AudioCodes One Voice Operations Center

OVOC

Installation, Operation and Maintenance

Version 8.4





Notice

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

This document is subject to change without notice.

Date Published: September-08-2024

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

Document Name
One Voice Operations Center Product Description
One Voice Operations Center User's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Deployment Guide
Device Manager Pro Administrator's Manual
ARM User's Manual
Documents for Managed Devices
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500Li MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800 MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual

Document Name

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
LTRT- 94197	Initial Version for this release including: Added Section Restore from CentOS; Migration to Rocky Linux Operating System Updated Sections: Application Status ; General Information; Change Schedule Backup Time; OVOC Server Backup Processes; HTTP Security Settings Menu Options and removed version options for TLS1.0 and 1.1. Removed Section for installing DVD one from physical device Replaced all references to CentOS with Rocky Linux
LTRT- 94198	Update to procedure 'Migration to Rocky Linux Operating System'.
LTRT- 94199	Update to procedure 'Migration to Rocky Linux Operating System'.
LTRT- 94200	Correction to introduction in 'Migration to Rocky Linux Operating System'.

Table of Contents

1	Overview	1
Pa	rrt I	2
Pr	e-installation Information	2
2	Managed VoIP Equipment	3
3	Hardware and Software Specifications	7
	OVOC Server Minimum Requirements	7
	OVOC Client Requirements	8
	Bandwidth Requirements	8
	OVOC Bandwidth Requirements	8
	Voice Quality Bandwidth Requirements	8
	Device Manager Communication and Optimization	9 11
	Skype for Business Monitoring SQL Server Prerequisites	
4	OVOC Software Deliverables	13
Da	ert II	15
	ICC Server Installation	15
5		15
5		10
	Windows	16
	OV/OC Server Users	10
6	Installing OVOC Server on Virtual Machines on Cloud-based Platforms	18
Ŭ	Launching Public OVOC Image on Amazon Web Services (AWS)	18
	Launching Public DVOC Image on Amazon Web Services (AVV3)	18
	Configuring AWS SES Service	23
	Creating OVOC Virtual Machine on Microsoft Azure	26
	Deploying Older OVOC Versions using PowerShell	32
7	Installing OVOC Server on VMware Virtual Machine	34
	Deploying OVOC Image with VMware vSphere Hypervisor (ESXi)	34
	Deploying Standalone VMware VM using ESXi Wizard	34
	Deploying OVOC Image with VMware vSphere Cluster	38
	Configuring the Virtual Machine Hardware Settings	40
	Configuring OVOC Virtual Machines (VMs) in a VMware Cluster	42
	Cluster Host Node Failure on VMware	42
	Connecting OVOC Server to Network on VMware	
8	Installing OVOC Server on Microsoft Hyper-V Virtual Machine	
	Configuring the Virtual Machine Hardware Settings	53
	Expanding Disk Capacity	55

	Changing MAC Addresses from 'Dynamic' to 'Static'	60
	Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster	61
	Hyper-V Cluster Site Requirements	61
	Add the OVOC VM in Failover Cluster Manager	62
	Cluster Host Node Failure on Hyper-V	64
	Connecting OVOC Server to Network on HyperV	64
9	Installing OVOC Server on Dedicated Hardware	67
	Installing DVD1	67
	DVD3: OVOC Server Application Installation	73
10	Migrating to Rocky Linux Operating System	77
Par	rt III	80
Pos	st Installation	80
11	Registering OVOC Applications on Azure	81
	Registering Single Tenant in Organizational Directory	81
	Configuring OVOC Web Azure Settings - Single Tenant Setup	91
	Registering Multitenant Support	94
	Configuring OVOC Web Azure Settings - Multitenant Setup	107
	Upgrading from Single Tenant to Multitenant	112
	Configuring OVOC Web Azure Settings - Multitenant Upgrade	122
	Create Azure Groups and Assign Members	124
	Add External Tenant Operators and Assign Roles	129
	Troubleshooting - Granting Admin Consent	136
12	Setting Up Microsoft Teams Subscriber Notifications Services	400
CO	nnection	. 138
	Register Microsoft Teams Application	138
	Configure Microsoft Graph API Permissions	142
	Define OVOC FQDN and Load Certificate	145
	Microsoft Teams URLs	147
13	Managing Device Connections	. 148
	Establishing OVOC-Devices Connections	148
	Configure OVOC Server with NAT IP Address per Interface	149
	Configure OVOC Server with NAT IP per Tenant	150
	Establishing Devices - OVOC Connections	152
	Automatic Detection	152
	Configure OVOC Cloud Architecture Mode (WebSocket Tunnel)	153
	Configuring Cloud Architecture Mode (WebSocket Tuppel)	. 104
		100
	Setting up Multiple Ethernet Interfaces	157
	Setting up Multiple Ethernet Interfaces	
	Setting up Multiple Ethernet Interfaces Connecting Mediant Cloud Edition (CE) Devices on Azure Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using	157 159

	Configuring the OVOC Server Manager on Azure (Public IP)	160
	Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Public IP)	161
	Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address	163
	Configuring the OVOC Server Manager on Azure (Internal IP)	164
	Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Internal IP)	165
	Connecting Mediant Cloud Edition (CE) SBC Devices on AWS	167
	Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS	.168
	Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS	.168
	Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack	(
	Manager	.169
Par	Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface	169 171
	C Server Upgrade	171
		470
14	Upgrading OVOC Server on Amazon AWS and Microsoft Azure	172
	Before Upgrading on Microsoft Azure	172
	Cloud Upgrade Procedure	172
	After Upgrading on AWS	175
15	Upgrading OVOC Server on VMware and Microsoft Hyper-V Virtual	
Mac	chines	177
	Run the Server Upgrade Script	177
	Option 1: Standard Upgrade Script	.177
16	Upgrading OVOC Server on Dedicated Hardware	181
	Upgrading the OVOC Server-DVD	181
	Upgrading the OVOC Server using an ISO File	183
17	Installation and Upgrade Troubleshooting of the Operational	400
Env	ironment	180
Par	t V	189
OVO	OC Server Machine Backup and Restore	189
18	OVOC Server Backup Processes	190
	Change Schedule Backup Time	190
19	OVOC Server Restore	192
	Configuration Restore	193
	Full Restore	194
	Restore Backup Data to Separate Virtual Machine	195
	Restore from CentOS	195
Par	t VI	197
OVO	DC Server Manager	197
20	Getting Started	198

	Connecting to the OVOC Server Manager	
	Using the OVOC Server Manager	
	OVOC Server Manager Menu Options Summary	199
21	Viewing Process Statuses	
22	Viewing General Information	206
23	Collecting Full Logs	
	Selected Logs	
24	Application Maintenance	
	Start or Restart the Application	
	Stop the Application	
	Web Servers	
	License	
	OVOC License	
	analytics API	
	Guacamole RDP Gateway	
	VMware Tools	
	Shutdown the OVOC Server Machine	
	Reboot the OVOC Server Machine	
25	Network Configuration	
	Server IP Address	
	Ethernet Interfaces	
	Remove Interface	
	Modify Interface	230
	Ethernet Redundancy	231
	Add Redundant Interface	
	Remove Ethernet Redundancy	
	Modify Redundant Interface	
	DNS Client	
	Static Routes	
	Proxy Settings	
	SNMP Agent	
	SNMP Agent Listening Port	
	Linux System Trap Forwarding Configuration	
	NES	241 242
20	NTD 9 Cleak Settings	
20	NTD	
	NIP	
	Stopping and Starting the NTP Server	
	Activate DDoS Protection	
	Authorizing Subnets to Connect to OVOC NTP	

	Timezone Settings	247
	Date and Time Settings	248
28	Security	249
	Add OVOC User	. 250
	SSH	250
	SSH Log Level	. 251
	SSH Banner	251
	SSH on Ethernet Interfaces	252
	Add SSH to All Ethernet Interfaces	. 253
	Add SSH to Ethernet Interface	. 253
	Remove SSH from Ethernet Interface	. 253
	Enable/Disable SSH Password Authentication	. 254
	Enable SSH Ignore User Known Hosts Parameter	254
	SSH Allowed Hosts	255
	Allow ALL Hosts	255
	Deny ALL Hosts	255
	Add Hosts to Allowed Hosts	256
	Remove Host/Subnet from Allowed Hosts	257
	PostgreSQL DB Password	257
	Cassandra Password	259
	Elastic Search DB Password	. 260
	OS Users Passwords	260
	General Password Settings	261
	Operating System User Security Extensions	262
	File Integrity Checker	264
	Software Integrity Checker (AIDE) and Pre-linking	264
	USB Storage	265
	Network Options	. 265
	Auditd Agent Options	266
	OVOC Voice Quality Package - SBC Communication	266
	HTTPS SSL TLS Security	
	Server Certificates Update	268
	HTTP Security Settings Menu Options	273
	TLSv1.2 for Apache	274
	Show Allowed SSL Cipher Suites	. 274
	Edit SSL Cipher Suites Configuration String	275
	Restore SSL Cipher Suites Configuration Default	276
	Manage HTTP Service Port (80)	276
	Manage IPP Files Service Port (8080)	276
	Manage IPPs HTTP Port (8081)	276
	Manage IPPs HTTPS Port (8082)	277
	OVOC Rest (Port 911)	277
	Floating License (Port 912)	277
	OVOC WebSocket (Port 915)	277

	QoE Teams Server REST (Port 5010)	
	Trust Store Configuration	278
	SBC HTTPS Authentication Mode	
	Enable Device Manager Pro and NBIF Web Pages Secured Communication	
	Change HTTP/S Authentication Password for NBIF Directory	
	Disable Client's IP Address Validation	
	Host Header Validation Configuration	
29	Diagnostics	
	Server Syslog Configuration	
	Devices Syslog Configuration	
	Devices Debug Configuration	
	Server Logger Levels	
	Network Traffic Capture	
Par	t VII	
Cor	nfiguring the Firewall	
30	Configuring the Firewall	292
	Cloud Architecture Mode (WebSocket Tunnel) Firewall Settings	297
	Firewall Settings for NAT Deployment	297
	Firewall Rules for Service Provider with Single Node	298
Par	t VIII	301
Apr	pendix	301
24	Configuring OVOC as the Email Server on Microsoft Azura	202
31	Configuring OVOC as the Email Server on Microsoft Azure	
	Configuring OVOC as the Email Server on Microsoft Azure using SMTP Relay	302
20	Configuring PAID 0 for AudioCodes OVOC on HP ProLight DI 360n	
Ger	10 Servers	
	RAID-0 Prerequisites	307
	RAID-0 Hardware Preparation	307
	Configuring RAID-0	
	Step 1 Create Logical Drive	
	Step 2 Set Logical Drive as Bootable Volume	
33	Managing Clusters	
	Migrating OVOC Virtual Machines in a VMware Cluster	
	Moving OVOC VMs in a Hyper-V Cluster	
34	Supplementary Security Procedures	
	Installing Custom Certificates on OVOC Managed Devices	
	Gateways and SBC Devices	
	Step 1: Generate a Certificate Signing Request (CSR)	315
	Step 2: Receive the New Certificates from the CA	
	Step 3: Update Device with New Certificate	317

	Step 4: Update Device's Trusted Certificate Store	
	Step 5: Configure HTTPS Parameters on the Device	
	Step 6: Reset Device to Apply the New Configuration	
	MP-1xx Devices	
	Step 1: Generate a Certificate Signing Request (CSR)	
	Step 2: Receive the New Certificates from the CA	
	Step 3: Update Device with New Certificate	
	Step 4: Update Device's Trusted Certificate Store	
	Step 5: Configure HTTPS Parameters on Device	
	Step 6: Reset Device to Apply the New Configuration	
	Cleaning up Temporary Files on OVOC Server	
35	Transferring Files	
36	Verifying and Converting Certificates	
37	Self-Signed Certificates	
	Mozilla Firefox	
	Google Chrome	
	Microsoft Edge	
38	Datacenter Disaster Recovery	
	Introduction	
	Solution Description	
	Initial Requirements	
	New Customer Configuration	
	Data Synchronization Process	
	Recovery Process	

1 Overview

The One Voice Operations Center (OVOC) provides customers with the capability to easily and rapidly provision, deploy and manage AudioCodes devices and endpoints. Provisioning, deploying and managing these devices and endpoints with the OVOC are performed from a user-friendly Web Graphic User Interface (GUI). This document describes the installation of the OVOC server and its components. It is intended for anyone responsible for installing and maintaining AudioCodes' OVOC server and the OVOC server database.

Part I

Pre-installation Information

This part describes the OVOC server components, requirements and deliverables.

2 Managed VoIP Equipment

The following products (and product versions) can be managed by this OVOC release:

Table 2-1: Managed VoIP Equipment

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

¹This product does not support Voice Quality Management.

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

¹As above

²As above

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

Product	Supported Software Version					
Pro Edition						
CloudBond 365 Enterprise Edition	Version 7.6 (with MediantVersion 7.2.100 and later)					
CloudBond 365 Standard + Edition	Version 7.6 (with Mediant800B Version 7.2.100 and later)					
CloudBond 365 Standard	Version 7.6 (with Mediant 800B Version 7.2.100 and later)					
CloudBond 365	Version 8.0.0 (Skype for Business 2019 and Microsoft Teams					
User Management	Pack 365					
User Management Pack 365	Version 7.8.100					
User Management Pack 365 ENT	Version 8.0.0					
User Management Pack 365 SP Version	8.0.450, 8.0.400, 8.0.300, 8.0.220, 8.0.200, 8.0.100					
Meetings and Record	rdings					
SmartTAP 360° Live Recording	Version 5.6, 5.5, 5.4, Ver. 5.3, Ver. 5.2, Ver. 5.1, Ver. 5.0, Version 4.3					
Meeting Insights	Version 2.0.44.27					
Voca Conversational Interaction Center	Version 8.4					
Voice Al Connect	Version 3.12					
AudioCodes	ATS STT Server					
Services (ATS) Devices	ATS Diarization Server					
Generic Application	s					
Fax and Auto- Attendant (IVR)	Version 2.6.200					
Microsoft Teams Di	rect Routing SBA					
Mediant 800B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.					
Mediant 800C DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.					
Mediant 1000B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.					
Mediant 2600B DR-SBA	SBA Version 1.0.1xx and later with SBC certified by Microsoft.					
Mediant DR-SBA Virtual Appliance	SBA Version 1.0.1x.x and later with SBC certified by Microsoft.					
AudioCodes Routing Manager (ARM)	Version 9.8					

Product	Supported Software Version						
Device Management							
400HD Series Lync server	From Version 2.0.13: 420HD, 430HD 440HD						
Generic SIP server	From Version 2.2.2: 420HD, 430HD 440HD, 405HD and 405 From Version 3.4.3: C450HD, 450HD, 445HD and RX50						
400HD Series Skype for Business-Teams- compatible devices	 From Version 3.0.0: 420HD, 430HD 440HD and 405HD. From Version 3.0.1: 420HD, 430HD 440HD, 405HD and 450HD. From Version 3.0.2: HRS 457 (with Jabra firmware support). From Version 3.1.0: 445HD, 430HD 440HD, 405HD, 450HD and HRS. From Version 3.2.1 C450HD. From Version 3.2.1: C450HD, 435HD, 430HD 440HD, 405HD,450HD, HRS 457D and HRS 458. From Version 3.4.2: RX50 Conference Phone From Version 1.5: C448HD and C450HD From Version 1.12.33: C435HD From Version 1.2: A3: C435HD From Version 1.15: C455HD From Version 1.15: C455HD From Version 1.15: C455HD From Version 1.18: RXV81 Meeting Room Solution From Version 2.2: RX-PANEL From Version 2.2: RXV200 ✓ From Version 2.6: AudioCodes RXVCam360 ✓ From Version 2.6: AudioCodes RXVCam70 From Version 2.3: C430HD 						
Device Management - Third-party Vendor Products							
Spectralink	Spectralink 8440						
Polycom							
Polycom Trio 8800	Polycom Trio 8800						
Polycom VVX	Polycom VVX						
CCX 500/600 phones	CCX 500/600 phones						
Jabra Headset Support*	All Jabra devices that are supported by the Jabra Integration Service.						
EPOS	For a list of supported devices, see: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/epos/fact-sheet-epos-manager-en.pdf						

All Versions VoIP equipment work with the SIP control protocol. Bold refers to new product support and Version support.

3 Hardware and Software Specifications

This section describes the hardware and software specifications of the OVOC server.

OVOC Server Minimum Requirements

The table below lists the minimum requirements for running the different OVOC server platforms.

Resources	Virtual Platform	Memory	Recommended Disk Space	Minimum Disk Space (OS + Data)	Processors	
Low Profile						
VMWare	VMware: ESXi 8.0VMware HA cluster: VMware ESXi 6.0	24 GiB RAM	500 GB	320 GiB	 1 core with at least 2.5 GHz 2 cores with at least 2.0 GHz 	
HyperV	 Microsoft Hyper-V Server 2016 Microsoft Hyper-V Server 2016 HA Cluster 	24 GiB RAM	500 GB	320 GiB	 1 core with at least 2.5 GHz 2 cores with at least 2.0 GHz 	
Azure	Size: D8ds_v4	32 GiB	500 GB SSD Premium	320 GiB	8 vCPUs	
AWS	InstanceSize: m5.2xlarge	32 GiB	AWS EBS: General Purpose SSD (GP2) 500 GB	320 GiB	8 vCPUs	
High Profile						
VMWare	VMware: ESXi 8.0VMware HA cluster: VMware ESXi 6.0	40 GiB RAM	1.2 TB	520 GiB	6 cores with at least 2 GHz	
HyperV	 Microsoft Hyper-V Server 2016 Microsoft Hyper-V Server 2016 HA Cluster 	40 GiB RAM	1.2 TB	520 GiB)	6 cores with at least 2 GHz	
Azure	Size: D16ds_v4	64 GiB	2 TB SSD Premium	520 GiB	16 vCPUs	
AWS	InstanceSize: m5.4xlarge	64 GiB	AWS EBS: General Purpose SSD (GP2) 2TB	520 GiB	16 vCPUs	
Bare Metal (HP DL360	lp Gen10)					
	-	64 GiB	Disk: 2x 1.92 TB SSD configured in RAID 0		 Intel *Xeon *Cascade Gold 6226R (16 cores 2.6 GHz each) Intel *Xeon * Gold 6126 (12 cores 2.60 GHz each) 	
SP Single						
	VMware: ESXi 8.0 and VMware HA cluster: VMware ESXi 6.0	256 GB	Standalone mode: SSD 6TB with Ethernet ports: 10GB ports	~1.25T SSD	24 cores at 2.60 GHz	

Table 3-1: OVOC Server Minimum Requirements

OVOC Client Requirements

Table 3-2: OVOC Client Minimum Requirements

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

Bandwidth Requirements

This section lists the OVOC bandwidth requirements.

OVOC Bandwidth Requirements

The bandwidth requirement is for OVOC server <-> Device communication. The network bandwidth requirements per device is 500 Kb/sec for faults, performance monitoring and maintenance actions.

Voice Quality Bandwidth Requirements

The following table describes the upload bandwidth speed requirements for Voice Quality for the different devices. The bandwidth requirement is for OVOC server <- > Device communication.

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
SBC		
Mediant 500 E-SBC	-	-
Mediant 500L E-SBC	-	-
Mediant 800 Mediant 850	60	135 Kbits/sec
Mediant 1000	150	330 Kbits / sec

Table 3-3: Voice Quality Bandwidth Requirements

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
Mediant 2000	_	_
Mediant 2600	600	1.3 Mbit/sec
Mediant Software (Server Edition) SBC	-	-
Mediant Software(Virtual Edition) SBC	-	-
Mediant Cloud Edition	-	-
Mediant 3100 SBC	-	-
Mediant 3000	1024	2.2 Mbit/sec
Mediant 4000	4,000	8.6 Mbit/sec
Gateway		
MP-118	8	15 Kbits/sec
MP-124	24	45 Kbits/sec
Mediant 800 Mediant 850	60	110 Kbits/sec
Mediant 1000	120	220 Kbits/sec
Mediant 2000	480	880 Kbits/sec
Mediant 2600	_	_
Mediant 3000	2048	3.6 Mbit/sec
Mediant 4000	_	_
Endpoints	_	56 Kbits/sec

OVOC Capacities

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

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server			
OVOC Management Capacity							
Managed devices	100	5,000	5,000	10,000			
Links	200	10,000	10,000	10,000			
Operators		1	25	'			
Device Manager Pro							
Managed devices (see Device Manager Communication and Optimization on the next page) for further details).	1,000	 30,000 Microsoft Lync/Skype for Business and third- party vendor devices 20,000 Microsoft Teams devices 	 10,000 Microsoft Lync/Skype for Business and third-party vendor devices Including phones, headsets and Conference Suite devices. 20,000 Microsoft Teams devices 	 30,000 Skype for Business devices and third-party vendor devices Including phones, headsets and Conference Suite devices. 20,000 Teams device 			
Disk space allocated for firmware files	5 GB	5 GB 10 GB					
Alarm and Journal Capacity	Alarm and Journal Capacity						
History alarms		Up to 3	12 months or 10,000,000 million alarn	ıs			
Journal logs		Up to 12 months					
Steady state		20 alarms pe	er second	50 alarms per second			
Performance Monitoring							
Polled parameters per polling interval per OVOC- managed device	50,000	100,000	100,000	500,000			
Polled parameters per polling interval per OVOC instance	50,000	500,000	500,000	1,000,000			
Storage time			One year				
QoE Call Flow (for SBC calls on	ly)						
Maximum managed devices with QoE call flows	10	100	100	300			
CAPS per OVOC instance	6	25	100	300			
Maximum number of calls	1,000,000	1,000,000	1,000,000	10,000,000			
OVOC QoE for Devices							
QoE for managed devices	100	1,200	3,000	10,000			
CAPS (calls attempts per second) per device	30	120	300	1,000			
CAPS per OVOC instance (SBC and SFB/Teams and RFC SIP	30	120	300	1,000			

Table 3-4: OVOC Capacities

Machine Specifications	Low Profile	Low Profile High Profile Bare Metal		Service Provider Single Server			
Publish 6035)	Teams CAPS=30 ¹	Teams CAPS=120 ²		Teams CAPS= ³			
QoE concurrent sessions	3,000	12,000	30,000	100,000			
Call Details Storage - detailed information per call	Up to one year or 6,000,000	Up to one year or 80,000,000	Up to one year or 80,000,000	Up to one year or 200,000,000			
Calls Statistics Storage - statistics information storage	Up to one year or 12,000,000	Up to one year or 150,000,000	Up to one year or 150,000,000	Up to one year or 500,000,000			
QoE Capacity with SBC Floating License Capability							
CAPS (calls attempts per second) per OVOC instance with SIP call flow.	5	22	90	-			
CAPS (calls attempts per second) per OVOC instance without SIP call flow.	27	108	270	-			
Managed devices with floating license.	100	500	1,000	-			
Lync and AD Servers- applicable for QoE license only							
MS Lync servers	Up to 2						
AD Servers for Users sync	nc Up to 2						
Users sync Up to 150,000							
TEAMS Customer	up to 7 ⁴						

Device Manager Communication and Optimization

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

By adjusting the keep-alive interval based on the number of devices in the system, it is possible to optimize the response time for device actions. However, it is crucial to consider the tradeoffs between response time and network overhead. Regular monitoring and performance

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

²As above

³Please contact AudioCodes OVOC Product Manager

⁴For additional support, contact AudioCodes Product Manager

tuning should be conducted to ensure the system operates efficiently and meets the desired performance goals.

Skype for Business Monitoring SQL Server Prerequisites

The following are the Skype for Business Monitoring SQL Server prerequisites:

The server must be defined to accept login in 'Mix Authentication' mode.

- The server must be configured to collect calls before the OVOC can connect to it and retrieve Skype for Business calls.
- Call Detail Records (CDRs) and Quality of Experience (QoE) Data policies must be configured to capture data.
- Network administrators must be provisioned with the correct database permissions (refer to the One Voice Operations Center User's Manual).
- Excel macros must be enabled so that the SQL queries and reports can be run; tested with Excel 2010.
- Detailed minimum requirements for Skype for Business SQL Server can be found in the following link:

http://technet.microsoft.com/en-us/library/gg412952.aspx

4 OVOC Software Deliverables

The following table describes the OVOC software deliverables.

Table 4-1: OVC	C Software	Deliverables
----------------	------------	--------------

Installation/Upgrade Platform	Media		
Installation			
Dedicated	 DVD1-Rocky Linux version 8.x Operating System DVD3-OVOC Software Installation 		
VMware	DVD5-OVOC Software Installation OVA file		
HyperV	DVD5-OVOC Software Installation 7z file		
Amazon AWS	Create OVOC instance from Public AMI image provided by AudioCodes		
Microsoft Azure	Create OVOC virtual machine from Azure Marketplace.		
Upgrade			
Dedicated	DVD3-OVOC Server Application DVD		
	OR		
	DVD3-OVOC Server Application ISO file		
Microsoft HyperV	DVD3-OVOC Server Application ISO file		
Amazon AWS	DVD3-OVOC Server Application ISO file		

Note the following

- **DVD1:** Operating System DVD (OVOC server and Client Requirements):
- **DVD3:** Software Installation and Documentation DVD:

The DVD 'SW Installation and Documentation' DVD comprises the following folders:

- 'EmsServerInstall' OVOC server software (including Management server, PM server and VQM server) to install on the dedicated OVOC server machine.
- Documentation All documentation related to the present OVOC version. The documentation folder includes the following documents and sub-folders:
 - OVOC Release Notes Document includes the list of the new features introduced in the current software version as well as version restrictions and limitations.
 - OVOC Server IOM Manual Installation, Operation and Maintenance Guide.

- OVOC Product Description
- OVOC User's Manual
- OVOC Integration with Northbound Interfaces
- OVOC Security Guidelines
- OVOC Alarms Monitoring Guide
- OVOC Performance Monitoring Guide

Installation and upgrade files can also be downloaded from the Website by registered customers at https://www.audiocodes.com/services-support/maintenance-and-support.

Part II

OVOC Server Installation

This part describes the testing of the installation requirements and the installation of the OVOC server.

5 Files Verification

You need to verify the contents of the ISO file received from AudioCodes using an MD5 checksum. As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications, and is also commonly used to check the integrity of file, and verify download. Perform the following verifications on the relevant platform:

- Windows (Windows below)
- Linux (Linux below)

Windows

Use the WinMD5 tool to calculate md5 hash or checksum for the file:

Verify the checksum with WinMD5 (see www.WinMD5.com)

Linux

Copy the checksum and the files to a Linux machine, and then run the following command:

md5sum -c filename.md5

The "OK" result should be displayed on the screen (see figure below).

Figure 5-1: ISO File Integrity Verification

```
[root@isocreator VMWare]# 11
total 9959260
-rwx----- 1 root root 58 Nov 1 10:49 0V0C-VMware-7.4.328.md5
-rwx----- 1 root root 10158278656 Oct 31 17:43 0V0C-VMware-7.4.328.ova
[root@isocreator VMWare]#
[root@isocreator VMWare]# md5sum -c OVOC-VMware-7.4.328.md5
OVOC-VMware-7.4.328.ova: OK
```

OVOC Server Users

OVOC server OS user permissions vary according to the specific application task. This feature is designed to prevent security breaches and to ensure that a specific OS user is authorized to perform a subset of tasks on a subset of machine directories. The OVOC server includes the following OS user permissions:

- 'root' user: User permissions for installation, upgrade, maintenance using OVOC Server Managerand OVOC application execution.
- *acems* user: The only available user for login through SSH/SFTP tasks.
- emsadmin user: User with permissions for mainly the OVOC Server Manager and OVOC application for data manipulation and database access.

PostgreSQL user: User permissions for the PostgreSQL database access for maintenance such as installation, patches upgrade, backups and other PostgreSQL database tasks.

In addition the OVOC server includes the following DB operator permissions:

analytics user: User used to connect to Northbound DB access clients

6

Installing OVOC Server on Virtual Machines on Cloud-based Platforms

This section describes how to install the OVOC server on the following Cloud-based platforms:

- Launching Public OVOC Image on Amazon Web Services (AWS) below
- Creating OVOC Virtual Machine on Microsoft Azure on page 26

Launching Public OVOC Image on Amazon Web Services (AWS)

This chapter describes how to create the OVOC virtual machine in an AWS cloud deployment, including the following procedures:

- Launching Public Image on AWS below
- Configuring AWS SES Service on page 23



Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7).

Launching Public Image on AWS

This section describes how to setup and load the AWS image.

> To setup and load the AWS image:

- **1.** Log into your AWS account.
- 2. Choose one of the following regions:
 - eu-central-1 (Frankfurt)
 - us-east-1 N. Virginia)
 - ap-southeast-1 (Singapore)



See https://aws.amazon.com/premiumsupport/knowledge-center/copy-ami-region/ for instructions on how to copy AMIs from one of the provided regions above to any other region that the customer requests.



For verifying AMI IDs, refer to https://services.AudioCodes.com..

Ą	✓ Frankfurt ▲ Suppo
Helpful tips	US East (N. Virginia) US East (Ohio) US West (N. California)
Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now	US West (Oregon) Asia Pacific (Mumbai)
Create an organization Use AWS Organizations for policy-based management of multiple AWS accounts. Start now	Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo) Canada (Central)
Explore AWS Amazon Relational Database Service (RDS) RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.	EU (Frankfurt) EU (Ireland) EU (London) EU (Paris) South America (São Paulo)

Figure 6-1: Select Region

insights and react quickly. Learn more. 🗹

Stream and analyze real-time data, so you can get timely

3. In the "Services" menu, choose EC2.

	Figure	e 6-2:	Services Menu - EC2		
aws	Services 🔺	Res	source Groups 🗸 🔹 🛠		
History		Fin	id a service by name or feature (for exa	ample, E	EC2, S3 or VM, storage).
Console Home					
EC2			Compute	Ē	Management Tools
Billing			EC2		CloudWatch
IAM			Lightsail 🕼		AWS Auto Scaling
			Elastic Container Service		CloudFormation
			Lambda		CloudTrail
			Batch		Config
			Elastic Beanstalk		OpsWorks
					Service Catalog
					Systems Manager
			Storage		Trusted Advisor
			S3		Managed Services
			EFS		
			Glacier	— -	
			Storage Gateway	⊳¦1	Media Services

4. In the Dashboard, navigate to IMAGES > AMIs.

Fig	ure 6-3: Ima	ages
aws	Services	🗸 🛛 Resource Groups 🗸 🔹
EC2 Dashboard	^	Resources
Events	•	You are using the following Amazon Et
Tags		Tou are using the following Amazon Ex
Reports		0 Running Instances
Limits		0 Dedicated Hosts
		0 Volumes
INSTANCES		0 Key Pairs
Instances		0 Placement Groups
Launch Templates		
Spot Requests		
Reserved Instances	s	Learn more about the latest in AW
Dedicated Hosts		
IMAGES		Create Instance
AMIs		To start using Amazon EC2 you will wa
Bundle Tasks		Launch Instance 👻
ELASTIC BLOCK		

5. In the search bar, choose Public images and apply the following filter:

AMI ID : ami-0000000000 replacing ami-0000000000 with the AMI ID you received from AudioCodes according to the region you have chosen.

6. Right-click the AMI and choose Launch.

Public images v	Q AMI ID : ami-050	c84d75ac42949d8 🔊 Add filter			
Name	AMI Name	AMI ID		Source	0
	OVOC_7.4.3081	Launch Spot Request Deregister Register New AMI Copy AMI Modify Image Permissions Add/Edit Tags Modify Boot Volume Setting	949d8	952166219867/	9

Figure 6-4: Launch Public Images

- **7.** Choose an Instance type according to the requirements specified in OVOC Server Minimum Requirements on page 7.
- 8. Configure Instance (Optional). Using this option, you can edit network settings, for example, placement.
- **9.** Configure a Security Group; you should select an existing security group or create a new one according to the firewall requirements specified in the table below:

Table 0-1. Filewall IOI Alliazoff AVV3	Table 6-1:	Firewall for	Amazon AWS
--	------------	--------------	------------

Protocol	Port	Description
UDP	162	SNMP trap listening port on the OVOC server.
UDP	1161	Keep-alive - SNMP trap listening port on the OVOC server used for NAT traversal.
ТСР	5000	Communication for control, media data reports and SIP call flow messages
TCP (TLS)	5001	TLS secured communication for control, media data reports and SIP call flow messages
NTP	123	NTP server port (also configure the AWS IP address/Domain Name as the NTP server on both the managed device and OVOC server; see relevant procedures in Connecting Mediant Cloud Edition (CE) SBC Devices on AWS on page 167

10. Click **Review** and **Launch** > **Review** > **Launch**.

11. In the dialog shown in the figure below, from the drop-down list, choose Proceed without a key pair, check the "I acknowledge ..." check box, then click **Launch Instances**.

```
Figure 6-5: Select an Existing Key Pair
```



12. Click View Instances and wait for the instance to change the state to "running" and the status checks to complete. In the description, note the Public IP address of the instance as highlighted in the figure below.



	i-0bed82bb9	94c0221a8 m4.xlarge	eu-central-1b	running	2/2 checks	None	涛 ec	2-35-156-251-238.eu	35.156.251.238
istance: i-0b	ed82bb94c0221a8	Public DNS: ec2-35-156-	251-238.eu-central	-1.compute.amazor	naws.com				
Description	Status Checks	Monitoring Tags							
	Instance ID	i-Obed82bb94c0221a8			Pub	lic DNS (IPv4)	ec2-35-1	56-251-238.eu-central-1	.compute.amazonaws.
	Instance state	running				IPv4 Public IP	35.156.2	<mark>51.238</mark>	
	Instance type	m4.xlarge				IPv6 IPs	-		
	Elastic IPs					Private DNS	ip-172-3	1-43-55.eu-central-1.com	pute.internal
	Availability zone	eu-central-1b				Private IPs	172.31.4	3.55	
	Security groups	ovoc. view inbound rules			Second	ary private IPs			
	Scheduled events	No scheduled events				VPC ID	vpc-9044	1cbfb	
	AMI ID	OVOC_7.4.3081 (ami-05c84d)	75ac42949d8)			Subnet ID	subnet-a	66befdb	
	Platform				Netv	ork interfaces	eth0		
					-		-		

The AWS public IP address as its later configured in Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS on page 168.

Configuring AWS SES Service

This section describes how to configure the OVOC server as the Email server on Amazon AWS. These steps are necessary in to overcome Amazon security restrictions for sending emails outside of the AWS domain.



If AWS Simple Email Service (SES) runs in Sandbox mode, both sender and recipient addresses should be verified (see https://docs.aws.amazon.com/ses/latest/DeveloperGuide/requestaccess.html)

To configure OVOC as email server on AWS SES:

- **1.** Login to the OVOC server with root permissions.
- **2.** Open file /root/.muttrc:

cat .muttrc

- 3. Replace "OVOC@audiocodes.com" with authenticated source email.
- Open file /etc/exim/exim.conf and using a text editor, find the respective "begin ..." statements and paste the below configuration accordingly
 - Replace : AWS_SES_LOGIN : AWS_SES_PASSWORD with the credentials received from AWS
 - Replace : SOURCE_EMAIL with an authenticated source email address
 - Replace: HOSTNAME with the VM hostname

begin routers
<pre>send_via_ses:</pre>
driver = manualroute
<pre>domains = ! +local_domains</pre>
<pre>transport = ses_smtp</pre>
route_list = * email-smtp.eu-central- 1.amazonaws.com;

begin transports
ses_smtp:
driver = smtp
port = 587
hosts_require_auth = *
hosts_require_tls = *
begin authenticators
<pre>ses_login:</pre>
driver = plaintext
<pre>public_name = LOGIN</pre>
<pre>client_send = : AWS_SES_LOGIN : AWS_SES_PASSWORD</pre>
begin rewrite
<pre>^root@HOSTNAME SOURCE_EMAIL SFfrs</pre>

5. Remove old unsent emails from buffer and restart exim service:

systemctl restart exim
```
exim -bp | exiqgrep -i | xargs exim
-Mrm
rm -rf /var/spool/exim/db/*
```

6. Send test email using mutt:

```
echo "Hello!" > ~/message.txt
mutt -s "Test Mail from OVOC" -F /root/.muttrc EMAIL_ADDRESS <
    ~/message.txt</pre>
```

7. Verify in the exim log in /var/log/exim/main.log to check that the email was sent correctly.

Creating OVOC Virtual Machine on Microsoft Azure

This chapter describes how to install the OVOC server on a virtual machine in a Cloud-based deployment from the Microsoft Azure Marketplace.

- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7).
 - Azure OVOC cannot be deployed using APSS (Azure Partner Shared Services) subscriptions which do not support marketplace offers.

> To install OVOC from the Microsoft Azure Marketplace:

1. In the Azure Marketplace, search for "AudioCodes One Voice Operations Center (OVOC)" and click Get It Now.



2. Click Continue.



Products > AudioCodes One Vo	vice Operations Center		
A audiocodes	AudioCodes One Voice Operations Cen udioCodes verview Plans Reviews	ter	
CET IT NOW W CET IT NOW Au SAVE FOR LAT Categories Analytics Security Management Tools Support Legal License Agreement Privacy Policy Au	Veb-ba Create this app in Azure version AudioCodes One Voice Operations Center velsion By AudioCodes One Voice Operations Center velsion By AudioCodes so singly Software plan AudioCodes One Voice Operations Center (Staged) Details: velsion Details: web-based lifecycle management and monitoring for cloud or premises-based VolP deployments dinitation This app requires some basic profile information. You have provided the information already so you're good to gol Eait	X By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the providers on the they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's terms and privacy statement.	

3. You are now logged in to the Azure portal; click Create.

Figure 6-9: Create Virtual Machine



- **4.** Configure the following:
 - a. Choose your Subscription.
 - b. Choose your Resource Group or create a new one
 - c. Enter the name of the new Virtual Machine.
 - d. Choose the Region.
 - e. Choose the VM Size (see Hardware and Software Requirements).
 - f. Choose Authentication Type "Password" and enter username and user-defined password or SSH Public Key.

Microsoft Azure						
«	Dashboard > AudioCodes One Voice Ope	erations Center (preview) > Create a virtual machine				
+ Create a resource	Create a virtual machine					
🛧 Home						
🔲 Dashboard	Basics Disks Networking Man	agement Advanced Tags Review + create				
i∃ All services	Create a virtual machine that runs Linux or	Create a virtual machine that runc Linux or Windows Salert an imane from Ature marketolace or use your own customized				
+ FAVORITES	image. Complete the Parier tak then Paview + create to provide a victual parchine with default parameters or review each tak for full					
All resources	cumplete the basics tab anen neview + create to provision a virtual machine with denaut parameters of review each tab ion run customization.					
Virtual machines	Looking for classic VMs? Create VM from	Looking for classic VMs? Create VM from Azure Marketplace				
🔯 Images	PROJECT DETAILS					
😂 Disks	Select the subscription to manage deploye your resources.	2d resources and costs. Use resource groups like folders to organize and manage all				
anapshots (2015)	* Subscription 🚯	Newwave AZURE LAB				
🧮 Storage accounts	* Resource group 🙃					
📦 Resource groups	······································	Create new				
↔ Virtual networks	INSTANCE DETAILS)				
🕒 Monitor	★ Virtual machine name 👩	OVOC-7-6-1000 🗸				
Oost Management + Billing	* Region 🛛	West Europe				
	Availability options 👩	No infrastructure redundancy required				
	* Image 🛛	AudioCodes One Voice Operations Center 🗸 🗸				
		Browse all images				
	* Size 🚯	Standard F16s				
		16 vcpus, 32 GB memory Change size				
	ADMINISTRATOR ACCOUNT					
	Authentication type 🚯	Password SSH public key				
	* Username 👩	acovoc 🗸				
	* Password 👩	······				
	* Confirm password					
	V					
	Review + create Previ	ious Next : Disks >				

Figure 6-10: Virtual Machine Details

5. Click Next until Networking section to configure the network settings,

Microsoft Azure		\mathcal{P} - Search resources, services
«	Dashboard > AudioCodes One Voice Op	erations Center (preview) > Create a virtual machine
+ Create a resource	Create a virtual machine	
🛧 Home		
🔲 Dashboard	Basics Disks Networking Mar	nagement Advanced Tags Review + create
i≣ All services	Define network connectivity for your virtu	al machine by configuring network interface card (NIC) settings. You can control
- 🗙 Favorites	ports, inbound and outbound connectivity more	y with security group rules, or place behind an existing load balancing solution. Learn
All resources		
Virtual machines	When creating a virtual machine a netwo	rk interface will be created for you
👰 Images	CONFIGURE VIRTUAL NETWORKS	
😂 Disks	* Virtual network	AUDCvnet295
anapshots 😂		Create new
🧾 Storage accounts	* Subnet	default (10.0.7.0/24)
📦 Resource groups		Manage subnet configuration
↔ Virtual networks	Public IP 📵	(new) OVOC-7-6-1000-ip
🙆 Monitor		Create new
Oost Management + Billing	NIC network security group 🚯	None Basic • Advanced
		1 This VM image has preconfigured NSG rules
	* Configure network security group	(new) OVOC-7-6-1000-nsg V
		Create new
	Accelerated networking 🚯	On Off The selected image does not support accelerated networking.
	You can place this virtual machine in the t	backend pool of an existing Azure load balancing solution. Learn more
	, Discuttion is the large bias is a bias of an	
	Place this virtual machine behind an existing load balancing solution?	V Yes No
	Review + create Prev	ious Next : Management >

Figure 6-11: Network Settings

- a. From the Virtual Network and Subnet drop-down lists, select an existing virtual network/subnet or click **Createnew** to create a new virtual network/subnet.
- **b.** From the Public IP drop-down list, configure "none", use the existing Public IP or create a new Public IP.



If you do not wish the public IP address to change whenever the VM is stopped/started, choose **StaticSKU** or **BasicSKU+ Static**.

c. Under Configure network security group, click Create new to configure a Network Security Group. Configure this group according to the Firewall rules shown in the table below.

By default, only ports 22 and 443 are open for inbound traffic; open other ports for managing devices behind a NAT (outside the Azure environment) as described in the table below.

Protocol	Port	Description
UDP	162	SNMP trap listening port on the OVOC server.
UDP	1161	Keep-alive - SNMP trap listening port on the OVOC server used for NAT traversal.
		This rule is required if Auto-detection is used to add devices in OVOC. See Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on page 160
ТСР	5000	Communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC.
TCP (TLS)	5001	TLS secured communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC. This rule is used if the OVOC Server and managed devices (spe- cifically Mediant CE devices) are deployed in separate Azure Virtual networks communicating behind a firewall. See Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on page 160
NTP	123	NTP server port (set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source. Referenced in procedures in Connecting Mediant Cloud Edi- tion (CE) Devices on Azure on page 159

6. Click Next until **Review+Create** tab, make sure all the settings are correct and click **Create**.

Microsoft Azure				rices, and docs			
«	Dashboard > AudioCodes One Voice Ope	rations Center (preview) > Create a virtual machine					
+ Create a resource	Create a virtual machine						
🛧 Home	Validation bassed						
🛄 Dashboard	Validation passed						
i∃ All services	Rasics Disks Networking Man	agement Advanced Tags Review + create					
- 🗙 FAVORITES	Dasies Disks Networking Man	agement Advanced rags Review Cleate					
All resources	PRODUCT DETAILS						
Virtual machines	AudioCodes One Voice Operations	Pricing not available for this offering					
	Center by AudioCodes						
	Terms of use Privacy policy						
	Standard F16s	Pricing not available for this offering					
Snapshots	Terms of use Privacy policy						
Storage accounts	TERMS						
📦 Resource groups	By clicking "Create", I (a) agree to the legal ten	ms and privacy statement(s) associated with the Marketplace off	fering(s) listed above;				
 Virtual networks 	and (b) agree that Microsoft may share my cor support, billing and other transactional activiti	ntact, usage and transactional information with the provider(s) o es. Microsoft does not provide rights for third-party offerings. Se	ee the Azure				
🕒 Monitor	Marketplace Terms for additional details.						
Ost Management + Billing	Name	Mark Kemel					
	* Preferred e-mail address	Mark.Keme @audiocodes.com	~	🛇 Match found.			
	* Preferred phone number	+97239764373					
			•				
	PACTOC						
	Subscription	Newwave AZURE LAB					
	Resource group	AUDC					
	Virtual machine name	OVOC-7-6-1000					
	Region	West Europe					
	Availability options	No infrastructure redundancy required					
	Authentication type	Password					
	Username	acovoc					
	DISKS						
	OS disk type	Premium SSD					
	Use managed disks	Yes					
	NETWORKING						
	Virtual network	AUDCvnet295					
	Create Previo	Next Download a template for auto	omation				
	·						

7. Navigate to the "Virtual machines" section, where you can, for example, monitor the Virtual Machine creation process and find the Public or Private (Internal) IP addresses to access the Virtual Machine.

Note the public or private (Internal) IP addresses as you need to configure them in Configuring the OVOC Server Manager on Azure (Public IP) on page 160 and Configuring the OVOC Server Manager on Azure (Internal IP) on page 164 respectively.

Microsoft Azure		₽ Search re	sources, services, and docs	>_ 6	
	Dashboard > Virtual machines > OVOC-7-6-1000				
+ Create a resource	Virtual machines « 🖈 ×	OVOC-7-6-1000			\$ >
🟫 Home	+ Add Reservations ···· More	a kunt and a	🗢 Connect 🕨 Start 🤗 Restart 🔳 Stop 🌋 Captur	e 🧰 Delete 💍 Refresh	
🛄 Dashboard)> pearch (ctri+/)			0100.0.0.0.000
E All services	OVOC-7-6-1000	Q Overview	status : Creating	Operating system :	Linux
🛊 FAVORITES	NAME 15	Activity log	Location : West Europe	Size :	Standard F16s (16 vcpus, 32 GB memory)
All resources	QUOC-7-6-1000	📸 Access control (IAM)	Subscription (change) : Newwave AZURE LAB	Public IP address :	40.118.83.214
Virtual machines		🖉 Tags	Subscription ID : d5dcb05d-0f24-4679-970d-3e0309	d2bd79 Private IP address :	10.0.7.10
🐖 Images		X Diagnose and solve problems		Virtual network/subnet :	AUDCvnet295/default
😂 Disks		Settings		DNS name :	Configure
罵 Snapshots		A Networking	Tags (change) Click here to add tags	Ŕ	
Storage accounts		🛎 Disks			
😵 Resource groups		👰 Size	Show data for last: 1 hour 6 hours 12 hours 1 day	y 7 days 30 days	
Virtual networks		Security			
Monitor		Extensions	CPU (average)	Network (total)	\$7
Ost Management + Billing		🐔 Continuous delivery (Preview)	100%	1008	
		🤵 Availability set		808	
		Configuration	60%	605	
		🔥 Identity	20%	208	
		Properties		- 08	
		Locks	4:30 PM 4:45 PM 5 PM 5:15 PM Percentage CPU (Avg)	4:30 PM 4:45 PM 5 PM 5:15 PA Network In Billable Network Out Billable	4
		💷 Export template			
		Operations			
		Q Auto-shutdown	Disk bytes (total)	Disk operations/sec (average)	\$
		ackup	1008	100/s	
		Disaster recovery		355	
		Update management	608	60/1	
		🐊 Inventory	- 425	403	
ttps://portal.azure.com/#home		tracking	08.	0.4	

Figure 6-13: Azure Deployment Process Complete

Deploying Older OVOC Versions using PowerShell

Older OVOC versions can be deployed on Microsoft Azure using PowerShell CLI.

Example

```
az vm create -n OVOC803137 -g OVOC_DEPLOYMENT --image
audiocodes:audcovoc:acovoce4azure:8.0.3137 --size Standard_D8ds_v4 --admin-
username acovoc --admin-password pass_12345678
```

The following OVOC releases can be deployed in the Azure marketplace using PowerShell CLI:

- 7.6.1132
- 7.6.2125
- 7.6.2144
- 7.8.1117
- 7.8.1119
- 7.8.1130
- 7.8.126
- 7.8.2241
- 7.8.2265
- 8.0.1122
- 8.0.1139
- 8.0.114

- 8.0.25468.0.2555
- 8.0.3137
- 8.0.3180
- 8.2.265
- 8.2.265
- 8.2.277
- 8.2.280

7 Installing OVOC Server on VMware Virtual Machine

This describes how to install the OVOC server on a VMware vSphere machine. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Configuring the Virtual Machine Hardware Settings on page 53). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed.

- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the installation.
 - For obtaining the installation files, see OVOC Software Deliverables on page 13
 - ✓ Note that you must verify this file, see Files Verification on page 16

Deploying OVOC Image with VMware vSphere Hypervisor (ESXi)

This section describes how to deploy the OVOC image with the VMware ESXi Web client. This procedure is run using the VMware OVF tool that can be installed on any Linux machine or by running the ESXi wizard. See the following procedures:

- Deploying Standalone VMware VM using ESXi Wizard below
- Deploying OVOC Image with VMware vSphere Cluster on page 38

Deploying Standalone VMware VM using ESXi Wizard

This section describes how to create a Standalone Host VMware machine on VM ESXi Version 7.0.

> To create a VMware VM:

- Transfer the 7z file containing the VMware Virtual Machine installation package that you
 received from AudioCodes to your PC (see Transferring Files on page 328 for instructions on
 how to transfer files).
- 2. Login to the VMware virtual machine on which you wish to install OVOC.
- 3. In the Navigation pane, select Virtual Machines and the right-click Create/Register VM.

/m ware [,] Esxi ^{**}						root@10.3.180.170 +	Help - I Q Search
T Navigator 🗖	localhost.localdomain - Virtual Machines						
✓ ☐ Host Manage	" Create / Register VM 💣 Console 🕨 Power on 📲 Power o	iff 👖 Suspend 🥑 Refresh	Actions				Q. Search
Monitor	Virtual machine	~ Status	 Used space 	 Guest OS 	✓ Host name	✓ Host CPU	✓ Host memory ✓
- 🐉 Virtual Machines 🧐	m vm-high-small	Normal	530 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
👻 🔂 ovoctest 🔂 Virtual machin	200G	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
Monitor 🍪 Create/Regist	ter VM	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
More VMs 📇 Open in new	window Create or register a virtual machine using a wizard	Normal	20.09 GB	CentOS 7 (64-bit)	Unknown	8 MHz	447 MB
Storage	L. B Auto-zpora-172	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
🛛 🧕 Networking 📃 🔹 📃		Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	357 MHz	13.36 GB
	. 57.0_New_189	Normal	524.08 GB	Oracle Linux 7 (64-bit)	Unknown	708 MHz	11.41 GB
	C. 5 171	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	1.5 GHz	20.57 GB
	🗆. 🎒 199_new	Normal	521.05 GB	CentOS 7 (64-bit)	Unknown	339 MHz	13.16 GB
	Control Barrow	-					9 iteme
	Recent tasks Task Target	~ Initia	or V Queued	 Started 	✓ Result ▲		✓ Completed ▼

Figure 7-1: Create/Register VM

The New virtual machine wizard opens.

Figure 7-2: Select Creation Type

🔁 New virtual machine		
✓ 1 Select creation type	Select creation type	
2 Select OVF and VMDK files	How would you like to create a Virtual Machine?	
4 License agreements 5 Deployment options 6 Additional settings	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
7 Ready to complete	Register an existing virtual machine	
vm ware [®]		
		Back Next Finish Cancel

4. Select option **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.

🔁 New virtual machine - ovoctest	
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy Enter a name for the virtual machine. ovoctest Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
	Click to select files or drag/drop
vm ware [®]	
	Back Next Finish Cancel

Figure 7-3: OVF and VMDK Files

5. Enter the name of the virtual machine.

Figure	7-4:	Select OVF or O	VA
--------	------	-----------------	----

🔁 New virtual machine - ovoctest		
✓ 1 Select creation type	• You need to select an OVF or OVA	×
2 Select OVF and VMDK files	Select the OVF and VMDK files or OVA for the VM you would like to deploy	
3 Select storage		
5 Deployment options	Enter a name for the virtual machine.	
6 Additional settings	ovoctest	
7 Ready to complete	Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.	
	× 🚾 OVOC_VMware_8.2.146	
Vinware		
	Back Next Finish C	ancel

6. Click to browse to the saved location of the OVA file and then click **Next**.

🔁 New virtual machine - ovoctest							
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machine's	configuration file:	s and all of its' v	irtual disks.			
	Name	🗸 Capacity 🗸	Free ~	Туре	r Thin pro… ∽	Access	~
	datastore1	3.49 TB	320.08 GB	VMFS6	Supported	Single	
vm ware [*]							
			Ba	ick N	ext Finis	h Ca	incel

Figure 7-5: Select storage

7. Select the relevant Storage Device and then click Next.

Figure 7-6: Deployment options

🔁 New virtual machine - ovoctest			
 ✓ 1 Select creation type ✓ 2 Select OVF and VMDK files ✓ 3 Select storage 	Deployment options Select deployment options		
4 Deployment options 5 Ready to complete	Network mappings	VM Network	Net_10_36 ~
	Disk provisioning	● Thin ○ Thi	nick
	Power on automatically		
vm ware [*]			
			Back Next Finish Cancel

8. Accept default settings for Disk provisioning-thin and Power on automatically-enabled and then click Next.

The Ready to complete screen is displayed.

New virtual machine - ovoctest							
 ✓ 1 Select creation type ✓ 2 Select OVF and VMDK files ✓ 3 Select storage 	Ready to complete Review your settings selection before finishing the wizard						
 ✓ 4 Deployment options ✓ 5 Ready to complete 	Product	ovoc_base_for_8.0.114					
	VM Name Files	ovoctest					
	Datastore	datastore1					
	Provisioning type	Thin					
	Network mappings	VM Network: Net_10_36					
	Guest OS Name Unknown						
vm ware*	Do not refresh your brows	er while this VM is being deployed.					
		Back Next Finish Cancel					

Figure 7-7: Ready to complete

9. Click Finish.

The new Virtual Machine is displayed.



/m ware [,] ESXi ^{,,}						root@10.3.180.170 +	i Help 🗸 i 🔍 Search	
Navigator E	B localhost.localdomain - Virtual Machines							
 Host Manage 	😭 Create / Register VM 👹 Console 🕨 Power on 🔳	Power off 🔢 Suspend 🥑 Refresh	Actions				Q. Search	
Monitor	Virtual machine	✓ Status	 Used space 	✓ Guest OS	✓ Host name	✓ Host CPU	~ Host memory	~
- 🎒 Virtual Machines	9 🔲 💭 👸 vm-high-small	Normal	530 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB	
🕶 🚰 ovoctest	🗆., 🐉 vm-low-200G	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB	
Monitor	🗆. 🎒 ovoctest	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB	
More VMs	C. B vSS8C-188-CentOS8	Normal	20.09 GB	CentOS 7 (64-bit)	Unknown	7 MHz	443 MB	
Storage	1 D. B Auto-zipora-172	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB	
2 Networking	2 🌆 ovoc_8.2_500G_188	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	3.6 GHz	13.48 GB	
	. m 7.0_New_189	Normal	524.08 GB	Oracle Linux 7 (64-bit)	Unknown	596 MHz	12.1 GB	
	🗆. 🏚 171	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	1.6 GHz	20.6 GB	
	🗆. 👸 199_new	📀 Normal	521.05 GB	CentOS 7 (64-bit)	Unknown	494 MHz	11.94 GB	
	Recent tasks							
	Task ~ Target	✓ Init	ator ~ Que	ued v Started	✓ Result ▲		 Completed • 	

Deploying OVOC Image with VMware vSphere Cluster

This section describes how to deploy the OVOC image in a cluster with the VMware ESXi Web client. This procedure is run using the VMware OVF tool that can be installed on any Linux machine.

- This procedure describes how to deploy the image using the OVF tool, which can be downloaded from: https://www.vmware.com/support/developer/ovf/
 - The OVOC image can also be deployed using the vSphere web client GUI.

> To run VMware OVF tool:

- Transfer the 7z file containing the VMware Virtual Machine installation package that you
 received from AudioCodes to your PC (see Transferring Files on page 328 for instructions on
 how to transfer files).
- 2. Open the VMware OVF tool.
- 3. Enter the following commands and press Enter:

```
ovftool --disableVerification --noSSLVerify --name=$VMname --
datastore=$DataStore -dm=thin --acceptAllEulas --powerOn $ovaFilePath
vi://$user:$password@$vCenterIP/$dataCenterName/host/$clusterName/$ESXIHost
Name
```

Where:

- \$VMname(--name): is the name of the deployed machine
- \$DataStore: data store for deployment
- \$user:\$password is the user and password of the VMware Host machine
- \$ESXIHostName: deployed ESXI IP Address

Example:

```
ovftool --disableVerification --noSSLVerify --name=ovoctest --
datastore=Netapp04.lun1 -dm=thin --acceptAllEulas --powerOn c:\tmp\OVOC_
VMware_.ova vi://vmware:P@ssword123@host/10.3.180.170
```

Tophere Client					1111010804344400	V V	
0 0 9 9	10.3.180.20 ACTIONS -						
qasswcenter01.corp.audioc QassWDatacenter QassWDatacenter QassCluster01	Summary Monitor Configure Permissions VMs Datastores Networks Virtual Machines VM Templates						
0.3.180.20						Etter	
0.3.180.212	Name 1	v State v St	atus v Provisioned Space	v Used Space	V Host CPU	Host Mem	~
ARM-Conf_9.6.12-1	ARM-Conf. 9.6.12-10.3.180.241	Powered On	Alert 96.14 GB	96.14 GB	72 MHz	12.94 GB	
ARM-Router_9.6.12	ARM-Router_9.6.12-10.3.180.242	Powered On	Alert 48.14 GB	48.14 GB	24 MHz	5.54 GB	
ARM-ROUTEF_9.0.12	ARM-Router_9.6.12-10.3180.243	Powered On	Alert 48.14 GB	48.14 GB	24 MHz	5.54 GB	
EMS 6.6	B OVOC_High_200	Powered Off	Normal 1.2 TB	1.07 TB	0 Hz	08	
oit 🚯	B OVOC_high_233	Powered On	Alert 1.2 TB	1.2 TB	600 MHz	31.96 GB	
DVOC_High_200	B OVOC_Jow_199	Powered Off	Normal 524.21 GB	500.01 GB	0 Hz	0.8	
BOVOC_high_233	B ovoc_low_237	Powered Off	Normal 1.2 TB	582.96 GB	0 Hz	08	
DVOC_low_199	B OVOC_Low_239	Powered Off	Normal 524.19 GB	500 GB	0 Hz	0.8	
🖞 OVOC_Low_220 (d	B SBC-HAriso	Powered On	Alert 24.13 GB	24.13 GB	264 MHz	3.46 GB	
ovoc_low_237	test_deployment	Powered On	Alert 524.1 GB	119.43 GB	408 MHz	24.09 GB	
CVOC_Low_239	Center	Powered On	Alert 312.09 GB	225.98 GB	312 MHz	12.07 GB	
e test_deployment							
					Ć	🕒 Export 11	v items
ecent Tasks Alarms							
	Det Statur	Deta	ils 🛧	 Initiator 	 Start Time 	~ Cor	opletion

Figure 7-9: OVF Example

The following progress is displayed:

< All Y

Opening OVA source: /data1//DVD5/.xxxx/OVOC-VMware-.xxxx.ovaOpening VI target: vi://root@172.17.135.9:443/Deploying to VI: vi://root@172.17.135.9:443/Disk progress: 10%

```
Transfer CompletedThe manifest validatesPowering on VM: FirstDeployTask
CompletedWarning:- No manifest entry found for: 'OVOC-VMware-.xxxx-
disk1.vmdk'.Completed successfully
```

Configuring the Virtual Machine Hardware Settings

This section shows how to configure the Virtual Machine's hardware settings. Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see Hardware and Software Requirements.

