

OVOC

Integration with Northbound Interfaces

Version 8.4



Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published 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: October-12-2026

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
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
Mediant 2600 E-SBC User's Manual

Document Name
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
19230	Updates for Version 8.2: Updates to Section: analytics API; analytics API Database Tables
19231	Update for Version 8.2.1000: Updates to Section: Forwarding Alarms from OVOC to the NMS
19232	Update to Section :Alarm Forwarding Data Formats; Topology CSV, Topology.xml File (removed Migration script)
19233	Added Section: Forwarding Journal Entries from OVOC Server to an NMS Updated Section: Forwarding Alarms from OVOC Server to an NMS; Updates to the SNMP and REST formats.
19234	Added Sections: Configuring Email (SMTP) with TLS on a Non-Standard Port for OVOC Standard; Syslog Data Formats; Email Data Formats

Table of Contents

1	Overview	1
2	OVOC Integration	2
	OVOC Integration Elements	2
	OVOC Topology File	2
	Alarms	2
	Gateway Status	3
	Security	3
	Configuration and Maintenance	3
	MIB Folder	3
	NBIF Folder	3
3	Topology CSV File	7
4	Managing PM Files	10
	Saving PM Filter Queries	10
	Creating PM Data File	11
5	Fault Management	12
	Forwarding Alarms and Events to an NMS	12
	Forwarding Alarms from OVOC Server to an NMS	13
	Forwarding Alarms Directly from Devices to NMS	25
	Alarm Aggregation	26
	Examples of Aggregated Alarms	26
	Forwarding Journal Entries from OVOC Server to an NMS	27
	Alarm and Journal Forwarding Data Formats	31
	SNMP Data Formats	31
	REST Data Formats	35
	Syslog Data Formats	39
	Email Data Formats	40
	Configuring Email (SMTP) with TLS on a Non-standard Port for OVOC	44
	OVOC Server Alarm Settings	46
	Alarms Automatic Clearing (on Startup)	46
	Alarms Automatic Clearing Period (Days)	46
	Events Clearing Mechanism	46
	Alarm Suppression Mechanism	46
	Alarms Sequence Numbering	47
	SNMP Alarms Synchronization	49
	Resynchronization (Resync) Mechanism	50
	OVOC Keep-alive	52
	Status / State Management via Devices SNMP Interface	54
6	Voice Quality Reports	55
7	OVOC Server Backup and Restore	58
8	analytics API	60

9	Security	63
	Network Communication Protocols	63
	OVOC User Identity Management	64
	Authentication and Authorization using a Radius Server	64
	Configuring Radius Server Client	65
	Configuring RADIUS Server	66
	Authentication and Authorization using an LDAP Server	67
	Authentication and Authorization using Microsoft Azure	68
	HTTPS Connection	69
10	analytics API Database Tables	70
	Main Table Views	70
	Type Views	84

This page is intentionally left blank.

1 Overview

AudioCodes One Voice Operations Center OVOC delivers a comprehensive management tools suite comprising of base platform and add-on modular applications for the management, monitoring and operation of converged VoIP and data networks implemented in large-scale cloud or premise-based unified communications deployments using AudioCodes devices. The products that are managed by the OC include the Session Border Controllers (SBC), Media Gateways, Microsoft Survivable Branch Appliances (SBA), Multi Service Business Router (MSBR), residential gateways and devices .OVOC also integrates with the Microsoft Skype for Business environment platforms.

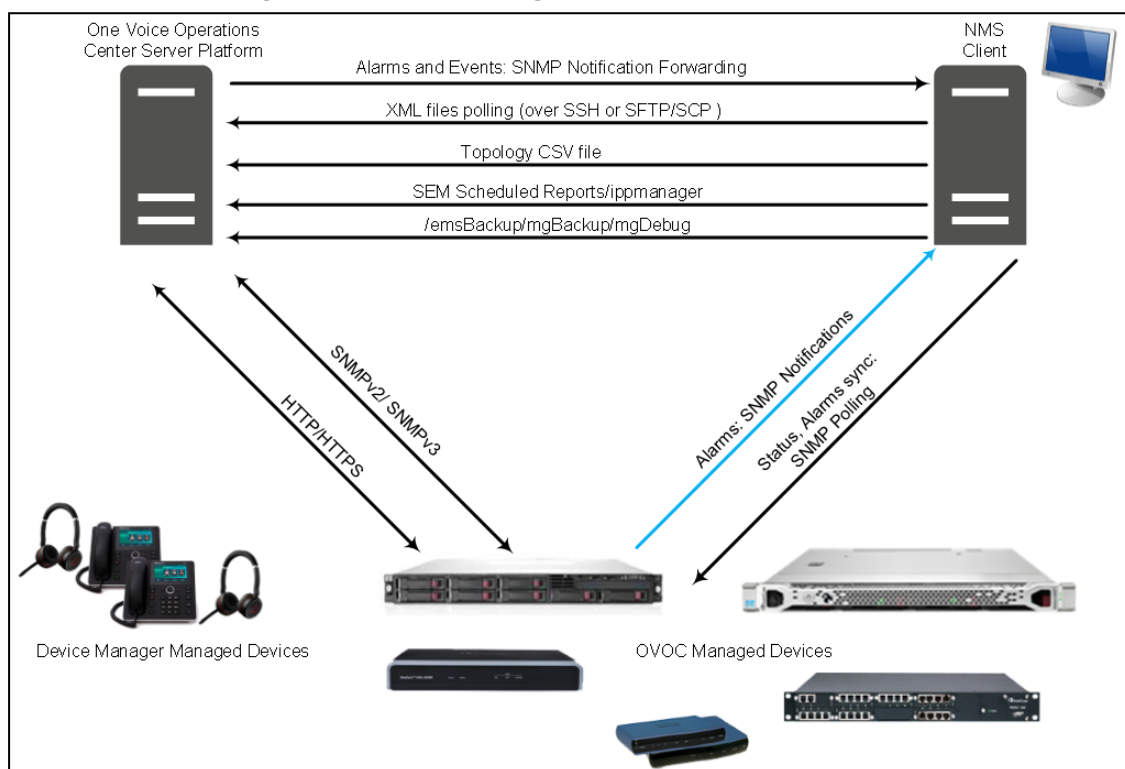
The Network Operations Center's core product, the Operations Center OC manages these products in a centralized device inventory via a Web client, enabling integrative network operations. The following describes the key products in the OC suite:

- **The One Voice Operations Center:** The OVOC is an advanced solution for remote standards-based management of AudioCodes products within VoP 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. The OVOC is in AudioCodes' assessment, the best tool to manage AudioCodes devices. However, it does not replace the NMS and OSS management systems, which displays to operators a comprehensive view of the network, including other vendors' equipment. After defining and initially provisioning a device via the device's embedded Web server tool, operators will usually work with an NMS / OSS for day-to-day maintenance. Only in the event of problems with a device or when significant maintenance tasks must be performed, will operators open the OVOC and work directly with it. Consequently, the OVOC provides APIs for faults monitoring (alarms) and security integration with a higher level management system.
- **Voice Quality Management:** Voice Quality Management involves the analyze of real-time Voice Quality statistics, which enables the rapid identification of the metrics responsible for degradation in the quality of any VoIP call made over the network nodes including AudioCodes devices and links. 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. In addition, it integrates with Microsoft Skype for Business monitoring server to provide end-to-end VoIP quality monitoring on Microsoft Skype for Business deployments. In addition, Voice Quality integrates and monitors with endpoints reporting RFC 6035 SIP PUBLISH packets.
- **The Device Manager Pro:** Enables enterprise network administrators to effortlessly and effectively set up, configure and update up to 30000 400HD Series IP phones in globally distributed corporations. These phones can upload configuration files from the OVOC server and send status updates over the REST protocol.

2 OVOC Integration

This document describes how to integrate the network elements of AudioCodes One Voice Operation Center (OVOC) with northbound interfaces. This includes the integration of alarms and events that are generated by the managed elements, the XML files polling and the Topology file. The figure below illustrates this integration.

Figure 2-1: OVOC Integration Overview



OVOC Integration Elements

This section describes the integration elements.

OVOC Topology File

The OVOC Topology file includes a snapshot of all the devices that are defined in the OVOC application. This file is located on the OVOC server and is available for the higher level management system (see [Topology Files](#)).

Alarms

Alarms are forwarded to the NMS as SNMP notifications (traps). These alarms can be forwarded using one of the following methods:

- Forwarded by the OVOC application to the NMS server (for all the network elements and the OVOC itself).

- Sent directly by each one of the network elements directly to the NMS server. In this case, there is the possibility to enable OVOC alarms. For example, when a connection between the OVOC server and device is established or lost, traps are forwarded to the NMS server.

For detailed information, see [Fault Management](#).

Gateway Status

The status of a device can be determined based on the set of supported IETF Management Information Base (MIB-II) tables (described in the SNMP Reference Guide).

Security

Security integration covers two main areas: Users Management and Network Communication protocols.

- OVOC Users Management (Authentication and Authorization) locally in the OVOC database or via a centralized RADIUS server or LDAP server.
- Network Communication Protocols:
 - HTTP/HTTPS:
 - ◆ NBIF Client- OVOC server connection is secured by default over HTTPS port 443 using AudioCodes default certificates or custom certificates
 - ◆ File transfer
 - SNMPv2 and SNMPv3: For Maintenance actions and Faults
 - SSH/SFTP/SCP: used for File transfer

For detailed information, see [OVOC Server Backup and Restore](#)

Configuration and Maintenance

A REST API will be available in a future release for performing configuration and maintenance actions from the NMS and running automation scripts using REST API URLs. For more information, contact your AudioCodes representative.

MIB Folder

AudioCodes MIB files are located under the following folder:

`/opt/ACEMS/server_<server.version>/externals/mibs/`

NBIF Folder

All OVOC and device information available for the NMS and other Northbound interfaces including Topology and Backup data is located in the OVOC server machine under the folder /NBIF. This folder can be accessed using HTTPS browsing by entering the URL `https://<OVOC server IP>/NBIF` in your Web browser.

NOTE

- The customer's Web browser must have installed the appropriate X.509 certificates signed by the same Certificate Authority (CA) as the OVOC server web browser certificates. Choose the appropriate certificate, and then click OK.
- For more information on the implementation of X.509 certificates, refer to the *OVOC Security Guidelines*.
- HTTP/S access to the NBIF folder requires a user name and password. This is required for multi-tenancy support where only authorized tenants should be able to access the NBIF folder. The Default user name is "nbif" and the default password "pass_1234". This password can be changed using the OVOC server Manager, for more information, refer to Section Change HTTP/S Authentication Password for NBIF Directory in the *OVOC Server IOM*.

The 'NBIF' folder content opens; double-click each one of the folders to list its contents. Double-click each file to open its contents.

Figure 2-2: NBIF Parent Directory

Index of /NBIF			
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 SEM/	21-Dec-2015 17:00	-	
 alarms/	17-Nov-2015 11:47	-	
 emsBackup/	18-Mar-2017 02:03	-	
 ippmanager/	14-Feb-2017 09:19	-	
 mgBackup/	22-Mar-2017 04:00	-	
 mgDebug/	13-Apr-2016 13:27	-	
 mgmt ca/	07-Jan-2016 17:18	-	
 pmFiles/	19-Apr-2016 09:25	-	
 tmp/	21-Mar-2017 14:03	-	
 topology/	21-Mar-2017 14:03	-	

Apache/2.2.3 (CentOS) Server at 10.3.180.2 Port 80

Figure 2-3: NBIF Topology Directory

Name	Last modified	Size	Description
Parent Directory		-	
MGsTopologyList.csv	21-Mar-2017 14:03	13K	

Apache/2.2.3 (CentOS) Server at 10.3.180.2 Port 80

The 'NBIF' folder contains the following sub-folders:

- **SEM:** this folder contains Scheduled Reports. For more information, see [Voice Quality Reports](#)
- **alarms:** this folder contains a file saved by the OVOC user (Actions > Save Alarms To File' which is available in the Active Alarms/History Alarms and Journal pages) where the action result displays no less than 1500 records. This file is created for local user requests and must not be collected by higher level Management or Backup systems.
- **emsBackup:** this folder contains the daily and weekly backup of the OVOC server. For more information, see [OVOC Server Backup and Restore](#).
- **ippmanager (Device Manager):** this folder contains the following folders:
 - generate: contains the device firmware files
 - regioncache: contains the device global cfg files
 - sess: contains system folder for sessions management
 - templates: contains the device cfg template files
 - tmp: contains system folder for temporary files
- **mgBackup:** This folder contains the backed up device configuration files. Up to five backup files can be stored for each managed device (for all formats) as follows:
 - AudioCodes SBC / Gateway Version 7.4.200 and later: .Zip Configuration Package.
 - MSBR: CLI script file
 - MP-202 or MP-204: Conf file
 - VoiceAI Connect: Zip file
 - Stack Manager: Json file

- For all other AudioCodes devices (except CloudBond, UMP and SmartTAP): ini files
- **mgDebug:** This folder contains Syslog and Packets debug information.
- **Mgmt_ca:** This folder contains the default certificate files for the OVOC Managed devices and the OVOC Root CA file.
- **pmFiles:** This folder contains the output XML file for Performance Monitoring data that is collected per polling interval according to the PM Profile and output to XML file according to the filter settings.
- **topology:** A Summary file of all the devices and their basic properties defined in the OVOC application. The summary file is located under the 'topology' folder and is always named MGsTopologyList.csv. For more information, see [Topology Files](#).

3 Topology CSV File

The Topology.csv file is used by the NMS system to synchronize the list of devices that are currently managed by the OVOC for the purposes of Alarms Forwarding integration. For example, if a specific device has not been receiving alarms, verify in the topology file if the relevant device is displayed in the list of connected gateways.

The Topology file is automatically updated upon the addition /removal of a device or upon updates to the device's properties, such as name, IP address or region modification. OVOC sends 'acEMSTopologyUpdateEvent' (Topology Update) for changes in the definition or update of a device and sends 'acEMSTopologyFileEvent' (Topology File Generated) for a topology file update. These events are displayed in the OVOC Alarm Browser and in the NMS Alarm Browser when the 'OVOC Events Forwarding' check box is selected in the Trap Configuration 'Destination Rule Configuration' dialog.

When multiple devices are added, the Topology file is updated approximately once per minute as the entire operation may take more than a few minutes. For detailed information on the exact event fields, refer to the *OVOC Alarms Guide*.

The file header is composed of two lines commencing with “;” file format version, and column names. Each row in the file represents a device in the OVOC topology and includes the following information:

Table 3-1: Topology CSV File

Parameter	Description
Device Serial Number	Displays either 32-bit and 64-bit serial numbers for SBC devices) according to the device firmware version and configuration settings in the externals/configurationProperties/generalConfig file for the include_serial_string.
IP Address	The IP address of the device.
Gateway Name	The gateway device name.
Region Name	The name of the region to which the device is attached.
Product Type	The device product type.
Software Version	The installed firmware version of the device.
Performance Polling	Indicates whether performance polling is enabled on the device.
Description	Device description field.
SBA FQDN	The FQDN name of the AudioCodes SBA device.

Parameter	Description
Name	
SBA IP Address	The IP address of the AudioCodes SBA device.
SNMP Version	The SNMP version enabled on the device (SNMPv2/SNMPv3).
SNMP Read	Encrypted SNMP read community string.
SNMP Write	Encrypted SNMP write community string.
SNMP User Profile	SNMP v3 user credentials in format: (EnginID;SecurityName;SecurityLevel;AuthProtocol;PrivacyKey)
Gateway User	Gateway user name for MG web access.
Gateway Password	Gateway user password for device web access.
HTTPS Enabled	Indicates whether HTTPS is enabled on the device (Enabled-1 and Disabled-0).
Device FQDN	The FQDN of the device.
Second Device Serial Number	See "Device Serial Number" above.
Tenant Name	The name of the tenant to which the device is attached.
Address	Geographical coordinates or actual IP address of the device in the geographical map.

See an example Excel file view in the figure below.

Figure 3-1: Topology File-Excel View

File		Home		Insert		Page Layout		Formulas		Data		Review		View		Automate		Help		Acrobat		Bad Ezerimisi		Comments		Share															
Cut		Copy		Paste		Clipboard		Font		Paragraph		Alignment		Number		Conditional Formatting		Format as Table		Styles		Insert		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity	
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity			
Calibri		11		A		General		Normal		Bad		Good		Delete		Format as Table		AutoSum		Sort & Find		Edit		Analyze Data		Sensitivity		Analyze		Sensitivity		Analyze		Sensitivity</							

Figure 3-2:

The Topology CSV file can be downloaded using the following methods:

- In the OVOC Web interface Devices page Actions menu (Maintenance > Download Topology). See [Download Topology](#).
- Using the 'Collect Logs' option in the OVOC Server Manager (see [Collect Logs](#)).
- By FTP or SFTP protocol

- Via Telnet or SSH using 'nbif' user with user nbif, pass_1234

4 Managing PM Files

Performance Monitoring data can be retrieved as follows:

- Data files can be generated for polled data according to PM profile for each polling interval (see [Creating PM Data File](#))
- Filter queries can be saved to an XML file which you can save to an external location (see [Saving PM Filter Queries](#))

NOTE

Performance Monitoring parameters can be managed using SNMP and REST API.

Saving PM Filter Queries

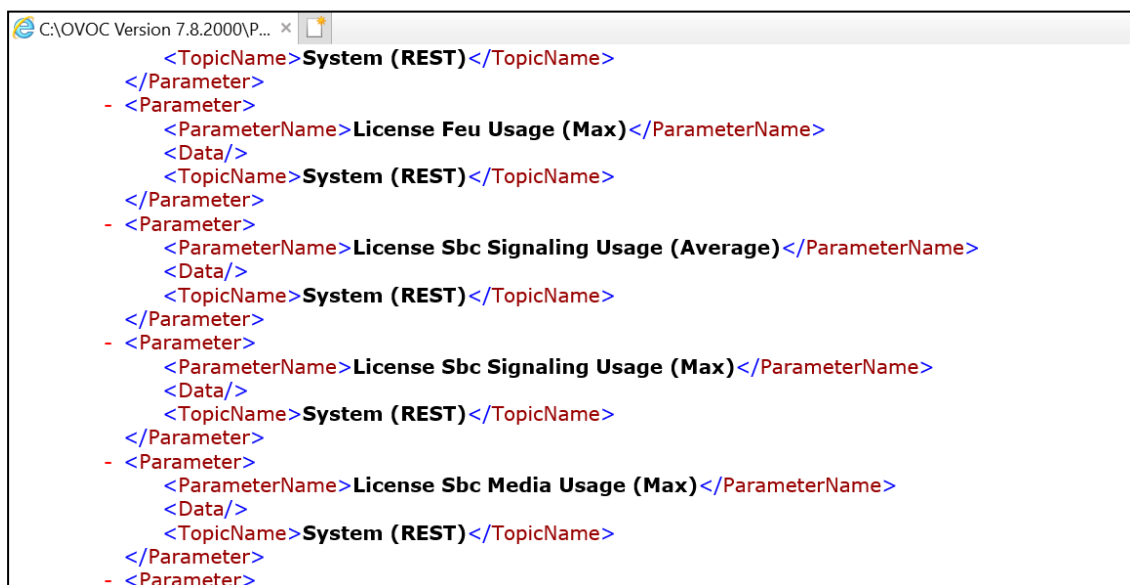
You can save PM filter queries to a CSV file by selecting the option **Save Device PM Data**.

➤ To save PM filter queries:

1. In the OVOC Web, open the Network Devices page (**Network** tab > **Devices** menu).
2. Select the device whose data you wish to extract and click **Show**.
3. Verify that the device is currently being polled.
4. Click the **Statistics** tab and add a new filter.
5. Click **Save Device PM Data**.

Filter output is saved to a CSV file; save the file to the desired external location. See example file below.

Figure 4-1: PM Data File



```

C:\OVOC Version 7.8.2000\P... x
<TopicName>System (REST)</TopicName>
</Parameter>
- <Parameter>
  <ParameterName>License Feu Usage (Max)</ParameterName>
  <Data/>
  <TopicName>System (REST)</TopicName>
</Parameter>
- <Parameter>
  <ParameterName>License Sbc Signaling Usage (Average)</ParameterName>
  <Data/>
  <TopicName>System (REST)</TopicName>
</Parameter>
- <Parameter>
  <ParameterName>License Sbc Signaling Usage (Max)</ParameterName>
  <Data/>
  <TopicName>System (REST)</TopicName>
</Parameter>
- <Parameter>
  <ParameterName>License Sbc Media Usage (Max)</ParameterName>
  <Data/>
  <TopicName>System (REST)</TopicName>
</Parameter>
- <Parameter>

```

Creating PM Data File

A PM data file can be automatically generated when the option "Create Data File" is selected in the PM Profile in the OVOC Web. The data file is generated for polled data for each polling interval for all parameters that are defined in the profile. These files can be retrieved from the NBIF directory (see [NBIF Folder](#)).

➤ **To create a PM data file:**

1. In the OVOC Web, open the Add PM Profile screen (**Statistics > PM Profiles > Add**).
2. Select the 'Create Data File' check box.

See example XML format in XML editor below.

Figure 4-2: Performance Monitoring XML Output

```

<root>
  <data>
    <topics>
      <topic>
        <topicName>SBC</topicName>
        <parameters>
          <parameter>
            <parameterData>
              <value>0.0</value>
            </parameterData>
            <paramName>acPMSBCAsrMax</paramName>
          </parameter>
          <parameter>
            <parameterData>
              <value>0.0</value>
            </parameterData>
            <paramName>acPMSBCAsrMin</paramName>
          </parameter>
          <parameter>
            <parameterData>
              <value>0.0</value>
            </parameterData>
            <paramName>acPMSBCAsrAverage</paramName>
          </parameter>
          <parameter>
            <parameterData>
              <value>0.0</value>
            </parameterData>
            <paramName>acPMSBCAsrAverage</paramName>
          </parameter>
        </parameters>
      </topic>
    </topics>
  </data>
</root>

```

5 Fault Management

AudioCodes devices report their faults (alarms and events) and state changes (Administrative/Operative state) via SNMP notification traps. Both standard and proprietary traps are supported. AudioCodes proprietary traps have the same variable bindings set. Each alarm includes information required by the ITU-T X.733 standard. Operative and Administrative states are managed according to the ITU-T X.731 standard. See the OVOC Alarms Guide for the exact list of standard, MG proprietary and OVOC proprietary traps that are supported for each device. For each trap description, it's indicated whether the trap is defined as an alarm or an event. This chapter includes the following:

- [Forwarding Alarms from OVOC Server to an NMS](#)
- [Forwarding Journal Entries from OVOC Server to an NMS](#)
- [Alarm and Journal Forwarding Data Formats](#)
- [Configuring Email \(SMTP\) with TLS on a Non-standard Port for OVOC](#)
- [OVOC Server Alarm Settings](#)
- [Status / State Management via Devices SNMP Interface](#)

Forwarding Alarms and Events to an NMS

Alarms can be forwarded to the NMS using one of the following methods:

- Alarms and events are forwarded by the OVOC application to the NMS for all network elements (devices, IP Phones and endpoints (purple-colored path in the figure below) or only Management alarms and events are forwarded (green-colored path in the figure below). See [Forwarding Alarms from OVOC Server to an NMS](#).
- Each one of the network elements (devices and devices) sends its own alarms directly to the NMS (blue-colored path in the figure below). The device can send alarms to several destinations (the exact number of destinations depends on the device type). For example, the device can send alarms to the OVOC and NMS. You can configure each destination with a different trap port. See [Forwarding Alarms Directly from Devices to NMS](#).

