and SBC – SBC)

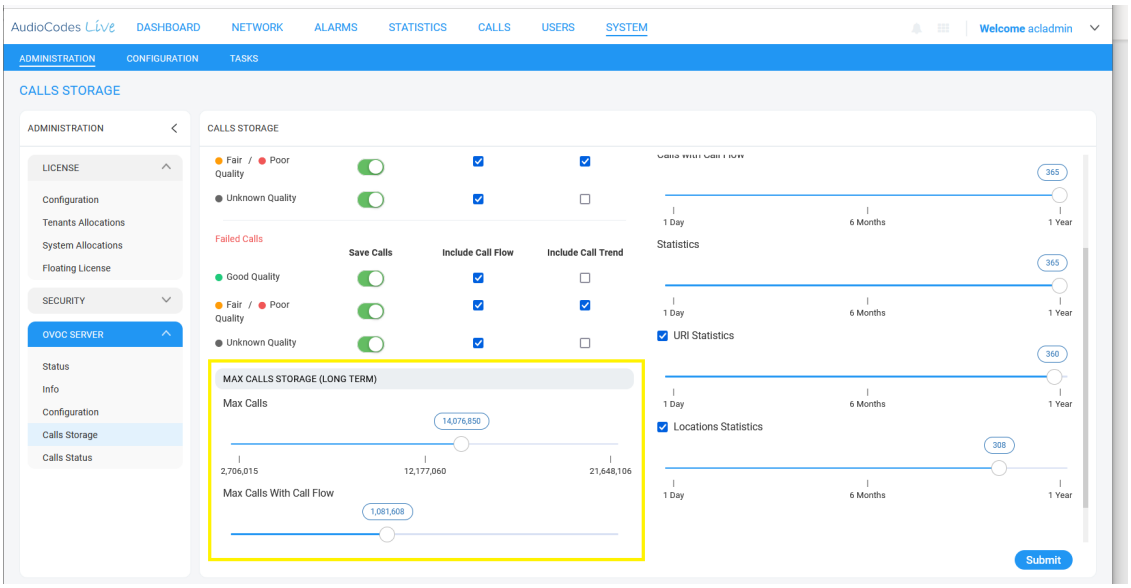
Calls which traverse multiple devices (Microsoft Teams and AudioCodes SBC devices) are reported to Live Platform as separate call legs; however, are displayed in the same call record. The correlation ID (GSID) is assigned to these calls. When calls are filtered using this value, information is retrieved for all call legs assigned that are associated with the GSID. When displaying Call Details, it’s possible to toggle between the call legs to display the details of each leg.



Control Storage of Call Flows

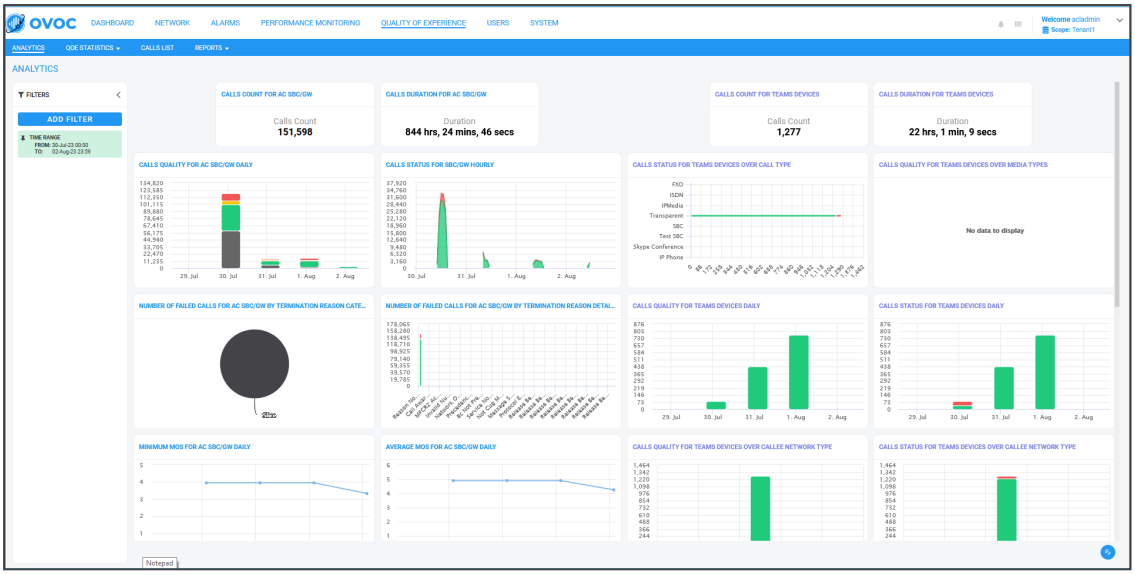
Customers who are specifically interested in call flow analysis can increase the maximum number of calls with Call Flow that are saved in the OVOC database relative to the Maximum Number of Calls. This action is performed in the Call Storage screen; when the Max Calls with Call Flow parameters is increased, the Max Calls value is decreased and vice-versa.

Control Storage



Analytics Report Module

The Analytics module is a licensed module which displays various types of QoE data aggregated from SBC and Teams devices. Operators can customize the dashboard to suit preferences; the icon allows widget locations, size and content to be customized. Analytics data is available for the last 7 days.



Analytics API

The Analytic API Voice Quality license enables access to specially designed views with selected data from the OVOC database for the purpose of integration with Northbound third-party interfaces. Customers can connect to the OVOC database using third-party DB access clients and retrieve topology and statistics. This data can then be used in management interfaces such as Power BI and Splunk to generate customized dashboards, reports and other representative management data. Customers can combine data from AudioCodes OVOC and enterprise voice or third-party data monitoring tools such as HP OpenView for data such as the following:

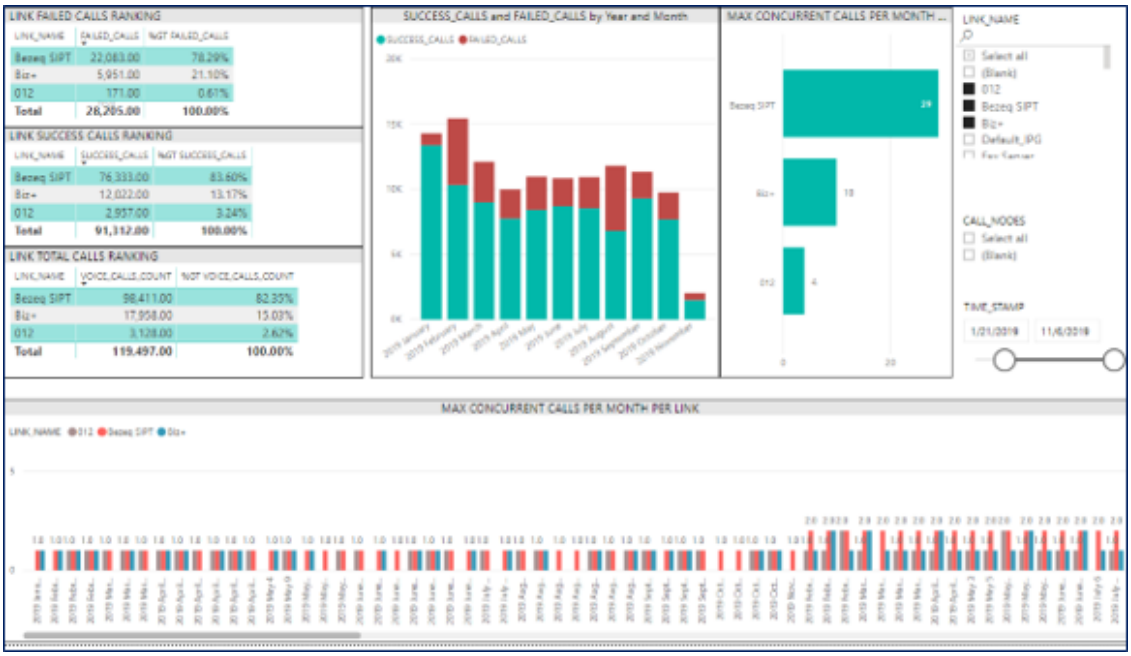
- Receive Alerts from HP OpenView
- Calls tariffs
- Data layer statistics
- User information from corporate directory

The following data is accessible from OVOC:

- Network Topology including Tenants, Regions, Devices, Non-ACL Devices, Links
- QoE Statistics including Calls, Nodes and Links Summaries
- Active and History Alarms

Analytics data can be viewed for up to the last 24 hours.

Figure 14-5: PowerBI Reports



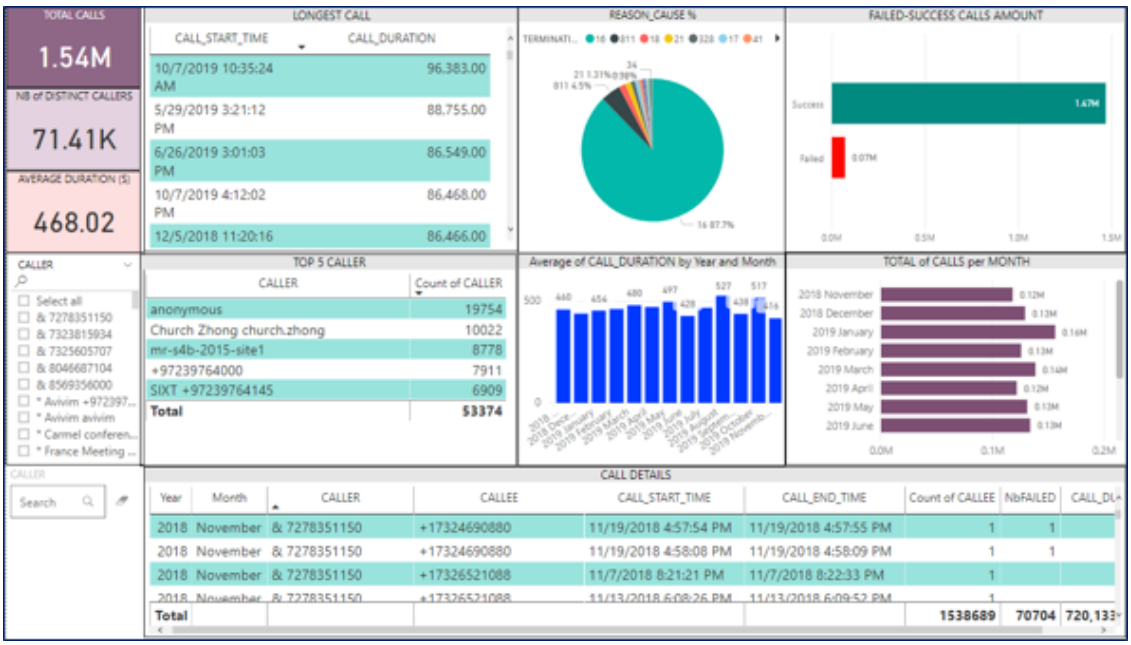


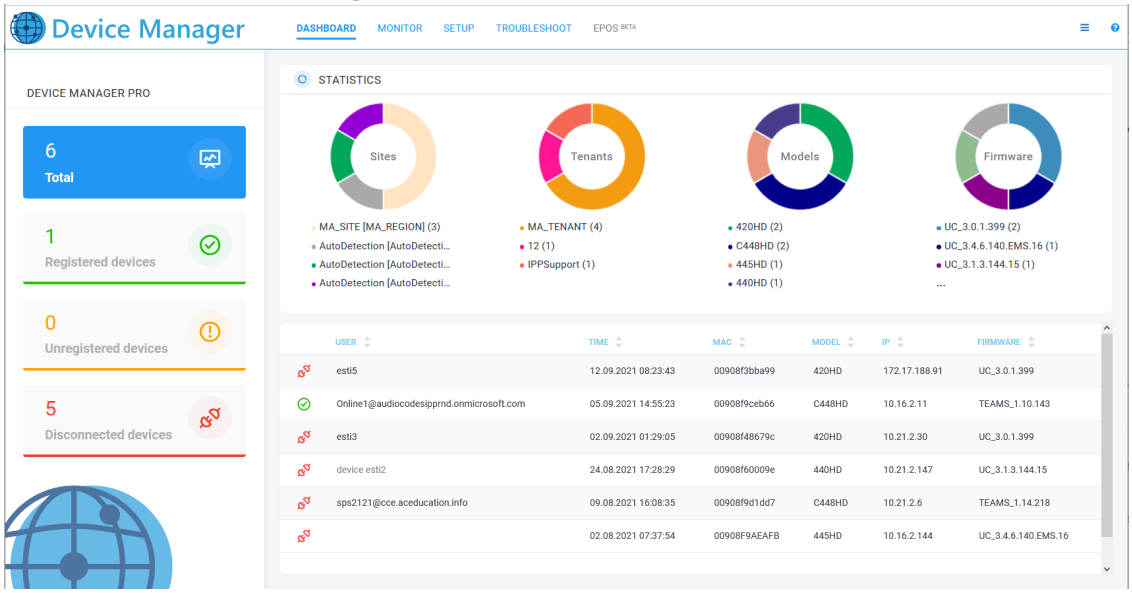
Figure 14-6: Splunk Report

15 Device Manager Pro

The IP Phone Manager Pro provides a very comprehensive zero touch provisioning and firmware updates per different templates which can be configured for tenants, regions, sites, device model and users. Administrators can perform actions on multiple phones including: uploading a CSV file with a devices' MAC addresses and SIP credentials; approving devices at the click of a button; sending messages to phones' LCDs, resetting devices, and moving devices between regions. The figure below displays the Device Manager Pro dashboard.