Table 7-1:	Virtual	Machine	Configuration
------------	---------	---------	---------------

Required Parameter	Value
Disk size	
Memory size	
CPU cores	

> To configure the virtual machine hardware settings:

1. Before powering up the machine, go to the virtual machine Edit Settings option.

vmware: ESXi							root@10.3.180.170 +	Help - I Q Search -
Navigator 🗉	🚯 ovoctest							
✓ ☐ Host Manage Monitor	Power	on 📮 Power off 🕕 Suspend 😋 Rese	t 📝 Edit 🖉 Refresh 🔅 Actio	ns			L.	0 00
Virtual Machines Soverest Monitor More VMs Storage Storage Soverest Sove		Guest OS Compatbility Vithuare Tools CPUs Memory	CentOS 7 (64-Jat) ESX 6.7 virtual machine No 1 24 GB					54 MHz
	VMware Tools is not installed in General Information	C this virtual machine. VMware Tools allows e	detailed guest information to be displaye	d as well as allow	ing you to perform	operations on the gue	st OS, e.g. graceful shutdown, reboot, etc. You should install VMware	Tools. 😨 Actions 🛛 ×
	Networking				D CPU		1 vCPUs	
	+ 📾 VMware Tools	VMware Tools is not installed.		Actions	Memory		24 GB	
	Storage	1 disk			Hard dis	k1	500 GB	
	Notes			/ Edit notes	USB con	troller	USB 2.0	
					INE Network	adapter 1	VM Network (Connected)	
	* Performance summary last hour				Video ca	rd	16 MB	
			Consumed host CPU		+ 🕤 CD/DVD	drive 1	ISO [datastore1] iso/DVD1_CentOS7_Linux_Rev19.iso	🕽 Select disc image
	100 @	•	Consumed host memory	20 8	Im Others		Additional Hardware	
	Recent tasks							
	Task	~ Target	 Initiator 	~ Queued		 Started 	~ Result .	Completed • ·
	Power On VM	🔐 vm-low-2003	1001	08/27/2022 14:2	:30	00/27/2022 14:22:30	Failed - The attempted operation cannot be performed in the c	00/27/2022 14:22:30
	Power On VM	👘 vm-low-2003	root	08/27/2022 14:2	:31	00/27/2022 14:20:31	Failed - The attempted operation cannot be performed in the c	00/27/2022 14:20:31
	Power Off VM	B 171	root	08/27/2022 14:2	08	06/27/2022 14:20:06	Completed auccessfully	08/27/2022 14:20:11
	Power On VM Research VM	(1) vm-low-2003	root	06/27/2022 14/2	100	06/27/2022 14:20:00	Pated - The attempted operation cannot be performed in the c Completed executivity	06/27/2022 14:20:09
	Power On VM	@ 7.0_New_180	root	08/27/2022 12:5	:27	06/27/2022 12:23:27	Completed successfully	06/27/2022 12:23:27

2. In the CPU, Memory and Hardware tabs set the required values accordingly to the desired OVOC server VMware Disk Space allocation. (Hardware and Software Specifications on page 7), and then click OK.

🖆 Edit settings - ovoctest (ESXi 6.7 virtual machine)								
Virtual Hardware VM Options							-	
🔜 Add hard disk 🛛 🛤 Add network ada	apter 📑 Add o	other device						
► 🔲 CPU	1 ~ (
► Memory	24		~					
► 🛄 Hard disk 1	500	GB	~				8	
► 🚱 SCSI Controller 0	VMware Para	virtual						
SATA Controller 0							8	
🖶 USB controller 1					~		8	
Network Adapter 1	VM Network				✓ Connect		8	
▶ i CD/DVD Drive 1	Datastore ISO) file			 Connect 		8	
▶ 🛄 Video Card	Dofault cotting	10						
						Save	Cancel	

Figure 7-11: CPU, Memory and Hard Disk Settings

- Once the hard disk space allocation is increased, it cannot be reduced to a lower amount.
- If you wish to create OVOC VMs in a cluster environment supporting High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (Configuring OVOC Virtual Machines (VMs) in a VMware Cluster on the next page).

3. Wait until the machine reconfiguration process has completed.

Figure	7-12.	Recent	Tasks
IIguic	/-12.	Necent	1 0 3 1 3

😨 Recent tasks						
Task ~	Target ~	Initiator	Queued	Started	Result	Completed • V
Power Off VM	街 199_new	root	06/27/2022 10:08:28	06/27/2022 10:08:28	Ocmpleted successfully	06/27/2022 10:08:33
Upload disk - OVOC_VMware_8.0.114	ovoctest1	root	06/26/2022 15:41:43	06/26/2022 15:41:43	Ocmpleted successfully	06/26/2022 16:53:02
Import VApp	Resources	root	06/26/2022 15:38:51	06/26/2022 15:38:51	Ompleted successfully	06/26/2022 16:50:16
Destroy	ovoctest1	root	06/26/2022 15:39:12	06/26/2022 15:39:12	Ocmpleted successfully	06/26/2022 15:39:14
Create VM	ovoctest1		06/26/2022 15:38:51	06/26/2022 15:38:51	Completed successfully	06/26/2022 15:38:51
Reconfig VM	F ovoctest	root	06/28/2022 13:08:47	06/28/2022 13:08:47	Completed successfully	06/28/2022 13:08:47

Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

This section describes how to configure OVOC VMs in a VMware cluster.

VMware Cluster Site Requirements

Ensure that your VMware cluster site meets the following requirements:

- The configuration process assumes that you have a VMware cluster that contains at least two ESXi servers controlled by vCenter server.
- The clustered VM servers should be connected to a shared network storage of type iSCSI or any other types supported by VMware ESXi.

For example, a datastore "QASWDatacenter" which contains a cluster named "qaswCluster01" and is combined of two ESXi servers (figure below).

Verify that Shared Storage is defined and mounted for all cluster members:

Figure 7-13: Storage Adapters

10.3.180.211 Actions -									
Summary Monitor Manage	Related Objects								
Settings Networking Storage	Aarm Definitions Tags Per	missions Scheduled	Tasks Up	date Manager					
	Storage Adapters								
Storage Adapters	+ 🖬 💷 🔯 🗛 -							Q Filter	
Storage Devices	Adapter	Type	Status	Identifier	Targets	Devices	Paths		
Host Cache Configuration	Patsburg 4 port SATA IDE C	Controller							
Protocol Endpoints	Ø vmhba32	Block SCSI	Unknown		0	0	0		
	💿 vmhba1	Block SCSI	Unknown		1	1	1		
	Smart Array P420i								
	🐼 vmhba0	Block SCSI	Unknown		1	1	1		
	ISC SI Software Adapter								
	🔕 vmhba33	ISCSI	Online	ign.1998-01.com.vmware:10.3.180.211	1	2	2		
	Adapter Details			-					
	Properties Devices P	aths Targets Netw	ork Port Bind	ing Advanced Options					
	Adapter Status								Disable
	Status Enabled								
	General								Edit
	Name vmh	ba33							
	Model ISC:	SI Software Adapter							

Ensure that the 'Turn On vSphere HA' check box is selected:

Figure 7-14: Turn On vSphere HA



Ensure that HA is activated on each cluster node:



ummary Monitor	Manage Relat	ted Objects					
7							
	10.3.180.211 Type: Model: Processor Type: Logic al Processors: NICs:	ESXI HP ProLiant DL360p Gen8 Intel(R) Xeon(R) CPU E5-2 20 4	1 1680 v2 @	2.80GHz			
Virtual Machines: 6 State: Connected Uptime: 29 days Image: Connected Uptime: 29 days							
 Hardware 			• C	onfiguration			
Manufacturer	HP		ES	X/ESXi Version	VMware ESXi, 6.0.0, 3620759		
Model	ProLiant	t DL360p Gen8	Ima	age Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5	5.0.48	
CPU	10 C	PUs x 2.79 GHz	▶ vSp	phere HA State	 Running (Master) 		
Memory	70,63	39 MB / 98,269 MB	▶ Fai	ult Tolerance (Legacy)	Unsupported		
🕨 🔚 Virtual Flash F	Resource 0.00	B / 0.00 B	▶ Fai	ult Tolerance	Unsupported		
Networking	localhos	t.corp.audiocodes.com	► EV	C Mode	Intel® "Sandy Bridge" Generation		
Storage	3 Datas	tore(s)	- R	elated Objects			
 Tags 			Clust	er 🚺 qaswCluster	01		
 Update Manage 	r Compliance	_	1		More	Related Objects	

Ensure that the networking configuration is identical on each cluster node:

Navigator I	10.3.180.211 Actions -		Z *
(Hosts and Clusters) 🔊	Summary Monitor Manage	Related Objects	
Construction Constend Constend Constructin Constructin Construct	Settings Networking Storage Virtual switches Virkernel adapters Proysical adapters	Mam. Definitions Tags Permissions Scheduled Tasks Update Manager Virtual switches Image: Compare Scheduled Tasks Update Manager Switch Image: Compare Scheduled Tasks Descreted Naces Switch Image: Compare Scheduled Tasks Descreted Naces Switch Image: Compare Scheduled Tasks Descreted Naces Switch Image: Compare Scheduled Tasks Descreted Naces	
	TCP/IP-configuration Advanced	Standard switch: vSwitch0 (Munagement Network)	۲

Figure 7-16: Networking

Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

Figure 7-17: Switch Properties



A VM will be movable and HA protected only when its hard disk is located on shared network storage on a cluster. You should choose an appropriate location for the VM hard disk when you deploy the OVOC VM. If your configuration is performed correctly, a VM should be marked as "protected" as is shown in the figure below:

Navigator	Actions =			
	DD COM-1.2.2033 Actions -			
Hosts and Clusters	Getting Started Summary Mo	onitor Manage Related Objects		
		Low -7.4.268		
👻 📴 qaswvcenter01.corp.audiocode		Guest OS: CentOS 4/5/6/7 (64-bit)		
▼ QASWDatacenter		Compatibility: ESXi 5.0 and later (VM	version 8)	
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓		VMw are Tools: Running, version:1024	6 (Current)	
10.3.180.211		DNS Name: VMw are-low		
10.3.180.212	Powered On	PAddresses: 10.3.180.201		
1.2.2123	Launch Remote Console	Host: 10.3.180.211		
EMS 203-7.2.2123	Download Remote Console	Α 🗛 🖪		
High-7.2.2055				
High217-LyDS-7.2.2110	 VM Hardware 		▼ VM Storage Policies	
🐴 Low-7.2.2055 🔉	Advanced Configuration	-	VM Storage Policies	
SSBC_01	(VM Storage Policy Compliance	
SSBC_02	 Notes 		Last Checked Date -	
SSBC_03	 VM Failure Response 		Check Compliance	
W vCenter	Failure	Failure response		
VEMS 7.2.1000	Host failure	Restart	► Tags	
	Host network isolation	Leave powered on	► Related Objects	
	Datastore under PDL	Disabled	✓ vApp Details	
	Datastore under APD	Disabled	Product	
	Guest not heartbeating	Ignore heartbeats	Version	
	vSphere HA Pro	tection: Protected	Vendor	
	 Update Manager Compliand 	ce 🛛 🖉 Prote	cted	
	Status 😵 Non-Compliant	vSphere	will attempt to restart the VM after supported failure.	
		Scan Detailed Status		
				_

Figure 7-18: Protected VM

If you wish to manually migrate the OVOC VMs to another cluster node, see Managing Clusters on page 310.

Cluster Host Node Failure on VMware

In case a host node where the VM is running fails, the VM is restarted on the redundant cluster node automatically.

When one of the cluster nodes fail, the OVOC VM is automatically migrated to the redundant host node. During this process, the OVOC VM is restarted and consequently any active OVOC process is dropped. The migration process may take several minutes.

Connecting OVOC Server to Network on VMware

After installation, the OVOC server is assigned a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network interface card connected to the 'trusted' virtual network switch during the OVOC server installation. You need to change this IP address to suit your IP addressing scheme.

> To connect to the OVOC server:

 Power on the machine; in the vCenter tree, right-click the AudioCodes One Voice Operations Center node (vOC) and in the drop-down menu, choose Power > Power On. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications (Hardware and Software Specifications on page 7).



Figure 7-19: Power On

- 2. Wait until the boot process has completed, and then connect the running server through the vSphere client console.
- 3. Login into the OVOC server by SSH, as 'acems' user and enter *acems* password.
- 4. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

- 5. Proceed to the network configuration using the OVOC Server Manager.
- 6. Type the following command and press Enter.

OvocServerManager

- **7.** Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify login to OVOC Web client is successful.
- Set the OVOC server network IP address to suit your IP addressing scheme (Server IP Address on page 228).
- **9.** Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 198).

This page is intentionally left blank.

8 Installing OVOC Server on Microsoft Hyper-V Virtual Machine

This section describes how to install the OVOC server on a Microsoft Hyper-V virtual machine.

- Before proceeding, ensure that the minimum platform requirements are met (see .Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the installation.
 - For obtaining the installation files, see OVOC Software Deliverables on page 13
 Note that you must also verify the ISO file, see Files Verification on page 16

> To install the OVOC server on Microsoft Hyper-V:

- Transfer the ISO file containing the Microsoft Hyper-V Virtual Machine installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 328 for instructions on how to transfer files).
- Open Hyper-V Manager by clicking Start > Administrative Tools > Hyper-V Manager; the following screen opens:

illa -	Hyper-V Manager	_ _ ×
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp		
(+ +) 2 🖬 🛛 🖬		
📑 Hyper-V Manager		Actions
WIN-VO01RE7B70M	ichines	WIN-VO01RE7B70M
Name	State CPU Usage Assigned Memory Uptime Status R3_HA1 Running 7 % 4128 MB 20:17:00	New New New Import Virtual Machine Hyper-V Settings
		If yper-v sectings If your v sectings
<	III	 Edit Disk Inspect Disk
<u>C</u> heckpoir	ts	Stop Service
	No virtual machine selected.	X Remove Server
		View 🕨
		2 Help
Details		
	No item selected.	
	Ad Ge	tivate Windows te System in Control Panel to activa

Figure 8-1: Installing the OVOC server on Hyper-V – Hyper-V Manager

Start the Import Virtual Machine wizard: click the Action tab, and then select Import
 Virtual Machine from the menu; the Import Virtual Machine screen shown below opens:

	Import Virtual Machine				
Before You E	Begin				
Before You Begin Locate Folder	This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.	n			
Choose Import Type Summary					
	Do not show this page again				
	< <u>Previous</u> <u>Next</u> > Einish Cancel				

Figure 8-2: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard

4. Click Next; the Locate Folder screen opens:

2	Import Virtual Machine	x
Locate Folder		
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	Specify the folder containing the virtual machine to import. Folder: :::::::::::::::::::::::::::::::::::	Browse
	< Previous Next > Finish	Cancel

Figure 8-3: Installing OVOC server on Hyper-V – Locate Folder

- Enter the location of the VM installation folder (extracted from the ISO file), and then click Next; the Select Virtual Machine screen opens.
- 6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

7	Import Virtual Machine					
Choose Impo	Choose Import Type					
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	Choose the type of import to perform: Register the virtual machine in-place (use the existing unique ID) Restore the virtual machine (use the existing unique ID) Copy the virtual machine (create a new unique ID) 					
	< <u>P</u> revious <u>N</u> ext > Einish Cancel					

Figure 8-4: Installing OVOC server on Hyper-V – Choose Import Type

7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

2	Import Virtual Machine	x				
Choose Fold	ers for Virtual Machine Files					
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination	You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.					
Choose Destination Choose Storage Folders Summary	C:\ProgramData\Microsoft\Windows\Hyper-V\ C:\ProgramData\Microsoft\Windows\Hyper-V\ Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V\	Browse Browse Browse				
	< <u>Previous</u> <u>N</u> ext > Einish	Cancel				

Figure 8-5: Installing OVOC server on Hyper-V – Choose Destination

8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

Machine						
Choose Folders to Store Virtual Hard Disks						
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	Where do you want to store the imported virtual hard disks for this virtual machine? Location: C:\Users\Public\Documents\Hyper-V\Wirtual Hard Disks\ Browse					
	< Previous Next > Einish Cancel					

Figure 8-6: Installing OVOC server on Hyper-V – Choose Storage Folders

- **9.** Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.
- **10.** Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

Figure 8-7: File Copy Progress Bar

This process may take approximately 30 minutes to complete.



11. Proceed to Configuring the Virtual Machine Hardware Settings below.

Configuring the Virtual Machine Hardware Settings

This section shows how to configure the Virtual Machine's hardware settings.

Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see Hardware and Software Requirements.

Table 8-1: Virtual Machine Configuration

Required Parameter	Value
Disk size	
Memory size	
CPU cores	

To configure the VM for OVOC server:

1. Locate the new OVOC server VM in the tree in the Hyper-V Manager, right-click it, and then select **Settings**; the Virtual Machine Settings screen opens:

Figure 8-8: Adjusting VM for OVOC server – Settings - Memory

2. In the Hardware pane, select **Memory**, as shown above, enter the 'Startup RAM' parameter as required, and then click **Apply**.

3. In the Hardware pane, select **Processor**; the Processor screen shown in the figure below opens.

OC_QA_High Image: Construction of the co	Setting for OVOC_QA_High on QAHYPERV1				
▲ Hardware Add Hardware BIOS BiOS Boot from CD Biot from CD Wemory 20000 MB Processor 6 Withuel processors BIDE Controller 0 Biot from CD Wemory 20000 MB Biot from CD Forcessor Biot from CD 6 Withuel processors Biot from CD Forcessor Biot for fored Forcessor	OC_QA_High	✓ ▲ ▶ Q.			
None [™] COM 2 None [™] Diskette Drive None [™] Diskette Drive None [™] Management [™] Name OVOC_QA_High [™] Integration Services Some services offered [™] Smart Paging File Location C: \ClusterStorage\volume1\0VOC [™] Automatic Start Action None	 ★ Hardware M Add Hardware BIOS Boot from CD ■ Memory 20000 MB ■ Processor 6 Virtual processors ■ IDE Controller 0 ■ Hard Drive OVOC_QA_High.vhdx ■ IDE Controller 1 OVOC_QA_High.vhdx ■ IDE Controller 1 OVD Drive None SCSI Controller ■ Network Adapter Virtual Switch 1 ▼ COM 1 	 Processor You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings. Number of virtual processors: 6 ↔ Resource control You can use resource controls to balance resources among virtual machines. Virtual machine reserve (percentage): 100 Percent of total system resources: 37 Virtual machine limit (percentage): 100 Percent of total system resources: 37 Relative weight: 100 			
OK Carrel Andy	None COM 2 None Diskette Drive None None None None None None None Non	Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.			

Figure 8-9: Adjusting VM for OVOC server - Settings - Processor

- 4. Set the 'Number of virtual processors' parameters as required.
- 5. Set the 'Virtual machine reserve (percentage)' parameter to **100%**, and then click **Apply**.
 - Once the hard disk space allocation is increased, it cannot be reduced.
 - If you wish to create OVOC VMs in a Cluster environment that supports High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster on page 61).

Expanding Disk Capacity

The OVOC server virtual disk is provisioned by default with a minimum volume. In case a higher capacity is required for the target OVOC server then the disk can be expanded.

> To expand the disk size:

- **1.** Make sure that the target OVOC server VM is not running Off state.
- 2. Select the Hard Drive, and then click Edit.

Figure 8-10: Expanding Disk Capacity

OC_test-new	~	۹ 🕨	Q		
OC_test-new Hardware Add Hardware Add Hardware BIOS Boot from CD Memory 4096 MB Frocessor 1 Virtual processor 1 Virtual processor 1 DE Controller 0 Frocessor DVD Drive None SCSI Controller None COM 1 None COM 2 None None		Ha You car operati virtual u Control IDE Co Media You by e IDE Co To rem delete	A A A C A C A C A C A C A C	hard disk is attached to the vi his disk, changing the attachn Location: 0 (in use) pand, merge, reconnect or sh Specify the full path to the file ts \Hyper-V\Virtual Hard Disks Edit Insp 0 Target 0 \v isk you want to use is not list sk Management on the physic click Remove. This disconnect	rtual machine. If an hent might prevent the v rink a virtual hard disk c. ovoc_test.vhdx ect Browse ed, make sure that the al computer to manage s the disk but does not
None Management Name OVOC_test-new Integration Services Some services offered Checkpoint File Location C:\ProgramData\Wicrosoft\Win Smart Paging File Location C:\ProgramData\WicrosoftWin					Remove

The Edit Virtual Disk Wizard is displayed as shown below.

	Edit Virtual Hard Disk Wizard	x
Locate Virtu	al Hard Disk	
Before You Begin Locate Disk Choose Action Summary	 Where is the virtual hard disk file located? Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ovoc_test.vhdx Browse Editing the following types of virtual hard disks might result in data loss: Virtual hard disks in a differencing disk chain that have child virtual hard disks associated with them. Virtual hard disks (.avhd/.avhdx) associated with virtual machine checkpoints. Virtual hard disks associated with a virtual machine that has replication enabled and is currently involved in initial replication, resynchronization, test failover, or failover. 	
	< Previous Next > Finish Cancel	

Figure 8-11: Edit Virtual Hard Disk Wizard

3. Click Next; the Choose Action screen is displayed:

ø	Edit Virtual Hard Disk Wizard
Choose Action	DN
Before You Begin Locate Disk Choose Action Configure Disk Summary	 What do you want to do to the virtual hard disk? Compact This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same. Convert This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk. Expand This option expands the capacity of the virtual hard disk.
	< Previous Next > Finish Cancel

Figure 8-12: Edit Virtual Hard Disk Wizard-Choose Action

4. Select the Expand option, and then click Next; the Expand Virtual Hard Disk screen opens.

ø	Edit Virtual Hard Disk Wizard		
Expand Virtual Hard Disk			
Before You Begin Locate Disk Choose Action Configure Disk Summary	What size do you want to make the virtual hard disk? Current size is 170 GB. New size: 300 GB (Maximum: 64 TB)		
	< Previous Next > Finish Cancel		

Figure 8-13: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk

5. Enter the required size for the disk, and then click **Next**; the Summary screen is displayed.

ø	Edit Virtual Hard Disk Wizard	x			
Completing t	Completing the Edit Virtual Hard Disk Wizard				
Before You Begin Locate Disk Choose Action Configure Disk Summary	You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to make the following changes. Description: Virtual Hard Disk: OC_test.vhdx (VHDX, dynamically expanding) Action: Expand Configuration: New virtual disk size: 300 GB To complete the action and close the wizard, click Finish.				
	< Previous Next > Finish Cancel]			

Figure 8-14: Edit Virtual Hard Disk Wizard-Completion

- 6. Verify that all of the parameters have been configured, and then click **Finish**. The settings window will be displayed.
- 7. Click OK to close.

Changing MAC Addresses from 'Dynamic' to 'Static'

By default, the MAC addresses of the OVOC server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license.

To prevent this from occurring, MAC Addresses should be changed from 'Dynamic' to 'Static'.

- > To change the MAC address to 'Static' in Microsoft Hyper-V:
- 1. Shutdown the OVOC server (Shutdown the OVOC Server Machine on page 225).
- 2. In the Hardware pane, select Network Adapter and then Advanced Features.
- 3. Select the MAC address 'Static' option.
- 4. Repeat steps 2 and 3 for each network adapter.

2	Settings for OVOC-QA on QAHYPERV1	x
OC-QA	✓ 4 ▶ Q	
 ★ Hardware ★ Add Hardware ▲ BIOS Boot from CD ■ Memory 4096 MB ■ Processor 1 Virtual processor ■ IDE Controller 0 ■ IDE Controller 0 ■ Controller 0 ■ Controller 0 	Advanced Features MAC address Dynamic	~
	DHCP guard DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers. □ Enable D <u>H</u> CP guard	=
COM 2 None Diskette Drive	Router guard Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.	
Management Name OVOCQA Integration Services Some services offered	Protected network Move this virtual machine to another cluster node if a network disconnection is detected. Protected network	
Checkpoint File Location C:\ClusterStorage\Volume1\0V0 Smart Paging File Location C:\ClusterStorage\Volume1\0V0 Automatic Start Action	Port mirroring Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring. V Mirroring mode: None V	~

Figure 8-15: Advanced Features - Network Adapter – Static MAC Address

Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster

This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

Hyper-V Cluster Site Requirements

Ensure that your Hyper-V cluster site meets the following requirements:

- The configuration process assumes that your Hyper-V failover cluster contains at least two Windows nodes with installed Hyper-V service.
- The cluster should be connected to a shared network storage of iSCSI type or any other supported type. For example, "QAHyperv" contains two nodes.
| 灎 | | Fail | over Cluster Manag | ger | |
|--|------------------------------------|------------------------|-------------------------|------------------------|-----------------|
| Eile Action View Hels | p | | | | |
| Failover Cluster Manage | Nodes (2)
Search | | | ام | Queries 🔻 🕁 👻 😒 |
| Koles
Nodes
Storage
Bisks
Pools
Networks
Bi Cluster Events | Name
R QAHyperV1
R QAHyperV2 | Status
(Up
(Up | Assigned Vote
1
1 | Current Vote
1
1 | Information |
| < III > | <
• | | | | |

Figure 8-16: Hyper-V-Failover Cluster Manager Nodes

The OVOC VM should be created with a hard drive which is situated on a shared cluster storage.

Add the OVOC VM in Failover Cluster Manager

After you create the new OVOC VM, you should add the VM to a cluster role in the Failover Cluster Manager.

> To add the OVOC VM in Failover Cluster Manager:

1. Right-click "Roles" and in the pop-up menu, choose Configure Role.

嶘				Failover Clus	ter Manager		
<u>F</u> ile <u>A</u> ction <u>V</u> i	ew <u>H</u> elp						
🗢 🄿 🔁 📰	?						
🗟 Failover Cluste	r Manage Roles (2)						
⊿ 🎲 QAHyperv	-Cl.corp.a Search						🔎 Queries 🔻 🔛 👻 👽
Noc	Configure Role		Status	Туре	Owner Node	Priority	Information
⊿ 📇 Stor	Virtual Machines	•	Running	Virtual Machine	QAHyperV1	Medium	
	Create Empty Role		Running	Virtual Machine	QAHyperv2	Medium	
Net Net	View	•					
E Clus	Refresh						
	Help						

Figure 8-17: Configure Role

2. In the Select Role window, select the Virtual Machine option and then click Next.

	-						
- <u>8</u>		Failover Cluster Manager					
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> e	elp						
🗢 🔿 🖄 📅 🛛 🖬							
📲 Failover Cluster Manag	Roles (2)						
⊿ 🎲 QAHyperv-Cl.corp.:	.a Search					🔎 Queries 🔻	
Nodes	Name	Status	Type	Owner Node	Priority	Information	
🛛 📇 Storage	ào		High Ava	ilability Wizard			×
B Pools	~		mgnAva			_	
Networks	Select R	ole					
	Before You Begin Select Role	Select the role	that you want to confi	gure for high availability	K.		
	Select Virtual Machine	Generic Se	rvice eplica Broker		 Description: A situal machine 	a ie a uistualizad	
	Confirmation	GrisCSI Targ	et Server		computer system	n running on a physical	
	Availability	Message Q	ar Jueuing		run on one com	puter.	
	Summary	C Other Serve	er kine		=		
		WINS Serv	/er		_		<u>iy node</u>
					~		
							=
					Province	t) Canod	
					Nex Nex	Cancel	

Figure 8-18: Choose Virtual Machine

A list of available VMs are displayed; you should find the your new created OVOC VM:

Figure 8-19: Confirm Virtual Machine

<u>u</u>			Failover Cl	uster Manag	er	
File Action View Help Image: Constraint of the second seco						
 Hailover Cluster Manage ▲ 2000 QAHyperv-Cl.corp.a ■ Roles 	Roles (2) Search					🔎 Queries 🔻 📘
Nodes	Name	Status	Туре	Owner No	de Pric	prity Information
Disks	8 0		High Availa	bility Wizard	l	X
📑 Pools 🐃 Networks 🔝 Cluster Events	Select Virt	ual Machine				
	Before You Begin Select Role	Select the virtual m	achine(s) that you war	nt to configure for	high availability.	
	Select Virtual Machine	Name		Status	Host Server	
	Confirmation			Uff	QAHyperV I.c	corp.audiocodes.com
	Configure High Availability					
	Summary					
l i	-	Shutdown S	ave			<u>Refresh</u>
	-					
				_		
					< <u>P</u> revious	<u>N</u> ext > Cancel

3. Select the check box, and then click Next.

At the end of configuration process you should see the following:

Figure 8-20: Virtual Machine Successfully Added

剱	High Availability Wizard	x
Summary		
Before You Begin Select Role	High availability was successfully configured for the role.	
Select Virtual Machine	EN	
Confirmation	Virtual Machine	
Configure High Availability	All of the virtual machine configurations chosen were successfully made highly	
Summary	available.	
	Name Result Description	
	OVOC Success	
		~
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	rt
	<u> </u>	h

4. Click Finish to confirm your choice.

Now your OVOC VM is protected by the Windows High Availability Cluster mechanism.

If you wish to manually move the OVOC VMs to another cluster node, see Appendix Managing Clusters on page 310.

Cluster Host Node Failure on Hyper-V

In case a host node where the VM is running fails, then the VM is restarted on the redundant cluster host node automatically.

When one of the cluster hosts fails, the OVOC VM is automatically moved to the redundant server host node. During this process, the OVOC VM is restarted and consequently any running OVOC process are dropped. The move process may take several minutes.

Connecting OVOC Server to Network on HyperV

After installation, the OVOC server is assigned, a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network

interface card connected to the 'trusted' virtual network switch during the OVOC server installation. You need to change this IP address to suit your IP addressing scheme.

To reconfigure the OVOC server IP address:

1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

V <u>i</u> rtual Machines					
Name	State	CPU	Usage	Assigned Memory	l
Stress_tool SSBC_AlexR3_HA1 SSBC_AlexR2_HA2 SSBC_AlexR2_HA1	Running Off Off Off	0 %		2048 MB	1
ESBC_alexr1	Running	0 %		2048 MB	1
OVOC_QA	Off		Connect.		
OVOC_QA_ High	Running		Settings		1
			Start		
			Checkpoi	nt	
<	III	_	Move		

Figure 8-21: Power On Virtual Machine

2. Connect to the console of the running server by right-clicking the OVOC server virtual machine, and then in the drop-down menu, choose **Connect**.

Figure 8-22: Connect to OVOC server Console

Virtual Machines				
Name 🔹	State	CPU Usage	Assigned Memory	Uptime
Stress_tool SSBC_AlexR3_HA1 SSBC_AlexR2_HA2 SSBC_AlexR2_HA1	Running Off Off Off	0 %	2048 MB	1.04:34:22
ESBC_alexr1 OVOC_QA	Running Off	0 %	2048 MB	1.04:10:46
OVOC_HA_HIGH	Running	Connect	00000 MD	1.02:37:53
		Settings		
<		Turn Off Shut Down		

3. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.

4. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

5. Start the OVOC Server Manager utility by specifying the following command:

OvocServerManager

- 6. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify login to OVOC Web client is successful.
- Set the OVOC server network IP address to suit your IP addressing scheme (Server IP Address on page 228).
- 8. Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 198).

9 Installing OVOC Server on Dedicated Hardware

The OVOC server installation process supports the Linux platform. The installation includes two separate components, where each component is supplied on a separate DVD:

- **DVD1:** OS installation: OS installation DVD (see Installing DVD1 below)
- DVD3: OVOC application: OVOC server application installation DVD (see DVD3: OVOC Server Application Installation on page 73)
 - Ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the installation.
 - Installation of OVOC Version 7.8 and later must be performed on HP DL Gen10 machines. Installation on HP DL G8 machines is not supported.
 - For obtaining the installation files, see OVOC Software Deliverables on page 13
 - ✓ Note that you must verify this file, see Files Verification on page 16

Installing DVD1

This section describes how to install DVD1 including the Rocky Linux Operating system.



Before commencing the installation, you must configure RAID-0 (see Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers on page 307)

To install DVD1 without a DVD:

- 1. Download the DVD1.ISO file to your PC.
- **2.** Using the WinSCP utility (see Transferring Files on page 328) transfer the **DVD1**.ISO file to the virtual machine installation platform.
- 3. Login to ILO 5 with "Administrator" privileges.
- 4. Launch the Integrated Remote Console.

iLO 5 × 1.20 Feb 02 2018	Inform	ation - iLO O)verv	/iew		
Information	Overview	Session List	ilo Ev	vent Log Int	egrated Management Log	Active He
System Information		•				
Firmware & OS Software				Informatio	on	
Remote Console & Media		Server Name Product Name		Prol iant DI 360) Gen10	
Power & Thermal		UUID		39373638-3935	5-5A43-4A38-313531443851	1
iLO Dedicated Network Port		Server Serial Number	r	CZJ8151D8Q		
iLO Shared Network Port		Product ID System ROM		867959-B21 U32 v1.36 (02/	14/2018)	
Remote Support		System ROM Date		02/14/2018		
Administration		Redundant System R	ROM	02/14/2018		
Security		Integrated Remote Co	onsole	HTML5 .NET	Java Web Start	
- Management		iLO Firmware Version	<u>1</u>	1.20 Feb 02 20	18	
		IP Address		10.3.181.9		
Intelligent Provisioning		Link-Local IPv6 Addre	ess	FE80::EEEB:B	8FF:FE93:CB08	
		iLO Hostname		ILOCZJ8151D8	3Q.	

Figure 9-1: Information-iLO Overview

5. From Integrated Remote Console, click Virtual Drives and select the saved location of the ISO file.

	Information			Status
Name	localhost.corp.audiocodes.com		System Health	A Degraded
t Name	ProLiant DL360 Gen10 1	0.3.181.181	iLO Health	°°≔ ⊾² ×
Serial Nu	Centus Etres 2 (Cent) Republication in the the Floppy (Second Virtual Media URL) Gen-18 Tagina			
ROM ROM Da	Centos Lin Karwel 3.1 Gan 38 Jay Passaurd:			
lant Syst	Lagin incorrect Gen-10 Jagin: ^C			
ted Remo	Password :			
nware Ve ess <u>cal IPv6.</u> stname	Mag Inf Handran. Mars 199 Jogin: Accome Parsurafi Barst failed Jogin: San Jan 39 12-22:12 BST 2824 on tigi There was 1 failed Jogin: Alkongi time the last successful login. Jacks Jogin: San Jan 39 11:86-84 from 172.17.13.33 Jacks Jogin: San Jan 39 11:86-94 from 172.17.13.34 Jacks Jogin: San Jan 30 11:86-94 from 172.17.13.35 Jacks Jogin: San Jan 30 11:86-95 2824 on ptz/0 GroutGean 10 730 GroutGean 10 730 _			

Figure 9-2: iLO Integrated Remote Console

	Informatior	ı		Status				Connection
Server Name	localhost.corp.au	idiocodes.com	Sys	tem Health 🔺 Degraded	ł			🛕 Not regi
Product Name	ProLiant DL360	Con 10 40	3 404 404	Health OK				
Server Serial Nutriel 3.	ых 7 (Care) 8.8-1168.182.1.cl7.a86_61 on an x8	← → ~ ↑ 📙 « net	app1 > ems > Versions > Extensions :	Linux > Linux_Distributions	» Rocky_8.9_OVOC_e	dition	5 V	Search Rocky_8.9_OVO
Product ID System ROM	ın: mx 7 (Care) 8.8-1168.182.1.el7.×86_64 on an ×8	Organize 👻 New folde	r					 Ⅲ ▼
System ROM Da	^{in:} -	Elisheva 🖈 ^	Name	Date modified	Туре	Size		
Redundant Syste		vmware 📌	old(bios)	6/24/2024 10:48 AM	File folder			
Integrated Remo		voc	DVD1_Rocky8_Linux_Rev1.iso	6/23/2024 2:41 PM	Disc Image File	13,510,708		
License Type		Recommended						
il O Eirmware Ve		Rocky_8.9_OVO(
IP Address		semFkGen_8.0.3						
Link-Local IPv6		OneDrive - Audio						
iLO Hostname		💻 This PC						
		3D Objects						

 From Integrated Remote Console, click Power Switch > Momentary Press, the server is shutdown. Click Momentary Press to power the server back on.



After server boot process has commenced, press F11 to enter the boot menu.



📧 iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 iLO: ILOCZJ8151D8Q,			-	D X
Power Switch Virtual Drives Keyboard Help				
HPE ProLiant		Hew Ente	lett Pa erprise	ckard
(C) Copyright 1982-2018 Hewlett Packard Enterprise Development LP HPE ProLiant DL360 Gen10 System ROM Version: U32 v1.36 (02/14/2018) Serial Number: CZJ8151D8Q Installed System Memory: 64 GB, Available System Memory: 64 GB			1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
1 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled Proc 1: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz				
Workload Profile: General Power Efficient Compute Power Regulator Mode: Dynamic Power Savings Advanced Memory Protection Mode: Advanced ECC Support Boot Mode: UEFI HPE SmartMemory authenticated in all populated DIMM slots.				
Starting required devices. Please wait, this may take a few moments			Secure Start	Smart Storage Battery
		Smart Array	Dynamic Power Capping	HPE SmartMemory
iL0 5 IPv4: 10.3.181.9 iL0 5 IPv6: FE80::EEEB:B8FF:FE93:CB08		HPE RESTful API	Intelligent Provisioning	Sea of Sensors 3D
F9 System Utilities F10 Intelligent Provisioning F11 Boot Menu	F12 Network Boot	iLO Management Engine	iLO Advanced	Agentiess Management
1024 x 768	₩4 11 🕨 🥥		🔒 A	ES 🕘 🖲 💽

7. On boot menu, scroll down by mouse or arrows keys and select the "iLO Virtual USB 3 : iLO Virtual CD-ROM" to start the boot sequence.

10 iLO Integrated Remote Console - Server: ProLiant DL360 Gen	10 iLO: ILOCZJ8151D8Q. — 🗆 🗙
Power Switch Virtual Drives Keyboard Help	
Hewlett Packard Boot Menu	۶ 🗲
♠ One-Time Boot Menu	
ЧОС	Generic USB Boot
ProLiant DI 360 Gen10	Internal SD Card 1 : Generic USB3.0-CRW
Server SN: CZJ8151D8Q	Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv4)
iLO IPv6: FE80::EEEB:B8FF:FE93:CB08 User Default: OFF	Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv4)
	Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv6)
	Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv6)
	Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv4)
	Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv4)
	Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv6)
Enter: Select ESC: Exit	Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv6)
F1: Help F7: Load Manufacturing Defaults	Embedded SATA Port 12 CD/DVD ROM : hp DVDRW GUD0N
F10: Save F12: Save and Exit	Embedded RAID 1 : HPE Smart Array E208i-a SR Gen10 - 3.4 TiB, RAID0 Logical Drive 1(Target:0, Lun:0)
	iLO Virtual USB 3 : iLO Virtual CD-ROM
	Run a UEFI application from a file system
http://www.hpe.com/qref/ProLiantGen10UEFI-Help	Legacy BIOS One-Time Boot Menu
Exit O Changes Pending	O Reboot Required
1024 x 768	🚧 11 🕨 🔍 🙆 AES 🔷 🔿 🕲

Figure 9-5: Boot Sequence

8. The following screen appears, select "Install Rocky Linux version 8.x ..." and press Enter.



Figure 9-6: Install Rocky Linux version 8.x

9. After a while the Rocky Linux version 8.x installation commences:



localitost.corp.addiocodos.com	<u>оузют поант</u>	- Dogradou
ProLiant DL360 Gen10 10.3.181.181	iLO Health	° 1 _ ~ 7
Stopping Open-3831 C 0% 3 Stopped target Inited Default Target. C 0% 3 Stopped target Inited Noth Device. C 0% 3 Stopped Gpen-1831. C 0% 3 Stopped Open-1831. C 0% 3 Stopped Open-1831. C 0% 3 Stopped Open-1831. C 0% 3 Stopped Target Stol. C 0% 3 Stopped Target Stol. C 0% 3 Stopped Target Stol. C 0% 3 Stopped Target Store. C 0% 3 Stopped Target Device Initialization. C 0% 3 Stopped Target Store. C 0% 3 Stopped Target Device Rodes in Advo. C 0% 3 Stopped Target Store. C 0% 3 Stopped Target Device Rodes in Advo. C 0% 3 Stopped Target Store. C 0% 5 Stopped Target Device Rodes in Advo. C 0% 5 Stopped Target Store. C 0% 5 Stopped Target St	JINIT - UTHE -LINCRYPTSETU	* •CERYPT «GNITLS •ACL »
[96.907156] system(11): Detected architecture x06-64.		

- **10.** Wait for the installation to finish, from "Virtual Drives" menu deselect the selected drive and press Enter, the server is rebooted.
- **11.** Login as 'root' user with password *root*.
- 12. Type network-config, and then press Enter; the current configuration is displayed:

Figure 9-8: Rocky Linux version 8.x Network Configuration

```
[acems@OVOC-7 ~]$ su -
Password:
Last login: Thu Dec 14 12:08:24 GMT 2017 on pts/0
[root@0V0C-7 ~]# TMOUT=0
[root@OV0C-7 ~]# network-config
Current network configuration:
Hostname
                   : 0V0C-7
IP Address
                  : 10.3.180.7
Prefix
                  : 16
Default Gateway : 10.3.0.1
Do you wish to change it? (y/[n]) : y
Hostname
                  : ovoc-server-7
IP Address
                  : 10.3.180.7
Prefix
                  : 16
Default Gateway
                  : 10.3.0.1
Apply new configuration? ([y]/n) : y
Activate the network configuration.
```

This script can only be used during the server installation process. Any additional Network configuration should later be performed using the OVOC Server Manager.

- **13.** You are prompted to change the configuration; type **y**.
- 14. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.
- **15.** Confirm the changes; enter **y**.
- **16.** Type the following command:

reboot

DVD3: OVOC Server Application Installation

The procedure below describes how to install the OVOC server application. This procedure takes approximately 20 minutes.

> To perform DVD3 installation:

- 1. Download the DVD3-OVOC Server Application Installation. ISO file containing the Rocky Linux Operating system to your PC.
- 2. Using the WinSCP utility (see Transferring Files on page 328) transfer the DVD3.ISO file to the OVOC Version 8.2 server acems user home directory: /home/acems
- 3. Login into the OVOC server by SSH, as 'acems' user, and enter the password *acems*.
- 4. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

5. Mount the .ISO file to make it available:

mount /home/acems/DVD3_EMS_.iso /mnt

6. Change directory to the script location:

cd /mnt/EmsServerInstall/

5. Run the installation script from its location:

./install





7. Enter y, and then press Enter to accept the License agreement.

Figure 9-10: OVOC server Application Installation – License Agreement

pased upon the net income of bicensol.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement or any of Licensee's rights or obl
tten permission of Licensor and any attempt to do so shall be without effe
sferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regu
, and may require a license to export such. Licensee is solely responsible
11.7. Relationship of Parties Nothing herein shall be deemed to create an
the parties. Neither party shall have the right to bind the other to any o
11.8. Integration This Agreement is the complete and exclusive agreement b
ated hereto. Any Licensee purchase order issue for the software, documenta
erms hereof.
11.9. Counterparts This Agreement may be executed in multiple original cou
ing an authorized signature of Licensor and Licensee.
Do you accept this agreement? (y/n)y

 When you are prompted to change the *acems* and *root* passwords, enter new passwords or enter existing passwords. You are then prompted to reboot the OVOC server machine; press Enter. Figure 9-11: OVOC server Application Installation (cont)

udev.x86_64 wget.x86_64 wireshark.x86_64	095-14.20.e15_3 1.11.4-2.e15_4.1 1.0.11-1.e15_5.5	ems-local ems-local ems-local
Hardening Linux OS for DoD STIG complia	ncy	
<pre>>>> Enter new password for user 'acems' Changing password for user acems. New UNIX password: BAD PASSWORD: it is too short Retype new UNIX password: passwd: all authentication tokens update</pre>	ed successfully.	
<pre>>>> Enter new password for user 'root' Changing password for user root. New UNIX password: BAD PASSWORD: it is too short Retype new UNIX password: passwd: all authentication tokens updat HIMIN HIMIN HIMIN HIMIN EMS Server must be rebooted to proceed to</pre>	ed successfully.	
After the reboot completes, re-login to re-run the installation script to comple	the EMS Server and ete the installation.	
Press Enter to reboot		

- The installation process verifies whether Rocky Linux version 8.x that you installed from DVD1 includes the latest OS patch updates; do one of the following:
 - If OS patches are installed, press Enter to reboot the server.
 - If there are no OS patches to install, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

After the OVOC server has rebooted, repeat steps Login into the OVOC server by SSH, as 'acems' user and enter password acems (or customer defined password). on page 181 to Enter y, and then press Enter to accept the License agreement. on page 182

Figure 9-12: OVOC Server Installation Complete



- **10.** Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
- **11.** When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.

12. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

13. Type the following command:

OvocServerManager

- **14.** Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify login to the OVOC Web client is successful.
- **15.** Verify that the Date and Time are set correctly (Date and Time Settings on page 248).
- **16.** Configure other settings as required (Getting Started on page 198).

10 Migrating to Rocky Linux Operating System

This procedure describes how to migrate your Version 8.2 data to the Version 8.4 OVOC server machine running the Rocky Linux Operating system. Before starting the process:

- Extract current OVOC backup files to an external machine (see OVOC Server Backup Processes on page 190).
- Ensure that the OVOC server has been upgraded to version 8.2.3000 GA:
 - Upgrading OVOC Server on Dedicated Hardware on page 181
 - Upgrading OVOC Server on VMware and Microsoft Hyper-V Virtual Machines on page 177
 - Upgrading OVOC Server on Amazon AWS and Microsoft Azure on page 172
- Stop OVOC from OvocServerManager (see Start or Restart the Application on page 214).



'EmsServerManager' has been renamed to 'OvocServerManager'. Both command strings can be typed in the SSH console.

Make sure both Postgres and Cassandra database processes are active (see Viewing Process Statuses on page 203).

Do the following:

- Download the DVD3-OVOC Server Application Installation ISO file containing the Rocky Linux Operating system to your PC.
- Using the WinSCP utility (see Transferring Files on page 328) transfer the DVD3.ISO file to the OVOC Version 8.2 server acems user home directory: /home/acems
- **3.** Login into the OVOC server Version 8.2 machine by SSH, as 'acems' user, and enter the password *acems*.
- 4. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

5. Verify that the folder /mnt exists, and if not then create it:

mkdir /mnt

6. Mount the ISO to make it available:

mount /home/acems/DVD3_EMS_XXX.iso /mnt

7. Change directory to the script location:

cd /mnt/EmsServerInstall/

8. Run the installation script:

perl upgrade_DBs_centos.pl

9. Change directory to the location of the OVOC backup archives:

cd /data/NBIF/emsBackup

[root@low-185 ~]# cd /data/ [root@low-185 emsBackup]#] total 935556	′NBIF∕emsBa 1	ւշ kup		
-rw-rr 1 emsadmin nbif	1546240	Jun 20	04:01	cassandraBackup_8.4.20_2406200200_171884526
-rw-rr 1 emsadmin nbif drwxrwxr-x 2 postgres dba -rw-rr 1 emsadmin nbif -rw-rr 1 emsadmin nbif [root@low=185 emsBackun]#	955596800 6 313462 547455	Jun 20 Jun 20 Jun 20 Jun 20 Jun 20	04:00 04:00 04:00 04:00 04:00	emsServerBackup_8.4.20_2405200200.tar export ovocConfigBackup_8.4.20_2405200200.tar.gz ovocFullBackup_8.4.20_2405200200.tar.gz

- **10.** Copy the following archives: EMSServerBackup, ovocFullBackup and cassandraBackup to your PC.
- **11.** Perform OVOC Version 8.4 clean installation on the same server or on another server:
 - Installing OVOC Server on Dedicated Hardware on page 67
 - Launching Public OVOC Image on Amazon Web Services (AWS) on page 18
 - Creating OVOC Virtual Machine on Microsoft Azure on page 26
 - Installing OVOC Server on VMware Virtual Machine on page 34
 - Installing OVOC Server on Microsoft Hyper-V Virtual Machine on page 48
- **12.** Login into the OVOC server Version 8.4 machine by SSH, as 'acems' user, and then enter the password *acems*.
- **13.** Switch to 'root' user and provide *root* password (default password is *root*):

su - root

- **14.** Transfer the archive files using the WinSCP utility (see Transferring Files on page 328) to /data/NBIF/ directory.
- **15.** Start the OVOC Server Manager utility by specifying the following command:

OvocServerManager

 Run the option 'Restore from CentOS' (Application Maintenance menu > Restore) (see Restore from Rocky Linux version 8.x). At the end of the process, the OVOC server is rebooted.



17. Apply the OVOC license (see OVOC License on page 217). At the end of the process, you must restart the OVOC Server application.

Part III

Post Installation

This part describes how to restore the OVOC server machine from a backup.

11 Registering OVOC Applications on Azure

The OVOC application on Azure can be registered under one of the following scenarios. For each procedure the corresponding OVOC setup is described:

- Allow access to operators from Single Organization tenant where operators are mapped to Azure groups (Registering Single Tenant in Organizational Directory below
- Allow access to operators from multiple organizational tenants external where operators are assigned roles (Registering Multitenant Support on page 94).
- Upgrade from Single Organization tenant to Multitenant (Upgrading from Single Tenant to Multitenant on page 112

Registering Single Tenant in Organizational Directory

This section describes how to register access to OVOC for operators from a single organizational tenant in the Organizational directory. For this deployment operators retrieve their security level from OVOC through a mapped Azure security group. A security group must be defined on Azure for each required security level. You must then assign operators to the relevant group accordingly. After performing this procedure, add the Azure groups and their operator members (see Create Azure Groups and Assign Members on page 124). These groups are mapped to OVOC for retrieving the operator security levels.

> Do the following:

- 1. Login to the Azure portal with tenant admin permissions.
- 2. In the Navigation pane, select App registrations and then click New registration.

	Microsoft Azure	𝒫 Search resources, services, and docs (G+/)		₽ Q		ଡ ନ	Admin@ocshost.emea audiocodes netherlands i	I BV 📍				
Hon	Home > AudioCodes Netherlands BV											
	AudioCodes N Azure Active Directory	letherlands BV App registrations 🛷 …						×				
0	Overview	Kerresh Verweigktration Endpoints Provideshooting Defined by Preview features	🗢 Got	feedback	2							
	Preview features Diagnose and solve problem	s Try out the new App registrations search preview! Click to enable the preview. \rightarrow						×				
Man	lage Users	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Likeary (ADAL security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Aut) and Azure AD hentication Libi	Graph. Wi rary (MSAL	e will cont) and Mic	inue to provi rosoft Graph	ide technical support and . Learn more	×				
24 ()	Groups External Identities	All applications Owned applications Deleted applications										
2.	Roles and administrators	Start typing a name or Application ID to filter these results										
a. 11	Administrative units Enterprise applications	Display name Application (client	:) ID		с	reated on	Certificates & secrets	^				
	Devices	MyApp b55f4d0c-e47f-41e	af-8c96-764af	238f25d	3,	/3/2017	 Current 					
Щ.	App registrations	UMP customer portal 46fad081-f3b2-41:	37-a7b4-d183	4133cead	1,	/24/2020	-					
۵	Identity Governance	skype2TeamsMigrator 4322a7ce-38b2-46	fa-9dd3-966c	f9ea0a35	1	1/25/2020	🕑 Current					
15	Application proxy	My UWP App fd013cea-f9eb-4dd	df-96f6-ade32	7d056b0	1	1/27/2020	-					
Å.	Licenses	Demo auth tenant f8f0a43b-71f4-4eb	6-a087-cf68c	7d43e23	2,	/10/2021	-					
	Azure AD Connect	Resgister-demo d573a2dc-b7ee-44	153-ab68-d61	94428fb8o	d 2,	/11/2021	-					
-	Custom demois serves	TodoList-API 714ad139-ed99-44	170-abd2-facc	855634a7	2	/11/2021	-	~				

Figure 11-1: App registrations

- 3. Enter the name of the OVOC registration tenant.
- 4. Select Accounts in this organizational directory only (Tenant name- Single tenant).

Figure 11-2: Single Organizational Tenant

E Microsoft Azure P Search resources, services, and docs (G+/)	Σ.	Ŗ	Q	۵	0	host.emea
Home > AudioCodes Netherlands BV >						
Register an application						×
* Name						
The user-facing display name for this application (this can be changed later).						
OVOCApplication 🗸						
Supported account types						
Who can use this application or access this API?						
Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)						
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)						
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)						
Personal Microsoft accounts only						
Help me choose						
Redirect URI (optional)						
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be						
By proceeding, you agree to the Microsoft Platform Policies 😴						
Register						
Register						

5. Enter the HTTPS Redirect URI (REST endpoint) for connecting to OVOC Web in the following format:

https://x.x.x.x/ovoc/v1/security/actions/login



■ Microsoft Azure	۶.	Ģ	Q	٢	0	ନ୍ଦ	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >							
Register an application							×
Supported account types							
Who can use this application or access this API?							
Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)							
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) 							
O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)							
O Personal Microsoft accounts only							
Help me choose							
Redirect URI (optional)							
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.							
Web V https://xxxx/ovoc/v1/security/actions/login V							
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.							
By proceeding, you agree to the Microsoft Platform Policies 🕾							
Register							

6. Click Register.

The new registered application is displayed.

Figure 11-4: New Registered Application

Home > AudioCodes Netherlands	BV					
AudioCodes Net	herl	ands BV App registrations 🛷 …				×
Enterprise applications	~	+ New registration 🔀 Endpoints 🤌 Troubleshooting 🖒 Refresh 🛓 Downlo	ad 💽 Preview features 🛛 ♡ Got feedback?			
Devices App registrations		1 Try out the new App registrations search preview! Click to enable the preview. $ ightarrow$				×
Identity Governance						
Application proxy		Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory.	Authentication Library (ADAL) and Azure AD Graph. We will	continue to provide t	echnical support and	×
🔓 Licenses	а.	security updates but we will no longer provide feature updates. Applications will need to b	e upgraded to Microsoft Authentication Library (MSAL) and	Microsoft Graph. Le	arn more	
🚸 Azure AD Connect						
🐖 Custom domain names		All applications Owned applications Deleted applications				
Ø Mobility (MDM and MAM)		P OVOC				×
📍 Password reset		Display name	Application (client) ID	Created on	Certificates & secret	te
📕 Company branding				5 (35 (303)		
🎒 User settings			59809002-9984-4506-9607-017873529500	5/25/2021	Current	
Properties		ovocxppication	/2e91409-9da5-4cc1-a5t0-72416111ba23	10/7/2021	Current	
Security						
Monitoring						
Sign-in logs						
Audit logs	~					

- 7. Double-click the new application i.e. OVOCApplication (in this example) to configure it.
- 8. In the navigation pane, select Certificates & secrets.

