Installation, Operation and Maintenance Manual

AudioCodes One Voice Operations Center

OVOC

Installation, Operation and Maintenance

Version 8.4

OVOC
One Voice Operations Center

audiocodes

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**

Part I **2**

Pre-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
OVOC Capacities 9
Device Manager Communication and Optimization 11
Skype for Business Monitoring SQL Server Prerequisites 12

4 OVOC Software Deliverables **13**

Part II **15**

OVOC Server Installation **15**

5 Files Verification **16**

Windows 16
Linux 16
OVOC Server Users 16

6 Installing OVOC Server on Virtual Machines on Cloud-based Platforms **18**

Launching Public OVOC Image on Amazon Web Services (AWS) 18
Launching Public Image on AWS 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
VMware Cluster Site Requirements 42
Cluster Host Node Failure on VMware 45
Connecting OVOC Server to Network on VMware 45

8 Installing OVOC Server on Microsoft Hyper-V Virtual Machine **48**

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
Part III 80
Post 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 Connection 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
Before Enabling Cloud Architecture Mode 154
Configuring Cloud Architecture Mode (WebSocket Tunnel) 155
Setting up Multiple Ethernet Interfaces 157
Connecting Mediant Cloud Edition (CE) Devices on Azure 159
Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address 160

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
Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface 169

Part IV 171

OVOC Server Upgrade 171

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 Machines 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 Environment 186

Part V 189

OVOC 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

Part VI 197

OVOC Server Manager 197

20 Getting Started 198

Connecting to the OVOC Server Manager 198
Using the OVOC Server Manager 199
OVOC Server Manager Menu Options Summary 199
21 Viewing Process Statuses 203
22 Viewing General Information 206
23 Collecting Full Logs 209
Selected Logs 210
24 Application Maintenance 214
Start or Restart the Application 214
Stop the Application 215
Web Servers 216
License 216
OVOC License 217
analytics API 221
Guacamole RDP Gateway 222
VMware Tools 224
Shutdown the OVOC Server Machine 225
Reboot the OVOC Server Machine 225
25 Network Configuration 227
Server IP Address 228
Ethernet Interfaces 229
Remove Interface 230
Modify Interface 230
Ethernet Redundancy 231
Add Redundant Interface 232
Remove Ethernet Redundancy 233
Modify Redundant Interface 234
DNS Client 234
Static Routes 235
Proxy Settings 238
SNMP Agent 239
SNMP Agent Listening Port 240
Linux System Trap Forwarding Configuration 241
Server SNMPv3 Engine ID 241
NFS 242
26 NTP & Clock Settings 243
NTP 243
Stopping and Starting the NTP Server 246
Restrict Access to NTP Clients 246
Activate DDoS Protection 246
Authorizing Subnets to Connect to OVOC NTP 246

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 267
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) 277
Trust Store Configuration 278
SBC HTTPS Authentication Mode 278
Enable Device Manager Pro and NBIF Web Pages Secured Communication 279
Change HTTP/S Authentication Password for NBIF Directory 279
Disable Client's IP Address Validation 280
Host Header Validation Configuration 280

29 Diagnostics 282

Server Syslog Configuration 282
Devices Syslog Configuration 285
Devices Debug Configuration 286
Server Logger Levels 287
Network Traffic Capture 288

Part VII 291

Configuring the Firewall 291

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

Part VIII 301

Appendix 301

31 Configuring OVOC as the Email Server on Microsoft Azure 302

Configuring Internal Azure Mail Server on Microsoft Office 365 302
Configuring OVOC as the Email Server on Microsoft Azure using SMTP Relay 304

32 Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers 307

RAID-0 Prerequisites 307
RAID-0 Hardware Preparation 307
Configuring RAID-0 307
Step 1 Create Logical Drive 307
Step 2 Set Logical Drive as Bootable Volume 308

33 Managing Clusters 310

Migrating OVOC Virtual Machines in a VMware Cluster 310
Moving OVOC VMs in a Hyper-V Cluster 311

34 Supplementary Security Procedures 315

Installing Custom Certificates on OVOC Managed Devices 315
Gateways and SBC Devices 315
Step 1: Generate a Certificate Signing Request (CSR) 315
Step 2: Receive the New Certificates from the CA 317
Step 3: Update Device with New Certificate 317

Step 4: Update Device's Trusted Certificate Store 318
Step 5: Configure HTTPS Parameters on the Device 319
Step 6: Reset Device to Apply the New Configuration 322
MP-1xx Devices 322
Step 1: Generate a Certificate Signing Request (CSR) 322
Step 2: Receive the New Certificates from the CA 323
Step 3: Update Device with New Certificate 324
Step 4: Update Device's Trusted Certificate Store 324
Step 5: Configure HTTPS Parameters on Device 327
Step 6: Reset Device to Apply the New Configuration 327
Cleaning up Temporary Files on OVOC Server 327
35 Transferring Files 328
36 Verifying and Converting Certificates 329
37 Self-Signed Certificates 330
Mozilla Firefox 330
Google Chrome 330
Microsoft Edge 331
38 Datacenter Disaster Recovery 332
Introduction 332
Solution Description 332
Initial Requirements 333
New Customer Configuration 333
Data Synchronization Process 333
Recovery Process 334

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

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

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

[1] As above

[2] As above

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

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

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 3.2.0 C450HD. ■ From Version 3.2.1: C450HD, 445HD, 430HD 440HD, 405HD,450HD, HRS 457D and HRS 458. ■ From Version 3.4.2: RX50 Conference Phone ■ From Version 1.5: C448HD and C450HD ■ From Version 1.12.33: C435HD ■ From Version 1.8: C470HD ■ From Version 1.9: RXV80 Video Collaboration Bar ■ From Version 1.15: C455HD ■ From Version 1.18: RXV81 Meeting Room Solution ■ From AudioCodes AppSuite Version 1.0.0.0: MTRfW/RXV100 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.

Table 3-1: OVOC Server Minimum Requirements

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

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 7.4 ■ Angular 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.

Table 3-3: Voice Quality Bandwidth Requirements

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

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.

Table 3-4: OVOC Capacities

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server
OVOC Management Capacity				
Managed devices	100	5,000	5,000	10,000
Links	200	10,000	10,000	10,000
Operators	25			
Device Manager Pro				
Managed devices (see Device Manager Communication and Optimization on 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	10 GB		
Alarm and Journal Capacity				
History alarms	Up to 12 months or 10,000,000 million alarms			
Journal logs	Up to 12 months			
Steady state	20 alarms per second			50 alarms per second
Performance Monitoring				
Polled parameters per polling interval per OVOC- managed device	50,000	100,000	100,000	500,000
Polled parameters per polling interval per OVOC instance	50,000	500,000	500,000	1,000,000
Storage time	One year			
QoE Call Flow (for SBC calls only)				
Maximum managed devices with QoE call flows	10	100	100	300
CAPS per OVOC instance	6	25	100	300
Maximum number of calls	1,000,000	1,000,000	1,000,000	10,000,000
OVOC QoE for Devices				
QoE for managed devices	100	1,200	3,000	10,000
CAPS (calls attempts per second) per device	30	120	300	1,000
CAPS per OVOC instance (SBC and SFB/Teams and RFC SIP	30	120	300	1,000

Machine Specifications	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	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 trade-offs between response time and network overhead. Regular monitoring and performance

[1]The TEAMS CAPS estimation is based on round trip delay of 500 milliseconds to Microsoft Azure.
[2]As above
[3]Please contact AudioCodes OVOC Product Manager
[4]For additional support, contact AudioCodes Product Manager

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: OVOC 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)

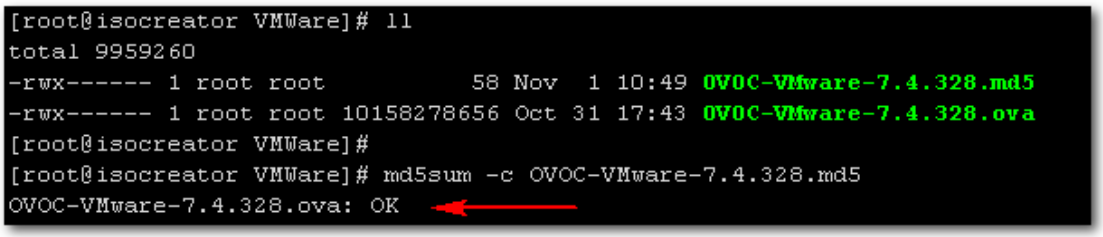
Linux

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



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.

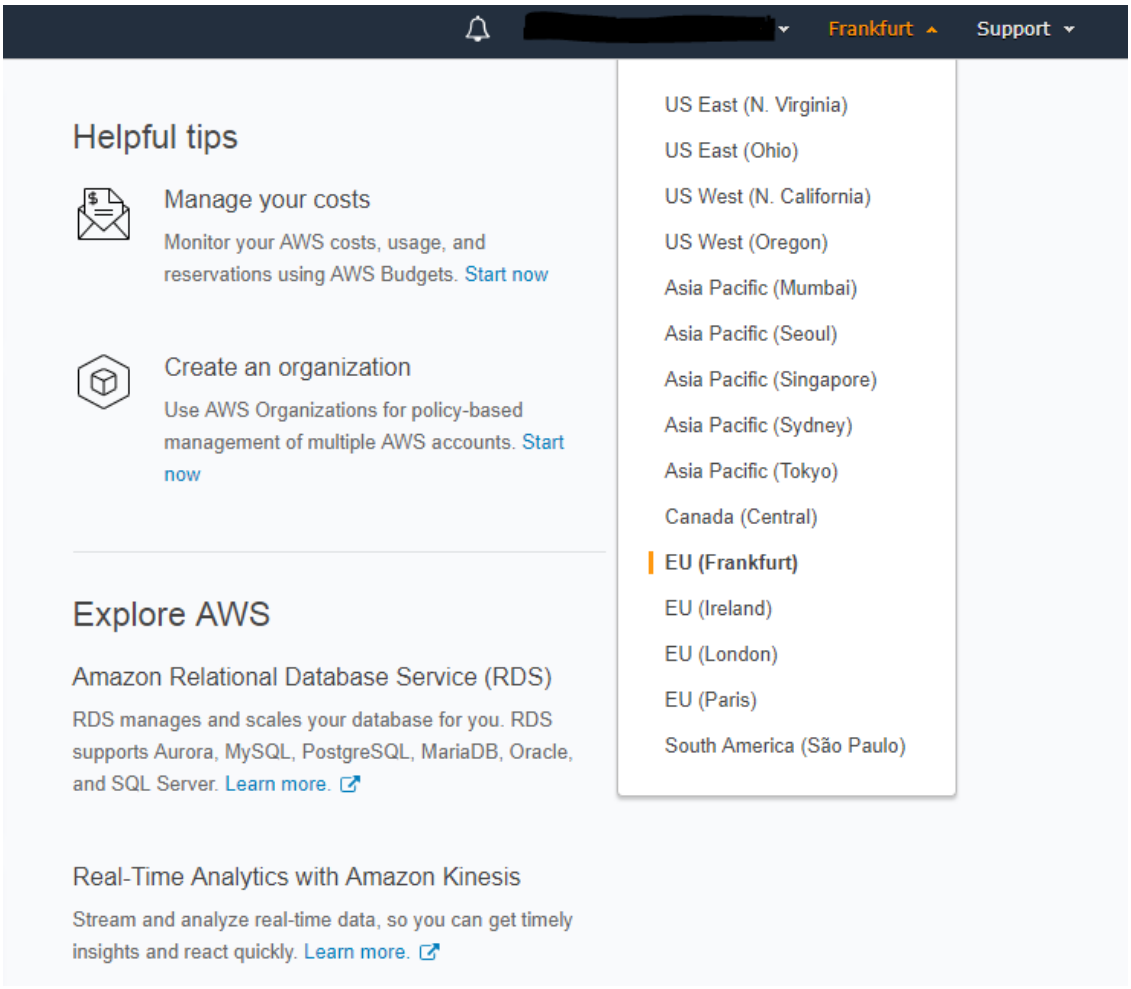
➢ **To setup and load the AWS image:**

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.

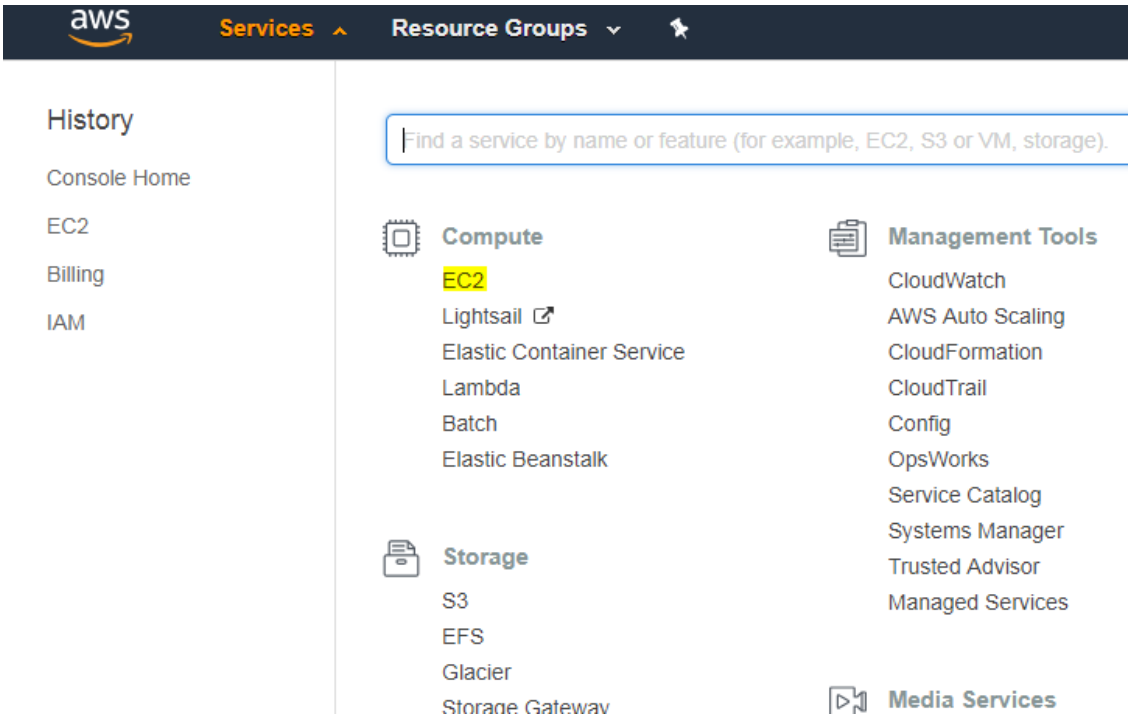
For verifying AMI IDs, refer to https://services.AudioCodes.com..

Figure 6-1: Select Region



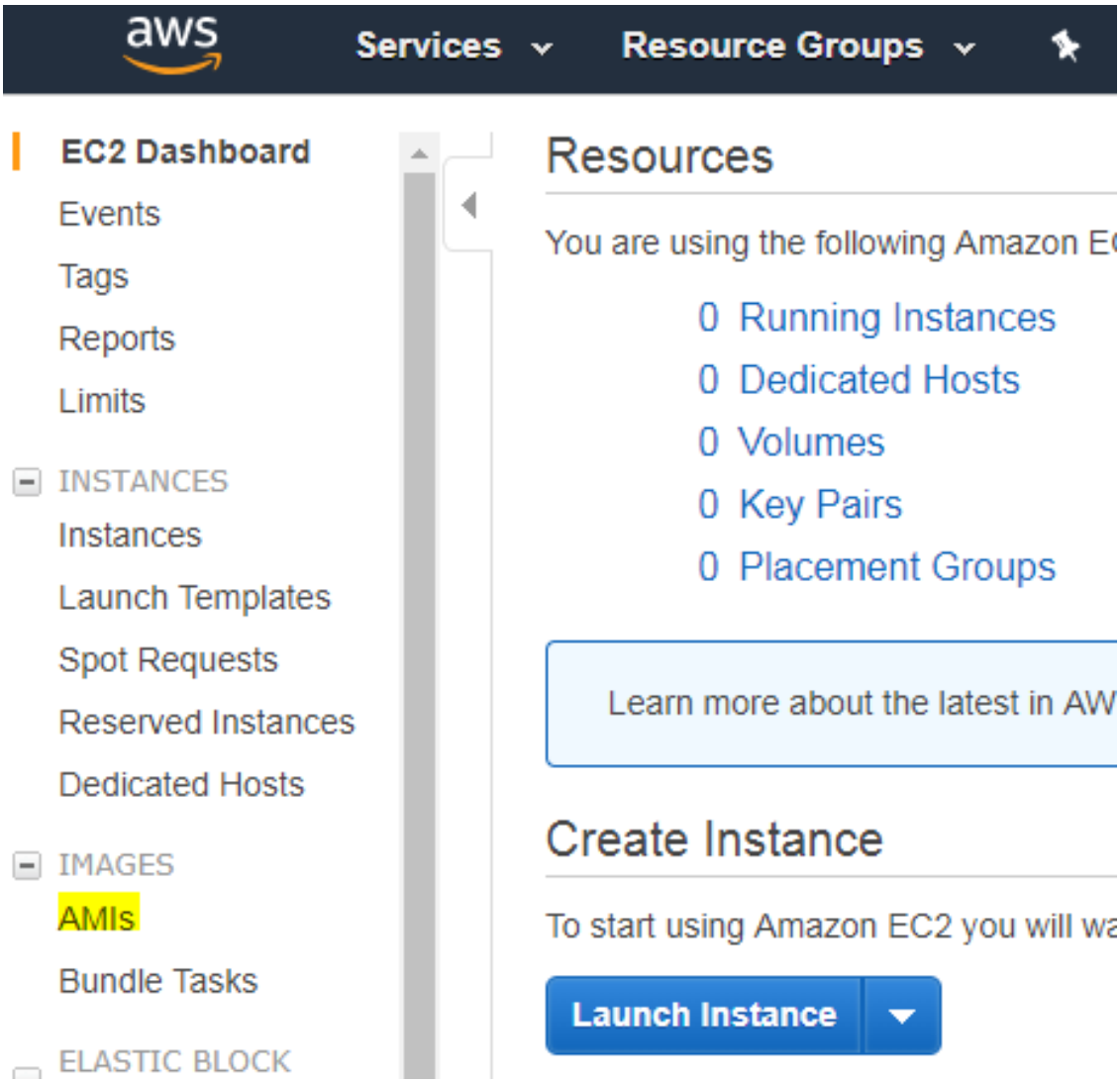
3. In the "Services" menu, choose EC2.