Figure 15-1: Device Manager Pro

Figure 15-2:

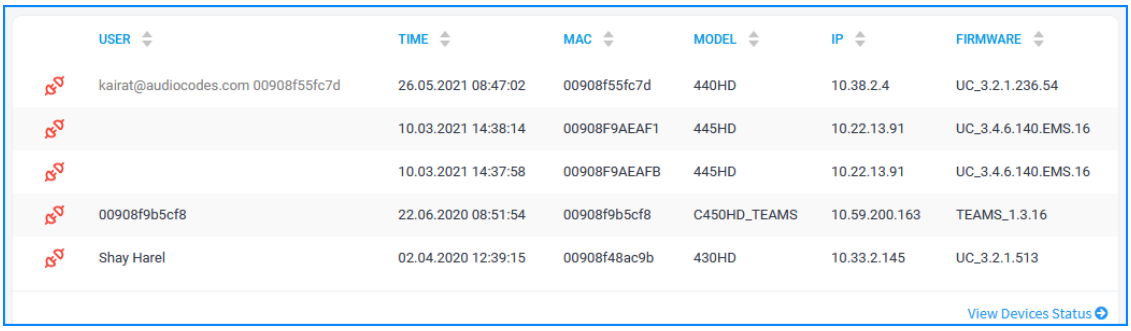


The Dashboard page lets you quickly identify:

- A breakdown of the number of registered, unregistered and disconnected devices in the network.
- A breakdown of the key data for Tenants, Sites, Phone models and firmware.
- System data including the Web language, the IP address, session time left and the running OVOC server version.

The Recent Reports pane at the bottom of the status screen shows recent operations performed on specific phones. Color icons are used to indicate the status of updates on the phone. For example, the icon below indicates that the device has been registered.

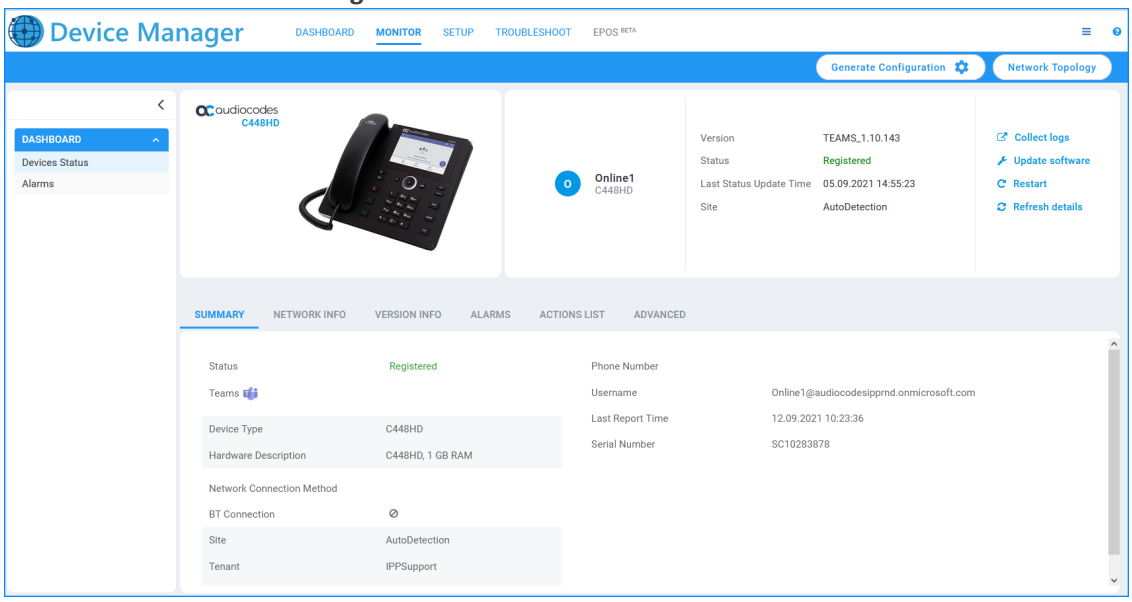
Figure 15-3: Recent Reports



When you click the **Monitor** tab, the Device Status screen opens displaying the details for the category of devices that you selected. For example, 'Registered Devices'.

Figure 15-4: Teams Devices Status

Figure 15-5:

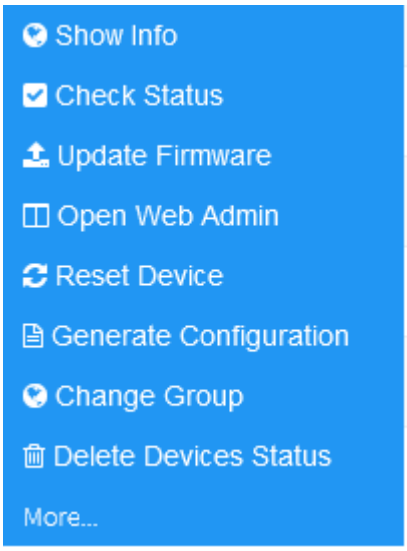


Status information that is displayed for the Teams device includes the following:

- Full version information
- Detailed network status including whether Wi-Fi is enabled.
- Whether the BtoE (Better Together Status) auto pairing is enabled on the device and a list of connected devices
- Filtering capabilities. For example per user, phone #, MAC, IP address, model, version, status
- Whether a device is set as a VIP device

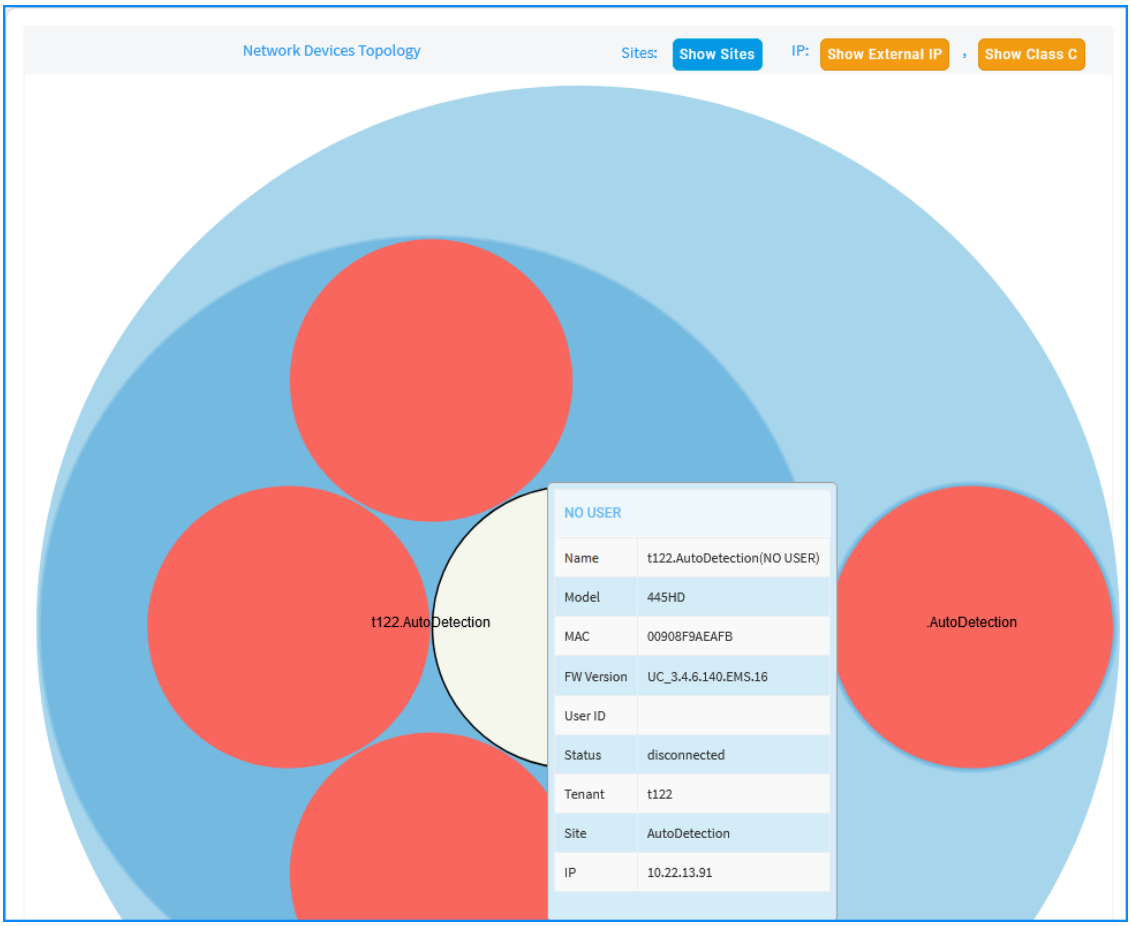
You can perform various right-click operations on each phone record as shown in the figure below.