Figure 11-5: Certificates & secrets

≡ Microsoft Azure 🔎 Searc	h resources, services, and docs (G+/))			E 🗣 🗘 🤅	3 O R	Admin@ocshost.emea
Home > AudioCodes Netherlands BV >	> OVOCApplication						
OVOCApplication	Certificates & secre	ts 🖈 …					×
	♡ Got feedback?						
Overview	Certificates						^
🚳 Quickstart	Certificates can be used as secret	ts to prove the application's identi	ty when requesting a tok	en. Also can be referred t	o as public keys.		
🚀 Integration assistant	↑ Upload certificate						
Manage	Thumbprint		Start date	Expires	Certificate ID		
Branding	No certificates have been added	for this application.					
Authentication							
🕈 Certificates & secrets							
Token configuration	Client secrets						
API permissions	A secret string that the application	n uses to prove its identity when	requesting a token Also	can be referred to as ann	lication password		
Expose an API	T secret string that the applicate	si ases to prove its identity when	equesting a toten 7450	can be referred to as app	ication passiona.		
App roles	+ New client secret						
A Owners	Description	Expires	Value		Secret ID		
& Roles and administrators Preview	No client secrets have been creat	ted for this application.					
Manifest							
Support + Troubleshooting							~

9. Click New client secret.

≡ Microsoft Azure 🔎 Searc	ch resources, services, and docs (G+/)			Σ	G 🖉 🎯 Ø R	Admin@ocshost.emea Audiocodes netherlands by
Home > AudioCodes Netherlands BV	> OVOCApplication			Add a client s	secret	×
OVOCApplication	Certificates & secrets 🔗			Description	over corret]
✓ Search (Ctrl+/) «	♡ Got feedback?			Evoires	24 months	
🗮 Overview	Certificates			Expires	24 1101113	
🗳 Quickstart	Certificates can be used as secrets to prove the	e application's identity	when requesting a token. Also			
💉 Integration assistant	↑ Upload certificate					
Manage	Thumbprint		Start date I			
🖬 Branding	No certificates have been added for this applic	ation				
Authentication ■	No certificates have been added for this applic	auon.				
↑ Certificates & secrets						
III Token configuration	Client secrets					
→ API permissions	A secret string that the application uses to pro	ve its identity when re	questing a token. Also can be n			
Expose an API	researce string that the application uses to pro	vents identity when re	quisting a token. Also can be n			
App roles	+ New client secret					
A Owners	Description	Expires	Value			
& Roles and administrators Preview	No client secrets have been created for this ap	plication.				
Manifest						
Support + Troubleshooting				Add Cance	el	

Figure 11-6: New client secret

- **10.** Enter a description and from the drop-down list select **24 months**.
- 11. Click Add.

Figure 11-7: Client Secret Generated

E Microsoft Azure 🔎 Search	n resources, services, and docs (G+/)				Þ	Ģ	e 🖗	0	Ŕ	Admin@ocshost.emea
Home > AudioCodes Netherlands BV >	OVOCApplication									
OVOCApplication	Certificates & secret	5 🖈 …								×
	♡ Got feedback?									
Sverview	Certificates									^
i Quickstart	Certificates can be used as secrets	to prove the application's identity	when requesting a toke	en. Also can be referred to	as public k	eys.				
💉 Integration assistant	→ Upload certificate									
Manage	Thumbprint		Start date	Expires	Cert	tificate II)			
Branding	No certificates have been added fo	r this application								
Authentication	No contracto nuve been adaea re	r this upplication.								
📍 Certificates & secrets										
Token configuration	Client secrets									
 API permissions 	A secret string that the application	uses to prove its identity when re	questing a token. Also r	an he referred to as applic	ation pass	word				
 Expose an API 	A secret string that the upplication	uses to prove to identity interve	questing a tokeni 7050 t	an be referred to us applie	atton passi	nord.				
10 App roles	+ New client secret									
A Owners	Description	Expires	Value	Copy to	lipboard e	t ID				
& Roles and administrators Preview	ovoc_secret	10/7/2023	n3F7Q~JPgcXqNG	0wNCVJjvaNuviFx2nY .	eecc0e	bf-e5d9-	4aa1-baei	a-231470	de7f24d	ъ 💼
Manifest										

- **12.** Copy the secret Value to clipboard as its required in later configuration and cannot be retrieved once you leave this screen.
- **13.** In the navigation pane, select **Authentication**.

Figure 11-8: Authentication



- 14. Under Implicit grant and hybrid flows select the following:
 - Access tokens (used for implicit flows)
 - ID tokens (used for implicit and hybrid flows)
- 15. Click Save.
- **16.** In the navigation pane, select **Token configuration**.

Figure	11-9:	Token	config	uration

≡ Microsoft Azure 🔎 Sear	ch resources, services, and docs (G+/)		P © P	Admin@ocshost.emea
Home > AudioCodes Netherlands BV	> OVOCApplication	Add optional clain	n	×
OVOCApplication	Token configuration 🛷 …			
Search (Ctrl+/) «	Sof feedback?	Once a token type is selected, you	may choose from a list of	available optional claims.
B Overview	Optional claims	• Token type		
Quickstart	Optional claims are used to configure additional information which is returned in one or more toker	Access and ID tokens are used by	applications for authentica	tion. Learn more 🖓
💉 Integration assistant	+ Add optional claim + Add groups claim	Access		
Manage		SAML		
Branding	Claim ↑↓ Description	_		
Authentication	No results.	Claim 🔨	Description	
Certificates & secrets		pwd_exp	The datetime at which the	ne password expires
Token configuration		pwd_url	A URL that the user can	visit to change their password
API permissions		sid sid	Session ID, used for per-	session user sign out
Expose an API		tenant_ctry	Resource tenant's count	ry/region
App roles		tenant_region_scope	Region of the resource t	enant
A Owners		🔽 upn	An identifier for the user	that can be used with the user
Roles and administrators Proviour		verified_primary_email	Sourced from the user's	PrimaryAuthoritativeEmail
Manifest		verified_secondary_email	Sourced from the user's	SecondaryAuthoritativeEmail
Support + Troubleshooting		Add Cancel	ution (from the from the data of the ofference)	NUL Control - Printer Control Anno

17. Select Add optional claim.

- 18. Under Token Type, select ID.
- **19.** Under Claims, select the **upn** check box.
- 20. Click Add.

Figure 11-10: Add Optional claim



21. Select the **Turn on the Microsoft Graph profile permission** check box and then click **Add**. This adds the Profile permission to the API permissions list.

The new claim is displayed.

Figure 11-11: New UPN Claim

≡ Microsoft Azure 🔎 Searc	Microsoft Azure P Search resources, services, and docs (G+/)						9	ନ୍ଦି	Admin@ocshost.emea. AUDIOCODES NETHERLANDS B	
Home > AudioCodes Netherlands BV	Home > AudioCodes Netherlands BV > OVOCApplication									
OVOCApplication	Token configuratio	n 🖈 …								×
Search (Ctrl+/) «	♡ Got feedback?									
Ovieletart	Optional claims									
	Optional claims are used to con	figure additional information which is returned in one or more tokens. Learn more 🗗								
Integration assistant	+ Add optional claim +	Add groups claim								
Manage										
Branding	Claim ↑↓	Description			Toke	n type	¢↓		Optional settings	
Authentication		An identifier for the user that can be used with the username hint parameter: not a due	able iden	tifier f	ID				Default	
📍 Certificates & secrets	- upri	variacitation for all data and can be abea that the abernance_init parameter, not a dat	able lach		10				Denant	
Token configuration										
→ API permissions										
Expose an API										
App roles										
A Owners										
& Roles and administrators Preview										
Manifest										
Support + Troubleshooting										

22. Right-click the newly added token and select Edit.

Figure 11-12: Edit Optional Claim

	n resources, services, and docs (G	·/)		β (⊛ №	0	ନ୍ଦି	Admin@ocshost.emea Audiocodes Netherlands BV	Ð
Home > AudioCodes Netherlands BV >	Home > AudioCodes Netherlands BV > OVOCApplication								
OVOCApplication	Token configuration	on 🖈 …						×	
	♡ Got feedback?								
Soverview	Optional claims								
🍊 Quickstart	Optional claims are used to co	nfigure additional information which is returned in one or more tokens. Learn more 🗗							
💉 Integration assistant	+ Add optional claim $+$	Add groups claim							
Manage									
Branding	Claim 个	Description			Token tv	ne tu		Ontional settings	
Authentication	unn	An identifier for the user that can be used with the username hint parameter; not a dura	able identi	fior f	ID	p			
📍 Certificates & secrets	upii	An identifier for the user that can be used with the userhame_init parameter, not a dure	able identi	ner I	10		6	P Edit	
III Token configuration							Ū	Delete	
API permissions									
Expose an API									
App roles									
A Owners									
& Roles and administrators Preview									
Manifest									

23. Under Edit UPN (ID token), select **Yes** to Externally authenticate guest users (users that are not members of the organization's Azure defined groups).

Figure 11-13: Edit UPN (ID token)

≡ Microsoft Azure 🔎 Searc	h resources, services, and docs (G	+/)	🖸 🕼 🤔 🔅 🕐 R Admin@ocshost.emea 🕐
Home > AudioCodes Netherlands BV >	> ovocApplication Token configuration	on 🖈 …	Edit UPN (ID token) ×
Search (Ctri+/) Gverview Quickstart Integration assistant	Cot feedback? Optional claims Optional claims are used to co + Add optional claim +	onfigure additional information which is returned in one or more toker - Add groups claim	User Principal Name (UPN) is an identifier for the user that can be used with the username_hint parameter. Learn more about UPN claimco Externally authenticated This option includes the guest UPN as stored in the resource tenant.
Manage Branding Authentication Certificates & secrets	Claim 个U upn	Description An identifier for the user that can be used with the username_hint	Replace hash marks This option replaces the hash marks (#) in the guest UPN with underscores (_). No
Token configuration API permissions Expose an API			
App roles Convers Roles and administrators Preview			
Manifest Support + Troubleshooting			Save Cancel

- 24. Click Save.
- 25. In the Navigation pane, select API permissions.



Figure 11-14: API Permissions

Home > AudioCodes Netherlands BV > OVOCApplication			Request API permission	IS		>		
OVOCApplication Search (Ctrl+/) « Overview Quickstart Integration assistant	API permissions Refresh C Got feedt The "Admin consent requine organization, or in organization, org	> back? ed" column shows the titions where this app v	Select an API Microsoft APIs APIs my organization Commonly used Microsoft APIs Microsoft Graph Take advantage of the tree	n uses My APIs	e Mobility = Security, and Windows 10.			
Branding Authentication	Configured permissions Applications are authorized to ca all the permissions the application	all APIs when they ar on needs. Learn more	Access Actie Au, Exce, incure, Outdoor, Exchange, OneUnive, OneVole, Sharevoni, Planner, and more imough a single endpoint.					
Certificates & secrets Token configuration API permissions Expose an API	+ Add a permission Gr API / Permissions name Microsoft Graph (3)	ant admin consent f Type Delegated	Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Rights Management Services Allow validated users to read and write protected content			
App roles Owners Roles and administrators Preview Manifest	To view and manage permission:	Delegated Delegated s and user consent, t	Azure Service Management Programmatic access to much of the functionality available through the Azure portal	Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination	Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central			
Support + Troubleshooting								

26. Click Add a permission and then click the Microsoft Graph link.

Figure 11-15: Delegated permissions

\equiv Microsoft Azure ρ Searc	h resources, services, and docs (G+/)		D 🕼 🗘 🏟 Ø	Admin@ocshost.emea
Home > AudioCodes Netherlands BV >	OVOCAdmin	Request API permissions		×
🕘 OVOCAdmin API p	permissions 🖈 …			
Search (Ctrl+/) « Overview	Nefresh 🔗 🖓 Got feedback?	Microsoft Graph Microsoft Graph https://graph.microsoft.com/ Docs 👌 What twoe of nermissions does your application require?		
QuickstartIntegration assistant	A Starting November 9th, 2020 end users will no k	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a back signed-in user.	ground service or daemon without a
Manage	The "Admin consent required" column shows the	e		
Branding & properties	your organization, or in organizations where this			
Authentication	Configured permissions			
📍 Certificates & secrets	Applications are authorized to call APIs when they a	a.		
Token configuration	all the permissions the application needs. Learn mo	n		
 API permissions 	+ Add a permission 🗸 Grant admin consent	f		
Expose an API	API / Permissions name Type			
App roles	✓ Microsoft Graph (2)			
A Owners	profile Delegated			
& Roles and administrators Preview	User.Read Delegated			
Manifest				
Support + Troubleshooting	To view and manage permissions and user consent,	Add permissions Discard		

27. Click Delegated permissions.

😑 Microsoft Azure 🔎 Se	earch resources, services, and docs (G+/)		D 🕼 🗳 Ø R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands B 	v > ovocApplication API permissions 🛷 …	Request API permissions		×
 ✓ Search (Ctrl+/) ✓ Integration assistant 	« 🕐 Refresh 🛛 🛇 Got feedback?	Group (1)		,
Manage	1 The "Admin consent required" column shows the	Group.Read.All ① Read all groups	Yes	
 Branding Authentication 	organization, or in organizations where this app v	Group.ReadWrite.All ① Read and write all groups	Yes	
↑ Certificates & secrets	Configured permissions Applications are authorized to call APIs when they ar	> GroupMember		
Token configuration API permissions	all the permissions the application needs. Learn mon	> IdentityProvider		
Expose an API	API / Permissions name Type	> IdentityRiskEvent		
App roles	✓ Microsoft Graph (2)	> IdentityRiskyUser		
& Roles and administrators Preview	User.Read Delegated	> IdentityUserFlow		
Manifest	To view and manage permissions and user consent t	> IMAP		
Support + Troubleshooting Troubleshooting New support request	v view and manage permissions and user consent, t	Add permissions Discard		

Figure 11-16: Microsoft Graph Permissions

- **28.** Select **Group.Read.All** for OVOC to read permissions from all user groups defined for the tenant, and then click **Add permissions**.
- 29. Add another Delegated permission User.Read.All and then click Add permissons.

\equiv Microsoft Azure \checkmark Search	h resources, services, and docs (G+/)	D 🗣 🗘 🔅	Admin@ocshost.emea 🕐					
Home > AudioCodes Netherlands BV >	OVOCAdmin	Request API permissions	×					
 OVOCAdmin API p	ermissions 🖈 …							
	🕐 Refresh 🕅 Got feedback?	C All AVIS permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more						
Overview								
🗳 Quickstart	A Starting November 9th, 2020 end users will no l	Permission	Admin consent required					
🚀 Integration assistant		> IdentityRiskyUser						
Manage	The "Admin consent required" column shows th your organization, or in organizations where thi	✓ User (2)						
Branding & properties	, , , , ,	User.Read ①						
Authentication	Configured permissions	Sign in and read user profile	NO					
Certificates & secrets Token configuration	Applications are authorized to call APIs when they all the permissions the application needs. Learn mo	User.Read.All ① Read all users' full profiles	Yes					
API permissions	+ Add a permission ✓ Grant admin consent	User.ReadBasic.All O Read all users' basic profiles	No					
Expose an API	API / Permissions name Type	User.ReadWrite ①	No					
App roles	✓ Microsoft Graph (2)	Read and write access to user profile	NO					
A Owners	profile Delegated	User.ReadWrite.All ① Read and write all users' full profiles	Yes					
& Roles and administrators Preview	User.Read Delegated		v					
🔟 Manifest								
Support + Troubleshooting	To view and manage permissions and user consent	Add permissions Discard						

Figure 11-17: Delegated permissions

The configured API permissions are displayed.

Figure 11-18: Configured API Permissions

Figure 11-19:

≡ Microsoft Azure 🔎 Sear	P Search resources, services, and docs (G+/)								R ;	Admin@ocshost.em AUDIOCODES NETHERLAND	еа s вv 🥐
Home > AudioCodes Netherlands BV	> OVOCAdmin										
_{Ə-} OVOCAdmin API	permissions 🛷 …										\times
Search (Ctrl+/) Gverview Quickstart	C Refresh A Got feedba	ack?	n, users will have to consent even if they've already do	one so previously.							
 Integration assistant Manage 	The "Admin consent required your organization, or in organization."	d" column shows th nizations where th	e default value for an organization. However, user co is app will be used. Learn more	nsent can be customiz	ed per pe	rmissior	ı, user, or ap	p. This co	olumn may r	not reflect the value in	×
Branding & properties Authentication Certificates & secrets	Configured permissions Applications are authorized to cal all the permissions the application	I APIs when they n needs. Learn mo	are granted permissions by users/admins as part or about permissions and consent	of the consent proce	ss. The li	st of cor	nfigured pe	rmissior	ns should in	clude	
API permissions	+ Add a permission V Gra	nt admin consent Type	t for AudioCodes Netherlands BV Description	Admir	1 consen	t requ	. Status				
Expose an API	✓ Microsoft Graph (4)										
App roles	Group.Read.All	Delegated	Read all groups	Yes			🔺 Not	granted	for AudioC.		
A Owners	profile	Delegated	View users' basic profile	No							
& Roles and administrators Preview	User.Read	Delegated	Sign in and read user profile	No							
Manifest	User.Read.All	Delegated	Read all users' full profiles	Yes			🔺 Not	granted	for AudioC.		
Support + Troubleshooting											

30. Click **Grant admin consent for <Tenant_Name>** link to grant consent for the requested permissions for all accounts for this tenant, and then click **Yes** to confirm.

≡ Microsoft Azure 🔎 Search	icrosoft Azure 🔎 Search resources, services, and docs (G+/) 🗵 💀 🗘 🛞 🕐 R Admini@ecs-thost.emea							
Home > AudioCodes Netherlands BV > OVOCAdmin								
_ə OVOCAdmin API p	ermissions 🛷						×	
	Refresh Refresh Refresh Refresh Constant admin cons Do you want to grant c already has to match w Yes No Configured permissi Applications are authoriz	ent confirmationsent for the request of the second	on. uested permissions for all account they are granted permissions by	nts in AudioCodes Netherlands BV? T Jusers/admins as part of the consent proc	his will update a	ny existing admin cons	ent records this application	
Token configuration	+ Add a permission	. Crant admin.co	ncent for AudioCodes Netherland	ic PV				
→ API permissions	API / Permissions name	e Type	Description	Adm	in consent requ	Status		
 Expose an API 	✓ Microsoft Graph (4)							
Not the second s	Group.Read.All	Delega	ated Read all groups	Yes		🛕 Not granted for A	udioC ***	
A Owners	profile	Delega	ated View users' basic profile	No				
& Roles and administrators Preview	User.Read Delegated Sign in and read user profile No ····							
0 Manifest	User.Read.All	Delega	ated Read all users' full profiles	Yes		A Not granted for A	udioC •••	
Support + Troubleshooting								~ ~

31. In the Navigation pane, select the **Overview** page for the application.

Figure 11-21: Overview Page

≡ Microsoft Azure 🔎 Sea	rch resources, services, and docs (G+/)	E 🕼 🖓 🕲 🔗 R Admin@ocshost.emea 🛞
Home > AudioCodes Netherlands BV	>	
UVOCApplication	\$	×
Search (Ctrl+/) «	Delete Endpoints Endpoints Preview features	
Overview	Got a second? We would love your feedback on Microsoft identity platform (previous	sly Azure AD for developer). $ ightarrow$
 Quickstart Integration assistant 	↑ Essentials	
Manage	Display name : OVOCApplication	Client credentials : 0 certificate, 1 secret
Branding	Application (client) ID : 72e9f409-9da5-4cc1-a5f0-724f611fba23	Redirect URIs : 1 web, 0 spa, 0 public client
Authentication	Object ID : ddb67f46-a857-4e9c-a915-2829b3e377c1	Application ID URI : Add an Application ID URI
📍 Certificates & secrets	Directory (tenant) ID : c524b5t5-td18-43c0-964c-bc5d35525eaa	Managed application in I : OVOCApplication
Token configuration	supported account types : My organization only	
 API permissions 	Starting June 30th, 2020 we will no longer add any new features to Azure Active E and security updates but we will no longer provide feature updates. Applications	Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support swill need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more
Expose an API		
🌇 App roles	Get Started Documentation	
🎎 Owners		
& Roles and administrators Preview	Build your application	with the Microsoft identity platform
Manifest	The Microsoft identity platform is an authenticatic create modern, standards-based authentication sol	on service, open-source libraries, and application management tools. You can lutions, access and protect APIs, and add sign-in for your users and customers.
Support + Troubleshooting	v	reau more (3.

- **32.** Note the following values as they must later be configured in Configuring OVOC Web Azure Settings Single Tenant Setup below
 - Application (client) ID
 - Directory (tenant) ID
- **33.** Add Main Tenant Azure groups and add members as described in Create Azure Groups and Assign Members on page 124
- **34.** Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings Single Tenant Setup below

Configuring OVOC Web Azure Settings - Single Tenant Setup

This section describes how to configure Azure authentication in the OVOC Web interface for the Main Tenant. When an Azure-authenticated operator logs into the OVOC, they are assigned an OVOC security levels, e.g., 'Operator' based on their Group mapping on Azure.

- > To configure OVOC operators :
- In the OVOC Web, open the Authentication page (System > Administration > Security > Authentication), and then from the 'Authentication Type' drop-down, select AZURE.

0			
AZURE AUTHENTICATION SETTINGS		AUTHORIZATION LEVEL SETTINGS	
Security Azure Hostname	login.microsoftonline.com	System Administrator User Group Name	EMS_Admin
Azure AD Path Type File	(Tenant 💌	System Operator User Group Name	EMS_Operator
Azure Tenant ID*	tenant-Id	System Monitor User Group Name	EMS_Monitor
Azure Client ID	client-Id	Tenant Administrator User Group Name	EMS_Tenant_Admin
Change Azure Client Secret		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		ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS	
Enable combined authentication		Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group
Authentication order	External First		
GW / SBC / MSBR AUTHENTICATION			
Use AD Credentials for Device Page Opening			

Figure 11-22: Azure Main Tenant Authentication Settings

- 2. From the 'Azure AD Path Type File' drop-down, select Tenant.
- **3.** Enter the 'Azure Tenant ID' field. Extract value from the Overview page in the application registration for your **Single Tenant**.
- 4. In the 'Azure Client ID' field, enter the ID of the Azure AD client for your Single Tenant.
- 5. In the 'Azure Client Secret' field, enter the shared secret (password) that you generated and saved for your Single Tenant.
- 6. In the screen section 'GW / SBC / MSBR Authentication', select the option 'Use AD Credentials for Device Page Opening' for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to OVOC. The AudioCodes device will then perform authentication with the Azure AD and login to the device is attempted with same AD user name / password instead of the local device user name / password. Note that the device must also be configured to authenticate with the same AD.

When a Main Tenant operator attempts to connect to OVOC, OVOC verifies the mapped Azure User Group to which the operator is a member.

- In the Tenant Details screen under the **Operators** tab, the parameter **AD Authentication: Group Name** points to the Azure group which includes the Tenant operators who are authorized to login to OVOC using this method.
- If the Azure AD successfully validates that the operator belongs to the AD Authentication group (see highlighted group in the example below), its and allowed access.

Figure 11-23: AD Authentication Group Name

TEN	IANT DETAILS				
	General	SNMP	HTTP	Operators	License
	Local Authentication: Assigned	Operators			
	AD Authentication: Group Name		audio-code		



Home > audio-code >				
Groups All groups audio-code - Azure Active Directory				×
«	🗚 New group 🚽 Download groups 💼 Delete 💍 Refr	esh 🛛 😨 Columns 🛛 🛜 Got feedback?		
All groups				
Deleted groups		🖌 🍸 Filter 🗸		
X Diagnose and solve problems	Search mode Contains			
Settings	1 group found			
🛞 General	✓ Name	Object Id	Group Type	Membership T
Expiration		o0f6005o-76o0-4568-2510-502730d0f317	Microsoft 365	Assigned
Naming policy		e910093e-1069-4008-8310-368130001317	MICIOSOT 505	Assigned

7. In the screen section Authorization Level Settings, configure the user group names exactly as defined on Azure in Create Azure Groups and Assign Members on page 124. When an operator is not assigned to a group on Azure, the parameter 'Default Operator Type and Security Level' is applied.

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
ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS	
Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group

Figure 11-25: Authorization Level Settings



Figure 11-26: Matching Groups on Azure

Registering Multitenant Support

This procedure describes how to allow access to OVOC for operators from multiple Azure tenants. This procedure describes how to register the Main Tenant which include the OVOC system operators that belong to mapped Azure Groups. After performing this procedure, add operators for external tenants and assign roles to those operators you wish to allow access to OVOC (Add External Tenant Operators and Assign Roles on page 129):

Registered Service Provider Tenants

- Registered Channels
- Registered Customers

Guest user login is not supported for both Main Tenant and external tenant guest users once multitenancy is enabled in this procedure.

To configure OVOC multitenancy:

- **1.** Login to Azure portal as Global Administrator.
- 2. In the Navigation pane, select App registrations and then click New registration.

≡ Microsoft Azure 🔎 Searc	ch resources, services, and docs (G+/)		\$ 0 \$	Admin@ocshost.emea	- P			
Home > AudioCodes Netherlands BV				nonocobes nemeno mos o				
AudioCodes Nethe	rlands BV App registrations 🛷 …				×			
Overview	+ New registration 🕀 Endpoints 🤌 Troubleshooting 🖒 Refresh 🞍	Download 🐱 Preview features 🛛 🌣 Got feedback?						
 Preview features X Diagnose and solve problems 	1) Try out the new App registrations search preview! Click to enable the preview. $ ightarrow$				×			
Manage	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more							
Groups Groups External Identities Roles and administrators	All applications Owned applications Deleted applications							
Administrative units Enterprise applications	Display name	Application (client) ID	Created on	Certificates & secrets	^			
Devices	му МуАрр	b55f4d0c-e47f-41af-8c96-764af238f25d	3/3/2017	🛛 Current				
App registrations	uc UMP customer portal	46fad081-f3b2-4137-a7b4-d1834133cead	1/24/2020	-	11			
Identity Governance	sx Skype2TeamsMigrator	4322a7ce-38b2-46fa-9dd3-966cf9ea0a35	11/25/2020	Current				
Application proxy	My UWP App	fd013cea-f9eb-4ddf-96f6-ade327d056b0	11/27/2020	-				
🔓 Licenses	DA Demo auth tenant	f8f0a43b-71f4-4eb6-a087-cf68c7d43e23	2/10/2021	-				
Azure AD Connect	RE Resgister-demo	d573a2dc-b7ee-4453-ab68-d6194428fb8d	2/11/2021	-				
	TO TOdoList-API	714ad139-ed99-4470-abd2-facc855634a7	2/11/2021	-	~			

Figure 11-27: App Registrations

Figure 11-28: New Registration

	, P Search resources, services, and docs (G+/)	D 🖓	¢ © Ø	ጽ	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands B\					
Register an application	n				×
* Name					ĺ
The user-facing display name for this ap	plication (this can be changed later).				
OVOCAdmin	✓				
Supported account types					
Who can use this application or access the	his API?				
 Accounts in this organizational dire 	ctory only (AudioCodes Netherlands BV only - Single tenant)				
 Accounts in any organizational dire 	ctory (Any Azure AD directory - Multitenant)				
 Accounts in any organizational direction 	ctory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)				
Personal Microsoft accounts only					
Help me choose					
Redirect URI (optional)					
We'll return the authentication response	to this URI after successfully authenticating the user. Providing this now is optional and it can be				
changed later, but a value is required for	most authentication scenarios.				
Web ~	https://xxxx/ovoc/v1/security/actions/login				
By proceeding, you agree to the Microso	ft Platform Policies 🗗				
Register					
<					

3. Enter the name of the OVOC registration tenant.

- 4. Under Implicit grant and hybrid flows, select Accounts in any organizational directory (Any Azure AD Directory- Multitenant)
- 5. Click Register.

The newly registered application is displayed.

Figure 11-29: New Registered Application

= Microsoft Azu	Search resources, services, and docs (G+/)			3 @ A	AUDIOCODES NETHERLANDS BV			
Home > AudioCodes Netherlands BV								
AudioCoc Azure Active Directo	es Netherlands BV App registrations 🛷 …				×			
 Overview 	≪ + New registration ⊕ Endpoints ⊘ Troubleshooting ○ Refresh	2 Download 🖾 Preview features 🛛 🛇 Got feedback?						
 Preview features X Diagnose and solve 	(1) Try out the new App registrations search preview! Click to enable the preview. \rightarrow oblems				×			
Manage	Starting June 30th, 2020 we will no longer add any new features to Azure Active D provide feature updates. Applications will need to be upgraded to Microsoft Auther	irectory Authentication Library (ADAL) and Azure AD Graph. We will continu ntication Library (MSAL) and Microsoft Graph. Learn more	e to provide technical suppo	rt and security updat	tes but we will no longer \times			
 Groups External Identities 	All applications Owned applications Deleted applications							
Roles and administra	vrs 🔎 OVOC				×			
Administrative units								
Enterprise application	Display name	Application (client) ID		Created on	Certificates & secrets			
Devices	OVOC	59ab90b2-99a4-45d6-96c7-c	17e7352950c	5/25/2021	🔮 Current			
App registrations	OVOCApplication	72e9f409-9da5-4cc1-a5f0-72	4f611fba23	10/7/2021	🕑 Current			
Identity Governance	ov OVOCAdmin	db348b8c-c6e3-4afc-9dc7-11	2a84706843	10/17/2021	100 B			
Application proxy								
🔓 Licenses								
Azure AD Connect								
💭 Custom domain nan	5							
Mobility (MDM and	AM)							
Password reset	×							

- 6. Double-click the new application i.e. OVOCAdmin (in this example) to configure it.
- 7. In the navigation pane, select **Certificates & secrets**.

Figure 11-30:	Certificates	& secrets
---------------	--------------	-----------

	, P Search resources, services, and d	ocs (G+/)				Σ	Ŗ	ی 🧐	유 Ad	min@ocshost.eme Hocodes Netherlands	a 5 gv 🥐
Home > AudioCodes Netherlands BV >	OVOCAdmin										
🔶 OVOCAdmin Certif	icates & secrets 👒 …										×
•											
✓ Search (Ctrl+/) «	♡ Got feedback?										
Overview	Credentials enable confidential applications t	o identify themselves to t	he authentication servi	ce when receiving token	s at a web addressable locati	on (using	an HTTPS				^
di Quickstart	scheme). For a higher level of assurance, we i	ecommend using a certin	cate (instead or a client	t secret) as a credential.							
🚀 Integration assistant	Certificates										
Manage	Certificates can be used as secrets to prove the	ne application's identity w	hen requesting a toker	n. Also can be referred to	as public keys.						
Branding	_										
Authentication	↑ Upload certificate										
Certificates & secrets	Thumbprint		Start date	Expires	Certificate ID						
Token configuration	No certificates have been added for this appl	ication.									
API permissions											
Expose an API											
App roles	Client secrets										
A Owners	A secret string that the application uses to pr	ove its identity when requ	esting a token. Also ca	in be referred to as appli	cation password.						
Roles and administrators Preview	+ New client secret										
Manifest	Description	Expires	Value		Secret ID						
Support + Troubleshooting	bestipton	Dipres			beactio						
Troubleshooting	No client secrets have been created for this a	pplication.									
New support request											
-											× .

8. Click New client secret.

Figure 11-31: New client secret

			D 🖟 🖉		Admin@ocshost.emea AUDIOCODES NETHERLANDS BV	P
Home > AudioCodes Netherlands BV >	OVOCAdmin	Add a clie	nt secret		:	×
🛉 💡 OVOCAdmin Certif	icates & secrets 👒 🐇					
	m	Description		ovoc_mtsecret		
Search (Ctrl+/) «	Got feedback?	Expires		24 months	,	\sim
Overview	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at	a web				_
🏜 Quickstart	scheme), nor a righter rever or associatice, we recommend using a certainate (instead of a circle secret) as a credential.					
🚀 Integration assistant	Certificates					
Manage	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as	oublic				
Branding	, ,					
Authentication	↑ Upload certificate					
📍 Certificates & secrets	Thumbprint Start date Expires	Ce				
Token configuration	No certificates have been added for this application.					
 API permissions 						
 Expose an API 						
K App roles	Client secrets					
2 Owners	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application	in pas				
Roles and administrators Preview	A strandback sound					
11 Manifest	T New Clent secret					
Support + Troubleshooting	Description Expires Value	Seci				
/> Troubleshooting	No client secrets have been created for this application.					
New support request						
		Add	Cancel			

- 9. Enter a description and from the drop-down list select 24 months.
- 10. Click Add.

Figure 11-32: Client Secret Generated

	,○ Search resources, services, and	id docs (G+/)				D. 🗗 😳	'® 0 .	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >	OVOCAdmin							
🔶 OVOCAdmin Certif	ficates & secrets 👒 …							×
Search (Ctrl+/)	♡ Got feedback?							
📫 Quickstart	Credentials enable confidential applicatio scheme). For a higher level of assurance, v	ns to identify themselves to we recommend using a cert	the authentication servi ificate (instead of a client	ce when receiving tokens at a : secret) as a credential.	a web addressable loca	ion (using an HTTPS		Î
🚀 Integration assistant	Certificates							
Manage	Certificates can be used as secrets to prov	ve the application's identity	when requesting a toker	. Also can be referred to as p	oublic keys.			
Branding	Unlocal cont/Ecoto							
Authentication	T Upload certificate							
📍 Certificates & secrets	Thumbprint		Start date	Expires	Certificate ID			
Token configuration	No certificates have been added for this a	application.						
 API permissions 								
🔷 Expose an API								
App roles	Client secrets							
A Owners	A secret string that the application uses to	o prove its identity when re-	questing a token. Also ca	n be referred to as applicatic	in password.			
Roles and administrators Preview	have diget segret							
11 Manifest	+ New client secret							
Support + Troubleshooting	Description	Expires	3oJ70~6omHotZX8	Copy to dipt	e47e13c3-ae06-463d-9	cf8-901318dd7b37	n	
Troubleshooting		, 11) 2020	Sorra Sonniouska	Lon Drive of Data May in 1	e ne 1969 9600 4090 1			
New support request								U
								*

- **11.** Copy the secret Value to clipboard as its required in later configuration and cannot be retrieved once you leave this screen.
- **12.** In the navigation pane, select **Authentication**.
Figure 11-33: Authentication



- 13. Under Implicit grant and hybrid flows, select "ID tokens"
- 14. Click Save.
- 15. In the Navigation pane, select Token configuration

Figure 11-34: Token Configuration-Add

		DE 🕀 😷 🔅 🕐 Admin@ocshost.emea						
Home > AudioCodes Netherlands BV >	ovocAdmin a configuration 🛷 …	Add optional claim \times						
Search (Ctrl+/) «	♥ Got feedback?	Once a token type is selected, you may choose from a list of available optional claims.						
 Overview Quickstart Integration assistant Manage 	Optional claims Optional claims are used to configure additional information which is returned in one or more tokens. Learn more ge Add optional claim + Add groups claim	*Token type Access and ID tokens are used by applications for authentication. Learn morec? ● ID Access SAML						
Branding Authentication Certificates & secrets Certi	Claim 🖒 Description	Claim 1: Description so Sesson IL, Use Tor per-session User sign out tenant_try Resource tenant's country/region tenant_try Region of the resource tenant verified_primary_email Sourced from the user's PrimaryAuthoritativeEmail verified_secondary_email Sourced from the user's SecondaryAuthoritativeEmail verified_secondary_email verified_secondary_email Sourced from the user's SecondaryAuthoritativeEmail verified_secondary_email Zecondary_email Zecondary_email Zecondary_email Zecondary_email Zecondary_email Zecondary_email						
New support request		Add Cancel						

16. Click Add optional claim, choose ID type then upn optional claim and click Add to confirm.

Figure 11-35: Turn on Profile Permission



17. Select the **Turn on the Microsoft Graph profile permission** check box and then click **Add**. This adds the Profile permission to the API permissions list.

=	Microsoft Azure		vices, and docs (G+/)		E	Ę 9	چ ج	@ R	Admin@ocsho AUDIOCODES NETH	ost.emea IERLANDS BV
Home	Home > AudioCodes Netherlands BV > OVOCAdmin									
11	OVOCAdmin Toker	n configuration 👒								×
<mark>,</mark> ₽ s	earch (Ctrl+/) «	♡ Got feedback?								
👪 c	Overview	Optional claims								
6 4 C	Quickstart	Optional claims are used to confi	gure additional information which is returned in o	ne or more tokens. Learn more 🗗						
💉 Ir	ntegration assistant	+ Add optional claim + A	dd groups claim							
Mana	ge									
🚍 B	randing	Claim 🗈	Description			Token	tvpe ↑⊥		Optional settings	
Э А	uthentication	unn	An identifier for the user that can be used with	h the username hint narameter: not a durable identifie	r for the user and s	ID			Default	
📍 C	ertificates & secrets	apri	fariacitatici foi die dee diat can be abed me						beldart	
Т	oken configuration									
→ A	PI permissions									
🙆 E	xpose an API									
🔨 А	pp roles									
🎎 C	Jwners									
🤱 R	oles and administrators Preview									
II N	Manifest									
Supp	ort + Troubleshooting									
∥ Т	roubleshooting									
<u>2</u> N	lew support request									
,										

This configuration assumes that all operators have been added to the Active Directory in UPN format e.g. Johnb@firm.com. If operators have been added in email format e.g. John.Brown@firm.com then they will not be able to connect to OVOC in the multitenancy setup.

18. In the Navigation pane, select **API permissions**.

ome > AudioCodes Netherlands	3V > OVOCApplication		Poquest ADI permission		
0V/0CApplication	API pormissions		Request API permission	15	
	T API permissions ×		Select an API		
Search (Ctrl+/)	« O Refresh O Got feedbac	ck?	Microsoft APIs APIs my organization	n uses My APIs	
Overview			Commonly used Microsoft APIs		
Quickstart	The "Admin consent required"	column shows the			
Integration assistant	organization, or in organizatio	ons where this app v	Microsoft Graph		
anage	Configured permissions		Take advantage of the tren Access Azure AD, Excel, Int	nendous amount of data in Office 365, Enterpris tune, Outlook/Exchange, OneDrive, OneNote, Sh	e Mobility + Security, and Windows 10. arePoint, Planner, and more through a
Branding	Applications are authorized to call	APIs when they ar			
Authentication	all the permissions the application	needs. Learn more			
Certificates & secrets	+ Add a permission 🗸 Gran	t admin consent f			
Token configuration	API / Permissions name	Туре	Azure Data Catalog	Azure DevOps	Azure Rights Management Services
ioicen conngaration			Programmatic access to Data Catalog resources to register, annotate and	Integrate with Azure DevOps and Azure DevOps server	Allow validated users to read and write protected content
API permissions	✓ Microsoft Graph (3)				
API permissions Expose an API	Group.Read.All	Delegated	search data assets		
API permissions Expose an API App roles	Group.Read.All	Delegated Delegated	search data assets		
API permissions Expose an API App roles Owners	✓ Microsoft Graph (3) Group.Read.All profile User.Read	Delegated Delegated Delegated	search data assets	Data Export Service for	🙈 Dynamics 365 Business
API permissions Expose an API App roles Owners Roles and administrators Preview	Microsoft Graph (3) Group.Read.All profile User.Read	Delegated Delegated Delegated	search data assets Azure Service Management Programmatic access to much of the functionality available through	Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM consultation to an external	Dynamics 365 Business Central Programmatic access to data and functionabit in Damandic 265 Businese

Figure 11-37: API Permissions

19. Click Add a permission and then click the Microsoft Graph link.

Figure 11-38: Delegated permissions

\equiv Microsoft Azure \checkmark Search	h resources, services, and docs (G+/)		D 🕼 🗘 🏟 🕐	Admin@ocshost.emea
Home > AudioCodes Netherlands BV >	OVOCAdmin	Request API permissions		×
	Contractions of the second	All APIs		
Search (Ctrl+/) «	Got Teedback?	Inttps://graph.microsoft.com/ Docs ⊡ What type of permissions does your application require?		
 Quickstart Integration assistant 	A Starting November 9th, 2020 end users will no	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a bac signed-in user.	kground service or daemon without a
Manage Branding & properties	• The "Admin consent required" column shows th your organization, or in organizations where the	ie is		
 Authentication Certificates & secrets 	Configured permissions Applications are authorized to call APIs when they	ar		
Token configuration API permissions	all the permissions the application needs. Learn mo + Add a permission ✓ Grant admin consent	on I f		
 Expose an API App roles 	API / Permissions name Type			
Owners Roles and administrators Preview	profile Delegated User.Read Delegated			
Manifest Support + Troubleshooting	To view and manage permissions and user consent	Add permissions Discard		

- 20. Click Delegated permissions.
- 21. Select permission User.Read.All and then click Add permissons.

	ch resources, services, and docs (G+/)	∑ ₽ ¢ ⁹ ⊗	0 Admin@ocshost.emea					
Home > AudioCodes Netherlands BV	> OVOCAdmin permissions 🛷 …	Request API permissions						
	🕐 Refresh 🔰 🖗 Got feedback?	C All API: permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more						
 Overview Quickstart Integration assistant 	A Starting November 9th, 2020 end users will no	Permission to the second seco	Admin consent required					
Manage	The "Admin consent required" column shows th your organization, or in organizations where th	e V User (2)						
 Authentication Certificates & secrets 	Configured permissions	User.Read O Sign in and read user profile	No					
 Token configuration API permissions 	all the permissions the application needs. Learn no + Add a permission ✓ Grant admin consent	n Read all users' full profiles	No					
 Expose an API App roles 	API / Permissions name Type	User Read Write O Read and write access to user profile	No					
Owners Roles and administrators	profile Delegated	User.ReadWirite.All O Read and write all users' full profiles	Yes					
Preview Manifest Support + Troubleshooting	To view and manage permissions and user consent	Add permissions Discard	v					

Figure 11-39: Delegated permissions

The configured API permissions are displayed.

Figure 11-40: Co	nfigured API	Permissions
------------------	--------------	-------------

= Microsoft Azure	Search resources, services, and docs (G+/)			\sum	Ŗ	L ² &	3 (?)	<u>ه</u>	Admin@ocshost.eme audiocodes netherland	ea s bv 🅐
Home > AudioCodes Netherlands BV > OVOCAdmin											
₋ OVOCAdmin	API permissions 👒 🐇										\times
Search (Ctrl+/)	≪ 🕐 Refresh 🖗 Got feed	oack?									
Overview	A You are editing permission	s) to your applicatio	n, users will have to consent even if they	've already done so previously.							
 Guicestait Integration assistant Manage 	The "Admin consent requir your organization, or in org	ed" column shows th anizations where th	e default value for an organization. How is app will be used. Learn more	vever, user consent can be custor	nized per p	ermissior	i, user, or a	pp. This co	olumn may r	not reflect the value in	×
Branding & properties Configured permissions Authentication Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent							clude				
→ API permissions	API / Permissions name	Type	Description	Adr	nin conse	nt requ	. Status				
 Expose an API 	✓ Microsoft Graph (3)										
App roles	profile	Delegated	View users' basic profile	No							
A Owners	User.Read	Delegated	Sign in and read user profile	No							
Roles and administrators Preview	User.Read.All	Delegated	Read all users' full profiles	Yes			🔺 No	t granted	for AudioC		
 Manifest Support + Troubleshooting 	To view and manage permission	s and user consent	, try Enterprise applications.								

22. Click Grant admin consent for <Tenant_Name> link to grant consent for the requested permissions for all accounts for this tenant, and then click Yes to confirm.



Figure 11-41: Grant Admin Consent for all Accounts

23. In the Navigation pane, select App roles and then click Create app role.

Figure 11-42: App roles

		urces, services, and docs (G+/				Þ.	Ģ	 § Ø	ጽ	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >	OVOCAdmin									
🔢 OVOCAdmin App	roles 🖈 …									×
Search (Ctrl+/) « Overview Overview Quickstart Integration assistant	+ Create app role App roles App roles are custom ro as permissions during a How do I assign App rol	Cot feedback?	iers or apps. The application defines and	publishes the app r	oles and interprets them					
Branding	Display name	Description	Allowed member types	Value	ID	State				
 Authentication 	No app roles have bee	n added.								
📍 Certificates & secrets										
Token configuration										
 API permissions 										
Expose an API										
App roles										
Roles and administrators Preview										
Manifest										
Support + Troubleshooting										
Troubleshooting										
New support request										
¢										

24. Create an app role with Admin permissions:

- a. In the Display Name field, enter "Administrators" or "Admins"
- b. Select Users/Groups check box.
- c. Enter value "OVOCAdmin"
- d. Select the do you want to enable this app role check box.
- e. Click Apply

Figure 11-43: Admin Role

Edit app role	×
Delete	
Display name * (i)	
Administrator	
Allowed member types * (i)	
• Users/Groups	
Applications	
Both (Users/Groups + Applications)	
Description * ①	
OVOC Admins	
Do you want to enable this app role? 🕕	
Apply Cancel	

25. Repeat the above steps to create an App role with Operator permissions with value 'OVOCOperator''.

Figure	11-44:	Operator	Role
--------	--------	----------	------

Edit app role	×
Delete	
Display name * ①	
Operator	
Allowed member types * ① Output Outpu	
Applications	
Both (Users/Groups + Applications)	
Value * (i)]
Description * ()	
OVOC Operators	
Do you want to enable this app role? 🛈	
Apply Cancel	

26. Repeat the steps described for adding "Admin" role above to create an app role with Monitor permissions with value "OVOCMonitor".

Figure 11	-45: Ope	rator Role
-----------	----------	------------

Edit app role	×
🔟 Delete	
Display name * 🛈	
Monitor	
Allowed member types * 🥡	
• Users/Groups	
Applications	
Both (Users/Groups + Applications)	
Value * i	
OVOCMonitor	
Description * (i)	
OVOC Monitors	
Do you want to enable this app role? (i)	
Apply Cancel	

27. Repeat the steps described for adding "Admin" role above to create an app role with Monitor permissions with value "OVOCOperatorLite".

Figure 11-46: OVOC Operator Lite

Create app role	×
Display name * 🕡	
OperatorLite	~
Allowed member types * 🕡	
Users/Groups	
O Applications	
Both (Users/Groups + Applications)	
Value * 🛈	
OVOCOperatorLite	\sim
Description * 🕡	
OVOC Lite Operators	~
Do you want to enable this app role? 🕕	
Apply Capcel	
Apply Cancer	

The new roles are displayed:

Figure 11-47: App roles

\equiv Microsoft Azure		resources, services, and c	ocs (G+/)			D 🖓 🖨	\$ 0 A	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherla	inds BV >	OVOCAdmin						
👖 OVOCAdmin	Аррі	roles 🖈 …						×
Search (Ctrl+/) Overview Quickstart	~	+ Create app role App roles App roles are custom ri	Sot feedback?	or apps. The application defines and	publishes the app roles i	and interprets them		
💉 Integration assistant		as permissions during a	uthorization.					
Manage		How do I assign App ro	les					
Branding & properties		Display name	Description	Allowed member types	Value	ID	State	
Authentication		OVOCLite	OVOC Lite Operators	Users/Groups	OVOCOperatorLite	21b9b008-0e33-4d53	Enabled	
📍 Certificates & secrets		Monitor	OVOC Monitors	Users/Groups	OVOCMonitor	306f38aa-b02e-4c8f-	b Enabled	
III Token configuration		Operator	OVOC Operators	Users/Groups	OVOCOperator	fa355d53-7b7c-4b46	Enabled	
API permissions		Administrator	OVOC Administrators	Users/Groups	OVOCAdmin	c0ab92de-1dbb-4695	Enabled	
Expose an API								
App roles								
A Owners								
& Roles and administrators Preview								
Manifest								
Support + Troubleshooting	~							

- 28. In the Navigation pane, select the **Overview** page for the application.
 - Figure 11-48: Overview Page

	Dearch resources, services, and docs (G+/)	dmin@ocshost.emea DIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV	3V >	
👖 OVOCAdmin 🖉 🚽	m	×
	« 💼 Delete 🖶 Endpoints 🐻 Preview features	
Overview		î
📣 Quickstart	Disnlav name CNOCAdmin Client credentials D certificate 1 secret	
💉 Integration assistant	Application (client) ID : db348b8c-c6e3-4afc-9dc7-1b2a84706843 Redirect URIs : 1 web, 0 spa, 0 public client	
Manage	Object ID : e893a8a8-5435-480c-b9ec-1684f2c55872 Application ID URI : Add an Application ID URI	
Branding	Directory (tenant) ID : c524b5f5-fd18-43c0-964c-bc5d35525eaa Managed application in I : OVOCAdmin	
Authentication	Supported account types : Multiple organizations	
📍 Certificates & secrets	1 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates	but we will no
III Token configuration	longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more	
 API permissions 	A	×
📤 Expose an API	Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without vertiled publishers. Add MPN ID to verify publisher	
App roles	Get Started Documentation	
A Owners		
Roles and administrators Preview	Build your application with the Microsoft identity platform	
Manifest	build your application with the interopert identity platform	
Support + Troubleshooting	The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more management and set of the second seco	
Troubleshooting		
Rew support request	🌰 🙉 🛻 🏴 🗰 🐘 🔊 🔊	
< c		~

- **29.** Note the following values as they must later be configured in Configuring OVOC Web Azure Settings Multitenant Setup below
 - Application (client) ID
 - Directory (tenant) ID
- **30.** Add Main Tenant Azure groups and add members as described in Create Azure Groups and Assign Members on page 124
- **31.** Add operators of external tenants and assign them roles as described in Add External Tenant Operators and Assign Roles on page 129
- **32.** Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings Multitenant Setup below

Configuring OVOC Web Azure Settings - Multitenant Setup

This section describes how to configure Azure authentication in the OVOC Web interface for multitenant deployments. When operators login to OVOC, they're assigned with an OVOC security level, i.e. Admin, Operator or Monitor' based on their assigned role on Azure and their Tenant ID which reflects their tier permissions i.e. Tenant, Channel or Customer operator permissions. These details are sent to OVOC Azure via the Token authentication mechanism.

- > To configure authentication of OVOC operators using Azure AD:
- In the OVOC Web, open the Authentication page (System > Administration > Security > Authentication), and then from the 'Authentication Type' drop-down, select AZURE.

Figure 11-49: Azure Authentication

Links
or_Links
r_Links
nts_Group
Submit
10

- 2. From the 'Azure AD Path Type File' drop-down, select **Organizations** (default). OVOC can access Azure AD in the enterprise network if a standard service is purchased.
- 3. In the 'Azure Tenant ID' field, enter the Tenant ID of the Main Tenant.
- 4. In the 'Azure Client ID' field, enter the ID of the Azure AD client of the Main Tenant.
- 5. In the 'Azure Client Secret' field, enter the client secret of the Main Tenant.
- 6. In the screen section 'GW / SBC / MSBR Authentication', select the option 'Use AD Credentials for Device Page Opening' for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to OVOC. The AudioCodes device will then perform authentication with the Azure AD and login to the device is attempted with same AD username / password instead of the local device user name / password. Note that the device must also be configured to authenticate with the same AD.

When a Main Tenant operator attempts to connect to OVOC, OVOC verifies the mapped Azure User Group to which the operator is a member.

- In the Tenant Details screen under the **Operators** tab, the parameter **AD Authentication: Group Name** points to the Azure group which includes the **Main Tenant** operators who are authorized to login to OVOC using this method.
- If the Azure AD successfully validates that the operator belongs to the AD Authentication group (see highlighted group in the example below), its and allowed access.

Figure 11-50: AD Authentication Group Name

TENANT DETAILS				
General	SNMP	HTTP	Operators	License
Local Authentication: Ass	igned Operators			
AD Authentication: Group	Name	hdvoip		



 > Diagnose and solve problems > Manage > Members > Members > Members > Members > Members > Members > Source > Cloud > Source > Cloud > Source > Cloud > Type > Security > Object Id > 9f5e30af-2391-420b-b011-86ac9f79921c > 0 Object Id > 9f5e30af-2391-420b-b011-86ac9f79921c > 0 Object Id > 9f5e30af-2391-420b-b011-86ac9f79921c > 0 Object Id > 9f5e30	0 Overview	Cot feedback	?		
IProperties IProperties <	X Diagnose and solve problems Manage	HD hdvoip			
▲ Members Membership type Assigned □ ▲ Owners Source Cloud □ ▲ Roles and administrators Type Security □ ▲ Administrators Type Security □ ▲ Administrators Object Id 9f5e30af-2391-420b-b011-86ac9f79921c □ ▲ Applications Creation date 3/26/2020, 2:51:03 PM □ ▲ Licenses □ □ □ ↑ Azure role assignments Direct members □	Properties				
▲ Owners Source Cloud □ ▲ Roles and administrators Type Security □ ▲ Administrative units Object Id 9f5e30af-2391-420b-b011-86ac9f79921c □ ● Applications Creation date 3/26/2020, 2:51:03 PM □ ■ Applications Creation date 3/26/2020, 2:51:03 PM □ ● Azure role assignments Direct members □ ▲ Access reviews Direct members □ □ ▲ Advitlogs Group memberships Owners Total members ▲ Advitlogs ▲ 0 ④ 4 ④ 4 ●	A Members	Membership type	Assigned		D
▲ Roles and administrators ▲ Administrative units ④ Administrative units Object Id ● Object Id <td>A Owners</td> <td>Source</td> <td>Cloud</td> <td></td> <td>D</td>	A Owners	Source	Cloud		D
Administrative units open Group memberships Object Id Open attribution Applications Creation date 3/26/2020, 2:51:03 PM Licenses Azure role assignments Direct members Activity Activity Activity Activity Activity Activity Audit logs Group memberships Ourper Bulk operation results Audit logs Bulk operation results Audit logs Audit log	Roles and administrators	Turpe	Security		[Ps.
Group memberships Object Id 9f5e30af-2391-420b-b011-86ac9f79921c Applications Creation date 3/26/2020, 2:51:03 PM Licenses Licenses Azure role assignments Direct members Direct members Direct members Activity	Administrative units	1790	Security		41
Applications Creation date 3/26/2020, 2:51:03 PM ↓ Licenses Direct members Azure role assignments Direct members Activity ↓ 4 Total ▲ 4 User(s) ▲ 0 Group(s) 0 Device(s) ⊕ 0 Other(s) ▲ Access reviews Group memberships Owners Total members ▲ Audit logs Group memberships Owners Total members ▲ Bulk operation results ▲ 0 ▲ 2 0 ④ 4	🔅 Group memberships	Object Id	9f5e30af-2391-420b-b011-86	ac9f79921c	\square
Licenses Azure role assignments Direct members Activity Access reviews Audit logs Bulk operation results Bulk operation results Activity Acterst reviews Bulk operation results Activity Activity Activity	Applications	Creation date	3/26/2020, 2:51:03 PM		D
Azure role assignments Direct members Activity	Licenses				
Activity Image: Constraint of the state of the sta	Azure role assignments	Direct members			
Access reviews Group memberships Owners Total membersh Audit logs & 0 & 0 & 4	Activity	🕀 4 Total 🛛 🔒 4 User	(s) 🏼 🎎 0 Group(s)	0 Device(s)	0 Other(s)
Audit logs Group memberships Owners Total members Bulk operation results 20 20 0					
👃 Bulk operation results 🛛 🚨 0 🖉 4	Audit logs	Group memberships	Owners		lotal members
	🚴 Bulk operation results	▲▲ 0	<mark>2</mark> 0		ال 🐼 4

7. In the screen section Authorization Level Settings, configure the user group names exactly as defined on Azure in Create Azure Groups and Assign Members on page 124. When an operator is not assigned to a group on Azure, the parameter 'Default Operator Type and Security Level' is applied.

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
ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS	
Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group

Figure 11-52: Authorization Level Settings



Home > <u>AudioCodes - SQA LIVE</u> >					
AudioCodes - SQA LIVE - Azure Active Dir	 rectory				×
~	🗚 New group 🞍 Download groups 📋 Delete 💍 Ref	fresh 🔲 Columns 🛛 🖗 Got feedback?			
All groups					
Deleted groups	ems	× ∀ Filter ∨			
🗙 Diagnose and solve problems	Search mode Contains				
Settings	6 groups found				
l General	Name	Object Id	Group Type	Membership Type	Email
Expiration					
Naming policy Naming policy	EMS_Tenant_Operator_Links	3a413504-47d2-40b3-a061-0edbf797d2e1	Security	Assigned	
Activity	EM EMS_Tenant_Admin_Links	67741e92-d754-4e0b-b1ef-230dad8a730f	Security	Assigned	
Privileged access groups (Preview)	EM EMS_Tenant_Monitor_Links	c72c88a8-86d8-4c44-928d-0cdb7f584a9c	Security	Assigned	
Sint Access reviews	EM EMS_Operator	ca7cc0f2-5f27-478a-b1cd-4e3157141ab9	Security	Assigned	
 Audit logs Bulk operation results 	EM EMS_Monitor	eafbf1b2-6283-4d4b-a3c7-ab4cc2b715e0	Security	Assigned	
Troubleshooting + Support	EMS_Admin	f5893124-7eeb-41cd-92d5-9ca6c6cf8282	Security	Assigned	
New support request					

8. In the Tenant Details, enter the "Azure Tenant ID" of the **external managed tenant** as shown in the screen below.

SNMP	HTTP	Operators	License
	hdvoip_net		
	False		•
ool)			•
	*		
	XXXXXXXXXX		
	None		<u>۰</u>
			Close
	SNMP	SNMP HTTP hdvoip_net False [minimum] [minimum] [minimum] [minim]	SNMP HTTP Operators Indvoip_net False Indvoip_net Image: South State St

Figure 11-54: Tenant Details

9. If you are managing channels, in the Channels Details, enter the "Azure Tenant ID" of the **external managed tenant** as shown in the screen below

Figure 11-55: Channel Details

CHANNEL DETAILS	
Name	Itc_carmel
Description	
Tenant	hdvoin net
Azure Tenant ID	
Azore renancio	
	Close OK

Upgrading from Single Tenant to Multitenant

This procedure describes how to upgrade from Single tenant to Multitenant setup.



Guest user login is not supported for both Main Tenant and external tenant guest users once multitenancy is enabled in this procedure.

> To reconfigure a single tenant setup to multitenant:

- **1.** Login to the Azure portal as Global Administrator.
- 2. In the Navigation pane, select **App registrations** and select the registered OVOC application (the example used in this section "OVOCApplication" is selected below).