Figure 6-2: Services Menu - EC2



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

Figure 6-3: Images

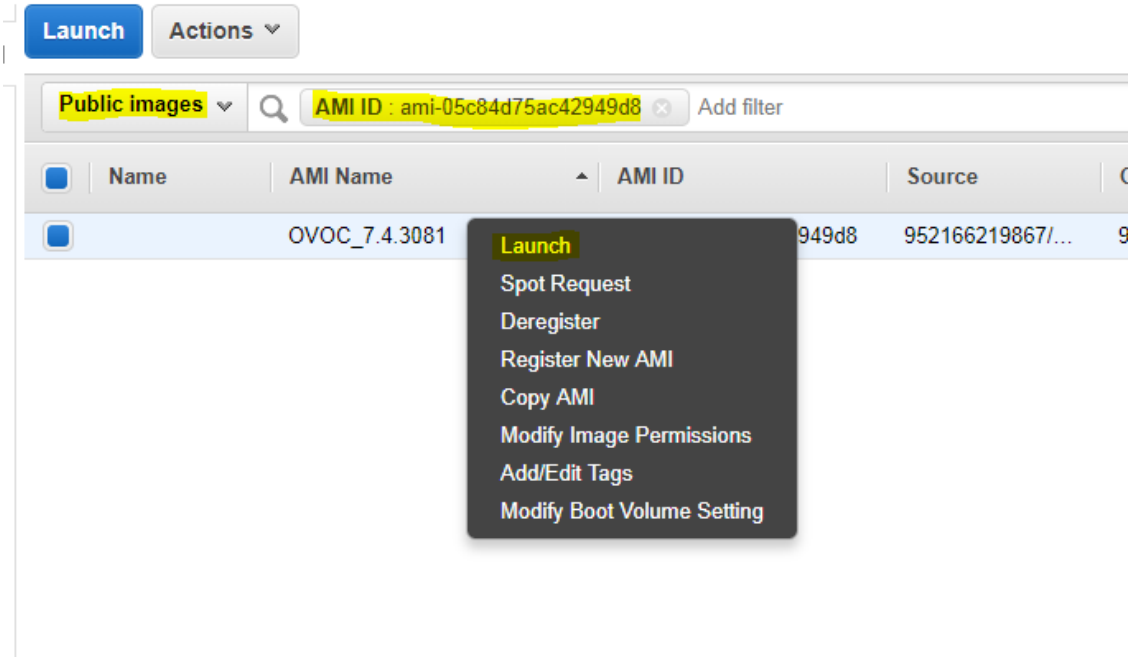


5. In the search bar, choose Public images and apply the following filter:

   AMI ID : ami-00000000000 replacing ami-00000000000 with the AMI ID you received from AudioCodes according to the region you have chosen.

6. Right-click the AMI and choose Launch.

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:

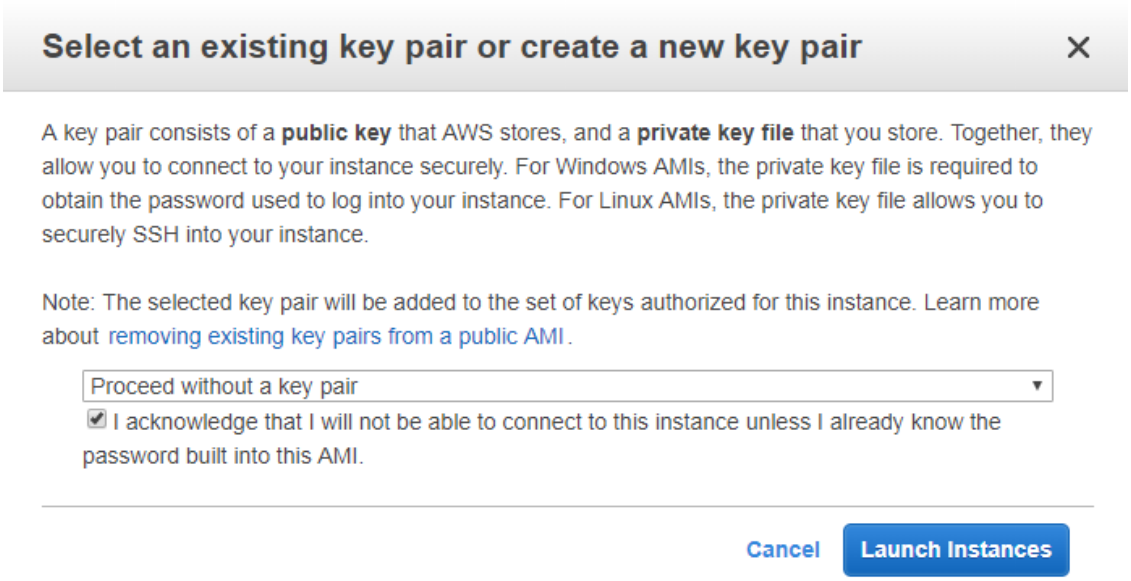
Table 6-1: Firewall for Amazon AWS

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.
TCP	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**.

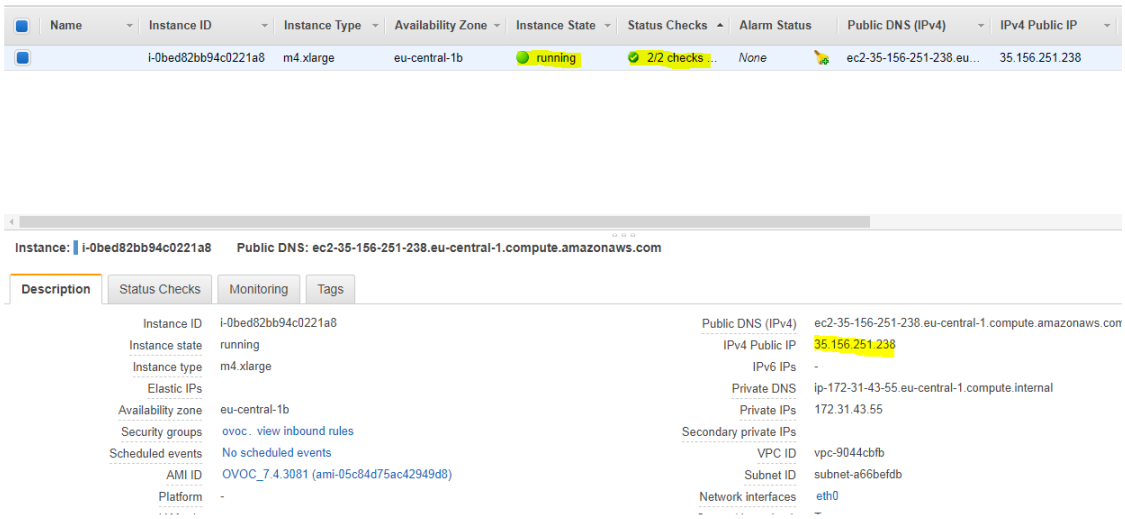
11. In the dialog shown in the figure below, from the drop-down list, choose Proceed without a key pair, check the "I acknowledge …" check box, then click **Launch Instances**.

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.

Figure 6-6: Instance State and Status Checks



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/request- production-access.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.
4. 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
send_via_ses:
driver = manualroute
domains = ! +local_domains
transport = ses_smtp
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
ses_login:
driver = plaintext
public_name = LOGIN
client_send = : AWS_SES_LOGIN : AWS_SES_PASSWORD
==========================================================
begin rewrite
^root@HOSTNAME SOURCE_EMAIL SFfrs
==========================================================
```

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
```

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

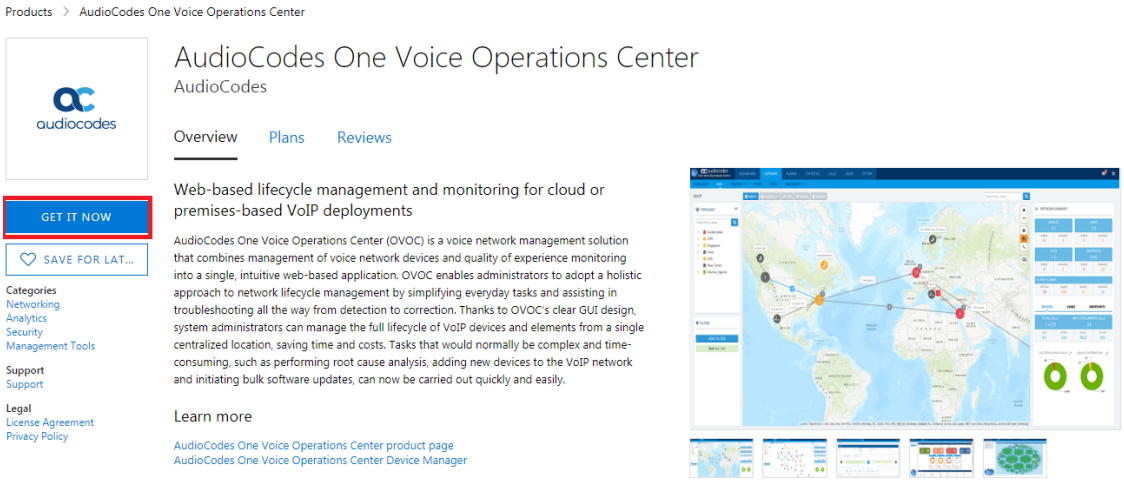
This chapter describes how to install the OVOC server on a virtual machine in a Cloud-based deployment from the Microsoft Azure Marketplace.

- 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:**

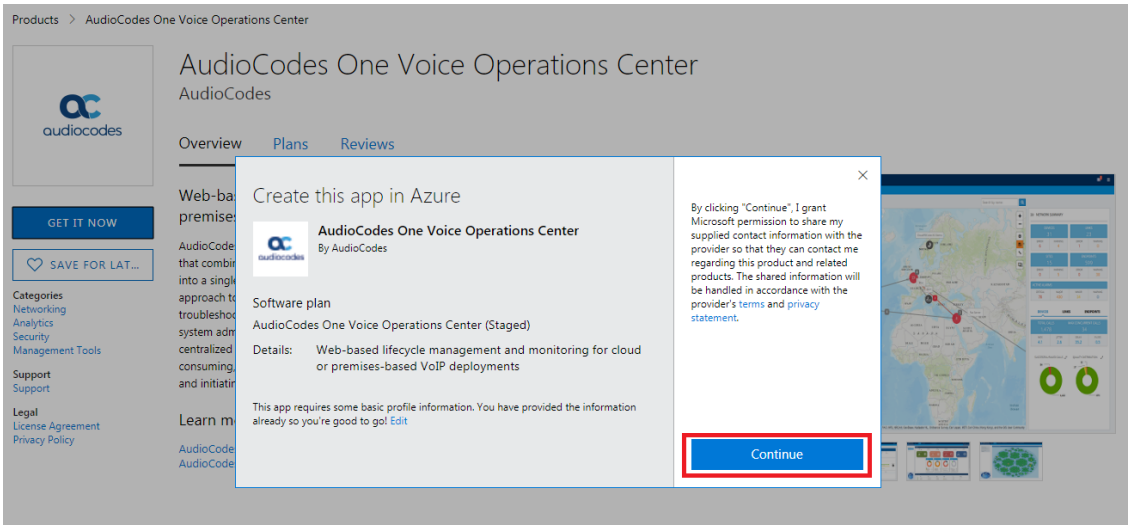
1. In the Azure Marketplace, search for "AudioCodes One Voice Operations Center (OVOC)" and click **Get It Now.**

Figure 6-7: Get it Now



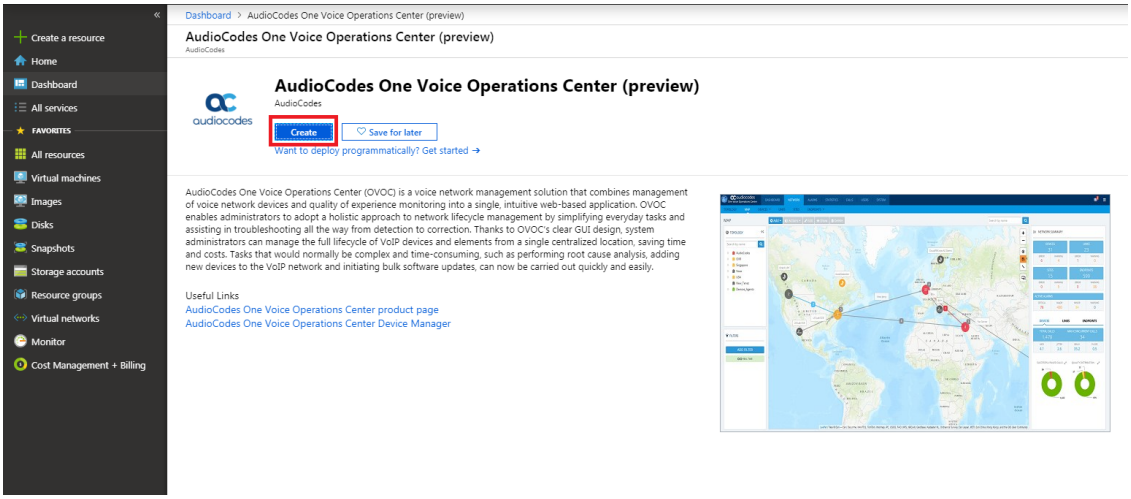
2. Click **Continue.**

Figure 6-8: Create this App in Azure



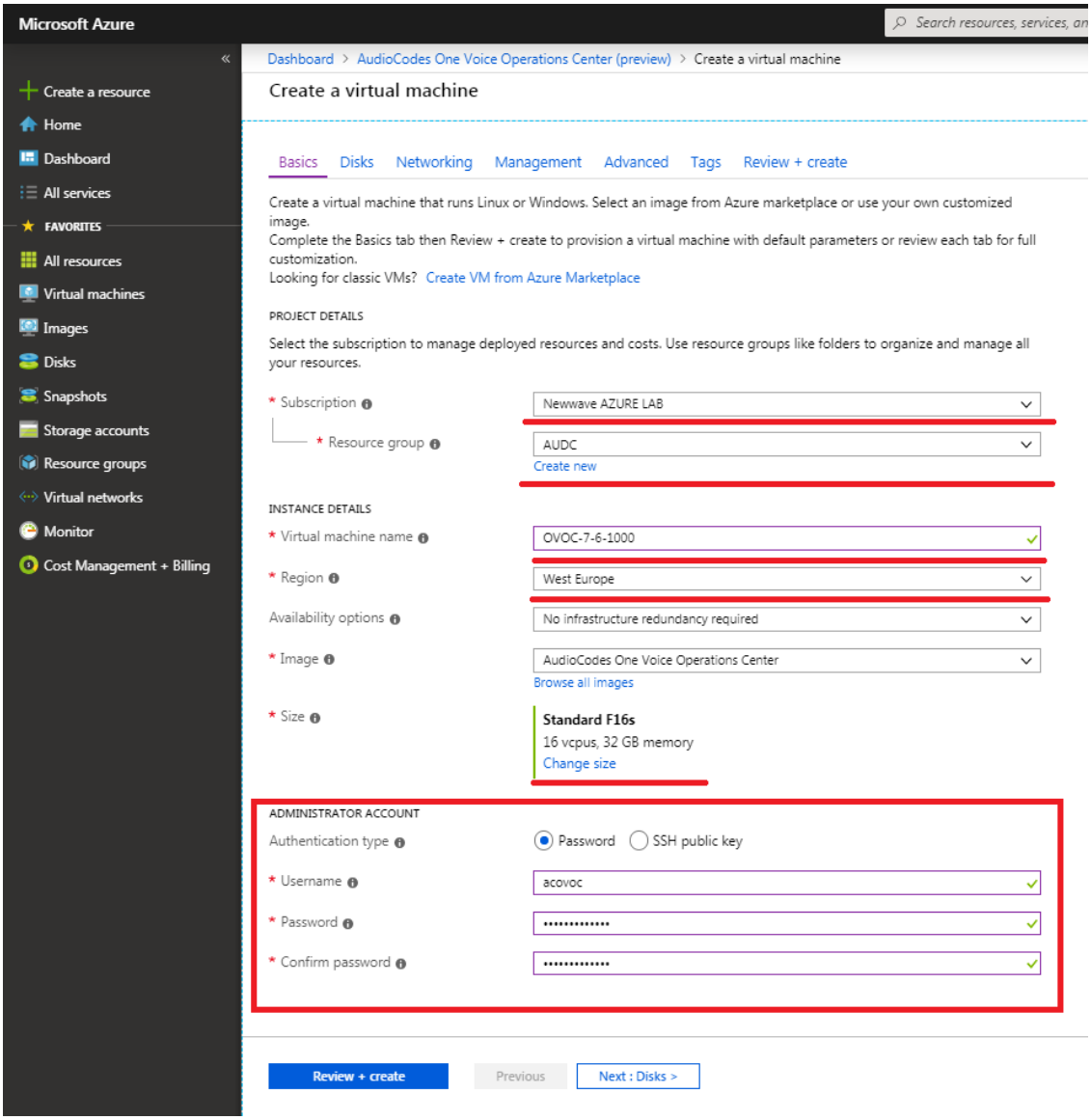
3. You are now logged in to the Azure portal; click **Create**.

Figure 6-9: Create Virtual Machine



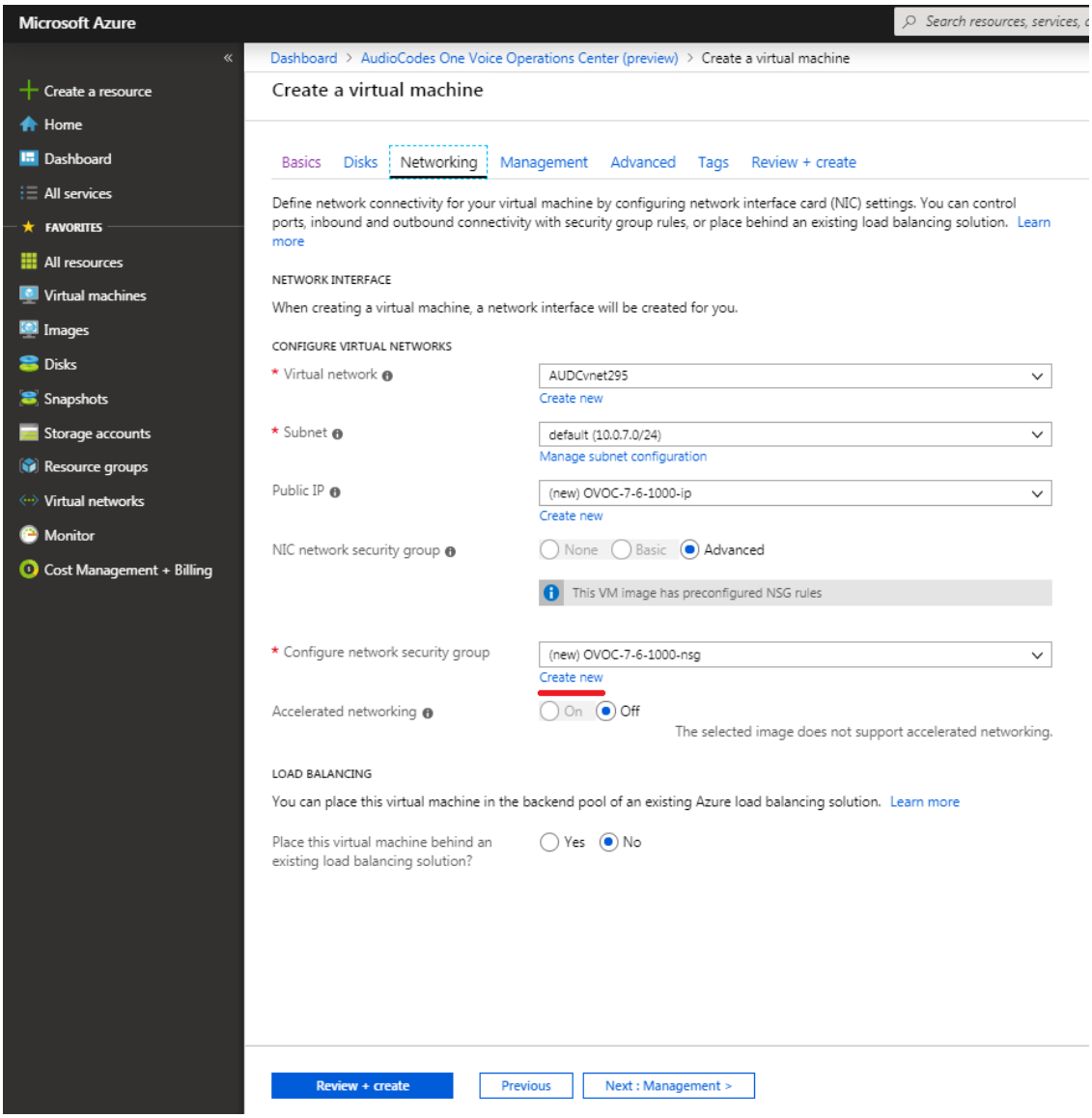
4. Configure the following:
   a. Choose your Subscription.
   b. Choose your Resource Group or create a new one
   c. Enter the name of the new Virtual Machine.
   d. Choose the Region.
   e. Choose the VM Size (see Hardware and Software Requirements).
   f. Choose Authentication Type "Password" and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

Figure 6-10: Virtual Machine Details



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

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.