Figure 15-6: Phone Actions



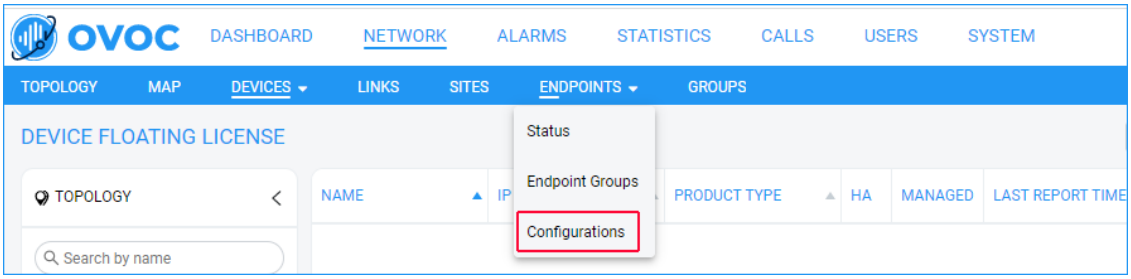
You can use filters to display device status according to specified criteria. The IP Phones active alarms are displayed in a Dashboard, including information such as alarm description. After an alarm is cleared, it disappears from the Alarms screen. The Network Topology map view allows administrators to view a snapshot of the network's tenants and subnets; its possible to toggle to display either IP addresses, classes or site labels. The page allows administrators, for example, to determine at a glance which subnets are causing traffic overload.

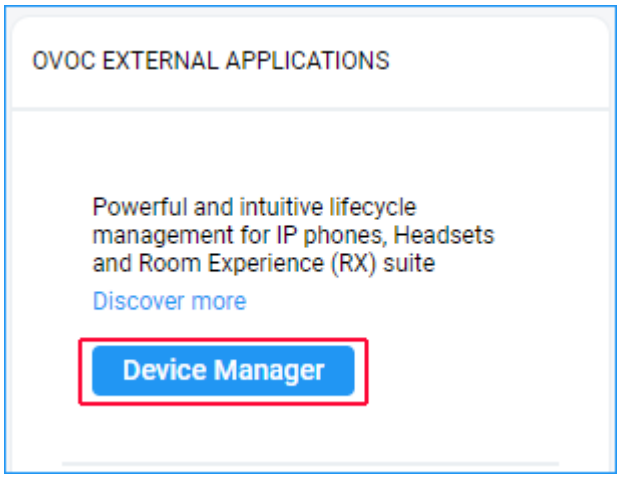
Figure 15-7: Network Device Topology Page



Single Sign-on to Device Manager

This version supports Single Sign-on from OVOC to the Device Manager. When users are logged in to OVOC, then navigate to Endpoints > Configuration or select the Device Manager link under OVOC External Applications, the Device Manager opens automatically without the need to enter a username and password.