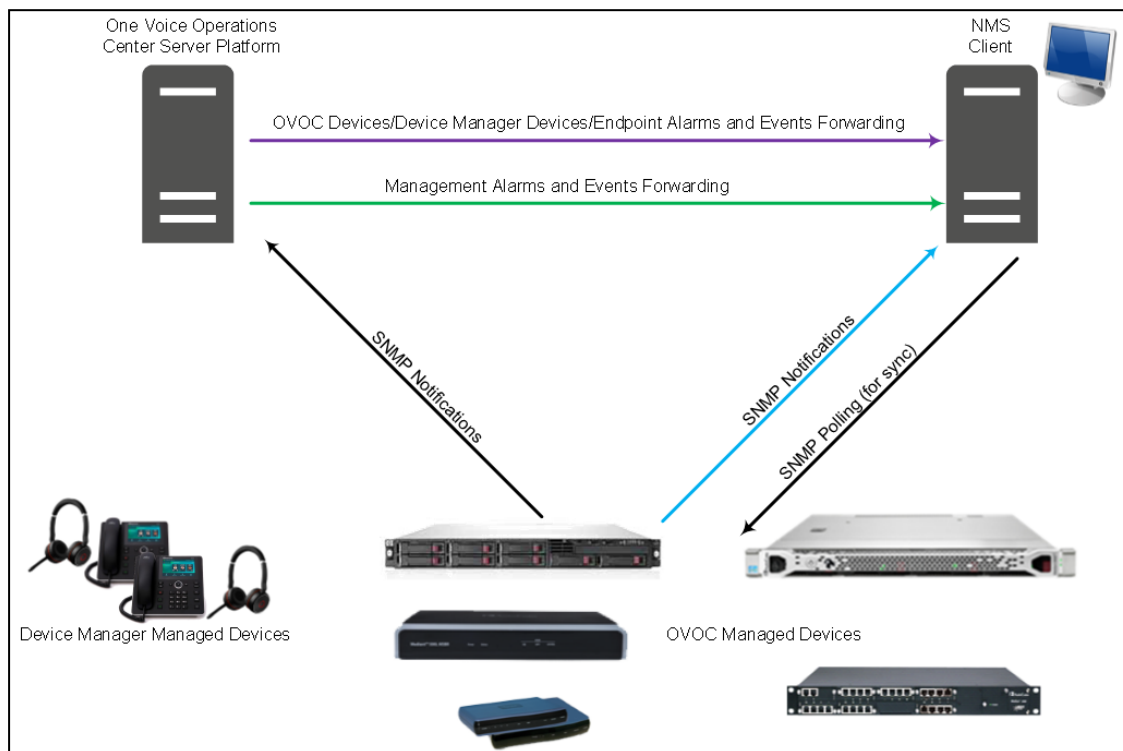
Alarms and events are forwarded to an NMS in one of the following formats:

- SNMPv2 or SNMPv3 traps. The SNMPv3 protocol provides more sophisticated security mechanisms than SNMPv2c. It implements a user-based security model (USM), allowing both authentication and encryption of the requests sent between the OVOC Manager and their agents, as well as user-based access control. SNMP can be configured in the OVOC at the global level using an SNMP Connectivity template, at the tenant level (Tenant SNMP Profile). You must configure identical SNMP settings on all managed devices.
- REST updates

NOTE

Alarms and events are always sent to an NMS as SNMP notifications for purposes of NMS integration.

Figure 5-1: Alarm and Event Forwarding



Forwarding Alarms from OVOC Server to an NMS

Alarms can be forwarded to an NMS either over SNMP or REST. Topology and Rule conditions can be configured per destination. Alarm rules can be configured by both Tenant and Global scope.

➤ To forward alarms from the OVOC to the NMS:

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

Figure 5-2: Alarms – Forwarding – Topology Conditions

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:	all Site/s,	All / None	

Topology Groups

Close

OK

- Configure using the table below as a reference:

Table 5-1: Forwarding Alarms – Topology Conditions - Parameter Descriptions

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events - or- Prevent forwarding matching alarms/events	Allows or prevents forwarding alarms according to the selected topology conditions. For example, in the figure below all alarms from tenant "102_102_1-15" and its sub-entities are not forwarded. Rule Owner* System - all tenants ATTACHMENTS Tenants: 1 Tenant/s, All / None Regions: 1 Region/s, All / None Devices: 6 Device/s, All / None Links: 1 Link/s, All / None Sites: 1 Site/s, All / None Topology Groups Open Topology Tree Search by Name, IP or Serial Number 4 ☒ 102_102_1-15 4 ☒ AutoDetection ▷ ☒ devices ▷ ☒ links ▷ ☒ sites ▷ ☐ Auto_test 4 ☐ default ▷ ☐ AutoDetection ▷ ☐ miryam ▷ ☐ New
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.
Rule Owner	From the Rule Owner drop-down list, select System – all tenants ; the rule is applied to all tenants and to all regions/links/devices/sites under all tenants. Alternatively, select a specific tenant; the rule is applied to all regions/links/devices/sites under this tenant.
Attached	Select All or None adjacent to each entity: Tenant; Region; Devices; Links; Sites Open Topology Tree Open Topology Tree and select the required entities to apply to the rule.

3. Click the **Rule Conditions** tab.

Figure 5-3: Alarms – Forwarding – Rule Conditions

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

- Configure using the table below as a reference:

Table 5-2: Forwarding Alarms – Rule Conditions - Parameter Descriptions

Parameter	Description
Forward matching alarms/events - or- Prevent forwarding matching alarms/events	Allows or prevents forwarding alarms according to rule conditions. In the example below, Management, Devices and QoE alarms and events are forwarded when raised with status 'Critical' and 'Major' for 'Communications', 'Quality of Service' and 'Equipment' alarms. ALARMS FORWARDING RULE DETAILS Rule Name* AlarmRuleExample ☒ 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 Management × Devices × QoE × none Event Origin Management × Devices × QoE × none Severities critical × major × Alarm Names All Selected Alarm Types Communications Alarm × Quality Of Service Alarm × Equipment Alarm × Close OK
Alarm Origin	Select the origin from which alarms will be forwarded: ■ Management ■ QoE ■ Devices ■ Endpoints ■ External Apps (ARM and Zoom)

Parameter	Description
	☒ VIP Endpoint Users
Event Origin	Select the origin from which events will be forwarded: ☒ Management ☒ QoE ☒ Devices ☒ Endpoints ☒ External Apps (ARM and Zoom) ☒ VIP Endpoint Users
Severities	From the 'Severities' dropdown, select the severity level of the alarms you want to receive: ☒ Warning ☒ Minor ☒ Major ☒ Critical ☒ Indeterminate Default: All Selected.
Alarm Names	Allows forwarding alarms according to specific alarm names. For example, if you select Power Supply Failure then only this alarm will be forwarded. Default: All Selected.
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.
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).

5. Click the **Destination** tab.
6. **SNMP Destination:** From the Destination Type drop-down, select **SNMP**.

Figure 5-4: Alarms – Forwarding – Destination SNMPv2

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 5-5: Alarms – Forwarding – Destination SNMPv3

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 Host IP Address*

Destination Host Port

162

☐ SNMP v2

☒ SNMP v3

Security Name*

Security Level*

No Security

Authentication Protocol

No Protocol

Authentication Key

Privacy Protocol

None

Privacy Key

Close

OK

7. Configure the parameters using the table below as a reference.

Table 5-3: Forwarding Alarms - Destination - SNMP

Parameter	Description
SNMPv2	
Destination Host IP Address	Enter the destination NMS host IP address to which to forward alarms. Make sure you receive the alarms and events in the specified IP address on the port specified below.
Destination Host Port	Enter the destination host port to which to forward alarms. Make sure you receive the alarms and events on the specified port in the IP address specified above. In the 'Destination Host port' field, enter the port number of the destination host (the default SNMP port for trap reception is 162).
SNMP v2/SNMP v3	Select either SNMP v2 or SNMP v3. Default: SNMP v3. Forwards only those alarms that are in the format of the SNMP version you select. Note: ensure that you configure identical SNMPv2 or SNMPv3 account details on the NMS.
Trap Community	[Only available if SNMP v2 is selected above]. Note: OVOC by default sends SNMPv2c traps with the field 'SNMPv2c Trap Community' set to public.
Security Name	Enter the name of the operator.
Security Level	From the drop-down select either: ☐ No security ☐ Authentication ☐ Authentication & Privacy See the table below for OVOC-Syslog mapping.
SNMPv3	
Authentication Protocol	Only available if you select Authentication or Authentication & Privacy from the list above. Select either: ☐ No Protocol ☐ MD5 ☐ SHA
Authentication Key	Only available if you select MD5 or SHA from the list above.
Privacy Protocol	From the drop-down list, select the SNMP v3 operator's privacy

Parameter	Description
	protocol. ☐ None ☐ DES ☐ AES-128
Privacy Key	Enter the privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.

8. **REST Interface:** From the Destination Type drop-down, select **REST**.

Figure 5-6: Alarms – Forwarding – Destination REST

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

9. Configure the parameters using the table below as a reference.

Table 5-4: Forwarding Alarms - Destination - REST

Parameter	Description
Host	FQDN name of the REST Server Host. For example corporate-firm-.siptrunk.com
Path	URL path of the REST Server. For example: https://corporate-firm-.siptrunk.com/tenantui
Authentication Header Key	Authorization (Default)
Authentication Header Value	Bearer <Bearer Value>

10. Select the **Active Time** tab.

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

NOTE

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.

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

Parameter	Description
All / None	Select a day days in the week on which the Journal forwarding feature will be active. ■ 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.
	Click this icon adjacent to a day to define the start and end time the Journal forwarding feature will be active on this day; optionally use the clock icon to configure the times. In the example below, alarms are not forwarded on weekends and between midnight and 0600 during week days.

Parameter	Description
	ALARMS FORWARDING RULE DETAILS Rule Name* ForwardingActiveTime ☒ 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 ☒ Monday 06:00 - 24:00 start 06:00 end 24:00 ☒ Tuesday 06:00 - 24:00 ☒ Wednesday 06:00 - 24:00 ☒ Thursday 06:00 - 24:00 ☒ Friday 06:00 - 24:00 ☐ Saturday Not Active ☐ Sunday Not Active Close OK

Forwarding Alarms Directly from Devices to NMS

Alarms are forwarded directly from the network element to the NMS over SNMPv2 or SNMPv3. On the managed devices, configure the NMS Trap Destination and identical SNMPv2 or SNMPv3 account settings. On the NMS, also configure identical SNMPv2 or SNMPv3 account settings. If you wish to forward alarms directly from devices to the NMS; however, forward alarms from the other network elements via the OVOC server, then you can configure the alarm forwarding rules, see [Forwarding Alarms and Events to an NMS](#).

Alarm Aggregation

An aggregated list of alarm notifications can be forwarded from OVOC in a batch in a single email with the alarm filter settings according to the Forwarding rule. "Max number of alarms to aggregate in single Email" sets the maximum number of alarms to aggregate into a single mail and "Email alarms aggregation time interval (seconds)" sets the time interval between sending the batch of alarms. For example, if the number of alarms to aggregate is set to 10, the time interval is set to 60 seconds and then after 60 seconds there are only 5 alarms raised according to the forwarding rule, then 5 alarms are forwarded.

Examples of Aggregated Alarms

The following shows examples of alarm alerts that are sent from OVOC to an NMS.

NOTE

Alarms are separated by ***** Info*****

Subject: OVOC received 10 new alarms

***** Event Info *****

Alarm Name: OVOC server Started

Date & Time: 1:12:54 PM Aug 8, 2018

Source: OVOC Mgmt

Source Description:

Severity: major

Unique ID: 0

Alarm Type: communicationsAlarm

Alarm Probable Cause : other

Description: Server Startup

Additional Info 1:

Additional Info 2:

Additional Info 3:

***** System Info *****

System Name: OVOC Mgmt

System IP Address: 172.17.118.148

***** Alarm Info *****

Alarm Name: License Pool Infra Alarm

Date & Time: 12:13:03 PM Aug 6, 2018

Source: Board#1

Source Description:

Severity: clear

Unique ID: 12

Alarm Type: communicationsAlarm

Alarm Probable Cause : keyExpired

Description: Alarm cleared: License Pool Alarm. Device was unable to access the License Server.

Additional Info 1:

Additional Info 2:

Additional Info 3:

***** Device Info *****

Device Name: 172.17.118.51

Device Tenant: Eran

Device Region: Tel Aviv

Device IP Address: 172.17.118.51

Device Type: Mediant 500 MSBR

Device Serial: 5856696

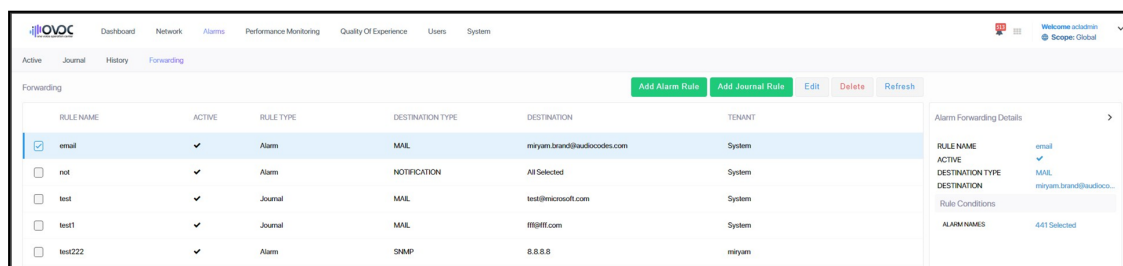
Device Description:

Forwarding Journal Entries from OVOC Server to an NMS

Journal entries can be forwarded to an NMS over REST. Topology and Rule conditions can be configured per destination. Journal rules can only be configured with Global scope permissions.

➤ To configure Journal forwarding:

1. Access the 'Global' scope.
2. Open the Forwarding page (**Alarms > Forwarding**).



3. Click **Add Journal Rule**.

JOURNAL FORWARDING RULE DETAILS

Rule Name*

JournalForwardingActiveTime

☒ Enable/Disable Rule

Rule Conditions

Destination

Active Time

Journal Names

All Selected

Action: Send Email

ARM Journal

Backup Service

Call: Read

Calls: Export to File

Calls: Read

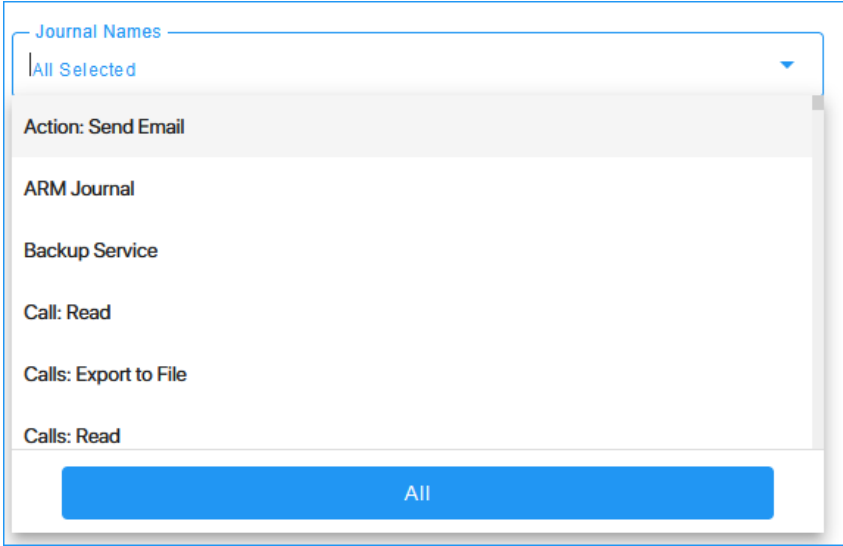
All

Close

OK

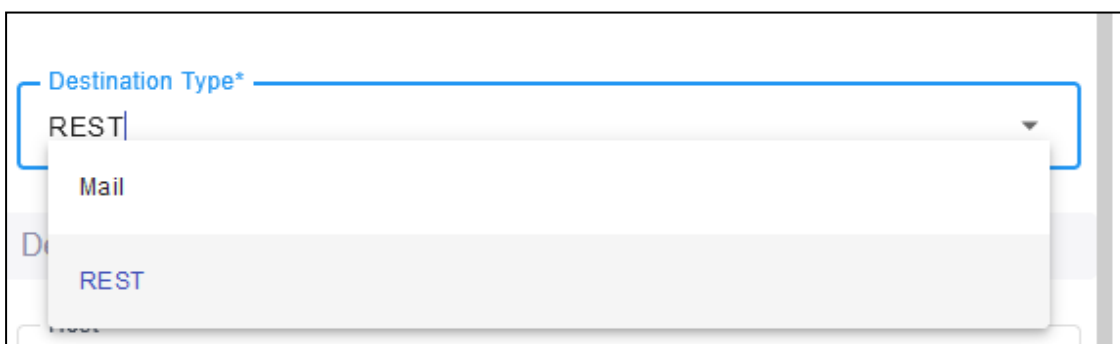
4. Configure the rule using the following table as reference.

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.

Parameter	Description
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. OVOC can forward Journal activity to the following Destination types:

- External Mail / Internal Mail
- REST



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

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

Parameter	Description
All / None	Select a day days in the week on which the Journal forwarding feature will be active. ■ Click All for the Journal forwarding feature to be active on all days in

Parameter	Description
	the week. ■ Click None for the Journal forwarding feature to be active on no days in the week.
+	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. In the example below, journal entries are forwarded from 0600 to 2100 during weekdays. JOURNAL FORWARDING RULE DETAILS Rule Name* JournalForwardingActiveTime ☒ Enable/Disable Rule Rule Conditions Destination Active Time All / None ☒ Monday 06:00 - 21:00 start 06:00 end 21:00 + + ^ ☒ Tuesday 06:00 - 21:00 + + + ☒ Wednesday 06:00 - 21:00 + + + ☒ Thursday 06:00 - 21:00 + + + ☒ Friday 06:00 - 21:00 + + + ☐ Saturday Not Active + ☐ Sunday Not Active + Close OK

Alarm and Journal Forwarding Data Formats

The formats of the data fields that are including in the alarms and journal s that are forwarded from OVOCvia SNMP and REST are shown below:

■ [SNMP Data Formats](#)

■ [REST Data Formats](#)

SNMP Data Formats

The table below describes the SNMP fields for forwarding alarm data to Northbound destinations.

Table 5-5: Alarm Forwarding SNMP Fields

MIB Name	Type	Description
Name (1)	- Integer 0..1000 - The Alarm/event number as listed by product (usually matches the last digit in the trap OID)	The alarm title.
TextualDescription(2)	OCTET STRING 0..200	Summary of the reported issue that is forwarded in the varbinds for the following alarm types: OVOC: acEMSTrapG-lobalsTextualDescription SBC: acBoardTrapG-lobalsDeviceDescription ARM: acARMTrapG-lobalsDeviceDescription Zoom: acZoomTrapG-lobalsDeviceDescription
Source (3)	- OCTET STRING 0..255 (Devices + OVOC: currently defined as 0..100) - The entity source of the problem, usually in the following format: ✓ Trunk#1 ✓ SEM/Link#2 ✓ Entity1#x/Entity2#y/Entity3#z	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.
Severity (4)	- cleared(0) - indeterminate(1) - warning(2) - minor(3) - major(4) - critical(5)	Possible severity value . This value is displayed from the variable-binding tgTrapGlobalsSeverity.
UniqID (5)	- String (1-255 chars) - The running number of alarms since the installation of the OVOC instance. - The value of this number should be managed by the system separately for alarms and events. - The OVOC application uses this number to recognize if alarms were missed and to retrieve them using the Carrier-grade system. - The forwarded information includes OVOC alarms sequencing for NMS carrier-grade alarms: where the running number events: always -1	Unique ID that is extracted from the managed device. NOTIFICATION-TYPE OID as it appears in the MIB. Corrective Action Possible corrective action when applicable. - 1
Type (6)	other(0)	Alarm type according to ITU X.733 definition.

MIB Name	Type	Description
	■ communicationsAlarm(1) ■ qualityOfServiceAlarm(2) ■ processingErrorAlarm(3) ■ equipmentAlarm(4) ■ environmentalAlarm(5) ■ integrityViolation(6) ■ operationalViolation(7) ■ physicalViolation(8) ■ securityServiceOrMechanismViolation(9) ■ timeDomainViolation(10)	This value is displayed from the variable-binding tgTrapGlobalsType.
ProbableCause (7)	■ other(0) ■ adapterError(1) ■ applicationSubsystemFailure(2) ■ bandwidthReduced(3) ■ callEstablishmentError(4) ■ communicationsProtocolError(5) ■ communicationsSubsystemFailure(6) ■ configurationOrCustomizationError(7) ■ congestion(8) ■ corruptData(9) ■ cpuCyclesLimitExceeded(10) ■ dataSetOrModemError(11) ■ degradedSignal(12) ■ dteDceInterfaceError(13) ■ enclosureDoorOpen(14) ■ equipmentMalfunction(15) ■ excessiveVibration(16) ■ fileError(17) ■ fireDetected(18) ■ floodDetected(19) ■ framingError(20) ■ heatingVentCoolingSystemProblem(21) ■ humidityUnacceptable(22) ■ inputOutputDeviceError(23) ■ inputDeviceError(24) ■ lanError(25) ■ leakDetected(26) ■ localNodeTransmissionError(27) ■ lossOfFrame(28) ■ lossOfSignal(29) ■ materialSupplyExhausted(30) ■ multiplexerProblem(31) ■ outOfMemory(32) ■ outputDeviceError(33) ■ performanceDegraded(34) ■ powerProblem(35) ■ pressureUnacceptable(36) ■ processorProblem(37) ■ pumpFailure(38)	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.