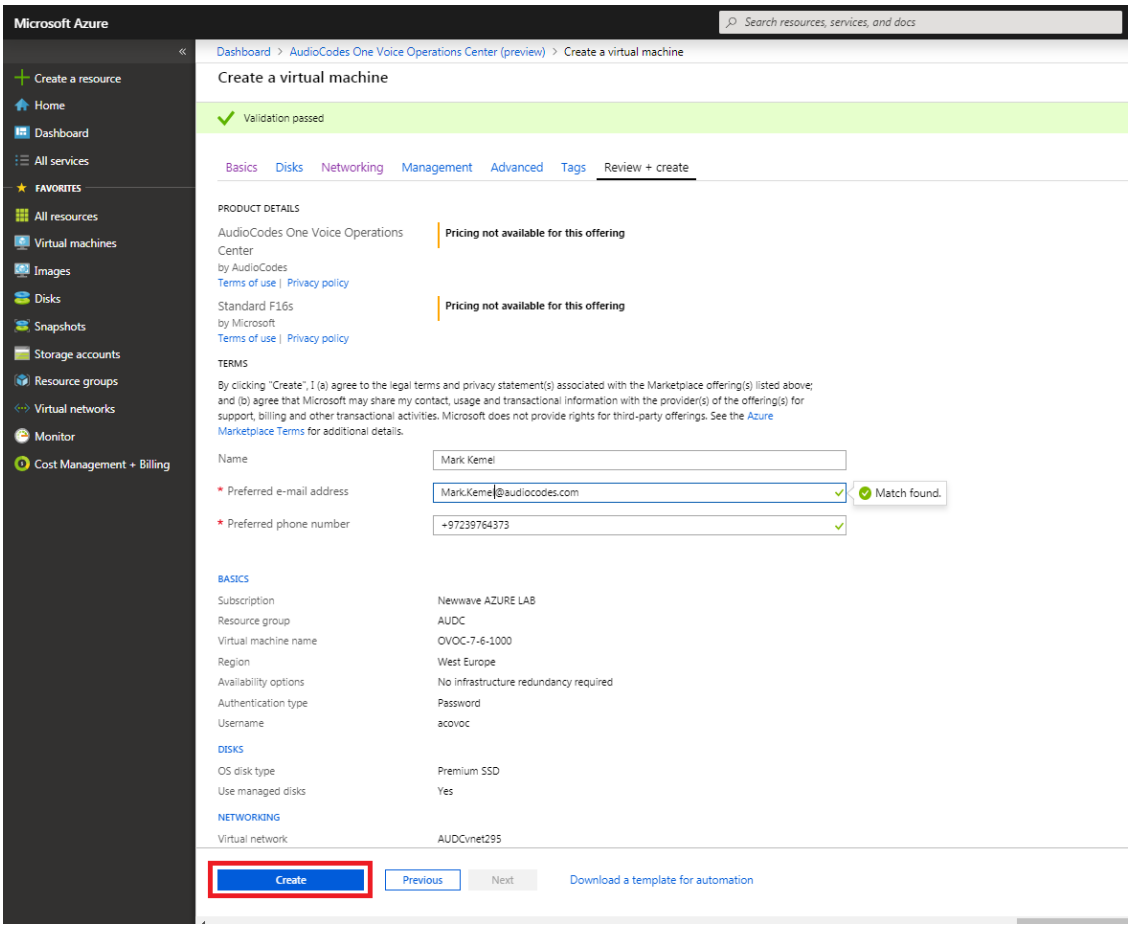
By default, only ports 22 and 443 are open for inbound traffic; open other ports for managing devices behind a NAT (outside the Azure environment) as described in the table below.

Table 6-2: Microsoft Azure Firewall

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
TCP	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 (specifically 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 Edition (CE) Devices on Azure on page 159

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

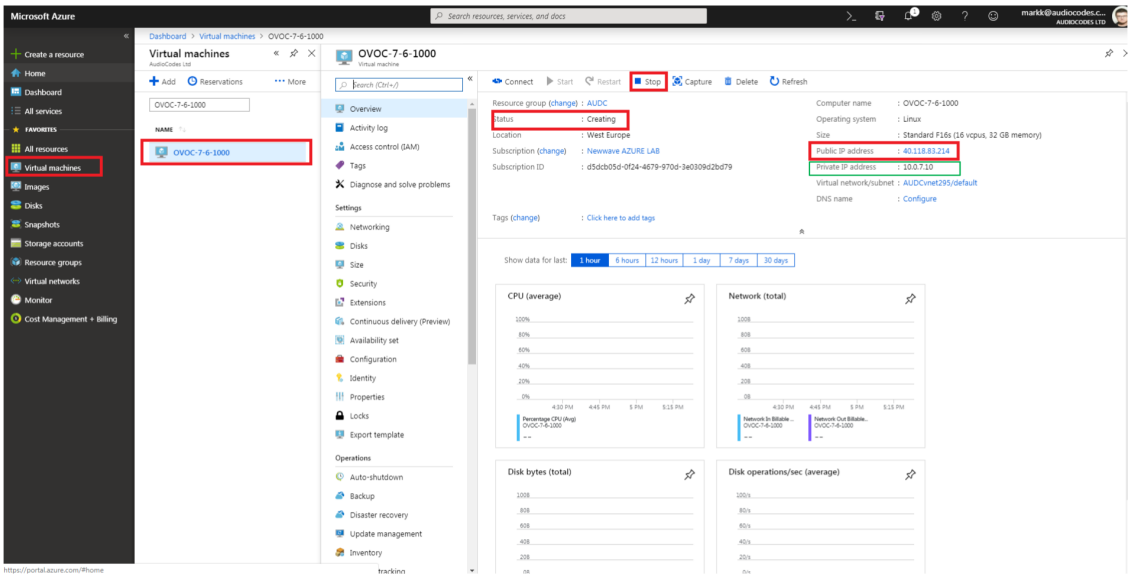
Figure 6-12: Review and Create



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.

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

- 8.0.2546
- 8.0.2555
- 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

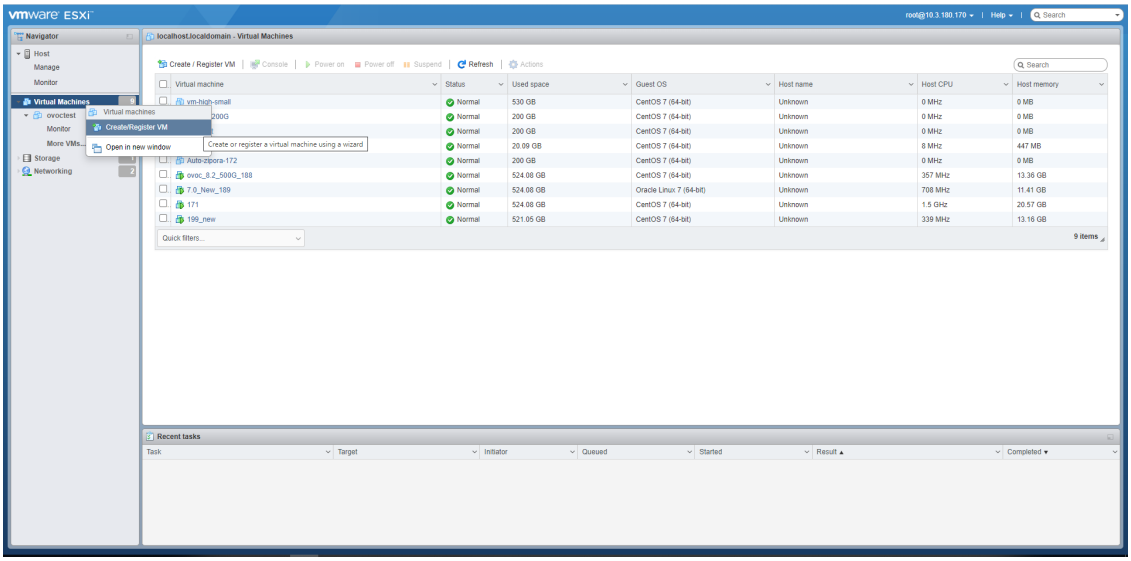
Deploying Standalone VMware VM using ESXi Wizard

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

➢ **To create a VMware VM:**

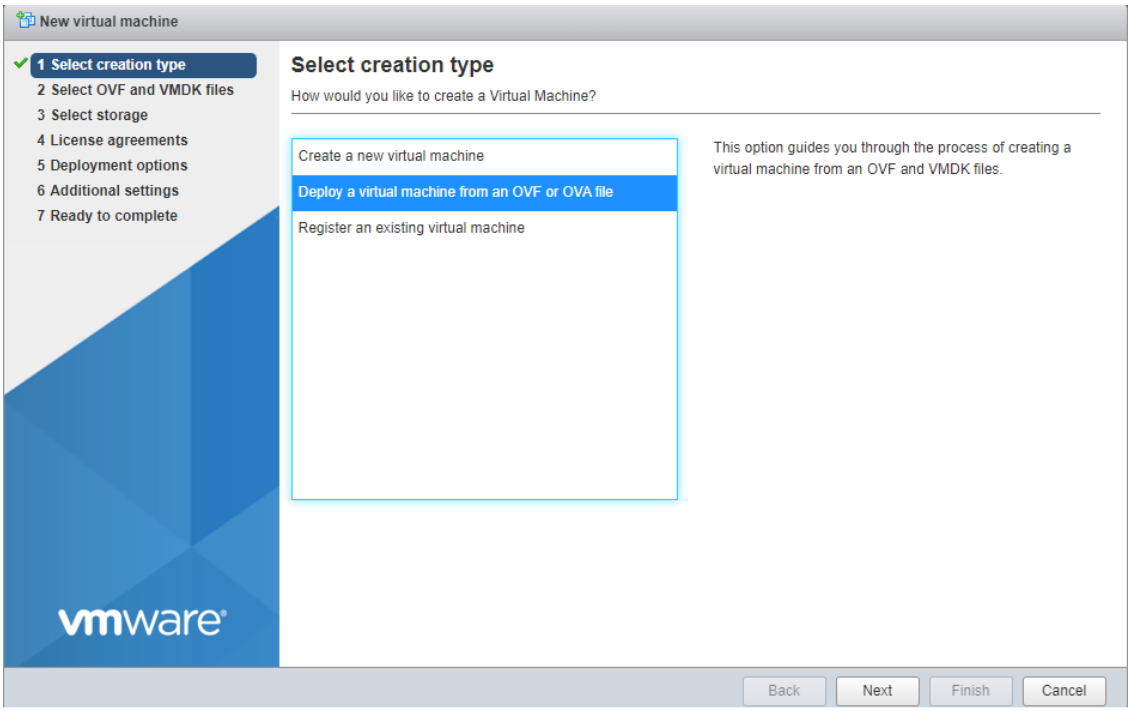
1. Transfer the 7z file containing the VMware Virtual Machine installation package that you received from AudioCodes to your PC (see Transferring Files on page 328 for instructions on how to transfer files).
2. Login to the VMware virtual machine on which you wish to install OVOC.
3. In the Navigation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

Figure 7-1: Create/Register VM



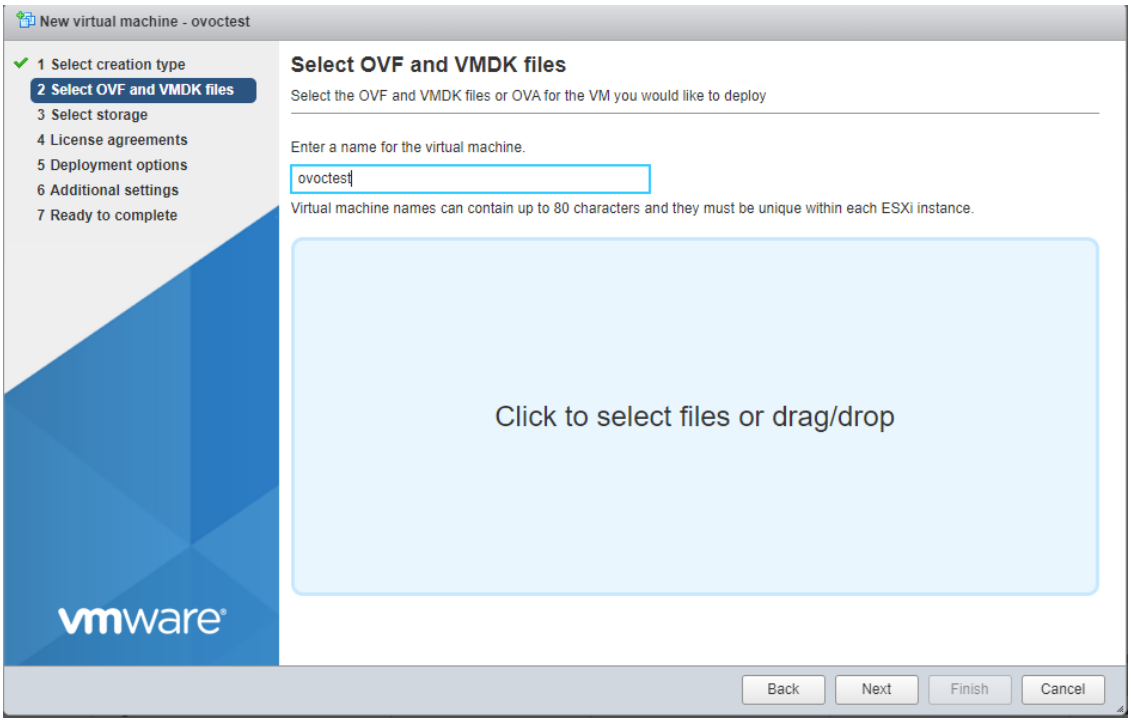
The New virtual machine wizard opens.

Figure 7-2: Select Creation Type



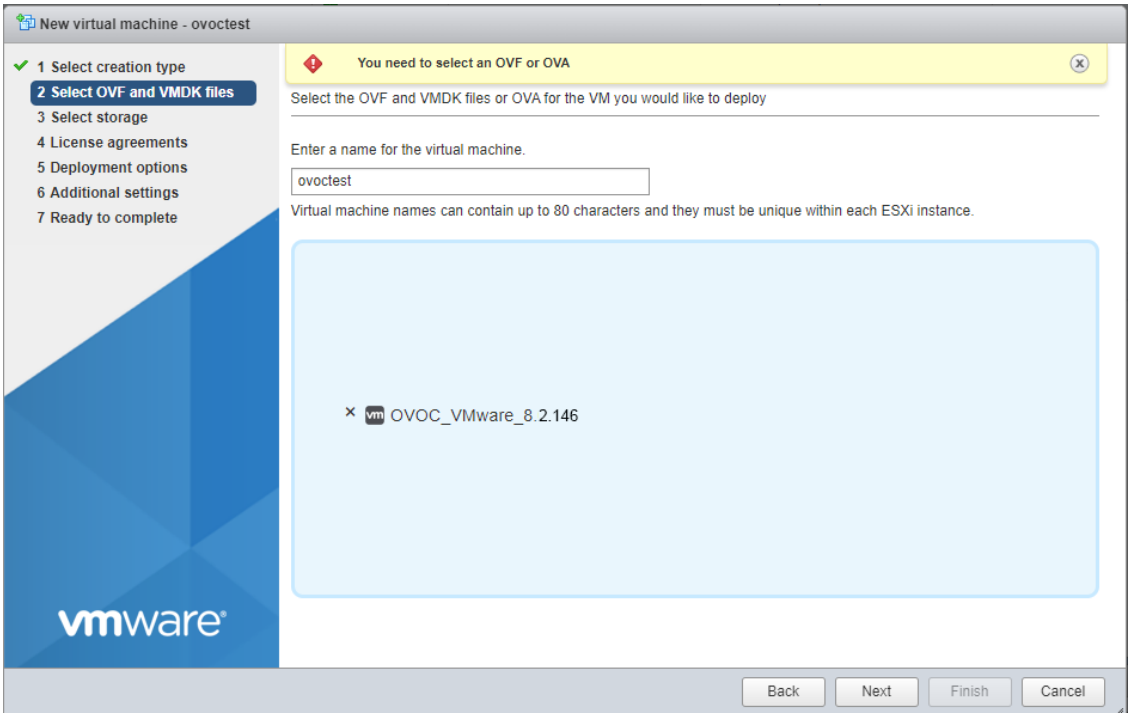
4. Select option **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.

Figure 7-3: OVF and VMDK Files



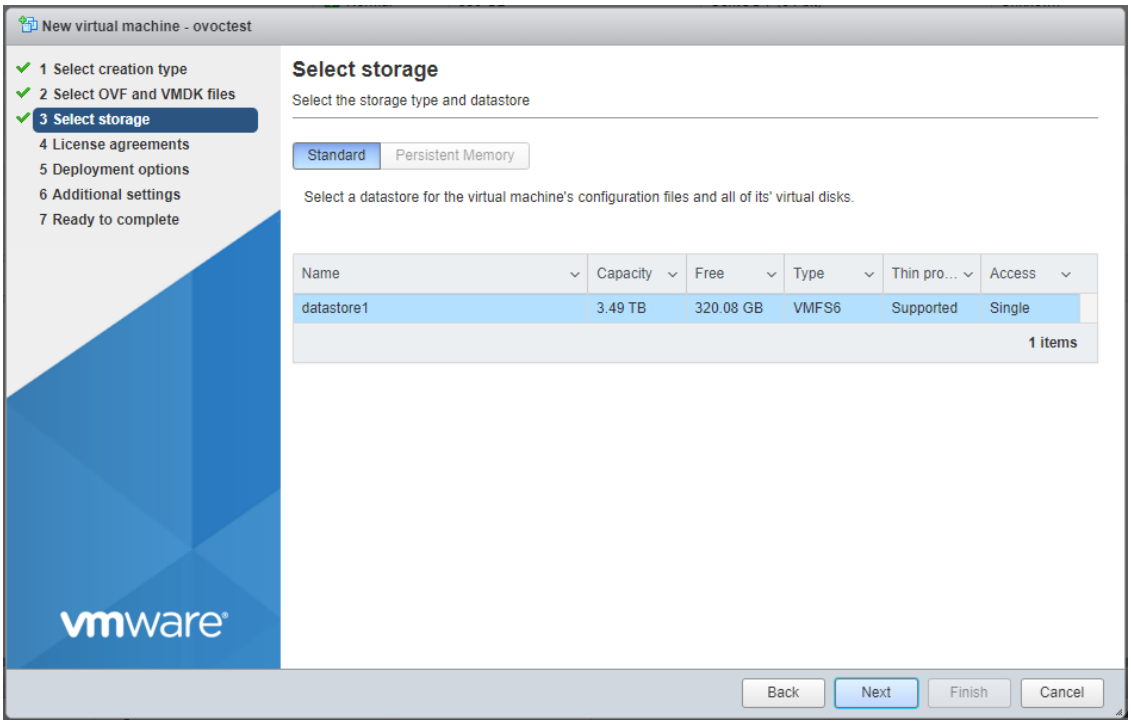
5. Enter the name of the virtual machine.