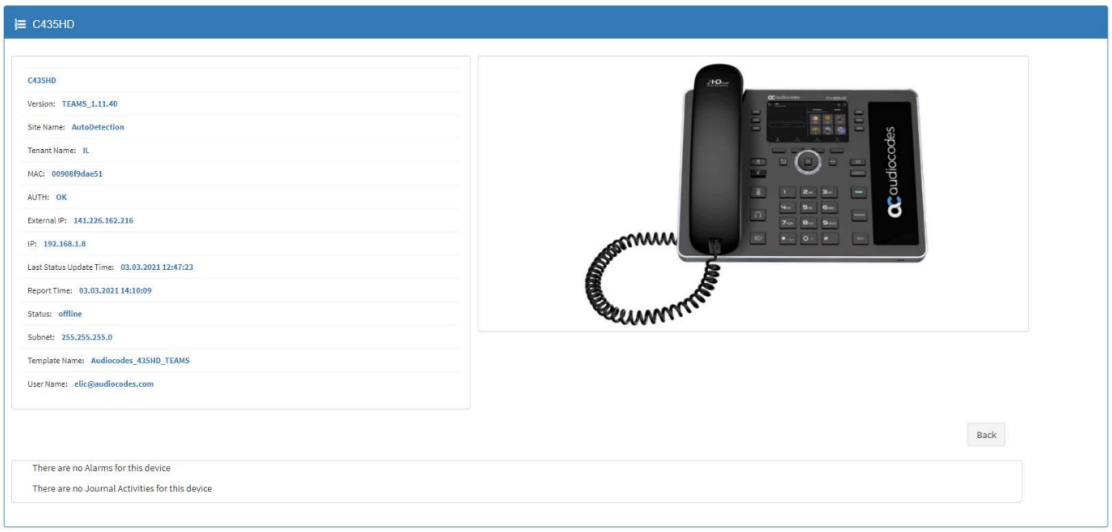




Microsoft Teams Android-based Device Management

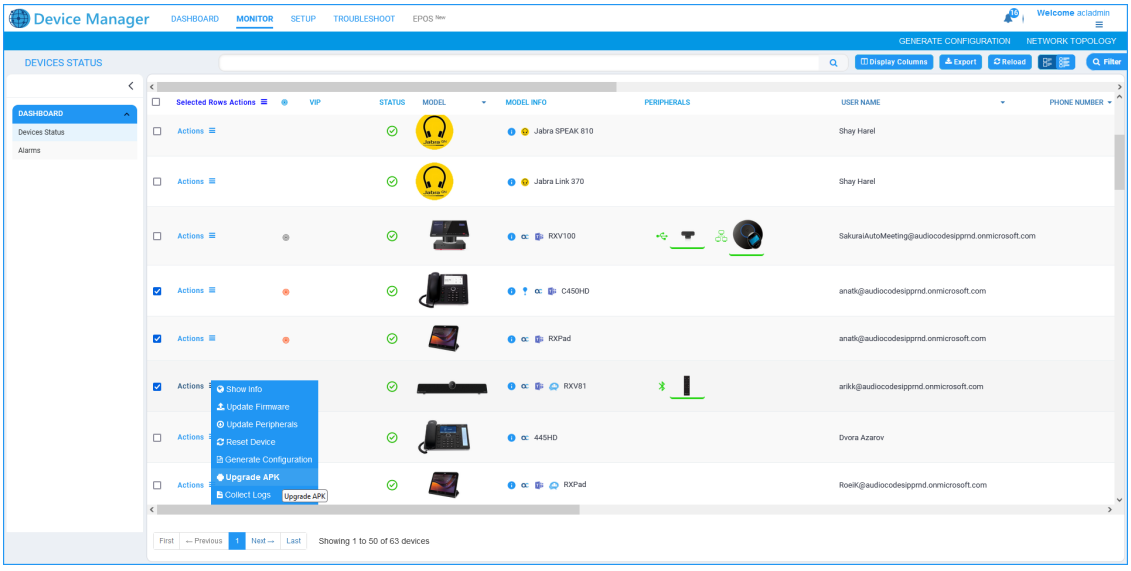
Support for Android- based Microsoft Teams devices (Device Manager Pro/Express version 7.8.2000 and later) including the C435HD and C470HD phones and the RXV80 Standalone Video Collaboration Bar The Device Manager manages the Android-based Teams phones in a similar way to Skype for Business/Microsoft Lync and Generic phones. Management actions include the provisioning of configuration and firmware and device restart.

Figure 15-8: C435HD Device



BULK Android APK Upgrade

Bulk and Single device Android APK update can be performed on devices in the Monitor or Show Info page using the **Upgrade APK** option.

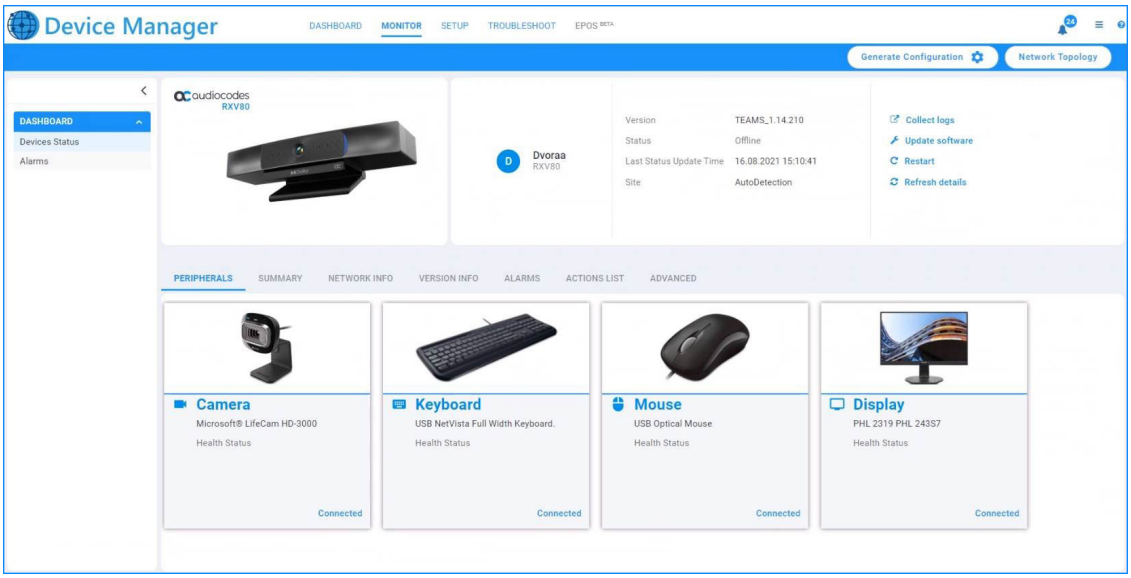


Android-based Peripheral Device Live Monitoring

Peripheral devices that are connected to Android-based devices deployed for Meeting Room solutions can be monitored to determine whether they have an active connection including:

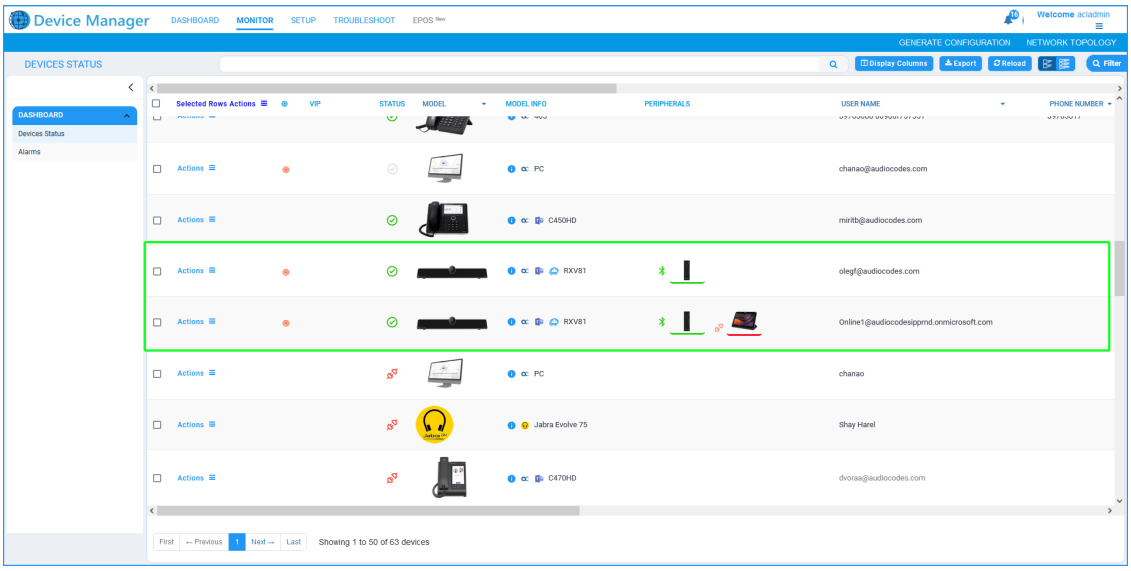
- Camera
- Keyboard
- Mouse
- Display

Figure 15-9: Peripheral Devices



Upgrade AudioCodes AppSuite

Bulk and Single AudioCodes' AppSuite upgrade can be performed on devices in the Monitor or Show Info page. This upgrade allows admins to immediately upgrade the AppSuite installed on the RXV100 or Desktop devices thereby ensuring that the Device Manager client is upgraded to the latest version.