Figure 11-56: App registrations

≡ Microsoft Azure 🔎	Search resources, services, and docs (G+/)	D 🕼 🗘	' © ଜି	Admin@ocshost.eme audiocodes netherlands	а вv 🥐
Home > AudioCodes Netherlands	BV				
AudioCodes Net	therlands BV App registrations 🛷 …				×
	« 🕂 Hew registration) Endpoints 🧷 Troubleshooting 🕐 Refresh 🞍 Download	Preview features 🕴 ♡ Got feedback	?		
0 Overview					
Preview features	igcell Try out the new App registrations search preview! Click to enable the preview. $ ightarrow$				×
X Diagnose and solve problems					
Manage	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authent	ication Library (ADAL) and Azure AD Graph. W	e will continue to prov	ide technical support and	×
🚨 Users	security updates but we will no longer provide feature updates. Applications will need to be upgra	ded to Microsoft Authentication Library (MSAI) and Microsoft Graph	n. Learn more	
A Groups					
External Identities	All applications Owned applications Deleted applications				
Roles and administrators	\mathcal{P} Start typing a name or Application ID to filter these results				
Administrative units	DE Demo-Dis-Client	39d85e72-b473-4f73-9035-8de345479fac	5/11/2021	A Expiring soon	^
Enterprise applications	ov <u>OVOC</u>	59ab90b2-99a4-45d6-96c7-c17e7352950	5/25/2021	🛛 Current	
Devices	sy SynergyApp-wave1-testing	fb6d5742-c44e-4b00-acec-fc5190a41a10	6/2/2021	🛛 Current	
App registrations	Demo-MS-Teams-PS-Module	d058ac2e-871e-426c-a67e-73f1e4772e8c	6/5/2021	🛛 Current	
Identity Governance	DE Demo111	35c18ae9-d35e-4d20-a8d9-77030bcb328	c 7/6/2021	-	
Application proxy	FD Fundatie Demo	18138483-2c21-45cd-b394-f98b228890d	8/20/2021	-	
Licenses	AuthenticationDemo	55191ad0-692e-41cd-a0e6-7ed938bad2e	1 9/3/2021	🛛 Current	
Azure AD Connect	ov OVOCApplication	72e9f409-9da5-4cc1-a5f0-724f611fba23	10/7/2021	Current	×

3. In the Navigation pane, select **Authentication**.

Figure 11-57: OVOC Application

\equiv Microsoft Azure P Search res	ources, services, and docs (G+/)	E	다 다 🖓 🕲 🕜 첫 Adm	in@ocshost.emea codes netherlands bv
Home > AudioCodes Netherlands BV >					
🔣 OVOCApplication 🖉					×
	<u> </u>				
Search (Ctrl+/)	📗 Delete 🌐 Endpoint	Preview features			
R Overview	∧ Eccentials				Í
🗳 Quickstart	Display pame	· OVOCAmplication	Client evidentials	· O sostificato 1 sosset	
💉 Integration assistant	Display name	: OVOCApplication	Client credentials	: U certificate, I secret	
Mapage	Object ID	 72691409-9085-4001-8510-724161110825 ddb67f46-8857-469c-8915-2829b3e377c1 	Application ID URI	: Add an Application ID LIRI	
Propring	Directory (tenant) ID	: c524b5f5-fd18-43c0-964c-bc5d35525eaa	Managed application in	: OVOCApplication	
	Supported account type	s: Multiple organizations	3 11		
Authentication					
Certificates & secrets	Starting June 30th, and security undate	2020 we will no longer add any new features to Azure Active D	irectory Authentication Library (ADAL) and A vill need to be ungraded to Microsoft Author	zure AD Graph. We will continue to provide tech	nical support ×
Token configuration	and security update	is but we will no longer provide reactire dpdates. Applications t	in need to be upgraded to Microsoft Addres	initiation clonary (work) and with osoft oraph. Le	anniore
 API permissions 	A Starting November	9th 2020 and users will no longer he shie to grant concent to	newly registered multitenant anne without y	arified publishers. Add MPN ID to varify publish	×
 Expose an API 	Juning Hovember	Sti, 2020 chu tacis mil no longer de adic lo grant consent to	newly registered matteriant upps without v	enned publishers. Add with the to serily publish	*
K App roles	Get Started Docum	entation			
A Owners					
& Roles and administrators Preview		Build your application v	vith the Microsoft ic	lentity platform	
Manifest Support + Troubleshooting		The Microsoft identity platform is an authentication create modern, standards-based authentication solu	n service, open-source libraries, and appl tions, access and protect APIs, and add s	ication management tools. You can ign-in for your users and customers.	

Figure 11-58: Authentication Screen



- 4. Under account types, select Accounts in any organizational directory (Any Azure AD directory Multitenant) and then click Save.
- 5. In the Navigation pane, select Token configuration

Figure 11-59: Token Configuration-Add

Home > AudioCodes Netherlands BV >	OVOCApplication	Add optional clair	m ×
OVOCApplication Search (Ctrl+/) «	Token configuration 🖈 … R Got feedback?	Once a token type is selected, you	u may choose from a list of available optional claims.
 Overview Quickstart Integration assistant Manage 	Optional claims Optional claims are used to configure additional information which is returned in one or more tokens. Learn more 2* + Add optional claim + Add groups claim	* Token type Access and ID tokens are used by ID Access SAML	applications for authentication. Learn more $\underline{\mathcal{C}}^{\mathfrak{g}}$
 Branding Authentication 	Claim 1 Description	Claim 1	Description
↑ Certificates & secrets	No results.	id sid	Session ID, used for per-session user sign out
III Token configuration		tenant_ctry	Resource tenant's country/region
		tenant_region_scope	Region of the resource tenant
 Expose an API 		🔽 upn	An identifier for the user that can be used with the user
App roles		verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
🎎 Owners		verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail
🕹 Roles and administrators Preview		vnet vnet	VNET specifier information
III Manifest		xms_pdl	Preferred data location
Support + Troubleshooting		xms_pl	User-preferred language
Troubleshooting		xms_tpl	Tenant-preferred language
New support request		ztdid	Zero-touch Deployment ID
		Add Cancel	

6. Click Add optional claim, choose ID type then upn optional claim and click Add to confirm.

Figure 11-60: Turn on Profile Permission



 Select the Turn on the Microsoft Graph profile permission check box and then click Add. This adds the Profile permission to the API permissions list.

Figure 11-61: Optional claims Added

Home > AudioCodes Netherlands BV >	> OVOCApplication				
 OVOCApplication	Token configuratio	n 🖈 …			×
	🖗 Got feedback?				
 ₩ Overview ▲ Quickstart ✓ Integration assistant Manage 	Optional claims Optional claims are used to con + Add optional claim +	ifigure additional information which is returned in one or more tokens. Learn more ²⁸ Add groups claim			
Branding	Claim 🔨	Description	Token type ↑↓	Optional settings	
Authentication Contificates Researcts	upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier f	ID	Default	
Token configuration					
 API permissions 					
Expose an API					
App roles					
A Owners					
& Roles and administrators Preview					
Manifest					
Support + Troubleshooting					

8. In the Navigation pane, select **API permissions**.

Figure 11-62: API Permissions



9. Click Add a permission and then click the Microsoft Graph link.

Figure 11-63: Delegated permissions

\equiv Microsoft Azure \checkmark Search	n resources, services, and docs (G+/)		\geq	Ç () _@	@ &	Admin@ocshost.emei audiocodes netherlands	а вv 🌳
Home > AudioCodes Netherlands BV >	OVOCAdmin	Request API permissions						×
_Ə OVOCAdmin API p	ermissions 🖉 …							
Search (Ctrl+/) « Overview	🕐 Refresh 🔰 🕅 Got feedback?	All APIs Microsoft Graph https://graph.microsoft.com/ Docs c? What have of permissione doce your application require?						
 Quickstart Integration assistant 	A Starting November 9th, 2020 end users will no lo	Delegated permissions does your application require: Delegated permissions Your application needs to access the API as the signed-in user.		Application Your applic signed-in u) permissions ation runs as	s s a backgrour	id service or daemon without	a
Manage	The "Admin consent required" column shows the your organization, or in organizations where this							
Branding & properties Authentication Certificates & secrets	Configured permissions Applications are authorized to call APIs when they an							
IOKen configuration API permissions	+ Add a permission ✓ Grant admin consent f							
 Expose an API App roles 	API / Permissions name Type							
A Owners	V Microsoft Graph (2) profile Delegated							
& Roles and administrators Preview	User.Read Delegated							
Manifest Support + Troubleshooting	To view and manage permissions and user consent,	Add permissions Discard						

10. Click Delegated permissions.

Figure 11-64: Microsoft Graph Permissions

≡ Microsoft Azure 🔎 Sea	rch resources, services, and docs (G+/)		D & \$ \$ \$ \$ \$ \$ \$	Admin@ocshost.emea Audiocodes Netherlands by
Home > AudioCodes Netherlands BV	> OVOCApplication	Request API permissions		×
		< All APIs		
Search (Ctrl+/) « Integration assistant	Refresh Got feedback?	✓ Group (1)		
Manage	() The "Admin consent required" column shows the	Group.Read.All ① Read all groups	Yes	
Branding Authentication	organization, or in organizations where this app v	Group.ReadWrite.All ① Read and write all groups	Yes	
🕈 Certificates & secrets	Configured permissions Applications are authorized to call APIs when they are	> GroupMember		
Token configuration APL nermissions	all the permissions the application needs. Learn more	> IdentityProvider		
 Expose an API 	+ Add a permission ✓ Grant admin consent f API / Permissions name Type	> IdentityRiskEvent		
App roles	✓ Microsoft Graph (2)	> IdentityRiskyUser		
Roles and administrators Preview	profile Delegated User.Read Delegated	> IdentityUserFlow		
Manifest		> IMAP		
Support + Troubleshooting	To view and manage permissions and user consent, t			,
Troubleshooting				
New support request	v	Add permissions Discard		

- 11. Select permission Group.Read.All and then click Add permission.
- 12. Add another Delegated permission User.Read.All and then click Add permissons.

	nd docs (G+/)	D D	🖉 🚳 🕐 🕅 Admin@ocshost.emea
Home > AudioCodes Netherlands BV > OVOCAdmin	\$	Request API permissions	×
Search (Ctrl+/) « C Refresh)	₹ Got feedback?	C All APIs permission, user, or app. This column may not reflect the value in your organizat more	tion, or in organizations where this app will be used. Learn
 Overview Quickstart Integration assistant 	mber 9th, 2020 end users will no lo	Permission > IdentityRiskyUser	Admin consent required
Manage The "Admin c Branding & properties	onsent required" column shows the tion, or in organizations where this	V User (2)	
Authentication Configured peri Certificates & secrets Applications are au Ithe permissions Ithe permissions	nissions thorized to call APIs when they ar the application needs. Learn mon	✓ User.Read ○ Sign in and read user profile ✓ User.Read All ○ Read all users' full profiles	No Yes
→ API permissions + Add a permission	ion 🗸 Grant admin consent f	User.ReadBasic.All ① Read all users' basic profiles	No
Expose an API API / Permissions API / Permissions API / Permissions	name Type	User.ReadWrite ① Read and write access to user profile	No
Owners Profile Profile	Delegated	User.ReadWrite.All ③ Read and write all users' full profiles	Yes
Interstand Gammaddors UserRead UserRead UserRead To view and manage Support + Troublechooting	Delegated e permissions and user consent, t	Add permissions Discard	

Figure 11-65: Delegated permissions

13. Click Grant admin consent for <Tenant_Name> link to grant consent for the requested permissions for all accounts for this tenant, and then click Yes to confirm.

	Figure 11-	-66: Gra	ant Admin (Consent for all	Accounts		
			s, services, and docs (G+/)			G 🖉 🐵 🛛 R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV.
Home > AudioCodes Netherlands BV :	> OVOCAdmin permissions 🖈 …						
P Search (Ctri+/) «	🕐 Refresh 🖗 Got fee	edback?					
🗮 Overview	Grant admin consent	confirmation.					
🚳 Quickstart	Do you want to grant conse	ent for the requested p	ermissions for all accounts in Aud	ioCodes Netherlands BV? This will update a	ny existing admin consent records this appl	ication already has to match w	hat is listed below.
🚀 Integration assistant	Yes No						
Manage							
Branding & properties							
Authentication	1 The "Admin consent requ	uired" column shows the	lefault value for an organization. Howev	ver, user consent can be customized per permission	, user, or app. This column may not reflect the valu	e in your organization, or in organi	zations where this app will be
📍 Certificates & secrets	used. Learn more						
Token configuration	Configured permissions						
 API permissions 	Applications are authorized to	call APIs when they are	granted permissions by users/admin	ns as part of the consent process. The list of cor	nfigured permissions should include		
lexpose an API	all the permissions the applica	ition needs. Learn more	about permissions and consent				
🔣 App roles	+ Add a permission 🗸	Grant admin consent fo	r AudioCodes Netherlands BV				
🎒 Owners	API / Permissions name	Type	Description	Admin consent requ	. Status		
 Roles and administrators Preview 	✓Microsoft Graph (4)						
Manifest	Group.Read.All	Delegated	lead all groups	Yes	▲ Not granted for AudioC •••		
Support + Troubleshooting	profile	Delegated	/iew users' basic profile	No			
P Troubleshooting	User.Read	Delegated	ign in and read user profile	No			
 Now support request 	User.Read.All	Delegated	lead all users' full profiles	Yes	▲ Not granted for AudioC ····		

14. In the Navigation pane, select App roles and then click Create app role.

To view and manage permissions and user consent, try Enterprise applie

Figure 11-67: Create App Roles

≡ Microsoft Azure		2	Ŗ	¢® s) 0	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >	OVOCApplication					
OVOCApplication	App roles 🖈 …					×
Search (Ctrl+/) «	+ Create app role S Got feedback?					
Overview	Ann roles					
i Quickstart	App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them					
💉 Integration assistant	as permissions during authorization.					
Manage	How do Lassign App roles					
Branding						
Authentication						
📍 Certificates & secrets						
Token configuration						
API permissions						
Expose an API						
App roles						
A Owners						
& Roles and administrators Preview						
Manifest						
Support + Troubleshooting						
Troubleshooting						
New support request						

15. Create an app role with Admin permissions:

- a. In the Display Name field, enter "Administrators" or "Admins"
- b. Select Users/Groups check box
- c. Enter value "OVOCAdmin"
- d. Select the do you want to enable this app role check box.
- e. Click Apply

Figure 11-68: Admin Role

Edit app role	×
Delete	
Display name * (i)	
Administrator	
Allowed member types * (i)	
• Users/Groups	
Applications	
Both (Users/Groups + Applications)	
Description * ①	
OVOC Admins	
Do you want to enable this app role? 🕕	
Apply Cancel	

16. Repeat the above steps to create an App role with Operator permissions with value 'OVOCOperator''.

Edit app role	×
Delete	
Display name * 🛈	
Operator	
Allowed member types * 🛈	
• Users/Groups	
O Applications	
Both (Users/Groups + Applications)	
Value * (i)	
OVOCOperator	
Description * (i)	
OVOC Operators	
Do you want to enable this and role?	
Apply Cancel	

17. Repeat the steps described for creating "Admin" role above to create an app role with Monitor permissions with value "OVOCMonitor".

Edit app role	×
🔟 Delete	
Display name * 🛈	
Monitor	
Allowed member types * (i)	
Users/Groups	
O Applications	
Both (Users/Groups + Applications)	
Value * (i)	
OVOCMonitor	
Description * ()	
OVOC Monitors	
Do you want to enable this app role? 🛈	
Apply Cancel	

The new roles are displayed:

Figure 11-71: App roles Configured

\equiv Microsoft Azure	Search resources, serv	ices, and docs (G+/)			Þ	₽,	ÇP &		ন্দ	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV > OVOCAdmin										
I OVOCAdmin App roles 🛷 ···										
	« + Create	app role 🛛 🔗 Got feedback?								
 Overview Quickstart Integration assistant Manage 	App roles App roles are as permission How do I ass	custom roles to assign permissions t is during authorization. ign App roles	o users or apps. The application defines	and publishes the app roles	and interp	rets them	1			
Branding & properties	Display nan	ne Description	Allowed member type	s Value	ID			State		
Authentication	OVOCLite	OVOC Lite Operators	Users/Groups	OVOCOperatorLite	21b9b	008-0e3	3-4d53	Enable	ed	
🕈 Certificates & secrets	Monitor	OVOC Monitors	Users/Groups	OVOCMonitor	306f3	8aa-b02e	-4c8f-b.	Enable	d	
III Token configuration	Operator	OVOC Operators	Users/Groups	OVOCOperator	fa355	d53-7b7c	-4b46	. Enable	ed	
→ API permissions	Administrat	or OVOC Administrators	Users/Groups	OVOCAdmin	c0ab9	2de-1dbl	o-4695	Enable	ed	
🙆 Expose an API										
App roles										
🎎 Owners										
& Roles and administrators Preview										
Manifest										
Support + Troubleshooting	~									

18. In the Navigation pane, select the **Overview** page for the application.

Figure 11-72: Overview Page

Home > AudioCodes Netherlands BV >			
NOCApplication	¢ …		\times
✓ Şearch (Ctrl+/) «	🔋 Delete 🜐 Endpoints 🐻 Preview features		
Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure /	AD for developer). \rightarrow	
n Quickstart			
🚀 Integration assistant	↑ Essentials		
Manage	Display name : OVOCApplication	Client credentials : 0 certificate, 1 secret	
Branding	Application (client) ID : 72e9f409-9da5-4cc1-a5f0-724f611fba23	Redirect URIs : 1 web, 0 spa, 0 public client	
Authentication	Object ID : ddb67f46-a857-4e9c-a915-2829b3e377c1	Application ID URI : Add an Application ID URI	
📍 Certificates & secrets	Directory (tenant) ID : c524b5f5-fd18-43c0-964c-bc5d35525eaa Supported account types : Multiple organizations	Managed application in I : OVOCApplication	
Token configuration			
→ API permissions	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory longer provide feature updates. Applications will need to be upgraded to Microsoft Auther	r Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no ntication Library (MSAL) and Microsoft Graph. Learn more	
 Expose an API 			
K App roles	A Starting November 9th, 2020 end users will no longer be able to grant consent to newly n	egistered multitenant apps without verified publishers. Add MPN ID to verify publisher	
A Owners			
 Roles and administrators Preview 	Get Started Documentation		
Manifest			
Support + Troubleshooting	Build your applicat	ion with the Microsoft identity platform	
Troubleshooting	The Microsoft identity platform is an authenticati	on service, open-source libraries, and application management tools. You can create modern,	
New support request	standards-based authentication solutions,	access and protect APIs, and add sign-in for your users and customers. Learn more	

- **19.** Note the Directory (tenant) ID value as it must later be configured inConfiguring OVOC Web Azure Settings Multitenant Upgrade below
- Add External tenant operators and assign roles as described in Add External Tenant Operators and Assign Roles on page 129
- 21. Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings - Multitenant Upgrade below

Configuring OVOC Web Azure Settings - Multitenant Upgrade

This section describes how to configure Azure settings in OVOC Web when upgrading from a Single Tenant configuration.

> To upgrade from a Single Tenant configuration:

1. In the Tenant Details, enter the "Azure Tenant ID" of the **external managed tenant** as shown in the screen below.

IANT DETAILS				
General	SNMP	HTTP	Operators	License
Tenant Name		hdvoip_net		
Is Default		False		•
HTTP Operator (License F	Pool)			•
Description				
Subnet (CIDR Notation)				
Users URI Regexp		*		
Azure Tenant ID		XXXXXXXXXX		
Tenant Logo		None		
				Close

Figure 11-73: Tenant Details

2. If you are managing channels, in the Channel Details, enter the "Azure Tenant ID" of the external managed tenant as shown in the screen below

Figure 11-74: Channel Details

CHANNEL DETAILS	
Name	Itc_carmel
Description	
Tonont	hduain nat
renant	hdvoip_her
Azure Tenant ID	xxxxxxxxxxxxxxxx
	Close OK

Create Azure Groups and Assign Members

This section describes how to create groups on Azure and assign them member operators. You should define a separate group for each required security level. These group names are configured in OVOC Azure Authentication Settings screen from where they are mapped to the relevant security level; see the list of security groups that are defined below. Identical group names must be configured on Azure. For example, for System Administrator User Group Name, configure "OVOC_Admin" string in OVOC and as the group name on Azure.

Security Group OVOC (Parameter Name)	Description
System Administrator User Group Name	The name of the User Group of the 'System' type operator whose security level is 'Administrator'.
System Operator User Group Name	The name of the User Group of the 'System' type operator whose security level is 'Operator'.
System Monitor User Group Name	The name of the User Group of the 'System' type operator whose security level is 'Monitor'.
Tenant Administrator User Group Name	The name of the name of the User Group of the 'Tenant' type operator whose security level is 'Administrator'.

Table 11-1: OVOC Security Groups

Security Group OVOC (Parameter Name)	Description
Tenant Operator User Group Name	The name of the User Group of the 'Tenant' type operator whose security level is 'Operator'.
Tenant Monitor User Group Name	The name of the name of the User Group of the 'Tenant' type operator whose security level is 'Monitor'.
Tenant Monitor Links User Group Name	The name of the User Group of the 'Tenant' type operator whose security level is 'Monitor Links'.
Tenant Endpoints Group User Group Name	The name of the User Group of the 'Tenant' type operator

> To assign groups on Azure:

- **1.** Login to the Azure portal as Global Administrator.
- 2. Navigate to the Tenant Overview page.

Figure 11-75: Tenant Overview Page

📃 Microsoft Azure 🔎 Se	earch resources, services, and docs (G+/)				° 🕸 O	Admin@ocshost.emea
Home > AudioCodes Neth Azure Active Directory	nerlands BV Overvie	W				×
Overview Preview features Diagonage and column problems:	 ≪ + Add ∨ [®] Manage te Overview Monitoring 	nants 🕜 What's new 🛛 🗔 Preview Tutorials	features 🔰 🖗 Got feedback? 🗸			ĺ
Manage	Search your tenant					
Groups External Identities Roles and administrators	Name Tenant ID	AudioCodes Netherlands BV c524b5f5-fd18-43c0-964c-bc5d3552	Users jeaa 🗋 Groups Applications	12,362 218		
 Administrative units Enterprise applications Devices 	License	OCSHOST.onmicrosoft.com Azure AD Free	Devices	22		
App registrations App registrations Application proxy Licenses Azure AD Connect	yy yy Bid63152-7a5d-414 Global administrate More info	f-8e62-129fc31f8815 🗋 r	TLS 1.0, 1.1 and 3DES deprecati Upcoming TLS 1.0, 1.1 and 3DES Azure AD. Please enable support clientStapplications/platform) to a impact.	ion deprecation for for TLS 1.2 on avoid any service		

3. In the Navigation pane, select Groups.

Figure 11-76: Create New Group

≡ Microsoft Azure 🔎 Search	h resources, services, and docs (G+/)			Þ.	R 🗘	©	@ &	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >								
🔒 Groups All groups								×
Audiocodes Nethenands BV - Azure Act	tive Directory							
All groups	+ New group ⊻ Download	groups 📗 Delete 💟 Refres	h == Columns	Preview features Ar G	ot feedback?			
Deleted groups	This page includes previews a	vailable for your evaluation. View pre	eviews →					
X Diagnose and solve problems		+ ₇ Add filte	rs					
Settings	Name	Object Id	Group Type	Membership Type	Email			Source
log General	23 200914 sknol	69e1b85b-4310-4f06-b04f	Microsoft 365	Assigned	200914	4sknol@O	SHOST.on	Cloud
Expiration	20 200915_Group_1	227c5f38-2e56-4286-bb26	Security	Assigned				Windows server AD
Naming policy	20 200915_Group_10	bffbe1e9-b2af-4eb2-8d3d-1	Security	Assigned				Windows server AD
Activity	20 200915_Group_11	0f9644f2-0135-4c60-882b-0	Security	Assigned				Windows server AD
Privileged access groups (Preview)	20 200915_Group_12	1e450e6a-21be-4fd4-98a0	Security	Assigned				Windows server AD
3∃ Access reviews	20 200915_Group_13	1857f7a6-87bd-4ea9-b187	Security	Assigned				Windows server AD
Audit logs	200 200915_Group_14	1b9eb203-3838-4026-8697	. Security	Assigned				Windows server AD
Bulk operation results	20 200915_Group_15	56e83fc9-13d2-4e79-b79e	Security	Assigned				Windows server AD
Troubleshooting + Support	20 200915_Group_16	9e24847a-055b-4b0a-ab83	Security	Assigned				Windows server AD
Rew support request	200915_Group_17	95cc0d85-950a-4086-a921	Security	Assigned				Windows server AD
	20 200915_Group_18	f58314c7-ab5b-4afa-ab26-7	Security	Assigned				Windows server AD
	20 200915 Group 19	643f0626-6da1-4f5e-ab0b	Security	Assianed				Windows server AD

4. Click New group.

Figure 11-77: New Group

E Microsoft Azure	Σ	Ŗ	¢14	ŵ	?	ନ୍ଦି	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV > Groups >							
New Group							×
Group type * 💿							
Security							
Group name * ①							
OVOC_Admin_New 🗸							
Group description ①							
Group for Administrators							
Membership type 💿							
Assigned V							
Owners							
No owners selected							
Members							
No members selected							
Create							

5. Enter the details of the new group and then click **Create**.



The same groups that you define must be configured in OVOC in the Authentication screen (see Configuring OVOC Web Azure Settings - Single Tenant Setup on page 91)

Figure 11-78: Created Group

≡ Microsoft Azure 🔎 Search	resources, services, and docs (G+/)			D (R © © R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >						
AudioCodes Netherlands BV - Azure Acti	 ive Directory					×
×	🕂 New group 🞍 Download g	roups 🏛 Delete 💍 Refres	h Ξ≣ Columns 💀 P	review features 🛛 🔗 Got fee	dback?	
All groups	7 This page includes provident automation	allable for your qualitation. View pro	adour -			
Deleted groups	 This page includes previews avoid 	silable for your evaluation, view pre	views ->			
X Diagnose and solve problems	Search groups	+ _▼ Add filter	s			
Settings	Name	Object Id	Group Type	Membership Type	Email	Source
🐯 General	OVOC_Admin_New	22e722a5-038f-4a4a-84d1	Security	Assigned		Cloud
Expiration	25 200914 sknol	69e1b85b-4310-4f06-b04f	Microsoft 365	Assigned	200914sknol@OCSHOST.on	Cloud
Naming policy Naming policy	20 200915_Group_1	227c5f38-2e56-4286-bb26	Security	Assigned		Windows server AD
Activity	20 200915_Group_10	bffbe1e9-b2af-4eb2-8d3d-1	Security	Assigned		Windows server AD
Privileged access groups (Preview)	20 200915_Group_11	0f9644f2-0135-4c60-882b-0	Security	Assigned		Windows server AD
Signature 3 and 3 an	200915_Group_12	1e450e6a-21be-4fd4-98a0	Security	Assigned		Windows server AD
Audit logs	200915_Group_13	1857f7a6-87bd-4ea9-b187	Security	Assigned		Windows server AD
👶 Bulk operation results	20 200915_Group_14	1b9eb203-3838-4026-8697	Security	Assigned		Windows server AD
Troubleshooting + Support	200915_Group_15	56e83fc9-13d2-4e79-b79e	Security	Assigned		Windows server AD
New support request	20 200915_Group_16	9e24847a-055b-4b0a-ab83	Security	Assigned		Windows server AD
	200915_Group_17	95cc0d85-950a-4086-a921	Security	Assigned		Windows server AD
	20 200915 Group 18	f58314c7-ab5b-4afa-ab26-7	Security	Assigned		Windows server AD

- 6. Select the new group.
- 7. In the Navigation pane, select Members.

Figure 11-79: Add Members to Group

E Microsoft Azure 🔎 Searc	h resources, services, and docs (G+/)			\$\$ @ \$P	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV	> Groups >				
OVOC_Admin_New	1 \$ ²				×
«	📋 Delete 🛛 🐱 Preview features	🔗 Got feedback?			
Overview Diagnose and solve problems	This page includes previews available	e for your evaluation. View previews \rightarrow			
Manage III Properties Members	OVOC_Adm Group for Administrat	tin_New	Copy to clipboard		
Owners Administrative units	Membership type	Assigned			
Group memberships	Source	Cloud	D		
Applications	Туре	Security	D		
🔒 Licenses	Object Id	22e722a5-038f-4a4a-84d1-4f54f8a21b9b	D		
Azure role assignments	Creation date	10/12/2021, 12:14:37 PM	D		
Activity					
š≡ Access reviews					
Audit logs	Direct members				
👶 Bulk operation results	🚨 0 User(s) 🏻 🎥 0	Group(s) 🔲 0 Device(s)	0 Other(s)		
Troubleshooting + Support	Group memberships		Owners		

- 8. Click Add members to add new members to the group.
- 9. Select the members to add to the Group.





The new members are added to the group.

■ Microsoft Azure	resources, services, and docs (G+/)		N 16 🖓	\$ 0 R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > AudioCodes Netherlands BV >	Groups > OVOC_Admin_New				
BOVOC_Admin_New	Members				×
«	+ Add members $ imes$ Remove ರ Re	iresh 🛛 🗋 Bulk operations 🗸 🛛	≡≡ Columns 🖾 Preview features 🕅 Got feed	lback?	
() Overview	This name includes previews available for	your evaluation. View previews. →			
X Diagnose and solve problems	 This page measure prements around to the 	four crosses in their presidents			
Manage	Direct members				
Properties	Name	Tune	Email	Usertupe	
🎎 Members		lises	Liian	Mambas	
🎎 Owners	As Abranam scheerer	User		Member	
Administrative units	Aaron Baumann	User	Aaron.Baumann@activevoice.lan	Member	
🔅 Group memberships	AH Aaron Husmann	User	Aaron.Husmann@activevoice.lan	Member	
Applications	AF Aaron Fetzer	User	Aaron.Fetzer@activevoice.lan	Member	
🔓 Licenses					
Azure role assignments					
Activity					
SE Access reviews					
Audit logs					
👶 Bulk operation results					
Troubleshootina + Support Y					,

Figure 11-81: New Group Members

10. Proceed to Configuring OVOC Web Azure Settings - Single Tenant Setup on page 91.

Add External Tenant Operators and Assign Roles

When you login to OVOC for the first time, a connection is established with Azure and the Application Registration for the main tenant, for example, 'OVLAdmin' is added under the Enterprise applications for your registered tenant on Azure. You must then login to the Azure portal, navigate to this application and assign the 'admin' role to the designated operators. This procedure is relevant for adding non-system service provider operators to OVOC.

> Do the following:

PASSWORD

1. Login to OVOC interface with the appropriate Admin permissions for the Azure tenant (login with Admin operators that you defined in Create Azure Groups and Assign Members on page 124.





The Azure authentication and Permissions request dialog is displayed:

Figure 11-83: Permissions requested



2. Select the **Consent on behalf of your organization** check box and then click **Accept**.

If for any reason, you did not select "Consent on behalf of your organization" or do not have 'Admin' permissions for this tenant, then this operation cannot be successfully applied until approved by Service Provider Admin, see Troubleshooting - Granting Admin Consent on page 136.

 Login to the Azure portal with Tenant 'Admin' permissions and navigate to the newly created OVOC application (Enterprise applications > OVOCApplication).

Figure 11-84: OVOC Application

≡	Microsoft Azure			D 🗗 🕆 🍥	Admin@ocshost.emea
Home	> Enterprise applications				
	Enterprise applications AudioCodes Netherlands BV - Azure Active Directo	All applications …			×
	« +	New application 🛛 🗮 Columns 🗍 🐼 Preview fea	atures 🛛 🖗 Got feedback?		
Overvi	ew C	Try out the new Enterprise Apps search preview! Click to enab	ble the preview. \rightarrow		
* Di	agnose and solve problems				
	agnose and solve problems	VINITER 365	https://w365.iwriter.eu/	281t5tte-edbt-4159-9eat-ae50a7c53c09	a89586ct-88b4-411a-aa38-63c8c7a590d6
Manag	ge	azyadmin-example		fbf6fbe5-ff06-4510-b011-0adccd64ed27	89b0fc07-c763-4dad-9a27-3b075b40ccb6
AI	l applications	Modern Workplace Tools		f43077e2-7bc3-443b-8d26-f670f0baed8a	fe6aa35b-7da8-44fd-a44e-e2d4bafbdab5
🐺 Ap	oplication proxy	MSFT Power Platform - Azure AD		62b5a85e-9d22-4365-9a30-ba8fc3b1716a	2bed6734-1911-40e6-ac44-00d79d70d2bc
() Us	ser settings	MS-Teams-Minimum-App-Permisions		5078430e-d3f8-4ff9-a56d-85c17b130ee4	ab529249-f275-45f8-a072-fe367675ba0a
Securi	ty	😚 МуАрр		cba1fc3d-7008-49cc-90bc-5c5d6f24ab86	b55f4d0c-e47f-41af-8c96-764af238f25d
🐁 Ca	onditional Access	Nine for Office 365		a9364c07-7da5-4245-9225-aa83f1e1faa1	516e4bcb-86da-4cfe-92cb-435c1e8dbf71
19 Cd	onsent and permissions	Office 365 Exchange Online	http://office.microsoft.com/outlook/	693828cc-6bc9-4463-bdc5-25f28eea6420	00000002-0000-0ff1-ce00-00000000000
A		Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	b3d6f67b-797b-4f1e-8a62-338f280573f1	00000003-0000-0ff1-ce00-00000000000
Activit	y is less	Office 365 Yammer	https://products.office.com/yammer/	ba472a33-77d8-43eb-9595-0fe8fe1e028c	00000005-0000-0ff1-ce00-00000000000
	gn-in logs	Oi-Auth-Demo		0446fe6c-9918-41ca-becd-1707ece0cafc	ed2b8442-b725-4f92-9349-2d62937d038b
	sage & insights	ovoc		9157663d-9dde-4636-812a-65f25d712bcd	59ab90b2-99a4-45d6-96c7-c17e7352950c
• AL	Jait logs	OVOCAdmin		57978d82-d74e-456a-9c7d-093351440ad3	db348b8c-c6e3-4afc-9dc7-1b2a84706843
Pr	ovisioning logs	OVOCApplication		c1c25735-9e96-4823-925d-097f146fe8c1	72e9f409-9da5-4cc1-a5f0-724f611fba23
3= AC	ccess reviews	PB Power BI Service		cb0bb5b3-b815-48c2-93de-dd17151f467f	00000009-0000-0000-c000-000000000000
- C - C - C - C - C - C - C - C - C - C	amin consent requests	preregistered-device-code-flow-sample		6008b46c-1063-45c7-9f2e-238cf91dac22	ebe2ab4d-12b3-4446-8480-5c3828d04c50
Troubl	eshooting + Support	PublicClientSample (DO NOT USE IN PRODUCTION	n.	56825452-84c6-4699-82e8-194d3cf32ea1	4a1aa1d5cc567c49d0cad0bccd957a47f842

4. In the Navigation pane, select Users and groups.

Figure 11-85: Users and Groups

			D 🕼 🖓 🎯 Ø Á	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > OVOCApplication Enterprise Application	Overview			×
III Overview	Properties			
Deployment Plan Manage	OV Name O Copy to clipboard OVOCApplication			
Properties	72e9f409-9da5-4cc1-a5f0-724 [b]			
 Owners Roles and administrators (Preview) 	Object ID ① c1c25735-9e96-4823-925d-09 [1]			
 Users and groups Single sign-on 	Getting Started			
 Provisioning Application proxy Self-service 	Assign users and groups Provide specific users and groups access to the applications Assign users and groups	2. Provision User Accounts You'll need to create user accounts in the application Learm more Cre	Conditional Access ure access to this application with a tomizable access policy. ate a policy	
Security				
 Conditional Access Permissions Token encryption 	4. Self service Enable users to request access to the amplication using their Amure AD			
Activity ➔ Sign-in logs	credentials Get started			

- **5.** Do one of the following:
 - Assign role to a new user
 - Assign role to existing user

	0	0	0	
		docs (G+/)	D & @ @ R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > OVOCApplication				
	Users and groups			×
. Oveniew	≪ + Add user/group 🖉 Edit 🕮 Rem	ove 🖉 Update Credentials 🗮 Columns 🕅 Got feedback?		
Deployment Plan	The application will not appear for assign	ed users within My Apps. Set 'visible to users?' to yes in properties to enable this. \rightarrow		
Manage	First 200 shown, to search all users & g	roups, enter a display name.		
Properties	Display Name	Object Type	Role assigned	
A Owners	🔲 🌱 Brad	User	Default Access	
Roles and administrators (Preview)				
Users and groups				
Single sign-on				
Provisioning				
Application proxy				
 Self-service 				
Security				
🝨 Conditional Access				
🖧 Permissions				
Token encryption				
Activity				
Sign-in logs				
🚮 Usage & insights	~			

Figure 11-86: Assign Role to New User /Existing User

> To assign a role to an existing user:

1. Choose a particular user in the list and then click Edit.

Figure 11-87: Edit Assignment

E Microsoft Azure	D 🖗	Φ 👳		Admin@ocshost.emea AUDIOCODES NETHERLANDS BV	9
Home > OVOCApplication > Edit Assignment ··· AudoCode Netherlands BV			Select Only a single	a role	×
Users			∠ Enter role n	ame to filter items	
1 user selected.			Administrator		
Select a role			Monitor		
None Selected			Operator		
			Selected Role		
			You haven't se	lected any role.	
Assign			Select		

Microsoft Azure	, P. Search resources, services, and docs (G+/)	E E O O ? O maksymi@audiocode
Home > AP_SAML_TEST > Enterp	se applications > OVOC	
Supervise Application	groups -	х
Cvervlev	The second of the second	
Deployment Plan	O The application will appear for assigned users within My Appc. Set Visible to users? to no in properties to prevent this. →	
Manage	P First 200 shown, to seal-	
III Properties	Digitzy Name Object Type	Role assigned
A Owners	🔟 🔞 Ron2 Uper	Operator
Roles and administrators (Preview)		
Users and groups		
Single sign-on		
Provisioning		
Self-service		
Security		
Conditional Access		
Permissions		
Token encryption		
Activity		
Sign-ins		
i Usage & insights		
Audit logs		
Provisioning logs		
- PLLES ROUTS		

- 2. In the left pane, under "Select a role" click None Selected.
- 3. In the right pane, choose the relevant role and then click Select.

Figure 11-88: Add Assignment

≡ Microsoft Azure		Σ	₽	₡ ⊗	0	R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > OVOCApplication >							
Edit Assignment … AudioCodes Netherlands BV							×
Users							
1 user selected.							
Select a role							
Administrator							
Assign							

4. Confirm by clicking Assign.
| | 8 | 8 | | |
|--|---|--|---------------|---|
| | ,P Search resources, services, and docs | (G+/) | D 🗟 🖓 🏟 🔿 R | Admin@ocshost.emea
AUDIOCODES NETHERLANDS BV |
| Home > OVOCApplication | | | | |
| OVOCApplication Enterprise Application | Users and groups | | | × |
| | 🔨 🕂 Add user/group 🖉 Edit 🗎 Remove | $ \mathcal{P} $ Update Credentials $ \equiv$ Columns $ \mathcal{P}$ Got feedback? | | |
| Overview Deployment Plan | The application will not appear for assigned us | ers within My Apps. Set 'visible to users?' to yes in properties to enable this. \rightarrow | | |
| Manage | First 200 shown, to search all users & group | s, enter a display name. | | |
| Properties | Display Name | Object Type | Role assigned | |
| 🍰 Owners | Brad | User | Administrator | |
| 8 Roles and administrators
(Preview) | | | | |
| Users and groups | | | | |
| Single sign-on | | | | |
| Provisioning | | | | |
| Application proxy | | | | |
| Self-service | | | | |
| Security | | | | |
| 🍨 Conditional Access | | | | |
| Permissions | | | | |
| Token encryption | | | | |
| Activity | | | | |
| Sign-in logs | | | | |
| 🖬 Usage & insights | ~ | | | |

Figure 11-89: Existing User Defined with "Admin" Role

> To Assign a role to a new user:

- 1. In the left pane under Users, click None Selected.
- 2. In the right pane, choose the relevant user and then click **Select**.

	AUDIOCODES NETHERLAND
Home > OVOCApplication >	Users
Add Assignment	
AudioCodes Netherlands BV	Q Search
	> hearen
Crows are not available for programment due to usur Artise Directory also level. You one period individual uncer to the	Aaron Baumann
application.	Aaron.Baumann@OCSHOST.onmicrosoft.com
	Aaron Christ
Users	Aaron.Christ@OCSHOST.onmicrosoft.com
None Selected	Aaron Eggers
None Selected	Aaron.Eggers@OCSHOST.onmicrosoft.com
	AF Aaron Fehrenbach
	Aaron.Fehrenbach@UCSHOS1.onmicrosoft.com
	AF Aaron Fetzer
	Aaron.retzer@GC.SHOST.onmicrosoft.com
	Aaron Fisch
	Adottrischeroccartosi toimiterosort.com
	Aaron Heid
	Allow Regocarios Commic asolicion
	Aaron Husmann Aaron Husmann@OCSHOST opmicrosoft com
	Aaron Jensen Aaron Jensen@OCSHOST opmicrosoft com

Figure 11-90: Choose User

Figure 11-91: User Selected

Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)		D 🛛	¢® 👳	@ R	Admin@ocsh Audiocodes Net
Home > OVOCApplication >						
Add Assignment						
Groups are not available for assignment of application.	due to your Active Directory plan level. You can assign individual users to the					
Jsers						
1 user selected.						
Select a role *						
None Selected						
Assign						
5						

3. In the left pane under Select a role, click None Selected.

Figure 11-92: Select a Role

≡ Microsoft Azure		D 🕼 🗘	O R Admin@ocshost.emea
Home > OVOCApplication > Add Assignment AudioCodes Netherlands BV			Select a role ×
Groups are not available for assignment due	to your Active Directory plan level. You can assign individual users to the		Administrator Monitor
appication.			Operator
Users			
1 user selected.			
None Selected			
			Selected Role
			You haven't selected any role.
Assign			Select

4. In the right pane, choose the relevant role and then click **Select**.

Figure 11-93: Assign Role to New User

le > ONCCApplication > dd Assignment Codes Networknots BV application. ser setected. a crice * vertor	> > OVOCApplication > d Assignment Groops are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.	e> POCCApplication > Cacess Pretorations F/ expensions	Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)		D 🖗	0 @	유 Admin
Id Assignment	Crices Networking BV Crices networking BV Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. reselected. a role * ator	Bd Assignment	ne > OVOCApplication >					
Concept retrievalues of Concept are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. ers user selected. ect an ofe * perstor	Groops are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.	Course received was of a subject to your Active Directory plan level. You can assign individual users to the opportants.	Add Assignment					
Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. Croups are not available for assignment due to your Active Directory plan level. Croups are not available for assignment due to your Active Directory plan level. You can assign are not available for assignment due to your Active Directory plan level. Croups are not available for assignment due to your Active Directory plan level. Croups are not available for assignment due to your Active Directory plan level. Croups are not available for assignment due to your Active Directory plan level. Croups are not available for assignment due to your Active Directory pla	Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application. reselected. a role * ator	Concept serve net available for assignment due to your Active Directory plan level. You can assign individual users to the concept served can be associated as a concept served can be associated by associated can be associated by associated can be associated by associa						
Crocket as not available for assignment due to your Active Directory plan level, You can assign individual users to the application. ers user selected. ect a note* perator	Groups an est available for assignment due to your Active Directory plan level. You can assign individual users to the application. If selected. a role * ator	b crucipitation.	A					
ers user selected. lect a role * lepator	rr selected. a role * ator	se selected. ct a role * erator	Groups are not available for assignme application.	ent due to your Active Directory plan level. You can assign individual users to the				
ers selected. lect a role *	ir selected. a role * ator	5 msm						
lect a role * liperator	a role * ator	starde*	1 user selected.					
1perator	iator	erator magn	elect a role *					
		xxg	Operator					
		мада						
		sogn						
		wogn						
		wagn						
		soign						
		ssign						
		wagn						
		ssign						
		xxxign						
		asagn						
		kuign						
		Resign						
			Assign					

5. Confirm by clicking Assign.

Figure 11-94: New User Assigned "Operator" Role

≡ Microsoft Azure		A.	5.6	P & O R	Admin@ocshost.emea AUDIOCODES NETHERLANDS BV
Home > OVOCApplication					
OVOCApplication Enterprise Application	Users and groups				×
 Overview Deployment Plan 	 Add user/group Edit Remove The application will not appear for assigned users v 	\Im Update Credentials $ $ == Columns $ $ \bigwedge Got feedback? within My Apps. Set Visible to users? to yes in properties to enable this. \rightarrow			
Manage	P First 200 shown, to search all users & groups, er	iter a display name.			
Properties	Display Name	Object Type		Role assigned	
2 Owners	Brad	User		Administrator	
 Roles and administrators (Preview) 	Aaron Baumann	User		Operator	
Users and groups					
Single sign-on					
Provisioning					
Application proxy					
Self-service					
Security					
🍨 Conditional Access					
Permissions					
Token encryption					
Activity					
Sign-in logs					
🕍 Usage & insights	~				

- 6. Do one of the following:
 - If configuring a Multitenant setup for the first time proceed to Configuring OVOC Web Azure Settings Multitenant Setup on page 107.
 - If upgrading from a Single Tenant setup proceed to Configuring OVOC Web Azure Settings Multitenant Upgrade on page 122

Troubleshooting - Granting Admin Consent

This procedure describes the actions required for granting admin consent for the OVOC application.

> To grant admin consent:

- **1.** Login to Azure portal with "admin" of Azure channel tenant.
- In the Navigation pane, select Active Directory > Enterprise applications > OVOC Application
- 3. Select Security > Permissions.

Figure 11-95: Permissions

E Mosselt Asure	P Seath rest	man, services, and door (Sm3	0	00078	administrationalitanes.
Hone 3 UveDoutDarrell 3 Energie	e applications > OVLAdmin				
OVLAdmin Permiss	iions –				×
	🖒 faltech 🗹 Review permissions	R Got beelback/			
Chenner					
Chapterment Plan	Permissions				
Manage	Applications can be provided permissions to	your benantility on administencenting to the application for all users chamin	converts a user converting to the application for him of	or herself (Day scenaril), or an admin	integrating an application and
X Popeties	enabling self-service access or assigning use button before to-grant adminisconsent.	es deadly to the application, to an administrator you can grant consent or	clubal of all uses in this beaut, ensuing that and use	rawlines be required to consert whe	er using the application. Club the
Domen	As an administrator you can pract consert of	to behalf of all users in this hervest, ensuring that end users will not be requi	ind to consert when using the application. Old the but	Aton below to grant admin consent,	
A fide and administrators (heries)		e admin.conumt for Live/Tourithanneth			
Uses and proups			-		
Single sign on	Admin consent User consent				
P Analyticity	P teach permittions				
Defranka	AR Rate	T ₄ Permission	To Type	Ty Granted Brough	To dramed by To
Security	Microsoft Graph				
Conditional Access	Mercell Graph	Sign coars in	Delegated	User consent	T total usertal
& Permissions	Maxwell draph	Ver-used band politie	Delegated	User consent	1 MAL UNKS

4. Click Grant admin consent for OVOC. The following screen is displayed:

Figure 11-96: Permissions Requested



5. Click Accept.

12 Setting Up Microsoft Teams Subscriber Notifications Services Connection

This section describes how to setup the connection between the OVOC server and the Microsoft Teams Subscriber service on Office 365/Microsoft 365/Microsoft Azure. In order to connect to Teams, the OVOC server Public IP should be accessible from the Global Internet and the OVOC server should have access to the Global Internet. In addition, the Directory (tenant) ID and the Client (application) ID are required to establish the connection. This section includes the following procedures:

- Register Microsoft Teams Application below
- Configure Microsoft Graph API Permissions on page 142
- Define OVOC FQDN and Load Certificate on page 145

Register Microsoft Teams Application

This procedure describes how to register the Microsoft Teams application that is used for retrieving Call Notifications for the managed Microsoft Teams tenant.

> To register the application:

1. Open the Azure Portal, the Overview page is displayed with the Tenant ID of the managed Teams tenant.

Home >			
AudioCodes Ltd Or Azure Active Directory	verview		
«	👁 Switch tenant 📋 Delete tenant 🕂 G	Create a tenant 🛛 🗹 What's new 🕴 🐼 Preview	w features 🛛 💙 Got feedback?
Overview	AudioCodes Ltd		
🌱 Getting started	O Search your tanant		
💀 Preview hub	> Search your tenant		
🗙 Diagnose and solve problems	Tenant information	💝 Azure AD Connect	
Manage	Your role	Status	
🚨 Users	User More info	Enabled	
🚨 Groups	License Azure AD Premium P2	Last sync	
External Identities	Tenant ID	Less than 1 hour ago	
🍰 Roles and administrators	1911c65c-893b-42f9-83fa-66c1b 🗈		
Administrative units	Primary domain		
Enterprise applications	audiocodes365.onmicrosoft.com		
Devices			

Figure 12-1: Tenant ID

2. In the Navigation pane, select App registrations.

≡	Microsoft Azure	𝒫 Search r	esources, services, and docs (G+/)			Σ.	Ŗ	Q	ŝ	?	\odot
Hor	Home >										
i	AudioCodes Ltd Overview … Azure Active Directory										
_		«	🕲 Switch tenant 📋 Delete tenant -	Create a tenant 🛛 🗹 What's new	💀 Pre	view fe	eatures	<	2 Got	feedba	ck?
24	Groups		AudioCodes Ltd								
Û	External Identities		P Search your tenant								
2.	Roles and administrators										
2	Administrative units	- 1	Tenant information	💝 Azure AD Connect							
Щ,	Enterprise applications	- 1	Your role	Status							
	Devices		User More info	Enabled							
Ш,	App registrations		License	Last sync							
۵	Identity Governance		Tenant ID	Less than 1 hour ago							

3. Click New registration.

≡ Microsoft Azure			Ŗ	Q	¢ې	?	C
Home > AudioCodes Ltd							
AudioCodes	Ltd App registrations 🛷 🚥						
	« + New registration	view feat	ures	\heartsuit	Got fee	dback?	
A Groups							
手 External Identities	() Try out the new App registrations search preview! Click to enable the preview. $ ightarrow$						
🔓 Roles and administrators							
Administrative units	Starting June 30th, 2020 we will no longer add any new features to Azure Active Director	Authenti	cation Li	ibrary (/	ADAL) ar	nd Azure	AD Graph.
Enterprise applications	provide technical support and security updates but we will no longer provide feature upd (MSAL) and Microsoft Graph. Learn more	ates. App	lications	will ne	ed to be	upgrad	ed to Micro
Devices							
App registrations	All applications Owned applications Deleted applications (Preview)						
Identity Governance	9 Start typing a name or Application ID to filter these results						

Figure 12-3: New registration

4. Enter the name of the application and then click **Register**.

Figure 12-4:	Name the	application
--------------	----------	-------------

Home > AudioCodes Ltd >
Register an application
5 11
* Name
The user-facing display name for this application (this can be changed later).
OVOC Teams
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (AudioCodes Ltd only - Single tenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
O Personal Microsoft accounts only
By proceeding, you agree to the Microsoft Platform Policies 🗗
Register



	n resources, services, and docs (G+/)		∑_	Ŗ	Ļ	ŝ	?	\odot
Home > AudioCodes Ltd > OVOC_Teams * ···								
	🔟 Delete 🌐 Endpoints 💀 Preview features							
R Overview	f) Got a second? We would love your feedback on Microsoft ider	ntity platform (previously Azu	re AD for	develop	er). →			
🗳 Quickstart	↑ Essentials							
Integration assistant	Display name OVOC_Teams	Supp My c	oorted ac organizat	count t ion only	ypes /			
Branding	Application (client) ID 4c252f59-59ef-40f0-a9e6-3675d494cdea	Redi Add	rect URIs a Redire	t URI				
 Authentication 	Directory (tenant) ID 1911c65c-893b-42f9-83fa-66c1b86fdf85	App Add	lication II an Appli	D URI cation I	D URI			
📍 Certificates & secrets	Object ID	Man	aged app	olicatior	n in loca	al direc	tory	
Token configuration	416bc251-6644-4758-b07a-m37e0c4030a	000	C_leams					
 API permissions 	• Welcome to the new and improved App registrations. Looking	to learn how it's changed fro	m App re	gistratio	ns (Lega	acy)? Le	arn mo	re
Expose an API								

5. In the Navigation pane select Certificate & Secrets.

\equiv Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)	Þ	Ŗ	L ¹	ŝ	?	0
Home > AudioCodes Ltd >	<i>☆</i> …						
♀ Search (Ctrl+/)	🛛 « 📋 Delete 🌐 Endpoints 🐼 Preview features						
Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azur	re AD for	develop	oer). →			
QuickstartIntegration assistant	▲ Essentials Display name Supplement OVOC Teams My c	ported ac	count	types ly			
Manage Branding	 Application (client) ID 4c252f59-59ef-40f0-a9e6-3675d494cdea Add a Redirect URI 						
Authentication	Directory (tenant) ID Appl 1911c65c-893b-42f9-83fa-66c1b86fdf85 Add	lication II an Appli	D URI cation	ID URI			
Certificates & secrets Token configuration	Object ID Man 416bc25f-6644-4758-b07d-ff37e0c4030d OVC	aged app C_Teams	olicatio	n in loc	al direc	tory:	
 API permissions Expose an API 	Welcome to the new and improved App registrations. Looking to learn how it's changed fro	m App re	gistratio	ons (Leg	acy)? L	earn more	

Figure 12-6: Certificate & Secrets

6. Click New client secret.

Figure 12-7: New Client Secret

≡ Microsoft Azure	Search resources, services, and docs (G+/)			Σ	P	\mathcal{L}^{1}			\odot		
Home > AudioCodes Ltd > OVC	Home > AudioCodes Ltd > OVOC_Teams										
✓ Search (Ctrl+/)	« 🛇 Got feedback?										
Nverview			Start date	-vhuy				-			
📣 Quickstart	No certificates have been added f	or this application.									
🚀 Integration assistant											
Manage											
🔤 Branding	Client secrets										
➔ Authentication	A secret string that the application	uses to prove its identity whe	en requesting a token. Also c	an be re	ferred t	o as ap	plicatio	on pass	sword.		
📍 Certificates & secrets	+ New client secret										
Token configuration	Description	Expires	Value				ID				
 API permissions Expose an API 	No client secrets have been create	d for this application.									

7. Click Add.

The newly added client secret is added as shown in the figure below.

■ Microsoft Azure	∽ Search resources, services, and docs (G+/)				
Home > AudioCodes Ltd > OVOC_Tean	าร				
🔶 OVOC_Teams Certi	ficates & secrets 👒 …				
·					
Search (Ctrl+/) «	Got feedback?				
Noverview	Add a client secret				
🗳 Quickstart	Description				
💉 Integration assistant					
Manage	Expires				
🔜 Branding	 In 1 year Is 2 year 				
 Authentication 	Never				
📍 Certificates & secrets	Add				
Token configuration					

Figure 12-8: Add a client secret

8. The client secret is added as shown in the screen below. Copy it to the clipboard as you will be required to enter it in later configuration.

	Figure 12-9: Added Ce	rtificates & Secrets
Home > AudioCodes Ltd > OVC OVOC_Teams (P Search (Ctrl+/)	RC_teams Certificates & secrets	
 Overview Ouickstart 	Copy the new client secret value. You won	n't be able to retrieve it after you perform another operation or leave this blade.
Integration assistant		
Manage	No certificates have been added for this appli	ication.
Branding		
Authentication	Client secrets	
📍 Certificates & secrets	A secret string that the application uses to pro	rove its identity when requesting a token. Also can be referred to as application password.
Token configuration		
API permissions	Thew client secret	

Configure Microsoft Graph API Permissions

Password uploaded on Mon Mar 08 2021

This procedure describes how to configure the appropriate permissions to connect to Microsoft Graph API that is used to interface with Microsoft Teams to retrieve the Call Notifications.

Expires

3/8/2022

Value

Copy to clip

EDvwCO2ucE-R6oi3zL4_hA_8BHDr5B-G... 🗈

bard

716f73c1-dbc1-4b45-ae4a-9591ed5ee

```
To configure Microsoft Graph permissions:
```

1. In the Navigation pane, select API permissions.

Description

Expose an API

🏜 App roles | Preview

Figure 12-10: API Permissions

OVOC_Teams Certi	ficates & secrets 👒 …				
✓ Search (Ctrl+/) «	♡ Got feedback?				
Overview	Copy the new client secret value. You won	't be able to retrieve it a	after you perform another	operation or leave this blac	Je.
Quickstart	manaprint		Start date	Enpires	
Integration assistant	No certificates have been added for this applic	cation.			
Manage					
🔤 Branding					
Authentication	Client secrets				
📍 Certificates & secrets	A secret string that the application uses to pro	ve its identity when r	equesting a token. Also	can be referred to as app	lication password.
Token configuration					
➔ API permissions	+ New client secret				
🙆 Expose an API	Description	Expires	Value	Copy to clip	iboard
🐣 App roles Preview	Password uploaded on Mon Mar 08 2021	3/8/2022	EDvwCO2ucE-R6oi3z	L4_hA_8BHDr5B-G 🗅	716f73c1-dbc1-4b45-ae4a-9591ed5ee

2. Click Add a permission.

Figure 12-11: Add a permission

🅤 OVOC_Teams | API permissions 🛷 …

7	Search (Ctrl+/)	«	🖒 Refresh 🛛 🛇 Go	t feedback?				
	Overview	^						
# 2	Quickstart		The "Admin consent	t required" co	lumn shows th	e default value for an organization. Ho	wever, user consent ca	an be customize
×	Integration assistant		may not reflect the	value in your	organization, o	r in organizations where this app will b	e used. Learn more	
Ma	anage		Configured permissio	ons				
-	Branding		Applications are authorize	ed to call API	ls when they a	re granted permissions by users/ad	mins as part of the c	consent proces
Э	Authentication		include all the permission	s the applica	ation needs. Le	arn more about permissions and co	onsent	
•	Certificates & secrets		+ Add a permission	🗸 Grant ad	dmin consent	for AudioCodes Ltd		
	Token configuration		API / Permissions	name	Туре	Description		Admin consei
-9-	API permissions		∽Microsoft Graph	(1)				
2	Expose an API		User.Read		Delegated	Sign in and read user profile		No
24	App roles Preview							
ß	Owners		τ			and Production and the state of		

3. Select Grant Admin Consent for and select Yes.



If the App hasn't been granted admin consent, users are prompted to grant consent the first time they use the App.