Figure 7-4: Select OVF or OVA



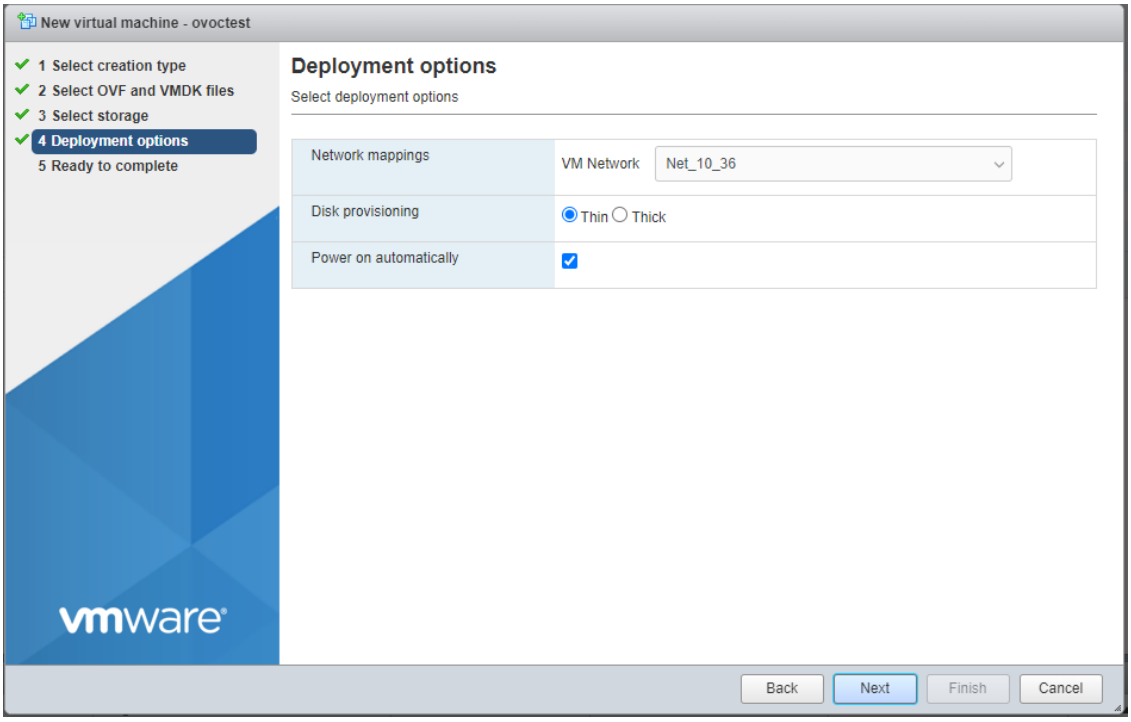
6. Click to browse to the saved location of the OVA file and then click **Next**.

Figure 7-5: Select storage



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

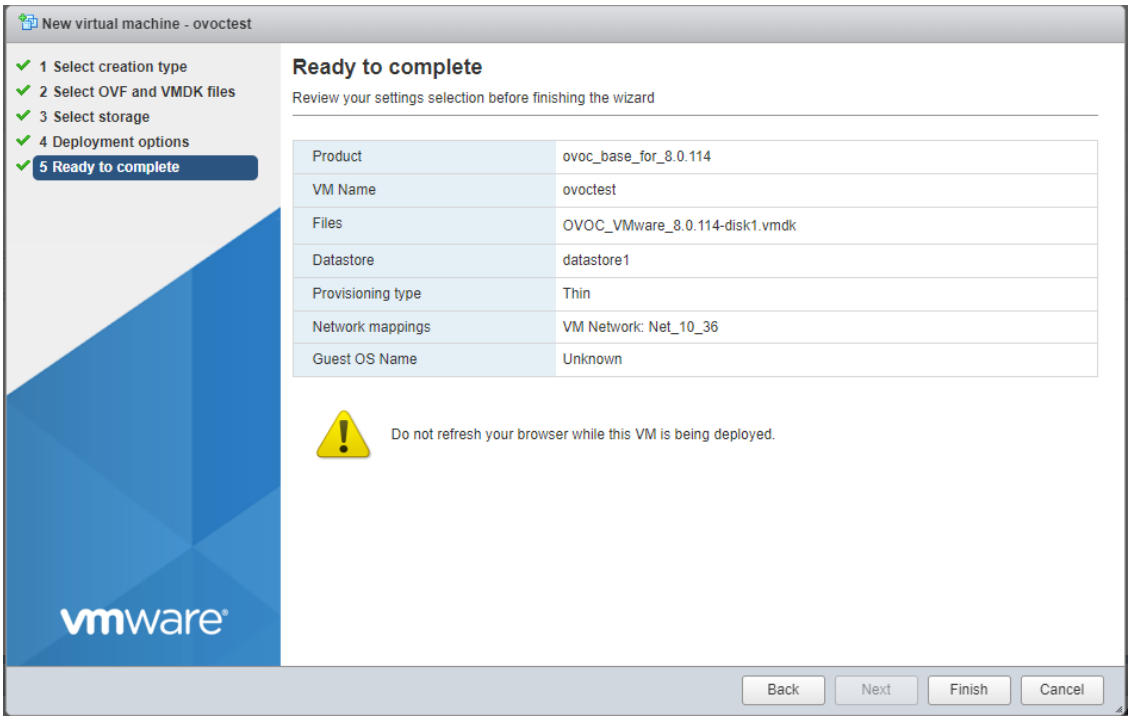
Figure 7-6: Deployment options



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

   The Ready to complete screen is displayed.

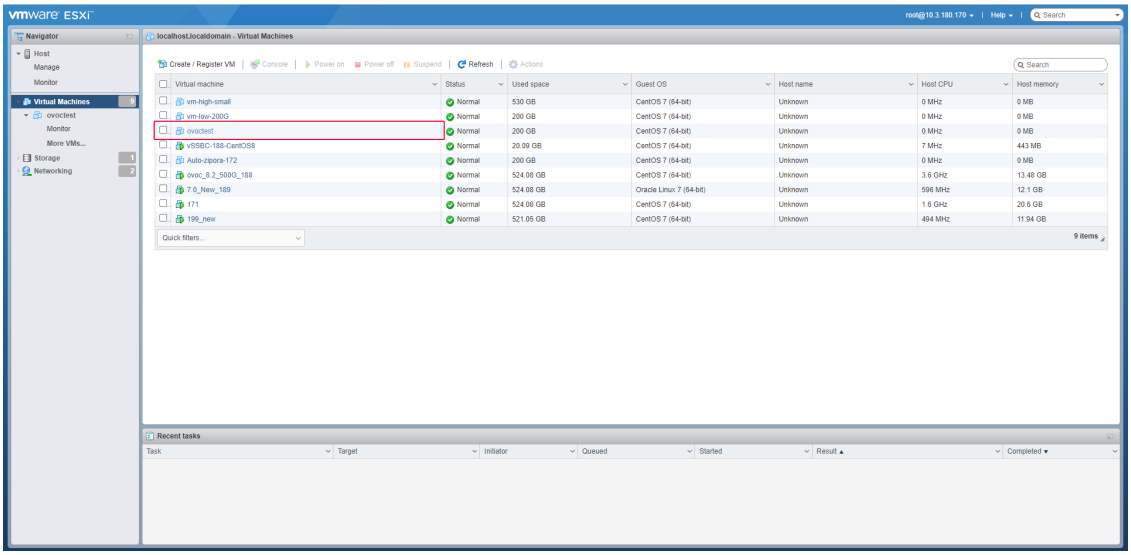
Figure 7-7: Ready to complete



9. Click **Finish**.

The new Virtual Machine is displayed.

Figure 7-8: New Virtual Machine Created



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:

1. 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
```

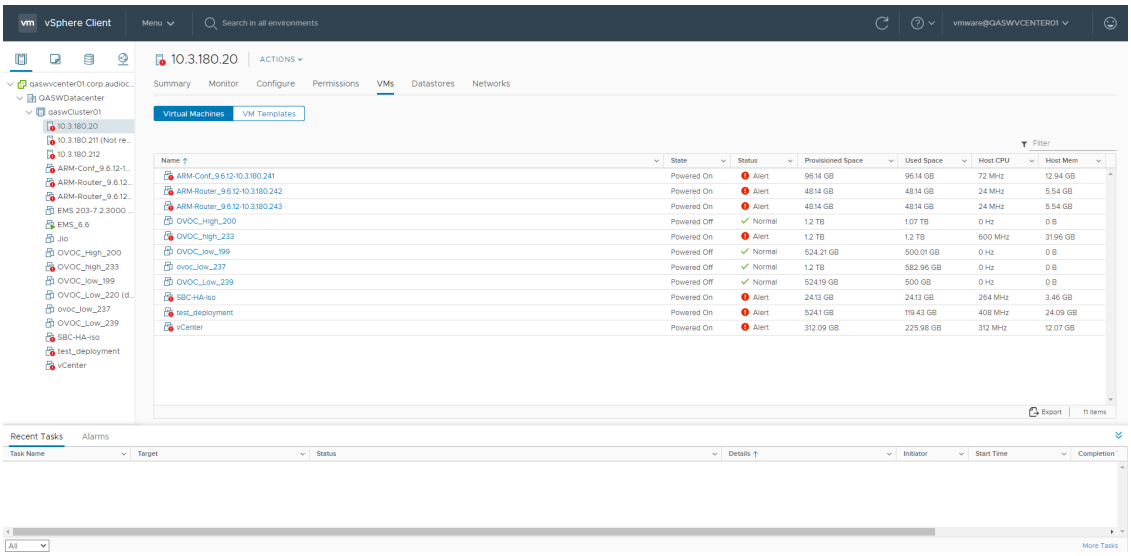
Where:

- $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
```