Mass Operations

You can perform mass operations on multiple users such as restart passwords, restart devices, generate and update device configuration files and send messages to multiple devices over an HTTP/S public internet connection. You can also perform mass operations on multiple devices such as change device type, change languages, restart multiple devices and generate and update device configuration files and send messages to multiple devices. When devices are

deployed behind a NAT, OVOC cannot establish a direct HTTP/S connection with managed devices:

- AudioCodes phones and Jabra devices send keep-alive messages to OVOC at one-minute intervals for the purpose of querying the OVOC server for firmware updates. OVOC then updates the devices with files retrieved from the ShareFile server.

> Polycom devices do not send keep alive messages and instead send status messages.

- For Microsoft Teams deployments, a special mechanism is deployed to reach the Teams phones by embedding commands from the OVOC server in the Keep-alive messages that are sent from these phones.

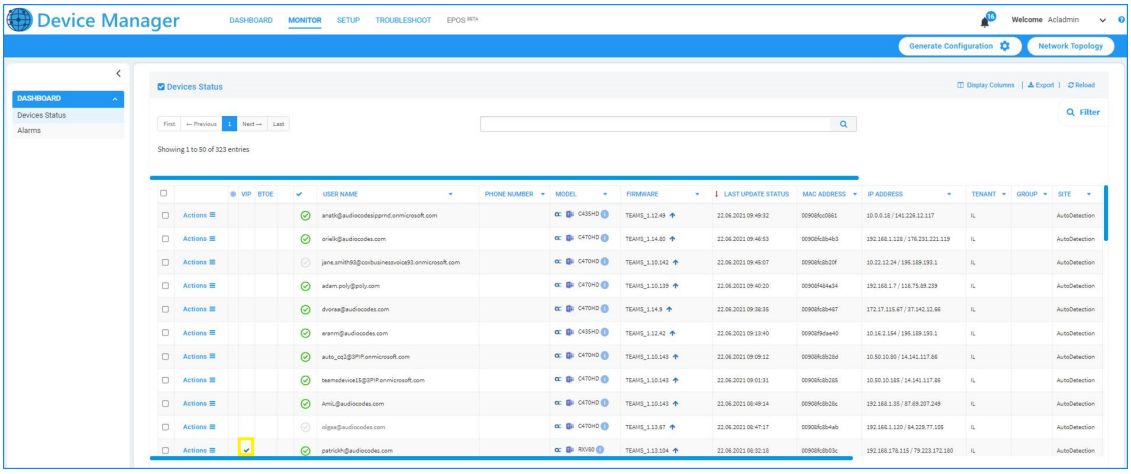
Group Level Management

Tenant Operator can define Endpoint Groups in OVOC to manage groups of phones with similar configuration. For example, you may wish to define separate groups for “Marketing” and “Logistics”. This enables greater control in the automatic provisioning (“Zero-touch”) process by preventing the misconfiguration of large number of phones system-wide. These groups are created in OVOC by the System Administrator and can then be configured in the Device Manager in a similar manner to Tenants, Sites and Users in the Manage Multiple Devices screen and using Configuration keys.

VIP Device Management

Devices can be set as VIP devices in the Device Status screen. This enables the prioritization for the monitoring of devices of key management personnel. In addition, in the Device System Settings, you can customize the global Keep-alive timeout to ensure that any disconnection for such devices are rapidly detected. Custom alarms are generated when the device connection is lost and when the device connection is unregistered.

Figure 15-10: VIP Devices



Jabra Device Management

Jabra devices can be managed by OVOC including for status and health monitoring, alarms, configuration and software upgrade of the Jabra devices. A Jabra Integration Service is installed on the workstation PCs that are connected to Jabra devices. This service sends alarms and Keep-alive messages to the Device Manager and receives firmware updates.

Polycom Device Management

Polycom Trio 8800 and VVX devices can be managed by the Device Manager Pro over REST API interface:

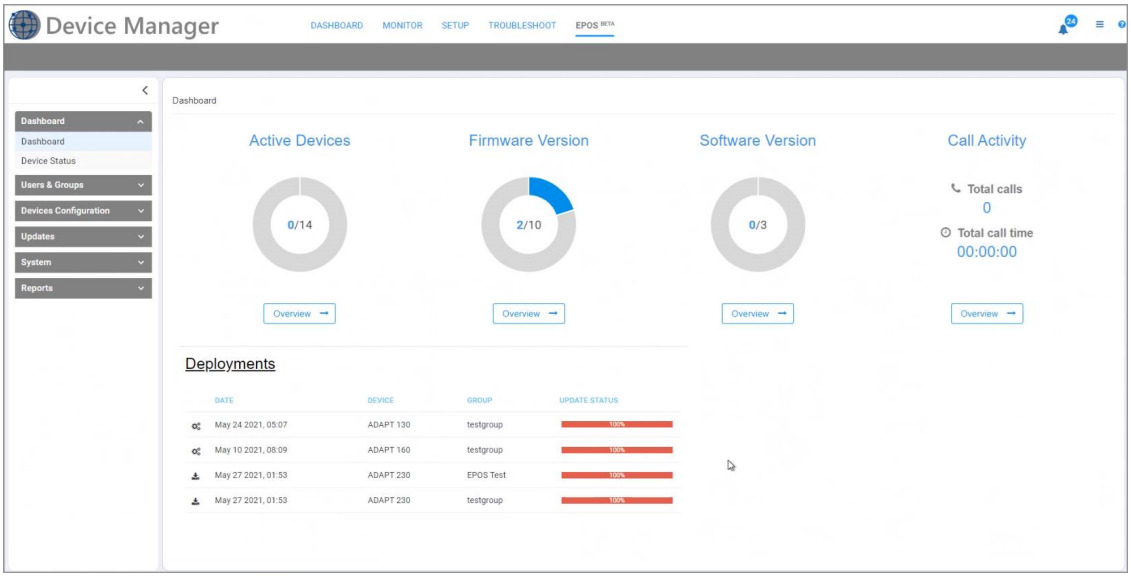
- Automatic provisioning with different templates per model from AudioCodes' provisioning server and added to specific sites according to the phones subnet mask.
- Synchronize with the AudioCodes' firmware Cloud repository to retrieve the latest Polycom device firmware files.
- Monitor the status of the Polycom devices including displaying presence, registration status and hardware information and viewing the assigned template.
- Access the Polycom device's Web Configuration Utility
- Reset the Polycom device