4. Select Microsoft Graph.

Figure 12-12: Request API Permissions D 🕼 🖉 🔅 Microsoft Azure Home > OVOC_Teams **Request API permissions OVOC_Teams** | API permissions Ś Select an API Search (Ctrl+/) 🕐 Refresh 🛛 💙 G Microsoft APIs APIs my organization uses My APIs Noverview Commonly used Microsoft APIs 📣 Quickstart The "Admin conser may not reflect the Microsoft Graph 💉 Integration assistant Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and mo Manage single endpoint. Configured permissi 🔤 Branding Applications are authoriz include all the permissio Authentication 📍 Certificates & secrets Azure Batch + Add a permission Azure Data Catalog Azure Data Ex Programmatic access to Data Catalog resources to register, annotate and search data assets Schedule large-scale parallel and HPC applications in the cloud Perform ad-hoc queri data to build near rea analytics solutions Token configuration API / Permissions API permissions ✓Microsoft Graph 🔷 Expose an API Liser Read

5. Select Application permissions.

Figure 12-13: Application permissions

Home > OVOC_Teams	ormissions 👌	Request API permissions		\times
	Jermissions ×	CALLADI-		
Search (Ctrl+/)	🕐 Refresh 🛛 🛇 G	Microsoft Graph https://graph.microsoft.com/ Docs 🗗 What type of permissions does your application require?		
QuickstartIntegration assistant	The "Admin conser may not reflect the	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a single in user	
Manage	Configured permissi		agnea in aser.	
Eranding	Applications are authoriz			
Authentication	include all the permission			
🕈 Certificates & secrets	+ Add a permission			

6. Search for Permission Call Records.

Figure 12-14: Call Records

Home > OVOC_Teams	Pl permissions 👒	Request API permissions	
Search (Ctrl+/) Overview	≪ ⁽⁾ Refresh ♡ G	C All APIs Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon withou signed-in user.
 Quickstart Integration assistant 	The "Admin conser may not reflect the	Select permissions	ехрі
Manage	Configured permissi	Permission	Admin consent required
Branding Authentication Certificates & secrets Token configuration API normiscione	Applications are authoriz include all the permission + Add a permission API / Permissions	CallRecord-PstnCalls CallRecords Calls	
 Arr permissions Expose an API 	✓ Microsoft Graph		

7. Set permission CallRecords.Read.All to enable access to retrieved call notifications.

✓ Search (Ctrl+/)	« 🕐 Refresh 🛛 🛇 Got feedback?		
Verview	You are editing permission(s) to your appli	ication, users will have to consent even if they've al	lready done so previously.
🗳 Quickstart			
🚀 Integration assistant	Configured permissions		
Manage	Applications are authorized to call APIs when t	they are granted permissions by users/admins	as part of the consent process. T
Manage	Applications are authorized to call APIs when t include all the permissions the application nee	they are granted permissions by users/admins ds. Learn more about permissions and consent	as part of the consent process. T t
Manage Branding Authentication	Applications are authorized to call APIs when the include all the permissions the application needs the application of the Add a permission of Grant admin control of the second	they are granted permissions by users/admins a ds. Learn more about permissions and consent nsent for AudioCodes Ltd	as part of the consent process. T t
Manage Branding Authentication Certificates & secrets	Applications are authorized to call APIs when the include all the permissions the application nee + Add a permission	they are granted permissions by users/admins eds. Learn more about permissions and consent nsent for AudioCodes Ltd Description	as part of the consent process. T t Admin consent r
Manage Branding Authentication Certificates & secrets Token configuration	Applications are authorized to call APIs when 1 include all the permissions the application nee + Add a permission \checkmark Grant admin con API / Permissions name Type \checkmark Microsoft Graph (2)	they are granted permissions by users/admins a ds. Learn more about permissions and consent nsent for AudioCodes Ltd Description	as part of the consent process. T t Admin consent r
Manage Branding Authentication Certificates & secrets III Token configuration API permissions	Applications are authorized to call APIs when the include all the permissions the application need the definition of the application of the API / Permissions name Type Microsoft Graph (2) CallRecords.Read.All Application	they are granted permissions by users/admins. eds. Learn more about permissions and consent nsent for AudioCodes Ltd Description ation Read all call records	as part of the consent process. T t Admin consent r Yes

Figure 12-15: API Permissions

 You can optionally set permission User.Read to display caller details in retrieved call records.

Figure	12-16:	User	Read	Permissions
--------	--------	------	------	-------------

Home > OVOC_Teams							
_– OVOC_Teams API p	permissions 🛷 …						
•							
	🖒 Refresh 🛛 ♡ Got feedbac	k?					
Noverview	A You are editing permission(s) to	o your applicatior	, users will have to consent even if the	y've already done so previously.			
📣 Quickstart							
🚀 Integration assistant	Configured permissions						
Manage	Applications are authorized to call A	APIs when they a	re granted permissions by users/ad	mins as part of the consent process. The list (
🔤 Branding	include all the permissions the appl	ication needs. Le	earn more about permissions and co	onsent			
∂ Authentication	+ Add a permission 🗸 Grant admin consent for AudioCodes Ltd						
📍 Certificates & secrets	API / Permissions name	Туре	Description	Admin consent req			
Token configuration	∽Microsoft Graph (2)						
API permissions	CallRecords.Read.All	Application	Read all call records	Yes			
🙆 Expose an API	User.Read.All	Application	Read all users' full profiles	Yes			
🐣 App roles Preview							

Define OVOC FQDN and Load Certificate

You need to define the OVOC server with an FQDN that binds to the OVOC Server Public IP address. This FQDN should bind to the OVOC server public IP address and be defined in the public DNS server – each request from every PC connected to the internet should be able to reach the OVOC Public IP address from the FQDN.

➤ Do the following:

1. Verify that the DNS resolving for the OVOC FQDN is successful, for example Google.com (include example with OVOC Hostname):

C:\Users www.goog	\enterprise1user>nslookup le.com	
Server:	tlc-ovoc.trunkpack.com	
Address:	10.1.1.10	
Non-auth	oritative answer:	
Name:	www.google.com	
Addresse	s: 2a00:1450:4006:801::2004	
172.217.	18.36	

In the OVOC Web, open the OVOC Server Configuration screen (System menu
 > Administration tab > OVOC Server folder > Configuration)

Figure 12-17: OVOC Server Configuration

One Voice Operations Center DAS	SHBOARD	NETWORK ALARMS	STATISTICS CA	ALLS USERS	SYSTEM		🌲 🏥 Welcome acladmin 🗸
ADMINISTRATION CONFI							
CONFIGURATION							
ADMINISTRATION	<	GENERAL SETTINGS				OVOC INTERNAL MAIL SERVER SETTINGS	
LICENSE	^	OVOC Hostname aclovoc01	Descri Audior	iption codes		Internal Mail Server From Address OVOC@audiocodes.com	
Tenants Allocations System Allocations		SBC Devices Communication IP Based				Internal Mail Server Real Name OVOC	
Floating License		Privacy Mode					
SECURITY	~	Masked Digits Number			0		
OVOC SERVER	^	globalLogo.png			· 1		
Status							
Info				odes			
Configuration			One Voice Operation	Center			
Calls Storage							
Calls Status					Submit		Submit

3. Generate a server certificate with a known Certificate Authority with the OVOC FQDN defined in the CN (or alternatively in SAN) and then import it to the OVOC server (overriding default server certificate) using "Option 3 Import Server Certificates from Certificate Authority (CA)" in the Server Certificates Update menu (see Server Certificates Update on page 268

Microsoft Teams URLs

The following URLs are used by the Microsoft Teams Call Notification Service.

- Incoming:
 - OVOC URL for incoming notifications and used by Azure to validates OVOC endpoint: callRecords

Outgoing:

- Authorization Token
- Subscription
- Calls retrieval
- Users retrieval

13 Managing Device Connections

When the connections between the OVOC server and the managed devices traverse a NAT or firewall, direct connections cannot be established (both for OVOC > Device connections and for Device > OVOC connections). OVOC provides methods for overcoming this issue. These methods can be used for both initial setup and Second-Day management:

- Establishing OVOC-Devices Connections below
- Establishing Devices OVOC Connections on page 152

The table below describes the different connection scenarios.

Configuration	ονος				Devices		
Option/Deploym ent Scenario	AWS	Azure	On- Premises	Public Network	AWS	Azure	On- Premises
AudioCodes SBC De	evices						
Cloud Archi- tecture Mode				-			\checkmark
OVOC Server Con- figured with Public IP	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark		\checkmark

Table 13-1: Device Connection Scenarios



For OVOC Managed devices: All remote connections for OVOC managed devices require a configured WAN interface on the managed device.

Establishing OVOC-Devices Connections

When OVOC is deployed behind a firewall or NAT in the cloud or in a remote network, it cannot establish a direct connection with managed devices using its private IP address. Consequently, you must configure the OVOC Server IP address as follows:

- For OVOC Cloud deployments: Configure the OVOC server public IP address.
- For OVOC deployments in a remote public network: Configure the IP address of the NAT router.

See Configure OVOC Server with NAT IP Address per Interface on the next page

If your deployment implements multitenancy, separate NAT applicative interfaces can be configured for each tenant. See Configure OVOC Server with NAT IP per Tenant on page 150

Configure OVOC Server with NAT IP Address per Interface

This option configures the OVOC server with a physical NAT interface for connecting to devices that are deployed behind a NAT in a remote Enterprise or Cloud network.

- When the "Cloud Architecture" mode is enabled for a specific interface, the NAT configuration is not relevant for this interface.
 - NAT configuration supports IPv4 only.
 - See Setting up Multiple Ethernet Interfaces on page 157 for details regarding the management of the different OVOC connections.
- > To configure OVOC Server with Public IP address:
- 1. From the Network Configuration menu, choose **NAT**, and then press Enter.

Figure 13-1: Configure NAT IP

Main	Menu> Networl	< Configuration> NAT Configuration
	>1.NAT Per	Interface Configuration
	2.NAT Per h.Back	Tenant Configuration
	q.Quit to	main Menu

2. Choose option NAT Per Interface Configuration.

Figure 13-2: NAT Per Interface Configuration

NAT: No	t Defined
Redunda	ncy: Not Defined
Main Menu> Network Con	figuration> NAT Configuration
Type: I	P6
NAT: No	t Defined
Redunda	hcy: Not Defined
Interface: ens2	66
IP: 10.	10.10.10
Type: I	P4
NAT: No	t Defined
Redunda	hcy: Not Defined
Interface: ens2	24
IP: 5.5	5.5
Type: I	P4
NAT: No	t Defined
Redunda	hcy: Not Defined
>1. <mark>Add NAT</mark> 2.Edit NAT 3.Delete NAT b.Back q.Quit to main	(OUOC Application will be restarted) (OUOC Application will be restarted) (OUOC Application will be restarted) Menu

- > To add a NAT interface:
- **1.** Choose option **1**.

Figure 13-3: Add NAT



- 2. Enter the NAT interface that you wish to add.
- 3. Enter the NAT IP address, and then press Enter.
- 4. Type **y** to confirm the changes.
- 5. Stop and start the OVOC server for the changes to take effect.

To edit a NAT interface:

- 1. Choose option 2.
- 2. Enter the NAT interface that you wish to edit.
- 3. Enter the IP address of the NAT interface, and then press Enter.
- 4. Type **y** to confirm the changes.
- 5. Stop and start the OVOC server for the changes to take effect.

> To remove a NAT interface:

- 1. Choose Option 3.
- 2. Enter the NAT interface that you wish to remove.
- **3.** Type **y** to confirm the changes.
- 4. Stop and start the OVOC server for the changes to take effect.

Configure OVOC Server with NAT IP per Tenant

This option can be configured when OVOC is deployed behind a different NAT to customer tenants. It allows the configuration of an applicative level NAT interface for each tenant domain; Devices' incoming communication like SNMP traps, license reports and file upload/download will communicate via the tenants' NAT interface.

> To configure NAT IP addresses per tenant:

1. From the Network Configuration menu, choose NAT, and then press Enter.

Figure 13-4: NAT Configuration per Tenant

Main	Menu> Network Configuration> NAT Configuration	
	>1.MAT Per Interface Configuration 2.NAT Per Tenant Configuration	
	b.Back q.Quit to main Menu	

2. Choose option NAT Per Tenant Configuration.

Choose a tenant Index:			
0> T_4-6		NAT:	
1>1	NAT:		
2) fg2	NAT:		
3) Tenant1		NAT:	
4) Tenant_Full_	Tests		NAT:
5) Tenant_Full2	_Tests2		NAT:
6) Tenant2		NAT:	
7) Tenant3		NAT:	
8> ZOOM	NAT :		
9> OC	NAT:		
10> OC-JSON		NAT:	
11) OC_and_Z00M		NAT:	
12> 0C_no_T_Id		NAT:	
13) A	NAT:		
14> ddddddddd		NAT:	
15) a	NAT:		
16 <u>></u> Quit			
:			

3. Enter the number corresponding to the tenant that you wish to configure.

Figure 13-5: NAT IP Address



4. Enter the NAT IP address of the Tenant. Restart is required to apply changes.

ote =	Restart will be n	eeded to	apply	the char	iges.		
	Ø> T_4-6		NAT:				
	1) 1	NAT:					
	2) fg2	NAT:					
	3) Tenant_Full_	lests		NAT:			
	4) Tenant_Full2	_Tests2		NAT:			
	5) [enant2		NHI				
	b) lenantj	NAT -	NHI:				
	77 200n	NHI-					
	82 0C TEON	NH1 -	NOT -				
	10) 0C and 700M		NAT-				
	11) OC no T Id		NAT :				
	12) A	NAT:					
	13) ddddddddd		NAT:				
	14) a	NAT:					
	15) Tenant1		NAT: 1	.1.1.1			
		_					
	>1.Easts NAT Re- 2.Delete NAT P 3.Restart To A b.Back q.Quit to main	lenant er Tenant pply Chai Menu	t nges	<0U0C	Application	will be	restarted)

Figure 13-6: Configure WAN

- to change the NAT IP address:
- Choose option **1**.
- to delete the NAT IP address:
- Choose option 2
- To restart the server:
- Choose option 3.

Establishing Devices - OVOC Connections

When devices are deployed behind a firewall or NAT in the cloud or in a remote network, they cannot connect establish a direct connection with the OVOC server. Consequently, the following methods can be used to overcome this issue:

- Automatic Detection: devices are connected automatically to OVOC through sending SNMP Keep-alive messages. See Automatic Detection below.
- OVOC Cloud Architecture Mode: Communication between OVOC deployed in the AWS and Azure Cloud and devices deployed either in the AWS Cloud or in a remote network are secured over an HTTP/S tunnel overlay network. See Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on the next page

Automatic Detection

The Automatic Detection feature enables devices to be automatically connected to OVOC over SNMP. When devices are connected to the power supply in the enterprise network and/or are rebooted and initialized, they're automatically detected by the OVOC and added by default to the AutoDetection region. For this feature to function, devices must be configured with the OVOC server's IP address and configured to send keep-alive messages. OVOC then connects to

the devices and automatically determines their firmware version and subnet. Devices are then added to the appropriate tenant/region according to the best match for subnet address. When a default tenant exists, devices that cannot be successfully matched with a subnet are added to an automatically created AutoDetection Region under the default tenant. When a default tenant does not exist and the device cannot be matched with a subnet, the device isn't added to OVOC.

For more information, refer to Adding Devices Automatically.

Configure OVOC Cloud Architecture Mode (WebSocket Tunnel)

When OVOC is deployed in a public cloud and managed devices are either deployed in the Cloud or in an enterprise network, an automatic mechanism can be enabled to secure the OVOC server > SBC/UMP-365 Management Pack/SmartTAP 360° Live device communication through binding to a dedicated HTTP/S tunnel through a generic WebSocket server connection. This mechanism binds several different port connections including SNMP, HTTP, syslog and debug recording into an HTTP/S tunnel overlay network. This eliminates the need for administrators to manually manage firewall rules for these connections and to lease third-party VPN services. When operating in this mode, Single Sign-on can also be performed from the Devices Page link in the OVOC Web interface to devices deployed behind a NAT. The figure below illustrates the OVOC Cloud Architecture.





- This mode is supported on Microsoft Azure, Amazon AWS, VMware and HyperV platforms for all SBC devices Version 7.2.256 and later; SmartTAP Version 5.5 and later and UMP 365 Management Pack Version 8.0.220 and later.
 - This mode only supports IPv4 networking.
 - See also Setting up Multiple Ethernet Interfaces on page 157

This section includes the following:

Before Enabling Cloud Architecture Mode on the next page

- Configuring Cloud Architecture Mode (WebSocket Tunnel) on the next page
- Change the Cloud Architecture Mode Service Password on page 156

Before Enabling Cloud Architecture Mode

Before enabling Cloud Architecture mode, ensure the following:

- Ensure HTTP port 80 or HTTPS port 443 are open on the Enterprise firewall.
 - For maximum security, its advised to implement this connection over HTTPS port 443 with One-way authentication. Mutual authentication is not supported for this mode.
 - This connection can be secured using either AudioCodes certificates or custom certificates.
 - Port 915 used for WebSocket Client and OVOC Server communication (internal) see Configuring the Firewall on page 292.
- Ensure that all managed devices have been upgraded to the software version that supports this feature (refer to SBC-Gateway Series Release Notes for Latest Release)



If devices are not appropriately upgraded then they cannot be managed in OVOC.

- Ensure that the following parameters have been configured for the managed devices (see Configuring SBC for Tunnel Mode):
- In the OVOC Web interface, the SBC Devices Communication parameter must be set to IP Based in the Configuration screen (System tab > Administration menu > OVOC Server folder > Configuration)

Configuring OVOC Web Interface for Tunnel Mode

This section describes how to configure the OVOC Web SBC device communication.

To configure SBC devices communication:

1. Open the OVOC Server Configuration screen.

	n tasks	
CONFIGURATION		
ADMINISTRATION <	GENERAL SETTINGS	OVOC INTERNAL MAIL SERVER SETTINGS
LICENSE ^	OVOC Hostname Description	Internal Mail Server From Address OVOC@saudiocodes.com
Configuration Tenants Allocations System Allocations Eloating License	BBC Devices Communication IP Based Privacy Mode	Internal Mail Server Real Name OVOC
SECURITY ^	globalLogo.png Č	
Authentication Operators SAML		
OVOC SERVER	Masked Digits Number 4	
Status	Submit	Submit
Configuration		
Calls Storage Calls Status		

Figure 13-8: SBC Devices Communication

2. Set parameter SBC Devices Communication to IP Based.

Configuring Cloud Architecture Mode (WebSocket Tunnel)

This option configures the OVOC server in a cloud topology. When configured, a "secure tunnel" overlay network" is established between the connected devices and the OVOC server. This connection is secured over a WebSocket connection. The Tunnel Status indicates the status for all sub-processes running for this architecture.

> To setup cloud architecture:

1. From the Network Configuration menu, choose Cloud Architecture.

Figure 13-9: Cloud Architecture

Main Menu> Network Configuration> Cloud Architecture						
Cloud Architecture Status: ENABLED Tunnel Interface: eth0 (main) Tunnel Status: UP						
>1.Disable Cloud Architecture (The server will be rebooted)						
2.Add new user						
3.Edit user password						
b.Back						
g.Quit to main Menu						

- 2. Select option Enable Cloud Architecture.
- 3. Select the IPv4 interface for which to enable this mode and then press Enter.

Figure 13-10: Choose IP Interface







When this option is configured, the NAT configuration option is disabled.

Add New Cloud Architecture Mode User

This option allows you to create new users for the Cloud Architecture mode.

To create new users:

1. Select option 2 Add New User

```
Figure 13-11: Create New Cloud Architecture User
         Existing users:
         1) VPN
         Provide new Username:
         UPN1
          Please provide new password:
```

- 2. Enter the name of the new user.
- 3. Enter the new password and confirm (passwords must be between 2-20 characters).

Change the Cloud Architecture Mode Service Password

This section describes how to change the password for a Cloud Architecture mode user.

> To change the password:

1. Select Option 3 Edit User Password.

Figure 13-12: Edit User Password



- 2. Select the user whose password you wish to change and confirm.
- 3. Enter the new password and confirm (passwords must be between 2-20 characters).

Setting up Multiple Ethernet Interfaces

OVOC supports configuration of multiple ethernet interfaces. This allows SBC devices to establish connection with OVOC over different subnets. Interfaces can be configured for IPv4 and IPv6 with the following exceptions:

- The OVOC Main Management interface only supports IPv4.
- Each IPv4 interface can be configured for NAT and one of the IPv4 interfaces can be configured to work in the Cloud Architecture mode.

In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound network interfaces' to each one of the subnets. For Static Routes configuration, see Static Routes on page 235.

OVOC supports the management of multiple ethernet interfaces with the following scenarios:

- NAT IP Interface (Configure OVOC Server with NAT IP Address per Interface on page 149
- WebSocket Tunnel (Cloud Architecture Mode) (Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153)
- Public IP address
- Private IP address

The IP address that is sent to the SBC devices upon connection establishment and the IP address that is used for License Management, Software download and backup configuration is determined according to the following logic:

- If this interface is configured with Cloud architecture mode (see Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153) OVOC will sent/use tunneling websocket IP 169.254.0.1.
- If this interface is configured with a NAT IP address (see Configure OVOC Server with NAT IP Address per Interface on page 149), OVOC will use the NAT IP address of this interface.
- If this interface is configured with a public IP address, OVOC will use the public IP address, otherwise, OVOC sends the private IP address of the interface.

The interface used can be verified manually by using the following command with root permissions:

ip route get <IP>

[root@aclovoc01 ~]# ip route get 10.15.77.35 10.15.77.35 via 10.1.0.1 dev ens160 src 10.1.8.24

In the output it can be seen that ens160 is used for this IP address. Only one interface can be selected from all interfaces on the server to be use for routing this IP address.

In the event where the customer wants to use the private IP address of the interface while the interface still uses the public IP address, it is recommended to configure the NAT IP address (see Configure OVOC Server with NAT IP Address per Interface on page 149) with the value of the private IP address for the relevant interface. This affects the OVOC IP configuration on the SBC for license management, trap destination and the URL for software upgrade/backup INI and does not prevent using the public IP address for client management.

> To add a new Interface:

1. From the Ethernet Interfaces menu, choose option **1**; a list of currently available interfaces (not yet configured) is displayed.



Figure 13-13: Add Interface

- 2. Enter the number of the IP interface that you wish to modify (on HP machines the interfaces are called 'eno1', 'eno2', etc) and then press Enter.
- 3. Choose the IP interface type and then press Enter:
 - Enter 4 for IPv4
 - Enter 6 for IPv6

Figure 13-14: Add Interface



 Enter the IP Address, Hostname and Network Prefix and confirm;. the new interface parameters are displayed.

Figure 13-15: Confirm Update



5. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Connecting Mediant Cloud Edition (CE) Devices on Azure

This section describes how to connect Mediant Cloud Edition (CE) devices to OVOC using one of the following options:

- Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on the next page
- Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address on page 163

Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address

This section describes how to establish a secure connection between the OVOC server and Mediant Cloud Edition (CE) SBC devices which are both deployed in the Azure Cloud in separate Virtual networks. Communication between OVOC and Mediant CE SBC devices is carried over the public IP addresses on both sides, requiring NAT translation from internal to public IP addresses. This is performed by configuring the OVOC server with the public IP address of the Azure platform where the OVOC server is installed (see Configure OVOC Server with NAT IP Address per Interface on page 149). The figure below illustrates this topology.

The Mediant CE SBC devices must be added to OVOC using Automatic Detection. Refer to Section "Adding AudioCodes Devices Automatically" in the OVOC User's Manual.





This section includes the following procedures:

- 1. Configuring the OVOC Server Manager on Azure (Public IP) below
- 2. Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Public IP) on the next page

Configuring the OVOC Server Manager on Azure (Public IP)

This section describes the required configuration actions on the OVOC server deployed in the Azure Cloud.

⚠

Restart the OVOC server where specified in the referenced procedures for changes to take effect.

To configure the OVOC server:

- Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 198).
- 2. Change the following default passwords:
 - acems OS user (see OS Users Passwords on page 260)
 - root OS user (see OS Users Passwords on page 260)

Unless you have made special configurations, the Azure instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change theses default passwords to minimize exposure to password hacking.

- 3. Load the OVOC license (see License on page 216).
- 4. Configure the OVOC server with Azure Public IP address to enable devices deployed behind a NAT to connect to OVOC (see Configure OVOC Server with NAT IP Address per Interface on page 149). See the setup of the virtual machine to find the Azure Public IP (see Creating OVOC Virtual Machine on Microsoft Azure on page 26
- Configure the Azure IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 243).

The same clock source should be configured on the managed devices (see Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface on the next page).

Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Public IP)

This step describes the following configuration procedures on the Mediant CE to connect to the OVOC server that is deployed in the Azure Cloud:

- 1. Configuring Mediant CE SNMP Public IP Connection using Stack Manager below
- 2. Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface on the next page

Configuring Mediant CE SNMP Public IP Connection using Stack Manager

This step describes how to configure the SNMP communication between the OVOC server deployed in the Azure Cloud and the Mediant CE using the Stack Manager.

To configure the Stack Manager:

- 1. Log in to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual.*
- 2. Click the "Mediant CE stack".
- Click the Modify button and append 161/udp port (for SNMP traffic) to "Management Ports" parameter.
- 4. Click **Update** to apply the new configuration.

Modify stack	
Automatic scaling scale-out step	1
Signaling Compone	nts
Number of network interfaces	2 👻
Interfaces with public IP	eth1
Interfaces with additional IP	
Management Ports	22/tcp.80/tcp.443/tcp.161/udp
Signaling Ports	5060/udp,5060/tcp,5061/tcp
Media Components	
Number of network interfaces	2 🗸
Interfaces with public IP	eth1
Interfaces with additional IP	
Network Subnets	
Signaling 1 subnet	
Martin Canad	

Figure 13-17: Modify Stack

Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface

This section describes how to configure the communication settings between the Mediant CE device and the OVOC server deployed in the Azure Cloud.

The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

- **To configure the Mediant Cloud Edition (CE) SBC :**
- **1.** Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
- Open the Quality of Experience Settings screen (Setup Menu > Signaling & Media tab > Media folder > Quality of Experience > Quality of ExperienceSettings).
- 3. Click Edit and configure the Keep-Alive Time Interval to 1.
- 4. Click Apply to confirm the changes.
- Open the TIME & DATE page (Setup menu > Administration tab) and in the NTP Server Address field, set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source.
- 6. Click Apply to confirm the changes.
- Open the SNMP Community Settings Page (Setup menu > Administration tab > SNMP folder).
- 8. Set parameter SNMP Disable to No ('Yes' by default).
- 9. Click Apply to confirm changes.
- **10.** Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

```
HostName = <Load Balancer IP>
SendKeepAliveTrap = 1
KeepAliveTrapPort = 1161
SNMPManagerIsUsed_0 = 1
SNMPManagerTableIP_0 = <OVOC Public IP Address>
```

 Reset the device for your settings to take effect (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address

This section describes how to establish a secure connection between the OVOC server and Mediant CE devices which are both deployed in the Azure Cloud in the same Virtual network. Communication between OVOC and Mediant CE SBC devices is carried over internal IP addresses (Private IP addresses) on both sides. The figure below illustrates this topology.



The Mediant CE SBC devices must be added manually to OVOC. Refer to Section "Adding AudioCodes Devices Manually" in the OVOC User's Manual.

Figure 13-18: Internal IP Connection



This section includes the following procedures:

- Configuring the OVOC Server Manager on Azure (Internal IP) below
- Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Internal IP) on the next page



The Mediant CE SBC devices must be added to OVOC manually. Refer to Section "Adding AudioCodes Devices Manually" in the OVOC User's Manual.

Configuring the OVOC Server Manager on Azure (Internal IP)

This section describes the required configuration actions on the OVOC server deployed in the Azure Cloud when CE devices are deployed in the same Virtual network.



Restart the OVOC server where specified in the referenced procedures for changes to take effect.

To configure the OVOC server:

- 1. Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 198).
- 2. Change the following default passwords:
 - acems OS user (see OS Users Passwords on page 260)

root OS user (see OS Users Passwords on page 260)

Unless you have made special configurations, the Azure instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change theses default passwords to minimize exposure to password hacking.

- 3. Load the OVOC license (see License on page 216).
- 4. Configure the OVOC server with its internal (private) IP address to enable devices deployed in the same Azure Virtual network to connect to OVOC (see Server IP Address on page 228). See the setup of the virtual machine Step 1: Creating Virtual Machine on Azure to find the Azure Internal IP.
- Configure the Azure IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 243).



The same clock source should be configured on the managed devices (see Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface on the next page

Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Internal IP)

This step describes the following configuration procedures on the Mediant CE to connect to the OVOC server that is deployed in the Azure Cloud in the same Virtual network by connecting through internal IP addresses on both sides:

- Configuring Mediant CE SNMP Internal IP Connection with OVOC using Stack Manager below
- Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface on the next page

Configuring Mediant CE SNMP Internal IP Connection with OVOC using Stack Manager

This step describes how to configure the SNMP communication between the OVOC server and Mediant CE devices using the Stack Manager when both are deployed in the same Azure Virtual network.

To configure the Stack Manager:

- 1. Log in to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual.*
- 2. Click the "Mediant CE stack".
- Click the Modify button and append 161/udp port (for SNMP traffic) to "Management Ports" parameter.
- 4. Click **Update** to apply the new configuration.

Figure 13-19: Modify Stack

Modify stack		
Number of network interfaces ⁽²⁾	2 🗸	•
Interfaces with public IP ⁽²⁾		
Interfaces with additional IP ⁽²⁾		
Management Ports ⁽¹⁾	22/tcp,80/tcp,443/tcp,161/udp	
Signaling Ports ⁽¹⁾	5060/udp,5060/tcp,5061/tcp	
Instance Type ⁽²⁾	Standard_DS3_v2	
Media Components		
Number of network interfaces ⁽²⁾	2 🗸	
Interfaces with	all	-
Modify Cancel		

Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface

This section describes how to configure the connection settings between the Mediant CE device and the OVOC server deployed in the Azure Cloud in the same Virtual network.



The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

- To configure the Mediant Cloud Edition (CE) SBC:
- **1.** Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
- Open the TIME & DATE page (Setup menu > Administration tab) and in the NTP Server Address field, set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source.
- 3. Click Apply to confirm the changes.
- Open the SNMP Community Settings Page (Setup menu > Administration tab > SNMP folder).
- 5. Set parameter SNMP Disable to No ('Yes' by default).
- 6. Click Apply to confirm changes.
- 7. Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

HostName = <Load Balancer IP> SNMPManagerIsUsed_0 = 1 SNMPManagerTableIP_0 = <OVOC Server Internal IP>

 Reset the device for your settings to take effect (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

Connecting Mediant Cloud Edition (CE) SBC Devices on AWS

This section describes the procedure for establishing a secure connection between the OVOC server which is installed in the AWS Cloud and Mediant Cloud Edition (CE) SBC devices which are also deployed in the AWS Cloud. Communication between OVOC and Mediant CE SBC devices is carried over the public IP addresses on both sides, requiring NAT translation from internal to public IP addresses. This can be performed by either configuring the OVOC server with the public IP address of the AWS platform where the OVOC server is deployed (see Configure OVOC Server with NAT IP Address per Interface on page 149) or by configuring OVOC Cloud Architecture mode (seeConfigure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153



The Mediant CE SBC devices must be added to OVOC using Automatic Detection. Refer to Section "Adding AudioCodes Devices Automatically" in the OVOC User's *Manual*.

This section includes the following procedures:

- Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS on the next page
- Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS on the next page

Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS

This section describes the required configuration actions on the OVOC server deployed in the AWS Cloud.

⚠

Restart the OVOC server where specified in the referenced procedures for changes to take effect.

To configure the OVOC server:

- 1. Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 198).
- 2. Change the following default passwords:
 - acems OS user (see OS Users Passwords on page 260)
 - root OS user (see OS Users Passwords on page 260)



Unless you have made special configurations, the AWS instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change theses default passwords to minimize exposure to password hacking.

- 3. Load OVOC license (see License on page 216).
- 4. Configure the OVOC server with AWS Public IP address to enable devices deployed behind a NAT to connect to OVOC server (see Configure OVOC Server with NAT IP Address per Interface on page 149). See the setup of the virtual machine Launching Public Image on AWS on page 18 to find the AWS Public IP.
- Configure the AWS Public IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 243).



The same clock source should be configured on the managed devices (see Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface on the next page).

Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS

This step describes the following configuration procedures on the Mediant CE SBC devices to connect them to the OVOC server that is deployed in the AWS Cloud:

- Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager on the next page
- Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface on the next page

Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager

This step describes how to configure the SNMP communication between the OVOC server deployed in the Azure Cloud and the Mediant CE using the Stack Manager.

- **To configure the Stack Manager:**
- 1. Log in to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual.*
- 2. Click the "Mediant CE stack".
- **3.** Click the **Modify** button and append **161/udp port** (for SNMP traffic) to "Management Ports" parameter.
- 4. Click **Update** to apply the new configuration.

Figure	13-20:	Modify	Stack

Automatic scaling	1
scale-out step	
Signaling Componer	nts
Number of network interfaces	2 👻
Interfaces with public IP	eth1
Interfaces with	
additional IP	
Management Ports	22/tcp.80/tcp.443/tcp.161/udp
Signaling Ports	5060/udp.5060/tcp.5061/tcp
Media Components	
Number of network	2 👻
interfaces	
Interfaces with public IP	eth1
Interfaces with	
additional IP	
Network Subnets	
Signaling 1 subnet	

Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface

This section describes how to configure the communication settings between the Mediant CE device and the OVOC server deployed in the AWS Cloud.
The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

To configure the Mediant Cloud Edition (CE) SBC for AWS:

- 1. Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
- Open the Quality of Experience Settings screen (Setup Menu > Signaling & Media tab > Media folder > Quality of Experience > Quality of Experience Settings).
- 3. Click Edit and configure the Keep-Alive Time Interval to 1.
- 4. Click Apply to confirm changes.
- Open the TIME & DATE page (Setup menu > Administration tab) and configure the AWS site IP address/FQDN Domain Name(where the OVOC server is installed) as the NTP server clock source.
- 6. Click Apply to confirm changes.
- Open the SNMP Community Settings Page (Setup menu > Administration tab > SNMP folder).
- 8. Set parameter SNMP Disable to No ('Yes' by default).
- 9. Click Apply to confirm changes.
- **10.** Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

HostName = <Load Balancer IP> SendKeepAliveTrap = 1 KeepAliveTrapPort = 1161 SNMPManagerIsUsed_0 = 1 SNMPManagerTableIP_0 = <OVOC Public IP Address>

Reset the device for your settings to take effect (Setup menu > Administration tab
 Maintenance folder > Maintenance Actions).

Part IV

OVOC Server Upgrade

This part describes the upgrade of the OVOC server on dedicated hardware and on virtual and cloud platforms.



- This version can be upgraded from versions 8.2. or 8.2.1000.
- Before proceeding, it is highly recommended to backup the OVOC server files to an external location (OVOC server Backup).
- When upgrading from Version 8.0 and above to Version 8.2: Calls, alarms and statistics data are not preserved; you must restore this data to a separate virtual machine (see Restore Backup Data to Separate Virtual Machine on page 195).
- When upgrading from Version 7.2.3000: Optionally migrate topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the upgrade.
- Upgrade of OVOC Version 7.8 and later must be performed on HP DL Gen10 machines. Upgrade on HP DL G8 machines is not supported.
- For obtaining the upgrade file, see OVOC Software Deliverables on page 13
 - ✓ Note that you must verify this file, see Files Verification on page 16

14 Upgrading OVOC Server on Amazon AWS and Microsoft Azure

This section describes how to upgrade the OVOC server on the Amazon AWS and Microsoft Azure platforms.

- Before proceeding, it is highly recommended to backup the OVOC server files to an external location (seeOVOC Server Backup Processes on page 190).
 - Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the upgrade.
 - For obtaining the upgrade file, see OVOC Software Deliverables on page 13
 Note that you must verify this file, see Files Verification on page 16
 - For pre-upgrade actions, see Before Upgrading on Microsoft Azure below
 - For post-upgrade actions, see After Upgrading on AWS on page 175

Before Upgrading on Microsoft Azure

This procedure describes the actions required before upgrading to OVOC version 8.0 instance with updated memory requirements.

> Do the following:

- 1. Stop your OVOC instance (see Stop the Application on page 215
- 2. Change Instance type to the following:
 - Low Profile: D8ds_v4
 - High Profile: D16ds_v4
- 3. Start new OVOC instance.
- 4. Upgrade OVOC Software to the new OVOC software version as described in Upgrading OVOC Server on Amazon AWS and Microsoft Azure above.

Cloud Upgrade Procedure

This section describes how to upgrade OVOC on the Azure and AWS platforms.

To upgrade the OVOC server on Azure and AWS:

➤ To install DVD3:

- 1. Download the DVD3.ISO file Version 8.4.45 to your PC.
- 2. Using the WinSCP utility (see Transferring Files on page 328) transfer the DVD3.ISO to the OVOC server acems user home directory: /home/acems

- **3.** Open an SSH connection.
- 4. Login into the OVOC server as 'acems' user with password *acems* (or customer defined password).
- 5. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

6. Mount the DVD to make it available:

mount /home/acems/DVD3_OVOC_ 8.4.45.iso /mnt

cd /mnt/EmsServerInstall/

7. Run the installation script from its location:

./install





8. Enter y, and then press Enter to accept the License agreement.





9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter y to run the full Upgrade.



Upgrade with migration can be very long (8 hours or longer), depending on the number of tenants, volume of QoE data, and data distribution.

- Due to Postgres slowness with a large number of partitions, the upgrade is prevented depending on the number of partitions (which is approximately calculated as the number of tenants):
 - Approximately 5 tenants for VM Low profile (depending on QoE data and distribution)
 - Approximately 20 tenants for VM High profile and Bare Metal (depending on QoE data and distribution)
 - ✓ SP spec no limitation
- **10.** The process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).
- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 14-3: OVOC Server Installation Complete

1HF0: Initializing c3p0-0.1 [built 16-3muny-2007 14:46:42; dbug/ true; trace: 10] Du 66; 2021 00:322 Af CoastAnnas 27:260; mol.aktractarSource getBolkmager DHF0; Initializing c3p0 ppd com.ehonger2: c3p2 housercedtBolks / comment uncollatiSource - com.mehonger27:2690 WrapperConnectionPoolDataSourceddBabdF1 [acquireIncrement -> 3. acquireIn DHF0; Initializing c3p0 ppd com.ehonger2: c3p2 housercedtBolks / comment uncollatiSource - can.mehonger27: c3p0 WrapperConnectionPoolDataSourceddBabdF1 [acquireIncrement -> 3.
06 Jun 2022 10:03:23:233 Entity manager initialization completed >>> Copy ENS document files
iritables: No chain/target/match by that name. ipitables: No chain/target/match by that name. ipitables: No chain/target/match by that name. ipotables: No chain/target/match by that name.
>>> Renove /tsp all contents
>>> VVC Installation completed [rootdems.servers Enserverinstall]#

- **11.** Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
- 12. Login to the OVOC server by SSH, as 'acems' user and enter password acems.
- **13.** Switch to 'root' user and provide *root* password (default password is *root*):

su - root

14. Type the following command:

OvocServerManager

15. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify that login to OVOC Web client is successful.

After Upgrading on AWS

This procedure below describes the required actions on AWS following the upgrade to versionOVOC Version 8.0.

> Do the following:

- 1. Run full OVOC backup (see OVOC Server Backup Processes on page 190)
- 2. Create new AWS instance on m5.4xlarge (High Profile) machine with OVOC Software version 8.0.
- 3. Restore OVOC data from the backup (see OVOC Server Restore on page 192).



The OVOC version from where the backup is taken must be identical to the OVOC version on which the restore is run.

15 Upgrading OVOC Server on VMware and Microsoft Hyper-V Virtual Machines

This chapter describes how to upgrade the OVOC server on VMware and Microsoft Hyper-V Virtual machines.

- Before proceeding, it is highly recommended to back up the OVOC server files to an external location (OVOC Server Backup Processes on page 190).
 - If you are upgrading from Version 7.2.3000, you can optionally migrate OVOC topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
 - Ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the upgrade.
 - For obtaining the upgrade file, see OVOC Software Deliverables on page 13
 - ✓ Note that you must verify this file, see Files Verification on page 16

Run the Server Upgrade Script

This section describes how to run the OVOC server upgrade script.

Option 1: Standard Upgrade Script

Once you have setup the virtual machines, you can run the OVOC Server upgrade script.



Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

➤ To install DVD3:

- 1. Download the DVD3.ISO file Version 8.4.45 to your PC.
- 2. Using the WinSCP utility (see Transferring Files on page 328) transfer the DVD3.ISO to the OVOC server acems user home directory: /home/acems
- **3.** Open an SSH connection.
- 4. Login into the OVOC server as 'acems' user with password *acems* (or customer defined password).
- 5. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

6. Mount the DVD to make it available:

mount /home/acems/DVD3_OVOC_ 8.4.45.iso /mnt

cd /mnt/EmsServerInstall/

7. Run the installation script from its location:

./install





8. Enter y, and then press Enter to accept the License agreement.

Figure 15-2: OVOC server Upgrade – License Agreement

relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship between the parties. Neither party shall have the right to bind the other to any obligation, nor have the right to incur any liability on behalf of the other. 10.8. Integration This Agreement is the complete and exclusive agreement between the parties with regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda related hereto. Any Licensee purchase order issue for the software, documentation, or services provided hereto. Any Licensee purchase order issue for the software, documentation, or services provided hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the terms hereof. 10.9. Counterparts This Agreement may be executed in multiple original counterparts, each of which will be an original, but all of which taken together shall constitute one and the same document if bearing an authorized signature of Licensor and Licensee. Do you accept this agreement? (y/n)y>>> Checking the operational environment >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020 >>> >>> PASSED >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020 ... PING EMS-server-17 (10.3.180.17) 56(84) bytes of data. 64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms --- EMS-server-17 ping statistics ---l packets transmitted, l received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms >>> PASSED >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020 >>> >>> Free Space in /var/tmp directory: 16190944

9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter y to run the full Upgrade.



Upgrade with migration can be very long (8 hours or longer), depending on the number of tenants, volume of QoE data, and data distribution.

- Due to Postgres slowness with a large number of partitions, the upgrade is prevented depending on the number of partitions (which is approximately calculated as the number of tenants):
 - Approximately 5 tenants for VM Low profile (depending on QoE data and distribution)
 - Approximately 20 tenants for VM High profile and Bare Metal (depending on QoE data and distribution)
 - ✓ SP spec no limitation
- **10.** The process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).
- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 15-3: OVOC Server Installation Complete

INFO: Initializing cape-0.6.1 (built 16-January-2007 14:66:42; debug? true; trace: 10) Jon 66; 2021 (bailt 16-January-2007 14:66:42; debug? true; trace: 10) Jon 66; 2021 (bailt 16-January-2007 16:16:42; debug? true; estiol/Manager JAFO: Initializing cape poolcom.echange.v2:c3pe UrapperConnectionPoolDataSource@capetoOMmager JAFO: Initializing cape poolcom.echange.v2:c3pe UrapperConnectionPoolDataSource@capetoOMmager JAFO: Initializing cape JAFO: Init
06 Jun 2022 10:03:23:233 Entity manager initialization completed >>> Copy EMS document files
>>> Copy Mib files
Disables: No chain/target/match by that name. Ustables: No chain/target/match by that name. State security of the state of
>>> Remove /trp all contents >>> Restarting Apache httpd
·····
>>> OVC Installation completed [codems-syntam Emsorrange]

- **11.** Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
- 12. Login to the OVOC server by SSH, as 'acems' user and enter password acems.
- **13.** Switch to 'root' user and provide *root* password (default password is *root*):

su - root

14. Type the following command:

OvocServerManager

15. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify that login to OVOC Web client is successful.

16 Upgrading OVOC Server on Dedicated Hardware

This section describes the upgrade of the OVOC server on dedicated hardware.

Upgrading the OVOC Server-DVD

This section describes how to upgrade the OVOC server from the AudioCodes supplied installation DVD. To upgrade the OVOC server, only **DVD3** is required (see OVOC Software **Deliverables** on page 13). Verify in the OVOC Manager 'General Info' screen that you have installed the latest Linux revision (seeHardware and Software Specifications on page 7). If you have an older OS revision, a clean installation must be performed using all three DVDs (see Installing the OVOC server on Dedicated Hardware). The upgrade includes the installation of the



Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

- To upgrade the OVOC server:
- 1. Insert DVD3-OVOC Server Application Installation into the DVD ROM.
- Login into the OVOC server by SSH, as 'acems' user and enter password acems (or customer defined password).
- 3. Switch to 'root' user and provide root password (default password is root):

su - root

4. Mount the CDROM to make it available (if required):

mount /home/acems/DVD3_OVOC_/mnt

5. Run the installation script from its location:

cd /misc/cd/EmsServerInstall/

./install

Figure 16-1: OVOC server Upgrade



6. Enter y, and then press Enter to accept the License agreement.



11.4. Severability If any provision herein is ruled too broad in any respe on shall be limited only so far as it is necessary to allow conformance to shall be deleted from the Agreement, but the remaining provisions shall r 11.5. Assignment Neither this Agreement or any of Licensee's rights or obl tten permission of Licensor and any attempt to do so shall be without effe sferred to any person; (ii) the Licensee being merged or consolidated with 11.6. Export Licensee understands that the Licensed Software may be a regu , and may require a license to export such. Licensee is solely responsible 11.7. Relationship of Parties Nothing herein shall be deemed to create an the parties. Neither party shall have the right to bind the other to any o 11.8. Integration This Agreement is the complete and exclusive agreement b ated hereto. Any Licensee purchase order issue for the software, documenta erms hereof. 11.9. Counterparts This Agreement may be executed in multiple original cou ing an authorized signature of Licensor and Licensee.

```
Do you accept this agreement? (y/n)y
```

- The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:
 - If you are prompted to reboot, press Enter to reboot the OVOC server, and then repeat steps 2-7 (inclusive).
 - If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. on the next page





- 8. Wait for the installation to complete and reboot the OVOC server by typing reboot.
- **9.** When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
- 10. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

11. Type the following command:

OvocServerManager

12. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify that login to OVOC Web client is successful.

Upgrading the OVOC Server using an ISO File

This section describes how to upgrade the OVOC server using an ISO file.

➤ To upgrade using an ISO file:

- 1. Login into the OVOC server by SSH, as 'acems' user and enter password *acems* (or customer defined password).
- Using WinSCP utility (see Transferring Files on page 328), copy the .ISO file that you
 received from AudioCodes from your PC to the OVOC server acems user home directory:
 /home/acems
- 3. Switch to 'root' user and provide root password (default password is root):

su - root

4. Specify the following commands:

mount /home/acems/DVD3_OVOC_ 8.4.45.iso /mnt

cd /mnt/EmsServerInstall

5. Run the installation script from its location:

./install





6. Enter y, and then press Enter to accept the License agreement.



based upon the net income of bicensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement or any of Licensee's rights or obl
tten permission of Licensor and any attempt to do so shall be without effe
sferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regu
, and may require a license to export such. Licensee is solely responsible
11.7. Relationship of Parties Nothing herein shall be deemed to create an -
the parties. Neither party shall have the right to bind the other to any o
11.8. Integration This Agreement is the complete and exclusive agreement b
ated hereto. Any Licensee purchase order issue for the software, documenta
erms hereof.
11.9. Counterparts This Agreement may be executed in multiple original cou
ing an authorized signature of Licensor and Licensee.
Do you accept this agreement? (y/n)y

7. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server, login as 'acems' user, enter password *acems* (or customer defined password) and then repeat steps 4-8 (inclusive).
- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below.

Figure 16-6: OVOC server Installation Complete

<pre>HMFD: Initializing cape-0.0.1 [built is-Jahuary-2007 14:66:82; debug? true; trace: 10] Jun 66; 2021 (10):322 Af Cose Knamey 2:2:69; bool Back AddataSource getBool Knamger Jun 67; Jun 10:3:22 Af Cose Knamey 2:2:69; bool Back AddataSource getBool Knamger Jun 69; Jun 10:3:22 Af Cose Knamey 2:2:69; bool Back AddataSource getBool Knamger Jun 69; Jun 10:3:22 Af Cose Knamge 2:2:69; bool Back AddataSource getBool Knamger Jun 70; Jun 10:3:22 Af Cose Knamge 2:2:69; bool Back AddataSource getBool Knamger Jun 70; bool Knamger 2:2:69; bool Back AddataSource getBool Knamger Jun 70; bool Knamger 2:2:69; bool Knamger 2:2:69; bool Back AddataSource getBool Knamger Jun 70; bool Knamger 2:2:69; bool Knamger</pre>
06 Jun 2022 10:03:23:233 Entity manager initialization completed >>> Copy EMS document files
>>> Copy Mib files
upibles: No chain/target/match by that name. uptables: No chain/target/match by that name. uptables: No chain/target/match by that name. uptables: No chain/target/match by that name. State security of the security of t
>>> Remove /tmp all contents >>> Restarting Apache httpd
···· · · · · · · · · · · · · · · · · ·
>>> OVC Installation Completed [rodgems-server a Ensavervirust1]#

- 8. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
- **9.** When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
- **10.** Switch to 'root' user and provide *root* password (default password is *root*):

su - root

11. Type the following command:

OvocServerManager

12. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify that login to OVOC Web client is successful.

17 Installation and Upgrade Troubleshooting of the Operational Environment

This section describes the different scenarios for troubleshooting the operational environment.

If you attempted to upgrade and your system did not meet the minimum hardware requirements, the following message is displayed:

Figure 17-1: Minimum Hardware Requirements Upgrade

>>> Checking the operational environment
>>> Checking hardware spec - Tue Feb 5 13:14:36 IST 2019
•••
ERROR: Your system does not meet the minimal requirements for VM
Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
Actual setup: CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB

FATAL ERROR: Could not install the application - the system does not meet minimal hardware requirements
+++++++++++++++++++++++++++++++++++++++

If the OVOC server hardware configuration is changed and then the server is restarted, the following message is displayed in the /var/log/ems/nohup.out file.

Figure 17-2: Minimum Hardware Requirements System Error



Whenever an upgrade or clean installation is performed, and then the hardware settings are changed, which results in the minimum requirements not being met, the following message is displayed in the OVOC Server ManagerStatus screen :

Application	- Status
Watchdog	DOWN
0VOC Server	DOWN
SEM CPEs Server	DOWN
SEM MS Lync Server	DOWN
SEM Endpoints Server	DOWN
Floating License Server	DOWN
Pref Monitoring Server	DOWN
Tomcat Server	DOWN
Apache HTTP Server	DOWN
Oracle DB	UP
0racle Listener	UP UP
Cassandra	DOWN
SNMP Agent	DOWN
NTP Daemon	UP UP
Your system does no	
Minimal requirement	ts: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
Actual setup:	CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
· ·	
Press 'Ente	er' key to go back to the main menu

Figure 17-3: Status Screen Error

Whenever an upgrade or clean installation is performed, and then the hardware settings are changed, which results in the minimum requirements not being met, the following message is displayed in the OVOC Server Manager General Info screen: Figure 17-4: General Info Minimum Requirements

Collecting information...

```
Machine information
|Environment: Virtual(Manufacturer: VMware, Inc.)
Product Name: VMware Virtual Platform
Spec: Minimal system require
                               ents not met. See Status screen for more details.
CPU: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz, total cores: 1
Memory: 14877 MB
Network:
 VMware VMXNET3 Ethernet Controller (rev 01)
ACEMS Usage: 11G
Disk:
NAME
              MOUNTPOINT SIZE FSTYPE
                                            TYPE STATE
                                                         VENDOR
fdθ
                            4K
                                            disk
                          500G
                                            disk running VMware
sda
-sdal
                            2G xfs
                                            part
 -sda2
                          498G LVM2_member
                                            part
  -vg-root
                           20G xfs
                                            lvm running
  -vg-swap
                                                running
              [SWAP]
                          7.8G swap
                                            lvm
                                            lvm running
  |-vg-data
              /data
                          254G xfs
  -vg-meta
              /meta
                          512M xfs
                                            lvm
                                                 running
                           20G xfs
  -vg-opt
                                            lvm
                                                running
              /opt
                           25G xfs
   -vg-oracle /oracle
                                            lvm
                                                running
  |-vg-var
`-vg-home
              /var
                           20G xfs
                                            lvm
                                                 running
                          150G xfs
                                                 running
              /home
                                                                                     lvm
srθ
                         1024M
                                            rom running NECVMWar
                          2.1G iso9660
ιοορθ
              /misc/cd
                                            loop
|Data usage:
/dev/mapper/vg-data
                                            254G 179G
                                                         76G 71% /data
10.3.180.50:/data1/7.6.1000/DVD3/7.6.1082 459G 281G 155G 65% /ins
Versions
OVOC Version
                  : 7.6.1075
OS Version
                  : Linux 3.10.0-957.1.3.el7.x86_64 x86_64
OS Revision
                  : CentOS 7 for EMS Server (Rev. 18)
                  : java full version "1.8.0_201-b09"
Java Version
Apache version : Apache/2.4.6 (CentOS) Server built:
Cassandra version: 3.11.2
                                                           Nov 5 2018 01:47:09
```

Part V

OVOC Server Machine Backup and Restore

This part describes how to restore the OVOC server machine from a backup.

18 OVOC Server Backup Processes

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 below).

- **Cassandra backup:** Contains the backup of the Cassandra database. Backs up to the archive file cassandraBackup_<version>_<date>_<snapshotId>_<Role>_numberOfNodes.tar.
- 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.
 - 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	18-1:	Backup	Log
--------	-------	--------	-----

[root@low-185 ~]# c [root@low-185 emsBa total 935556	d ∕data ckup]#	INBIĒ∕emsB 11	ackup			
-rw-rr 1 emsadr	in nbif	1546240	Jun 🗄	20 04	:01	cassandraBackup_8.4.20_2406200200_171884526
1564_NGNT_1.tar						
-rw-rr 1 emsadr	in nbif	955596800	Jun 🗄	20 04	1:00	ensServerBackup_8.4.20_2406200200.tar
drwxrwxr-x 2 postgi	es dba	6	Jun 🗄	20 04	:00	export
-rw-rr 1 emsadr	in nbif	313462	Jun 🗄	20 04	:00	ovocConfigBackup_8.4.20_2406200200.tar.gz
-rw-rr 1 emsadr	in nbif	547455	Jun 3	20 04	:00	ovocFullBackup 8.4.20 2406200200.tar.gz
[root@low-185_emsBa	ckun 1#					1 0

➤ Do the following:

- **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

Change Schedule Backup Time

This step describes how to reschedule the time to run the automatic backup of the files described in OVOC Server Backup Processes above. By default, the backup is run daily at 2:00

am. You can alternatively schedule it to run on specific days.

> To schedule backup time:

- 1. From the Application Maintenance menu, choose Change Schedule Backup Time.
- 2. Enter the number corresponding to the days of the week that you wish to perform the backup according to the following (use commas to separate entries):
 - 0-Sunday
 - 1-Monday
 - 2-Tuesday
 - 3-Wednesday
 - 4-Thursday
 - 5-Friday
 - 6-Saturday

Figure 18-2: Backup Scheduling

Backup Scheduling The following backup files and directories will be created in /data/NBIF/emsBackup:
emsServerBackup_8.2.1179_cox.tar ovecPullBackup_8.2.1179_cox.tar.gz cassandraBackup_8.2.1179_cox.tar
These files should be backed up externally Note: The backup can be restored only on the same OVOC version.
Current Schedule: Sunday Monday Tuesday Vednesday Thursday Friday Saturday at 2:80
Choose the days of the week to perform DB full backup separated by a comma {0,1,2,3,4,5,6> or 'q' to quit scheduling 9 Sunday,1-Honday,2-Tuesday,3-Wednesday,4-Thursday,5-Friday,6-Saturday (q-quit)
Choose a valid pattern:days separated by a comma (0,1,2,3,4,5,6) or 'q' to quit scheduling Ø-Sunday,1-Monday,2-Tuesday,3-Wednesday,4-Thursday,5-Friday,6-Saturday (q-quit) 3 Choose an hour to perform backup (0-23) 19 New Schedule: Wednesday at 19:00 Are you sure that you want to continue? (y/n)y

3. Type y to confirm.

19 OVOC Server Restore

The OVOC server can be restored from the original machine where the backup files were created or from any other machine.

- If you're running the restore process on a different machine, its disk size should be the same as the original machine from which the backup files were taken.
 - Restore actions can be performed only with backup files which were previously created in the same OVOC version.
 - If you are restoring to a new machine, make sure that you have purchased a new license file machine ID. AudioCodes customer support will assist you to obtain a new license prior to the restore process.

To restore the OVOC server:

- 1. 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.
- 2. Use the OVOC server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.
- 3. For more details, see Getting Started on page 198.
- 4. Make sure all server processes are up in OVOC Server Manager / Status menu and the server functions properly.
- Copy all the files you backed up in OVOC Server Backup Processes on page 190 to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
- 6. From the Application Maintenance menu, choose the **Restore** option.

Figure 19-1: Restore Menu



- 7. Choose one of the following options:
 - Configuration Restore on the next page

- Full Restore on the next page
- Restore from CentOS on page 195

Configuration Restore

This option restores OVOC topology and OVOC Web configuration. The following data is restored:

- Network Topology
- License configuration
- Alarm Forwarding Rules
- Report Definitions
- PM Profiles
- QOE Thresholds
- QOE Status and Alarm definitions
- The entire configuration performed under System Configuration and System Administration menus

Data is restored from the following backup files:

- emsServerBackup_<version>_<time&date>.tar
- ovocConfigBackup_<version>_<time&date>.tar.gz



The restore process deletes all currently stored data as described above. Data that is retrieved from managed devices is not backed up, including: Alarms; Calls& SIP ladder; QoE & PM statistics; Users; Journals and Floating license reports.