MIB Name	Type	Description
	■ queueSizeExceeded(39) ■ receiveFailure(40) ■ receiverFailure(41) ■ remoteNodeTransmissionError(42) ■ resourceAtOrNearingCapacity(43) ■ responseTimeExcessive(44) ■ retransmissionRateExcessive(45) ■ softwareError(46) ■ softwareProgramAbnormallyTerminated(47) ■ softwareProgramError(48) ■ storageCapacityProblem(49) ■ temperatureUnacceptable(50) ■ thresholdCrossed(51) ■ timingProblem(52) ■ toxicLeakDetected(53) ■ transmitFailure(54) ■ transmitterFailure(55) ■ underlyingResourceUnavailable(56) ■ versionMismatch(57) ■ authenticationFailure(58) ■ breachOfConfidentiality(59) ■ cableTamper(60) ■ delayedInformation(61) ■ denialOfService(62) ■ duplicateInformation(63) ■ informationMissing(64) ■ informationModificationDetected(65) ■ informationOutOfSequence(66) ■ intrusionDetection(67) ■ keyExpired(68) ■ nonRepudiationFailure(69) ■ outOfHoursActivity(70) ■ outOfService(71) ■ proceduralError(72) ■ unauthorizedAccessAttempt(73) ■ unexpectedInformation(74)	
AdditionalInfo1 (8)	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) This field is used by the system to provide additional information regarding the reported alarm/event.	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo1.
AdditionalInfo2 (9)	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) This field is used by the system to provide additional information regarding the reported alarm/event.	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo2.
AdditionalInfo3 (10)	■ OCTET STRING 0..255 ■ This field is used by the system to provide additional information regarding the reported alarm/event ■ The forwarded information is filled in the following format: GW_IP: <Device IP>, GW_TRAP_ID: <device's alarm unique ID>	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo3.

MIB Name	Type	Description
DateAndTime (11)	DateAndTime SNMP Object	The timestamp when the alarm was raised.
SystemSeverity (12)	- cleared(0) - indeterminate(1) - warning(2) - minor(3) - major(4) - critical(5) Each value represents the entire system severity when a specific alarm/event is issued. Note: This varbind is not sent for system alarms (alarms that were generated by OVOC such as OVOC Disk Space alarm).	Possible severity value . This value is displayed from the variable-binding tgTrapGlobalsSeverity.
DeviceName(13)	- OCTET STRING 0..255 (Devices+ OVOC: currently defined as 0..250) - This field should not be filled by any of the products, as its reserved for OVOC when an alarm/event is forwarded. The information is filled in the following format: - Until Version 7.4: MG Region:<EMS Region Name>, MG Name:<EMS MG Name> - Until Version 7.6: <Entity Type> Name:<Entity Name>, Tenant:<Tenant Name>, Region:<Region Name> Where entity type can be one of the following: - Tenant, Region, Site, Device, Link, System etc. - Tenant: <Tenant Name> - exists only when the entity has tenant - Region: <Region Name> - exists only when the entity has region	The device entity name as described in the adjacent "Type" column.
DeviceInfo(14)	- OCTET STRING 0..255 (Devices + OVOC: currently defined as 0..100) - This field should not be filled by any of the products, as its reserved for OVOC when the alarm/event is forwarded. The information is filled in the following format: - Until Version 7.4: MG Type: <Device Type>, MG Serial: <primary device serial number>, <secondary device serial number> <secondary device serial number> is applicable for HA devices only - Until Version 7.6: Device Type: <Device Type> - Empty if entity not a device	The detailed device identifiers.
DeviceDescription(15)	- OCTET STRING 0..255 - This field should not be filled by any of the products, as its reserved for OVOC when the alarm/event is forwarded. The information is filled in the following formats: <Device Description> is filled when an alarm is raised on a Device entity. <SBA Description> is filled when an alarm is raised on the SBA entity (provisioned in the Device details under SBA definition rubric). <External application Description>: is filled when an alarm is raised on the ARM or Zoom entities. <Tenant Description> - is filled when an alarm is raised on a Tenant entity.	A free text description field can also be globally configured in the OVOC Server Configuration page (System > Administration > OVOC Server > Configuration) for all OVOC System alarms. This text is then sent to trap destinations in alarm forwarding in the varbind acEMSTrapGlobalsDeviceDescription field for all system alarms. For example, OVOC Disk Space alarm. Note: The hard-coded text description of the alarm that is sent in the TextualDescription(2) acEMSTrapGlobalsTextualDescription varbind (see above) is a separate description field that is different for each alarm OID.

MIB Name	Type	Description
	■ <Region Description> - is filled when an alarm is raised on a Region entity. ■ <Link Description> - is filled when an alarm is raised on a Link entity.	
SystemSerialNumber (16)	From Version 7.6: OCTET STRING 0..255 The information is filled in the following format: ■ For Stand-alone systems: <Device serial number> ■ For HA Systems: format <device serial #1>_<device serial #2> Device Serial Number (displays either 32-bit and 64-bit serial numbers for SBC devices) according to the device's firmware version and configuration settings in the externals/configurationProperties/generalConfig file for the include_serial_string.	Device serial number information as described in the adjacent 'Type' column.

REST Data Formats

The table below describes the REST fields for forwarding data to Northbound destinations.

Table 5-6: Alarm Forwarding REST Fields

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
name	String (1-100 chars)	The alarm title.	√	√
alarmType	String	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding.	√	×
isEvent	Boolean	Indicates whether the trap is an alarm or an event.	√	×
alarmTextualDescription	String (1-255 chars)	The alarm text description shown in the raised alarm.	√	√
alarmSource	String (1-255 chars)	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.	√	√
alarmUniqId	■ String (1-255 chars) ■ The running number of alarms since the installation of the OVOC instance. ■ The value of this number should be managed by the system separately for alarms and events. ■ The OVOC application uses this number to recognize if alarms were missed and to retrieve them using the Carrier-grade system. ■ The forwarded information includes OVOC alarms sequencing for NMS carrier-grade alarms: where the running number events: always -1	Unique ID that is extracted from the managed device. NOTIFICATION-TYPE OID as it appears in the MIB. Corrective Action Possible corrective action when applicable. - 1	√	×

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
alarmCategory	ItuAlarmType	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsType.	√	×
alarmProbCause	ItuAlarmProbableCause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.	√	×
alarmAddInfo1	String (0-255 chars)	Additional information fields according to the specific scenario.	√	×
alarmAddInfo2	String (0-255 chars)	Additional information fields according to the specific scenario.	√	×
alarmAddInfo3	String (0-255 chars)	Additional information fields according to the specific scenario.	√	×
alarmSourceDescription	String (0-255 chars)	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.	√	×
alarmSeverity	One of the following values: ■ cleared(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5) Each value represents the entire system severity when a specific alarm/event is issued. Note: This varbind is not sent for system alarms (alarms that were generated by OVOC such as OVOC Disk Space alarm).	This value is displayed from the variable-binding tgTrapGlobalsSeverity. In addition, the Textual description value is displayed from the variablebinding tgTrapGlobalsTextualDescription.	√	×
alarmDateAndTime	Date	Date and time when the alarm was raised.	√	√
unitType	Entity Type	The entity type on which the alarm was raised: ■ NotRelevant = -1 ■ Tenant = 0 ■ Region = 1 ■ Site = 2 ■ Device = 3 ■ Link = 4 ■ Endpoint = 5 ■ LdapUser = 6 ■ Group = 7 ■ ActiveDirectory = 25 ■ ARM = 29 ■ System = 100	√	√
alarmRemoteHost	IPv4/IPv6 // OPTIONAL	Remote host destination.	√	√
regionName	String (1-100 chars) //OPTIONAL	Name of the region upon which the alarm was raised.	√	√

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
unitName	String (1-100 chars) //OPTIONAL	The name of the entity on which the alarm was raised. For example, device or link name.	√	√
tenantName	String (1-100 chars) //OPTIONAL	Name of the managed tenant upon which the alarm was raised.	√	√
deviceInfo	{ // OPTIONAL - not sent in case it's not a device alarm "productType" : MGType "serialNum" : String (0-510) //in case of HA device - SN1_SN2 "description" : String (0-255) "severity" : ItuPerceivedSeverity }	Alarm raised on the managed device e.g. gateway/SBC	√	√
operator	String (1-100 chars)	The name of the operator performing the journal action.	✖	√
operatorIpAddress	String (1-100 chars)	The IP address of the operator performing the journal action.	✖	√

The REST formats for forwarding alarm data are shown below.

```
"alarms" :
```

```
[
```

```
{
```

```
"name" : String (1-100 chars),
```

```
"alarmType" : String,
```

```
"isEvent" : Boolean,
```

```
"alarmTextualDescription" : String (1-255 chars),
```

```
"alarmSource" : String (1-255 chars),
```

```
"alarmSeverity" : ItuPerceivedSeverity,
```

```
"alarmUniqId" : String (1-100 chars),
```

```
"alarmCategory" : ItuAlarmType,
```

```

    "alarmProbCause" : ItuAlarmProbableCause,

    "alarmAddInfo1" : String (0-255 chars),

    "alarmAddInfo2" : String (0-255 chars),

    "alarmAddInfo3" : String (0-255 chars),

    "alarmSourceDescription" : String (0-255 chars),

    "alarmDateAndTime" : Date,

    "unitType" : EntityType

    "alarmRemoteHost" : IPv4/IPv6 // OPTIONAL

    "regionName " : String (1-100 chars) //OPTIONAL

    "unitName" : String (1-100 chars) //OPTIONAL

    "tenantName " : String (1-100 chars) //OPTIONAL

    alarm    "deviceInfo":{ // OPTIONAL - not sent in case it's not a device
    "productType" : MGType

    "serialNum" : String (0-510) //in case of HA device - SN1_SN2

    "description" : String (0-255)

    "severity" : ItuPerceivedSeverity

    }

    }]

```

Syslog Data Formats

The table below describes the fields that are included in alarms that are forwarded to a Syslog server.

Table 5-7: Forwarding Fields: Syslog Server

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
alarmSeverity	One of the following values: ■ cleared(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5) Each value represents the entire system severity when a specific alarm/event is issued. Note: This varbind is not sent for system alarms (alarms that were generated by OVOC such as OVOC Disk Space alarm).	This value is displayed from the variable-binding tgTrapGlobalsSeverity. In addition, the Textual description value is displayed from the variablebinding tgTrapGlobalsTextualDescription.	√	×
source (alarm source+ source description)	string (1-255 chars)	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.	√	√
description (alarm textual description)	string (1-255 chars)	The alarm text description shown in the raised alarm.	√	√
name (alarm entity name)	string (1-100 chars)	The alarm title	√	√
tenant (alarm entity tenant)	string (1-100 chars)	The name of the managed tenant upon which the alarm was raised.	√	√
region (alarm entity region)	string (1-100 chars)	The name of the region upon which the alarm was raised.	√	√
ip address (alarm entity ip address)	string (1-100 chars)	The IP address of the entity upon which the alarm is raised.	√	√
device type (alarm device type)	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) ■ This field should not be filled by any of the products, as its reserved for OVOC when the alarm/event is forwarded. The information is filled in the following format: ■ Until Version 7.4: MG Type: <Device Type>, MG Serial: <primary device serial number>, <secondary device serial number> <secondary device serial number> is applicable for HA devices only ■ Until Version 7.6: Device Type: <Device Type> Empty if entity not a device	The detailed device identifiers.	√	×
device serial (alarm device)	From Version 7.6: OCTET STRING 0..255	Device serial number information.	√	×

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
serial number)	The information is filled in the following format: - For Stand-alone systems: <Device serial number> - For HA Systems: format <device serial #1>_<device serial #2> Device Serial Number (displays either 32-bit and 64-bit serial numbers for SBC devices) according to the device's firmware version and configuration settings in the externals/configurationProperties/generalConfig file for the include_serial_string.			
device description	string (1-100 chars)	The alarm text description shown in the raised alarm.	√	×
device severity	- cleared(0) - indeterminate(1) - warning(2) - minor(3) - major(4) - critical(5) Each value represents the entire system severity when a specific alarm/event is issued. Note: This varbind is not sent for system alarms (alarms that were generated by OVOC such as OVOC Disk Space alarm).	Possible severity value . This value is displayed from the variable-binding tgTrapGlobalsSeverity.	√	×

An example of an alarm forwarded to a syslog server is shown below.

```

10:27:02.725 syslog.notice OVOC: New Alarm - Security Alarm, received from VOCA CIC [redacted] with clear severity. Source: OVOC Mgmt,Description: Cre
10:39:02.752 syslog.alert OVOC: New Alarm - Connection Alarm, received from VOCA CIC [redacted] with critical severity. Source: OVOC Mgmt,Description: Connection L
10:42:02.766 syslog.notice OVOC: New Alarm - Security Alarm, received from VOCA CIC [redacted] with clear severity. Source: OVOC Mgmt,Description: Cre
10:48:02.788 syslog.notice OVOC: New Alarm - Security Alarm, received from VOCA CIC [redacted] with clear severity. Source: OVOC Mgmt,Description: Cre
11:17:32.834 syslog.alert OVOC: New Alarm - Voca Resource Pool Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConn
11:23:32.858 syslog.error OVOC: New Alarm - Scheduler Alarm, received from VOCA CIC [redacted] with minor severity. Source: /OperatorConnectManager,D
11:26:32.870 syslog.alert OVOC: New Alarm - Storage Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConnectManager,D
12:15:32.920 syslog.alert OVOC: New Alarm - Voca Resource Pool Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConn
12:15:32.924 syslog.error OVOC: New Alarm - Scheduler Alarm, received from VOCA CIC [redacted] with minor severity. Source: /OperatorConnectManager,D
12:15:32.927 syslog.alert OVOC: New Alarm - Storage Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConnectManager,D
12:15:32.930 syslog.notice OVOC: New Alarm - Authentication Failure Alarm, received from VOCA CIC [redacted] with clear severity. Source: /OperatorConn
12:15:32.932 syslog.error OVOC: New Event - Alarms Sync, received from VOCA CIC [redacted] with minor severity. Source: OVOC Mgmt,Description: Partia
12:18:22.950 syslog.alert OVOC: New Alarm - Voca Resource Pool Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConn
12:18:22.954 syslog.error OVOC: New Alarm - Scheduler Alarm, received from VOCA CIC [redacted] with minor severity. Source: /OperatorConnectManager,D
12:18:32.964 syslog.alert OVOC: New Alarm - Storage Alarm, received from VOCA CIC [redacted] with critical severity. Source: /OperatorConnectManager,D
12:18:32.968 syslog.error OVOC: New Event - Alarms Sync, received from VOCA CIC [redacted] with minor severity. Source: OVOC Mgmt,Description: Partia
13:07:03.047 syslog.alert OVOC: New Alarm - Connection Alarm, received from VOCA CIC [redacted] with critical severity. Source: OVOC Mgmt,Description: Cre
13:09:23.054 syslog.alert OVOC: New Alarm - Security Event, received from OVOC Mgmt [redacted] with critical severity. Source: OVOC Mgmt,Description: Partia
13:25:23.077 syslog.info OVOC: New Event - Topology Update, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:26:13.080 syslog.info OVOC: New Event - SSH Connection Status, received from [redacted] with info severity. Source: Board1,Descri
13:26:13.084 syslog.info OVOC: New Event - SSH Connection Status, received from [redacted] with info severity. Source: Board1,Descri
13:26:23.087 syslog.info OVOC: New Event - SSH Connection Status, received from [redacted] with info severity. Source: Board1,Descri
13:26:43.094 syslog.alert OVOC: New Alarm - Connection Alarm, received from [redacted] with critical severity. Source: OVOC Mgmt,Descri
13:26:43.104 syslog.info OVOC: New Event - Topology Update, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:26:43.104 syslog.info OVOC: New Event - Topology File Generated, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:27:13.119 syslog.notice OVOC: New Alarm - Connection Alarm, received from [redacted] with clear severity. Source: OVOC Mgmt,Description: Partia
13:27:13.129 syslog.info OVOC: New Event - Topology Update, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:27:13.139 syslog.notice OVOC: New Event - Cold Start Missed, received from [redacted] with clear severity. Source: OVOC Mgmt,Description: Partia
13:27:43.134 syslog.info OVOC: New Event - Topology File Generated, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:30:43.143 syslog.info OVOC: New Event - Topology File Generated, received from [redacted] with info severity. Source: OVOC Mgmt,Description: Partia
13:33:43.159 syslog.alert OVOC: New Alarm - Board Fatal Error, received from [redacted] with critical severity. Source: Board1,Descri

```

Email Data Formats

The table below describes the fields included in alarms that are forwarded to an email server.

Table 5-8: Forwarding Fields: Email Server

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
name (alarm name)	string (1-100 chars)	The alarm title.	√	√

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
date & time	string(\$date-time	date & timestamp indicating when the email was sent.	√	√
alarmSource	string (1-255 chars)	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.	√	√
alarm				
source description	string (0-255 chars)	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.	√	√
severity	ItuPerceivedSeverity	This value is displayed from the variable-binding tgTrapGlobalsSeverity. In addition, the Textual description value is displayed from the variablebinding tgTrapGlobalsTextualDescription.	√	×
unique id	string (1-100 chars)	NOTIFICATION-TYPE OID as it appears in the MIB. Corrective Action Possible corrective action when applicable. - 1	√	√
alarm type	string	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding.	√	×
alarm probable cause	ItuAlarmProbableCause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.	√	×
description	string (1-255 chars)	The alarm text description shown in the raised alarm.	√	×
additional info 1	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) This field is used by the system to provide additional information regarding the reported alarm/event.	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo1.	√	×
additional info 2	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) This field is used by the system to provide additional information regarding the reported alarm/event.	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo2.	√	×
additional info 3	■ OCTET STRING 0..255 ■ This field is used be the system to provide additional information regarding the reported alarm/event ■ The forwarded information is filled in the following format: GW_IP: <Device IP>, GW_TRAP_ID: <device's alarm unique ID>	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo3.	√	×
event				
operator	string (1-100 chars)	The name of the operator performing the journal action.	√	√
operator ip	string (1-100 chars)	The IP address of the operator	√	√

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
address		performing the journal action.		
description	string (1-100 chars)	The event text description shown in the raised event.	√	√
name (alarm entity name)	string (1-100 chars)	The alarm title	√	√
tenant (alarm entity tenant)	string (1-100 chars)	The name of the tenant entity upon which the alarm is raised.	√	√
region (alarm entity region)	string (1-100 chars) //OPTIONAL	The name of the region upon which the alarm is raised.	√	√
site (alarm entity region)	string (1-100 chars) //OPTIONAL	The name of the site upon which the alarm is raised.	√	√
ip address (alarm entity ip address)	string (1-100 chars)	The IP address of the entity upon which the alarm is raised.	√	√
service (service name)	string (1-100 chars)	The name of the service upon which the alarm is raised.	√	×
customer (customer name)	string (1-100 chars)	The name of the customer upon which the alarm is raised.	√	×
device type (alarm device type)	■ OCTET STRING 0..255 ■ (Devices + OVOC: currently defined as 0..100) ■ This field should not be filled by any of the products, as its reserved for OVOC when the alarm/event is forwarded. The information is filled in the following format: ■ Until Version 7.4: MG Type: <Device Type>, MG Serial: <primary device serial number>, <secondary device serial number> <secondary device serial number> is applicable for HA devices only ■ Until Version 7.6: Device Type: <Device Type> Empty if entity not a device	The detailed device identifiers.	√	×
device serial (alarm device serial number)	From Version 7.6: OCTET STRING 0..255 The information is filled in the following format: ■ For Stand-alone systems: <Device serial number> ■ For HA Systems: format <device serial #1>_<device serial #2> Device Serial Number (displays either 32-bit and 64-bit serial numbers for SBC devices) according to the device's firmware version and configuration settings in the externals/configurationProperties/generalConfig file for the include_serial_string.	Device serial number information.	√	×
device description	■ OCTET STRING 0..255 ■ This field should not be filled by any of the products, as its reserved for OVOC when the alarm/event is forwarded. The information is filled in the following formats:	A free text description field can also be globally configured in the OVOC Server Configuration page (System > Administration > OVOC Server > Configuration) for all OVOC System alarms. This text is then sent to trap	√	×

Entity Name	Type	Description	Alarm Forwarding	Journal Forwarding
	■ <Device Description> is filled when an alarm is raised on a Device entity. ■ <SBA Description> is filled when an alarm is raised on the SBA entity (provisioned in the Device details under SBA definition rubric). ■ <External application Description>: is filled when an alarm is raised on the ARM or Zoom entities. ■ <Tenant Description> - is filled when an alarm is raised on a Tenant entity. ■ <Region Description> - is filled when an alarm is raised on a Region entity. ■ <Link Description> - is filled when an alarm is raised on a Link entity.	destinations in alarm forwarding in the varbind acEMSTrapGlobalsDeviceDescription field for all system alarms. For example, OVOC Disk Space alarm. Note: The hard-coded text description of the alarm that is sent in the TextualDescription(2) acEMSTrapGlobalsTextualDescription varbind (see above) is a separate description field that is different for each alarm OID.		
device severity	■ cleared(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5) Each value represents the entire system severity when a specific alarm/event is issued. Note: This varbind is not sent for system alarms (alarms that were generated by OVOC such as OVOC Disk Space alarm).	Possible severity value . This value is displayed from the variable-binding tgTrapGlobalsSeverity.	√	×

An example of an alarm forwarded to an email is shown below.

OVOC received 6 new alarms

Summarize

OVOC <OVOC@audiocodes.com>

To: [REDACTED]

Reply

Reply All

Forward

More

Thu 9/12/2024 4:06 PM

We removed extra line breaks from this message.

***** Alarm Info *****

Alarm Name: QoE: Poor Voice Quality Alarm Date & Time: 2:05:00 PM Sep 12, 2024

Source: OVOC QoE/Device

Source Description:

Severity: clear

Unique ID: 5059055

Alarm Type: Quality Of Service Alarm

Alarm Probable Cause : Threshold Crossed

Description: Clearing currently active alarm before raising different severity alarm on the same source.

Additional Info 1: cleared severity threshold is 0 %.