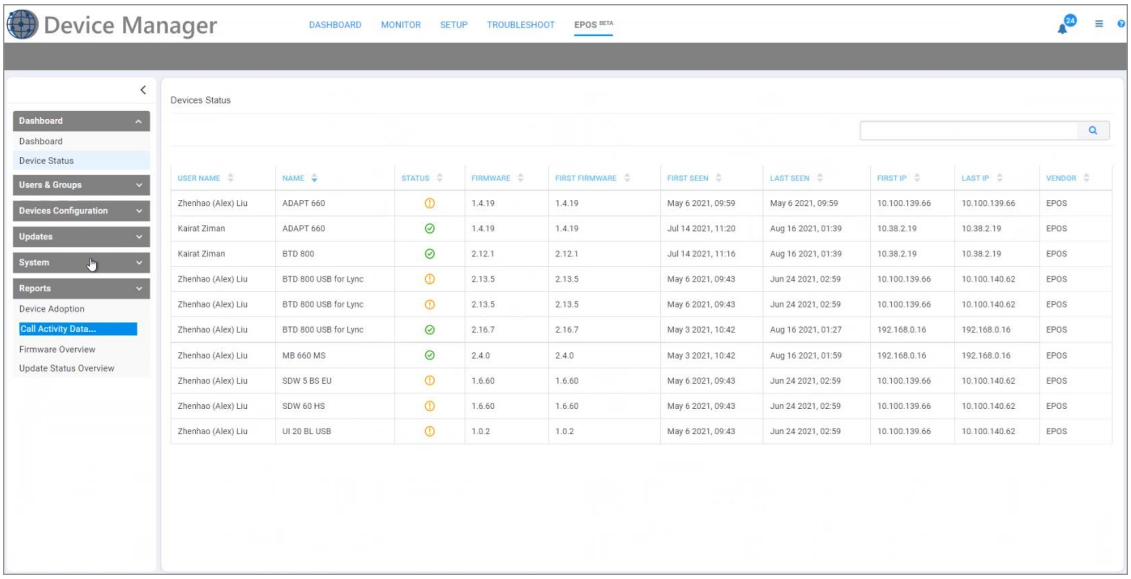
EPOS Integration

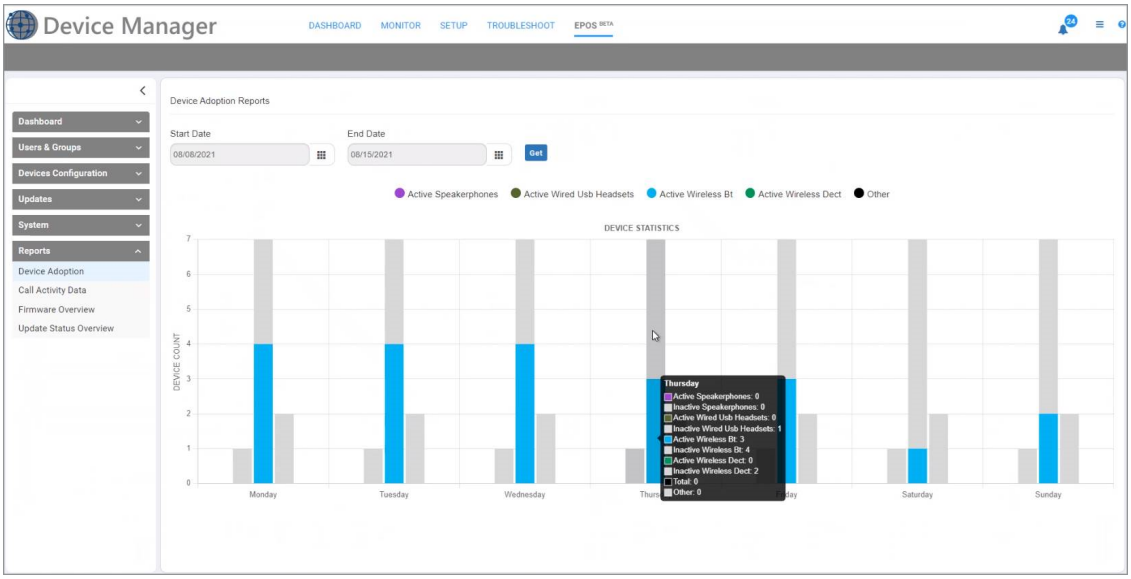
EPOS Manager is a powerful IT management solution that enables IT managers to manage, update and configure settings for EPOS headsets and speakerphones within an organization from any location. EPOS and AudioCodes integration enables IT administrators to manage EPOS devices directly in the AudioCodes One Voice Operations Center (OVOC) solution for a premium and seamless user experience. The full-fledged integration includes the following:

- Remote deployments of firmware and configurations
- Data insights to track EPOS device UC adoption progress through dashboard and reports.
- View active and inactive devices

Figure 15-11: EPOS IT Management





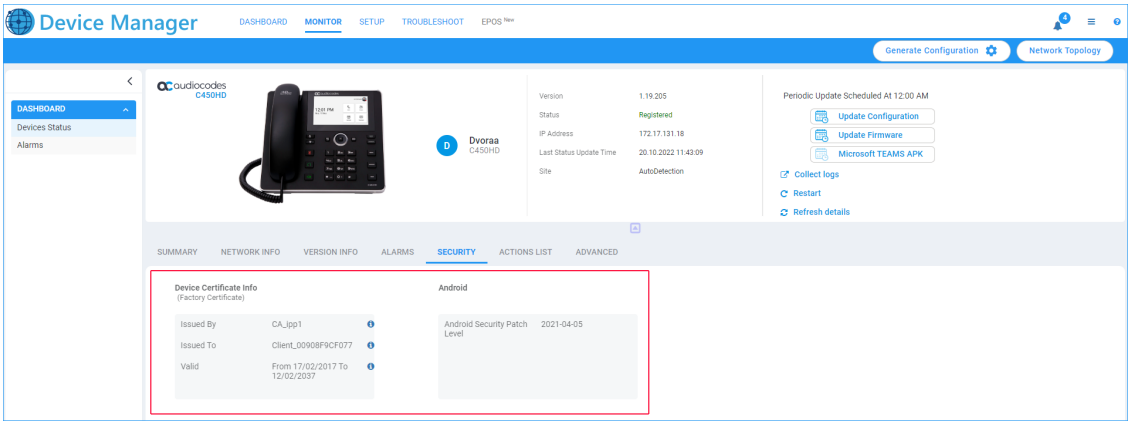


IP Phones Certificate Status Reporting

The Device Details screen includes a new Security tab which includes the Device Certificate Info and applied Android Security patches. This tab is displayed for Teams and Windows devices only. This tab appears only when certificates are installed on the device.

> For RXV100 devices, this tab only appears when certificates are installed on the device.