To run the configuration restore operation:

1. Select option Configuration Restore. A screen similar to the following is displayed:

Figure 19-2: Configuration Restore Prompt



2. Type y to proceed. A screen similar to the following is displayed:

Figure 19-3: Configuration Restore-Confirm



- 3. Type y to proceed.
- 4. After the restore operation has completed, you are prompted to reboot the OVOC server.
- 5. If you installed custom certificates prior to the restore operation, you must reinstall these certificates (see Supplementary Security Procedures on page 315).

Full Restore

This option restores OVOC topology, OVOC Web configuration (as detailed inConfiguration Restore on the previous page) and data that is retrieved from managed devices including PMs, calls, alarms and journals. Data from the following backup files is restored:

- emsServerBackup_<version>_<time&date>.tar
- cassandraBackup_<version>_<date>_<snapshotId>_<MGMT>_numberOfNodes.tar

ovocFullBackup_<version>_<time&date>.tar.gz



The restore process deletes all currently stored data including PMs, calls, alarms and journals.

To run the full restore operation:

1. Select option Full Restore. A screen similar to the following is displayed:

Figure 19-4: Full Restore Prompt

After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.	^
Restore can be performed only with backup of the same OUOC version.	
To perform the restore procedure, please make sure that the following files exist in /data/HBIP/ directory:	
em:ServerBackup B.2.1135_coc.tar cassandruBackup B.2.1135_coc.tar-gz oweFullBackup B.2.1355_coc.tar-gz	
Note: Restore process will DELETE all the currently stored data!	
Note: OUCC Server will be rebooted at the end of restore process.	
Are you sure that you want to continue?	
	1

- 2. Type y to proceed. You are prompted again.
- 3. Type y to proceed.
- 4. After the restore operation has completed, you are prompted to reboot the OVOC server.
- 5. If you installed custom certificates prior to the restore, you must reinstall these certificates (see Supplementary Security Procedures on page 315).

Restore Backup Data to Separate Virtual Machine

This section describes how to retrieve alarms, calls and call statistics data saved in OVOC backup.

> Do the following:

- 1. Create Virtual Machine with the OVOC version from which the backup was saved.
- 2. Make sure that the OVOC machine IP address is not accessible by SBC devices.
- 3. Disable NTP on the OVOC server machine (see NTP & Clock Settings on page 243).
- 4. Restore the backup (see Full Restore on the previous page).



During startup, calls older than one year are deleted. If the customer wishes to retrieve data older than one year, change the server time to the time of the backup prior to the restore.

Restore from CentOS

This option restores the OVOC backup archives emsServerBackup, ovocFullBackup and cassandraBackup to the OVOC Server platform with the Rocky Linux Operating system installed (see Migrating to Rocky Linux Operating System on page 77).

To restore from CentOS:

1. Select option **Restore from CentOS**. A screen similar to the following is displayed:



2. Type y to confirm the action.

Part VI

OVOC Server Manager

This part describes the OVOC server machine maintenance using the OVOC server Management utility. The OVOC server Management utility is a CLI interface that is used to configure networking parameters and security settings and to perform various maintenance actions on the OVOC server.

Warning: Do not perform OVOC Server Manageractions directly through the Linux OS shell. If you perform such actions, OVOC application functionality may be harmed. Note: To exit the OVOC Server Managerto Linux OS shell level, press q.

20 Getting Started

This section describes how to get started using the OVOC Server Manager.

Connecting to the OVOC Server Manager

You can either run the OVOC Server Managerutility locally or remotely:

- If you wish to run it remotely, then connect to the OVOC server using Secure Shell (SSH).
- If you wish to run it locally, then connect using the management serial port or keyboard and monitor.

Do the following:

- 1. Login into the OVOC server by SSH, as 'acems' user and enter password acems.
- 2. Switch to 'root' user and provide root password (default password is root):

su - root

3. Type the following command:

OvocServerManager



'OvocServerManager' has been renamed to 'EmsServerManager'. Both command strings can be typed in the SSH console.

The OVOC Server Manager menu is displayed:

Figure 20-1: OVOC Server Manager Menu



• Whenever prompted to enter Host Name, provide letters or numbers.

- Ensure IP addresses contain all correct digits.
- For menu options where reboot is required, the OVOC server automatically reboots after changes confirmation.
- For some of the configuration options, you are prompted to authorize the changes. There are three options: Yes, No, Quit (y,n,q). Yes implements the changes, No cancels the changes and returns you to the initial prompt for the selected menu option and Quit returns you to the previous menu.

Using the OVOC Server Manager

The following describes basic user hints for using the OVOC Server Manager:

- The screens displaying the Main menu options in the procedures described in this section are based on a Linux installation with 'root' user permissions.
- The current navigation command path is displayed at the top of the screen to indicate your current submenu location in the CLI menu. For example, Main Menu > Network Configuration > Ethernet Redundancy.
- You can easily navigate between menu options using the keyboard arrow keys or by typing the menu option number.
- Each of the menu options includes an option to return to the main Menu "Back to Main Menu" and in some cases there is an option to go back to the previous menu level by specifying either "Back" or "Quit".

OVOC Server Manager Menu Options Summary

The following describes the full menu options for the OVOC Server Management utility:

- Status Shows the status of current OVOC processes (Viewing Process Statuses on page 203)
- General Information Provides the general OVOC server current information from the Linux operating system, including OVOC Version, OVOC server Process Status, PostgreSQL Server Status, Apache Server Status, Java Version, Memory size and Time Zone (Viewing General Information on page 206).
- Collect Logs Collates all important logs into a single compressed file (Collecting Full Logs on page 209):
- Application Maintenance Manages system maintenance actions (Application Maintenance on page 214):
 - Start / Restart the Application
 - Stop Application
 - Web Servers
 - Change Schedule Backup Time

- Restore
- License
- analytics API
- Guacamole RDP Gateway
- VMware Tools
- Shutdown the machine
- Reboot the machine
- Network Configuration Provides all basic, advanced network management and interface updates (Network Configuration on page 227):
 - Server IP Address (The server is rebooted)
 - Ethernet Interfaces (The server is rebooted)
 - Ethernet Redundancy (The server is rebooted)
 - DNS Client
 - NAT
 - Static Routes
 - SNMP Agent
 - Configure SNMP Agent

-SNMP Agent Listening Port -Linux System Traps Forwarding Configuration -SNMPv3 Engine ID

- Start SNMP Agent
- SNMPv3 Engine ID
- Cloud Architecture
- NFS
- Date & Time Configures time and date settings (Date and Time Settings on page 248):
 - NTP
 - Timezone Settings
 - Date and Time Settings
- Security Manages all the relevant security configurations (Security on page 249):
 - Add OVOC user
 - SSH
 - PostgreSQL DB Password (OVOC server will be stopped)
 - Cassandra DB Password (OVOC server will be stopped)

- OS Users Passwords
- HTTP Security Settings:
 - Disable TLSv1.0 for Apache
 - Disable TLSv1.1 for Apache

Default: TLsv1.2

- Show Allowed SSL Cipher Suites
- Edit SSL Cipher Suites Configuration String
- Restore SSL Cipher Suites Configuration Default
- Manage HTTP Service (Port 80)
- Manage IPP Files Service (Port 8080)
- Manage IPPs HTTP (Port 8081)
- Manage IPPs HTTPS (Port 8082)
- OVOC REST (Port 911)
- Floating License REST (Port 912)
- OVOC WebSocket (Port 915)
- QoE Teams Server REST (Port 5010)
- Trust Store Configuration
- SBC HTTPS Authentication
- Enable Device Manager client secured communication (Apache will be restarted)
- Change HTTP/S Authentication Password for NBIF Directory
- Disable Client's IP Address Validation
- File Integrity Checker
- Software Integrity Checker (AIDE) and Prelinking
- USB Storage
- Network Options
- Audit Agent Options (the server will be rebooted)
- Server Certificates Update
- OVOC Voice Quality Package SBC Communication
- **Diagnostics** Manages system debugging and troubleshooting (Diagnostics on page 282):
 - Server Syslog
 - Devices Syslog

- Devices Debug
- Server Logger Levels
- Network Traffic Capture

21 Viewing Process Statuses

You can view the statuses of the currently running OVOC applications.

> To view the statuses of the current OVOC applications:

1. From the OVOC server Management root menu, choose **Status**, and then press Enter.

Figure 21-1: Application Status in Standalone Mode

		\sim
Application	Status	
l Watchdog l	UP	
OVOC Monitor	UP	
OVOC Server	UP	
I QoE CPEs Master	UP	
QoE CPEs Slave	UP	
I QoE Lync Server	UP	
QoE Endpoints Server	UP	
l QoE Teams Server	UP	
Floating License Server	UP	
Performance Monitoring	UP	
WebSocket Server	UP	
Kafka	UP	
Elasticsearch	UP	
l Cassandra l	UP	
PostgreSQL DB	UP	
PG Partitions Manager	UP	
Nodes Refresher	UP	
SNMP Server	UP	
Cloud Tunnel Service	DOWN	
Apache HTTP Server	UP	
SNMP Agent	DOWN	
I NTP Daemon	DOWN	
Press 'Enter	' key to go back to the main menu	\sim

The following table describes the application statuses when OVOC runs in Stand-alone mode.

 Table 21-1: Application Statuses in Stand-alone Mode

Application	Status
Watchdog	Indicates the status of the OVOC Watchdog process.
OVOC Monitor	Validates the local OVOC server connection, clock configuration and installed software version.
OVOC Server	Indicates the status of the OVOC server process.
QoE CPEs Master	Indicates the voice quality master process status on the local server.
QoE CPEs Slave	Indicates the voice quality slave process status on the local server (identical to QoE CPEs Master process in Stand-alone mode).
QoE Reporting Server	Indicates the status of the QoE Reporting Server for managing Microsoft Teams Calls Notifications ??
QoE Lync Server	Indicates the status of the process that is responsible for retrieving Skype for Business calls and for monitoring connectivity status with

Application	Status
	Microsoft Lync server.
QoE Endpoints Server	Indicates the status of the Endpoint Server, which manages the UDP connection with the Endpoints (IP Phones) for Voice Quality Package SIP Publish RFC 6035 messages.
QoE Teams Server	Indicates the status of the OVOC process (QoE Teams Server – Up/Down) that is responsible for retrieving Teams Call Records from defined MS Teams Tenants and for monitoring connectivity status with MS Teams Tenants.
Floating License Server	Indicates the status of the connection between the OVOC server and the Floating License service.
Performance Monitoring Server	Indicates the status of the internal SNMP connection used by the OVOC server for polling managed devices.
WebSocket Server	Indicates the status of the internal connection between the WebSocket client (OVOC Web interface) and the OVOC server. This connection is used for managing the alarm and task notification mechanism.
Kafka	Indicates the status of the Kafka process for managing alarms retrieved from the VQM and PM servers.
Cassandra	Indicates the status of the Cassandra database that manages Call Details and SIP Ladder messages.
PostgreSQL DB	Indicates the status of the PostgreSQL DB.
PG Partitions Manager	Indicates the status of the process used to partition database for saving OVOC data including Calls, Summaries, History Alarms and Floating License Manager tables.
Nodes Refresher	Indicates the status of the process used to cycle through all devices to verify SNMP or HTTP connectivity.
Cloud Tunnel Service	Indicates the status of the Cloud Tunnel Service (see Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153.
Apache HTTP Server	Indicates the status of the Apache server, which manages the following connections:
	HTTP/S connection with the AudioCodes device
	The OVOC server-Client connection.

Application	Status
	The HTTP connection that is used by Endpoints for downloading firmware and configuration files from the OVOC server.
SNMP Agent	Indicates the status of the Linux SNMP Agent process. This agent is not responsible for the SNMPv2/SNMPv3 connection with the AudioCodes devices.
NTP Daemon	Indicates the status of the NTP Daemon process.
22 Viewing General Information

This section describes the General Information and Logs collection options. The General Information option provides detailed information about the OVOC server configuration and current status variables. The following information is provided:

- Components versions
- Components Statuses
- Memory size and disk usage
- Network configuration
- Time Zone and NTP configuration
- User logged in and session type

> To view General Information:

1. From the OVOC Server Manager root menu, choose **General Information**, and then press Enter.

	•	
-sda1 -sda2 -yg-root / -vg-swap [SWAP] -vg-data /data -vg-meta /meta -vg-opt /opt -vg-opt /opt -vg-home /home sr0 !Data usage: /dev/mapper/vg-data	2G xfs part 298G LUM2_member part 10G xfs 10G xfs lvm running 17.6G swap lvm running 207G xfs lvm running 128M xfs lvm running 10G xfs lvm running 128M xfs lvm running 13G xfs lvm running 207G xfs lvm running 128M xfs lvm running 129G xfs lvm running 206 xfs lvm running 12.9G iso9660 rom running NECVINar 207G 3.8G 204G	~
Versions IOVOC Version : IOS Version : IOS Revision : IJava Version : IApache version : S5:48 ICassandra version : IPostgreSQL version: Kmore	8.4.20 Linux 4.18.0 513.5.1.e18_9.x86_64 x86_64 Rocky Linux release 8.9 (Green Obsidian) openjdk full version "1.8.0_412-b08" Apache/2.4.37 (Rocky Linux) Server built: Apr 29 2024 14: 3.11.16 14.11	>

Figure 22-1: General Information

2. Press <more> to view more information; the following is displayed:

Host Name	-	185-ipv6
IP Addres	s =	2010:0003:0000:0000:0000:0000:0180:0185
Subnet Na	sk :	FFFF:FFFF:FFFF:FFFF:0:0:0:0
Network A	ddmees =	2010-3-0-0-0-0-0
NOC	-	
Interfaces one256	-	50-50-27-a0-13-m
Not Defin	ad	
Not Derin	ea	
Date & line Infor	mation	
Date & Time :	119/06/202	
Time Zone :	Europe/Lon	don (BST, +0100)
r.		
Network Time Prot	ocol	
Server #1		
Peer :	158.207.in	terhost.co.il
Sync source :	158.207.in	terhost.co.il
Stratum :	4	
Туре :	Unicast	
Last response :	240 second	s ago
Polling interval:	10 seconds	
Reach :	377 (all a	ttempts successful)
Delay :	+734us	
Offset :	+671us	
Jitter :	30ms Kmore	

Figure 22-2: General Information 1

Press <more> again to view information on the second NTP server.



tter

: 4 <more>

```
Last response : +659us[ seconds ago
Polling interval: 377 seconds
Use of uninitialized value $rest[0] in join or string at /usr/share/per15/vendor
_per1/Term/ANSIColor.pm line 488, <> line 3.
Reach : 412
Delau
                                                                                                                                                                                                                                           ^
_per1/
Reach
Delay
Offset
Jitter
                                                : 24ms <more>
 Server #4
Server #4

Peer : 3

Sync source : 3

Stratum : 10

Type : Unicast

Last response : +3351us[+3414us] seconds ago

Polling interval: 367 seconds

Use of uninitialized value $rest[0] in join or string at /usr/share/per15/vendor

_per1/Term/ANSIColor.pm line 488, <> line 4.

Reach : 68

Polo: : :
Leach
Delay
Offset
Jitter
                                                aclads06.corp.audiocodes> <more>
 Last response : +3351us[+3414us] seconds ago
Polling interval: 367 seconds
Use of uninitialized value $rest[0] in join or string at /usr/share/per15/vendor
_per1/Term/ANSIColor.pm line 488, <> line 4.
Reach : 68
 Reach
Delay
Offset
  Jitter
                                                aclads06.corp.audiocodes> <more>
Server #5

Peer : 6

Sync source : 6

Stratum : 377

Type : Unicast

Last response : +/- seconds ago

Polling interval: 34 seconds

Use of uninitialized value $rest[0] in join or string at /usr/share/per15/vendor

Use of uninitialized value $rest[0] in join or string at /usr/share/per15/vendor

<u>per1/Term/ANSIColor.pm line 488, <> line 5.</u>

<u>Reach</u> : +6573us[+6573us]

:
```

23 Collecting Full Logs

This option enables you to collect important log files. All log files are collected in a single file log.tar that is created under the user home directory.

The following log files are collected:

- OVOC server Application logs
- General Info logs
- Apache logs and configuration files
- Cassandra DB logs
- OS logs
- PostgreSQL Database logs
- Hardware information (including disk)
- OS Configuration
- File Descriptors used by processes info
- Installation logs
- Server's Syslog Messages
- Yafic scan files
- Topology file
- License file and Decoded License file
- Relevant network configuration files (including static routes)

► To collect logs:

1. From the OVOC server Management root menu, choose Collect Logs, and then press Enter.

Figure 23-1: Collect Logs

OUOC Server 8.2.135 Management
Main Menu> Collect Logs
>1.Full Logs 2.Selected Logs q.Quit to main Menu

- 2. Select option Full Logs, and then press Enter.
- 3. You are prompted if you wish to collect logs, enter **y** to proceed. The logs are collected. This process can take a few minutes. Once all of the logs have been collected, a message is displayed informing you that a Diagnostic tar file has been created and the location of the tar file.



Are you sure that you want to collect logs? (y/n) y
Collecting logs from management server:
Collecting CenemalInfo logs
Collecting deneration logs
Collecting Avache logs + configuration files
Collecting npache 1998 · Contgaration files
Collecting Ossiantia DD Togstit
Collecting bardware configuration
Collecting OS configuration
Collecting FD information
Collecting memory statistics
Collecting Rman Log Files
Collecting Yafic Scan Files
Collecting Tcpdump capture files
Collecting Postgres DB logs
Collecting Java dumps
Collecting Installation Log Files
Collecting Topology File
Collecting ovoc_cluster File
Collecting ovoc_cluster_status File
Collecting_Decoded License File
Packing TAR file
adding: logs.tar (deflated 94%)
Logs can be found in /howe/acews/logs.tar.zip
Dunca Enter to continue
rress Enter to continue

Selected Logs

This option lets you filter the collection of specific types of logs, in addition to the set of Basic logs that are collected by default.

Table 23-1	Log Types
------------	-----------

Log Type	Description
OVOC Full Logs	Full set of OVOC logs including all logs described in this table.
Apache Logs	Apache HTTP/S server logs for OVOC server > client connections; OVOC > device connections and for endpoints downloading of firmware and configuration files.
Cassandra Logs	Cassandra database logs.

Log Type		Descriptio	n	
Kafka Logs	Kafka logs for managing alarms retrieved from the VQM and PM servers.			
Syslog	Operating system syslog files (see also Diagnostics on page 282).			
Hardware Configuration	OS dmidecode output.			
FD Information	OS File Descriptors summ	nary.		
Memory Statistics	OS Memory information.	OS Memory information.		
Yafic Scans	OS Yafic scan results.			
acems & Root dirt contents	acems & Root Output of the contents of all folders under "root" and "acems" directory			acems"
	Filename	Filecize Filetone	Last modified	Permissions Owner/Gro
	ACEMS ACEMS bin boot data data dev etc home bib bib bib bib bib bib bib bib bib bi	File folder File folder	Las Monted • 06/02/22 12:47:58 • 06/02/22 12:44:38 • 06/02/22 12:44:38 • 06/02/22 12:44:38 • 06/02/22 12:44:38 • 06/02/22 12:44:38 • 06/02/22 12:44:42 • 06/02/22 12:44:42 • 06/02/22 12:44:42 • 06/02/22 12:44:42 • 06/02/22 12:44:42 • 06/02/22 12:44:42 • 06/02/22 12:44:37 • 06/02/22 12:44:37 • 06/02/22 12:44:37 • 06/02/22 12:44:37 • 06/15/22 14:20:02 •	reminisions OwnerStot
	Filename meta mt opt proc run sisin siv siv siv siv siv 2 files and 22 directories. Total size: 1,024 bytes	Filesize Filetype File folder File folder	Last modified 06/02/22 12:44:37 01/05/16 17:38:36 06/15/22 14:2002 06/15/22 14:2051 06/15/22 14:251 06/15/22 14:251 06/02/22 14:2314 06/02/22 14:245 06/15/22 14:2055 06/15/22 16:04:39 06/15/22 16:04:39 06/02/22 14:2054 06/02/22 14:2	Permissions Owner/Gro
	Accems directory contents	Filesize Filetype File folder File folder	Last modified F 06/15/22 14:2007 06/15/22 14:542 06/02/22 13:1648 06/15/22 14:2007 06/15/22 14:542 06/15/22 14:545 06/15/22 14:545 06/15/22 14:545 06/15/22 14:1537 06/15/22 14:1537 06/15/22 14:1537 06/15/22 14:1537 06/15/22 14:1537 06/15/22 14:1537 06/15/22 15:1107 06/15/22 13:12:01	Permissions Owner/Gro Anwar-xr-x root root Anwa

Log Type	Description		
	iccense.txt 1,588 Text Document 06/08/22 07:17:21 -rw root root passwords/Changed.flag 0 FLAG File 06/02/22 13:01:49 -rw-r acems root postgreSQL_version 3 File 06/15/22 14:19:48 -rw-r root root 4 files and 12 directories. Total size: 1,594 bytes		
Backup Network Files	Network Backup Files		
Tcpdump Captures	TCPdump captures		
License File	OVOC license file (see OVOC License on page 217).		
Postgres Logs	PostgreSQL database log files.		

➤ To select logs:

1. Select option Select Logs, and then press Enter. A confirmation message is displayed that Basic OVOC logs are collected.





2. If you wish to collect additional log types, choose the number corresponding to the log type that you wish to collect, and then press Enter. You are prompted if you wish to collect logs in light mode, type **y**, and then press Enter.

In the example below, 'option 2 Apache Logs' was selected. Once all of the logs have been collected, a message is displayed informing you that a tar file has been created and the location of the tar file.

Collecting logs from management server:	
Collecting GeneralInfo logs Collecting OWOC logs Collecting Apache logs + configuration files Collecting OS logs Collecting Java dumps Collecting Installation Log Files Collecting Topology File Collecting ovoc_cluster File Collecting ovoc_cluster File Collecting Decoded License File Packing TAR file adding: logs.tar (deflated 93%)	
Logs can be found in /home/acems/logs.tar.zip Press Enter to continue	

Figure 23-4: Log Directory

3. Transfer the log file to your desired location (see Transferring Files on page 328).

The following screen shows the contents of the extracted tar file for the "OVOC Full Logs" directory:

*	↑ → This PC → Windows (C:) → OVOC_Version 8.2 → logs → server_8.2.220_Logs			
^	Name	Date modified	Туре	
	onf	15/06/2022 16:26	File folder	
	EMSLogs	15/06/2022 16:26	File folder	
	InstallationLogs	15/06/2022 16:26	File folder	
	License	15/06/2022 16:26	File folder	
	OSStats	15/06/2022 16:26	File folder	
	OSSysLogs	15/06/2022 16:26	File folder	
	ServerGeneralInfo	15/06/2022 16:26	File folder	
	📕 Topology	15/06/2022 16:26	File folder	

Figure 23-5: OVOC "Full Logs"

24 Application Maintenance

This section chapter describes the application maintenance actions for managing various OVOC processes.

> To configure application maintenance:

From the OVOC Server Manager root menu, choose **Application Maintenance**.





This menu includes the following options:

- Start/Restart Application .(Start or Restart the Application below
- Stop Application (Stop the Application on the next page)
- Web Servers (Web Servers on page 216)
- Change Schedule Backup Time (Change Schedule Backup Time on page 190)
- Restore (OVOC Server Restore on page 192)
- License (License on page 216)
- analytics API (analytics API on page 221)
- Guacamole RDP Gateway (Guacamole RDP Gateway on page 222)
- VMware Tools (see VMware Tools on page 224
- Shutdown the Machine (Shutdown the OVOC Server Machine on page 225)
- Reboot the Machine (Reboot the OVOC Server Machine on page 225)

Start or Restart the Application

This section describes how to start or restart the application.

> To start/restart the application:

1. From the Application Maintenance menu, choose **Start/Restart the Application**, and then press Enter.

Figure 24-2: Start or Restart the OVOC server



- 2. Do one of the following:
 - Select **Yes** to start/restart the OVOC server.
 - Select **No** to return to menu.

Stop the Application

This option describes how to stop the OVOC server application.

> To stop the application:

- 1. In the Application menu, choose option Stop Application.
- 2. You are prompted whether you wish to stop the OVOC server.

Figure 24-3: Stop OVOC server

Main Menu> Application	Maintenance
Stop OUOC Server? >1.758 2.No	

3. Type **1** to stop the OVOC server.

Web Servers

This option enables you to stop and start the Apache HTTP Web server.

To stop/start the Apache HTTP Web server:

1. From the Application maintenance menu, choose Web Servers, and then press Enter.

Figure 24-4: Web Servers

Main Menu> Application Maintenance> Web Servers			
The Apache HTTP Server Process	is: UP		
>1.Stop the Apache HIIP Server h.Back			
g.Quit to main Menu			

2. Select option Stop/Start the Apache HTTP Server, and then press Enter.

License

The License menu enables you to view the details of the existing license or upload a new license.

The OVOC server License (SBC License pool, IP Phones and Voice Quality) should have a valid license loaded to the server in order for it to be fully operational.

To obtain a valid license for your OVOC server License you should activate your product through License Activation tool at http://www.AudioCodes.com/swactivation.

You will need your Product Key (see below) and the Server Machine ID (see below) for this activation process:

- ProductKey: the Product Key string is used in the customer order for upgrading the OVOC product. For more information, contact your AudioCodes partner.
- Machine ID: indicates the OVOC Machine ID that should be taken from the server as shown in the screen below (enter this ID in the Fingerprint field in the Activation form). This ID is also used in the customer order process when the product key is not known (for more information contact your AudioCodes representative).
- License Status: indicates whether the OVOC license is enabled (OVOC License on the next page below).
- OVOC Advanced: indicates whether the Voice Quality license is enabled (default-no). When this parameter is set to default, the followingVoice Quality feature licenses are available:
 - Total Devices = 2
 - Total Endpoints = 10
 - Total Sessions = 10
 - Total Users = 10

When set to Yes, the above parameters can be configured according to the number of purchased licenses

Expiration Date: indicates the expiration date of the OVOC time license. By default, this field displays 'Unlimited' (below).

The time zone is determined by the configured date and time in the Date & Time menu (Timezone Settings on page 247).

- When you order AudioCodes devices (MediantSBC and MediantGateway AudioCodes products), ensure that a valid feature key is enabled with the "OVOC" parameter for those devices that you wish to manage. Note that this feature key is a separate license to the OVOC server license.
 - Licenses can be allocated to Tenants in the OVOC Web according to the license parameters displayed in the License screen (see example inOVOC License below).

OVOC License

The OVOC time license sets the time period for product use. When the time license is enabled and the configured license time expires, the connection to the OVOC server is denied. The time based license affects all the features in the OVOC including the SBC License Pool, Devices (entities managed by the Device Manager) and Voice Quality Management. When the OVOC server time license approaches or reaches its expiration date, the 'License alarm' is raised (Refer to the *One Voice Operations Center Alarms Guide*).

> To view the license details or upload a new license:

1. Copy the license file that you have obtained from AudioCodes to the following path on the OVOC server machine:

/home/acems/<License_File>

2. From the Application Maintenance menu, choose License option, and then press Enter; the current License details are displayed:

ain Menu> Application Maintenance> License	
License Configuration Hanager: Server Machine ID: D520BF058C41 Product Key: D520BF058C41 License Status: ENABLED OUOC Advanced: Yes Expiration Date: 01-01-2140	
Voice Quality Total Devices: 100,000,000 Total Endpoints: 300,000,000 Total Sessions: 100,000,000 Total Users: 300,000,000 Total Reports: 1,000,000 Analytics Stats: ENABLED	Cloud License Manager Status: DISABLED SBC Media: 10,000 SBC Registrations: 10,000 SBC Transcoding: 10,000 SBC Signaling: 10,000 WEB RTC Sessions: 10,000 SIP Rec Streams: 10,000
Fixed License Pool Managed Devices: 10,000,000 SBC Sessions: 10,000,000 SBC Registrations: 10,000,000 SBC Transcoding: 10,000,000 SBC Signaling: 10,000,000 CB Users: 10,000,000 CB PBX Users: 10,000,000 CB Analog Devices: 10,000,000	Flex License Status: ENABLED Managed Devices: 100 SBC Media: 100 SBC Registrations: 100 SBC Transcoding: 100 SBC Signaling: 100 WEB RTC Sessions: 50 SIP Rec Streams: 50 SBC Shutdown On Failure (Days): 90
Endpoints Managed Endpoints: 300,000,000	MasterScope License Status: ENABLED
>1. <u>Load License</u> b.Back q.Quit to main Menu	

Figure 24-5: License Manager

Table 24-1: License Pool Parameters

License Type	License Parameter
Voice Quality	
Total Devices	The maximum number of Voice Quality monitored devices.
Total Endpoints	The maximum number of Voice Quality monitored endpoints.
Total Sessions	The maximum number of concurrent Voice Quality monitored SBC call sessions.
Total Users	The maximum number of Voice Quality monitored users supported by the SBC.

License Type	License Parameter			
	 A license value higher than 10 must be purchased to enable adding Skype for Business and Teams devices in the OVOC Web interface. For customers with existing Skype for Business devices defined in OVOC with 10 or fewer licenses , there are no changes; however, new Skype for Business devices cannot be added. 			
Total Reports	The maximum number of customized Voice Quality reports that can be generated in OVOC.			
	 Template reports can be generated without purchasing licenses; however, to generate customized reports, licenses must be purchased. These licenses can be allocated to tenant or system operators in the OVOC Web interface. For OVOC upgrades prior to version 7.8 releases: OVOC migrates old Scheduled reports as Custom reports even if there are insufficient licenses; however, the operator will not be able to add additional Custom reports even if they delete existing reports until the Custom Reports count is below the Total Reports license value. 			
analytics Stats	Enables the analytics API feature for retrieving Voice Quality data from Northbound Database access clients. By default disabled when OVOC Advanced package is enabled.			
Cloud License Ma	anager			
SBC Media	The maximum number of concurrent SBC media sessions.			
SBC Registrations	The maximum number of SIP endpoints that can register with the SBC devices.			
SBC Transcoding	The maximum number of SBC transcoding sessions.			
SBC Signaling	The maximum number of SBC signaling sessions.			
SIP Web RTC Sessions	The maximum number of SIP Web RTC Sessions.			
SIP Rec Streams	The maximum number of SIP Rec streams.			

License Type	License Parameter		
Flex License			
Managed Devices	The maximum number of devices that can be managed by the Flex license. Default-250		
SBC Media	The maximum number of concurrent SBC media sessions.		
SBC Registrations	The maximum number of SIP endpoints that can register with the SBC devices		
SBC Transcoding	The maximum number of SBC transcoding sessions.		
SBC Signaling	The maximum number of SBC signaling sessions.		
SIP Web RTC Sessions	The maximum number of SIP Web RTC Sessions.		
SIP Rec Streams	The maximum number of SIP Rec streams.		
SBC Shutdown on Failure (Days) Default:- 90 days	When an SBC device does not receive acknowledgment from the OVOC server that Usage reports have been received within the specified grace period, then service is shutdown for this SBC device. The SBC must then re-establish connection with the OVOC server.		
Fixed License Poo	bl		
SBC Managed Devices	The total number of SBC devices that can be managed by the Fixed License Pool.		
SBC Sessions	The maximum number of concurrent license SBC call sessions		
SBC Registrations	The number of SIP endpoints that can register with the SBC devices.		
SBC Transcoding	The maximum number of SBC transcoding sessions.		
SBC Signaling	The maximum number of SBC signaling sessions.		
CB Users	The maximum number of CloudBond 365 users		
CB PBX Users	The maximum number of PBX users. Currently not supported.		
CB Analog Devices	The maximum number of CB Analog devices. Currently not supported.		

License Type	License Parameter
CB Voicemail Accounts	The maximum number of CB Voicemail accounts. Currently not supported.
Endpoints	
Managed Endpoints	The maximum number of endpoints that can be managed by the Device Manager Pro.
Masterscope	
MasterScope License	Enables Single Sign-on to the MasterScope network equipment analysis application from the OVOC Web interface.

- **3.** To load a new license, choose option **1**.
- 4. Enter the license file path and name.
- 5. Restart the OVOC server application (see Start or Restart the Application on page 214).

analytics **API**

The analytics API enables access to selected data from the OVOC database for the purpose of integration into 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, Splunk and other analytics tools to generate customized dashboards, reports and other representative management data. This may be particularly useful during management reporting periods. The following data can be retrieved:

- 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 opened on the customer firewall, once the relevant feature key is enabled (see OVOC License on page 217) and in the procedure described below.

For more information, refer to OVOC Northbound Integration Guide.

> To manage the analytics API:

1. From the Application Maintenance menu, choose Analytics API, and then press Enter.

The 'License status' indicates whether the license feature is enabled and the 'Operational status' indicates whether this option is enabled.





- 2. Select option Enable DB Access to enable the Analytics API.
- **3.** You are prompted to continue, type **y** to confirm, and then press Enter. The server is restarted.

Once enabled, an option 'Change DB User Password' to change the default authentication password for the Analytics user connection appears in the menu. Enter the desired password and confirm.



Guacamole RDP Gateway

This option supports the opening of an RDP connection from the UMP 365 Device page via the Apache Guacamole VPN gateway to the Windows server residing the UMP application. This feature supports 10 simultaneous Remote access sessions where the Administrator can view the list of active sessions and close (stop) sessions manually.

- **To activate the Guacamole RDP gateway:**
- 1. From the Application menu, choose Guacamole RDP Gateway, and then press Enter.



Figure 24-7: Guacamole RDP Gateway

2. Select Option 1 to enable the RDP Gateway.

The gateway is built and installed.



Installing server application
Installing guacamole dependencies
lihnng-develOK
freerdp-devel OK
Extracting guacamole build OK
Building guacamole OK
Enabling guacamole service OK
Prenaving guaramole configurations
guacamole properties. Created
user-mapping.xml Greated
Starting guacamole OK
Installing tomcat
Extracting tomcat files OK
Configuring CATALINA HOME OK
Fnabling tomcat service OK
Conving tomost configuration OK
lastalling general elisit
Installing guadamole client OK
starting tomeat UK
Uperation was successful, press ENIER to continue

Figure 24-9: Enabled Guacamole RDP Gateway



3. Do one of the following:

- **Change password:** Select Option **2**, enter the current password, enter new password and confirm (default username *umpman*, default password: *umppass*)
- **Restart Tomcat:** Select Option **3** and confirm.
- **Restart Guacomole:** Select Option **4** and confirm.

VMware Tools

This option installs VMware Tools on the OVOC Server file system. This feature requires the premounting of the VMware installer CD-ROM on the Host machine. OVOC Server verifies the existence of the Tools package and then mounts the tool to OVOC Server file system.

> To install VMware tools:

- 1. On the VMware Host machine, select the relevant OVOC Virtual Machine.
- 2. Select the Right-click menu, choose Guest OS > Install VMware Tools.



The Completed Successfully indication is displayed in the Task pane:

🖻 Recent tasks							
Task ~	Target ~	Initiator ~	Queued ~	Started ~	Result 🔺 🗸 🗸	Completed v	~
Mount Tools Installer	wm-low-166	root	11/21/2023 14:35:00	11/21/2023 14:35:00	Completed successfully	11/21/2023 14:35:14	
Answer VM	wm-low-166	root	11/21/2023 14:35:14	11/21/2023 14:35:14	Completed successfully	11/21/2023 14:35:14	
Mount Tools Installer	wm-low-166	root	11/21/2023 14:43:46	11/21/2023 14:43:46	Completed successfully	11/21/2023 14:43:46	

3. Open Server Manager Application Maintenance menu, choose VMware Tools, and then press Enter.



4. Type **y** to confirm. The server is restarted.



5. Upon restart, OVOC verifies that the VMware Tools process is up; open the menu again and note that the Status is shown as **Installed**.



Shutdown the OVOC Server Machine

This section describes how to shut down the OVOC server machine.

- **To shut down the OVOC server machine:**
- **1.** From the Application Maintenance menu, choose **Shutdown the Machine**, and then press Enter.
- 2. Type y to confirm the shutdown, and then press Enter; the OVOC server machine is shutdown.

Reboot the OVOC Server Machine

This section describes how to reboot the OVOC server machine.

> To reboot the OVOC server machine:

- **1.** From the Application Maintenance menu, choose **Reboot the Machine**, and then press Enter.
- 2. Type **y** to confirm the reboot, and then press Enter; the OVOC server machine is rebooted.

25 Network Configuration

This section describes the networking options in the OVOC Server Manager.

To run the network configuration:

From the OVOC Server Manager root menu, choose Network Configuration, and then press Enter.

Figure 25-1: Network Configuration

OUOC Server 8.0	0.1110 Management						
Main Menu> Network Configurati	Main Menu> Network Configuration						
 >1. Server IP Address 2. Ethernet Interfaces 3. Ethernet Redundancy 4. DNS Client 5. NAT Configuration 6. Static Routes 7. Proxy Settings 8. SNMP Agent 9. Cloud Architecture 10. NFS q. Quit to main Menu 	(The server will be rebooted) (The server will be rebooted) (The server will be rebooted)						

This menu includes the following options:

- Server IP Address (the server will be rebooted) (Server IP Address on the next page)
- Ethernet Interfaces (the server will be rebooted) (Ethernet Interfaces on page 229)
- Ethernet Redundancy (the server will be rebooted) (Ethernet Redundancy on page 231)
- DNS Client (DNS Client on page 234)
- NAT (Configure OVOC Server with NAT IP Address per Interface on page 149)
- Static Routes (Static Routes on page 235)
- OVOC Proxy Settings (Proxy Settings on page 238)
- SNMP Agent (SNMP Agent on page 239)
- Cloud Architecture (Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153)
- NFS (NFS on page 242)

The following options are not applicable in Cloud deployments:

- ✓ Server IP Address
- Ethernet interfaces
- Ethernet redundancy
- The following options support IPv6:
 - Ethernet Redundancy
 - DNS Client
 - Static Routes

Server IP Address

This option enables you to update the OVOC server's IP address. This option also enables you to modify the OVOC server host name.

• When this operation has completed, the OVOC automatically reboots for the changes to take effect.

This option does not support IPv6 interfaces.

To change Server's IP address:

1. From the Network Configuration menu, choose Server IP Address, and then press Enter.

Figure 25-2: OVOC Server Manager – Change Server's IP Address



2. Configure IP configuration parameters as desired.

Each time you press Enter, the different IP configuration parameters of the OVOC server are displayed. These parameters include the Server Host Name, IP address, Subnet Mask, Network Address and Default Gateway.

3. Type y to confirm the changes, and then press Enter.



<u>File E</u> dit <u>S</u> etup C <u>o</u> ntrol <u>W</u> indow <u>H</u> elp	
Current OUOC Server IP Configuration (Server Network): Host Name: 0UOC-4 IP: 10.3.180.4 Subnet Mask: 0.0.0.0 Network Address: 0.0.0.0 Default Gateway: 10.3.0.1	
o you want to change the server's network configuration ? (y/n) y	
ostname [OVOC-4]: P Address [10.3.180.4]: Wonet Mask [0.0.0.0]: Wefault Gateway [10.3.0.1]:	
lew OVOC Server IP Configuration (Server Network): Hostname: OVOC-4 IP: 10.3.180.4 Subnet Mask: 0.0.0.0 Network Address: 0.0.0.0 Default Gateway: 10.3.0.1	

Upon confirmation, the OVOC automatically reboots for the changes to take effect.

Ethernet Interfaces

This section describes the maintenance actions for managing multiple ethernet interfaces.



 Each IPv4 interface can be configured for NAT and one of the IPv4 interfaces can be configured to work in the Cloud Architecture mode.

In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound network interfaces' to each one of the subnets. For Static Routes configuration, Static Routes on page 235.

> To configure Ethernet Interfaces:

1. From the Network Configuration menu, choose Ethernet Interfaces, and then press Enter.

Figure 25-4: OVOC Server Manager – Configure Ethernet Interfaces



2. Choose from one of the following options:

- Add Interface Adds a new interface to the OVOC server (Setting up Multiple Ethernet Interfaces on page 157).
- Remove Interface Removes an existing interface from the OVOC server (Remove Interface below).
- Modify Interface Modifies an existing interface from the OVOC server (Modify Interface below).

Remove Interface

This section describes how to remove an Ethernet Interface.

> To remove an existing interface:

1. From the Ethernet Interfaces menu, choose option **2**.



Remove Interface:		
Choose Interface:		
1) ens192 2) ens256		
3) ens224		
4) Quit		

- 2. Enter the number corresponding to the interface that you wish to remove.
- **3.** Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Modify Interface

This section describes how to modify an existing Ethernet Interface.

- > To modify an existing interface:
- 1. From the Ethernet Interfaces menu, choose option 3.



Figure 25-6: Modify Interface

- 2. Enter the number corresponding to the interface that you wish to modify.
- 3. Change the interface parameters as required.
- **4.** Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Ethernet Redundancy

This section describes how to configure Ethernet Redundancy. Physical Ethernet Interfaces Redundancy balances traffic between multiple network interfaces that are connected to the same IP link and provides a failover mechanism.



When the operation is finished, the OVOC server automatically reboots for the changes to take effect.

To configure Ethernet Redundancy:

1. From the Network Configuration menu, choose **Ethernet Redundancy** option, and then press Enter.

Figure 25-7: Ethernet Redundancy Configuration

	_
NAT: Not Defined Redundancy: Not Defined Main Menu> Network Configuration> Ethernet Redundancy	
Type: IP6 NAT: Not Defined Redundancy: Not Defined Interface: ens256 IP: 10.10.10.10 Type: IP4 NAT: Not Defined Redundancy: Not Defined Interface: ens224 IP: 5.5.5 Type: IP4 NAT: Not Defined Redundancy: Not Defined	
>1. <mark>Add Redundant Interface</mark> 2.Remove Redundant Interface 3.Modify Redundant Interface b.Back g.Quit to main Menu	

- 2. This menu includes the following options:
 - Add Redundant Interface (Add Redundant Interface below).
 - Remove Redundant Interface (Remove Ethernet Redundancy on the next page).
 - Modify Redundant Interface (Modify Redundant Interface on page 234).

Add Redundant Interface

This section describes how to add redundant interfaces.

- > To add a redundant interface:
- 1. From the Ethernet Redundancy menu, choose option 1, and then press Enter.



2. Choose the Master Interface for which to create a new redundant interface (for example, 'OVOC Client-Server Network'), and then press Enter.

Figure 25-9: Ethernet Redundancy Mode



- **3.** Enter the number corresponding to the interface in the selected network that you wish to make redundant (for example, 'eno', 'eno1', 'eno2'), and then press Enter.
- **4.** Enter the number corresponding to the desired Ethernet Redundancy Mode (for example 'active-backup'), and then press Enter.





5. Type **y** to confirm the changes; the OVOC server automatically reboots for changes to take effect.

Remove Ethernet Redundancy

Remove a redundant interface under the following circumstances:

- You have configured at least one redundant Ethernet interface (Remove Ethernet Redundancy above).
- Your default router can respond to a 'ping' command, due to a heartbeat procedure between interfaces and the default router (to verify activity).

> To remove the Ethernet Redundancy interface:

- 1. From the Ethernet Redundancy menu, choose option 2, and then press Enter.
- 2. Choose the Master Redundant Interface, and then press Enter.
- **3.** Enter the number corresponding to the interface in the selected network that you wish to make remove (for example, 'eno', 'eno1', 'eno2').
- **4.** Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Modify Redundant Interface

This section describes how to modify a redundant interface.

- > To modify redundant interface and change redundancy settings:
- 1. From the Ethernet Redundancy, choose option **3**, and then press Enter.
- 2. Choose the Master Redundant Interface to modify, and then press Enter.
- **3.** Enter the number corresponding to the interface in the selected network that you wish to make modify (for example, 'eno', 'eno1', 'eno2'), and then press Enter..
- **4.** Type **y** to confirm the changes, and then press Enter; the OVOC server automatically reboots for the changes to take effect.

DNS Client

Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

This option enables you to configure the client side (Resolver). If there is no existing DNS configuration, the option **Configure DNS** is displayed. If already configured, the option **Modify DNS** is displayed.

> To Configure the DNS Client:

1. From the Network Configuration menu, choose DNS Client, press Enter, in the sub-menu, choose **Configure DNS**, and then press Enter.

Figure 25-11: DNS Setup



- 2. Specify the location domain. Type **y** to specify the local domain name or type **n**, and then press Enter.
- **3.** Specify a search list; type **y** to specify a list of domains (use a comma delimiter to separate search entries in the list) or type **n**, and then press Enter.
- 4. Specify DNS IP addresses 1, 2 and 3, and then press Enter.
- 5. Type **y** to confirm your configuration; the new configuration is displayed.

Static Routes

This option enables you to add or remove static route rules. Static routes are usually only used in conjunction with /etc/defaultrouter. Static routes may be required for network topology, where you don't want to traverse your default Gateway/Router. In this case, you will probably wish to make the routes permanent by adding the static routing rules. Static routes can be added with both IPv4 and IPv6 addresses.

To configure static routes:

1. From the Network Configuration menu, choose Static Routes, and then press Enter.

	•	•				
	OUOC Server 8.	2.191 Management				
Main Menu> Network Configuration> Static Routes						
Static	Routes Configur	ation				
Kernel IP rout	ing table					
Destination 0.0.0.0 169.254.0.0 172.17.118.0	Gateway 172.17.118.1 0.0.0.0 0.0.0.0 ution table	Genmask Ø.0.0.0 255.255.0.0 255.255.255.0	Flags UG U U	MSS Window 00 00 00	irtt Iface Ø eno1 Ø eno1 Ø eno1	
Nernel Irvo ro Destination	uting table	Next Hon		Elac Met	Raf Usa If	
fe80::/64 ff00::/8 >1.mn 2.Rem b.Bac q.Qui	Static Route ove Static Route k t to main Menu			U 256 U 256 U 256	0 0 eno1 2 5 eno1	

Figure 25-12: Routing Table and Menu

- 2. From the Static Routes configuration screen, choose one of the following options:
 - Add a Static Route
 - Remove a Static Route
- > To add a static route:
- **1.** From the Static Routes menu, choose option **1**, and then press Enter.





2. Enter the number corresponding to the desired interface, and then press Enter.

Figure 25-14: Enter Router (next hop)



3. Enter the Router IP address, and then press Enter.

Figure 25-15: Destination Network Address



4. Enter the Destination Network Address in specified format, and then press Enter.

Figure 25-16: Confirm New IP Address

Adding static route... Press 'q' and 'Enter' to exit Choose Interface: 1) Interface name: eno1 IP address: 172.17.118.146 q) Quit :1 Enter router (next hop) IP: 172.17.118.2 Destination Network Address : Please specify value in format ip4/1..32 or ip6[/1..128]: 10.10.10.1/24 Are you sure that you want to continue? (y/n/q) 5. Enter y to confirm the new IP address, and then press Enter.

> To remove a static route:

1. From the Static Routes menu, choose option **2**, and then press Enter.



Choose Static Route 1) 0.0.0.0 via 172.17.140.1 netmask 0.0.0.0 dev ens160 2) 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens256 11) fe80::/64 dev ens224 13) fe80::/64 dev ens224 13) fe80::/64 dev ens192 14) fe80::/64 dev ens192 15) ff00::/8 dev ens256 14) fe80::/64 dev ens224 15) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19) Quit :	Choose Static Route 1) 0.0.0.0 via 172.17.140.1 netmask 0.0.0.0 dev ens160 2) 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens256 11) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens192 15) ff00::/8 dev ens256 16) ff00::/8 dev ens256 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	Remove Static Route:
<pre>1) 0.0.0 via 172.17.140.1 netmask 0.0.0.0 dev ens160 2) 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::46 dev ens192 10) 2172:17::464 dev ens256 11) fe80::/64 dev ens256 12) fe80::/64 dev ens256 13) fe80::/64 dev ens192 16) ff00::/8 dev ens256 17) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19 y quit 10</pre>	<pre>1) 0.0.0 via 172.17.140.1 netmask 0.0.0.0 dev ens160 2) 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::40 ev ens192 10) 2172:17::40 dev ens192 12) fe80::/64 dev ens256 13) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens256 17) ff00::/8 dev ens256 18) ff00::/8 dev ens26 19) Quit :</pre>	Choose Static Boute
<pre>1/ 9.8.8.8 014 172.17.149.1 netmask 9.8.8.8 010 ensite 2) 5.5.0 netmask 255.255.0 dev ens224 3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens256 11) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens192 15) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19 y quit 19 Quit</pre>	<pre>17 9.9.9.9.9 014 172.17.149.1 metmask 9.9.9.9 dev ensite 2) 5.5.9 netmask 255.255.0 dev ens224 3) 10.10.0 netmask 255.255.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens256 177 ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	the G G G using 172 17 140 t patroak G G G G day anal(0)
<pre>27 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0 netmask 255.255.0.0 dev ens26 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens26 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens266 14) fe80::/64 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19) quit :</pre>	<pre>2) 5.5.5.0 netmask 255.255.255.0 dev ens224 3) 10.10.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens226 14) fe80::/64 dev ens192 16) ff00::/8 dev ens192 16) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	
<pre>3) 10.10.0.0 netmask 255.255.0.0 dev ens26 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens192 11) fe80::/64 dev ens226 11) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens192 15) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19) quit</pre>	<pre>3) 10.10.0.0 netmask 255.255.0.0 dev ens256 4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens192 16) ff00::/8 dev ens192 16) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	
<pre>4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.0.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::40 dev ens192 12) fe80::/64 dev ens192 12) fe80::/64 dev ens226 14) fe80::/64 dev ens256 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens256</pre>	<pre>4) 169.254.0.0 netmask 255.255.0.0 dev ens160 5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	3) 10.10.0.0 netmask 255.255.0.0 dev ens256
<pre>5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::/64 dev ens192 12) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19) Quit : ■</pre>	5) 169.254.0.0 netmask 255.255.0.0 dev ens192 6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens224 13) fe80::/64 dev ens266 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	42 169.254.0.0 netmask 255.255.0.0 dev ens160
<pre>6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17::40::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens256 18) ff00::/8 dev ens256 19) Quit : ■</pre>	6) 169.254.0.0 netmask 255.255.0.0 dev ens224 7) 169.254.0.0 netmask 255.255.0.0 dev ens256 8) 172.17.140.0 netmask 255.255.255.0 dev ens160 9) 2172:17::/64 dev ens192 10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	5) 169.254.0.0 netmask 255.255.0.0 dev ens192
<pre>7> 169.254.0.0 netmask 255.255.0.0 dev ens256 8> 172.17.140.0 netmask 255.255.255.0 dev ens160 9> 2172:17::/64 dev ens192 10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	<pre>7> 169.254.0.0 netmask 255.255.0.0 dev ens256 8> 172.17.140.0 netmask 255.255.255.0 dev ens160 9> 2172:17::/64 dev ens192 10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :</pre>	6) 169.254.0.0 netmask 255.255.0.0 dev ens224
<pre>8> 172.17.140.0 netmask 255.255.255.0 dev ens160 9> 2172:17::/64 dev ens192 10> 2172:17:140::/64 dev ens256 11> fe80::/64 dev ens192 12> fe80::/64 dev ens224 13> fe80::/64 dev ens160 15> ff00::/8 dev ens192 16> ff00::/8 dev ens224 17> ff00::/8 dev ens256 18> ff00::/8 dev ens160 19> Quit :</pre>	<pre>8> 172.17.140.0 netmask 255.255.255.0 dev ens160 9> 2172:17::/64 dev ens192 10> 2172:17:140::/64 dev ens256 11> fe80::/64 dev ens224 13> fe80::/64 dev ens256 14> fe80::/64 dev ens160 15> ff00::/8 dev ens192 16> ff00::/8 dev ens224 17> ff00::/8 dev ens256 18> ff00::/8 dev ens160 19> Quit :</pre>	7> 169.254.0.0 netmask 255.255.0.0 dev ens256
<pre>9> 2172:17::/64 dev ens192 10> 2172:17:140::/64 dev ens256 11> fe80::/64 dev ens192 12> fe80::/64 dev ens224 13> fe80::/64 dev ens256 14> fe80::/64 dev ens160 15> ff00::/8 dev ens192 16> ff00::/8 dev ens224 17> ff00::/8 dev ens256 18> ff00::/8 dev ens160 19> Quit : ■</pre>	<pre>9> 2172:17::/64 dev ens192 10> 2172:17:140::/64 dev ens256 11> fe80::/64 dev ens192 12> fe80::/64 dev ens224 13> fe80::/64 dev ens256 14> fe80::/64 dev ens160 15> ff00::/8 dev ens192 16> ff00::/8 dev ens224 17> ff00::/8 dev ens256 18> ff00::/8 dev ens160 19> Quit :</pre>	8) 172.17.140.0 netmask 255.255.255.0 dev ens160
10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	10) 2172:17:140::/64 dev ens256 11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	9> 2172:17::/64 dev ens192
11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit : ■	11) fe80::/64 dev ens192 12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	10> 2172:17:140::/64 dev ens256
12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	12) fe80::/64 dev ens224 13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit	11) fe80::/64 dev ens192
13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	13) fe80::/64 dev ens256 14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	12) fe80::/64 dev ens224
14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	14) fe80::/64 dev ens160 15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	13) fe80::/64 dev ens256
15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	15) ff00::/8 dev ens192 16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	14) fe80::/64 dev ens160
16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	16) ff00::/8 dev ens224 17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	15) ff00::/8 dev ens192
17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	17) ff00::/8 dev ens256 18) ff00::/8 dev ens160 19) Quit :	16) ff00::/8 dev ens224
18) ff00::/8 dev ens160 19) Quit :	18) ff00::/8 dev ens160 19) Quit :	17) ff00::/8 dev ens256
19) Quit	19) Quit	18) $ff00::/8$ dev ens160
		19) Auit

2. Enter the number of the static route that you wish to remove, and then press Enter.

Proxy Settings

This option enables the configuration of a proxy server connection for the sole purpose of connecting between OVOC and AudioCodes Cloud License Manager (CLM). The connection is configured over HTTPS/HTTP/FTP.

- > To configure proxy settings:
- 1. From the Network Configuration menu, choose **Proxy Settings**, and then press Enter.
- 2. Select **Configure Proxy**, type y to confirm, and then press Enter.
- **3.** Enter the FQDN (without underscores), IP address and port of the proxy server, and then press Enter.
- 4. Enter the Proxy server username, and then press Enter.
- 5. Enter the Proxy server password, and then press Enter.



The following special characters are allowed in the password : _ , #, *, =, +, ?, ^

6. Enter "No Proxy" addresses (a list of IP addresses for connecting directly from OVOC and not through a proxy server), and then press Enter.

Figure 25-18: Proxy Settings



SNMP Agent

The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP). This agent serves OVOC, NMS, or higher-level management system synchronization. This menu includes the following options:

- Stop and start the SNMP agent
- Configure the SNMP agent including:
 - Configure the SNMP agent listening port (SNMP Agent Listening Port on the next page)
 - Configure the northbound destination for linux system traps forwarding (Linux System Trap Forwarding Configuration on page 241).
 - Configure the SNMPv3 Engine ID (Server SNMPv3 Engine ID on page 241)
- **To configure SNMP Agent:**
- 1. From the Network Configuration menu, choose **SNMP** Agent, and then press Enter.

Figure 25-19: SNMP Agent

Main Menu> Network Configuration> SNMP Agent
SNMP Agent Status: DOWN >1.Configure SNMP Agent 2.Start SNMP Agent b.Back q.Quit to main Menu

The SNMP Agent status is displayed.

- To start the SNMP Agent:
- Choose option 2
- ➤ To configure SNMP Agent:
- 1. Choose option 1, and then press Enter.

Figure 25-20: Configure SNMP Agent

Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent	
>1. SMTP Agent Listening Port 2.Linux System Traps Forwarding Configuration 3.SNMPv3 Engine ID b.Back q.Quit to main Menu	

SNMP Agent Listening Port

The SNMP Agent Listening port is a bi-directional UDP port used by the SNMP agent for listening for traps from managed devices. You can change this listening port according to your network traffic management setup.

> To configure SNMP Agent Listening port

1. Choose option **1**, and then press Enter.





2. Configure the desired listening port (default 161), and then press Enter.

Linux System Trap Forwarding Configuration

This option enables you to configure the northbound interface for forwarding Linux system traps.

- > To configure the Linux System Traps Forwarding Configuration:
- 1. Choose option 2 ,and then press Enter.
- 2. Configure the NMS IP address and then press Enter.
- 3. Enter the Community string and then press Enter; the new configuration is applied.

Server SNMPv3 Engine ID

The OVOC server Engine ID is used by the SNMPv3 protocol when alarms are forwarded from the OVOC to an NMS. By default, the OVOC server SNMPv3 Engine ID is automatically created from the OVOC server IP address. This option enables the user to customize the OVOC server Engine ID according to their NMS configuration.

To configure the SNMPv3 Engine ID:

1. From the Network Configuration menu, choose SNMPv3 Engine ID, and then press Enter.

Figure 25-22: OVOC Server Manager – Configure SNMPv3 Engine ID


- Enter '12' separate bytes ranges of the Engine ID (each valid range from between -128 to 127). In each case, press Enter to confirm the current value insertion and then proceed to the next one.
- 3. When all Engine ID bytes are provided, type **y** to confirm the configuration, and then press Enter. To return to the root menu of the OVOC Server Manager, type **q**, and then press Enter.

s	SNMPv3 Engine ID Configuration
s	Server's SNMPv3 Engine ID (0 in all values return to default configuration)
E	Byte[0] (valid range -128 127):21
E	Byte[1] (valid range -128 127):23
E	<pre>3yte[2] (valid range -128 127):2</pre>
E	Byte[3] (valid range -128 127):5
E	Byte[4] (valid range -128 127):3
E	Byte[5] (valid range -128 127):78
E	Byte[6] (valid range -128 127):-17
E	3yte[7] (valid range -128 127):-56
E	Byte[8] (valid range -128 127):121
E	Byte[9] (valid range -128 127):117
E	3yte[10] (valid range -128 127):-111
E	Byte[11] (valid range -128 127):127
Engine I	ID: 21.23.2.5.3.781756.121.117111.127
Are you s	sure that you want to continue? (y/n/q)
1	

NFS

This section describes how to configure Network File System (NFS). This installs the NFS-utils package which enables OVOC to access an external storage system via NFS.