Additional Info 2: Time interval: 12-Sep-2024:11:05:00 - 12-Sep-2024:14:05:00.

Additional Info 3: 10.3.181.223

***** Device Info *****

Device Name: 10.3.181.223

Device Tenant: Tenant_2

Device Region: region2

Device IP Address: 10.3.181.223

Device Type: Mediant 800C E-SBC

Device Serial: 11811701

Device Description:

- 43 -

Configuring Email (SMTP) with TLS on a Non-standard Port for OVOC

This procedure configures **Exim** on OVOC to send email through Microsoft Office 365 (smtp.office365.com) over port 587 with STARTTLS enforced. The default Exim certificates are used and work without further configuration, however, you can optionally use custom certificates.

➤ **To configure Exim.conf:**

1. Login to the OVOC server machine with **root** permissions.
2. Open `/etc/exim/exim.conf`.
3. Add the following after **begin routers**:

```
send_via_o365:
```

```
driver = manualroute
```

```
domains = !+local_domains
```

```
transport = o365_smtp
```

```
route_list = * smtp.office365.com::587 byname
```

```
host_find_failed = defer
```

```
no_more
```

4. Add the following after **begin transports**:

```
o365_smtp:
```

```
driver = smtp
```

```
hosts = smtp.office365.com
```

```
hosts_require_auth = smtp.office365.com
```

```
hosts_require_tls = smtp.office365.com
```

```
port = 587
```

5. Add the following after **begin rewrite**:

```
<valid customer email address> Ffr
```

6. Add the following after **begin authenticators**:

```
o365_login:
```

```
driver = plaintext
```

```
public_name = LOGIN
```

```
client_send = : username : password
```

Where **username** and **password** are the credentials of the Office 365 mailbox used for sending mails.

7. Save and close **exim.conf**.
8. Open **/root/.muttrc** and change the following:

```
set from = "OVOC@audiocodes.com"
```

```
set realname = "OVOC"
```

```
set record=""
```

Where:

- **from**: The valid address in the customer's domain.
 - **realname**: The hostname of the customer's server.
9. (Optional): If you wish to use custom certificates instead of the Default Exim default certificates, add the following to **exim.conf**:

```
tls_certificate = /etc/ssl/certs/server.crt
```

```
tls_privatekey = /etc/ssl/private/server.key
```

```
tls_advertise_hosts = *
```

- Change the file paths to match your certificate and key locations.

10. Enter the following command to restart Exim:

```
service exim restart
```

OVOC Server Alarm Settings

This section describes the global alarm settings on the OVOC server.

Alarms Automatic Clearing (on Startup)

The Active Alarms page is cleared of all the current alarms for a specific device upon system GW startup (cold start event). Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Active Alarms Page (and transferred to the Alarms History page) when a Clear alarm is generated by the same entity (source) and the same device. This feature prevents older alarms from congesting the Active Alarms page. This feature is configured in the Alarms page (System tab > Configuration > Alarms).

Alarms Automatic Clearing Period (Days)

The operator can also configure the automatic clearing of Active alarms (disabled by default) according to a time period. When the Automatic Clearing feature is enabled, alarms are cleared by default every 30 days.

When the OVOC application performs automatic clearing, it moves the cleared Alarms to the Alarms History page with the text indication 'Automatic Cleared'. This feature is configured in the Alarms page (System tab > Configuration > Alarms).

Events Clearing Mechanism

Events are informative messages for OVOC and device actions (usually with low severity). Device events (originating from the device) are automatically cleared from the Active Alarms page upon GW startup (cold start event); however, device events originating in the OVOC (e.g. adding a gateway) are not cleared upon device restart. The OVOC consequently employs a mechanism to automatically clear these events from the Alarms page (by default this feature is enabled and events are cleared every three days). This feature prevents old events from congesting the Active Alarms page. When automatic clearing is performed, the cleared Events are moved to the Alarm History page with the text indication 'Automatic Cleared'. This feature is configured in the Alarms page (System tab > Configuration > Alarms).

Alarm Suppression Mechanism

This option enables the generating of the 'Alarm Suppression' alarm 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. This feature is configured in the Alarms page (System tab > Configuration > Alarms).

Alarms Sequence Numbering

1. When receiving alarms directly from the devices and endpoints:
 - These alarms and events have a different scala of sequence numbers. These sequence numbers are placed at 'TrapGlobalsUniqID' varbindings (respectively 'tgTrapGlobalsUniqID', 'acBoardTrapGlobalsUniqID').
 - OVOC alarms have a sequence number scala. Events are always sent with 'acEMSTrapGlobalsUniqID -1'.
2. When the OVOC server forwards device and OVOC alarms:
 - Cold Start Trap is the only standard event that is forwarded by the OVOC application. All other standard events are not forwarded.
 - Each one of the alarms and events are forwarded with the original Notification OID and variable bindings OIDs.
 - The original content of 'TrapGlobalsUniqID' varbinding (respectively 'tgTrapGlobalsUniqID', 'acBoardTrapGlobalsUniqID' and 'acEMSTrapGlobalsUniqID') is updated as follows:
 - ◆ For all the forwarded events, the 'TrapGlobalsUniqID' is set to -1.
 - ◆ For all the forwarded alarms, the original 'TrapGlobalsUniqID' is replaced with the OVOC sequence number, allowing the NMS to follow the forwarded alarms sequencing. The original device 'TrapGlobalsUniqID' is applied to 'TrapGlobalsAdditionalInfo3' varbinding.
 - ◆ For all the forwarded alarms and events, 'TrapGlobalsAdditionalInfo3' varbinding (respectively 'tgTrapGlobals AdditionalInfo3', 'acBoardTrapGlobals AdditionalInfo3' and 'acEMSTrapGlobals' 'AdditionalInfo3') is updated as follows: original device IP address and device 'TrapGlobalsUniqID' in the following format:

```
GATEWAY_IP:x ,GATEWAY_TRAP_ID:y
```

A carrier-grade alarm system is characterized by the following:

■ Active Alarms

The device can determine which alarms are currently active by maintaining an Active Alarms table. When an alarm is raised, it is added to the active alarms list. Upon alarm clearing, it is removed from the active alarms list.

The maximal size of the active alarms for each of the product is shown in the table below:

Table 5-9: Maximum Active Alarms according to Device

Product	Maximum Size of Active Alarms Table
MP-1xx	40
MP-124	100
MP-1288	200
Mediant 500 MSBR, Mediant 500 SBC, Mediant 500L MSBR, Mediant 500L SBC, Mediant 800 MSBR, Mediant 800 SBC and Mediant 1000 SBC	300
Mediant 3000	500
Mediant 2600 E-SBC and Mediant 4000 SBC	600
Mediant 9000 SBC and Mediant Software SBC	1000

When the active alarms list exceeds its maximum size, an enterprise Active Alarms Overflow alarm is sent to the Management system.

- The device sends a cold start trap to indicate that it is starting up. This allows the management system to synchronize its view of the device's active alarms.
- Two views of active alarms table are supported by devices:
 - ◆ Standard MIB: alarmActiveTable and alarmActiveVariableTable in the IETF ALARM MIB for all the devices.
 - ◆ Enterprise MIB:
 - acActiveAlarmTable in the AC-ALARM-MIB mib for devices products.
 - AudioCodes.acProducts.acEMS.acEMSConfiguration.acFaults (see [SNMP Alarms Synchronization](#) below).

■ History Alarms

The device allows the recovery of lost alarm raise and clear notifications by maintaining a log history alarms table. Each time an alarm-type trap (raise or clear) is sent, the Carrier-Grade Alarm System adds it to the alarms history list. The trap contains a unique Sequence Number. Each time a trap is sent, this number is incremented. The device allows detection of lost alarms and clear notifications by managing an alarm sequence number and displaying the current number.

The maximal size of the history alarms table is defined as follows:

Table 5-10: Maximum Active Alarms according to Device

Product	Maximum Size of History Alarms Table
MP-1xx	100
MP-1288	1000
Mediant 500 MSBR, Mediant 500 SBC, Mediant 500L MSBR, Mediant 500L SBC, Mediant 800 MSBR, Mediant 800 SBC and Mediant 1000 SBC	1000
Mediant 3000	500
Mediant 2600 E-SBC and Mediant 4000 SBC	1000
Mediant 9000 SBC and Software SBC	2000

When the history alarm list exceeds its maximum size, it starts overriding the oldest alarms in the list in cyclic order.

- The following views of log history alarms table are supported by the devices:
 - ◆ Standard MIB: 'nlmLogTable' and 'nlmLogVariableTable' in the NOTIFICATION-LOG-MIB for all the devices.
 - ◆ Enterprise MIB:
 - acAlarmHistoryTable in the 'AC-ALARM-MIB mib' for CPE and MP products.

SNMP Alarms Synchronization

A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account Operations Center system or network layer outages, and transport layer outages, such as SNMP over UDP. During such outages, alarms may be raised, however not forwarded. This mechanism is implemented at SNMP agent level, and serves OVOC, NMS, or higher level management system synchronization. During the OVOC server synchronization process, the OVOC server can recover such missed alarms from its database (events are not synchronized) and then forward them to the NMS according to the following:

- History alarms: By default, synchronization is performed with the Alarms History table. When only a partial Alarms History table is retrieved from the OVOC server database, the OVOC server notifies the user with one of the following events: 'Synchronizing Alarms Event' and 'Synchronizing Active Alarms Event'. For more information, see the OVOC Alarms Guide.
- Active alarms: By default, synchronization is not performed with the Active Alarms table; however, a mechanism can be implemented to perform random synchronization of this table (see below).

Resynchronization (Resync) Mechanism

The Resync mechanism enables you to perform random requests to retrieve the Active alarms table when there are network problems (as described above) or a discontinuation of the alarm sequence is detected.

This feature implements an SNMP agent on the OVOC server with the MIB AudioCodes.acProducts.acEMS.acEMSConfiguration.acFaults with the following fields:

Table 5-11: Faults MIBs

Name	Type	OID
acFaultsFwdHostIp	IpAddress	1.3.6.1.4.1.5003.9.20.1.1.1
acFaultsFwdHostPort	Integer	1.3.6.1.4.1.5003.9.20.1.1.2
acFaultsFwdUpdate	Integer (0-1)	1.3.6.1.4.1.5003.9.20.1.1.3

NOTE

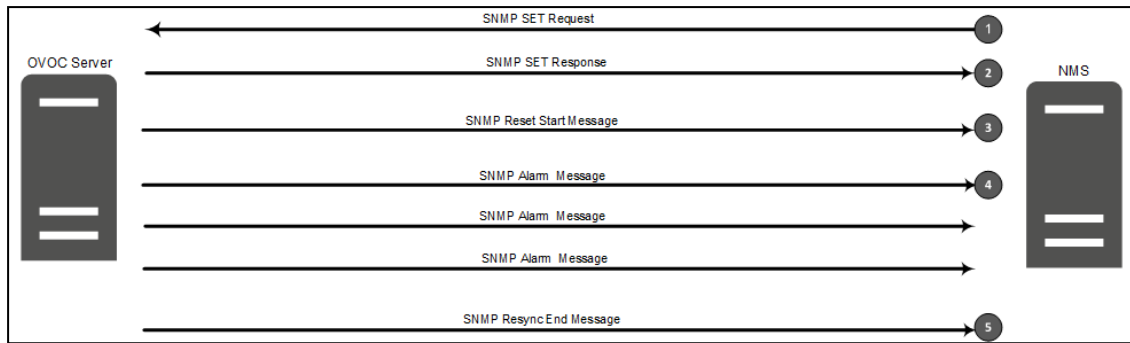
Each SNMP message should be processed in the order shown in the table above

When the acFaultsFwdUpdate field is set to 1, the SNMP agent reads the acFaultsFwdHostIp & acFaultsFwdHostPort fields and searches for all active SNMP Alarm Forwarding rules according to the configured 'Destination Host IP Address' and 'Destination Host Port'. It then resends all the current Active alarms according to SNMPv2/SNMPv3 account credentials and the other criteria defined in the rule. If a specific rule is not active (Enable/Disable check box is clear), then alarms are not sent to this destination.

NOTE

- The acFaultsFwdHostIp & acFaultsFwdHostPort parameters should be re-set each time after the Resync action is performed (they are set to default after each Resync action).
- The OVOC SNMP agent supports only SNMPv2 get/set commands. However, alarms can still be forwarded when configured with either SNMPv2 or SNMPv3 credentials in the alarm forwarding rule definition.
- The SNMP port used for this SNMP agent may be configured using the EMS Server Manager (Network Configuration > SNMP Agent > SNMP Agent Listener Port), instead of using the standard SNMP port number (161).
- When the SNMP agent is restarted, the acFaultsFwdHostIp & acFaultsFwdHostPort parameters need to be restart.
- The Resync feature is applicable only for alarms and is not relevant for events.

The figure below illustrates the Resync flow process:

Figure 5-7: Resync Flow

The following steps describe the flow illustrated in the figure above:

1. The NMS executes SNMP SET to acFaultsFwdHostIp & acFaultsFwdHostPort
2. The NMS executes SNMP SET to acFaultsFwdUpdate to 1 (acFaultsFwdHostIp & acFaultsFwdHostPort & acFaultsFwdUpdate are & set back to 0 automatically).
3. The OVOC server responds confirming successful SNMP SET.
4. The OVOC server finds all relevant Alarm Forwarding rules by acFaultsFwdHostIp & acFaultsFwdHostPort.
5. The OVOC server sends an event regarding the start of re-sending of all active alarms (acOvocReSyncEvent 1.3.6.1.4.1.5003.9.20.3.2.0.58) with Severity Indeterminate and 'TrapGlobalsUniqID' set to -1.
6. The OVOC server resends all active alarms according to the configured forwarding rules.
7. The OVOC server sends an event informing the end of resynchronization with Severity clear and 'TrapGlobalsUniqID' set to -1.

NOTE

- Alarms are not cleared from the Active alarms table when the OVOC server is restart.
- When a device is deleted or removed from the OVOC Web client, its active alarms are also removed from the Active Active alarms table.
- Alarms are forwarded in the sequence order that they were received on the OVOC server.
- SNMP traps are sent from source port 1164-1174 on the OVOC server.
- The Resync operation can be performed on up to three simultaneously active SNMP forwarding rules.
- The Resync operation can send up to 5000 of the last received alarms.
- New alarms raised during the Resync operation are also forwarded.
- There can be up to two concurrent Resync processes. If more than two processes are simultaneously active i.e. more than two users are concurrently attempting to perform this operation, then all the additional attempts (greater than two) fail and an error is sent to the log file (see below).
- Resync operation log failures are written to the log 'alarmsReSync.csv' (/var/log/ems).

OVOC Keep-alive

You can configure the OVOC to generate SNMP Keep-alive traps toward the SNMP destination. When the “OVOC Keep-Alive” check box is checked, this trap is sent from the OVOC to a configured destination according to a configured interval (default 60 seconds). You can send the Keep-alive trap to the desired SNMP destination, according to an existing configured forwarding destination rule.

➤ **To configure OVOC Keep-alive:**

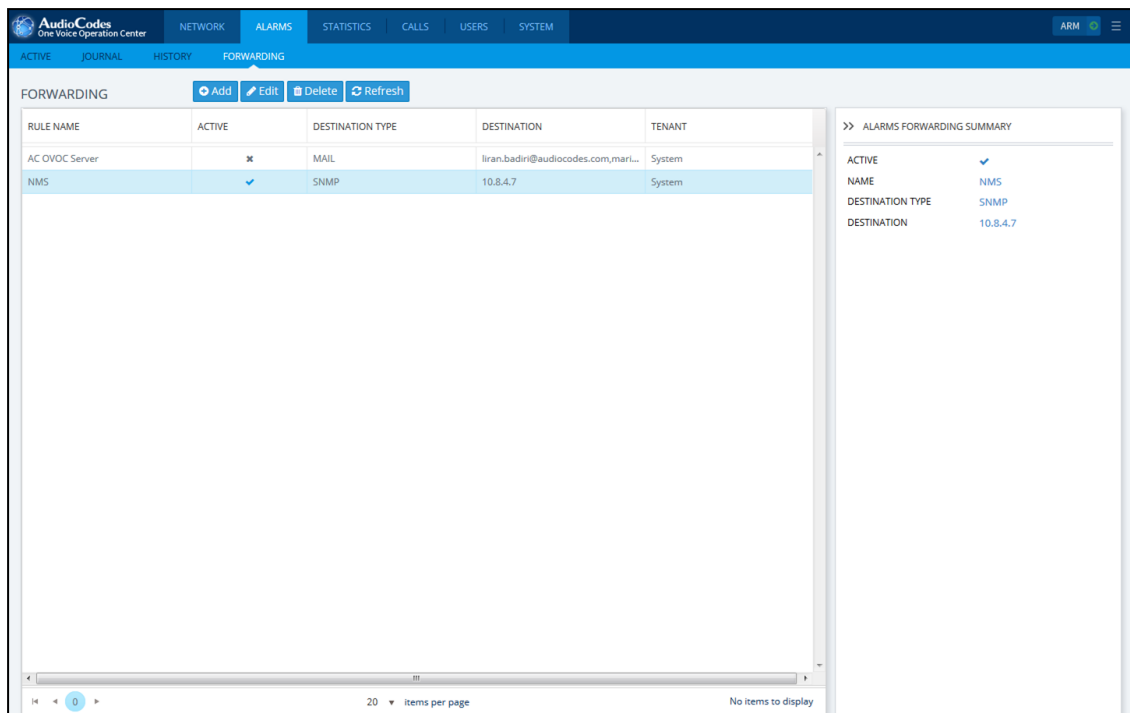
1. In the OVOC Web menu, open the Alarms page (System > Configuration > Alarms).

Figure 5-8: OVOC Keep-alive

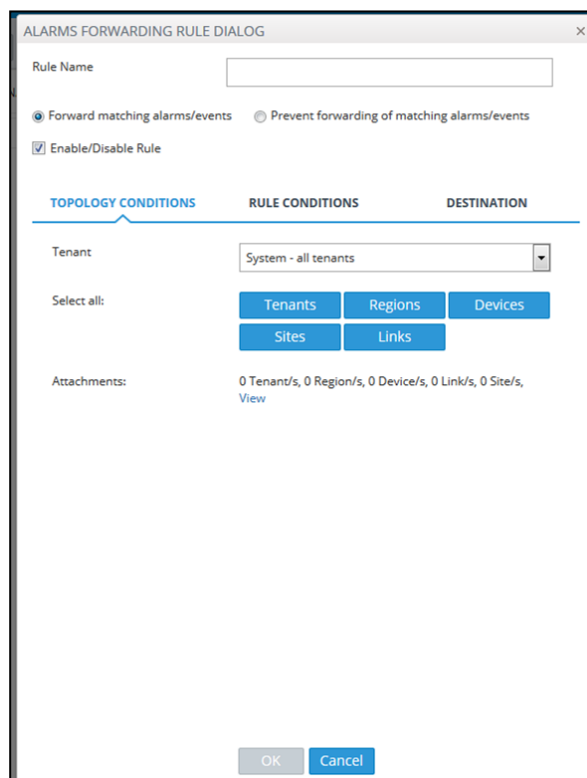
The screenshot displays the 'ALARMS' configuration page in the AudioCodes One Voice Operation Center. The left sidebar shows a navigation menu with 'ALARMS' selected. The main content area is divided into four sections: 'ALARMS AUTOMATIC CLEARING', 'ALARMS SUPPRESSION', 'EVENTS AUTOMATIC CLEARING', and 'OVOC KEEP-ALIVE'. In the 'OVOC KEEP-ALIVE' section, the 'OVOC Keep-Alive' checkbox is checked, and the 'OVOC Keep-Alive trap interval(seconds)' is set to 60. A 'Submit' button is located at the bottom right of the configuration area.

Section	Parameter	Value
ALARMS AUTOMATIC CLEARING	Alarms Automatic Clearing	☐
	Alarms Automatic Clearing Period (days)	30
ALARMS SUPPRESSION	Alarms Suppression	☒
	Alarms Suppression Counter Threshold	20
EVENTS AUTOMATIC CLEARING	Events Automatic Clearing	☒
	Events Automatic Clearing Period (days)	3
OVOC KEEP-ALIVE	OVOC Keep-Alive	☒
	OVOC Keep-Alive trap interval(seconds)	60

2. Select the OVOC Keep-Alive check box.
3. Open the Alarm Forwarding Rule page (Alarms > Forwarding); the Alarm Forwarding Rules Configuration window is displayed:

Figure 5-9: Alarm Forwarding Configuration

4. Select the SNMP forwarding rule and then click Edit.

Figure 5-10: Alarms Forwarding Rule Dialog

5. Ensure that the 'Enable/Disable Rule' check box is selected for each destination that you wish to forward the OVOC Keep-alive trap.

6. In the Alarm Names pane, click the Alarms Filter and ensure that the "OVOC Keep-Alive" alarm is selected.

Figure 5-11: Destination Rule Configuration

The screenshot shows the 'ALARMS FORWARDING RULE DIALOG' window. At the top, the 'Rule Name' is set to 'NMS'. Below this, there are two radio buttons: 'Forward matching alarms/events' (selected) and 'Prevent forwarding of matching alarms/events'. A checkbox labeled 'Enable/Disable Rule' is checked. The dialog is divided into three tabs: 'TOPOLOGY CONDITIONS', 'RULE CONDITIONS' (active), and 'DESTINATION'. Under 'RULE CONDITIONS', there are several fields: 'Alarm Origin' (All Selected), 'Event Origin' (All Selected), 'Severities' (All Selected), 'Filter Alarm names by category' (EMS Alarms), 'Alarm Names' (OVOC Keep-Alive), 'Alarm Types' (All Selected), and 'Source' (empty). At the bottom, there are 'OK' and 'Cancel' buttons.

TOPOLOGY CONDITIONS	RULE CONDITIONS	DESTINATION
Alarm Origin	All Selected	☐ none
Event Origin	All Selected	☐ none
Severities	All Selected	
Filter Alarm names by category	EMS Alarms	
Alarm Names	OVOC Keep-Alive	
Alarm Types	All Selected	
Source		

Status / State Management via Devices SNMP Interface

For details regarding supported SNMP MIBs, refer to the *SNMP Reference Guide for Gateways-SBCs-MSBRs*.