Figure 7-9: OVF Example



The following progress is displayed:

```
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.

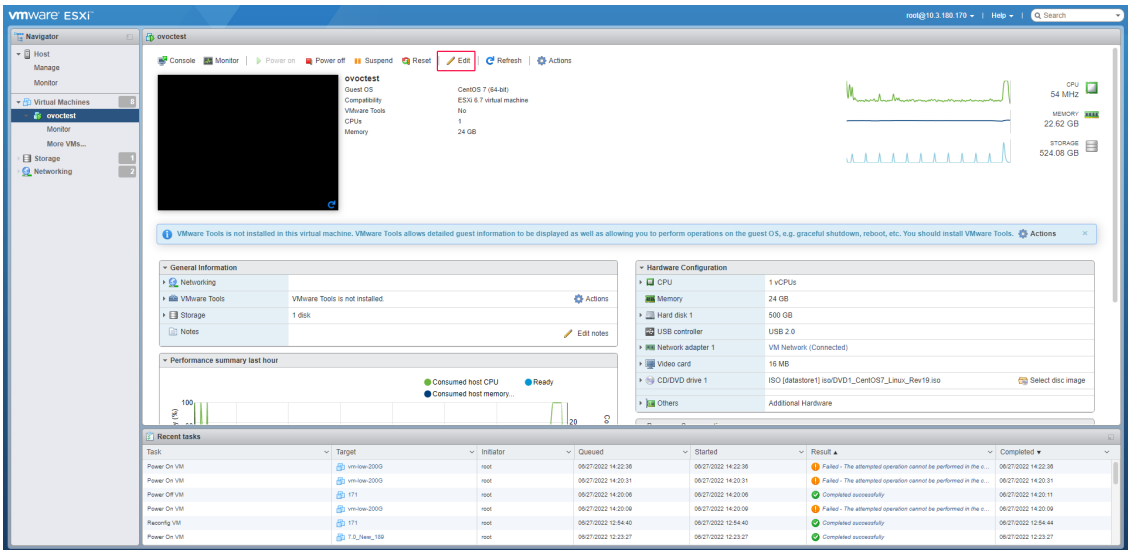
Table 7-1: Virtual Machine Configuration

Required Parameter	Value
Disk size	
Memory size	
CPU cores	

➢ **To configure the virtual machine hardware settings:**

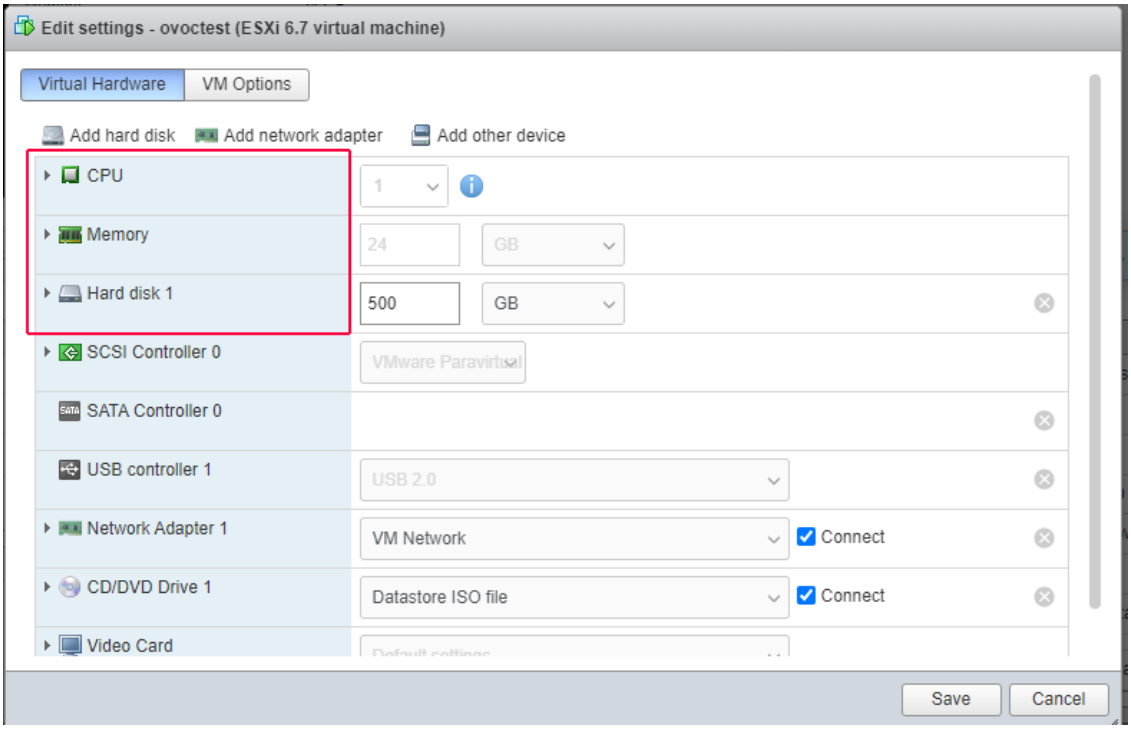
1. Before powering up the machine, go to the virtual machine **Edit Settings** option.

Figure 7-10: Edit Settings option



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**.

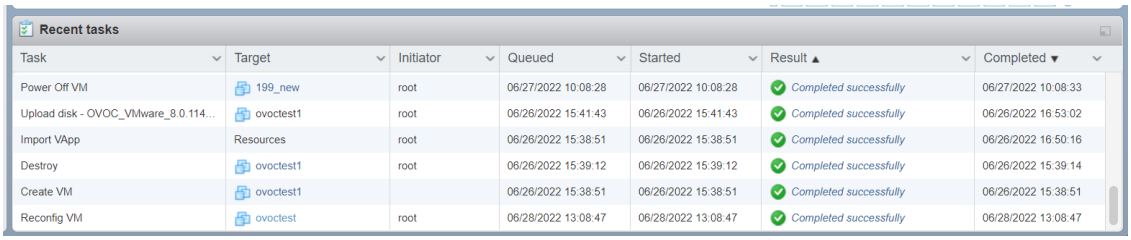
Figure 7-11: CPU, Memory and Hard Disk Settings



- 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



Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

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

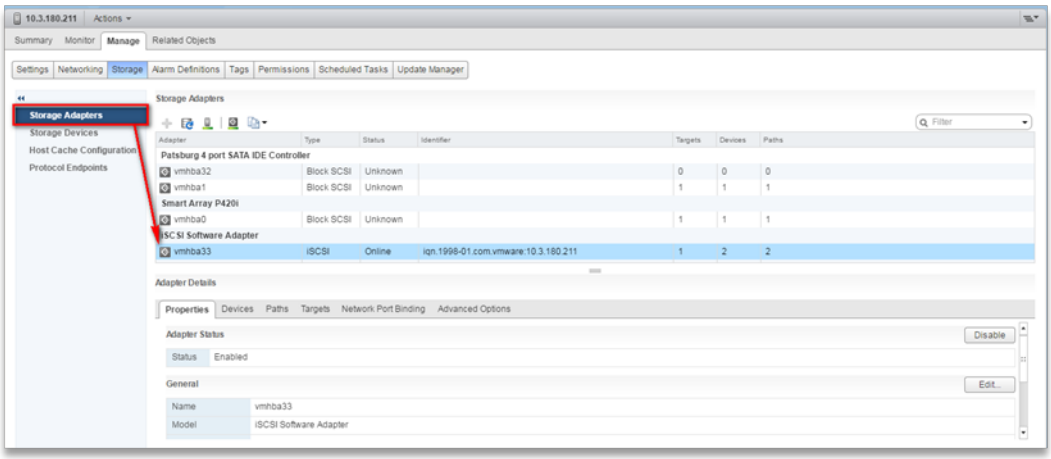
VMware Cluster Site Requirements

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.

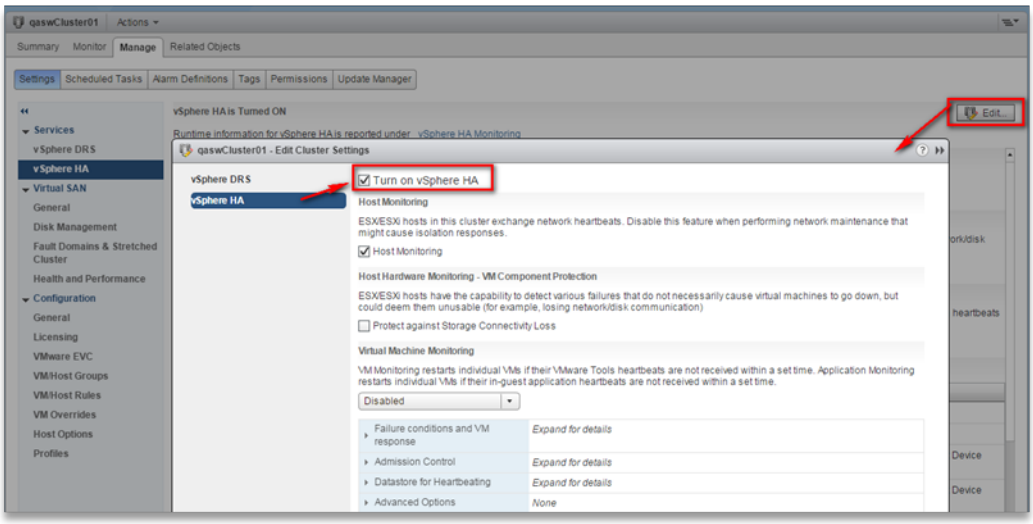
  For example, a datastore “QASWDatacenter” which contains a cluster named “qaswCluster01” and is combined of two ESXi servers (figure below).
- Verify that Shared Storage is defined and mounted for all cluster members:

Figure 7-13: Storage Adapters



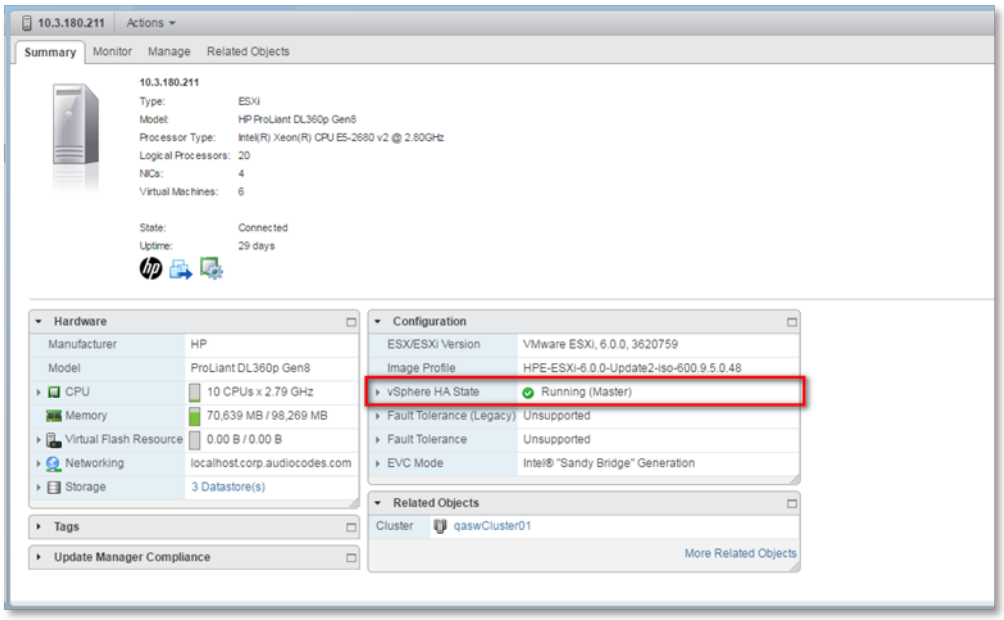
- Ensure that the 'Turn On vSphere HA' check box is selected:

Figure 7-14: Turn On vSphere HA



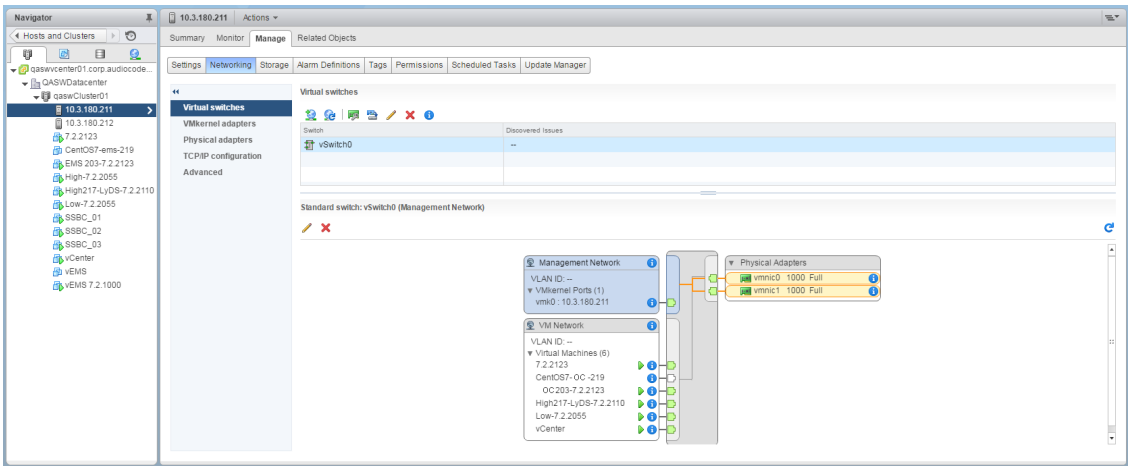
- Ensure that HA is activated on each cluster node:

Figure 7-15: Activate HA on each Cluster Node



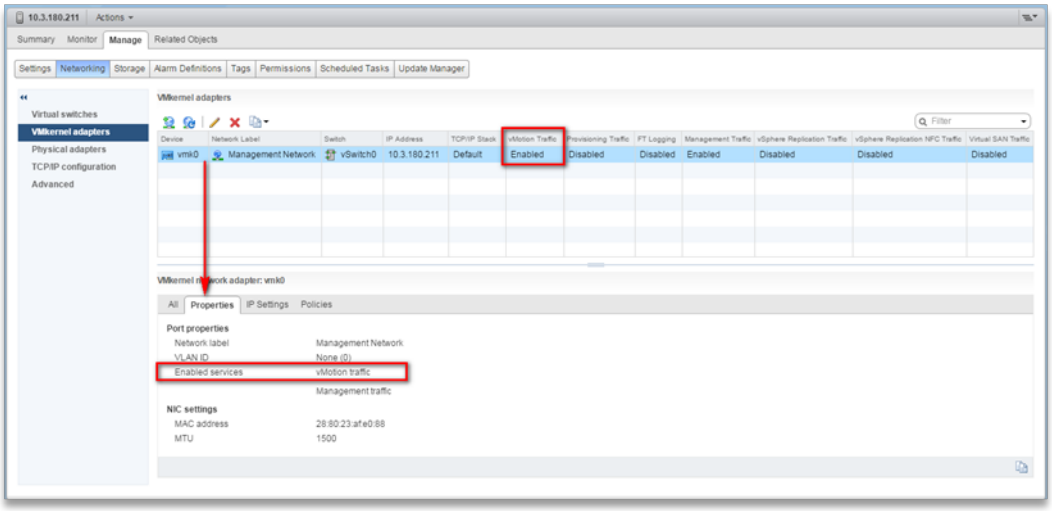
- Ensure that the networking configuration is identical on each cluster node:

Figure 7-16: Networking



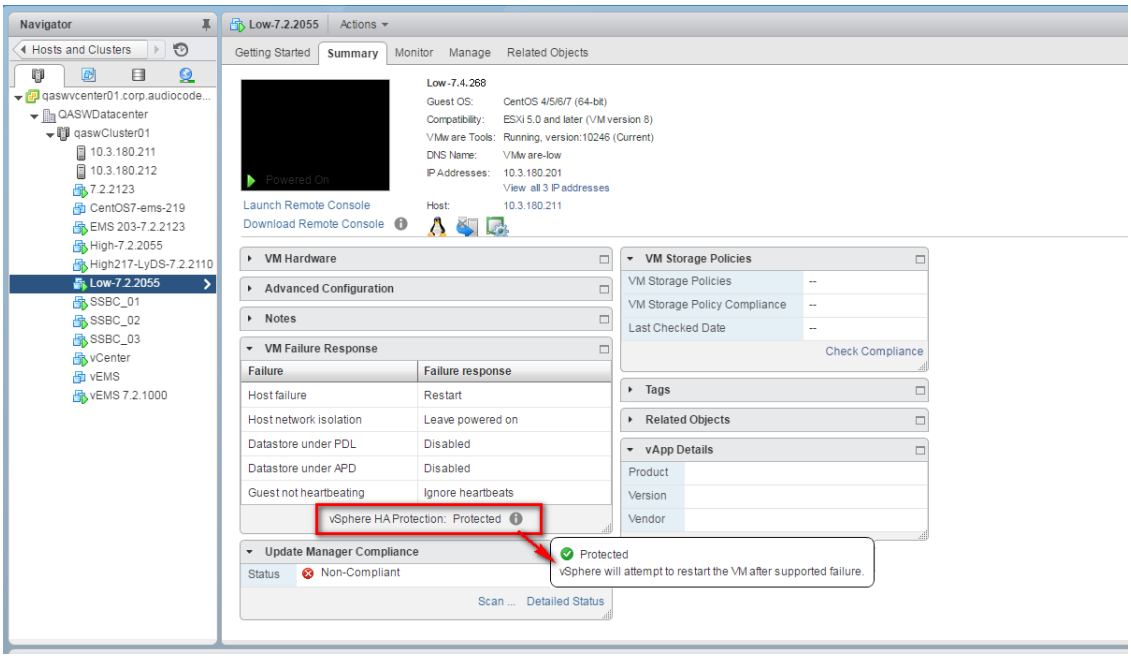
- Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

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:

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.

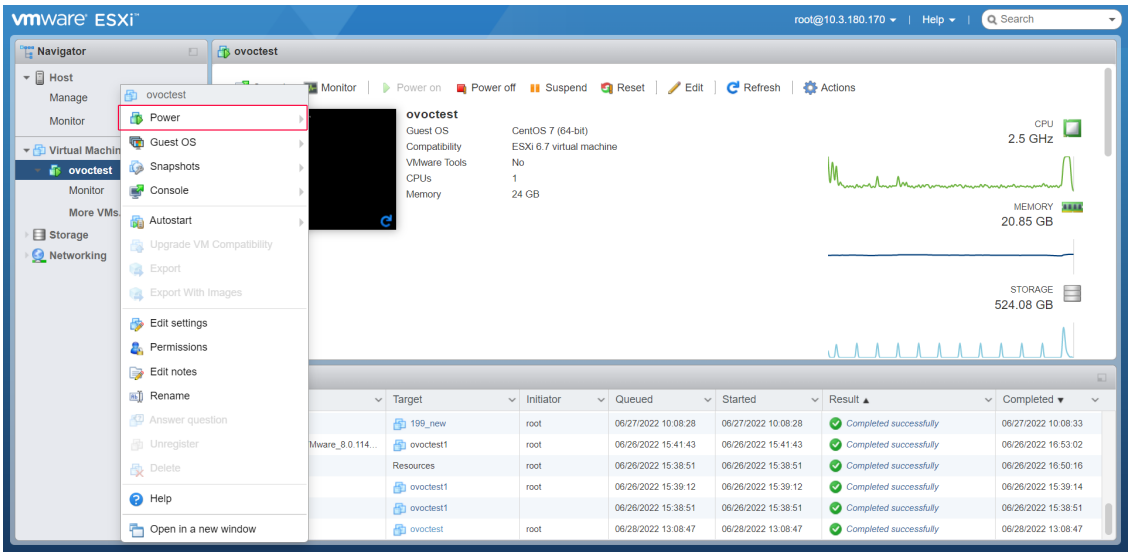
Connecting OVOC Server to Network on VMware

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:

1. 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.
8. 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

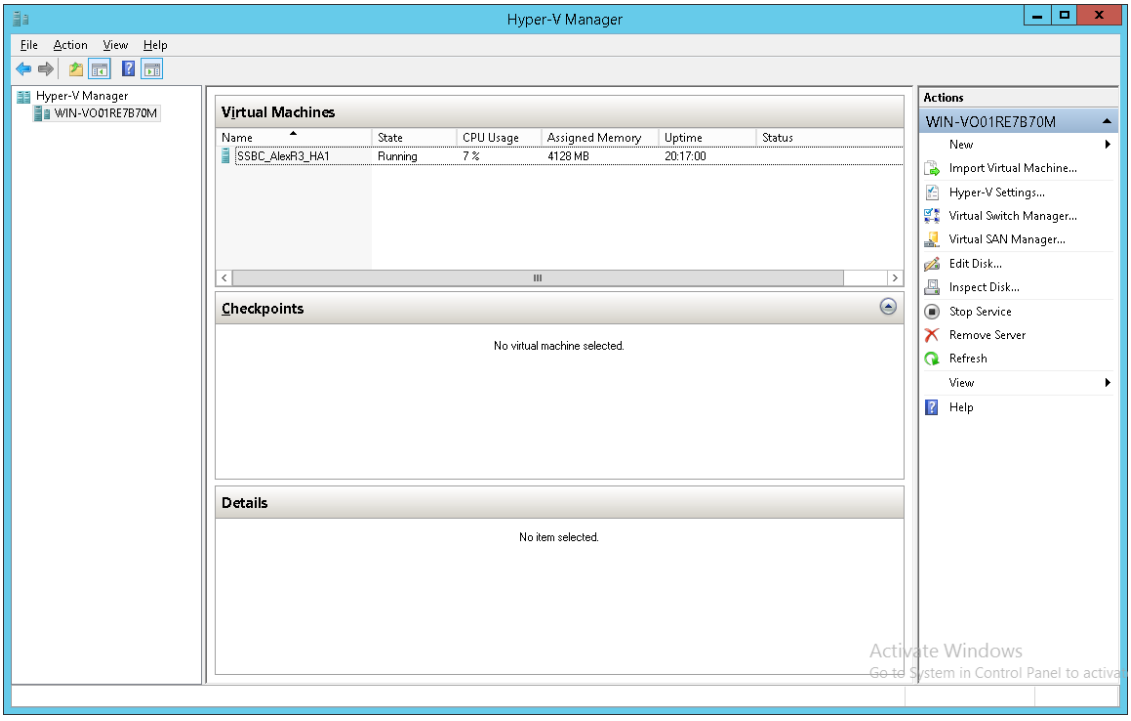
This section describes how to install the OVOC server on a Microsoft Hyper-V virtual machine.

- 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:

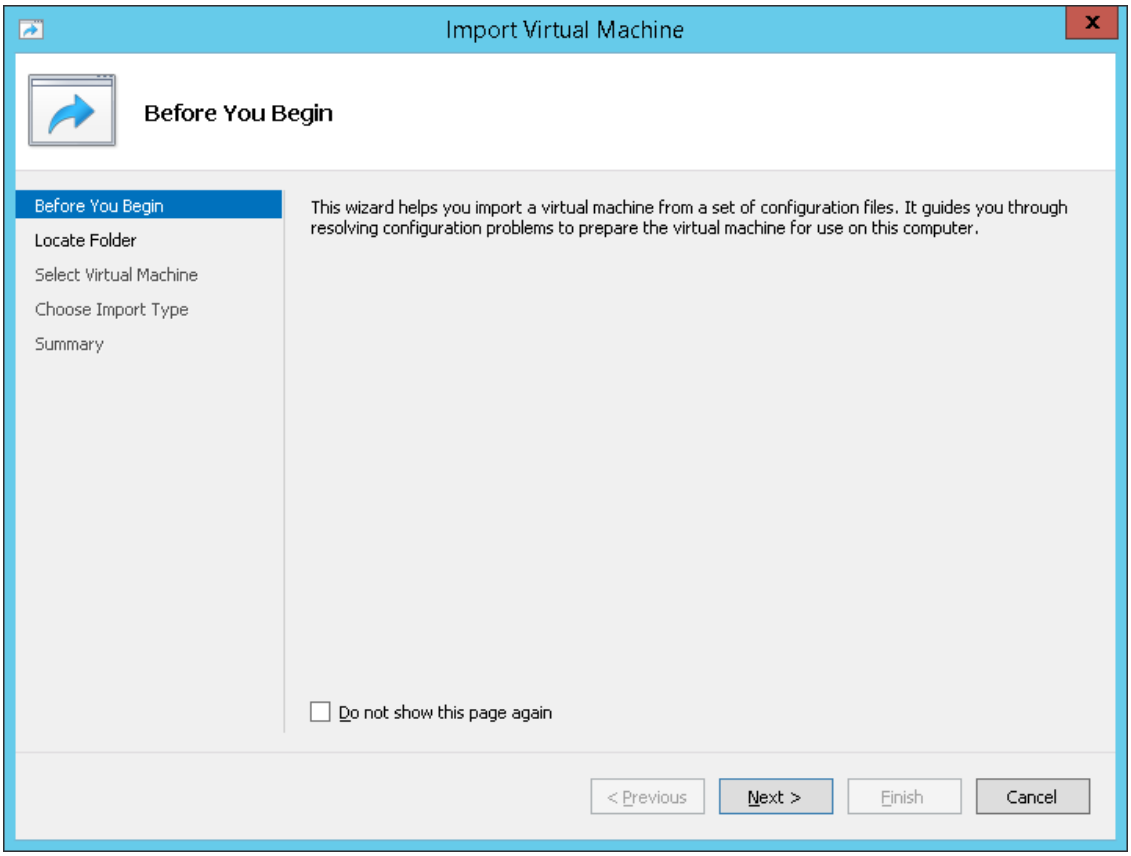
1. Transfer the ISO file containing the Microsoft Hyper-V Virtual Machine installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 328 for instructions on how to transfer files).
2. Open Hyper-V Manager by clicking **Start** > **Administrative Tools**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

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



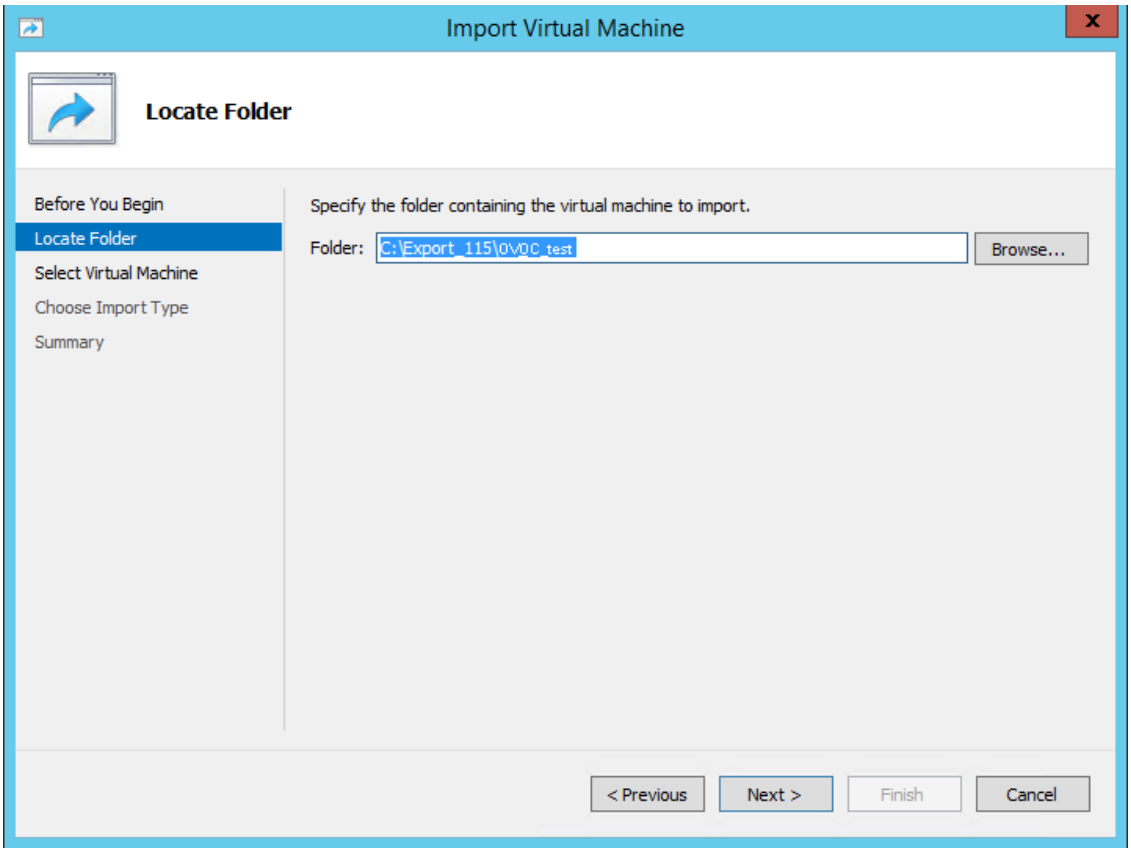
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

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



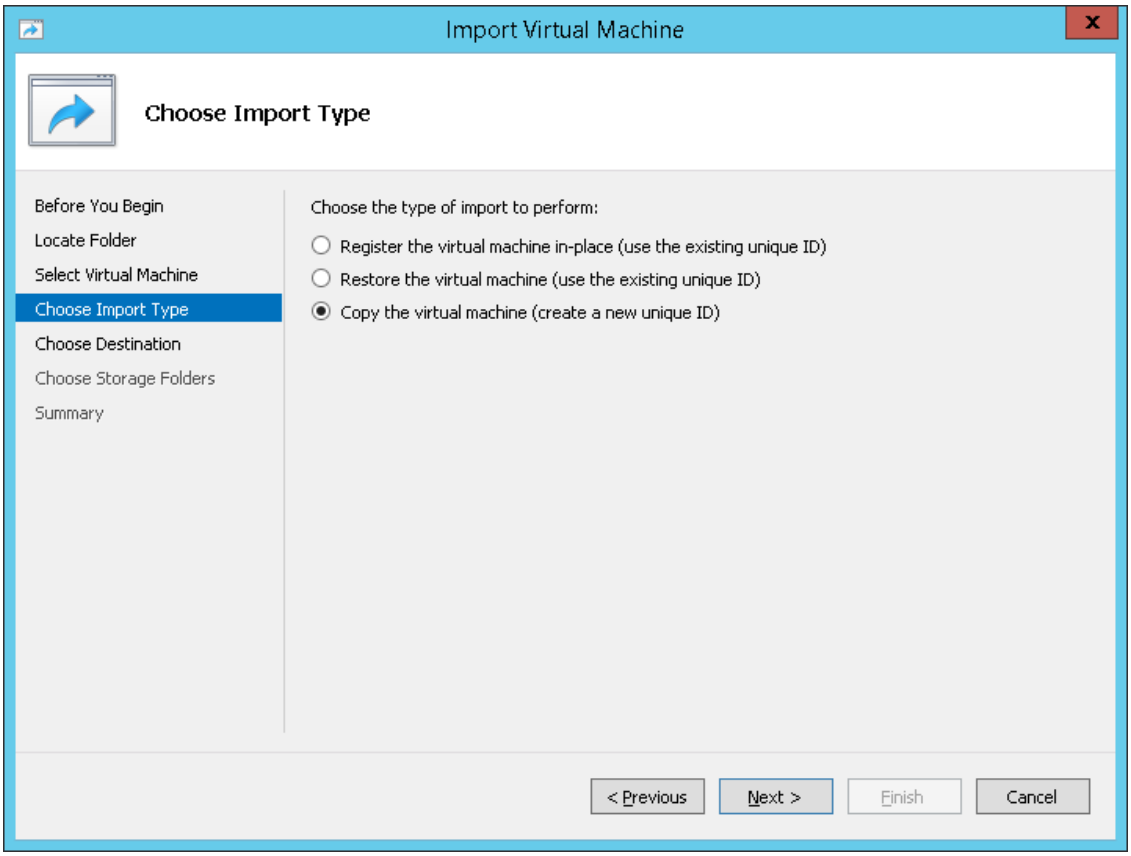
4. Click **Next**; the Locate Folder screen opens:

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



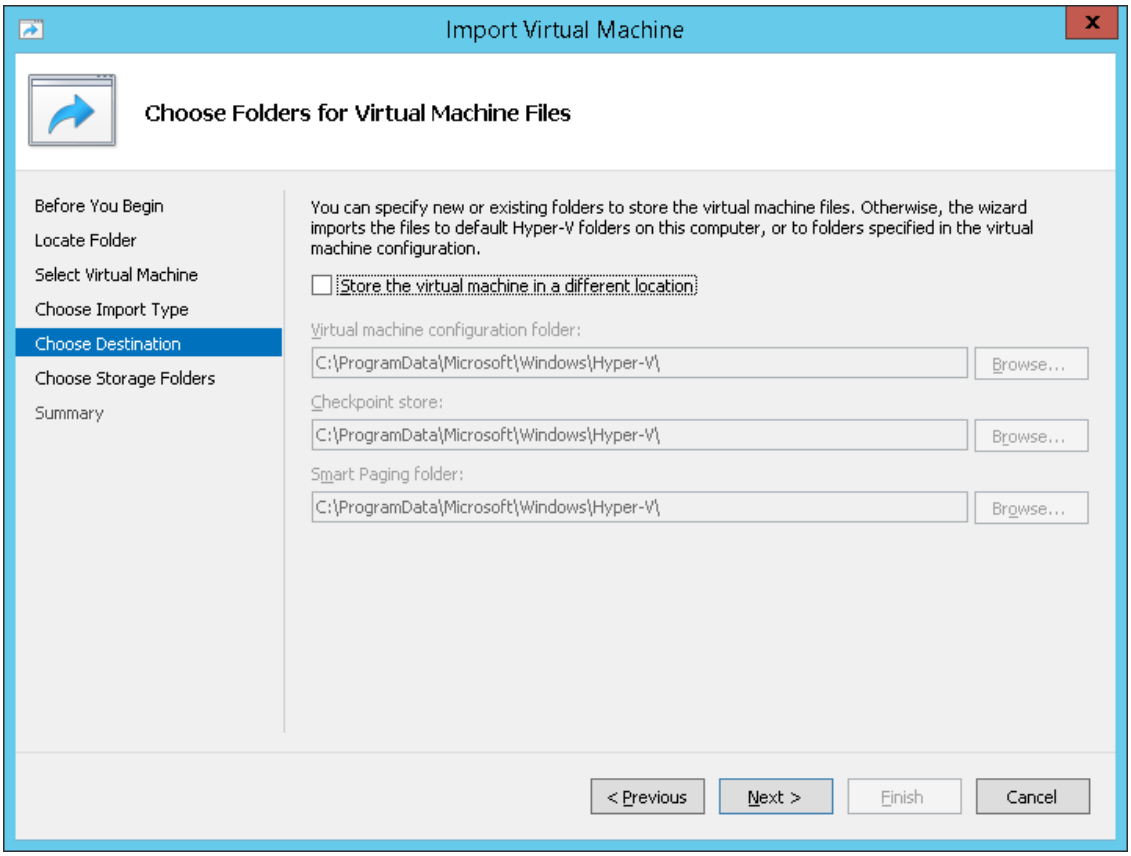
5. Enter the location of the VM installation folder (extracted from the ISO file), and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

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



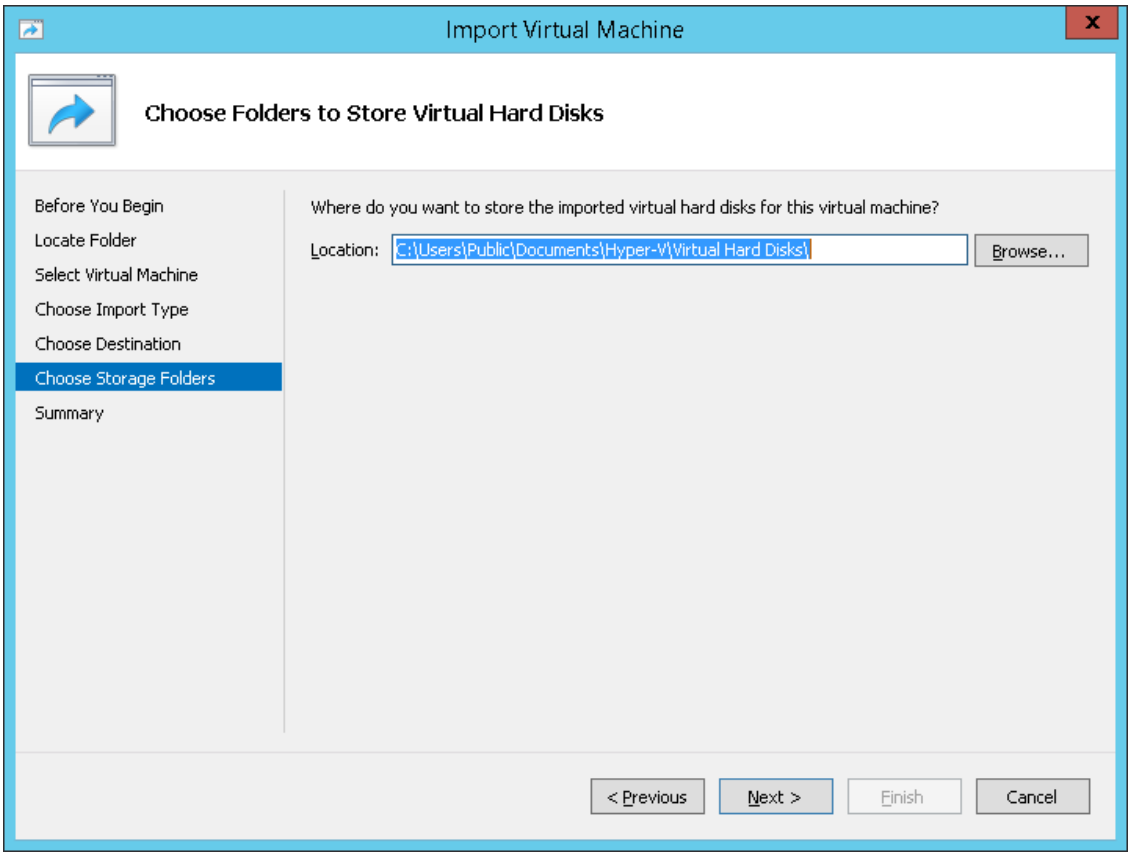