Figure 15-12: Security Tab



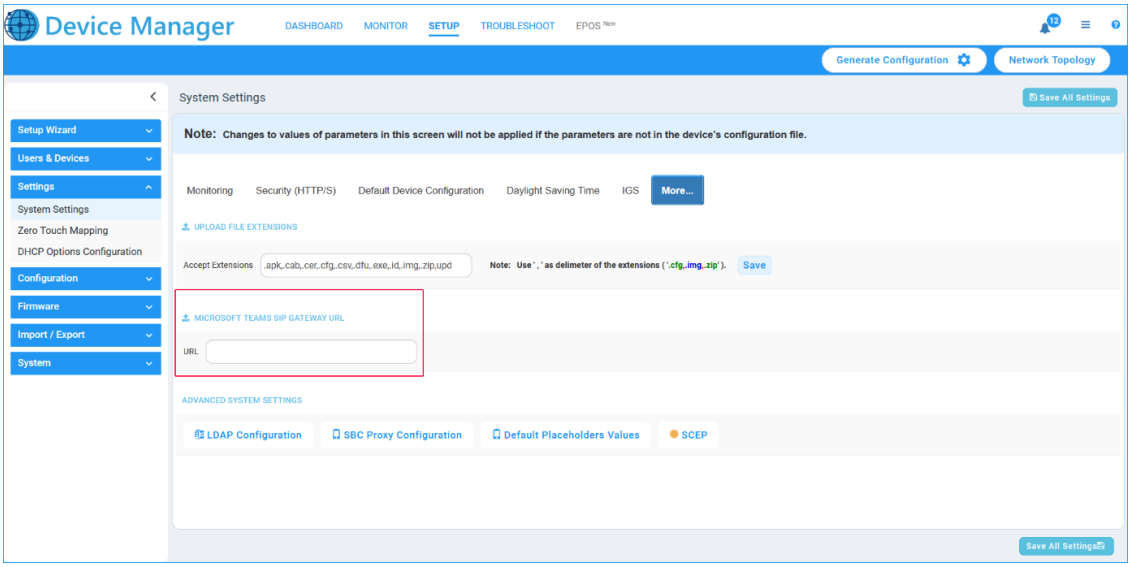
REST API Host Alarm Forwarding Destination

An alarm forwarding destination can be defined for a REST server host. This enables customers to categorize the alarms sent to the REST server through configuring Topology and Rule conditions according to their network logic. For example, enabling alarms forwarding for the default tenant and its sub-entities with rule conditions specified to retrieve only Quality of Service alarms with status "Critical".

Microsoft's SIP Gateway Integration

The Device Manager helps to migrate devices to Microsoft Teams SIP gateway and to monitor and apply configuration. The Microsoft's SIP Gateway allows users to convert non-Teams-certified AudioCodes' phones to Microsoft Teams phones which then enables these phones to connect to the Microsoft telephony cloud telephony service.

The following AudioCodes phone models can be converted to Teams phones: 405, 405HD, 420HD,440HD, 445HD, 450HD and C450HD. (Version 3.4.4.1000.61 and later is supported for the 445HD, 450HD and C450HD models).

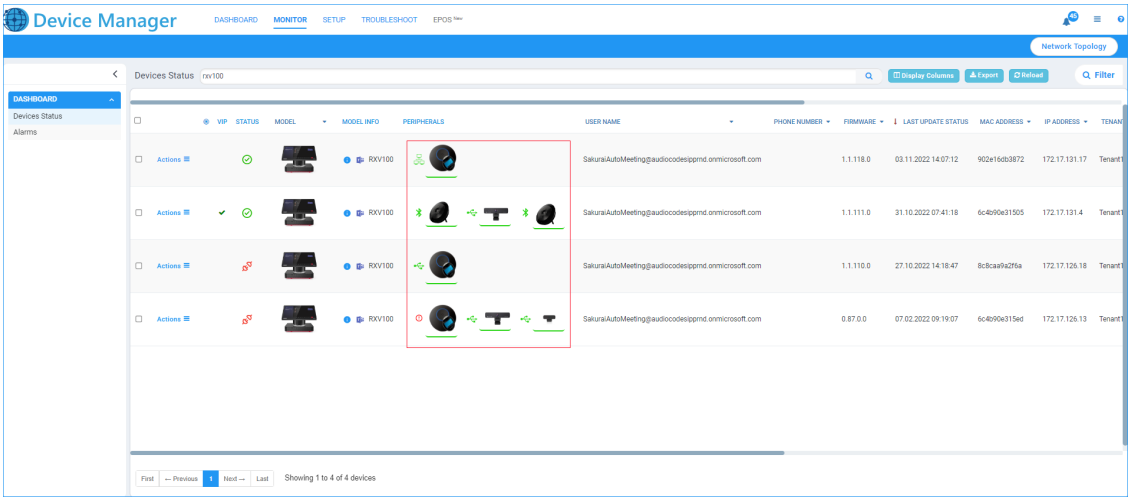


Converting C448HD and C450HD Teams Phones to SIP Gateway

Admins can use Device Manager to upgrade the C448HD and C450HD phones to Teams SIP Gateway.

Meeting Room Bundle Device Statuses

The device statuses for the Meeting Room bundles have a new look and feel with large color-coded icons that simulate the exact current state of Meeting Room bundles in a quick glance.

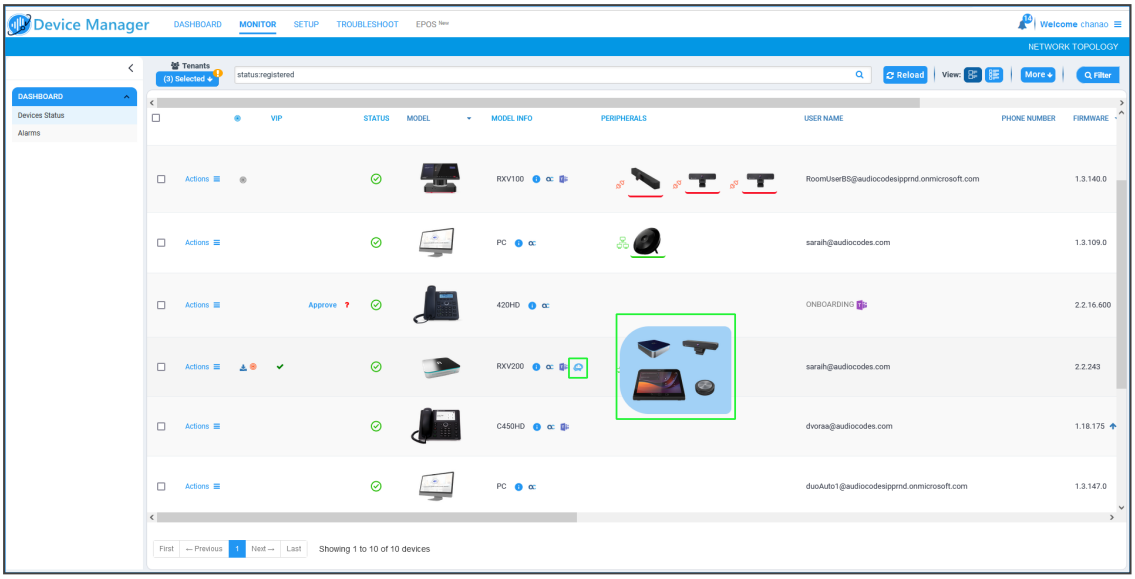


Peripheral Device Management

- RX40 USB audio bar connected to RXV200 and RXV100.
- RX-PAD paired to the RXV81/RXV200.
- RXV81 connected as a USB peripheral.
- RXVCam10 Content Camera connected to the RXV100 or RXV200 Meeting Rooms.

Bundling Icon

A new 'bundle' icon displays icons of all the peripherals in the bundle.



This page is intentionally left blank.

International Headquarters

Naimi Park

6 Ofra Haza Street

Or Yehuda, 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

Document #: LTRT-94036