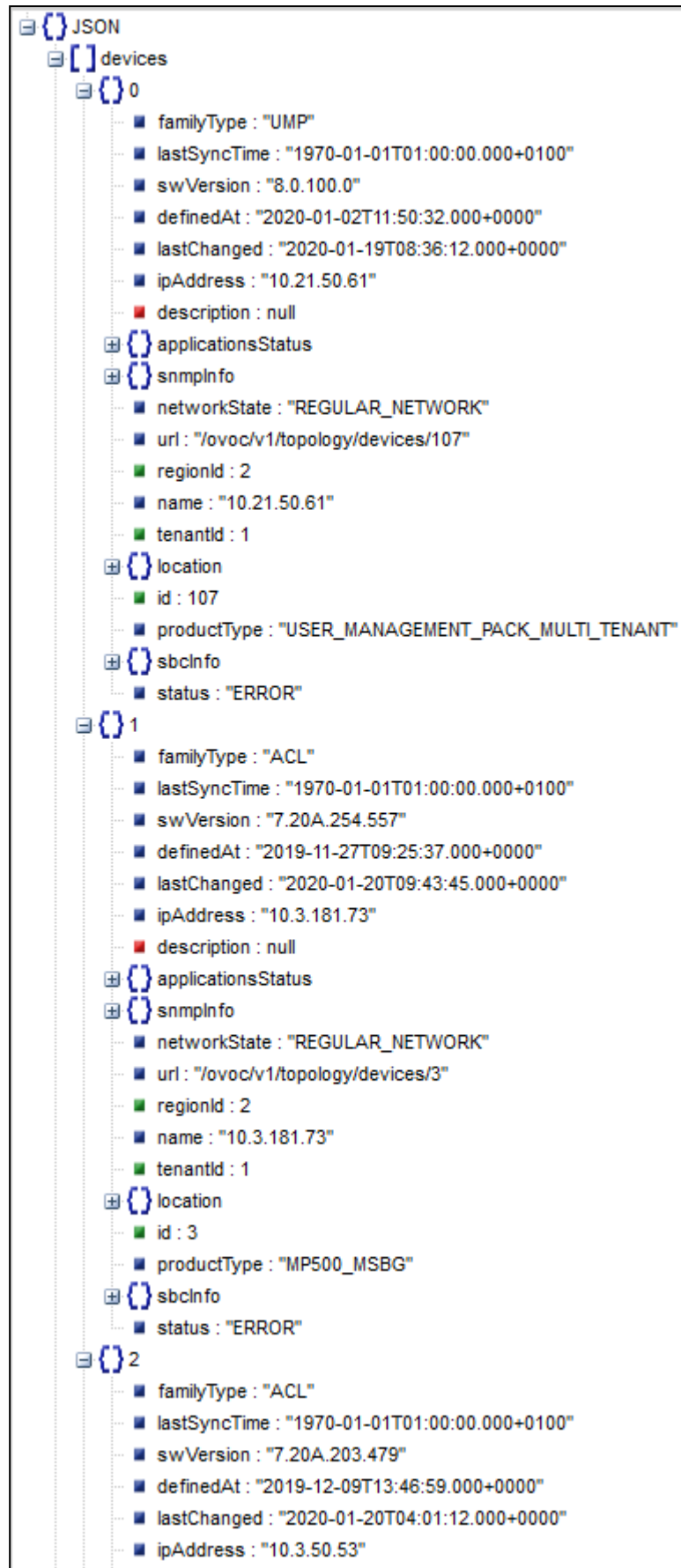
6 Voice Quality Reports

Both template and custom Voice Quality reports can be generated for devices, links and URIs for Tenants, Regions and Elements. You can export the report's definitions to JSON format from the Reports screen in the OVOC Web interface. The figure below shows an example of an exported JSON file.

NOTE

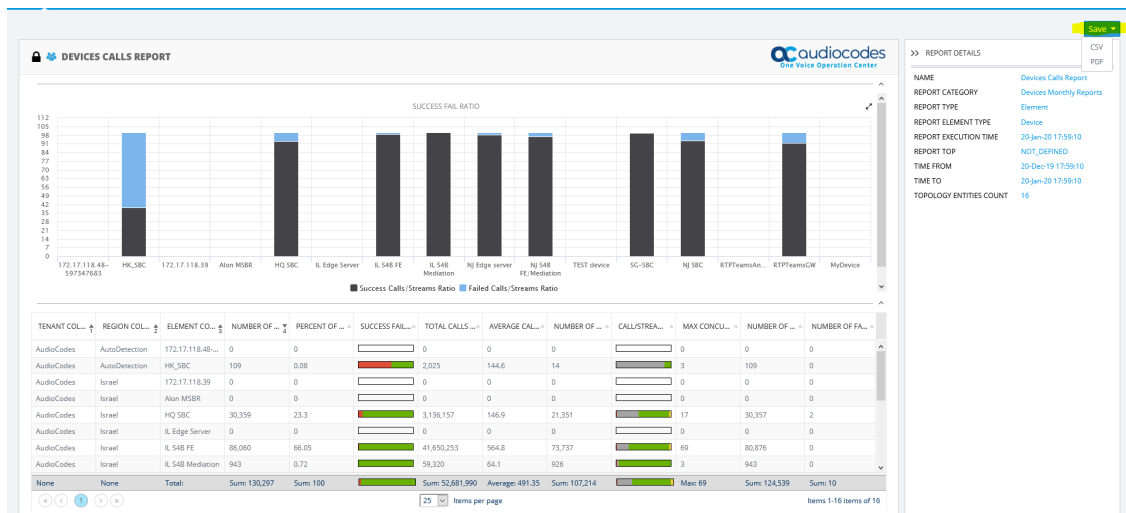
The generation of customized Voice Quality Reports requires a license. For more information, contact your AudioCodes representative.

Figure 6-1: Voice Quality Reports



You can also save the output of the run reports to a CSV or PDF file.

Figure 6-2: Run Report



7 OVOC Server Backup and Restore

The following backup processes are run on the OVOC server. All processes are run by default at 0200 (to change the scheduling, see [Change Schedule Backup Time](#)).

- **Cassandra backup:** Contains the backup of the Cassandra database. Backs up to the archive file `cassandraBackup_<version>_<date>_<snapshotId>_<Role>_numberOfNodes.tar`. When working in **Service Provider Cluster**, backup of the cluster node servers (VQM and PM) is performed on the Management server.
- **OVOC Server backup:** Contains the entire `/data/NBIF` directory's content, with the exception of the 'emsBackup' directory, OVOC Software Manager content and `server_XXX` directory content. Backs up to the archive file `emsServerBackup_<version>_<time&date>.tar`.
- **Configuration backup:** Contains the PostgreSQL database configuration-only backup. Backs up to the archive file `ovocConfigBackup_<version>_<time&date>.tar.gz`.
- **OVOC Full backup:** Contains the full backup of the PostgreSQL database. Backs up to the archive file `ovocFullBackup_<version>_<time&date>.tar.gz`.

NOTE

- The Backup process does not backup configurations performed using OVOC Server Manager, such as networking and security.
- It is highly recommended to maintain all backup files on an external machine. These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user.

Figure 7-1: Backup Log

```
[root@low-185 ~]# cd /data/NBIF/emsBackup
[root@low-185 emsBackup]# ll
total 935556
-rw-r--r-- 1 emsadmin nbif 1546240 Jun 20 04:01 cassandraBackup_8.4.20_2406200200_171884526
1564_MGMT_1.tar
-rw-r--r-- 1 emsadmin nbif 955596800 Jun 20 04:00 emsServerBackup_8.4.20_2406200200.tar
drwxrwxr-x 2 postgres dba 6 Jun 20 04:00 export
-rw-r--r-- 1 emsadmin nbif 313462 Jun 20 04:00 ovocConfigBackup_8.4.20_2406200200.tar.gz
-rw-r--r-- 1 emsadmin nbif 547455 Jun 20 04:00 ovocFullBackup_8.4.20_2406200200.tar.gz
[root@low-185 emsBackup]#
```

Backup OVOC Server

➤ to backup the OVOC server:

1. Copy the following backup files to an external machine:
 - `/data/NBIF/emsBackup/emsServerBackup_<version>_<time&date>.tar.gz`
 - `/data/NBIF/emsBackup/ovocFullBackup_<version>_<time&date>.tar.gz`
 - `/data/NBIF/emsBackup/ovocConfigBackup_<version>_<time&date>.tar.gz`
 - `/data/NBIF/emsBackup/cassandraBackup_<version>_<date>_<snapshotId>_<MGMT>_numberOfNodes.tar`

where:

- <time&date> is an example; replace this path with your filename.
 - <version> is the version number of the OVOC server release
2. In addition, when operating in **Service Provider Cluster**, copy Cassandra backup files to the /data/NBIF directory on the Cluster node of the respective server:
 - /data/NBIF/emsBackup/cassandraBackup__<version>_<date>_<snapshotId>_<VQM>_numberOfNodes.tar.gz
 - /data/NBIF/emsBackup/cassandraBackup__<version>_<date>_<snapshotId>_<PM>_numberOfNodes.tar.gz

Restore the OVOC Server

➤ To restore the OVOC server:

1. In the EMS Server Manager, choose the **Restore** option.
2. Install (or upgrade) OVOC to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.
3. Use the EMS Server Manager to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.
4. Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
5. Copy all the files you backed up to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
6. Choose one of the following options:
 - **Configuration Restore:** Restores OVOC topology and OVOC Web configuration
 - **Full Restore:** Restores OVOC topology, OVOC Web configuration and data that is retrieved from managed devices.

For more information, refer to "OVOC Server Restore" in the *OVOC IOM* manual.

NOTE

When operating in Service Provider Cluster:

- The restore cluster should be with identical system specifications as the backed up server i.e. the same number of VQM/PM servers.
- Following restore, restart slaves and then wait up to 24 hours for Cassandra DB data (call details and PM details) to synchronize on all servers.

8 analytics API

The analytics 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 (details of retrieved DB tables are shown below):

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

A dedicated DB operator("analytics") is used for securing connection to the OVOC server over port **5432**. This port must be open on the customer firewall once this feature is enabled (for more details, refer to the *OVOC IOM*).

NOTE

- Multitenancy is not supported for this feature.
- All data is read-only.
- Data is retrieved for the last 24 hours; it's recommended to synchronize daily with the OVOC database, save this data to an external server and then run the analytics tool on this server.
- Backup and restore is not applicable for this feature.
- The connector PostgreSQL driver must be used.

➤ To connect to the OVOC server:

1. Open your DB access client.
2. Configure the following parameters:
 - OVOC server IP address
 - OVOC server port: **5432**
 - Username: **analytics**
 - Service Name: **dbems**

An example database schema retrieved from an access client is displayed below:

Figure 8-1: Example Database schema

Name	Owner	T...
NODES_VIEW	ANALYTICS	View

NOCES_VIEW: Created: 18/04/2017 15:53:11 Last DDL: 18/04/2017 17:53:11 Status: Valid

Columns | Script | Data | Grants | Synonyms | Deps (Uses) | Deps (Used by) | Triggers | Constraints | Errors | Auditing

Columns: 10 | Script: 1 | Data: 1 | Grants: 1 | Synonyms: 1 | Deps (Uses): 1 | Deps (Used by): 1 | Triggers: 1 | Constraints: 1 | Errors: 1 | Auditing: 1

ID	NODE_ID	NODE_NAME	NODE_DESCRIPTION	FQDN	IP-ADDRESS	SW-VERSION	SERIAL_NUMBER	SECOND_SERIAL_NUMBER	DEFINED_AT	REGION_ID	REGION_NAME	TENANT_ID	TENANT_NAME	PRODUCT	TYPE	PRODUCED_AT
2125	169.254.0.73	10004			169.254.2.71	7.20A.204.360	10004	null	1201/01/08:44:08	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.73	10005			169.254.2.71	7.20A.204.360	10005	null	1201/01/08:44:08	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.73	10007			169.254.2.74	7.20A.204.360	10007	null	1201/01/08:44:10	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.77	10008			169.254.2.75	7.20A.204.360	10008	null	1201/01/08:44:36	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.75	10010			169.254.2.75	7.20A.204.360	10010	null	1201/01/08:44:36	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.157	10115			169.254.0.157	7.20A.204.360	10115		1201/01/08:47:45	1245	AusDetection	1201	Tenant1	80	Mednet	100
2126	169.254.0.157	10116			169.254.0.157	7.20A.204.360	10116		1201/01/08:47:45	1245	AusDetection	1201	Tenant1	80	Mednet	100
2000	172.17.118.36				172.17.118.36	7.20A.255.130	116631080		1201/01/08:31:55	1202	Regent	1201	Tenant1	60	Mednet	100
1897	169.254.0.157	10115			172.17.118.36	7.20A.255.130	8734999		1201/01/08:31:55	1202	Regent	1201	Tenant1	60	Mednet	100
2000	172.17.118.36				172.17.118.36	8.00A.250.005	8782393	null	30/01/2018:09:32:13	1202	Regent	1201	Tenant1	60	SW-SEC	100
2126	169.254.0.73	10004			169.254.0.40	7.20A.204.360	8781552		07/07/2018:09:00:05	1245	AusDetection	1245	Tenant1	168	Mednet	100
2140	169.254.0.84	10001			169.254.0.40	7.20A.204.360	10001	null	04/01/2018:15:25:20	1245	AusDetection	1201	Tenant1	60	Mednet	100
2140	169.254.0.110	10117			169.254.0.199	7.20A.204.360	10117		13/01/2018:18:47:45	1245	AusDetection	1201	Tenant1	60	Mednet	100
2147	169.254.0.200	10118			169.254.0.200	unknown-sw-version	10118		13/01/2018:18:47:45	1245	AusDetection	1201	Tenant1	0	UNKNOWN	100
2147	169.254.0.84	10102			169.254.0.84	7.20A.204.360	10102		13/01/2018:18:47:45	1245	AusDetection	1201	Tenant1	60	Mednet	100
2147	169.254.0.84	10102			169.254.0.84	7.20A.204.360	10102		13/01/2018:18:47:45	1245	AusDetection	1201	Tenant1	60	Mednet	100
2147	169.254.0.84	10102			169.254.0.84	7.20A.204.360	10102		13/01/2018:18:47:45	1245	AusDetection	1201	Tenant1	60	Mednet	100
2148	169.254.0.165	10163			169.254.0.165	7.20A.204.360	10163		1201/01/08:47:45	1245	AusDetection	1201	Tenant1	80	Mednet	100
2208	172.17.140.111				172.17.140.111	7.20A.256.719	8206995		17/05/2018:09:21:36	1202	Regent	1201	Tenant1	0	UNKNOWN	100
2209	9.9.9.9				9.9.9.9	10.0.0.0.108	105611078		04/05/2018:12:49:20	1202	Regent	1201	Tenant1	0	UNKNOWN	100

The following OVOC database tables are retrieved (for details, see [analytics_API_Database_Tables](#)):

■ **Main Table Views:**

- View Name: NODES_VIEW
- View Name: LINKS_VIEW
- View Name: CALLS_VIEW
- View Name: ALARMS_VIEW
- View Name: NODES_SUMMARY_VIEW
- View Name: LINKS_SUMMARY_VIEW

■ **Type Views:**

- Type Name: DisableEnableType
- Type Name: MGType
- Type Name: ItuPerceivedSeverity
- Type Name: ConnectionType
- Type Name: MismatchType
- Type Name: SemConnectionState
- Type Name: StatusType
- Type Name: VQThresholdStatus
- Type Name: SipMessageStatusType
- Type Name: NoYesType
- Type Name: NetworkState
- Type Name: ManagedType
- Type Name: FailSuccessType
- Type Name: BackupStatusType

- Type Name: ItuEntityAdministrativeState
- Type Name: AlarmStatusType
- Type Name: AlarmNameType
- Type Name: QualityLevelType
- Type Name: CallCauseType
- Type Name: CallOriginatorType
- Type Name: TerminationReasonType
- Type Name: TerminationReasonDetailsType
- Type Name: MediaType
- Type Name: EndpointType
- Type Name: CallSourceType
- Type Name: PstnTermReasonType
- Type Name: LinkType
- Type Name: LinkDirection

9 Security

The following aspects are relevant for the NMS application when integrating the OVOC and the managed device:

- Network Communication Protocols (see below)
- OVOC Users Management (Authentication and Authorization) (see [OVOC User Identity Management](#))
- HTTPS Connection (see [HTTPS Connection](#))

NOTE

For detailed information, refer to the *OVOC Security Guidelines* document.

Network Communication Protocols

The following describes the different OVOC network communication protocols:

- OVOC client - server communication is secured using an HTTPS tunnel with a single HTTPS port.
- OVOC server – managed devices communication can be secured as follows:
 - Devices:
 - ◆ SNMPv3 for Maintenance Actions and Faults Management
 - ◆ HTTPS for file transfer and for Single Sign-to the managed device
- OVOC server secure access:
 - Secure access to the OVOC server machine is possible via SSH and SFTP protocols for performing maintenance actions and accessing files.
 - SNMPv3 traps can be forwarded from the OVOC server machine to another SNMP Trap Manager.
 - OVOC User Authentication and Authorization is performed either via the OVOC Application local database, or via a centralized user database on RADIUS, LDAP or Microsoft Azure (see [OVOC User Identity Management](#)) according to the Security profile configured by the OVOC Administrator.

NOTE

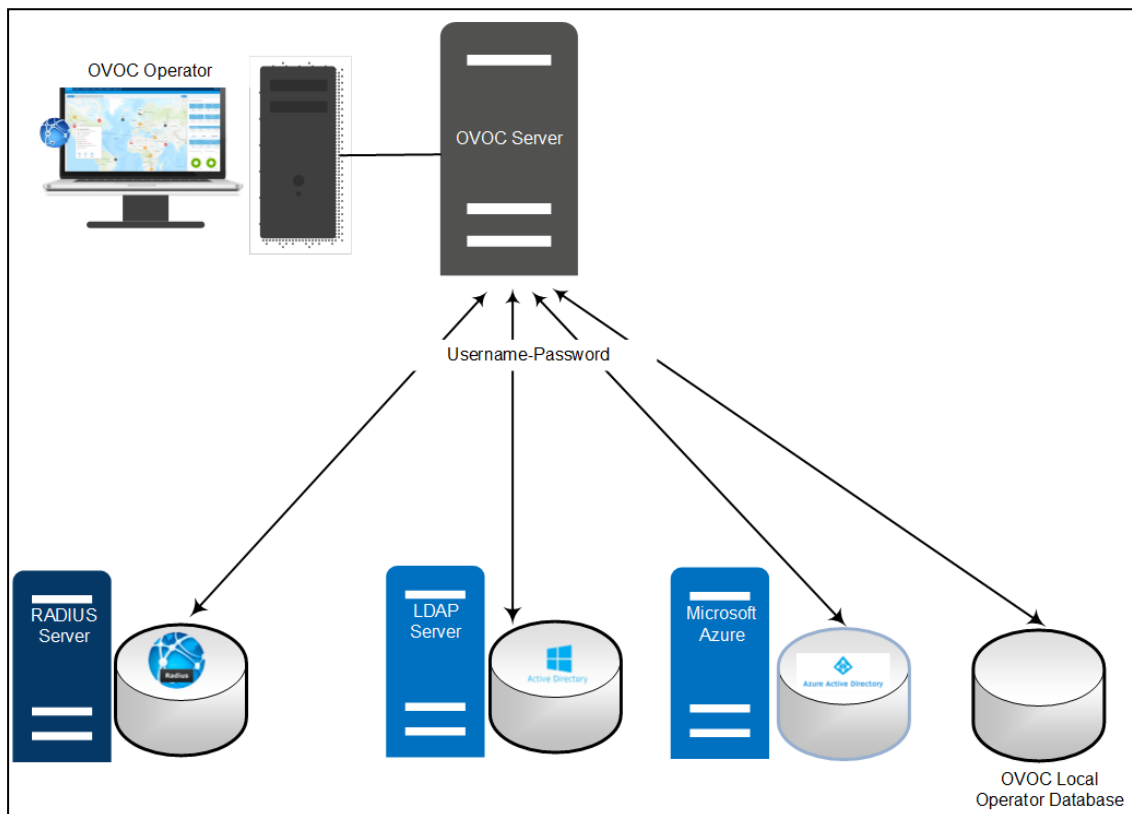
- Syslog messages and emails sent from the OVOC server to a northbound interface are not secured.
- Single sign-on is not supported for devices located behind a NAT, unless the Cloud Architecture feature is enabled, in which case, SBC device connections can be secured over an HTTP/S Tunnel Overlay network (refer to the IOM manual and the Security Guidelines for more information).

- An SSH connection from the OVOC server to the device is not supported.

OVOC User Identity Management

By default, OVOC users are managed in the OVOC server's local database. Users can also be managed via a centralized RADIUS or LDAP server or using Microsoft Azure. The figure below illustrates these options.

Figure 9-1: OVOC User Management



- For information on the local OVOC users database, refer to the *OVOC User's Manual*
- For OVOC user authentication with RADIUS server, see [Authentication and Authorization using a Radius Server](#)
- For OVOC user authentication with LDAP server, see [Authentication and Authorization using an LDAP Server](#)
- For OVOC user authentication with Microsoft Azure, see [Authentication and Authorization using Microsoft Azure](#)

Authentication and Authorization using a Radius Server

Customers may enhance the security and capabilities of logging into the OVOC application by using a Remote Authentication Dial-In User Service (RADIUS) to store numerous usernames, passwords and access level attributes. This feature allows multiple user management on a centralized platform. RADIUS (RFC 2865) is a standard authentication protocol that defines a

method for contacting a pre-defined server and verifying a given name and password pair against a remote database in a secure manner.

When accessing the OVOC application, users must provide a valid username and password of up to 128 Unicode characters. OVOC doesn't store the username and password; however, forwards them to the pre-configured RADIUS server for authentication (acceptance or rejection). If the login attempt to the RADIUS server fails, OVOC attempts to connect with the same credentials to the local database. An additional fallback mechanism 'Combined Authentication Mode' can also be implemented (for information, refer to the *OVOC User's Manual*)

OVOC supports the provisioning of up to three Radius servers for redundancy purposes. When the first server does not respond, the OVOC proceeds to the second server, and then to the third server. OVOC will always start working with the previously responded server that is indicated as the Current Active Radius servers.

Configuring Radius Server Client

This section describes an example of a RADIUS server configuration. You must configure the OVOC server as a RADIUS client to perform authentication and authorization of OVOC users using the RADIUS server from the OVOC application.

The example configuration is based on FreeRADIUS, which can be downloaded from the following location: www.freeradius.org. Follow the directions on this site for information on installing and configuring the server.

NOTE

If you use a RADIUS server from a different vendor, refer to the appropriate vendor documentation.