> To enable NFS Utils package:

1. From the Network Configuration menu, choose NFS, and then press Enter.



OVOC Server 8.0.1091 Management
Main Menu> Network Configuration> NFS
NFS Utils: DISABLED
>1.Enable NPS Utils b.Back
g.Quit to main Menu

2. Select Enable NFS Utils, and then press Enter. You are prompted to enable the package, enter Y, and then press Enter.

26 NTP & Clock Settings

This chapter describes how to configure the NTP clock source and the OVOC server system clock.

OVOC can be configured as an NTP server using either an IPv4 or IPv6 interface.

1. From the OVOC server Manager menu, choose **Date & Time**, and then press Enter.



This menu includes the following options:

- NTP (NTP below)
- Timezone Settings (Timezone Settings on page 247)
- Date & Time Settings (Date and Time Settings on page 248)

NTP

Network Time Protocol (NTP) is used to synchronize the time and date of the OVOC server and all its components with connected devices in the IP network. This option enables you to do the following:

- Configure the OVOC server to obtain its clock from an external NTP clock source. Other devices that are connected to the OVOC server in the IP network can synchronize with this clock source. These devices may be any device containing an NTP server or client.
- Configure the OVOC server as the NTP server source (Stand-alone NTP server) and allow other clients and subnets in the IP network to synchronize to this source.

• It is recommended to configure the OVOC server to synchronize with an external clock source because the OVOC server clock is less precise than other NTP devices. For example, for Cloud deployments, it is recommended to configure the Microsoft Azure or Amazon AWS platforms as the external clock source.

- Configure the same NTP server IP address/domain name and other relevant settings on both the OVOC server and on the AudioCodes device (Setup > Administration > Time & Date).
- When connecting OVOC to Skype For Business, ensure that the same NTP server clock source is configured on both ends.

To configure NTP:

1. From the Date & Time menu, choose NTP, and then press Enter.

OUOC Server 8.2.2233 Management											
Main Menu> Date & Time> NTP											
Current NTP status: ON Allow/Restrict access to NTP clients: Allow											
remote	refid	st t whe	n poll	reach	delay	offset	jitter				
*time.cloudflare +176-230-251-106 >1.conf 2.Stop M 3.Restri 4.Activa 5.Add au 6.Remove b.Back q.Quit t	10.149.8.72 192.168.221.15 TTP (Server ict access to N ict aDOS protec ithorized subne authorized subne authorized su	3 u 14 4 u 84 (Server b will be r TP clients tion t to sync bnet from	4 1024 1 1024 ill be estarte by NTP NTP ru]	377 257 restari	2.154 3.087 ted)	-0.296	13.253 1.861				

Figure 26-2: OVOC Server Manager - Configure NTP

- 2. From the NTP menu, choose **Configure NTP**, and then press Enter.
- **3.** At the prompt, do one of the following:
 - Type **y** for the OVOC server to act as both the NTP server and NTP client, and then press Enter. Enter the IP address or domain name of the NTP servers to serve as the clock reference source for the NTP client (Up to four NTP servers can be configured), and then press Enter. The NTP process daemon starts and the NTP status information is displayed on the screen.

Maın Menu> Date a	& Time> NTP						
Current N Allow/Res	TP status: ON trict access to	NTP clients: Allow					
remote	refid	st t when poll reach	delay	offset	jitter		
+aclads05.corp.a *aclads01.corp.a >1.Config 2.Stop N 3.Restric 4.Activat	52.148.114.188 10.1.1.10 Ure NIF TP ct access to NTI te DDoS protect	4 u 825 1024 377 5 u 272 1024 377 P clients	4.789 4.639	7.527 14.480	5.710 21.590		
5.Add au 6.Remove b.Back q.Quit to	thorized subnet authorized subn o main Menu	to sync by NTP net from NTP rules					

Figure 26-3: External Clock Source

• Type **n** for the OVOC server to function as a Stand-alone NTP server, and then press Enter. The NTP process daemon starts and the NTP status information is displayed on the screen.

Main Menu> Date & Time> NTP										
Current M Allow/Res	MTP status: ON strict access t	o NTP clients:	Allow							
remote	refid	st t when pol	l reach	delay	offset	jitter				
*LOCAL(0) >1. Config 2. Stop M 3. Restri 4. Activa 5. Add au 6. Remove b. Back q. Quit t	.LOCL. JUTE NTF ITF ct access to N tte DDOS protect thorized subne e authorized subne to main Menu	13] 1 G	9 Pules	0.000	0.000	0.000				

Figure 26-4: Local Clock Source

See also:

Stopping and Starting the NTP Server on the next page

- Restrict Access to NTP Clients below
- Activate DDoS Protection below
- Authorizing Subnets to Connect to OVOC NTP below

Stopping and Starting the NTP Server

This section describes how to stop and start the NTP server.

To start NTP services:

- 1. From the NTP menu, choose option 2, and then press Enter.
- 2. Choose one of the following options:
 - **Stop NTP**, and then press Enter.
 - Start NTP, and then press Enter.

The NTP daemon process starts; when the process completes, you return to the NTP menu.

Restrict Access to NTP Clients

When the OVOC server is configured as a Stand-alone NTP server, you configure NTP rules to authorize which clients can synchronize with the OVOC NTP clock.

> To allow access to NTP clients:

From the NTP menu, choose option **Restrict Access to NTP Clients** to allow or restrict access to NTP clients, and then press Enter; the screen is updated accordingly.

Activate DDoS Protection

This option enables you to activate DDos protection for preventing Distributed Denial of Service attacks on the OVOC server. For example, attacks resulting from security scans. This is relevant for both when the OVOC server is configured as a Stand-alone clock source and when an external clock source is used.

To activate DDoS protection:

From the NTP menu, select Activate/Deactivate DDoS Protection, and then press Enter.

Authorizing Subnets to Connect to OVOC NTP

When the OVOC server is configured as a Stand-alone NTP server, you can configure NTP rules to authorize which subnets can synchronize with the OVOC NTP clock.

> To authorize subnets:

From the NTP menu, select Add Authorized Subnet to Sync by NTP, and then press Enter.

> To remove authorized subnet from NTP rules:

From the NTP menu, select **Remove Subnet from NTP Rules**, and then press Enter.

Timezone Settings

This option enables you to change the timezone of the OVOC server.



The Apache server is automatically restarted after the timezone changes are confirmed.

To change the system timezone:

- 1. From the Date & Time menu, choose **Time Zone Settings**, and then press Enter.
- 2. Enter the required time zone.
- **3.** Type **y** to confirm the changes; the OVOC server restarts the Apache server for the changes to take effect.

Date and Time Settings

You can set the date and time for the OVOC server system clock.

- > To configure data and time:
- 1. From the Date & Time menu, select Date & Time Settings, and then press Enter.

Figure 27-1: New Server Time



2. Enter the new time as shown in the following example:

mmddHHMMyyyy.SS : month(08),day(16),Hour(16),Minute(08),year(2007),"." Second.

28 Security

The OVOC Management security options enable you to perform security actions, such as configuring the SSH Server Configuration Manager, and user's administration.

To configure security settings:

From the OVOC Server Manager root menu, choose **Security**, and then press Enter.

Figure 28-1: Security Settings

Main Menu> Security
XI.Add OVOC User
2.SSH
3.Postgres DB Password (OUOC Server will be stopped)
4.Cassandra DB Password (OUOC Server will be stopped)
5.Elasticsearch DB Password (OUOC Server will be stopped)
6.08 Users Passwords
7.HTTP Security Settings
8.File Integrity Checker
9.Software Integrity Checker (AIDE) and Prelinking
10.USB Storage
11.Network options
12.Audit Agent Options
13 Server Certificates Undate
14.000C Unice Quality Package - SBC Communication
r Quit to main Menu
J. Jazo os mazn nona

This menu includes:

- Add OVOC User (Add OVOC User on the next page)
- SSH (SSH on the next page)
- PostgreSQL DB Password (PostgreSQL DB Password on page 257)
- Cassandra Password (Cassandra Password on page 259)
- Elasticsearch DB Password (Elastic Search DB Password on page 260)
- OS Users Password (OS Users Passwords on page 260)
- HTTP Security Settings (HTTPS SSL TLS Security on page 267)
 - Server Certificate Update (Server Certificates Update on page 268)
- File Integrity Checker (File Integrity Checker on page 264)
- Software Integrity Checker (AIDE) and Pre-linking (Software Integrity Checker (AIDE) and Pre-linking on page 264)
- USB Storage (USB Storage on page 265)
- Network options (Network Options on page 265)
- Audit Agent Options (Auditd Agent Options on page 266)
- OVOC Voice Quality Package (OVOC Voice Quality Package SBC Communication on page 266)

Add OVOC User

This option enables you to add a new administrator user to the OVOC server database. This user can then log into the OVOC client. This option is advised to use for the operator's definition only in cases where all the OVOC application users are blocked and there is no way to perform an application login.

To add an OVOC user:

- 1. From the Security menu, choose Add OVOC User, and then press Enter.
- 2. Enter the name of the user you wish to add, and then press Enter.
- 3. Enter a password for the user, and then press Enter.
- 4. Type **y** to confirm your changes, and then press Enter.



Note and retain these passwords for future access.

SSH

This section describes how to configure the OVOC server SSH connection properties using the SSH Server Configuration Manager.

► To configure SSH:

1. From the Security menu, choose **SSH**, and then press Enter.

Figure 28-2: SSH Configuration



This menu includes the following options:

- Configure SSH Log Level (SSH Log Level on the next page).
- Configure SSH Banner (SSH Banner on the next page).
- Configure SSH on Ethernet Interfaces (SSH on Ethernet Interfaces on page 252).

- Disable SSH Password Authentication (Enable/Disable SSH Password Authentication on page 254).
- Enable SSH Ignore User Known Hosts Parameter (Enable SSH Ignore User Known Hosts Parameter on page 254).
- Configure SSH Allowed Hosts (SSH Allowed Hosts on page 255).

SSH Log Level

You can configure the log level of the SSH daemon server. The log files are found at the location '/var/log/secure' (older records are stored in secure.1, secure.2 etc.).

➤ To configure the SSH Log Level:

1. From the SSH menu, choose option **1**, and then press Enter.

Figure 28-3: SSH Log Level Manager

Main Menu> Security> SSH> Configure SSH Log Level
LogLevel DEFAULT Note: Changing LogLevel will restart SSH >1. 2.FATAL 3.ERROR 4.INFO 5.UERBOSE 6.DEBUG
7.DEBUG1 8.DEBUG2 9.DEBUG3 10.DEFAULT b.Back q.Quit to main Menu

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press Enter.

The SSH daemon restarts automatically. The Log Level status is updated on the screen to the configured value.

SSH Banner

The SSH Banner displays a pre-defined text message each time the user connects to the OVOC server using an SSH connection. You can customize this message. By default this option is disabled.

➤ To configure the SSH banner:

1. From the SSH menu, choose option 2, and then press Enter.



Figure 28-4: SSH Banner Manager

- 2. Edit a '/etc/issue' file with the desired text.
- 3. Choose option 1 to enable or disable the SSH banner, and then press Enter.

Whenever you change the banner state, SSH is restarted. The 'Current Banner State' is displayed in the screen.

SSH on Ethernet Interfaces

You can allow or deny SSH access separately for each network interface enabled on the OVOC server.

To configure SSH on Ethernet interfaces:

From the SSH menu, choose option **3**, and then press Enter.

```
Figure 28-5: Configure SSH on Ethernet Interfaces
```

Main Menu> Security> SSH> Configure SSH on Ethernet Interf	aces										
Ethernet Interfaces — SSH Manager: SSH Listener Statuses: ALL — SSH enabled on all the Interfaces Yes — SSH enabled on specific Interface No — SSH disabled on specific Interface											
Interface SSH Listener Status IP Address eth0 ALL 10.3.180.7 >1.Add SSH to All Ethernet Interface 2.Add SSH to Ethernet Interface 3.Remove SSH from Ethernet Interface b.Back q.Quit to main Menu	Host Name G8-Linux?										

This menu includes the following options:

- Add SSH to All Ethernet Interfaces on the next page
- Add SSH to Ethernet Interface on the next page
- Remove SSH from Ethernet Interface on the next page

Add SSH to All Ethernet Interfaces

This option enables SSH access for all network interfaces currently enabled on the OVOC server.

> To add SSH to All Ethernet Interfaces:

From the Configure SSH on Ethernet Interfaces menu, choose option 1, and then press Enter.

The SSH daemon restarts automatically to update this configuration action. The column 'SSH Listener Status' displays ALL for all interfaces.

Add SSH to Ethernet Interface

This option enables you to allow SSH access separately for each network interface.

To add SSH to Ethernet Interfaces:

1. From the Configure SSH on Ethernet Interfaces menu, choose option 2, and then press Enter.

After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.

2. Enter the appropriate interface number, and then press Enter.

The SSH daemon restarts automatically to update this configuration action. The column 'SSH Listener Status' displays 'YES' for the configured interface.

Remove SSH from Ethernet Interface

This option enables you to deny SSH access separately for each network interface.

To deny SSH from a specific Ethernet Interface:

1. From the Configure SSH on Ethernet Interfaces menu, choose option **3**, and then press Enter.

All the interfaces to which SSH access is currently enabled are displayed.

2. Enter the desired interface number, and then press Enter.

The SSH daemon restarts automatically to update this configuration action. The column 'SSH Listener Status' displays 'No' for the denied interface.



If you attempt to deny SSH access for the only enabled interface, a message is displayed informing you that such an action is not allowed.

Enable/Disable SSH Password Authentication

This option enables you to disable the username/password authentication method for all network interfaces enabled on the OVOC server.

- > To disable SSH Password Authentication:
- 1. From the SSH menu, choose option 4, and then press Enter.

```
Figure 28-6: Disable Password Authentication
```

Disable SSH Password	Authentication:
Current SSH Password	Authentication is ENABLED.
Note: Changing Passwo Are you sure you want	ord Authentication mode will restart SSH t to Disable SSH Password Authentication?(y/n)

2. Type y to disable SSH password authentication or n to enable, and then press Enter.

The SSH daemon restarts automatically to update this configuration action.

Once you perform this action, you cannot reconnect to the OVOC server using User/Password authentication. Therefore, before you disable this authentication method, ensure that you provision an alternative SSH connection method. For example, using an RSA keys pair. For detailed instructions on how to perform such an action, see www.junauza.com or search the internet for an alternative method.

Enable SSH Ignore User Known Hosts Parameter

This option enables you to disable the use of the '\$HOME/.ssh/known_host' file with stored remote servers fingerprints.

- > To enable SSH Ignore User Know Hosts parameter:
- 1. From the SSH menu, choose option 5, and then press Enter.





2. Type y to change this parameter value to either 'YES' or 'NO' or type n to leave as is, and then press Enter.

SSH Allowed Hosts

This option enables you to define which hosts are allowed to connect to the OVOC server through SSH.

To Configure SSH Allowed Hosts:

From the SSH menu, choose option **6**, and then press Enter.

Figure 28-8: Configure SSH Allowed Hosts



This menu includes the following options:

- Allow ALL Hosts (Allow ALL Hosts below).
- Deny ALL Hosts (Deny ALL Hosts below).
- Add Host/Subnet to Allowed Hosts (Add Hosts to Allowed Hosts on the next page).
- Remove Host/Subnet from Allowed Hosts (Remove Host/Subnet from Allowed Hosts on page 257).

Allow ALL Hosts

This option enables all remote hosts to access this OVOC server through the SSH connection (default).

> To allow ALL Hosts:

- **1.** From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter.
- 2. Type y to confirm, and then press Enter.

The appropriate status is displayed in the screen.

Deny ALL Hosts

This option enables you to deny all remote hosts access to this OVOC server through the SSH connection.

➤ To deny all remote hosts access:

- 1. From the Configure SSH Allowed Hosts menu, choose option 2, and then press Enter.
- 2. Type y to confirm, and then press Enter.

The appropriate status is displayed in the screen.



When this action is performed, the OVOC server is disconnected and you cannot reconnect to the OVOC server through SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM connection.

Add Hosts to Allowed Hosts

This option enables you to allow different SSH access methods to different remote hosts. You can provide the desired remote host IP, subnet or host name in order to connect to the OVOC server through SSH.

To add Hosts to Allowed Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **3**, and then press Enter.

Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allow ed Hosts >1.Add IP Address (x.x.x.x) 2.Add Subnet (n.n.n.n/m.m.m.m - network/netmask) 3.Add Host Name (without "/" or "," characters) b.Back g.Quit to main Menu

Figure 28-9: Add Host/Subnet to Allowed Hosts

- 2. Choose the desired option, and then press Enter.
- 3. Enter the desired IP address, subnet or host name, and then press Enter.

When adding a Host Name, ensure the following:

- Verify your remote host name appears in the DNS server database and your OVOC server has an access to the DNS server.
- Provide the host name of the desired network interface defined in "/etc/hosts" file.
- 4. Type y to confirm the entry, and then press Enter again.

If the entry is already included in the list of allowed hosts, an appropriate notification is displayed.

When the allowed hosts entry has been successfully added, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:



Figure 28-10: Add Host/Subnet to Allowed Hosts-Configured Host

Remove Host/Subnet from Allowed Hosts

If you have already configured a list of allowed hosts IP addresses, you can then remove one or more of these host addresses from the list.

- To remove an existing allowed host's IP address:
- 1. From the Configure SSH Allowed Hosts menu, choose option 1, and then press Enter.
- 2. Choose the desired entry to remove from the Allowed Hosts list, i.e. to deny access to the OVOC server through SSH connection, and then press Enter again.
- 3. Type **y** to confirm the entry, and then press Enter again.

When the allowed hosts entry has been successfully removed, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:



When you remove either the only existing IP address, Subnet or Host Name in the Allowed Hosts in the Allowed Hosts list, the configuration is automatically set to the default state "Allow All Hosts".

PostgreSQL DB Password

This option enables you to change the default PostgreSQL Database password "pass_1234". The OVOC server shuts down automatically before changing the PostgreSQL Database password.

- When upgrading to Version 8.2, the PostGreSQL database password is restored to default.
 - It is not possible to restore the database password or to access the database without it.

To change the DB Password:

1. From the Security menu, choose **PostgreSQL DB Password**, and then press Enter.

Figure 28-11: Postgre DB Password

Would you like to change Postgres DB password? (y/n) 📕



2. Type y to change the password.

Figure 28-12: Current Password

3. Enter the current password.

Figure 28-13: New Password

Would	you	like	to	change	Postgres	DB	passw	ord?	(y/n)	У			
***** Post *****	xxxx gres xxxx	xxxxx Chang xxxxx	xxxx ge p xxxx	XXXXXXX ASSWOP XXXXXX	××××××××× d Script ×××××××××	xxx sta xxx	×××××× rt ××××××		******	***			
User EMSAD Curre ***** The p two and t chara ds. New P	name: MIN nt Pa asswo lower wo uj cters	asswo: * ord s: rcase operc. s, and ord:	rd: houl ase d sh	d be a charac ould d	t least 1 ters, two iffer by	5 c. sp mor	haract ecial e thar	chara 1 cl	long, d acters haracte	 contain a (_ # * er from (at least = + ? ^ the previ	two) ious	digits, passwor

- 4. Enter the new password, which should be at least 15 characters long, contain at least two digits, two lowercase and two uppercase characters, two punctuation characters and should differ by one character from the previous passwords.
 - The OVOC server is rebooted when you change the PostgreSQL Database password.
 - Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the OVOC PostgreSQL Database without them.
- 5. After validation, a message is displayed indicating that the password was changed successfully.

Cassandra Password

This section describes how to change the Cassandra password.

- **To change the Cassandra Password:**
- From the Security menu, choose Cassandra DB Password, and then press Enter; the OVOC server is rebooted.
- 2. Press Enter until the New Password prompt is displayed.

Figure 28-14: Change Cassandra Password



3. Enter the new password and confirm.

Elastic Search DB Password

This option lets you change the Elastic Search DB password.

To change the Elastic Search DB Password:

- 1. From the Security menu, choose Elastic Search DB password, and then press Enter; the OVOC server is rebooted.
- 2. Press Enter until the New Password prompt is displayed.



3. Enter the new password and confirm.

OS Users Passwords

This section describes how to change the OS password settings.

To change OS passwords:

1. From the Security menu, choose OS Users Passwords, and then press Enter.



- Type **y** to change General Password settings (see General Password Settings on the next page).
- Type **n** to change User Security Extensions.



.

• Type y to change Operating System User Security Extensions (Operating System User Security Extensions on the next page).

General Password Settings

This option enables you to change the OS general password settings, such as 'Minimum Acceptable Password Length' and 'Enable User Block on Failed Login'. This feature also enables you to modify settings for a specific user, such as 'User's Password' and 'Password Validity Max Period'.

> To modify general password settings:

- **1.** The Change General Password Settings prompt is displayed; type **y**, and then press Enter.
- 2. Do you want to change general password settings? (y/n)y
- 3. The Minimum Acceptable Password Length prompt is displayed; type 10, and then press Enter.

Minimum Acceptable Password Length [10]: 10

4. The Enable User Block on Failed Login prompt is displayed; type y, and then press Enter.

Enable User Block on Failed Login (y/n) [y] y

5. The Maximum Login Retries prompt is displayed; type **3**, and then press Enter.

Maximum Login Retries [3]: 3

6. The Failed Login Locking Timeout prompt is displayed; type 900, and then press Enter.

Failed Login Locking Timeout [900]:900

7. You are prompted if you wish to continue; type **y**, and then press Enter.

Are you sure that you want to continue? (y/n/q) y

8. You are prompted if you wish to change the password for a specific user; type y, and then press Enter.

Do you wish to change this user's password?

9. Enter the username whose password you wish to change, and then press Enter.

Enter Username [username]

10. Enter the new password, confirm, and then press Enter.

Operating System User Security Extensions

This feature enables the administrator to configure the following additional user security extensions:

- Maximum allowed numbers of simultaneous open sessions.
- Inactivity time period (days) before the OS user is locked.

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure).

> To configure operating system users security extensions:

1. The Change General Password Settings prompt is displayed; type **n**, and then press Enter.

Do you want to change general password settings ? (y/n) n

2. The Change password for a specific user prompt is displayed; type y, and then press Enter.

Do you want to change password for specific user ? (y/n) y

3. Enter the Username upon which you wish to configure, and then press Enter.

Enter Username [acems]:

4. The change User Password prompt is displayed; type **n**, and then press Enter.

Do you want to change its password ? (y/n) n

5. An additional Password prompt is displayed, type y, and then press Enter.

Do you want to change its login and password properties? (y/n) y

6. The Password Validity prompt is displayed; press Enter.

Password Validity Max Period (days) [90]:

7. The Password Update prompt is displayed; press Enter.

Password Update Min Period (days) [1]:

8. The Password Warning prompt is displayed; press Enter.

Password Warning Max Period (days) [7]:

9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user, and then press Enter.

Maximum allowed number of simultaneous open sessions [0]:

10. The Inactivity Days prompt is displayed; enter the number of inactivity days before the user is locked. For example, if you'd like to suspend a specific user if they have not connected to the OVOC server for a week, enter 7 days, and then press Enter.

Days of inactivity before user is locked (days) [0]:

Figure 28-16: OS Passwords Settings with Security Extensions

OS Passwords Settings
Do you want to change general password settings? (y/n) n
Do you want to change password for specific user? (y/n) y Enter Username [acems]: testuser 🔫
Do you want to change its password ? (y/n) n
Do you want to change its login and password properties? (y/n) y Password Validity Max Period (days) [90]: Password Update Min Period (days) [1]: Password Warning Max Period (days) [7]: Maximum allowed number of simultaneous open sessions [0]: 3 Days of inactivity before user is locked (days) [0]: 3 Are you sure that you want to continue? (y/n/q) y
Adjusting aging data for user testuser. passwd: Success Done.

If the user attempts to open more than three SSH sessions simultaneously, they are prompted and immediately disconnected from the fourth session as displayed in the figure below.





By default you can connect through SSH to the OVOC server with user *acems* only. If you configure an inactivity days limitation on this user, the situation may arise, for example, where a user is away for an extended period and has no active user to access the OVOC server. Therefore, we strongly recommend to use this limitation very carefully and preferably to configure this option for each user to connect to the OVOC server through SSH other than with the *acems* user.

File Integrity Checker

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported through OVOC Security Events. The File Integrity checker tool runs on the OVOC server machine.

From the Security menu, choose File Integrity Checker, and then press Enter; the File Integrity Checker is started or stopped.

Software Integrity Checker (AIDE) and Pre-linking

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

Pre-linking is designed to decrease process startup time by loading each shared library into an address for which the linking of needed symbols has already been performed. After a binary has been pre-linked, the address where the shared libraries are loaded will no longer be random on a per-process basis. This is undesirable because it provides a stable address for an attacker to use during an exploitation attempt.

> To start AIDE and disable pre-linking:

1. From the Security menu, choose **Software Integrity Checker (AIDE) and Pre-linking**; the current status of these two processes is displayed:

Figure 28-18: Software Integrity Checker (AIDE) and Pre-linking

Software Integrity Checker (AIDE) and Prelinking:

```
Software integrity checker (AIDE) is <mark>disabled</mark> and Prelinking is <mark>enabled.</mark>
Enable integrity checker, and disable prelinking? (y/n)
```

- **2.** Do one of the following:
 - Type **y** to enable AIDE and disable pre-linking, and then press Enter.
 - Type **n** to disable AIDE and enable pre-linking, and then press Enter.

USB Storage

This menu option allows enabling or disabling the OVOC server's USB storage access as required.

> To enable USB storage:

1. From the Security menu, choose USB Storage, and then press Enter.





2. Enable or disable USB storage as required.

Network Options

This menu option provides the following options to enhance network security:

- Ignore Internet Control Message Protocol (ICMP) Echo requests: This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.
- Ignore ICMP Echo and Timestamp requests: This option ensures that the OVOC server does not respond to an ICMP timestamp request to query for the current time. This reduces exposure to spoofing of the system time.
- Send ICMP Redirect Messages: This option disables the sending of ICMP Redirect Messages, which are generally sent only by routers.
- Ignore ICMP Redirect Messages: This option ensures that the OVOC server does not respond to ICMP Redirect broadcasts, and therefore such replies are always discarded.

This prevents an intruder from attempting to redirect traffic from the OVOC server to a different gateway or a non-existent gateway.

> To enable network options:

1. From the Security menu, choose Network Options, and then press Enter.

Figure 28-20: Network Options

Main Menu> Security> Network options
Log packets with impossible addresses to kernel log: DISABLED [Ignore all ICMP ECHO requests: DISABLED [Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED [Send ICMP redirect messages: DISABLED [Accept ICMP redirect messages: DISABLED]
>1.Enable log packets with impossible addresses to kernel log
2.Enable ignore all ICMP ECHO requests
3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
4.Enable send ICMP redirect messages
5.Enable accept ICMP redirect messages
b.Back
q.Quit to main Menu

2. Set the required network options.

Auditd Agent Options

Auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk. Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

To set Auditd options according to STIG:

1. From the Security menu, choose Auditd Options, and then press Enter.

Figure 28-21: Auditd Options

Figure 28-22:

Auditd Options:

Not using STIG recommendations for auditd Change auditd settings according to STIG recommendations? (y/n)

2. Type y to enable auditd settings according to STIG recommendations.

Audit records are saved in the following /var/log/audit/ directory.

OVOC Voice Quality Package - SBC Communication

This option allows you to configure the transport type for the XML based OVOC Voice Quality Package communication from the OVOC managed devices to the OVOC server. You can enable the TCP port (port 5000), the TLS port (port 5001) connections or both port connections.

- > To configure the OVOC Voice Quality Package SBC Communication:
- 1. From the Security menu, select OVOC Voice Quality Package SBC Communication, and then press Enter.

Figure 28-23: OVOC Voice Quality Package – SBC Communication	
--	--



- 2. Choose one of the following transport types, and then press Enter:
 - TCP (opens port 5000)
 - TLS (opens port 5001)
 - TLS/TCP (this setting opens both ports 5000 and 5001).

HTTPS SSL TLS Security

This section describes the configuration settings for the HTTPS/SSL/TLS connections. The figure below shows the maximum security that can be implemented in the OVOC environment.



Figure 28-24: OVOC Maximum Security Implementation

• The above figure shows all the HTTPS/SSL/TLS connections in the OVOC network. Use this figure as an overview to the procedures described below. Note that not all of the connections shown in the above figure have corresponding procedures. For more information, refer to the OVOC Security Guidelines document.

- This version supports TLSv1.2 and TLSv1.3. Default: TLSv1.3
- See Server Certificates Update below
- See HTTP Security Settings Menu Options on page 273

Server Certificates Update

This menu option enables you to automatically generate custom SSL server certificates for securing connections between OVOC server and client processes. See . for an illustration of these connections.



If you are using self-generated certificates and private key, you can skip to step 4.

- > The procedure for server certificates update consists of the following steps:
- 1. Step 1: Generate Server Private Key.
- 2. Step 2: Generate Server Certificate Signing Request (CSR).
- 3. Step 3: Transfer the generated CSR file to your PC and send to CA.
- 4. Step 4: Transfer certificates files received from CA back to OVOC server.
- 5. Step 5: Import new certificates on OVOC server.
- 6. Step 6: Verify the installed Server certificate.
- 7. Step 7: Verify the installed Root certificate.
- 8. Step 8: Perform Supplementary procedures to complete certificate update process (see Supplementary Security Procedures on page 315).
- > To generate server certificates:
- 1. From the Security menu, choose Server Certificates Update, and then press Enter.

Figure 28-25: Server Certificate Updates



Information on the currently installed certificate is displayed (the currently installed certificate is the installation default).

Step 1: Generate a server private key:

1. Select option 1, and then press Enter. The following screen is displayed:

Figure 28-26: Generate Server Private Key



- 2. Select the number of bits required for the server private key, and then press Enter.
- Enter and reenter the server private key password, type y to continue, and then press Enter.

The private key is generated.





Step 2: Generate a CSR for the server:

- 1. Select option 2, and then press Enter.
- 2. Enter the private key password (the password that you entered in the procedure above).
- **3.** Enter the Country Name code, state or province, locality, organization name, organization unit name, common name (server host name) and email address.
- 4. Enter a challenge password and optionally a company name.

You are notified that a server Certificate Signing Request has successfully been generated and saved to the specified location.

Figure 28-28: Generating a Server Certificate Signing Request (CSR)



- Step 3: Transfer the CSR file to your PC and send to CA:
- Transfer the CSR file from the /home/acems/server_cert/server.csr directory to your PC and then sent it to the Certificate Authority (CA). For instructions on transferring files, see Transferring Files on page 328.





Step 4: Transfer server certificates from the CA:

Transfer the files that you received from the CA to the /home/acems/server_certs directory. The root certificate should have the name root.crt and that the server certificate should have the name server.crt. If you received intermediate certificates, then rename them to ca1.crt and ca2.crt. Make sure that all certificates are in PEM format. For instructions on transferring files, see Transferring Files on page 328.

If your certificates are self-generated (you did not perform steps 1-3), the /home/acems/server_certs directory does not exist; therefore you must create it using the following commands:

- mkdir /home/acems/server_certs
- chmod 777 /home/acems/server_certs

Step 5: Import certificates:

Select option **3**, press Enter and then follow the prompts. The certificate files are installed.

- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
 - Make sure that all certificates are in PEM format and appear as follows (see Verifying and Converting Certificates on page 329 for information on converting files):

-----BEGIN CERTIFICATE-----

MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1 UEAxMM

RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0 MFowKjET

TI6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0 L6V8IzUYOfHrEiq/6g==--

---END CERTIFICATE-----

Step 6: Verify the installed server certificate:

Select option **4** ,and then press Enter. The installed server certificate is displayed:



Step 7: Verify the installed root certificate:

Select Option 5, and then press Enter. The installed root certificate is displayed:

Figure	28-31:	Installed	Root	Certificate
--------	--------	-----------	------	-------------

<u>File Edit Setup Control Window Help</u>	
Installed Server Root Certificate Chain:	~
Certificate:	
Data:	
Version: 3 (Øx2)	
Serial Number: 2416023367 (0x90019747)	
Signature_Algorithm:_md5WithRSAEncryption	
Issuer: CN=EMS ROOT CA	
Validity	
Not Before: Feb 20 18:54:27 2010 GMI	
Not Hiter : Feb 20 18:54:27 2020 GMI	
Subject: CN=EMS ROUL CH2	
Subject rubic Key info:	
PED TIC REY HIGOFILM. PSALICFYPLION	
Modulus (1024 bit):	
00 hc : dd : dd : eb : 71 : c8 : 79 : de : f4 : 12 : 31 : 51 : 21 : e6 :	
7h:e9:3a:a3:9f:10:bc:4c:37:90:1d:da:4a:40:58:	
36:bb:43:f7:bb:c5:80:02:9e:66:21:7f:20:cc:48:	
c4:40:4a:ad:07:3b:48:3c:31:7a:db:9c:7c:a9:3e:	
76:f8:e9:d2:1a:40:c1:7d:db:16:18:67:66:34:13:	
50:74:08:ec:5b:3d:75:37:8a:d7:53:b2:59:a9:ff:	
a2:f2:23:2b:58:2c:b8:78:99:df:ca:3e:65:60:99:	-
More	Ŧ

Step 8: Install device certificates and perform supplementary procedures

See Supplementary Security Procedures on page 315.

HTTP Security Settings Menu Options

From the OVOC Server Manager root menu, choose HTTP Security Settings.

Figure 28-32: HTTP Security Settings



This menu allows you to configure the following Apache server security settings:

Disable TLSv1.2 (TLSv1.2 for Apache on the next page)

Default: TLSv1.3

- Show Allowed SSL Cipher Suites below
- Edit SSL Cipher Suites Configuration String on the next page
- Restore SSL Cipher Suites Configuration Default on page 276
- Manage HTTP Service Port (80) on page 276
- Manage IPP Files Service Port (8080) on page 276
- Manage IPPs HTTP Port (8081) on page 276
- Manage IPPs HTTPS Port (8082) on page 277
- OVOC Rest (Port 911) on page 277
- (Floating License (Port 912) on page 277
- OVOC WebSocket (Port 915) on page 277
- QoE Teams Server REST (Port 5010) on page 277
- (Trust Store Configuration on page 278)
- (SBC HTTPS Authentication Mode on page 278)
- (Enable Device Manager Pro and NBIF Web Pages Secured Communication on page 279)
- (Change HTTP/S Authentication Password for NBIF Directory on page 279)
- (Disable Client's IP Address Validation on page 280)
- (Host Header Validation Configuration on page 280)

TLSv1.2 for Apache

This option enables and disables TLS Version 1.2 on port 443 (Apache server is restarted).

> To enable or disable TLSv1.2:

From the HTTP Security Settings menu, select option Enable TLSv1.2 for Apache, and then press Enter.

Default (enabled). Apache server is restarted.

Show Allowed SSL Cipher Suites

This option allows you to view the currently configured SSL cipher suites.

To show allowed SSL cipher suites:

1. From the HTTP Security Settings menu, select option **Show Allowed SSL Cipher Suites**, and then press Enter.

The currently configured SSL cipher suites are displayed. The overall figure indicates the total number of entries.

Figure 28-33:	Show	Allowed	SSL	Cipher	Suites
---------------	------	---------	-----	--------	--------

File Edit Setup Control Window	Help			
) AEAD DH-RSA-AES128-GCM-SHA256	TLSv1.2	DH⁄RSA	DH	AESGCM<128
DH-RSA-AES128-SHA256	TLSv1.2	DH∕RSA	DH	AES(128)
DH-DSS-AES128-SHA256 SHA256	TLSv1.2	DH/DSS	DH	AES(128)
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH/RSA	ECDH	AESGCM<128
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM<128
ECDH-RSA-AES128-SHA256 SHA256	TLSv1.2	ECDH/RSA	ECDH	AES(128)
ECDH-ECDSA-AES128-SHA256 SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AES<128>
AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM<128
AES128-SHA256 SHA256	TLSv1.2	RSA	RSA	AES<128>
Overall: 28				
Press ENTER to continue				

Edit SSL Cipher Suites Configuration String

This option allows you to edit the SSL Cipher Suites configuration string.

> To edit the SSL cipher suites configuration string:

1. From the HTTP Security Settings menu, select option Edit SSL Cipher Suites Configuration String, and then press Enter.

Figure 28-34: 3	Show SSL	Cipher Suites	Configuration
-----------------	----------	----------------------	---------------

<u>File Edit Setup Control Window</u>	<u>H</u> elp					
) AEAD DH-RSA-AES128-GCM-SHA256	TLSv1.2	DH/RSA	DH	AESGCM<128		
DH-RSA-AES128-SHA256	TLSv1.2	DH∕RSA	DH	AES(128)		
DH-DSS-AES128-SHA256 SHA256	TLSv1.2	DH/DSS	DH	AES<128>		
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH/RSA	ECDH	AESGCM<128		
ECDH-ECDSA-AES128-GCM-SHA256 > AEAD	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM<128		
ECDH-RSA-AES128-SHA256 SHA256	TLSv1.2	ECDH/RSA	ECDH	AES(128)		
ECDH-ECDSA-AES128-SHA256 SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AES(128)		
AES128-GCM-SHA256 > AEAD	TLSv1.2	RSA	RSA	AESGCM<128		
AES128-SHA256 SHA256	TLSv1.2	RSA	RSA	AES(128)		
Overall: 28						
New configuration: !EDH:!ADH:!DSS:!RC4:HIGH:!3DES:!aNULL Would you like to apply this configuration? ⟨y/n/q⟩						

- 2. Edit the new configuration and select **y** to apply the changes.
- 3. Run the Show Allowed SSL Cipher Suites command to display the new configuration.

Restore SSL Cipher Suites Configuration Default

This option allows you to restore the SSL Cipher Suites to the OVOC default values.

- > To restore the SSL Cipher Suites Configuration default:
- From the HTTP Security Settings menu, select Restore SSL Cipher Suites Configuration Default, and then press Enter.

Manage HTTP Service Port (80)

This option allows you to open and close HTTP Service Port 80.

➤ To open/close HTTP Service (Port 80):

In the HTTP Security Settings menu, choose option Open/Close HTTP Service (Port 80), and then press Enter.

This HTTP port is used for the connection between the OVOC server and all AudioCodes devices with the Device Manager Pro Web browser.

Manage IPP Files Service Port (8080)

This option allows you to open and close Service Port 8080.

➤ To open/close IPPs files service (port 8080):

In the HTTP Security Settings menu, choose option Open/Close IPPs files(Port 8080), and then press Enter.

This HTTP port is used for downloading firmware and configuration files from the OVOC server to the endpoints.



This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTP Port (8081)

This option allows you to open and close HTTP port 8081.

➤ To open/close IPPs HTTP (Port 8081):

In the HTTP Security Settings menu, choose option Open/Close IPPs HTTP (Port 8081), and then press Enter.

This HTTP port is used for sending REST updates from the endpoints to the OVOC server, such as alarms and statuses.



This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTPS Port (8082)

This option allows to open and close HTTPS port 8082.

➤ To open/close IPPs HTTPS (Port 8082):

In the HTTP Security Settings menu, choose option Open/Close IPPs HTTPS (Port 8082), and then press Enter.

This HTTPS port is used for sending secure REST updates from the endpoints to the OVOC server, such as alarms and statuses (HTTPS without certificate authentication).



This option is reserved for backward compatibility with older device versions.

OVOC Rest (Port 911)

This option allows you to open and close the REST port connection for (internal) port and server debugging.

➤ To configure OVOC REST:

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC REST (Port 911)**, and then press Enter.

Floating License (Port 912)

This option allows you to open and close the Floating license REST service (internal) and Floating license service debugging.

To open/close the Floating License port:

 From the HTTP Security Settings menu, choose option Open/Close Floating License REST (Port 912), and then press Enter.

OVOC WebSocket (Port 915)

This option allows you to open and close the OVOC WebSocket (Port 915) connection between the Websocket client and OVOC server.

To open/close the WebSocket port:

From the HTTP Security Settings menu, choose option Open/Close OVOC WebSocket (Port 915), and then press Enter.

QoE Teams Server REST (Port 5010)

This option allows you to open and close the QoE Teams server (Port 5010) connection between Microsoft Teams and OVOC server.
To open/close QoE Teams server port 5010:

1. From the HTTP Security Settings menu, choose option **QoE Teams Server REST (Port 5010)**, and then press Enter.

Trust Store Configuration

This procedure describes how to add a custom trusted root certificate to the OVOC server installation for securing endpoint connections. These certificates are loaded for supporting the mutual authentication mechanism (see IPP HTTPS Authentication Mode).

> To add a trusted root certificate:

1. From the HTTP Security Settings menu, choose **Trust Store Configuration**, and then press Enter..

Figure	28-35:	Trust Store	Configuration
--------	--------	--------------------	---------------

Main Menu> Security> HTTP	Security	Settings>	Trust	Store	Configuration
>1.Add Trusted Roo	t Certific	ate:			
b.Back					
q.Quit to main Me	nu				

- 2. Select option Add Trusted Root Certificate.
- Type the relevant valid root certificate file path and name. For example: /home/acems/root.crt

SBC HTTPS Authentication Mode

This option enables you to configure whether certificates are used to authenticate the connection between the OVOC server and the devices in one direction or in both directions:

- Mutual Authentication: the OVOC authenticates the device connection request using certificates and the device authenticates the OVOC connection request using certificates. When this option is configured:
 - The same root CA must sign the certificate that is loaded to the device and certificate that is loaded to the OVOC server.
 - Mutual authentication must also be enabled on the device (Step 5: Configure HTTPS Parameters on the Device on page 319).
- One-way Authentication option: the OVOC does not authenticate the device connection request using certificates; only the device authenticates the OVOC connection request.



- You can use the procedure described in Server Certificates Update on page 268 to load the certificate file to the OVOC server.
- See Step 5: Configure HTTPS Parameters on the Device on page 319 for equivalent settings on devices.

> To enable HTTPS authentication:

1. In the HTTP Security Settings menu, choose the SBC HTTPS Authentication option, and then press Enter.

Main	Menu>	Security>	Apache	Security	Settings>	SBC	HTTPS	Authentication	Mode
HTTPS	Auther	ntication: Set Mutual	Mutual Authen	tication					
	2.: b.1 q.(Set One-Wa Back Quit to ma	y Authen in Menu	ntication					

Figure 28-36: SBC HTTPS Authentication

- 2. Choose one of the following options, and then press Enter:
 - 1-Set Mutual Authentication
 - 2. Set One-Way Authentication

Enable Device Manager Pro and NBIF Web Pages Secured Communication

This menu option enables you to secure the connection between the Device Manager Server and NBIF Web pages and the Apache server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 443 (instead of port 80-HTTP).

- > To secure connection the Device Manager Pro and NBIF Web pages connection:
- From the HTTP Security Settings menu, choose IP Phone Manager and NBIF Web pages Secured Communication, and then press Enter; the connection is secured.

Change HTTP/S Authentication Password for NBIF Directory

This option enables you to change the password for logging to the OVOC client from a NBIF client over an HTTP/S connection. The default user name is "nbif" and default password is "pass_1234".

To change the HTTP/S authentication password:

1. From the HTTP Security Settings menu, choose Change HTTP/S Authentication Password for NBIF Directory ,and then press Enter.

You are prompted to change the HTTP/S authentication password. Enter **y** to change the password.

<u>F</u> ile	<u>E</u> dit	<u>S</u> etup	C <u>o</u> ntrol	<u>W</u> indow	<u>H</u> elp)]
Woul	d yo	u like	to ch	ange H]	TP/S	authenti	ication	password	for	NBIF	directory	(User 🔺	1
name	- 11,0	11.1:	9/11/										
													l
												-	

Figure 28-37: Change HTTP/S Authentication Password for NBIF Directory

- 2. Enter the new password.
- 3. Reenter the new password.

A confirmation message is displayed and the Apache server is restarted.

Disable Client's IP Address Validation

This option controls whether the OVOC server validates the WebSocket IP address and client's logged in IP address (REST connection) for connection requests from the OVOC Web client. This maybe necessary to avoid scenarios where a Web Application Firewall (WAF) may randomly change the Client IP address in the packets and therefore the OVOC server receives the WebSocket packet from an IP address that is different to the client's logged in IP address (REST IP address). As a result, the Client-Server WebSocket connection cannot be established and the operator is logged out.

> To disable client's IP address validation:

1. From the HTTP Security Settings menu, choose **Disable Client's IP Address Validation**, and then press Enter.

Figure 28-38: Confirm Disabling of Client IP Address Validation

Are you sure you want to update client's IP address validation and restart the OVOC Server (y/n)

2. Enter y to confirm update. The OVOC Server is restarted.

Host Header Validation Configuration

This option prevents host header injection attacks through the configuration of a list of valid OVOC server IP addresses and FQDNs.

> To enable Host Header validation:

1. From the HTTP Security Settings menu, choose **Enable Host Header Validation**, and then press Enter.





2. Choose option 1 and then press Enter.



3. Enter the IP address of the host to add.

```
Current allowed hosts:
Please specify host to add:
10.1.1.1
```

You are prompted to restart the Apache server.

```
Current allowed hosts:

1> 10.1.1.1

1> Add Host(s)

2> Apply(Hpache will restart)

3> Cancel

Please select option:
```

29 Diagnostics

This section describes the diagnostics procedures provided by the OVOC Server Manager.

An IPv6 address can be configured for the following:

- Server Syslog
- Devices Syslog
- Network Traffic Capture

To run OVOC server diagnostics:

From the OVOC Server Manager Root menu, choose **Diagnostics**, and then press Enter.

OVOC Server 8.0.1091 Management
Main Menu> Diagnostics
X1. Server Syslog 2. Devices Syslog 3. Devices Debug 4. Logger Levels 5. Network Traffic Capture g.Quit to main Menu

Figure 29-1: Diagnostics

This menu includes the following options:

- Server Syslog Configuration (Server Syslog Configuration below).
- Devices Syslog Configuration (Devices Syslog Configuration on page 285).
- Devices Debug Configuration (Devices Debug Configuration on page 286).
- Server Logger Levels (Server Logger Levels on page 287)
- Network Traffic Capture (Network Traffic Capture on page 288)

Server Syslog Configuration

This section describes how to send OVOC server Operating System (OS)-related syslog EMERG events to the system console and other OVOC server OS related messages to a designated external server.

- > To send EMERG event to the syslog console and other events to an external server:
- 1. From the Diagnostics menu, choose Server Syslog, and then press Enter.

2. To send EMERG events to the system console, type **y**, press Enter, and then confirm by typing **y** again.

Syslog configuration
Send EMERG events to system_console: y
Forward messages to external server: n
Cond EMERC quanta to quotem concolo? (u/n) u
Formand messages to external semien? (U/n) u
Facility (choose from this list):
*
AUTH
AUTHPRIV
CRON
DAEMON
FTP
KERN
LOCALZ
LOCALS
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
979PAG

Figure 29-2: Syslog Configuration

- **3.** You are prompted to forward messages to an external server, type **y**, and then press Enter. The OVOC server is rebooted.
- **4.** Type one of the following **Facilities** from the list (case-sensitive) or select the wildcard * to select all facilities in the list, and then press Enter:
 - auth and authpriv: for authentication;
 - cron: Task scheduling services, cron and atd
 - daemon: affects a daemon without any special classification (DNS, NTP, etc.)
 - ftp: FTP server logs
 - **kern:** kernel messages
 - **Ipr:** printing subsystem messages
 - mail: e-mail subsystem messages
 - news: Usenet subsystem message (especially from an NNTP Network News Transfer Protocol — server that manages newsgroups);
 - **syslog:** syslogd server messages
 - user: user messages (generic)
 - **uucp:** messages from the UUCP server (Unix to Unix Copy Program, an old protocol notably used to distribute e-mail messages);

- **local0 to local7:** reserved for local use.
- 5. Each message is also associated with a **Severity** or priority level. Type one of the following severities (in decreasing order) and then press Enter:

LOCAL2			
LOCAL3			
LOCAL4			
LOCAL5			
LOCAL6			
LOCAL7			
LPR			
MAIL			
NEWS			
SYSLOG			
USER			
UUCP			
[]: AUTH			
Severity	(choose from thi	s list):	
×			
EMERG			
ALERT			
CRIT			
ERR			
WARNING			
NOTICE			
INFO			
DEBUG			

Figure 29-3: Syslog Severities

For the selected facilities, indicates one of the following:

- **emerg**: Indicates an emergency situation, the system is most likely unusable.
- alert: Indicates that an action must be taken immediately.
- **crit**: Indicates that conditions are critical.
- err: Indicates an error.
- warn: Indicates a warning (potential error).
- **notice**: Indicates that conditions are normal, however, the message is important.
- info: An informative message.
- **debug**: A debugging message.
- 6. Type the external server Hostname or IP address of the Syslog server.

Figure 29-4: Syslog Hostname



The example Message forwarding configuration is shown below.



Devices Syslog Configuration

The capture of the device's Syslog can be logged directly to the OVOC server without the need for a third-party Syslog server in the same local network. The OVOC Server Manager is used to enable this feature.



Syslog is captured according to the device's configured Syslog parameters. For more information, see the relevant device User's manual.

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the OVOC server machine.

The syslog log file 'syslog' is located in the following OVOC server directory:

/data/NBIF/mgDebug/syslog

The syslog file is automatically rotated once a week or when it reaches 100 MB. The Operating System creates up to **5** rotated zip files in the default configuration (in addition to the Main Syslog file).

> To enable device syslog logging:

1. From the Diagnostics menu, choose **Devices Syslog**, and then press Enter.



2. Type y to enable device syslog logging, and then press Enter.

Devices Debug Configuration

Debug recordings packets from all managed machines can be logged directly to the OVOC server without the need for a 3rd party network sniffer in the same local network.



Debug recording packets are collected according to the AudioCodes device's configured Debug parameters. For more information, see the relevant device User's Manual.

The OVOC server runs the Wireshark network sniffer, which listens on a particular configured port. The sniffer records the packets to a network capture file in the Debug Recording (DR) directory. You can then access this file from your PC through FTP. The OVOC Server Manager is used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the OVOC server IP. The DR capture file is located in the following OVOC server directory:

/data/NBIF/mgDebug/DebugRecording

The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close; if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the OVOC server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

> To enable or disable devices debug:

1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.

A message is displayed indicating that debug recording is either enabled or disabled.



2. Type y and then press Enter to enable Device Debug Recording.

```
Device Debug Recording Configuration
Device Debug Recording is <mark>Not running</mark>, do you wish to start it? (y/n) y
Don't forget to disable Device Debug Recording when you are done.
Press Enter to continue...
```

3. Press Enter to continue.

Recording files are saved in /data/NBIF/mgDebug directory on the server.



It is highly recommended to disable this option when you have completed recording because this feature heavily utilizes system resources.

Server Logger Levels

This option allows you to change the log level for the different OVOC server log directories.



After completing the debugging, revert to the previous configuration to prevent over utilization of CPU resources.

To change the <tc> server logger level:

1. From the Diagnostics menu, choose Logger Levels.

osu : DEBUG v52 : INFO watchdog : ALL ssl : INFO	^
watchdog : ALL ssl : INFO	
sslTunneling : INFO vqServer : INFO	
vgmDB : INFO lyncServer : INFO	
endPointsServer : INFO rmiSocket : INFO	
http : INFO addRemove : INFO	
addŪersion : INFO refresh : INFO	
refreshClientServer : INFO pm : INFO	
dbUpgrade : INFO dc : INFO	
nodesFile : INFO miniIds : INFO	
ssh : INFO cliUsersSync : INFO	
nbif : INFO usersCache : INFO	
proxy : INFO org.hibernate : ERROR	
org.apache : ERROR adintegration : INFO	
concurrentCalls : INFO mgBackup : INFO	
license : INFO sipServerTestRunner : INFO	
security : INFO sites : INFO	
alarmRule : INFO ovocClient : INFO	
alarmsReSync : INFO asyncActions : INFO	
kafka : INFO HTTPRefresher : INFO	
Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF	
Enter logger name:	T

- 2. Enter the name of the log whose level you wish to change.
- 3. Enter the desired logger level.
- 4. Select **Yes** at the prompt to confirm the change.

<u>File Edit Setup Control</u>	Window Help			
watchdog	ALL	ss1	: INFO	
sslTunneling	= INFO	vqServer	= INFO	
vqmDB	= INFO	lyncServer	= INFO	
endPointsServer	= INFO	rmiSocket	= INFO	
http	: INFO	addRemove	= INFO	
addVersion	= INFO	refresh	= INFO	
refreshClientServer	= INFO	քո	= INFO	
dbUpgrade	= INFO	dc	= INFO	
nodesFile	= INFO	minilds	= INFO	
ssh	= INFO	cliUsersSync	= INFO	
nbif	= INFO	usersCache	= INFO	
proxy	= INFO	org.hibernate	= ERROR	
org.apache	= ERROR	adintegration	= INFO	
concurrentCalls	= INFO	mgBac kup	= INFO	
license	= INFO	sipServerTestRunner	= INFO	
security	= INFO	sites	= INFO	
alarmRule	= INFO	ovocClient	= INFO	
alarmsReSync	= INFO	asyncActions	= INFO	
kaf ka	= INFO	HTTPRefresher	= INFO	
Levels: ALL < DEBUG <	(INFO < WAR	N < ERROR < FATAL < OF	R	
<u>Enter logger name: nl</u>	oif			
<u>Enter logger level:</u> i	info			T

Figure 29-5: Server Logger Name and Level

Network Traffic Capture

Network traffic can be captured to a PCAP capture file according to a list of IP addresses and ports and a specified time period. The PCAP files can later be opened with a network sniffer program such as Wireshark.

> To capture TCP traffic:

1. From the Diagnostics menu, choose option Network Traffic Capture.

Figure 29-6: Network Traffic Capture



- 2. Select option 1 Start tcpdump.
- **3.** Select **y** to start the tcpdump.





- 4. Enter comma separated IP address (es) or accept the default "any" IP address.
- 5. Enter comma separated port (s) or accept the default "any".
- 6. Enter the capture time (in minutes). Default: network traffic for the last ten minutes is captured.



Figure 29-8: Starting TCP Dump

7. Select y to proceed.

Main	Menu> Diagnostics> Network Traffic Capture
	<pre>ITcpdump: RUNNING IPID: 5713 IStart time: 09:57:00 13.02.19 IRun timeout: 10 minutes IPort Filter: 80 or 443 or 162 or 1161 IOutput file: /var/log/ems/capture/190213095700_capture.pcap#ID</pre>
	>1. <mark>Stop tepdump</mark> b.Back q.Quit to main Menu

Figure 29-9: TCP Dump Running

Part VII

Configuring the Firewall

This part describes how to configure the OVOC firewall.

30 Configuring the Firewall

The OVOC interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. You need to define firewall rules to secure communications for the OVOC client-server processes. Each of these processes use different communication ports. By default, all ports are open on the OVOC server side. When installing the OVOC server, you need to configure its network and open the ports in your Enterprise LAN according to your site requirements; based on the firewall configuration rules (representing these port connections) that are described in the table and figure below.