7. Select the option ''Copy the virtual machine (create a new unique ID)'', and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

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:

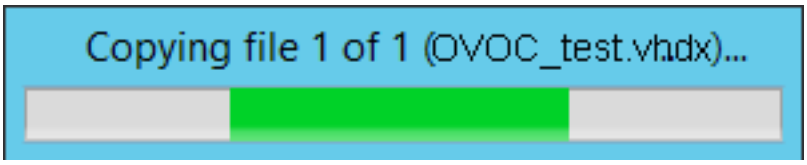
Figure 8-6: Installing OVOC server on Hyper-V – Choose Storage Folders



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.

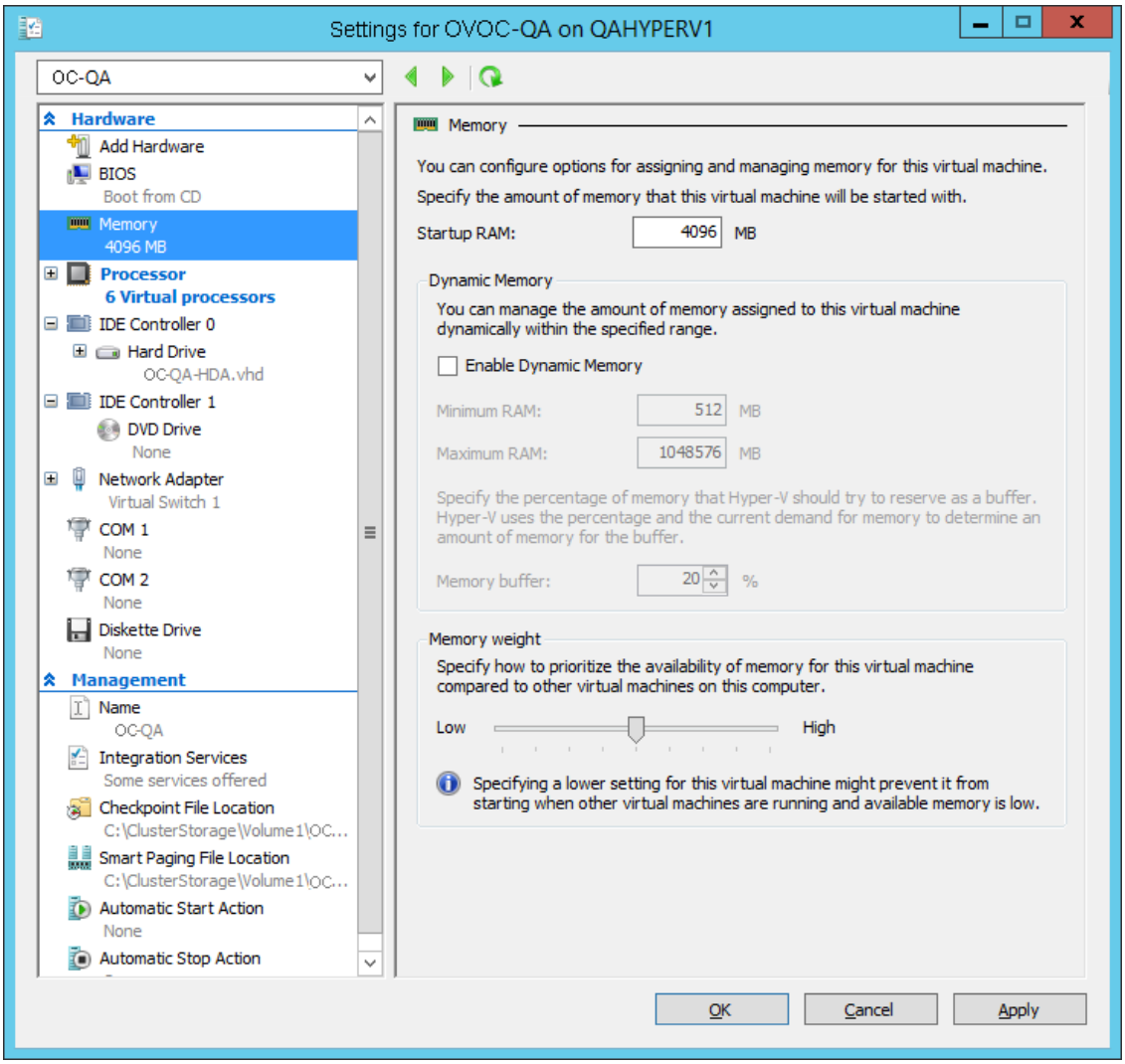
Table 8-1: Virtual Machine Configuration

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:

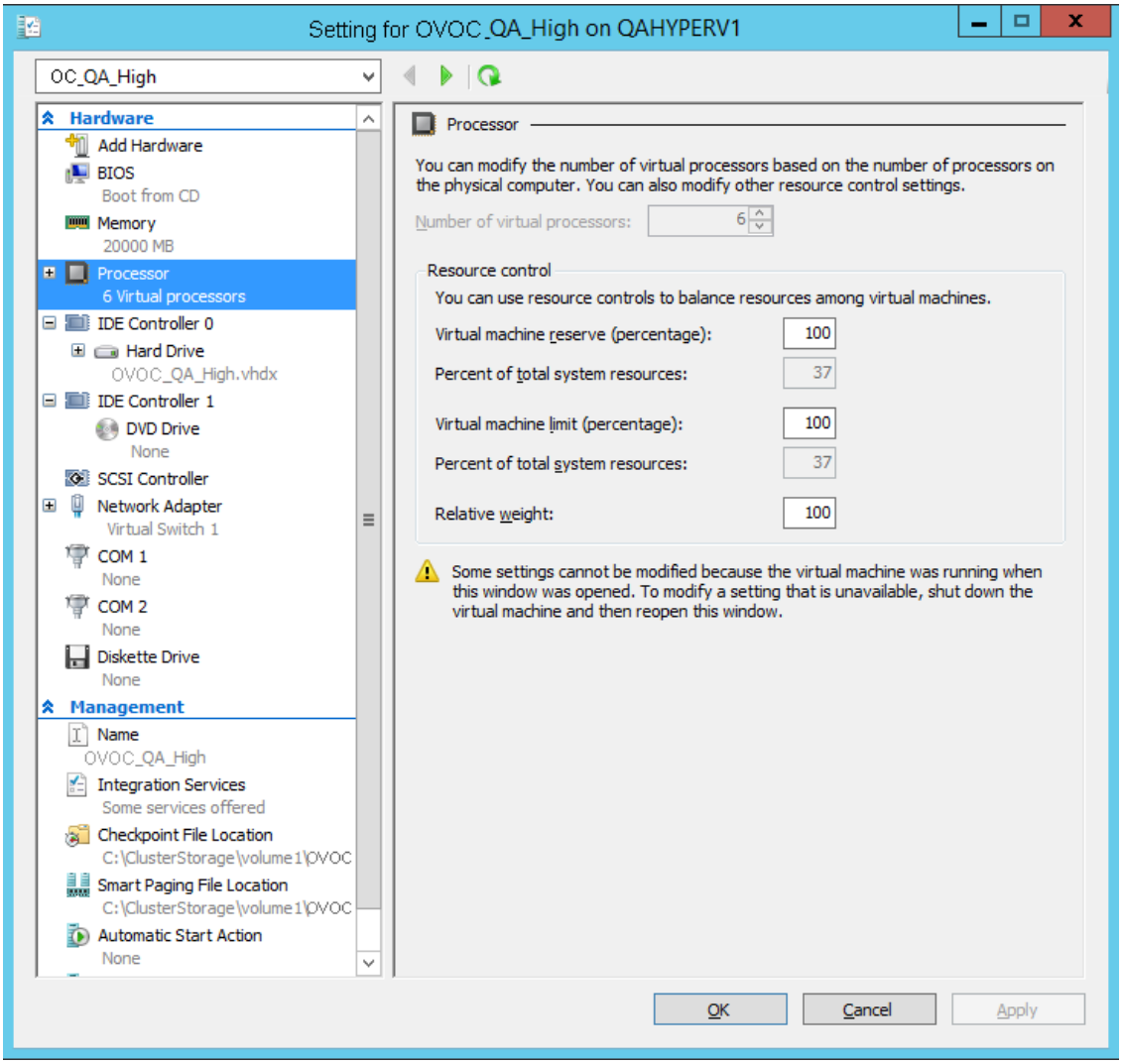
Figure 8-8: Adjusting VM for OVOC server – Settings - Memory



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.

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).

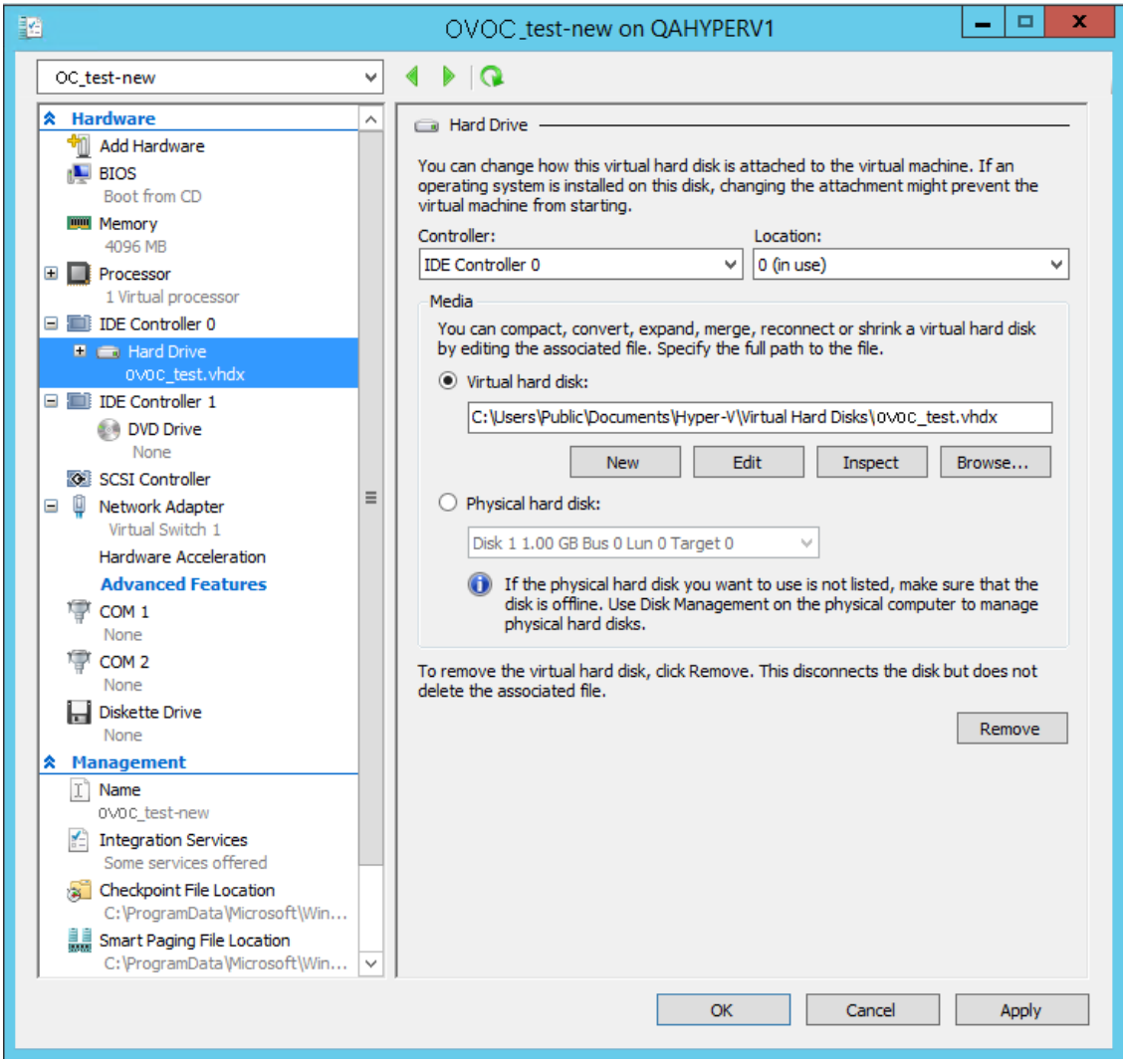
Expanding Disk Capacity

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:

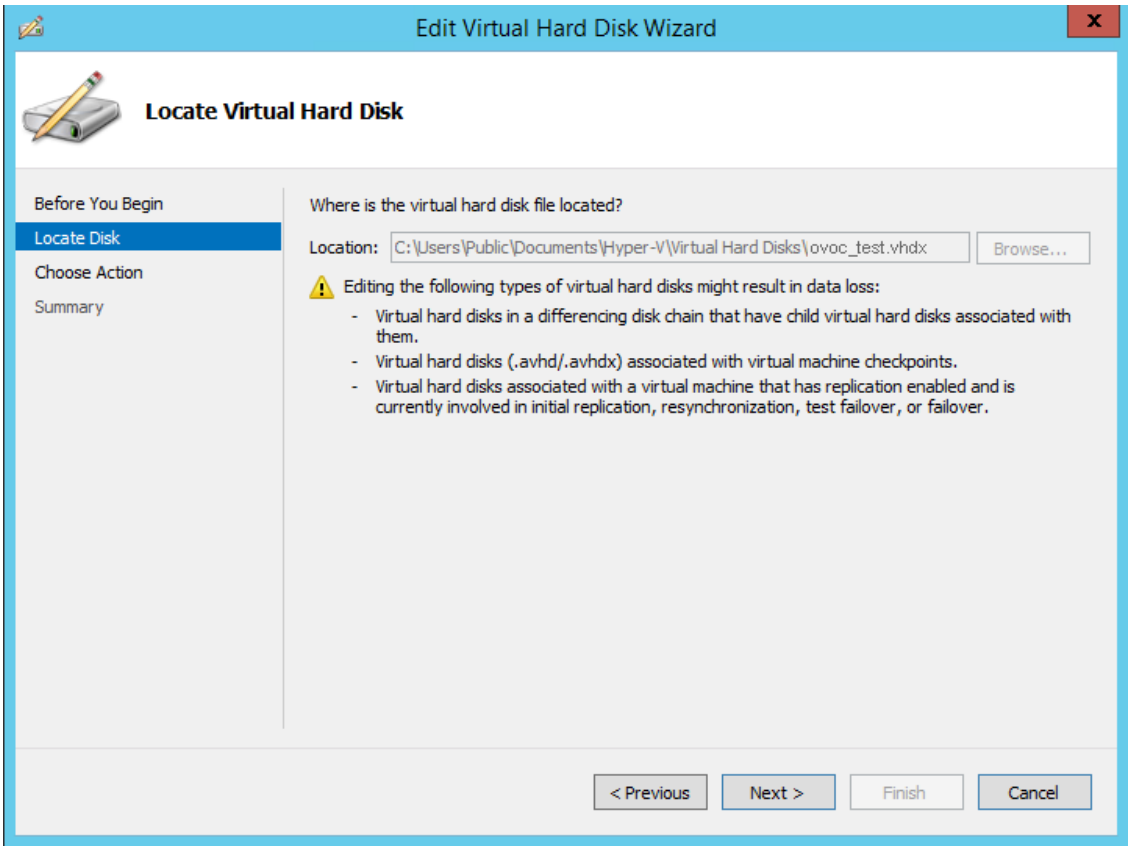
1. Make sure that the target OVOC server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

Figure 8-10: Expanding Disk Capacity



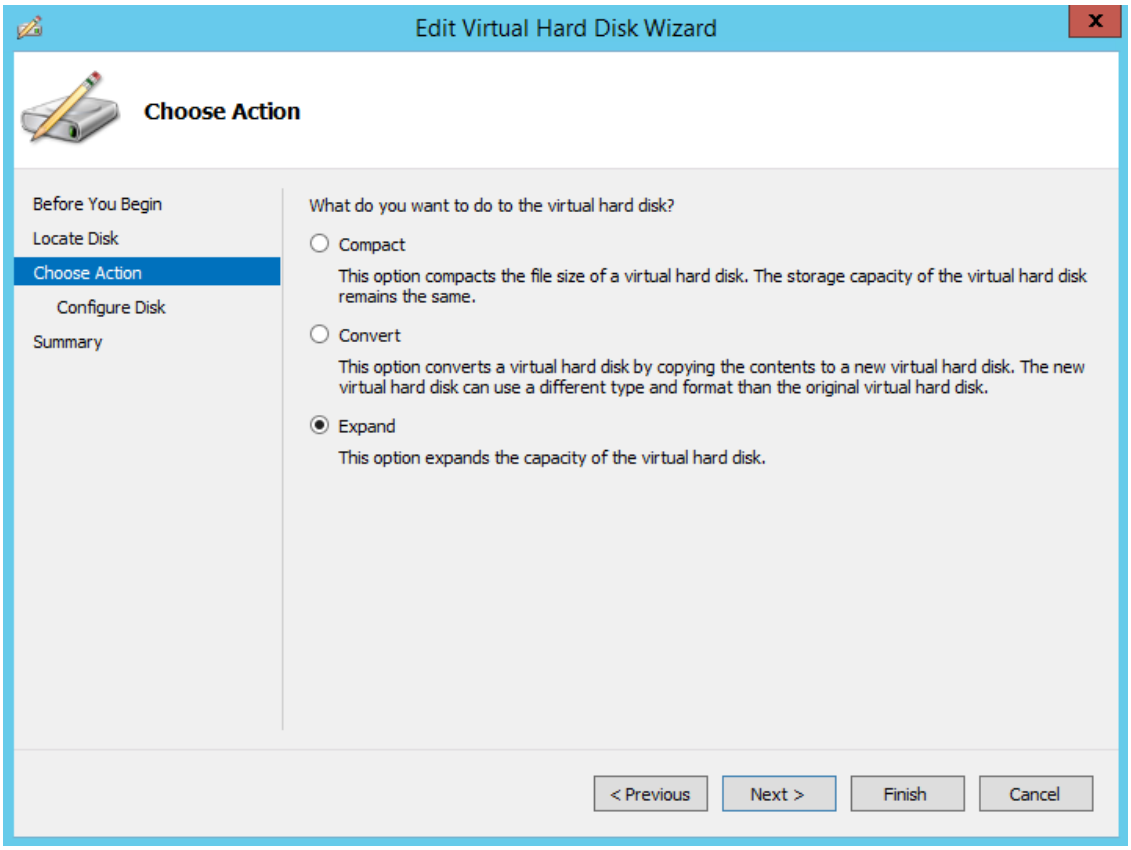
The Edit Virtual Disk Wizard is displayed as shown below.

Figure 8-11: Edit Virtual Hard Disk Wizard



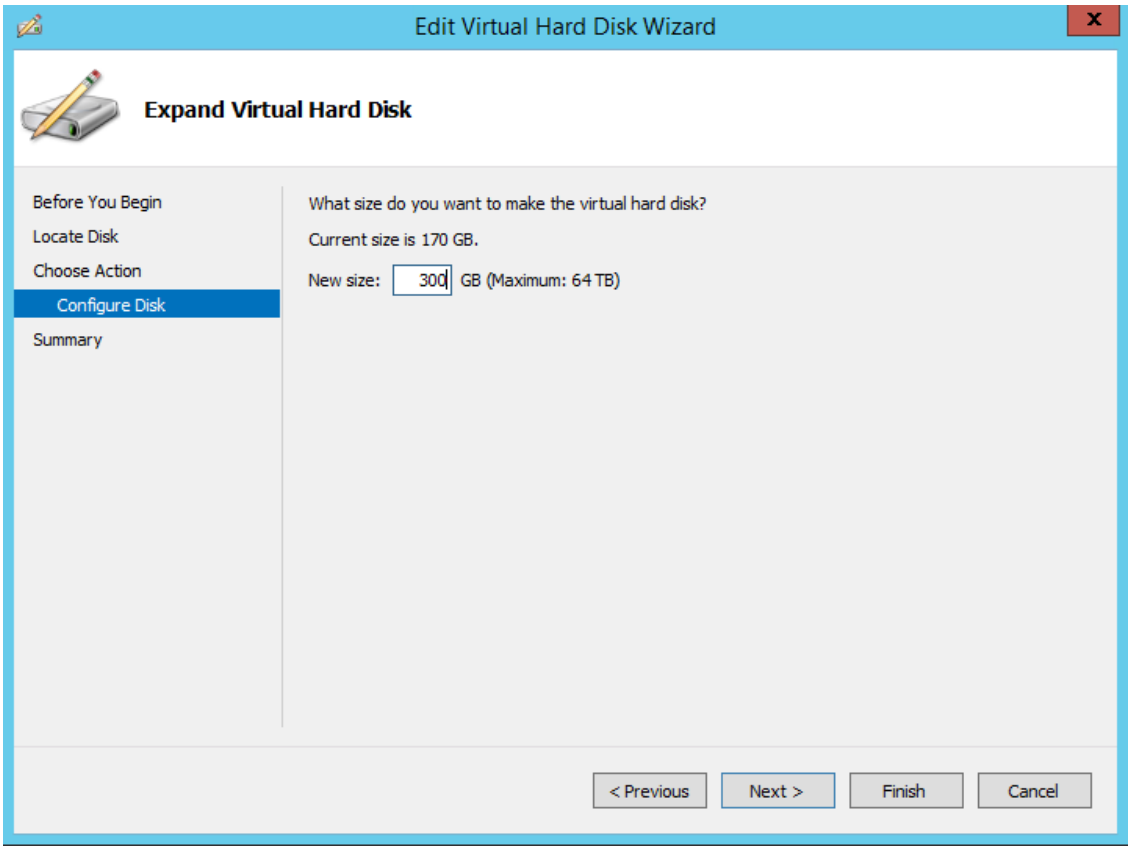
3. Click **Next**; the Choose Action screen is displayed:

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



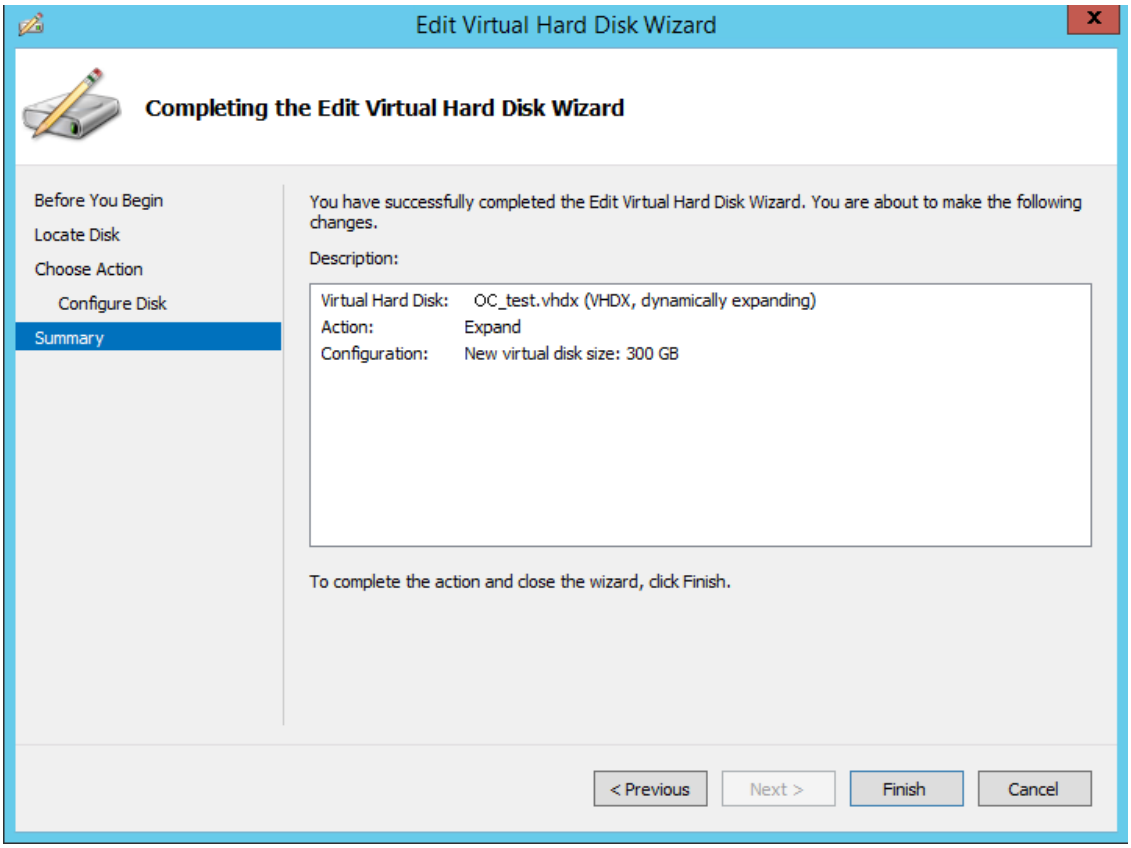
4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

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.

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'

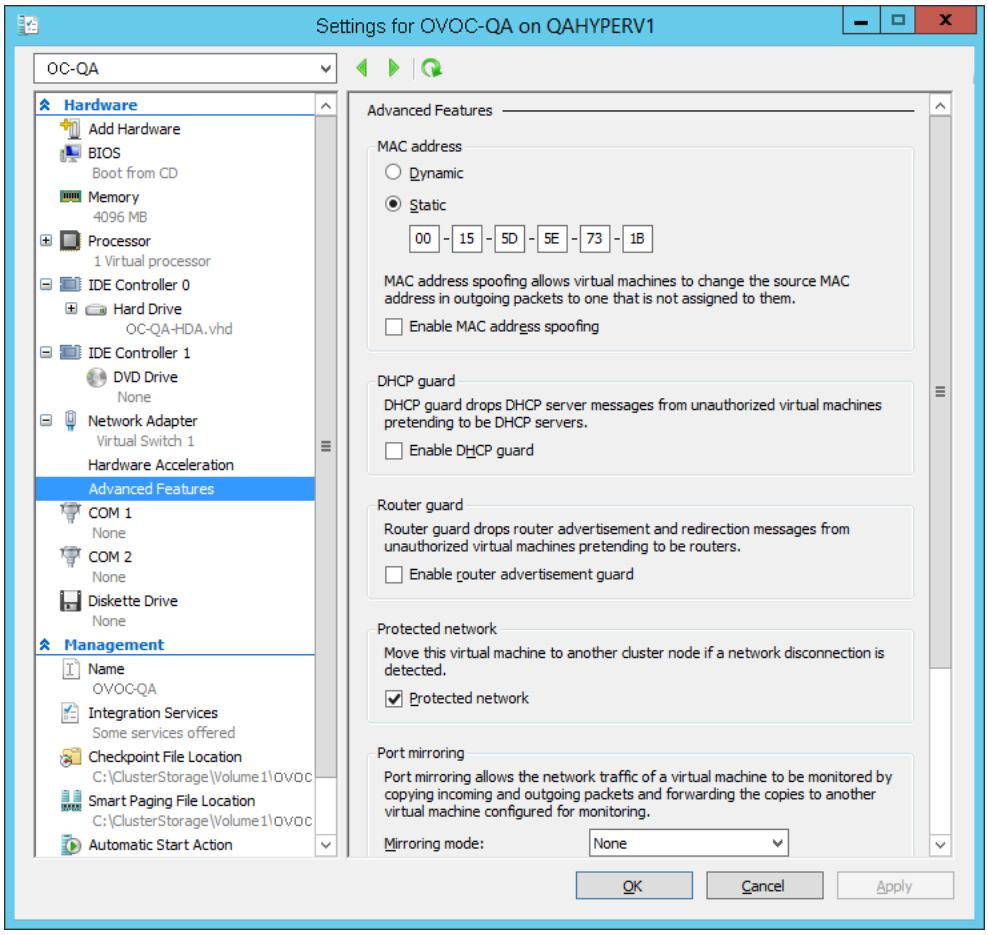
By default, the MAC addresses of the OVOC server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license.

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.