➤ To set up OVOC RADIUS client using FreeRADIUS:

1. Define the OVOC server as an authorized client of the RADIUS server with a predefined 'shared secret' (a password used to secure communication) and a 'vendor ID'. The figure below displays an example of the file 'clients.conf' (FreeRADIUS client configuration).

Example of the File clients.conf (FreeRADIUS Client Configuration)

```
#
# clients.conf - client configuration directives
#
client 10.31.4.47 {
    secret      = FutureRADIUS
    shortname   = OVOC
}
```

2. If access levels are required, set up a VSA dictionary for the RADIUS server and select an attribute ID that represents each user's access level. The following example shows a dictionary file for FreeRADIUS that defines the attribute 'ACL-Auth-Level' with ID=35.

Example of a Dictionary File for FreeRADIUS (FreeRADIUS Client Configuration)

```
#
# AudioCodes VSA dictionary
#
VENDOR AudioCodes 5003
ATTRIBUTE ACL-Auth-Level 35 integer AudioCodes
VALUE ACL-Auth-Level ACL-Auth-Monitor 50
VALUE ACL-Auth-Level ACL-Auth-Operator 100
VALUE ACL-Auth-Level ACL-Auth-Admin 200
```

3. In the RADIUS server, define the list of users who are authorized to use the device, using one of the password authentication methods supported by the OVOC server implementation. The following example shows a user configuration file for FreeRADIUS using a plain-text password.

Example of a User Configuration File for FreeRADIUS Using a Plain-Text Password

```
# users - local user configuration database
john  Auth-Type := Local, User-Password == "qwerty"
      Service-Type = Login-User,
      ACL-Auth-Level = ACL-Auth-Monitor
larry Auth-Type := Local, User-Password == "123456"
      Service-Type = Login-User,
      ACL-Auth-Level = ACL-Auth-Admin
```

4. Record and retain the IP address, port number, 'shared secret', vendor ID and VSA access level identifier (if access levels are used) used by the RADIUS server.
5. Provision the relevant OVOC parameters according to the section below.

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

➤ To configure using a RADIUS server.

1. In the OVOC Web, open the RADIUS Authentication Settings page (System tab > Security > Authentication), and then from the Authentication Type drop-down list, select **RADIUS**.

Figure 9-2: RADIUS Authentication and Authorization

The screenshot shows the 'AUTHENTICATION' configuration page for RADIUS. It includes sections for 'RADIUS AUTHENTICATION SETTINGS', 'COMBINED AUTHENTICATION MODE', 'RADIUS servers', and 'TEST CONNECTIVITY'.

RADIUS AUTHENTICATION SETTINGS:

- RADIUS retransmit timeout (msec): 3000
- RADIUS auth number of retries: 1
- Default Auth level: System Operator

COMBINED AUTHENTICATION MODE:

- ☒ Enable combined authentication
- Authentication order: External First

RADIUS servers:

	Server IP	Server Port	Change Server Secret
1st:	10.3.180.92	1812	
2nd:		1812	
3rd:		1812	

GW / SBC / MSRR AUTHENTICATION:

- ☐ Use RADIUS Credentials for Device Page Opening

TEST CONNECTIVITY:

- ☐ Test Connectivity with Username and Password
- User Name:
- Password:
-

- For each one of the three RADIUS servers, define the IP address, port and Secret. Note, that at least one RADIUS server must be provisioned.
- Define the following parameters:
 - RADIUS Auth Retransmit Timeout' (default-3000 milliseconds)
 - RADIUS Auth Number of Retries (default-1)

NOTE

These parameters will be used for each of the Radius Servers.

- Configure other parameters as required according to your RADIUS server configuration. For more information, refer to the *OVOC User's Manual*.

Authentication and Authorization 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 OVOC, they're assigned one of OVOC's security levels, e.g., 'Operator'. The equivalent names for these security levels on the LDAP server are displayed in the screen below. When one of these security levels is not defined on the LDAP server, OVOC by default allows access to the LDAP-authenticated operator with 'Operator' permissions.

➤ To configure using an LDAP server.

- In the OVOC Web, open the LDAP Authentication Settings page (System tab > Security > Authentication), and then from the Authentication Type drop-down list, select **LDAP**.

Figure 9-3: LDAP Authentication and Authorization

The screenshot shows the 'AUTHENTICATION' page with the 'LDAP' tab selected. The page is divided into several sections:

- LDAP AUTHENTICATION SETTINGS:**
 - Authentication Server FQDN / IP Address: 10.3.180.11
 - Authentication Server Port: 389
 - Connectivity DN: Admin2
 - Change Connectivity Password: (empty)
 - User DN Search Base: OU=TestEMS,OU=QA-DC-QA-EMS,DC=LOCAL
 - Filter: (empty)
 - Server Number of Retries: 4
 - ☐ Enable SSL
 - ☐ Verify Certificate Subject Name
 - Certificate File: (empty)
- AUTHORIZATION LEVEL SETTINGS:**
 - System Administrator User Group Name: EMS_Admin
 - System Operator User Group Name: EMS_Operator
 - System Monitor User Group Name: EMS_Monitor
 - Tenant Administrator User Group Name: EMS_Tenant_Admin
 - Tenant Operator User Group Name: EMS_Tenant_Operator
 - Tenant Monitor User Group Name: EMS_Tenant_Monitor
 - Tenant Monitor Links User Group Name: EMS_Tenant_Monitor_Links
 - Default Operator Type and Security Level: Reject
- COMBINED AUTHENTICATION MODE:**
 - ☒ Enable combined authentication
 - Authentication order: External First
- GW / SBC / MSBR AUTHENTICATION:**
 - ☐ Use AD Credentials for Device Page Opening

A 'Submit' button is located at the bottom right.

2. Configure parameters as required (refer to the *OVOC User's Manual*).

Authentication and Authorization using Microsoft Azure

Authentication of OVOC operators can be centrally configured using the Microsoft 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 OVOC's security levels, e.g., 'Operator'. The equivalent names for these security levels in the Azure AD are displayed in the screen below. When no security level is configured in the Azure AD, the parameter 'Default Operator Type and Security Level' in OVOC's Authentication page (when 'Authentication Type' is **AZURE**) is applied.

For configuration on Microsoft Azure, see [Configuring OVOC Web Azure Settings](#)

Figure 9-4: Azure Authentication

The screenshot shows the 'AUTHENTICATION' page with the 'AZURE' tab selected. The page is divided into several sections:

- AZURE AUTHENTICATION SETTINGS:**
 - Security Azure Hostname: login.microsoftonline.com
 - Azure AD Path Type File: Tenant
 - Azure Tenant ID: 9ebf097d-3f40-4e00-8629-7455f6c...
 - Azure Client ID: c6177c21-bd44-4282-8408-d355101
 - Change Azure Client Sec...: (empty)
- AUTHORIZATION LEVEL SETTINGS:**
 - System Administrator Us...: EMS_Admin
 - System Operator User Gr...: EMS_Operator
 - System Monitor User Gro...: EMS_Monitor
 - Tenant Administrator Us...: EMS_Tenant_Admin
 - Tenant Operator User Gr...: EMS_Tenant_Operator
 - Tenant Monitor User Gro...: EMS_Tenant_Monitor
 - Tenant Monitor Links User Group Name: EMS_Tenant_Monitor_Links
 - Default Operator Type and Security Level: System Operator
- COMBINED AUTHENTICATION MODE:**
 - ☒ Enable combined authentication
 - Authentication order: External First
- ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS:**
 - Tenant Endpoints Group User Group Name: EMS_Tenant_Endpoints_Group
- GW / SBC / MSBR AUTHENTICATION:**
 - ☐ Use AD Credentials for Device Page Opening

A 'Submit' button is located at the bottom right.

HTTPS Connection

The connection between the NBIF client and the OVOC server is by default secured over HTTPS (port 443). This security is managed by the EMS Server Manager option 'IP Phone Manager Pro and NBIF Web pages Secured Communication'. You can secure this connection either using AudioCodes default self-signed certificates or by applying custom certificates signed by an external CA. For more information, refer to the *OVOC Security Guidelines* document.

10 analytics API Database Tables

This chapter describes the database tables that are accessible using the analytics API:

■ [Main Table Views](#)

■ [Type Views](#)

Main Table Views

This section describes the Main Table Views that are accessible in the OVOC database by the analytics API.

Table 10-1: View Name: NODES_VIEW

Name	Null?	Supported Enumerator
NODE_ID	√	NUMBER(28)
NODE_NAME	√	NVARCHAR2(100)
NODE_DESCRIPTION	√	NVARCHAR2(255)
FQDN	√	NVARCHAR2(255)
IP_ADDRESS	√	VARCHAR2(20)
SW_VERSION	√	VARCHAR2(100)
SERIAL_NUMBER	√	VARCHAR2(255)
SECOND_SERIAL_NUMBER	√	VARCHAR2(255)
DEFINED_AT	√	DATE
REGION_ID	√	NUMBER(28)
REGION_NAME	√	NVARCHAR2(100)
TENANT_ID	√	NUMBER(28)
TENANT_NAME	√	VARCHAR2(100)
PRODUCT_TYPE	√	NUMBER(3)
PRODUCT_TYPE_NAME	√	VARCHAR2(100)
ADMIN_STATE	√	VARCHAR2(20)

Name	Null?	Supported Enumerator
ADMIN_STATE_VALUE	√	VARCHAR2(100)
MGMT_STATUS	√	NUMBER(3)
MGMT_STATUS_VALUE	√	VARCHAR2(100)
SEVERITY_STATE	√	VARCHAR2(20)
SEVERITY	√	VARCHAR2(100)
CONNECTION_STATE	√	NUMBER(3)
CONNECTION_STATE_VALUE	√	VARCHAR2(100)
CONNECTION_LOST_TIME	√	DATE
MISMATCH_STATE	√	NUMBER
MISMATCH_STATE_VALUE	√	VARCHAR2(100)
RESET_NEEDED	√	NUMBER
RESET_NEEDED_VALUE	√	VARCHAR2(100)
BURN_NEEDED	√	NUMBER
BURN_NEEDED_VALUE	√	VARCHAR2(100)
NETWORK_STATE	√	NUMBER
NETWORK_STATE_VALUE	√	VARCHAR2(100)
SBA_CONNECTION_STATE	√	NUMBER
SBA_CONNECTION_STATE_VALUE	√	VARCHAR2(100)
VQM_CONNECTION_STATE	√	NUMBER
VQM_CONNECTION_STATE_VALUE	√	VARCHAR2(100)
VQ_STATUS	√	NUMBER(3)
VQ_STATUS_VALUE	√	VARCHAR2(100)
VQ_CONTROL_STATUS	√	NUMBER(3)
VQ_CONTROL_STATUS_VALUE	√	VARCHAR2(100)

Name	Null?	Supported Enumerator
VQ_MEDIA_STATUS	√	NUMBER(3)
VQ_MEDIA_STATUS_VALUE	√	VARCHAR2(100)
SIP_MESSAGE_STATUS	√	NUMBER
SIP_MESSAGE_STATUS_VALUE	√	VARCHAR2(100)
CALLS_COUNT	√	NUMBER(10)
MANAGED_STATE	√	NUMBER
MANAGED_STATE_VALUE	√	VARCHAR2(100)
MANAGED_STATE_SEM	√	NUMBER
MANAGED_STATE_SEM_VALUE	√	VARCHAR2(100)
LICENSE_STATUS	√	NUMBER(3)
LICENSE_STATUS_VALUE	√	VARCHAR2(100)
LICENSE_POOL_STATUS	√	NUMBER
CLM_STATUS	√	NUMBER
SNMP_PORT	√	NUMBER
SNMP_VERSION	√	NUMBER
HTTPS_PROXY_ENABLED	√	NUMBER
HTTPS_ENABLED_VALUE	√	VARCHAR2(100)
LAST_BACKUP_STATUS	√	NUMBER
LAST_BACKUP_STATUS_VALUE	√	VARCHAR2(100)
LAST_PERFORMED_BACKUP_TIME	√	DATE
POLLING_ENABLED	√	NUMBER
POLLING_ENABLED_VALUE	√	VARCHAR2(100)
LAST_POLLING_STATUS	√	NUMBER
LAST_POLLING_STATUS_VALUE	√	VARCHAR2(100)

Name	Null?	Supported Enumerator
LAST_POLLING_FAIL_REASON	√	NUMBER
LAST_SUCCESFUL_POLLING	√	DATE
LAST_UNSUCCESFUL_POLLING	√	DATE
LAST_NUM_POLLING	√	NUMBER
NETWORK_X_LOCATION	√	FLOAT(126)
NETWORK_Y_LOCATION	√	FLOAT(126)
NETWORK_LATITUDE	√	VARCHAR2(25)
NETWORK_LONGITUDE	√	VARCHAR2(25)
REPORTED_NODE_ID	√	NUMBER
SQL_SERVRE_IP	√	NVARCHAR2(50)
SQL_SERVER_PORT	√	NUMBER
SQL_SERVER_INSTANCE_NAME	√	VARCHAR2(50)

Table 10-2: View Name: LINKS_VIEW

Name	Null?	Supported Enumerator
LINK_ID	NOT NULL	NUMBER(10)
LINK_NAME	√	VARCHAR2(50)
TENANT_ID	NOT NULL	NUMBER(28)
SRC_TENANT_NAME	√	VARCHAR2(100)
SECOND_TENANT_ID	NOT NULL	NUMBER(28)
DEST_TENANT_NAME	√	VARCHAR2(100)
REGION_ID	NOT NULL	NUMBER(28)
REGION_NAME	√	NVARCHAR2(100)
SRC_NODE_ID	NOT NULL	NUMBER(28)
SRC_NODE_NAME	√	NVARCHAR2(100)

Name	Null?	Supported Enumerator
SRC_N_NODE_NAME	√	NVARCHAR2(100)
DEST_NODE_ID	NOT NULL	NUMBER(28)
DEST_NODE_NAME	√	NVARCHAR2(100)
DEST_N_NODE_NAME	√	NVARCHAR2(100)
LINK_TYPE	√	NUMBER(3)
LINK_TYPE_VALUE	√	VARCHAR2(100)
TYPE_IP_GROUP	√	NUMBER(10)
TYPE_TRUNK_GROUP	√	NUMBER(10)
TYPE_IP_PREFIX	√	VARCHAR2(250)
TYPE_PHONE_PREFIX	√	VARCHAR2(250)
TYPE_MEDIA_REALM	√	NUMBER(10)
TYPE_MEDIA_IP_PREFIX	√	VARCHAR2(250)
TYPE_SRC_FQDN	√	NVARCHAR2(100)
TYPE_DEST_FQDN	√	NVARCHAR2(100)
SRC_PRODUCT_TYPE	√	NUMBER(3)
SRC_PRODUCT_TYPE_NAME	√	VARCHAR2(100)
DEST_PRODUCT_TYPE	√	NUMBER(3)
DEST_PRODUCT_TYPE_NAME	√	VARCHAR2(100)
LINK_DIRECTION	√	NUMBER(3)
LINK_DIRECTION_VALUE	√	VARCHAR2(100)
DEFINED_AT	√	NOT NULL
VQ_STATUS	√	NOT NULL
VQ_STATUS_VALUE	√	VARCHAR2(100)
VQ_CONTROL_STATUS	√	NUMBER(3)

Name	Null?	Supported Enumerator
VQ_CONTROL_STATUS_VALUE	√	VARCHAR2(100)
VQ_MEDIA_STATUS	√	NUMBER(3)
VQ_MEDIA_STATUS_VALUE	√	VARCHAR2(100)
VQ_CALL_DURATION_STATUS	√	NUMBER(3)
VQ_CALL_DURATION_STATUS_VALUE	√	VARCHAR2(100)
VQ_MAX_CONCURRENT_CALLS_STATUS	√	NUMBER(3)
VQ_MAX_CONC_CALLS_STATUS_V	√	VARCHAR2(100)
VQ_BANDWIDTH_STATUS	√	NUMBER(3)
VQ_BANDWIDTH_STATUS_VALUE	√	VARCHAR2(100)
CALLS_COUNT	√	NUMBER(10)

Table 10-3: View Name: CALLS_VIEW

Name	Null?	Supported Enumerator
CALL_INDEX	NOT NULL	NUMBER(28)
EMS_CALL_IDENTIFIER	NOT NULL	NUMBER(28)
NODE_ID	NOT NULL	NUMBER(28)
NODE_NAME	√	NVARCHAR2(100)
SESSION_ID	NOT NULL	NUMBER(28)
CALL_START_TIME	NOT NULL	DATE
CALL_END_TIME	NOT NULL	DATE
CALL_DURATION	√	NUMBER(10)
CALL_STATUS	√	NUMBER(3)
CALL_STATUS_VALUE	√	VARCHAR2(100)
VQ_COLOR	√	NUMBER(3)
VQ_COLOR_VALUE	√	VARCHAR2(100)

Name	Null?	Supported Enumerator
QUALITY_CAUSE	√	NUMBER(3)
QUALITY_CAUSE_VALUE	√	VARCHAR2(100)
RED_COLOR_PERCENT	√	NUMBER(10,2)
YELLOW_COLOR_PERCENT	√	NUMBER(10,2)
GREEN_COLOR_PERCENT	√	NUMBER(10,2)
TERMINATION_INITIATOR	√	NUMBER(3)
TERMINATION_INITIATOR_VALUE	√	VARCHAR2(100)
TERMINATION_REASON_CATEGORY	√	NUMBER(3)
TERM_REASON_CATEGORY_VALUE	√	VARCHAR2(100)
TERMINATION_REASON_DETAILS	√	VARCHAR2(100)
TERM_REASON_DETAILS_VALUE	√	VARCHAR2(100)
SIP_TERMINATION_REASON	√	VARCHAR2(50)
SIP_TERMINATION_DESC	√	VARCHAR2(100)
PSTN_TERMINATION_REASON	√	NUMBER(4)
PSTN_TERM_REASON_VALUE	√	VARCHAR2(100)
MEDIA_TYPE	√	NUMBER(3)
MEDIA_TYPE_VALUE	√	VARCHAR2(100)
ENDPOINT_TYPE	√	NUMBER(10)
ENDPOINT_TYPE_VALUE	√	VARCHAR2(100)
CALLER_URI	√	VARCHAR2(160)
CALLEE_URI	√	VARCHAR2(160)
ORIGINAL_CALLEE_URI	√	VARCHAR2(160)
NO_EVENT_FLAG	√	NUMBER(3)
CALL_NODES	√	VARCHAR2(300)

Name	Null?	Supported Enumerator
CALL_LINKS	√	VARCHAR2(300)
CALL_SOURCE_TYPE	√	NOT NULL
CALL_SOURCE_TYPE_VALUE	√	VARCHAR2(100)
MOS	√	NUMBER(10,2)
JITTER	√	NUMBER(10,2)
PLOSS	√	NUMBER(10,2)
DELAY	√	NUMBER(10,2)
RERL	√	NUMBER(10,2)

Table 10-4: View Name: ALARMS_VIEW

Name	Null?	Supported Enumerator
ALARM_ID	√	NUMBER(28)
IS_EVENT	√	NUMBER(8)
ALARM_REMOTE_HOST	√	NVARCHAR2(100)
ALARM_UNIQUE_ID	√	NVARCHAR2(100)
ALARM_NAME	√	VARCHAR2(100)
ALARM_DESCRIPTION	√	NVARCHAR2(255)
ALARM_SEVERITY	√	NUMBER(3)
ALARM_SEVERITY_VALU	√	VARCHAR2(100)
ALARM_SOURCE	√	NVARCHAR2(255)
ALARM_ADDITIONAL_INFO1	√	NVARCHAR2(255)
ALARM_ADDITIONAL_INFO2	√	NVARCHAR2(255)
ALARM_ADDITIONAL_INFO3	√	NVARCHAR2(255)
ALARM_REMOTE_PORT	√	NUMBER(8)
ALARM_SYSTEM_UP_TIME	√	NVARCHAR2(100)

Name	Null?	Supported Enumerator
ALARM_SNMP_VERSION	√	NUMBER(3)
ALARM_OID	√	VARCHAR2(100)
ALARM_STATUS	√	NUMBER(3)
ALARM_STATUS_VALUE	√	VARCHAR2(100)
LAST_ACTION_TIME	√	DATE
LAST_ACTION_OPERATOR	√	NVARCHAR2(100)
ALARM_RECIEVED_TIME	√	DATE
ALARM_UNIT_NAME	√	NVARCHAR2(100)
ALARM_REGION_ID	√	NUMBER(28)
ALARM_REGION_NAME	√	NVARCHAR2(100)
ALARM_UNIT_ID	√	NUMBER(28)
TENANT_ID	√	NUMBER(28)
TENANT_NAME	√	VARCHAR2(100)
ALARM_SOURCE_NAME	√	NVARCHAR2(255)
ALARM_DATE_TIME	√	NVARCHAR2(255)

Table 10-5: View Name: NODES_SUMMARY_VIEW

Name	Null?	Supported Enumerator
DEVICE_NAME	√	NVARCHAR2(100)
NODE_ID	NOT NULL	NUMBER(28)
TIME_STAMP	NOT NULL	DATE
NODE_NAME	√	VARCHAR2(100)
REGION_ID	√	NUMBER(28)
CALLS_COUNT	√	NUMBER(10)
CALLS_DURATION_TOTAL	√	NUMBER(10)

Name	Null?	Supported Enumerator
CALLS_DURATION_COUNT	√	NUMBER(10)
SUCCESS_CALLS	√	NUMBER(10)
FAILED_CALLS	√	NUMBER(10)
RED_CALLS	√	NUMBER(10)
YELLOW_CALLS	√	NUMBER(10)
GREEN_CALLS	√	NUMBER(10)
GRAY_CALLS	√	NUMBER(10)
MOS_CAUSE	√	NUMBER(10)
JITTER_CAUSE	√	NUMBER(10)
PLOSS_CAUSE	√	NUMBER(10)
DELAY_CAUSE	√	NUMBER(10)
RERL_CAUSE	√	NUMBER(10)
MOS_MIN	√	NUMBER(10,2)
JITTER_MIN	√	NUMBER(10)
PLOSS_MIN	√	NUMBER(10)
DELAY_MIN	√	NUMBER(10)
RERL_MIN	√	NUMBER(10)
MOS_MAX	√	NUMBER(10,2)
JITTER_MAX	√	NUMBER(10)
PLOSS_MAX	√	NUMBER(10)
DELAY_MAX	√	NUMBER(10)
RERL_MAX	√	NUMBER(10)
MOS_TOTAL	√	NUMBER(10,2)
JITTER_TOTAL	√	NUMBER(10,2)