See also:

- Cloud Architecture Mode (WebSocket Tunnel) Firewall Settings on page 297
- Firewall Settings for NAT Deployment on page 297
- Firewall Settings for OVOC Server Provider (Single Node)

 Table 30-1: Firewall Configuration Rules

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC clients and OVOC server					
TCP/IP client \leftrightarrow OVOC server	ТСР	V	22	SSH communication between OVOC server and TCP/IP client. Initiator: client PC	OVOC server side / Bi-directional.
HTTPS/NBIF Clients \leftrightarrow OVOC server	TCP (HTTPS)	\checkmark	443	Connection for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi-directional
REST client	TCP (HTTP)	×	911	Connection for OVOC server	OVOC server side /

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				REST (internal) port and server debugging. Initiator (internal): OVOC server Initiator (debugging): REST client	Bi-directional
	TCP (HTTP)	×	912	Floating license REST service (internal) communication and Floating license service debug- ging. Initiator (internal): OVOC server Initiator (debugging): REST client	OVOC server side / Bi-directional
Microsoft Teams↔ OVOC Communication	TCP (HTTPS)	~	443	Connection to Microsoft Teams Initiator: Microsoft Teams The following link includes a list of IP addresses that need to be opened on the Customer Firewall to allow Calls Notifications from Microsoft (refer to item 23 in below link): Microsoft Teams IP List	Bi-directional
Microsoft Teams↔ OVOC Com- munication (Internal Connection)	TCP (HTTPS)	V	5010	Internal	OVOC server side / Receive only
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	V	915	WebSocket Client and OVOC Server communication (internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	OVOC server side / Bi-directional
OVOC server and OVOC Managed Device	25				
Device ↔ OVOC server (SNMP)	UDP	V	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Used also by Fixed License Pool and Floating License Service. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	1	162	SNMP trap listening port on the OVOC. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	1	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Used also by Fixed	MG side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				License Pool and Floating License Service. Initiator: OVOC server	
Device ↔ OVOC server (NTP Server)	UDP (NTP server)	×	123	 NTP server synchronization for external clock. Initiator: MG (and OVOC server, if configured as NTP client) Initiator: Both sides 	Both sides / Bi-directional
Device ↔ OVOC server	TCP (HTTP)	x	80	HTTP connection for files transfer and REST communication. Initiator: Both sides can initiate an HTTP connection	OVOC server side / Bi-directional
	TCP (HTTPS)	V	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: Both sides can initiate an HTTPS connection.	OVOC server side / Bi-directional
Device↔ OVOC server Floating License Management	TCP (HTTPS)	V	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management. Initiator: Device	OVOC server side / Bi-directional
Devices Managed by the Device Manage	r]			
Endpoints ↔ OVOC Device Manager	TCP (HTTP)	×	80	 HTTP connection between the Endpoints and the OVOC Device Manager. Initiator: Endpoints HTTP connection that is used by endpoints for downloading firmware and configuration files . Initiator: Endpoints 	OVOC Device Manager side/ Bi- Directional
Endpoints ↔ OVOC Device Manager	TCP (HTTPS)	V	443	 HTTPS connection between the Endpoints and the OVOC Device Manager. Initiator: Endpoints HTTPS connection that is used by endpoints for downloading firmware and configuration files . Initiator: Endpoints 	OVOC Device Manager side / Bi- Directional
OVOC Device Manager ↔ ShareFile	TCP (HTTPS)	1	443	HTTPS connection used by OVOC Device Manager for downloading firmware and configuration files from ShareFile.	OVOC Device Manager Side / Bi- Directional

Connection	Port Type	Secured	Port	Purpose	Port side /
		connection	Number		Flow Direction
				Initiator: OVOC Device Manager For information on ShareFile IP Ranges, see ShareFile Firewall Configuration.	
OVOC Voice Quality Package Server and	Devices	,		,	
Media Gateways ↔ Voice Quality Package	ТСР	×	5000	XML based communication for control, media data reports and SIP call flow messages. Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	V	5001	XML based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device	OVOC server side / Bi-directional
Skype for Business MS-SQL Server					
OVOC Voice Quality Package server ↔ Skype for Business MS-SQL Server	ТСР	\checkmark	1433	Connection between the OVOC server and the MS-SQL Skype for Business Server. This port should be configured with SSL. Initiator: OVOC server	Skype for Business SQL server side / Bi-directional
LDAP Active Directory Server		1	1]	
Voice Quality Package ↔ Active Directory LDAP server (Skype for Business user authentication)	ТСР	×	389	Connection between the Voice Quality Package server and the Active Directory LDAP server.	Active Directory server side/ Bi-directional
	TCP (TLS)	V	636	Connection between the Voice Quality Package server and the Active Directory LDAP server with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	ТСР	x	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side/ Bi-directional
	TCP (TLS)	~	636	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users) with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional
RADIUS Server					
OVOC server \leftrightarrow RADIUS server	ТСР	x	1812	Direct connection between the OVOC server and the RADIUS server (when OVOC user is authenticated using RADIUS server). Initiator: OVOC server	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction	
AudioCodes Floating License Service					'	
OVOC server ↔AudioCodes Floating License Service	ТСР	1	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional	
External Server Connections					'	
OVOC server \leftrightarrow Mail Server	ТСР	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional	
OVOC server \leftrightarrow Syslog Server	ТСР	×	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side /Bi-directional	
OVOC server ↔ Debug Recording Server	UDP	×	925	Trap Forwarding to Debug Recording server. Initiator: OVOC server	Debug Recording server /Bi- directional	
OVOC server ↔Remote Managed Device	TCP RDP	V	3389	Remote Desktop access Apache to Managed Device through the Guacamole VPN gateway. Initiator: OVOC server	Managed Device/Bi- directional	
Voice Quality						
Voice Quality Package ↔ Endpoints (RFC 6035)	UDP	x	5060	SIP Publish reports sent to the SEM server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics.	SEM server / Bi-directional	

Table 30-2: Northbound Interfaces Flows: NOC/OSS \rightarrow OVOC

Source IP Address Range	Destination IP Address Range	Protocol	Secure	Source Port Range	Destination Port Range
NOC/OSS	OVOC	SFTP	\checkmark	1024 - 65535	20
		FTP	×	1024 - 65535	21
		SSH	V	1024 - 65535	22
		Telnet	×	1024 - 65535	23
		NTP	×	123	123
		HTTP/HTTPS	×/√	N/A	80/443
		SNMP (UDP) Set for the Active alarms Resync feature.	×	N/A	161
		TCP connection for Data analytics DB Access Initiator: DB Access client This port is open when the "Data analytics" Voice Quality feature license has been purchased and the feature has been enabled (see analytics API on page 221).	×	N/A	5432

Source IP Address Range	Destination IP Address Range	Protocol	Secure	Source Port Range	Destination Port Range
OVOC	NOC/OSS	NTP	×	123	123
		SNMP (UDP) Trap	×	1024 — 65535	162
		SNMP (UDP) port for the Act- ive alarms Resync feature.	×	1164 - 1174	-
		SNMP (UDP) port for alarm for- warding.	×	1180-1220	-

Table 30-3: C	DAM Flows:	$OVOC \rightarrow$	NOC/OSS
---------------	------------	--------------------	---------



The above figure displays images of devices. For the full list of supported products, see Managed VoIP Equipment on page 3.

Cloud Architecture Mode (WebSocket Tunnel) Firewall Settings

When the OVOC server is deployed in a public cloud and the Cloud Architecture feature is enabled (see Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 153), all proprietary connections between SBC devices and the OVOC server are bundled into an HTTP/S tunnel overlay network over ports 80/443, therefore these ports must be open on the Enterprise firewall. Configuring other Enterprise firewall rules for SBC and OVOC server connections is not necessary.

Firewall Settings for NAT Deployment

The table below describes the mandatory firewall rules to configure in the Enterprise firewall for connecting devices behind a NAT as described in Managing Device Connections on page 148.

Configuration Option Ports to Configure		Purpose	Port side / Flow Direction
SBC Devices			
Cloud Architecture Mode (Device > OVOC Server)	 TCP HTTP 80 TCP HTTPS 443 	See Cloud Architecture Mode (WebSocket Tunnel) Firewall Settings above.	OVOC server side / Bi-directional
OVOC Server NAT Mode (OVOC > Devices)	SNMP UDP port 1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Used also by Fixed License Pool and Floating License Service. Initiator: AudioCodes device	OVOC server side / Receive only
	SNMP UDP port 162	SNMP trap listening port on the OVOC. Initiator: AudioCodes device.	OVOC server side / Receive only
	TCP 5000	 XML based communication for control, media data reports and SIP call flow messages. Initiator: Media Gateway. 	OVOC server side / Bi-directional

Configuration Option	Ports to Configure	Purpose	Port side / Flow Direction
	TCP 5001 (Voice Quality Management over TLS)	 XML based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device. 	OVOC server side / Bi-directional
	NTP 123	NTP server port (OVOC server's Public IP address is configured as the NTP server). See Establishing OVOC-Devices Connections on page 148.	.Both sides / Bi-directional
Devices Managed by the Device Manager			
Endpoints ↔ OVOC Device Manager	TCP (HTTPS) 443	 HTTPS connection between the endpoints and the OVOC Device Manager. Initiator: Endpoints HTTPS connection that is used by endpoints for downloading firmware and configuration files from the OVOC Device Manager. Initiator: Endpoints 	OVOC Device Manager side / Bi-Directional
OVOC Device Manager ↔ ShareFile	TCP (HTTPS) 443	 HTTPS connection used by OVOC Device Manager for downloading firmware and configuration files from ShareFile. Initiator: OVOC Device Manager For information on ShareFile IP Ranges, see ShareFile Firewall Configuration. 	OVOC Device Manager Side / Bi-Directional

Firewall Rules for Service Provider with Single Node

The table below describes the OVOC Server Provider firewall settings for a Service Provider with a single node.

Tab	le	30-4:	Enterprise	Firewall
-----	----	-------	------------	----------

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction			
OVOC clients and OVOC server								
HTTPS/NBIF Clients \leftrightarrow OVOC server	TCP (HTTPS)	\checkmark	443	Connection for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi- directional			
Microsoft Teams↔ OVOC Communication	TCP (HTTPS)	\checkmark	443	Connection to Microsoft Teams Initiator: Microsoft Teams	Bi-directional			
WebSocket Client ↔ OVOC Server Communication	тср (нттр)	\checkmark	915	WebSocket Client and OVOC Server communication (internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	OVOC server side / Bi- directional			
OVOC server and OVOC Managed Devices								
Device \leftrightarrow OVOC server (SNMP)	UDP	V	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Used also by Fixed License Pool and Floating License Service.	OVOC server side / Receive only			

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				Initiator: AudioCodes device	
	UDP	1	162	SNMP trap listening port on the OVOC. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	~	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Used also by Fixed License Pool and Floating License Service. Initiator: OVOC server	MG side / Bi-directional
Device↔ OVOC server (NTP Server)	UDP (NTP server)	~	123	NTP server synchronization for external clock. Initiator: MG (and OVOC server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional
Device \leftrightarrow OVOC server	ТСР (НТТР)	×	80	 HTTP connection for files transfer and REST communication. Initiator: Both sides can initiate an HTTP connection 	OVOC server side / Bi- directional
	TCP (HTTPS)	V	443	 HTTPS connection for files transfer (upload and download) and REST communication. Initiator: Both sides can initiate an HTTPS connection. 	OVOC server side / Bi- directional
Device↔ OVOC server Floating License Management	TCP (HTTPS)	1	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management.	OVOC server side / Bi- directional
Devices Managed by the Device N	lanager				
Endpoints ↔ OVOC Device Manager	TCP (HTTPS)	×	80	HTTP connection between the Endpoints and the OVOC Device Manager. Initiator: Endpoints	OVOC Device Manager side/ Bi-Directional
Endpoints ↔ OVOC Device Manager	TCP (HTTPS)	√	443	 HTTPS connection between the Endpoints and the OVOC Device Manager. Initiator: Endpoints HTTPS connection that is used by endpoints for downloading firmware and configuration files . Initiator: Endpoints 	OVOC Device Manager side / Bi-Directional
OVOC Device Manager ↔ ShareFile	TCP (HTTPS)	V	443	 HTTPS connection used by OVOC Device Manager for downloading firmware and configuration files from ShareFile. Initiator: OVOC Device Manager For information on ShareFile IP Ranges, see ShareFile Firewall 	OVOC Device Manager Side / Bi-Directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				Configuration.	
OVOC Voice Quality Package Serve	er and Devices	1	1]	
Media Gateways ↔ Voice Quality Package	ТСР	×	5000	XML based communication for control, media data reports and SIP call flow messages. Initiator: Media Gateway	OVOC server side / Bi- directional
	TCP (TLS)	1	5001	 XML based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device 	OVOC server side / Bi- directional
LDAP Active Directory Server	,	,	1	'	
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	ТСР	×	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side/ Bi-directional
	TCP (TLS)	√	636	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users) with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional
AudioCodes Floating License Servi	ce]	1	1	
OVOC server ↔AudioCodes Floating License Service	ТСР	V	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi- directional
External Servers	,	,	1		
OVOC server \leftrightarrow Mail Server	ТСР	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
OVOC server \leftrightarrow Syslog Server	ТСР	×	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side /Bi- directional
OVOC server ↔ Debug Recording Server	UDP	×	925	Trap Forwarding to Debug Recording server. Initiator: OVOC server	Debug Recording server /Bi- directional
OVOC server ↔Remote Managed Device	TCP RDP	V	3389	Remote Desktop access Apache to Managed Device through the Guacamole VPN gateway. Initiator: OVOC server	Managed Device/Bi- directional
Voice Quality					
Voice Quality Package ↔ Endpoints (RFC 6035)	UDP	×	5060	SIP Publish reports sent to the SEM server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics.	SEM server / Bi-directional

Part VIII

Appendix

This part describes additional OVOC server procedures.

31 Configuring OVOC as the Email Server on Microsoft Azure

This section describes how to configure the OVOC server as the Email server on Microsoft Azure. These steps are necessary in to overcome Microsoft Azure security restrictions for sending emails outside of the Microsoft Azure domain. The following options can be configured:

- Configuring Internal Azure Mail Server on Microsoft Office 365 below
- Configuring OVOC as the Email Server on Microsoft Azure using SMTP Relay on page 304

Configuring Internal Azure Mail Server on Microsoft Office 365

This procedure describes how to forward alarms by email through the configuration of a user account on the Microsoft Office 365 platform. Office365 configuration on exim.conf is not supported by AudioCodes security policy.



The Office 365 user name is not necessarily the email address.

> Do the following:

- 1. Subscribe to sendgrid appfrom the Azure marketplace.
- 2. When subscription is confirmed and permissions granted, verify the email destination for forwarding alarms.
- 3. Create an API key.
- 4. Login into the OVOC server by SSH, as 'acems' user and enter password acems.
- 5. Switch to 'root' user and provide root password (default password is root):

su - root

6. Backup the exim configuration file:

cp /etc/exim/exim.conf /etc/exim/exim.conf.bak

7. Edit the exim configuration file:

vim /etc/exim/exim.conf

8. After the line "begin transports", add the following configuration:

```
begin transports
sendgrid_smtp:
driver = smtp
hosts = smtp.sendgrid.net
hosts_require_auth = <; $host_
address
hosts_require_tls = <; $host_
address</pre>
```

9. After the line "begin routers", add the following configuration:

```
begin routers
   send_via_sendgrid:
    driver = manualroute
    domains = ! +local_domains
    transport = sendgrid_smtp
    route_list = "* smtp.sendgrid.net::587
byname"
    host_find_failed = defer
    no_more
```

10. After the line "begin authenticators", add the following configuration, replacing Username and Password with your SendGrid User/Pass:



```
sendgrid_login:
driver = plaintext
public_name = LOGIN
client_send = : Username :
Password
```



The User name is always apikey. The password is the key you generated in Step 3.

- 11. Open /root/.muttrc
- 12. Replace the default email address set from = OVOC@audiocodes.com with the proper email address of the owner of the OFFICE365_USERNAME account.
- 13. Restart the Exim service:

systemctl restart exim

14. Type the following command to test the mail setup via OVOC:

```
echo "server 243" | mutt -s "OVOC received 10 new alarms" -F /root/.muttrc 
<yourEmailAddress>
```



AudioCodes may block emails from sendGrid, use other email addresses other than xx@audiocodes.com for testing sendGrid.

Configuring OVOC as the Email Server on Microsoft Azure using SMTP Relay

This procedure describes how to configure the OVOC server to forward alarms by email using SMTP Relay. This setup is recommended by Microsoft, and SendGrid is one of the available options. SendGrid service can be easily configured in the Azure Portal and in addition, includes a free tier subscription, supporting up to 25,000 emails per month.

> Do the following:

- 1. Create SendGrid service on the Azure platform:
 - a. Open portal.azure.com

- **b.** Go to "SendGrid Accounts" section, (via Search or in "All services" section).
- c. Click Add.
- d. Fill in the following fields:

Name: Choose a name Password Subscription Resource Group (create a new one or choose existing) Pricing tier: choose Free or one of the other plans Contact Information Read legal terms

- e. Click Create.
- f. Wait for the service to be created.
- g. Go back to "SendGrid Accounts", click on the new account name
- h. Click the "Configurations" section in the Settings tab.
- i. Copy the Username it will be used in the next step along with the password (format azure_xxxxxxx@azure.com)
- 2. Configure the Exim service on the OVOC server:
 - a. Login into the OVOC server by SSH, as 'acems' user and enter password acems.
 - **b.** Switch to 'root' user and provide root password (default password is root):

su - root

c. Backup the exim configuration file:

cp /etc/exim/exim.conf /etc/exim/exim.conf.bak

d. Edit the exim configuration file:

vim /etc/exim/exim.conf

e. After the line "begin transports", add the following configuration:

```
begin transports
sendgrid_smtp:
driver = smtp
hosts = smtp.sendgrid.net
hosts_require_auth = <; $host_address
hosts_require_tls = <; $host_address</pre>
```

f. After the line "begin routers", add the following configuration:

```
begin routers
send_via_sendgrid:
driver = manualroute
domains = ! +local_domains
transport = sendgrid_smtp
route_list = "* smtp.sendgrid.net::587 byname"
host_find_failed = defer
no_more
```

g. After the line "begin authenticators", add the following configuration, replacing Username and Password with your SendGrid User/Pass:

```
begin authenticators
sendgrid_login:
driver = plaintext
public_name = LOGIN
client_send = : Username : Password
```

- h. Save the file and exit back to the command line.
- i. Restart the Exim service.

systemctl restart exim

j. Check that the alarm forwarding by email functions correctly.

You can access the SendGrid Web interface using the same username/password, where among other features you can find an Activity log, which may be useful for verifying issues such as when emails are sent correctly; however, are blocked by a destination email server.

32 Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers

This appendix describes the required equipment and the steps for configuring the HP ProLiant server to support RAID-0 Disk Array configuration for the OVOC server installation.

• This procedure erases any residual data on the designated disk drives.

If you have purchased the server hardware from AudioCodes then this procedure is not necessary.

RAID-0 Prerequisites

This procedure requires the following:

- ProLiant DL360p Gen10 server pre-installed in a compatible rack and connected to power.
- Two SATA DS 1.92 TB SSD disk drives
- A VGA display, USB keyboard, and USB mouse must be connected to the server back I/O panel.

RAID-0 Hardware Preparation

Make sure that two SATA DS 1.92 TB SSD disk drives are installed on slot 1 and 2 of the server. If required, refer to the *HP Service Manual*.





Configuring RAID-0

The following procedures describe how to configure RAID-0 using the HP Smart Storage Administrator utility:

- Step 1 Create Logical Drive below
- Step 2 Set Logical Drive as Bootable Volume on the next page

Step 1 Create Logical Drive

This section describes how to create a logical drive on RAID-0.

➤ To create a logical drive on RAID-0:

- 1. Power up the server. If the server is already powered up and running, use the 'reboot' command (from system console as user root) to reboot the server.
- 2. While the server is powering up, monitor the server.
- 3. During restart, press <F9> to open the System Utilities.
- 4. Choose Embedded Applications > Intelligent Provisioning > Smart Storage Administrator.
- 5. Wait for the Smart Storage Administrator utility to finish loading.
- In the left-hand pane, choose HPE Smart Array Controllers > HPESmart Array E208i-a SRGen10; an Actions menu is displayed.
- 7. Click Configure, and then click Clear Configuration to clear any previous configuration.
- 8. Click Clear to confirm; a summary display appears.
- 9. Click **Finish** to return to the main menu.
- **10.** In the left-hand pane, select **Unassigned Drives (2)**; make sure that both the drives are selected, and then click **Create Array**.
- 11. Select RAID 0 for RAID Level.
- 12. Select the 'Custom Size' check box, and then enter 2000GiB.
- **13.** At the bottom of the screen, click **Create Logical Drive**.

After the array is created, a logical drive should be created.

- 14. Click Finish.
- 15. Proceed to Section Step 2 Set Logical Drive as Bootable Volume below

Step 2 Set Logical Drive as Bootable Volume

This section describes how to set the new logical drive as a bootable volume.

> To set new logical drive as bootable volume:

- In the left-hand pane, select HPE Smart Array E208i-a SR Gen10, and then click Set Bootable Logical Drive/Volume.
- Select the "Local Logical Drive 1" as Primary Boot Logical Drive/Volume, and then click Save.

A summary window is displayed.

- 3. Click Finish.
- **4.** Exit the Smart Storage Administrator utility by clicking the **X** sign on the top right-hand side of the screen, and then confirm.
- 5. Click Exit at the bottom left-hand corner of the screen.
- 6. Click the **Power** icon in the upper right-hand corner of the screen.

7. Click **Reboot** to reboot the server.

The Disk Array configuration is now complete.

8. Install the OVOC server (Installing OVOC Server on Dedicated Hardware on page 67).

33 Managing Clusters

This appendix describes how to manually migrate or move OVOC VMs to another cluster node.

Migrating OVOC Virtual Machines in a VMware Cluster

This section describes how to migrate your OVOC Virtual machine from one ESXi host to another.

To migrate your OVOC virtual machine:

1. Select the OVOC virtual machine that you wish to migrate and then choose the Migrate option.



Figure 33-1: Migration

2. Change a cluster host for migration.

Figure 33-2: Change Host



3. Choose the target host for migration.

ð	7.2.2123 - Migrate		(?) }					
~ ~	Select the migration type Select a compute resource 2 Select a compute resource Select a cluster, host, vApp or resource pool to run the virtual machines.							
	 3 Select network 4 Select Motion priority 5 Ready to complete 	Filter Hosts Clusters Resource Pools vApps Image: Second state of the second state	-) 2 Objects					
		Compatibility: Compatibility checks succeeded. Back Next Finish	Cancel					

Figure 33-3: Target Host for Migration

The migration process commences.



Navigator I	📋 10.3.180.211 Actions 👻							
(Hosts and Clusters 🕨 🕤	Summary Monitor Manag	e Related Objects						
	10.3.100. Type: Model: Processo: Vehual Me State: Uptime:	211 HSN HP ProLiant DL300p Gen (*Type: Inter(R) Xeon(R) GPU ES- coessors: 20 4 chines: 6 Connected 30 days	8 2880 v2 @ 2.800Hz				0PU VSED 183 0HH MELORY USED 839 089 8100A04 USED 243 18	FREE: 20.25 GHz CAPACITY: 27.93 GHz FREE: 20.97 GB CAPACITY: 85.97 GB FREE: 3.10 TB CAPACITY: 5.58 TB
SSBC_01 SSBC_02	- Hardware	0	Configuration					
A SSBC_03	Manufacturer	HP	ESX/ESXI Version	VMware	ESXI, 6.0.0, 3620759			
Center	Model	ProLiant DL360p Gen8	Image Profile	HPE-ES	(i-6.0.0-Update2-iso-600.	9.5.0.48		
K VEMS 7.2.1000	> 🖬 CPU	10 CPUs × 2.79 GHz	 vSphere HA State 	📀 Runn	ing (Master)			
	Memory	70,657 MB / 98,269 MB	 Fault Tolerance (Le 	gacy) Unsuppo	rted			
	Virtual Flash Resource	0.00 B / 0.00 B	 Fault Tolerance 	Unsuppo	rted			
	Networking	localhost.corp.audiocodes.com	 EVC Mode 	Intel® "S	andy Bridge" Generation			
	> 🗐 Storage	3 Datastore(s)	- Palatad Objects					
	h. There	Keisted Objects						
	• rags		Justeru I					
	Update Manager Completion	iance C			More Relate	d Objects		
🛐 Recent Tasks		1						
Task Name	Target Status	ini ini	tiator Que	ued For	Start Time	Completion Time	Server	
Relocate virtual machine	7.2.2123	56 % © V	mware	14 ms	10/5/2016 2:25:05 PM		qaswvcenter01.corp.audiocodes.com	

After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's host.

Moving OVOC VMs in a Hyper-V Cluster

Moving OVOC VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

> To move a Virtual Machine to another node of the cluster:

 Select the Virtual Machine, right-click and from the menu, choose Move > Live Migration > Select Node.

- 44		Failov	er Clu	ster Manag	er					x
File Action View Hel	lp									
🗢 🌩 🖄 📰 🖬										
📲 Failover Cluster Manage	Roles (2)							Acti	ons	
⊿ QAHyperv-Cl.corp.a				ı و	Queries 🔻 🔒	• •	Rol	es	• ^	
Nodes	Name	Status	Туре		Owner Node	Priority	Informa	20	Configur	
🔺 🙇 Storage	EMS_High_1	Running	Virtu	al Machine	QAHyperV1	Medium			Virtual M	•
Disks	EMS_L	Q-	•••	al Machine	QAHyperV1	Medium		1	Create E	
Networks		Start							View	•
🔢 Cluster Events	l o	Save						a	Refresh	
	0	Shut Down						2	Help	_
		Turn Off						-	C L avr. 1	
		Settings						EM	S_LOW_I	-
	1	Manage							Connect	
	20	Replication	•						Save	
		Move	•	😣 Live Mig	ration	🕨 🔝 🛛 Best	Possible N	Node	en	
	× 🔬	Cancel Live Migration	_	Quick M	igration	• 📝 Selec	ct Node			
	v 🔣 🔞	Change Startup Priority	•	1 Virtual N	Aachine Storage	Owners: A	ny node	R	Settings	
		Information Details							Manage	
	Virtual Mar	Show Critical Events					Â	20	Replication	•
		Add Storage		Running			=		Move	•
	1	Add Resource	•	0%	Up Time:		6:1:0	3	Cancel Li	
		More Actions	•	4096 MB 4096 MB	Available M Integration	Services:	0 ME	۲	Change S	•
	X	Remove			-		>	8	Informati	
< III >	Summary	Properties						1	Show Cri	~
Roles: EMS_Low_1										

Figure 33-5: Hyper-V Live Migration

The following screen is displayed:

pok for: P Search		Cigar
luster nodes:	Cash-c	
- OAldward/1	(1) Un	

Figure 33-6: Move Virtual Machine

2. Select the relevant node and click **OK**.

The migration process starts.
灎			Failover Clu	ster Manager				- • ×
<u>F</u> ile <u>A</u> ction ⊻iew <u>H</u> el	р							
🗢 🌩 🖄 📰 📓 🖬								
📲 Failover Cluster Manage	Roles (2)						Ac	tions
⊿ CAHyperv-Cl.corp.a	Search					🔎 Queries 🔻 🔛 🔻 (R	oles 🔺 🗹
Nodes	Name	Status	Туре	Owner Node	Priority	Information	-	Configur
🔺 📇 Storage	EMS_High_1	Running	Virtual Machine	QAHyperV1	Medium			Virtual M >
💾 Disks	EMS_Low_1	🙀 Live Migrating	Virtual Machine	QAHyperV1	Medium	Live Migrating, 3% completed		Create E
Pools Networks								View 🕨
Cluster Events								Refresh
							2	Help
								Theip
							EN	IS_Low_1 ▲
								Connect
							0	Start
								Save
							0	Shut Down
	<		ш				20	Turn Off
						Preferred Owners: Any no		Settings
						The end of miles. Any no	ິ 🏅	Manage
							<u>_</u>	Replication >
	Virtual Machine EMS_Lov	r_1	Duration				_ 👳	Move +
		Status: CPU Usage:	Nunning 0%	Up Time:		0.00.06	- 1	Cancel Li
		Memory Demand:	4096 MB	Available	Memory:	0 MB		Change S >
		Assigned Memory:	4096 MB	Integratio	on Services:			Informati
		Heartbeat:	OK				- I 🗖	Show Cri
< III >	Summary Resources							Add Stor
Roles: EMS_Low_1								

Figure 33-7: Hyper-V Migration Process Started

After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's node.

34 Supplementary Security Procedures

The procedures in this appendix describe supplementary procedures for completing the setup of X.509 Custom certificates.



For more information on the implementation of custom certificates, refer to the OVOC Security Guidelines document.

This appendix describes the following procedures:

- Downloading certificates to the AudioCodes device (Installing Custom Certificates on OVOC Managed Devices below)
- Cleaning up Temporary files on the OVOC server (Cleaning up Temporary Files on OVOC Server on page 327)

Installing Custom Certificates on OVOC Managed Devices

This section describes how to install Custom certificates on OVOC managed devices. These certificates will be used to secure the connection between the device and OVOC server. This procedure is performed using the device's embedded Web server. This section describes how to install certificates for the following devices:

- Enterprise gateways and SBC devices (Gateways and SBC Devices below).
- MP-1xx devices (MP-1xx Devices on page 322).
 - When securing the device connection over HTTPS, the certificate loaded to the device must be signed by the same CA as the certificate loaded to the OVOC server.
 - The Single Sign-on mechanism is used to enable automatic login to the devices embedded Web server tool from the device's status screen in the OVOC. This connection is secured over port 443. OVOC logs into the OVOC managed device using the credentials that you configure in the AudioCodes device details or Tenant Details in the OVOC Web. You can also login to the AudioCodes device using the RADIUS or LDAP credentials (refer to RADIUS or LDAP Authentication).

Gateways and SBC Devices

This section describes how to install custom certificates on gateways and SBC devices. The device uses TLS Context #0 to communicate with the OVOC server. Therefore, the configuration described below should be performed for **TLS Context #0**.

Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

> To generate certificate signing request:

- **1.** Login to the device's Web server.
- Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
- 3. In the table, select the TLS Context Index #0, and then click the TLS Context Certificate button, located below the table; the Context Certificates page appears.

Figure 34-1: Context Certificates

FICATE SIGNING REQUEST			
Common Name [CN]		mike	
Organizational Unit [OU] (optional)			
Company name [O] <i>(optional)</i>			
Locality or city name [L] (optional)			
State [ST] (optional)			
Country code [C] (optional)			
1st Subject Alternative Name [SAN]		EMAIL	
2nd Subject Alternative Name [SAN]		EMAIL	
3rd Subject Alternative Name [SAN]		EMAIL	
4th Subject Alternative Name [SAN]		EMAIL	
5th Subject Alternative Name [SAN]		EMAIL	
Signature Algorithm		SHA-256	~
	Create CSR		

- 4. Under the Certificate Signing Request group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the device's DNS name, if such exists, or device's IP address.
 - **b.** Fill in the rest of the request fields according to your security provider's instructions.
 - c. Click the Create CSR button; a textual certificate signing request is displayed in the area below the button:

IFICATE SIGNING REQUEST			
Common Name [CN]		mike	
Organizational Unit [OU] (optional)			
Company name [O] (optional)			
Locality or city name [L] (optional)			
State [ST] (optional)			
Country code [C] (optional)			
1st Subject Alternative Name [SAN]		EMAIL	
2nd Subject Alternative Name [SAN]		EMAIL	
3rd Subject Alternative Name [SAN]		EMAIL	
4th Subject Alternative Name [SAN]		EMAIL	
5th Subject Alternative Name [SAN]		EMAIL	
Signature Algorithm		SHA-256	~
	Create CSR		
After creating the CSR, copy the text below (including the BEGIN/END lines) and sen	d it to your Certification Authority for sign	ng.	
BEGIN CERTIFICATE REQUEST			
ADCBiQKBqQDUZ2c6DLHOnfvvzcTJpNOw7jEK/SgeogcEf5Vnt1+XMS+saD3iF/dy			
8X4t0xFc675KR146LL0JrhfZSTVyZNLjIA5FgIXqIyxxvQcC8Kr1+Fgx2+d1TvK0			
IXDpbdwlGilPKC8GZDZF8AQXddXBPXHIKJDVKZGp8Cp4wd8iT6BXQIDAQABOCIW TAVJZA7ThwaNAOxOMDMWETAPBaNUHDFECDAGaaPteWt1MAOGCSaGSTb3DOFBCWDA			
A4GBAMkgQ7IOqTXOaCMnZWMv72Zx1YNd1c8CRAVQHePFIJY//jXQxxJJDGqGGq8x			
nOpnhdXNcyKbLQoBkMNA23BcggX9Jr5rs8zYd/Aat2frkXtTcEAPBWM97bKOA57Z			
YOattxV6ySCapXaKXaFqrC+6v2oNSqk/uNQ1gI5Nb2LJXwYL			

Figure 34-2: Certificate Signing Request Group

5. Copy the text and send it to the certificate authority (CA) to sign this request.

Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate rename this file to "device.crt"
- Root certificate rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

BEGIN CERTIFICATE
MIIBuTCCASKgAwIBAgIFAKK1MbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0MFowKjET
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0
L6V8lzUYOfHrEiq/6g==
END CERTIFICATE

• The above files are required in the following steps. Make sure that you obtain these files before proceeding and save them to the desired location.

• Use the exact filenames as mentioned above.

Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

> To update device with new certificate:

- Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
- 2. In the table, select **TLS Context #0**, and then click the **Change Certificate** button, located below the table; the Context Certificates page appears.

+ New Edit 📄	14.44	Page 1 of 1 🔛 🖭 Show 10 🗸 reco	rds per page			Q
NDEX 🗢	NAME	TLS VERSION	DTLS VER	ISION	CIPHER SERVER	
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any		DEFAULT	
1	miketls	TLSv1.1 and TLSv1.2	Any		RC4:AES128	
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any		DEFAULT	
#0[default]						Edit
GENERAL			OCSP			
Name	• default		OCSP Server	Disable		
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2		Primary OCSP Server	0.0.0.0		
DTLS Version	Any		Secondary OCSP Server	0.0.0.0		
Cipher Server	DEFAULT		OCSP Port	2560		
Cipher Client	DEFAULT		OCSP Default Response	Reject		
Strict Certificate Extension Valid	Disable					
DH key Size	1024					
TLS Renegotiation	Enable					
Certificate Information >> Chang	ge Certificate >> Trusted Root Cer	tificates >>				

Figure 34-3: TLS Contexts Table

3. Under the Upload certificates files from your computer group, click the Browse button corresponding to the 'Send Device Certificate...' field and then navigate to the device.crt file, and click Send File.

Figure 34-4: Upload Certificate Files from your Computer Group

UPLOAD CERTIFICATE FILES FROM YO	UR COMPUTER	
Private key pass-phrase (optional)		audc
Send Private Key file from your comput The file must be in either PEM or PFX (PK Browse No file selected.	er to the device. CS#12) format. Send File	
Note: Replacing the private key is r	not recommended but if it's	done, it should be over a physically-secure network link.
Send Device Certificate file from The file must be in textual PEM for	n your computer to the device. mat.	
Browse No file selected.	Send File	

Step 4: Update Device's Trusted Certificate Store

This step describes how to update the device's Trusted Certificate Store.

> To update device's trusted certificate store:

- 1. Open the TLS Contexts page (Configuration tab > System menu > TLS Contexts).
- 2. In the table, select the TLS Context #0, and then click the Trusted Root Certificates button, located below the table; the Trusted Certificates page appears.

TLS Contexts (3)						
+ New Edit		rec << Page 1 of 1 >> >> Show 10 v rec	ords per page			Q
INDEX 🗢	NAME	TLS VERSION	DTLS VER	SION	CIPHER SERVER	
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	. Any		DEFAULT	
1	miketls	TLSv1.1 and TLSv1.2	Any		RC4:AES128	
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any		DEFAULT	
#0[default]						Edit
GENERAL			OCSP			
Name	 default 		OCSP Server	Disable		
TLS Version	TLSv1.0 TLSv1.1 and T	LSv1.2	Primary OCSP Server	0.0.0.0		
DTLS Version	Any		Secondary OCSP Server	0.0.0.0		
Cipher Server	DEFAULT		OCSP Port	2560		
Cipher Client	DEFAULT		OCSP Default Response	Reject		
Strict Certificate Extension Valid	Disable					
DH key Size	1024					
TLS Renegotiation	Enable					
Certificate Information >> Ch	nange Certificate >> T	rusted Root Certificates >>				

Figure 34-5: Trusted Root Certificates

3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

Figure 34-6: Importing Certificate into Trusted Certificates Store

TLS 📀	O TLS Context [#0] > Trusted Root Certificates							
View				Import Export Remove				
INDEX	SUBJECT	ISSUER	EXPIRES					
		I < << Page 1 of 1 >> >I 1 v		No records to view				

 If you received intermediary CA certificates – ca1.crt, ca2.crt, etc. – import them in a similar way.

Step 5: Configure HTTPS Parameters on the Device

This section describes how to configure HTTPS related parameters on the device.

- You can optionally pre-stage the device with a pre-loaded ini file including this configuration (for more information, contact your AudioCodes representative).
- If you have enabled the Interoperability Automatic Provisioning feature, ensure that your template file is also configured as described in this procedure to maintain an active HTTPS connection after the template file has been loaded to the device.

> To configure HTTPS parameters on the device:

1. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).

Figure	34-7.	Tenant	Details
liguic	34-7.	ICHAIL	Details

TE	NANT DETAILS				
	General	SNMP	НТТР	Operators	License
	Edit HTTP Settings				
	Device Admin User*		Admin		
	Change Device Admin Passw	vord*			
	Communication Protocol*		HTTPS		•



AC DEVICE DETAILS						
General	SNMP	HTTP	SBA	First Connection		
Device Admin U	lser	Admi	n			
Change Device	Admin Password					
Communication	n Protocol	HTTF	S	▼		

- 2. Create a new text file using a text-based editor (e.g., Notepad).
- **3.** Enable mutual authentication on the device. This configuration instructs the Automatic Update mechanism to verify the TLS certificate received from the OVOC server.
 - For Media Gateway and SBC devices:

AUPDVerifyCertificates=1

• For MP-1xx devices, the ini file should include the following two lines::

AUPDVerifyCertificates=1 ServerRespondTimeout=10000

- 4. Save and close the file.
- Load the generated file as "Incremental INI file" (Maintenance menu > Software Update > Load Auxiliary Files > INI file (incremental).
- 6. In the SBC Web interface, open the Web Settings page and set parameter Secured Web Connection (HTTPS) to one of the following:
 - HTTP and HTTPS

HTTPS Only

		Figure 34-9: SBC We	eb Settings Pag	e	
C audiocodes	SETU	P MONITOR TROUBLESHOOT		Save Reset	Actions - Admin -
Mike IP NETWORK SIGNAL	ING & MED	ADMINISTRATION			<i>D</i> Entity, parameter, value
SRD All 💌					
🟠 TIME & DATE		Web Settings			
WEB & CLI	\sim	GENERAL		SECURITY	
Authentication Server Login OAuth Servers (1) Web Settings CLI Settings Access List Active Users Additional Management Interfaces (0) Customize Access Level (0) SNIMP	~	Secured Web Connection (HTTPS) Require Client Certificates for HTTPS connectio Web Hostname Local Users Table can be Empty SESSION	HTTP and HTTPS n Disable abc.com No Vo	Deny Authentication Timer Blocking Duration Factor Valid time of Deny Access counting Deny Access On Fail Count (0 = No Deny) Display Last Login Information DNS Rebinding Protection	60 1 60 3 v Disable v Disable v
LICENSE MAINTENANCE PERFORMANCE MONITORING		Password Change Interval (minutes) User Inactivity Timeout (days) Session Timeout (minutes)	0 90 15	invalia Login keport	general information V
			Cancel	APPLY	

 If you configured the SBC Devices Communication parameter to Hostname-Based in the OVOC Web, you must configure the parameter "Verify Certificate SubjectName" on the managed device (Setup Menu > Signaling & Media tab > Media folder > Quality of Experience Settings).

Figure 34-10: Quality of Experience Settings

- Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
- **9.** In the table, select the TLS Context #0 (Management interface), and then click **Edit**. The following screen is displayed:

S Contexts [default]					-
GENERAL			OCSP		
Index	0		OCSP Server	Disable 🗸	
Name	default		Primary OCSP Server	0.0.0.0	
TLS Version	TLSv1.2 and TLSv1.3	~	Secondary OCSP Server	0.0.0.0	
DTLS Version	DTLSv1.0 and DTLSv1.2	~	OCSP Port	2560	
Cipher Server	DEFAULT		OCSP Default Response	Reject 🗸	
Cipher Client	DEFAULT				
Cipher Server TLS1.3	TLS_AES_256_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	×'			
Cipher Client TLS1.3	TLS_AES_256_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	4			
Key Exchange Groups	X25519:xxxxxxxxxx				
Strict Certificate Extension Validation	Disable	~			
DH key Size	2048	~			
TLS Renegotiation	Enable	~			
Cancel APPLY					

Figure 34-11: TLS Contexts

10. Set the required 'TLS Version' (default TLS Version 1.0).

OVOC supports TLS versions 1.0, 1.1. and 1.2

- 11. Ensure 'Cipher Server' is set to DEFAULT.
- **12.** Ensure 'Cipher Client' is set to **DEFAULT**.

Step 6: Reset Device to Apply the New Configuration

This step describes how to restart the device to apply the new configuration.

To save the changes and restart the device:

 Reset the device with a save-to-flash for your settings to take effect (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

MP-1xx Devices

This section describes how to install Custom certificates on the MP 1xx devices.



For installing certificates on MP2xx devices, refer to "Securing Remote Management with Certificates" in the *MP-20x Telephone Adapter User's Manual*.

Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➤ To generate a CSR:

- Your network administrator should allocate a unique DNS name for the device (e.g., dns_ name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
- 2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to HTTP and HTTPS (refer to the *MP-11x and MP-124 User's Manual*). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
- 3. Login to the MP-1xx Web server.
- Open the Certificates page (Configuration tab > System menu > Certificates).
- 5. Under the Certificate Signing Request group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the DNS name.
 - **b.** Fill in the rest of the request fields according to your security provider's instructions.
 - c. Click the Create CSR button; a textual certificate signing request is displayed in the area below the button:

 Certificate Signing Request 				
Subject Name [CN]	audio.com			
Organizational Unit [OU] (optional)	Headquarters			
Company name [O] (optional)	Corporate			
Locality or city name [L] (optional)	Poughkeepsie			
State [ST] (optional)	New York			
Country code [C] (optional)	US			
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.				
nLnQpVCmbdva/B1QyEpPbQhZqpULJ8CSeSrrY3ru23AZeDUbYyhO901kRbAp//+3 ZvnZZe5M5CBSLg== END CERTIFICATE REQUEST				

Figure 34-12: Certificate Signing Request Group

6. Copy the text and send it to the certificate authority (CA) to sign this request.

Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate rename this file to "device.crt"
- Root certificate rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

-----BEGIN CERTIFICATE-----

MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQ QGEwJGUJETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2Vyd Glwb3N0ZSBTZXJ2ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4 MDAwMFowPzELMAkGA1UEBhMCRIIxEzARBgNVBAoTCkNlcnRpcG9zdGUxG zAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZlhvcNAQE BBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkonWnNm`+Yhb7+ 4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv1 7uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJgHYez YHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==

-----END CERTIFICATE-----



- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above.

Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

- > To update the device with the new certificate:
- In the Certificates page, scroll down to the Upload certificates files from your computer group, click the Browse button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click Send File.
- 2. After the certificate successfully loads to the device, save the configuration with a device restart (Step 6: Reset Device to Apply the New Configuration on page 327 below).

Step 4: Update Device's Trusted Certificate Store

For the device to trust a whole chain of certificates you need to combine the contents of the root.crt and ca.crt certificates into a single text file (using a text editor).

> To update the device with the new certificate:

- **1.** Open the root.crt file (using a text-based editor, e.g., Notepad).
- 2. Open the ca.crt file (using a text-based editor, e.g., Notepad).
- **3.** Copy the content of the ca.crt file and paste it into the root.crt file above the existing content.

Below is an example of two certificate files combined (the file "ca2.crt" and the "root.crt") where the ca2.crt file contents are pasted above the root.crt file contents:

----BEGIN CERTIFICATE-----

MIIDNjCCAh6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx

ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw

9w8BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5Ugxf1PjJeNggwn1QiUYhOKkPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/0fmXKHw1PIIbovWpZddgz8U1pEzD+SeGMUwCnqw99rbUseAHdwkxsXtOquwqE4ykihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cu5B6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOv1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Va1stIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/MIkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWoG6g5Ugxf1PjJeNggwn1QiUYhOKKPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/0fmXKHW1PIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4yk1hiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKKR4cu5B6wYNPoTjJX5OXgd9Yf+0IQYB2EIP06uzLt1yWL3AENGwDVeOv1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsyyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOSGafrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+KNOSIqgVwSZISCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0NtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNfQ0EyMIIBIjANBgkqhkiG
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/0fmXKHW1PIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4ykihiWesMp54LwX5dUB46GWKUFT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cu586wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLt1yWL3AENGwDVeOv1fZgppLEZPBKIhFULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+cNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0RUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/OfmXKHW1PIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4ykihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cuSB6wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLt1yWL3AENGwDVeOv1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZ6jJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAA0CAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0RUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END_CERTIFICATEBEGIN_CERTIFICATE	9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggwnlQiUYhOK
0fmXKHW1PIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4ykihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu5B6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOv1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0hlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0RUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	0fmXKHW1PIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4ykihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cu5B6wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLt1yWL3AENGwDVeOv1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctwvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAA0CAQEAdASYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+cNV5Ya1st1z7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG00KUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6Cccj6oHGLq8RInda==END_CERTIFICATEBEGIN_CERTIFICATE	kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/
<pre>ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cu SB6wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVe0vlfZgppLEZPBKI hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQAB030weDAM BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNV HSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAA0CAQEAdAsYyfcg TdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+ CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yikb4B0hlCq hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0 RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6Cc Cj6oHGLq8RIndA==END_CERTIFICATE</pre>	<pre>ihiWesMp54LwX5dUB46GWKUFT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu SB6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI hfULeMjay4fzE4Xn59LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQlyZrvN4GifsXUB7AvctWvrTBJBgNV HSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcg TdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+ CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0NNhjLDUoLre1GDC00yiKb4B0hlCq hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGO RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6Cc Cj6oHGLq8RIndA==END CERTIFICATEEND CERTIFICATE</pre>	0fmXKHWlPIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4yk
SB6wYNPoTjJXS0Xgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQbO5b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0hlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	SB6wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLt1yWL3AENGwDVe0v1fZgppLEZPBKIhfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5t16nEJQ/7SLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb0Sb0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAA0CAQEAdASYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0hlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0RUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj90gKkR4cu
hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGuOnNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQbOSb0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsyyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0NNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	5B6wYNPoTjJX50Xgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI
BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQb0Sb0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0NNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJG0RUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPc1m9L/M1kVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNVHSMEQjBAgBThf6GbMQbO5b0CkLV8kW+Rg0AAhqE1pCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOSGafrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNY1uYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+VCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM
HSMEQjBAgBThf6GbMQbOSb0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdASYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0hlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VCoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END_CERTIFICATE	HSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WF0S6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0h1CqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END_CERTIFICATEBEGIN_CERTIFICATE	BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNV
MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC00yiKb4BOhlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END_CERTIFICATE	MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdASYyfcgTdkF/uDx10Gk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5Ya1stIz7BDIEIjTzCDrp09sUsiHqxGu0nNhjLDUoLre1GDC00yiKb4B0hlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	HSMEQjBAgBThf6GbMQb05b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM
TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC00yiKb4BOhlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBl0+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATE	TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC00yiKb4BOhlCqhiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHH0yDEKJGORUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+VXoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6CcCj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE	MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcg
CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhlCq hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBlO+np/08F+P551uH0iOYA6Cc Cj6oHGLq8RIndA== END CERTIFICATE	CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhlCq hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6Cc Cj6oHGLq8RIndA== END CERTIFICATE	TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+
<pre>hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0iOYA6Cc Cj6oHGLq8RIndA==END CERTIFICATE</pre>	<pre>hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcs0WtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0iOYA6Cc Cj6oHGLq8RIndA==END CERTIFICATEBEGIN CERTIFICATE</pre>	CNV5YalstIz7BDIEIjTzCDrp09sUsiHqxGuOnNhjLDUoLre1GDC00yiKb4BOhlCq
RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBl0+np/08F+P551uH0iOYA6Cc Cj6oHGLq8RIndA== END CERTIFICATE	RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBl0+np/08F+P551uH0i0YA6Cc Cj6oHGLq8RIndA== END CERTIFICATE BEGIN CERTIFICATE	hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO
<pre>XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0iOYA6Cc Cj6oHGLq8RIndA==END CERTIFICATE</pre>	XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEB10+np/08F+P551uH0i0YA6Cc Cj6oHGLq8RIndA== END CERTIFICATE BEGIN CERTIFICATE	RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V
Cj6oHGLq8RIndA==	Cj6oHGLq8RIndA== END CERTIFICATE BEGIN CERTIFICATE	XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBl0+np/08F+P551uH0i0YA6Cc
END CERTIFICATE	BEGIN CERTIFICATE	Cj6oHGLq8RIndA==
	BEGIN CERTIFICATE	END CERTIFICATE
BEGIN CERTIFICATE		BEGIN CERTIFICATE

 $\tt MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx$

 ${\tt ETAPBg} NV {\tt BAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw}$

MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhnUQrS
667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+7/q
ebESJyW8pTLTszGQns2E214+U18sKHItpUZvs1dVUIX6xQiSYFDG1CDIPR5/70pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOIp6LR72Ta9HMJFJ4gyxJPUQA
jV3Led2Y4JObvBTNlka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPUf1wRjDWgl4G
BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9lXI/HQkKRSTf8CAwEAAaN6MHgw
DAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAIYwSQYD
VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBAoTA0FD
TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggEBAHqkg4F6
wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFCz1q4QVpQNYAwdBdEAKENznZttoP3aPZE
3EOx1C8Mw2wU4p0xD7B6pH0X0+oJ4LrxLB3SAJd5hW495X1RDF99BBA9eGUZ2nXJ
9pin4PWbnfc8eppq8Tpl8jJMW0Zl3prfPt012q93iEalkDEZX+wxkHGZEqS4ayBn
8bU3NHt5qh0Egpai8hB/nth1xnA1m841wxCbJW86AMRs2NznROyG695InAYaNlIo
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2k9STOpN
itSUgGYwEagnsMU=
END CERTIFICATE



The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

- 4. Save the combined content to a file named "chain.pem" and close the file.
- 5. Open the Certificates page and upload chain.pem file using the 'Trusted Root Certificate Store' field.

Step 5: Configure HTTPS Parameters on Device

Configure HTTPS Parameters on the device (Step 5: Configure HTTPS Parameters on the Device on page 319 above).

Step 6: Reset Device to Apply the New Configuration

This section describes how to apply the new configuration.

- To save the changes and restart the device:
- Reset the device with a save-to-flash for your settings to take effect (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

Cleaning up Temporary Files on OVOC Server

It is highly recommended to cleanup temporary files on the OVOC server after certificates have been successfully installed. This is necessary to prevent access to security-sensitive material (certificates and private keys) by malicious users.

> To delete temporary certificate files:

- 1. Login to the OVOC server as user root.
- 2. Remove the temporary directories:

rm -rf /home/acems/server_certs rm -rf /home/acems/client_certs

35 Transferring Files

This appendix describes how to transfer files to and from the OVOC server using any SFTP/SCP file transfer application.



> To transfer files to and from the OVOC server:

- 1. Open your SFTP/SCP application, such as WinSCP or FileZilla.
- 2. Login with the acems/acems credential (all files transferred to the OVOC server host machine are then by default saved to /home/acems directory).
- **3.** Copy the relevant file(s) from your PC to the host machine (or vice-versa). For example, using the FileZilla program, drag the logs.tar file from the /home/acems directory on the OVOC server host machine pane to your PC directory pane.



Figure 35-1: FileZilla

36 Verifying and Converting Certificates

This appendix describes how to verify that certificates are in PEM format and describes how to convert them from DER to PEM format if necessary.

> To verify and convert certificates:

- 1. Login to the OVOC server as user root.
- 2. Transfer the generated certificate to the OVOC server.
- **3.** Execute the following command on the same directory that you transfer the certificate to verify that the certificate file is in PEM format:

Openssl x509 -in certfilename.crt -text -noout

- 4. Do one of the following:
 - **a.** If the certificate is displayed in text format, then this implies that the file is in PEM format, and therefore you can skip the steps below.
 - b. If you receive an error similar to the one displayed below, this implies that you are trying to view a DER encoded certificate and therefore need to convert it to the PEM format.

unable to load certificate 12626:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_ lib.c:647:Expecting: TRUSTED CERTIFICATE

5. Convert the DER certificate to PEM format:

openssl x509 -inform der -in certfilename.crt -out certfilename.crt

.

37 Self-Signed Certificates

When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

Mozilla Firefox

When you are prompted with a message that the web page that you are trying to open using Mozilla Firefox is insecure, do the following:

- **1.** Click the "I Understand the Risks" option.
- 2. Click the Add Exception button, and then click the Confirm Security Exception button.

Figure 37-1: Mozilla Firefox Settings

This Connection is Untrusted You have asked Firefox to connect securely to 10.4.2.60 connection is secure. Normally, when you try to connect securely, sites will pr are going to the right place. However, this site's identity	k9400, but we can't confirm that your resent trusted identification to prove that you can't be verified.
What Should I Do? If you usually connect to this site without problems, th impersonate the site, and you shouldn't continue. Get me out of here! > Technical Details I Understand the Risks If you understand what's going on, you can tell Firefox you trust the site, this error could mean that someo Don't add an exception unless you know there's a goor identification. Add Exception_	Add Security Exception You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this. Server Location: https://10.4.2.60.9400/EMS-VQ/Main.htmlf Certificate Status This site attempts to identify itself with invalid information. Wrong Site The certificate blongs to a different site, which could mean that someone is trying to impersonate this site. Unknown Identity The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
	Permanently store this exception Confirm Security Exception Cancel

Google Chrome

When you are prompted with a message that the web page that you are trying to open using Google Chrome is insecure, do the following:

1. Click Advanced and then click the "Proceed to <Server IP> (unsafe)" link.

Figure 3	17-2.	Chrome	Browser	Settings
rigule a	<i>)/-</i> 2.	CIIIOIIIE	DIOWSEI	Jettings

Yo	ur connection is not private	
Atta pass	:kers might be trying to steal your information from 172.17.11 words, messages, or credit cards). Learn more	8.146 (for examp
NET:	ERR_CERT_AUTHORITY_INVALID	
i i	Ielp improve Chrome security by sending <u>URLs of some pages you visit.</u> formation_and_some_page_content to Google. <u>Privacy_policy</u>	limited system
		_

Microsoft Edge

When you are prompted with a message that the web page that you are trying to open using Microsoft Edge is insecure, do the following:

Click **Details** and then click the link **Go on to the webpage**.

Figure 37-3: Microsoft Edge Browser

Image: Certificate error: Naviga × + ∨		
← → Ů ⋒ A Certificate error https://10.3.180.17/web-ui-ovoc/		
	This site is not secure	
	This site is not secure	
	This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.	
	E Go to your Start page	



🖻 🕫 🖯 Certificate er	ror: Naviga × + ×
\leftrightarrow \rightarrow O \Leftrightarrow	△ Certificate error https://10.3.180.17/web-ui-ovoc/

This site is not secure

Details

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

🗖 Go to your Start page

Details

Vour PC doesn't trust this website's security certificate. The hostname in the website's security certificate differs from the website you are trying to visit. Error Code: DLG_FLAGS_INVALID_CA DLG_FLAGS_SEC_CERT_CM_INVALID

Go on to the webpage (Not recommended)

38 Datacenter Disaster Recovery

Introduction

This appendix describes the OVOC Disaster Recovery procedure for deployments where OVOC is deployed in two separately geographically located datacenters with two different network spaces, in which minimal impact on the SBC/Gateway and OVOC downtime is desired.



Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

Solution Description

The Disaster Recovery solution is composed of two virtual machines in accordance with the OVOC system requirements (see Hardware and Software Requirements). Virtual Low and Virtual High setups are supported. It is recommended that each OVOC machine will have a VMware High Availability (HA) setup to support local Data Center (DC) HA.

- Both machines should have identical hardware configuration and installed with the exactly same OVOC software version. One of the machines will work as 'Active' and will be constantly up and running. The second machine is defined as 'Redundant'. It should not be turned off and the application should be stopped and always remain off.
- The primary machine backup files should be saved and periodically transferred to the external storage of the standby location.
- If the primary machine fails, the user should run the Disaster Recovery procedure as shown below.



Figure 38-1: Disaster Recovery Between Two DataCenters with VMware HA

Initial Requirements

The following initial requirements need to be adhered to before implementing the Disaster Recovery procedure:

- Both machines should have identical hardware (CPU, Memory, Disk, IO).
- An identical Linux OS (the same DVD), database, and the OVOC software version should be used.
- Identical database passwords need to be configured on both servers.
- Identical OVOC Server Manager settings must be configured on both servers (e.g., HTTP/HTTPS communication, etc.).
- If non-default certificates are used, they must be pre-installed on both servers.
- Both machines should have a valid license per each Machine ID with identical capabilities.
- When upgrading the OVOC server software, both machines should be upgraded. Make sure that redundant machine is not rebooted after the upgrade process and the OVOC application remains closed.

When upgrading OVOC, the backup that was created before the upgrade cannot be used anymore. You should only use the backups created after the upgrade process. For more information on backing up the OVOC server, see OVOC Server Backup Processes on page 190.

Make sure that active server backups are not stored on the server machine.

New Customer Configuration

The procedure below describes the steps for a New Customer configuration.

> To perform a New Customer configuration:

- 1. Install and properly configure both servers.
- 2. Make sure the primary OVOC server is up and running.
- **3.** For each device added and managed by the OVOC server, the following features should be provisioned with both primary and secondary servers' IP addresses:
 - Trap Destination Server
 - Session Experience Manager
 - NTP Server Address

Data Synchronization Process

To save recovery time, it is advised that at the end of the backup, transfer the latest backup files from the primary to the secondary server machine. The data transfer may be performed

automatically using a customer- defined script.

The data transfer is the responsibility of the Enterprise's IT implementation team.

Recovery Process

The procedure below describes the recovery process.

To run the recovery process:

- 1. If the primary machine fails, use the Server Manager to make sure the OVOC application has been closed, before starting the secondary machine recovery process.
- 2. Do not run the OVOC software on the secondary machine at this stage. Just make sure the machine is up and running.
- **3.** Verify that server software version is the same as on the Primary server, by checking the OVOC server Manager title.
- 4. Start the secondary server machine, making sure that all the processes are up and running.
- 5. Make sure that all backup files are in the /data/NBIF directory.
- In OVOC Server Manager, go to the Application Maintenance menu and select the Restore option (OVOC Server Restore on page 192).
- 7. Follow the instructions during the process; you might need to press Enter a few times.
- 8. After the restore operation has completed, you are prompted to reboot the OVOC server.
- 9. If you have installed custom certificates prior to the restore, you must re-install them.
- **10.** Login to the OVOC Web client and verify that there is connectivity and the application is functioning correctly.
- If you are using one or more features which are marked in the table below as 'Not Supported', please provision all the managed devices with a new Management Server IP address.
- **12.** For SBC Fixed and Floating License Pool customers, run the *Update* command for all the managed devices .

See the table below summarizing the features affected byDisaster Recovery functionality.

Table 38-1: Features Affected by Disaster Recovery Functionality

Feature	Status
Management	
Alarms+ NAT communication based on Keepalive traps	Supported

Feature	Status
Fixed License Pool and Floating License	Not Supported
IP Phones Manager Pro: Alarms / Status reports	Not Supported
Advanced Quality Package	-
SBC/Gateway Voice Quality Monitoring	Supported
Endpoint Quality monitoring (RFC 6035)	Not Supported
Server	
Server: Device NTP Server	Supported
Server: Device Syslog Server	Not Supported
Server: Device TP Debug recording server	Not Supported

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

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-94200