Name	Null?	Supported Enumerator
PLOSS_TOTAL	√	NUMBER(10,2)
DELAY_TOTAL	√	NUMBER(10,2)
RERL_TOTAL	√	NUMBER(10,2)
MOS_COUNT	√	NUMBER(10)
JITTER_COUNT	√	NUMBER(10)
PLOSS_COUNT	√	NUMBER(10)
DELAY_COUNT	√	NUMBER(10)
RERL_COUNT	√	NUMBER(10)
SNR_MIN	√	NUMBER(10)
SNR_MAX	√	NUMBER(10)
SNR_TOTAL	√	NUMBER(10,2)
SNR_COUNT	√	NUMBER(10)
RX_KB_TOTAL	√	NUMBER(28)
TX_KB_TOTAL	√	NUMBER(28)
VOICE_CALLS_COUNT	√	NUMBER(10)
FAX_CALLS_COUNT	√	NUMBER(10)
MOS_RED_CALLS	√	NUMBER(10)
MOS_YELLOW_CALLS	√	NUMBER(10)
MOS_GREEN_CALLS	√	NUMBER(10)
MOS_GRAY_CALLS	√	NUMBER(10)
JITTER_RED_CALLS	√	NUMBER(10)
JITTER_YELLOW_CALLS	√	NUMBER(10)
JITTER_GREEN_CALLS	√	NUMBER(10)
JITTER_GRAY_CALLS	√	NUMBER(10)

Name	Null?	Supported Enumerator
PLOSS_RED_CALLS	√	NUMBER(10)
PLOSS_YELLOW_CALLS	√	NUMBER(10)
PLOSS_GREEN_CALLS	√	NUMBER(10)
PLOSS_GRAY_CALLS	√	NUMBER(10)
DELAY_RED_CALLS	√	NUMBER(10)
DELAY_YELLOW_CALLS	√	NUMBER(10)
DELAY_GREEN_CALLS	√	NUMBER(10)
DELAY_GRAY_CALLS	√	NUMBER(10)
RERL_RED_CALLS	√	NUMBER(10)
RERL_YELLOW_CALLS	√	NUMBER(10)
RERL_GREEN_CALLS	√	NUMBER(10)
RERL_GRAY_CALLS	√	NUMBER(10)
MAX_CONCURRENT_CALLS	√	NUMBER(10)
INCOMING_CALLS	√	NUMBER(10)
OUTGOING_CALLS	√	NUMBER(10)

Table 10-6: View Name: LINKS_SUMMARY_VIEW

Name	Null?	Supported Enumerator
REAL_LINK_NAME	x	VARCHAR2(50)
LINK_ID	NOT NULL	NUMBER(28)
TIME_STAMP	NOT NULL	DATE
LINK_NAME	x	VARCHAR2(50)
REGION_ID	x	NUMBER(28)
CALLS_COUNT	x	NUMBER(10)
CALLS_DURATION_TOTAL	x	NUMBER(10)

Name	Null?	Supported Enumerator
CALLS_DURATION_COUNT	x	NUMBER(10)
SUCCESS_CALLS	x	NUMBER(10)
FAILED_CALLS	x	NUMBER(10)
RED_CALLS	x	NUMBER(10)
YELLOW_CALLS	x	NUMBER(10)
GREEN_CALLS	x	NUMBER(10)
GRAY_CALLS	x	NUMBER(10)
MOS_CAUSE	x	NUMBER(10)
JITTER_CAUSE	x	NUMBER(10)
PLOSS_CAUSE	x	NUMBER(10)
DELAY_CAUSE	x	NUMBER(10)
RERL_CAUSE	x	NUMBER(10)
MOS_MIN	x	NUMBER(10,2)
JITTER_MIN	x	NUMBER(10)
PLOSS_MIN	x	NUMBER(10)
DELAY_MIN	x	NUMBER(10)
RERL_MIN	x	NUMBER(10)
MOS_MAX	x	NUMBER(10,2)
JITTER_MAX	x	NUMBER(10)
PLOSS_MAX	x	NUMBER(10)
DELAY_MAX	x	NUMBER(10)
RERL_MAX	x	NUMBER(10)
MOS_TOTAL	x	NUMBER(10,2)
JITTER_TOTAL	x	NUMBER(10,2)

Name	Null?	Supported Enumerator
PLOSS_TOTAL	x	NUMBER(10,2)
DELAY_TOTAL	x	NUMBER(10,2)
RERL_TOTAL	x	NUMBER(10,2)
MOS_COUNT	x	NUMBER(10)
JITTER_COUNT	x	NUMBER(10)
PLOSS_COUNT	x	NUMBER(10)
DELAY_COUNT	x	NUMBER(10)
RERL_COUNT	x	NUMBER(10)
SNR_MIN	x	NUMBER(10)
SNR_MAX	x	NUMBER(10)
SNR_TOTAL	x	NUMBER(10,2)
SNR_COUNT	x	NUMBER(10)
RX_KB_TOTAL	x	NUMBER(28)
TX_KB_TOTAL	x	NUMBER(28)
VOICE_CALLS_COUNT	x	NUMBER(10)
FAX_CALLS_COUNT	x	NUMBER(10)
MOS_RED_CALLS	x	NUMBER(10)
MOS_YELLOW_CALLS	x	NUMBER(10)
MOS_GREEN_CALLS	x	NUMBER(10)
MOS_GRAY_CALLS	x	NUMBER(10)
JITTER_RED_CALLS	x	NUMBER(10)
JITTER_YELLOW_CALLS	x	NUMBER(10)
JITTER_GREEN_CALLS	x	NUMBER(10)
JITTER_GRAY_CALLS	x	NUMBER(10)

Name	Null?	Supported Enumerator
PLOSS_RED_CALLS	x	NUMBER(10)
PLOSS_YELLOW_CALLS	x	NUMBER(10)
PLOSS_GREEN_CALLS	x	NUMBER(10)
PLOSS_GRAY_CALLS	x	NUMBER(10)
DELAY_RED_CALLS	x	NUMBER(10)
DELAY_YELLOW_CALLS	x	NUMBER(10)
DELAY_GREEN_CALLS	x	NUMBER(10)
DELAY_GRAY_CALLS	x	NUMBER(10)
RERL_RED_CALLS	x	NUMBER(10)
RERL_YELLOW_CALLS	x	NUMBER(10)
RERL_GREEN_CALLS	x	NUMBER(10)
RERL_GRAY_CALLS	x	NUMBER(10)
MAX_CONCURRENT_CALLS	x	NUMBER(10)
INCOMING_CALLS	x	NUMBER(10)
OUTGOING_CALLS	x	NUMBER(10)

Type Views

This appendix describes the Type Views that are accessible in the OVOC database by the analytics API.

Table 10-7: Type Name: DisableEnableType

Type Values
(0) Disable
(1) Enable

NOTE

The table below is divided into two columns for readability. In the database, there is a single column for “MGType” e.g. (0) UNKNOWN.

Table 10-8: Type Name: MGType

Type Values	MGType
(0)	UNKNOWN
(1)	Mediant 8000
(2)	STRETTO 8000
(3)	Mediant 5000
(4)	STRETTO 5000
(5)	Mediant 2000
(6)	STRETTO 2000
(7)	MP102
(8)	MP104 FXS
(9)	MP104 FXO
(10)	MP108 FXS
(11)	MP108 FXO
(12)	MP124
(13)	IPAT 8000
(14)	IPAT 5000
(15)	IPAT 2000
(16)	CA IPAT 8000
(17)	CA IPAT 5000
(18)	CA IPAT 2000
(20)	UNKNOWN MP102
(21)	UNKNOWN MP104 FXS

Type Values	MGType
(22)	UNKNOWN MP104 FXO
(23)	UNKNOWN MP108 FXS
(24)	UNKNOWN MP108 FXO
(25)	UNKNOWN MP124
(26)	UNKNOWN Mediant 2000
(27)	UNKNOWN STRETTO 2000
(28)	UNKNOWN Mediant 8000
(29)	UNKNOWN STRETTO 8000
(30)	UNKNOWN Mediant 5000
(31)	UNKNOWN STRETTO 5000
(32)	UNKNOWN IPAT 8000
(33)	UNKNOWN IPAT 5000
(34)	UNKNOWN IPAT 2000
(35)	UNKNOWN CA IPAT 8000
(36)	UNKNOWN CA IPAT 5000
(37)	UNKNOWN CA IPAT 2000
(38)	IPMedia 2000
(39)	UNKNOWN IPMEDIA 2000
(40)	IPMedia 5000
(41)	UNKNOWN IPMEDIA 5000
(42)	IPMedia 8000
(43)	UNKNOWN IPMEDIA 8000
(44)	Mediant 1000
(45)	UNKNOWN Mediant 1000

Type Values	MGType
(46)	Mediant 3000
(47)	UNKNOWN Mediant 3000
(9)	UNKNOWN MP118FXS
(50)	MP114 FXS
(51)	UNKNOWN MP114FXS
(52)	MP112
(53)	UNKNOWN MP112
(54)	MP118 FXO
(55)	UNKNOWN MP118FXO
(56)	MP114 FXO
(57)	UNKNOWN MP114FXO
(58)	IPMedia 3000
(59)	UNKNOWN IPMEDIA 3000
(60)	MP118 FXSFXO
(61)	UNKNOWN MP118 FXS/FXO
(62)	MP114 FXSFXO
(63)	UNKNOWN MP114 FXS/FXO
(64)	Mediant 260
(65)	UNKNOWN Mediant 260
(66)	IPMedia 260
(67)	UNKNOWN IPMEDIA 260
(68)	Mediant 3000 8410
(69)	UNKNOWN Mediant 3000 8410
(70)	IPMedia 3000 8410

Type Values	MGType
(71)	UNKNOWN IPMedia 3000 8410 8410
(72)	Mediant 3000 8410 V5.2
(73)	UNKNOWN Mediant 3000 8410 V5.2
(74)	IPMedia 3000 8410 VIDEO
(75)	UNKNOWN IPMedia 3000 8410 8410 VIDEO
(76)	Mediant 600
(77)	UNKNOWN Mediant 600
(78)	Mediant 800 MSBR
(79)	UNKNOWN Mediant 800 MSBR
(80)	Mediant 1000 MSBR
(81)	UNKNOWN Mediant 1000 MSBR
(82)	Mediant 800 E-SBC
(83)	UNKNOWN Mediant 800 E-SBC
(84)	Mediant 1000 E-SBC
(85)	UNKNOWN Mediant 1000 E-SBC
(86)	Mediant 4000 E-SBC
(87)	UNKNOWN Mediant 4000 E-SBC
(88)	SW SBC
(89)	UNKNOWN S
(90)	Mediant 500 MSBR
(91)	UNKNOWN Mediant 500 MSBR
(92)	Mediant 500 E-SBC
(93)	UNKNOWN Mediant 500 E-SBC
(94)	Mediant 850 MSBR

Type Values	MGType
(95)	UNKNOWN Mediant 850 MSBR
(96)	Mediant 850 E-SBC
(97)	UNKNOWN Mediant 850 E-SBC
(98)	Mediant 2600 E-SBC
(99)	UNKNOWN Mediant 2600 E-SBC
(100)	Mediant 500L MSBR
(101)	UNKNOWN Mediant 500L MSBR
(102)	Mediant 500L E-SBC
(103)	UNKNOWN Mediant 500L E-SBC
(104)	Mediant 800B MSBR
(105)	UNKNOWN Mediant 800B MSBR
(106)	Mediant 800B E-SBC
(107)	UNKNOWN Mediant 800B E-SBC
(108)	SW SE SBC
(109)	UNKNOWN SW SE SBC
(110)	SW SE-H SBC
(111)	UNKNOWN SW SE-H SBC
(112)	SW VE SBC
(113)	UNKNOWN SW VE SBC
(114)	SW VE-H SBC
(115)	UNKNOWN SW VE-H SBC
(116)	Mediant 9000 SBC
(117)	UNKNOWN Mediant 9000 SBC
(118)	SW SBC CM

Type Values	MGType
(119)	UNKNOWN SW SBC CM
(120)	Mediant 4000B E-SBC
(121)	UNKNOWN Mediant 4000B E-SBC
(122)	Mediant 9000 SBC CM
(123)	UNKNOWN Mediant 9000 SBC CM
(124)	SW VE SBC CM
(125)	UNKNOWN SW VE SBC CM
(126)	MP1288
(127)	UNKNOWN MP1288
(128)	SW SE SBC CM
(129)	UNKNOWN SW SE SBC CM
(19)	MP124-E
(130)	UNKNOWN MP124E
(131)	Mediant 2600B E-SBC
(132)	UNKNOWN Mediant 2600B E-SBC
(133)	Mediant 500LI MSBR
(134)	UNKNOWN Mediant 500LI MSBR
(200)	Generic Device
(250)	CloudBond 365 Standard Edition
(251)	UNKNOWN CloudBond 365 Standard Edition
(252)	CloudBond 365 Standard Plus Edition
(253)	UNKNOWN CloudBond 365 Standard Plus Edition
(254)	CloudBond 365 Pro Edition
(255)	UNKNOWN CloudBond 365 Pro Edition

Type Values	MGType
(256)	CloudBond 365 Enterprise Edition
(257)	UNKNOWN CloudBond 365 Enterprise Edition
(258)	CloudBond 365 Virtualized Edition
(259)	UNKNOWN CloudBond 365 Virtualized Edition
(260)	User Management Pack
(261)	UNKNOWN User Management Pack
(262)	Mediant 800 CCE Appliance
(263)	UNKNOWN Mediant 800 CCE Appliance
(264)	Mediant Server CCE Appliance
(265)	UNKNOWN Mediant Server CCE Appliance
(266)	SmartTap
(267)	null
(268)	User Management Pack Multi-Tenant
(269)	UNKNOWN User Management Pack Multi-Tenant
(299)	SBA
(300)	Skype Front End Server
(301)	Skype Mediation Server
(302)	Skype Edge Server
(303)	Skype SBA
(304)	MP202 B
(305)	UNKNOWN MP202 B
(306)	MP204 B
(307)	UNKNOWN MP204 B
(308)	MP202

Type Values	MGType
(309)	UNKNOWN MP202
(310)	MP204
(311)	UNKNOWN MP204
(326)	MP202 R
(327)	UNKNOWN MP202 R
(328)	MP204 R
(329)	UNKNOWN MP204 R
(312)	SW SE SBC SC
(313)	UNKNOWN SW SE SBC SC
(314)	SW SE-H SBC SC
(315)	UNKNOWN SW SE-H SBC SC
(316)	SW VE SBC SC
(317)	UNKNOWN SW VE SBC SC
(318)	SW VE-H SBC SC
(319)	UNKNOWN SW VE-H SBC SC
(320)	SW ESBC SC
(321)	UNKNOWN SW ESBC SC
(322)	Mediant 800C MSBR
(323)	UNKNOWN Mediant 800C MSBR
(324)	Mediant 800C E-SBC
(325)	UNKNOWN Mediant 800C E-SBC

Table 10-9: Type Name: ItuPerceivedSeverity

Values
(0) cleared

Values
(1) indeterminate
(2) warning
(3) minor
(4) major
(5) critical

Table 10-10:Type Name: ConnectionType

Type Values
(0) Not Connected
(1) Connected

Table 10-11:Type Name: MismatchType

Type Values
(0) No Mismatch
(1) Hardware Mismatch
(2) Sw Version Unsupported
(3) Configuration Mismatch
(4) Predefine Mismatch
(5) Predefine Mismatch with upload configuration
(6) Predefine Mismatch with Download configuration

Table 10-12:Type Name: SemConnectionState

Type Values
(0) Not defined
(1) Not defined not connected
(2) Not connected
(3) connected

Type Values
(4) Not connected no resources

Table 10-13:Type Name: StatusType

Type Values
(0) ERROR
(1) WARNING
(2) OK
(3) UNMONITORED

Table 10-14:Type Name: VQThresholdStatus

Type Values
(0) CRITICAL
(1) MAJOR
(2) CLEAR
(3) UNMONITORED

Table 10-15:Type Name: SipMessageStatusType

Type Values
(0) UNDEFINED
(1) SBC_IND_START_SENDING_SIPM
(2) SBC_IND_STOP_SENDING_SIPM

Table 10-16:Type Name: NoYesType

Type Values
(0) No
(1) Yes

Table 10-17:Type Name: NetworkState

Type Values
(0) Regular
(1) NAT

Table 10-18:Type Name: ManagedType

Type Values
(0) Not Defined
(1) Managed
(2) Unmanaged

Table 10-19:Type Name: FailSuccessType

Type Values
(0) Fail
(1) Success

Table 10-20:Type Name: BackupStatusType

Type Values
(0) No backup info
(1) File uploaded
(2) File not changed
(3) MG not connected
(4) Upload error
(5) Not enough disk space
(6) Backup error

Table 10-21:Type Name: ItuEntityAdministrativeState

Type Values
(0) Locked

Type Values
(1) ShuttingDown
(2) Unlocked

Table 10-22:Type Name: AlarmStatusType

Type Values
(0) New
(1) Acknowledged
(2) Cleared
(3) Automatically Cleared
(4) Coldstart Cleared

NOTE

The table below is divided into two columns for readability. In the database, there is a single column for “Type Values” e.g. (.1.3.6.1.4.1.5003.9.10.1.21.2.0.41) acSonetLineRDIArm.

Table 10-23:Type Name: AlarmNameType

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.41)	acSonetLineRDIArm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.40)	acSonetLineAISAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.43)	acHwFailureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.42)	acSonetIfHwFailureAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.70)	IPPhoneRequiresReset
(.1.3.6.1.4.1.5003.9.30.2.2.0.5)	acSbaCertificateExpiredAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.72)	acAlarmsFwOverflow
(.1.3.6.1.4.1.5003.9.30.2.2.0.4)	acSBADiskSpaceAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.71)	acAlarmsOverflow
(.1.3.6.1.4.1.5003.9.20.3.2.0.74)	acPmTimeOutEvent

OID	Type Values
(.1.3.6.1.4.1.5003.9.20.3.2.0.73)	acEMSFQDNResolveEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.76)	acDevicePmPollingEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.75)	acTokenPoolsEmpty
(.1.3.6.1.4.1.5003.9.20.3.2.0.78)	acPmHasNoSnmpConnection
(.1.3.6.1.4.1.5003.9.20.3.2.0.77)	acPmBatchOverflowAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.79)	JabraFirmwareUpgradeFailed
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.49)	acTrunksAlarmNearEndLOS
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.48)	acHitlessUpdateStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.45)	acDialPlanFileReplaced
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.44)	acH248LostConnectionWithCA
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.47)	acAnalogPortHighTemperature
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.46)	acAnalogPortSPIOutOfService
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.52)	acTrunksAlarmFarEndLOF
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.51)	acTrunksAlarmRcvAIS
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.54)	acAMSProcedureResult
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.53)	acIPv6ErrorAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.50)	acTrunksAlarmNearEndLOF
(.1.3.6.1.4.1.5003.9.20.3.2.0.61)	floatingLicenseExtended
(.1.3.6.1.4.1.5003.9.20.3.2.0.60)	acSEMSipMessageStatusAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.63)	acClmRegisterSuccessfulEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.62)	acClmDeviceReportAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.65)	acClmFailToSendUsageReportAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.64)	acClmRegisterFailureAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.67)	acClmServiceShutdownAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.20.3.2.0.66)	acCImFailToSendUsageReportExtendedAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.69)	acCImMaxDeviceCapacityAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.68)	acCImMaxDeviceMismatchEvent
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.59)	acGWSASEmergencyModeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.56)	acTMInconsistentRemoteAndLocalPLLStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.55)	acWeakRedundancy
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.58)	acTMReferenceChange
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.57)	acTMReferenceStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.21)	acSS7LinkBlockStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.20)	acSS7LinkInhibitStateChangeAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.50)	acSEMLicenseKeyAlarmDevice
(.1.3.6.1.4.1.5003.9.20.3.2.0.52)	acEMSNotEnoughOracleSpaceAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.51)	acEMSDiskSpaceAlarmCheck
(.1.3.6.1.4.1.5003.9.20.3.2.0.54)	IPPhoneSpeakerFirmDownloadFailure
(.1.3.6.1.4.1.5003.9.20.3.2.0.53)	acLicenseAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.55)	IPPhoneSpeakerFirmUpgradeFailure
(.1.3.6.1.4.1.5003.9.20.3.2.0.56)	IPPhoneConferSpeakerConnectFailure
(.1.3.6.1.4.1.5003.9.20.3.2.0.58)	acOvocReSyncEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.57)	IPPhoneGeneralLocalEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.59)	IPPhoneWebSuccessiveLoginFailure
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.27)	acPerformanceMonitoringThresholdCrossing
(.1.3.6.1.2.1.10.18.15.0.1)	ds1LineStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.26)	acSS7RedundancyAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.29)	acFanTrayAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.28)	acHTTPDownloadResult
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.23)	acSS7LinkSetStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.22)	acSS7LinkCongestionStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.25)	acSS7SNSetStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.24)	acSS7RouteSetStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.30)	acPowerSupplyAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.32)	acSAMissingAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.31)	acPEMAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.41)	IPPhoneLyncLoginFailure
(.1.3.6.1.4.1.5003.9.20.3.2.0.40)	IPPhoneSurvivableModeStart
(.1.3.6.1.4.1.5003.9.30.2.2.0.1)	acSBAServicesStatusAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.43)	acSEMRuleBandwidthAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.42)	acEMSAlarmSuppression
(.1.3.6.1.4.1.5003.9.30.2.2.0.3)	acSBAMemoryStatusAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.45)	acEMSKeepAliveAlarm
(.1.3.6.1.4.1.5003.9.30.2.2.0.2)	acSBACpuStatusAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.44)	acSEMRuleMaxConcurrentCallsAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.47)	acEndpointPublishAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.46)	acEMSPreProvisioningAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.49)	acEndpointServerOverloadAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.48)	acEndpointLicenseAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.38)	acSonetSectionLOFAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.37)	acDChannelStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.39)	acSonetSectionLOSAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.34)	acHASystemConfigMismatchAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.33)	acHASystemFaultAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.36)	acUserInputAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.35)	acHASystemSwitchOverAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.3)	acEMSNodeConnectionLostAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.9)	acEMSNoMismatchNodeAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.7)	acEMSConfigurationMismatchNodeAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.12)	acARMTopologyReloaded
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.13)	acARMRoutingRuleMatch
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.10)	acBoardEthernetLinkAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.10)	acARMLicenseMissing
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.11)	acARMQualityChanged
(.1.3.6.1.2.1.47.2.0.1)	entConfigChange
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.16)	acARMRegistrationStatusResyncThreshold
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.17)	acARMExternalWebService
(.1.3.6.1.4.1.5003.9.10.1.5.2)	resettingBoard
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.14)	acARMRouterReloaded
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.15)	acARMNoAvailableRouter
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.19)	acSS7LinkStateChangeAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.1)	acEMSSnmpCannotBindError
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.16)	acKeepAlive
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.15)	acOperationalStateChange
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.18)	acEnhancedBITStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.17)	acNATTraversalAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.12)	acActiveAlarmTableOverflow
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.11)	acBoardOverloadAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.14)	acAudioProvisioningAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.13)	acAtmPortAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.141)	acAnalogLineLeftOffhookAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.142)	acCDRServerAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.140)	acInstallationFailureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.138)	acFloatingLicenseAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.139)	acAWSSecurityRoleAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.136)	acHANetworkMonitorAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.137)	acHAEthernetGroupAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.134)	acMediaClusterRemoteInterfaceAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.135)	acHANetworkMismatchAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.132)	acCloudLicenseManagerAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.133)	acMediaClusterAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.81)	endpointVipDisconnected
(.1.3.6.1.2.1.255.3.1)	rtcpXrVoipThresholdViolation
(.1.3.6.1.4.1.5003.9.20.3.2.0.80)	endpointVipUnregistered
(.1.3.6.1.4.1.5003.9.20.3.2.0.83)	acReportSchedulersLoadAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.82)	acReportSchedulersTimeEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.85)	acFlexPoolLicenseUsage
(.1.3.6.1.4.1.5003.9.20.3.2.0.84)	acReportSchedulersExecutionEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.86)	acUMPUsersSchedulerAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.145)	acRemoteMonitoringAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.143)	acDSPFarmsMismatchAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.144)	acFlexLicenseManagerAlarm
(.1.3.6.1.6.3.1.1.5.1)	coldStart
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.120)	acMtcePsuFailureAlarm
(.1.3.6.1.6.3.1.1.5.2)	warmStart
(.1.3.6.1.6.3.1.1.5.3)	linkDown
(.1.3.6.1.6.3.1.1.5.4)	linkUp
(.1.3.6.1.6.3.1.1.5.5)	authenticationFailure
(.1.3.6.1.4.1.5003.9.80.3.2.0.50)	acUmpEndUserAuthFailEvent
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.116)	acMtceNetworkFailureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.117)	acMtceSwUpgradeFailureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.114)	acIpGroupNoRouteAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.115)	acMtcMClusterHaAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.112)	acACDThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.113)	acNERThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.110)	acResetNeededAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.111)	acASRThresholdAlarm
(.1.3.6.1.4.1.5003.9.40.3.2.0.13)	acVaCallRecordingErrorEvent
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.118)	acMtceHwTemperatureFailureAlarm
(.1.3.6.1.4.1.5003.9.40.3.2.0.11)	acVaResourceThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.119)	acMtceHwFanTrayFailureAlarm
(.1.3.6.1.4.1.5003.9.40.3.2.0.12)	acVaConnectionFailureAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.49)	acUmpUserSettingsFailEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.48)	acUmpO365CommandExEvent

OID	Type Values
(.1.3.6.1.4.1.5003.9.80.3.2.0.45)	acUmpAzureADSyncAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.44)	acUmpEndUserLicThresholdAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.47)	acUmpSBCFailureAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.46)	acUmpO365FailureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.130)	acNGINXConfigurationIsInvalidAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.41)	acUmpTenantLicThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.131)	acNGINXPprocessIsNotRunningAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.43)	acUmpSuAdminAuthFailEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.42)	acUmpUserLicThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.127)	acLicensePoolExpirationAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.128)	acCertificateExpiryAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.1.0.2)	acARMAdminStateChanged
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.125)	acLicensePoolOverAllocationAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.126)	acClusterBandwidthAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.123)	acModuleOperationAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.124)	acPortServiceAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.121)	acTrackIdStateChangeAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.1.0.1)	acARMConfigurationInconsistency
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.122)	acModuleServiceAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.1.0.0)	acARMDefaultTrap
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.129)	acLicenseKeyHitlessUpgradeAlarm
(.1.3.6.1.4.1.5003.9.10.1.5.1)	boardStarted
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.8)	acARMNTPSyncStatus
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.7)	acARMRouterUsingOtherConfigurator

OID	Type Values
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.6)	acARMLicenseHasExpired
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.5)	acARMLicenseAboutToExpire
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.9)	acARMLicenseSessionNumber
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.105)	acActivityLog
(.1.3.6.1.4.1.5003.9.40.3.2.0.28)	acVaDiskSpaceAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.106)	acLicensePoolInfraAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.103)	acBoardSignalingCpuUsageThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.9)	acBoardControllerFailureAlarm
(.1.3.6.1.4.1.5003.9.40.3.2.0.26)	acVaCompEventViewerDropped
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.8)	acBoardCallResourcesAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.104)	acWirelessCellularModemStatusChanged
(.1.3.6.1.4.1.5003.9.40.3.2.0.27)	acVaCompCertificateExpiredAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.101)	acIDSBlacklistNotification
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.102)	acProxyConnectivity
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.100)	acIDSThresholdCrossNotification
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.3)	acBoardTemperatureAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.2)	acBoardConfigurationError
(.1.3.6.1.4.1.5003.9.40.3.2.0.21)	acVACompPcGenAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.1)	acBoardFatalError
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.7)	acgwAdminStateChange
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.109)	acHTTPEMSService
(.1.3.6.1.4.1.5003.9.40.3.2.0.24)	acVaCompEventViewer
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.6)	acFeatureKeyError
(.1.3.6.1.4.1.5003.9.40.3.2.0.25)	acVaCompEventLogAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.5)	acBoardEvResettingBoard
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.107)	acLicensePoolApplicationAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.108)	acHttpProxyService
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.4)	acBoardEvBoardStarted
(.1.3.6.1.4.1.5003.9.40.3.2.0.23)	acVaCompSrvAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.85)	acBChannelAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.16)	acCbCompEventViewerDropped
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.84)	acNFASGroupAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.15)	acCbCompEventLogAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.87)	acMediaRealmBWThresholdAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.86)	acEthernetGroupAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.81)	acMediaProcessOverloadAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.12)	acCbCompPcServAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.80)	acPowerOverEthernetStatus
(.1.3.6.1.4.1.5003.9.80.3.2.0.11)	acCbCompPcGenAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.83)	acDataInterfaceStatus
(.1.3.6.1.4.1.5003.9.80.3.2.0.14)	acCbCompEventViewer
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.82)	acWirelessCellularModemAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.13)	acCbCompSrvAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.30)	acSEMRuleFailedCallsAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.32)	acSEMRuleAvrgCallDurationAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.31)	acSEMRulePoorQualityCallsAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.34)	acSEMCallDroppedAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.33)	acSEMLicenseKeyAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.20.3.2.0.36)	acSEMConnectionStatusAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.35)	acSEMClientLoadFlagAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.38)	acSEMMSLyncADServerAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.37)	acMSLyncConnectionAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.39)	IPPhoneRegisterFailure
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.89)	acNqmRttAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.88)	acNqmConnectivityAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.96)	acNqmLqMosAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.95)	acNqmCqMosAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.98)	acHANetworkWatchdogStatusAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.97)	acRedundantBoardAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.92)	acCertificateExpiryNotifiaction
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.4)	acARMDiskSize
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.91)	acNqmPacketLossAlarm
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.3)	acARMDiskSpaceUsage
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.94)	acProxyConnectionLost
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.2)	acARMLimitReached
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.93)	acWEBUserAccessDisabled
(.1.3.6.1.4.1.5003.9.70.1.2.2.0.1)	acARMOperationStatusChanged
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.90)	acNqmJitterAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.21)	acEMSMGBBackupEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.20)	acEMSNodeColdStartMissedEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.23)	acEMSSecurityAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.22)	acEMSMGEmsIpMismatchEvent

OID	Type Values
(.1.3.6.1.4.1.5003.9.20.3.2.0.25)	acEMSTopologyUpdateEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.24)	acEMSSecurityEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.27)	acEMSSyncAlarmEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.26)	acEMSTopologyFileEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.3)	acCbManEnvRestartEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.29)	acEMSLicenseKeyAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.2)	acCbManEnvUnreachableAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.28)	acEMSSyncActiveAlarmEvent
(.1.3.6.1.4.1.5003.9.40.3.2.0.43)	acVaManLicViolationEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.1)	acCbManLicenseCommitAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.99)	acIDSPolicyAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.63)	acSonetPathSTSARDIAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.62)	acSonetPathSTSASISAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.37)	acCceWindowsLicenseAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.65)	acSonetPathSignalLabelMismatchAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.64)	acSonetPathUnequippedAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.34)	acCceWrongSettingsAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.33)	acCceWrongOperatingAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.61)	acSonetPathSTSLOPAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.36)	acCceDiskSpaceAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.60)	acV52InterfaceAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.35)	acCceLoginFailedAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.32)	acCceAdminCertificateExpiredAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.31)	acCceAdminSystemCloudStatusAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.20.3.2.0.12)	acEMSNotEnoughDiskSpaceAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.11)	acEMSServerStartup
(.1.3.6.1.2.1.10.30.15.0.1)	dsx3LineStatus
(.1.3.6.1.4.1.5003.9.20.3.2.0.14)	acEMSSoftwareReplaceAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.13)	acEMSMGSoftwareUpgradeAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.15)	acEMSHardwareReplaceAlarm
(.1.3.6.1.4.1.5003.9.20.3.2.0.18)	acEMSPmFileGenerate
(.1.3.6.1.4.1.5003.9.40.3.2.0.9)	acVaCompResFailedEvent
(.1.3.6.1.4.1.5003.9.20.3.2.0.19)	acEMSPmHistoryAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.67)	acDS3AISAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.66)	acDS3RAIAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.69)	acDS3LOSAAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.68)	acDS3LOFAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.74)	acSS7UalGroupStateChangeAlarm
(.1.3.6.1.4.1.5003.9.40.3.2.0.1)	acVAManEnvUnreachableAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.73)	acSS7AliasPcStateChangeAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.76)	acAnalogPortGroundFaultOutOfService
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.75)	acLDAPLostConnection
(.1.3.6.1.4.1.5003.9.40.3.2.0.2)	acVAManEnvRestartEvent
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.70)	acSWUpgradeAlarm
(.1.3.6.1.4.1.5003.9.80.3.2.0.23)	acCbAdminOpsUsrFailedEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.22)	acCbAdminLicViolationEvent
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.72)	acThreeWayConferenceOutOfResources
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.71)	acNTPServerStatusAlarm

OID	Type Values
(.1.3.6.1.4.1.5003.9.80.3.2.0.24)	acCbAdminOpsBackupEvent
(.1.3.6.1.4.1.5003.9.80.3.2.0.21)	acCbAdminLicInvalidAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.78)	acOCSPServerStatusAlarm
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.77)	acSSHConnectionStatus
(.1.3.6.1.4.1.5003.9.10.1.21.2.0.79)	acBoardWanLinkAlarm

Table 10-24:Type Name: QualityLevelType

Type Values
(0) Poor
(1) Fair
(2) Good
(3) Undefined

Table 10-25:Type Name: CallCauseType

Type Values
(0) NONE
(1) MOS
(2) MOS LQ
(3) JITTER
(4) DELAY
(5) PACKET LOSS
(6) RERL

Table 10-26:Type Name: CallOriginatorType

Type Values
(0) Unknown
(1) Caller

Type Values
(2) Callee
(3) Device
(10) Conference server
(11) Conference user

Table 10-27:Type Name: TerminationReasonType

Type Values
(0) Unknown
(1) Normal Call Clear
(2) No Answer
(3) Busy
(4) No Resources
(5) No Match
(6) Forwarded
(7) General Failed
(8) Abnormally Terminated

Table 10-28:Type Name: TerminationReasonDetailsType

Type Values
(0) Reason Not Relevant
(1) Unassigned Number
(2) No Route To Transit Net
(3) No Route To Destination
(4) Send Special Information Tone
(5) Misdialed Trunk Prefix
(6) Channel Unacceptable

Type Values
(7) Call Awarded And
(8) Preemption
(9) Preemption Circuit Reserved For Reuse
(16) Normal Call Clear
(17) User Busy
(18) No User Responding
(19) No Answer From User Alerted
(20) MFCR2 Accept Call
(21) Call Rejected
(22) Number Changed
(23) Redirection
(25) Exchange Routing Error
(26) Non Selected User Clearing
(27) Release Because Trunk Disconnected
(28) Invalid Number Format
(29) Facility Reject
(30) Response To Status Enquiry
(31) Normal Unspecified
(32) Circuit Congestion
(33) User Congestion
(34) No Circuit Available
(38) Network Out Of Order
(41) Network Temporary Failure
(42) Network Congestion

Type Values
(43) Access Information Discarded
(44) Requested Circuit Not Available
(47) Resource Unavailable Unspecified
(39) Perm Fr Mode Conn Out Of S
(40) Perm Fr Mode Conn Operational
(46) Precedence Call Blocked
(49) Quality Of Service Unavailable
(50) Requested Fac Not Subscribed
(57) Bc Not Authorized
(58) Bc Not Presently Available
(63) Service Not Available
(53) Cug Out Calls Barred
(55) Cug Inc Calls Barred
(62) Access Info Subs Class Incons
(65) Bc Not Implemented
(66) Channel Type Not Implemented
(69) Requested Fac Not Implemented
(70) Only Restricted Info Bearer
(79) Service Not Implemented Unspecified
(81) Invalid Call Ref
(82) Identified Channel Not Exist
(83) Suspended Call But Call Id Not Exist
(84) Call Id In Use
(85) No Call Suspended

Type Values
(86) Call Having Call Id Cleared
(88) Incompatible Destination
(91) Invalid Transit Network Selection
(95) Invalid Message Unspecified
(87) Not Cug Member
(90) Cug Non Existent
(96) Mandatory Ie Missing
(97) Message Type Non Existent
(98) Message State Inconsistency
(99) Non Existent Ie
(100) Invalid Ie Content
(101) Message Not Compatible
(102) Recovery On Timer Expiry
(103) Parameter Non Existent
(110) Message With Unrecognized Param
(111) Protocol Error Unspecified
(112) Unknown Error
(127) Interworking Unspecified
(128) Q931 Last Reason
(304) Release Because Unknown Reason
(306) Release Because Remote Cancel Call
(307) Release Because Unmatched Capabilities
(308) Release Because Unmatched Credentials
(309) Release Because Unable To Handle Remote Request

Type Values
(310) Release Because No Conference Resources Left
(311) Release Because Conference Full
(312) Release Because Voice Prompt Play Ended
(313) Release Because Voice Prompt Not Found
(315) Release Because Manual Disc
(316) Release Because Silence Disc
(317) Release Because Nortel Xfer Success
(318) Release Because Rtp Conn Broken
(319) Release Because Disconnect Code
(320) Release Because Gw Locked
(321) Release Because Fail
(322) Release Because Forward
(323) Release Because Anonymous Source
(324) Release Because Preemption Analog Circuit Reserved For Reuse
(325) Release Because Precedence Call Blocked
(326) Release Because Held Timeout
(327) Release Because Media Mismatch
(328) Release Because Max Duration Timer Expired
(329) Release Because Transcoding Full
(330) Release Because No Transcoding Resources Left
(331) Release Postpone Possible
(332) Release Because Preemption Due To High Priority
(333) Release Because Preemption Failed
(805) Release Because Ip Profile Call Limit

Type Values
(806) Release Because Media Limits Exceeded
(807) Release Because Call Transferred
(808) Release Because Classification Failed
(809) Release Because Authentication Failed
(810) Release Because Ipgroup Registration Mode
(811) Release Because Arm Drop
(812) Release Because Media Dest Unreachable
(813) Release Because Start Arm Routing
(814) Release Because Forward Supplementary
(815) Release Because Fax ReRouting
(816) Release Because Ldap Failure
(817) Release Because Callsetuprules Failure
(818) Release Because No User Found
(819) Release Because In Admission Failed
(820) Release Because out Admission Failed
(821) Release Because In Media Limits Exceeded
(822) Release Because User Blocked
(823) Release Because Bad Info Package
(824) Release Because Src Ip Is Not Dedicated Registrar
(850) Release Because ACD Threshold Crossed
(851) Release Because ASR Threshold Crossed
(852) Release Because NER Threshold Crossed
(853) Release Because Ipgroup Registration Mode
(854) Release Because Featurekey Changed

Type Values
(855) Release Because Internal Route
(856) Release Because CID CMD Failure
(857) Release Because Other Forked Call Answered
(858) Release Because Media Sync Failed
(859) Release Because Reg Max Threshold Crossed

Table 10-29:Type Name: MediaType

Type Values
(0) Voice
(1) Video
(2) Audio Video
(3) Image
(4) Data
(5) Audio V150
(6) Text
(7) Unknown
(8) MSRP
(27) Application Sharing
(28) Chat

Table 10-30:Type Name: EndpointType

Type Values
(0) FXO
(1) FXS
(2) EANDM
(3) ISDN

Type Values
(4) CAS
(5) DAA
(6) IPMedia(7) NETANN
(8) Streaming
(9) Transparent
(10) MSCML
(11) VXML
(12) SBC
(13) IP2IP
(14) Test
(18) Test SBC
(19) HTTP
(100) Skype
(101) Skype Conference
(200) IP Phone

Table 10-31:Type Name: CallSourceType

Type Values
(0) AudioCodes
(1) MSlync
(2) IPPhone
(10) Site
(11) Link

Table 10-32:Type Name: PstnTermReasonType

Type Values
(1) UNALLOCATED_NUMBER
(2) NO_ROUTE_TO_SPECIFIED_TRANSIT_NETWORK
(3) NO_ROUTE_TO_DESTINATION
(4) SEND_SPECIAL_INFORMATION_TONE
(5) MISDIALED_TRUNK_PREFIX
(6) CHANNEL_UNACCEPTABLE
(7) CALL_AWARDED_BEING_DELIVERED
(8) PREEMPTION
(9) PREEMPTION_CIRCUIT_RESERVED_FOR_REUSE
(10) NORMAL_CALL_CLEARING
(17) USER_BUSY
(18) NO_USER_RESPONDING
(19) NO_ANSWER_FROM_USER
(20) SUBSCRIBER_ABSENT
(21) CALL_REJECTED
(22) NUMBER_CHANGED
(26) NONSELECTED_USER_CLEARING
(27) DESTINATION_OUT_OF_ORDER
(28) INVALID_NUMBER_FORMAT
(29) FACILITIES_REJECTED
(30) RESPONSE_TO_STATUS_INQUIRY
(31) NORMAL_UNSPECIFIED
(34) NO_CIRCUIT_CHANNEL_AVAILABLE

Type Values
(35) CALL_QUEUED
(38) NETWORK_OUT_OF_ORDER
(39) PERMANENT_FRAME_MODE_CONNECTION_OUTOFSERVICE
(40) PERMANENT_FRAME_MODE_CONNECTION_OPERATIONAL
(41) TEMPORARY_FAILURE
(42) SWITCHING_EQUIPMENT_CONGESTION
(43) ACCESS_INFORMATION_DISCARDED
(44) REQUESTED_CIRCUIT_CHANNEL_NOT_AVAILABLE
(46) PRECEDENCE_CALL_BLOCKED
(47) RESOURCE_UNAVAILABLE_UNSPECIFIED
(49) QUALITY_OF_SERVICE_NOT_AVAILABLE
(50) REQUESTED_FACILITY_NOT_SUBSCRIBED
(52) OUTGOING_CALLS_BARRED
(53) OUTGOING_CALLS_BARRED_WITHIN_CUG
(54) INCOMING_CALLS_BARRED
(55) INCOMING_CALLS_BARRED_WITHIN_CUG
(57) BEARER_CAPABILITY_NOT_AUTHORIZED
(58) BEARER_CAPABILITY_NOT_PRESENTLY_AVAILABLE
(62) INCONSISTENCY_IN_OUTGOING_INFORMATION_ELEMENT
(63) SERVICE_OR_OPTION_NOT_AVAILABLE
(65) BEARER_CAPABILITY_NOT_IMPLEMENTED
(66) CHANNEL_TYPE_NOT_IMPLEMENTED
(69) REQUESTED_FACILITY_NOT_IMPLEMENTED
(79) ONLY_RESTRICTED_DIGITAL_INFORMATION_AVAILABLE

Type Values
(81) INVALID_CALL_REFERENCE_VALUE
(82) IDENTIFIED_CHANNEL_DOES_NOT_EXIST
(83) A_SUSPENDED_CALL_EXISTS_BUT
(84) CALL_IDENTITY_IN_USE
(85) NO_CALL_SUSPENDED
(86) CALL_HAVING_THE_REQUESTED_BEEN_CLEARED
(87) USER_NOT_A_MEMBER_OF_CUG
(88) INCOMPATIBLE_DESTINATION
(90) NONEXISTENT_CUG
(91) INVALID_TRANSIT_NETWORK_SELECTION
(95) INVALID_MESSAGE_UNSPECIFIED
(96) MANDATORY_INFORMATION_ELEMENT_IS_MISSING
(97) MESSAGE_TYPE_NONEXISTENT_OR_NOT_IMPLEMENTED
(98) MESSAGE_NOT_COMPATIBLE_NONEXISTENT
(99) INFORMATION_ELEMENT_PARAMETER_NONEXISTENT
(100) INVALID_INFORMATION_ELEMENT_CONTENTS
(101) MESSAGE_NOT_COMPATIBLE_WITH_CALL_STATE
(102) RECOVERY_ON_TIMER_EXPIRY
(103) PARAMETER_NONEXISTENT_OR_NOT_IMPLEMENTED
(110) MESSAGE_WITH_UNRECOGNIZED_PARAMETER_DISCARDED
(111) PROTOCOL_ERROR_UNSPECIFIED
(127) INTERWORKING_UNSPECIFIED

Table 10-33:Type Name: LinkType

Type Values
(1) IP Group
(2) Trunk Group
(4) Phone Prefix
(8) Control IP
(16) Media IP
(32) Media Realm
(64) Remote Media Subnet
(128) FQDN
(256) Media Server

Table 10-34:Type Name: LinkDirection

Type Values
(1) BI DIRECTIONAL
(2) INGRESS
(3) EGRESS

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, 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>

©2026 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, 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-19234