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



Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster

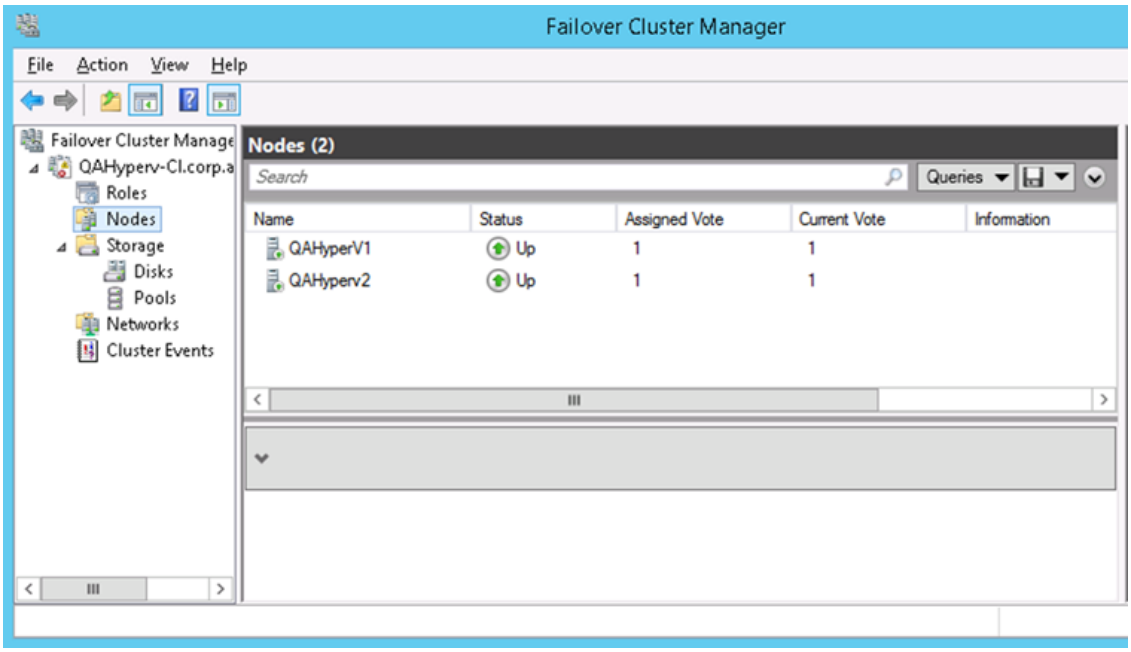
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

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.

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.

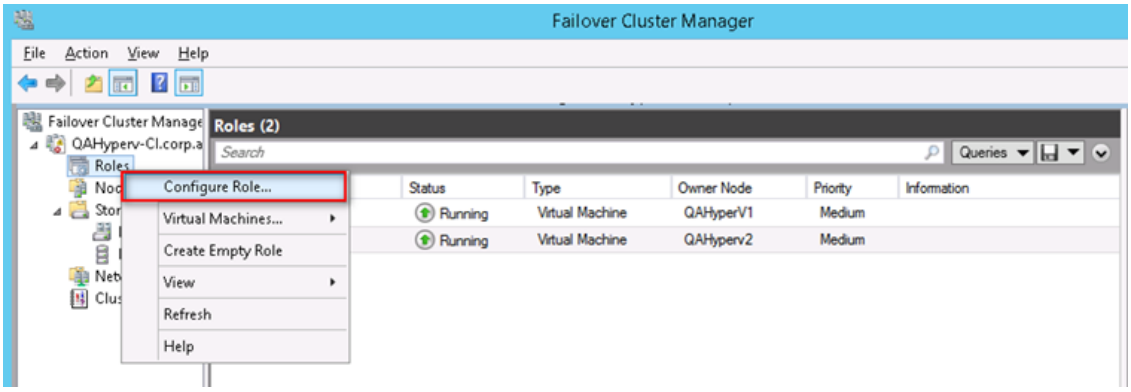
Add the OVOC VM in Failover Cluster Manager

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:**

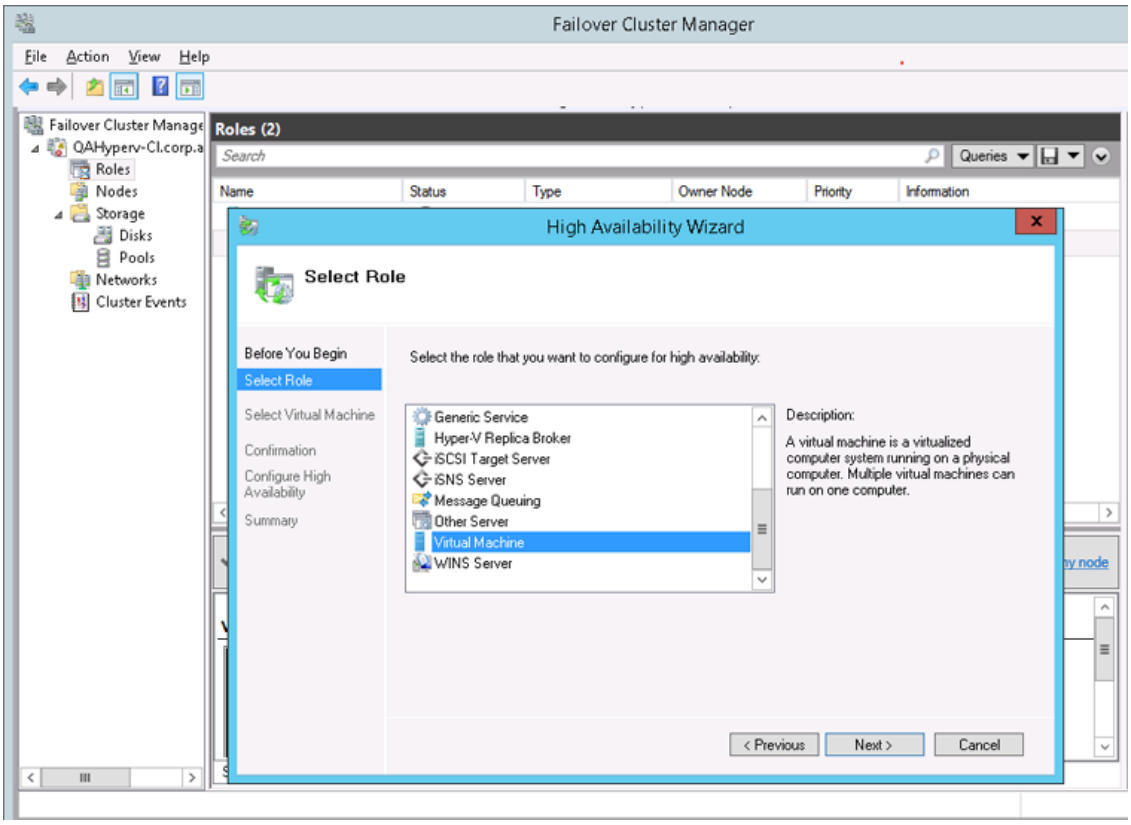
1. Right-click "Roles" and in the pop-up menu, choose **Configure Role.**

Figure 8-17: Configure Role



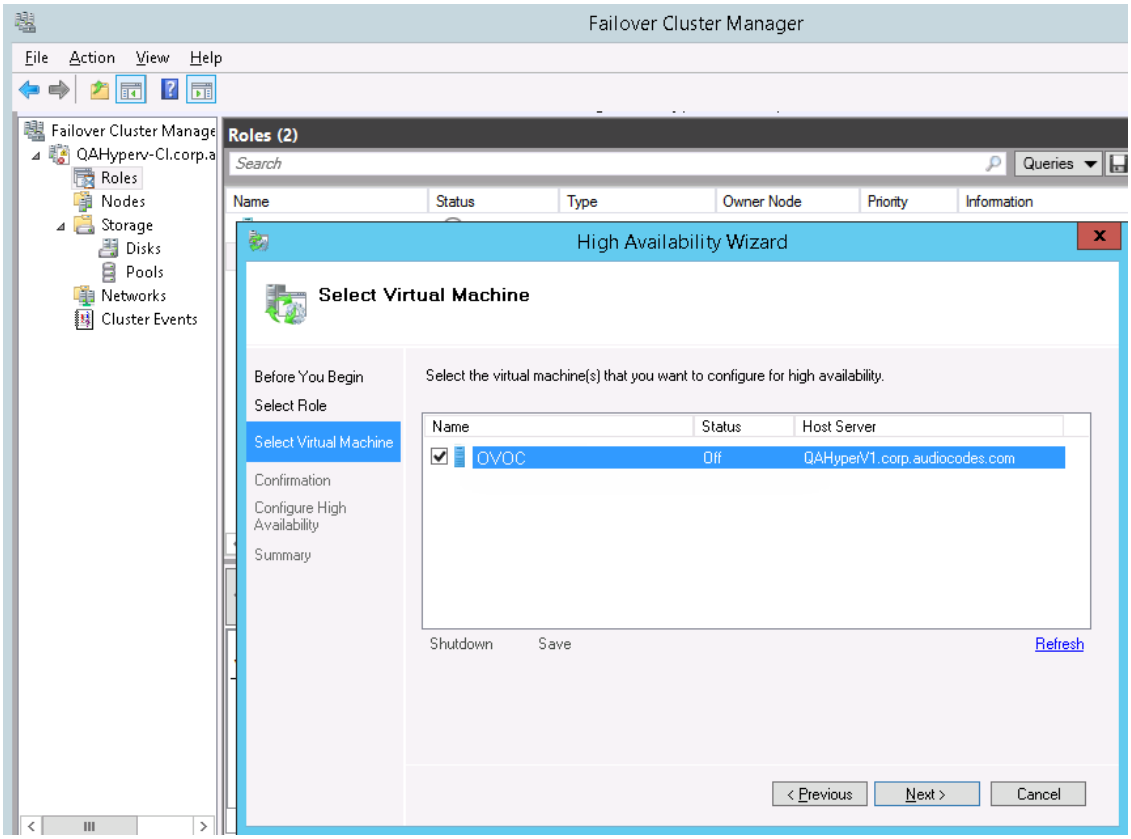
2. In the Select Role window, select the **Virtual Machine** option and then click **Next**.

Figure 8-18: Choose Virtual Machine



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

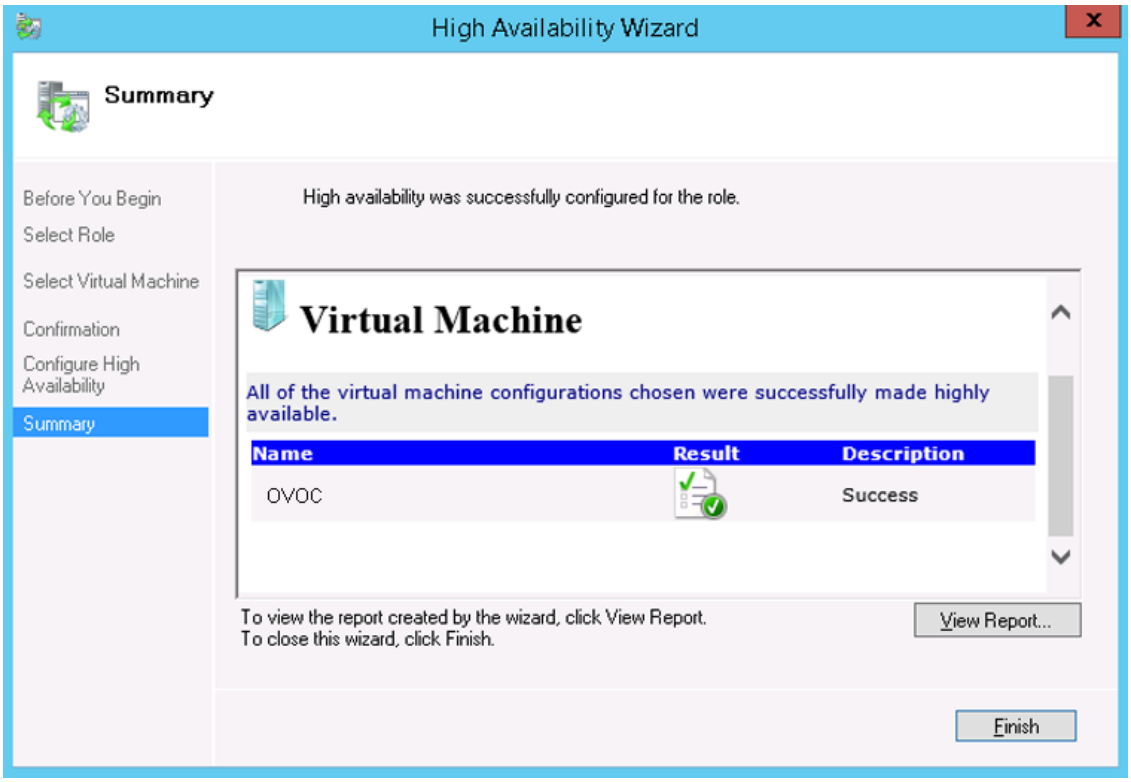
Figure 8-19: Confirm Virtual Machine



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



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

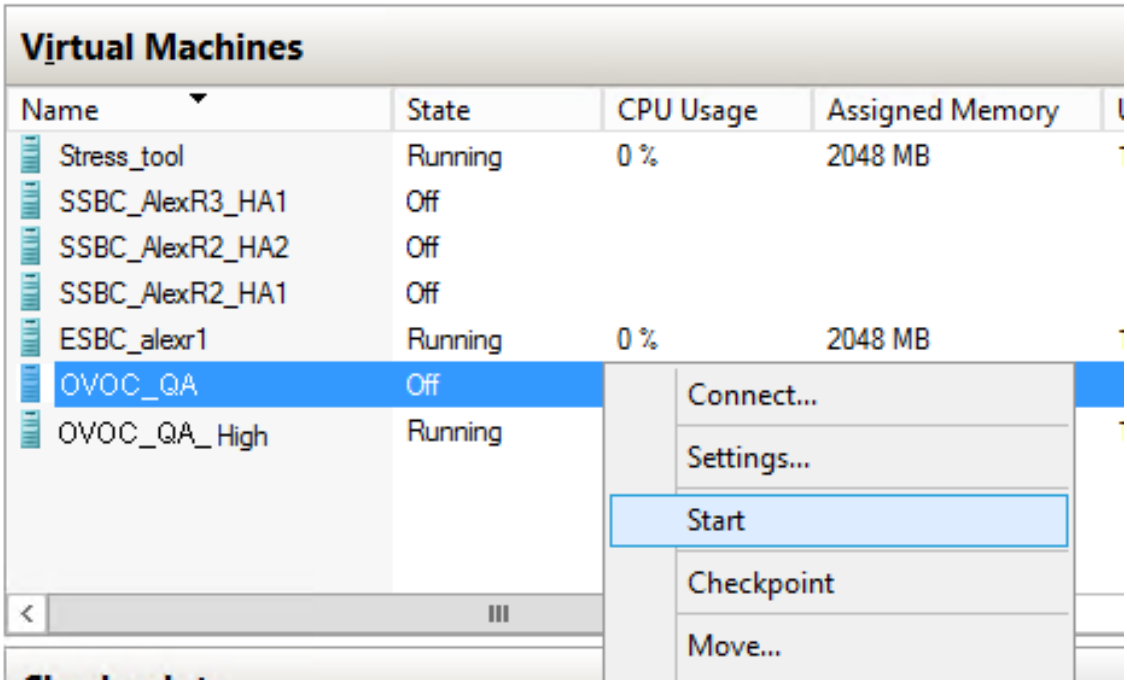
After installation, the OVOC server is assigned, a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network

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:

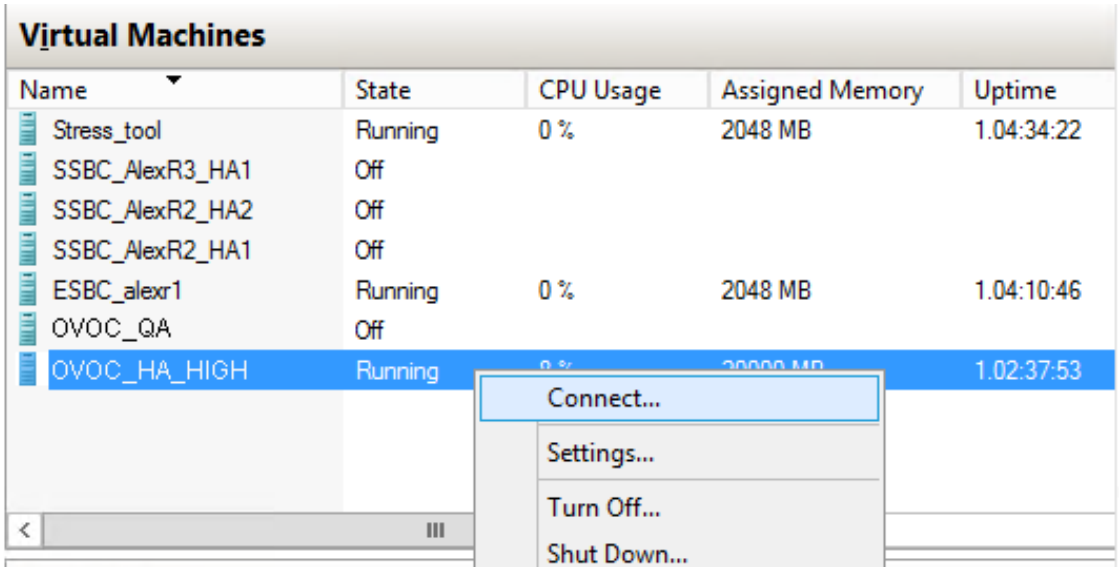
1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

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



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.
7. 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

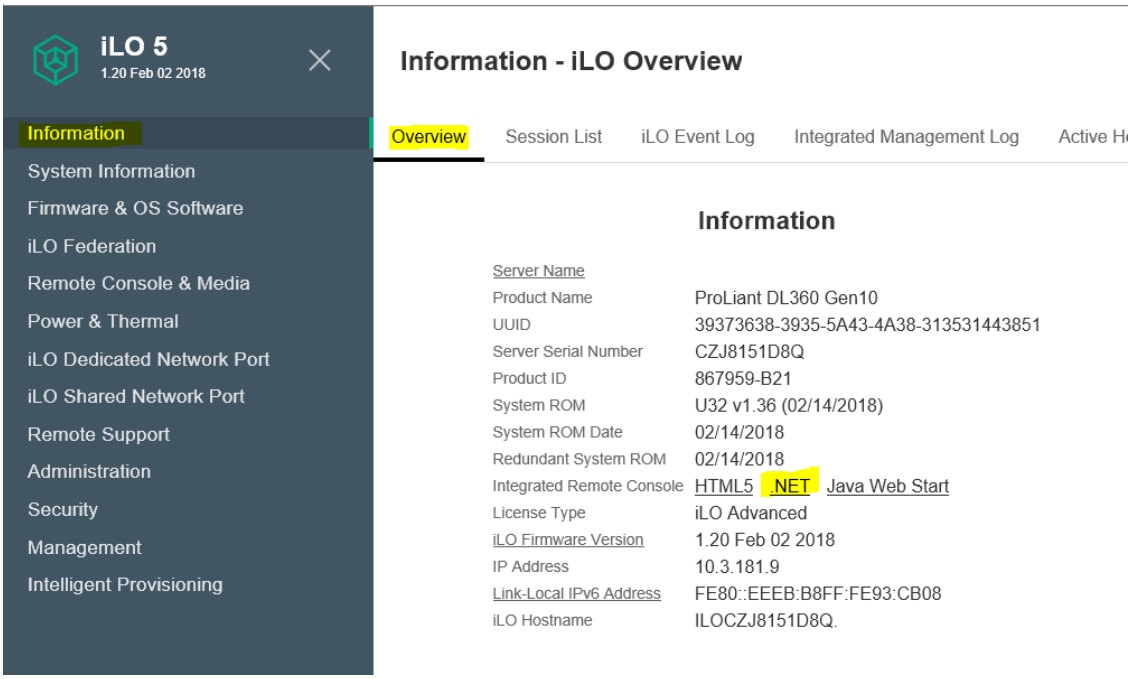
This section describes how to install DVD1 including the Rocky Linux Operating system.

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:**

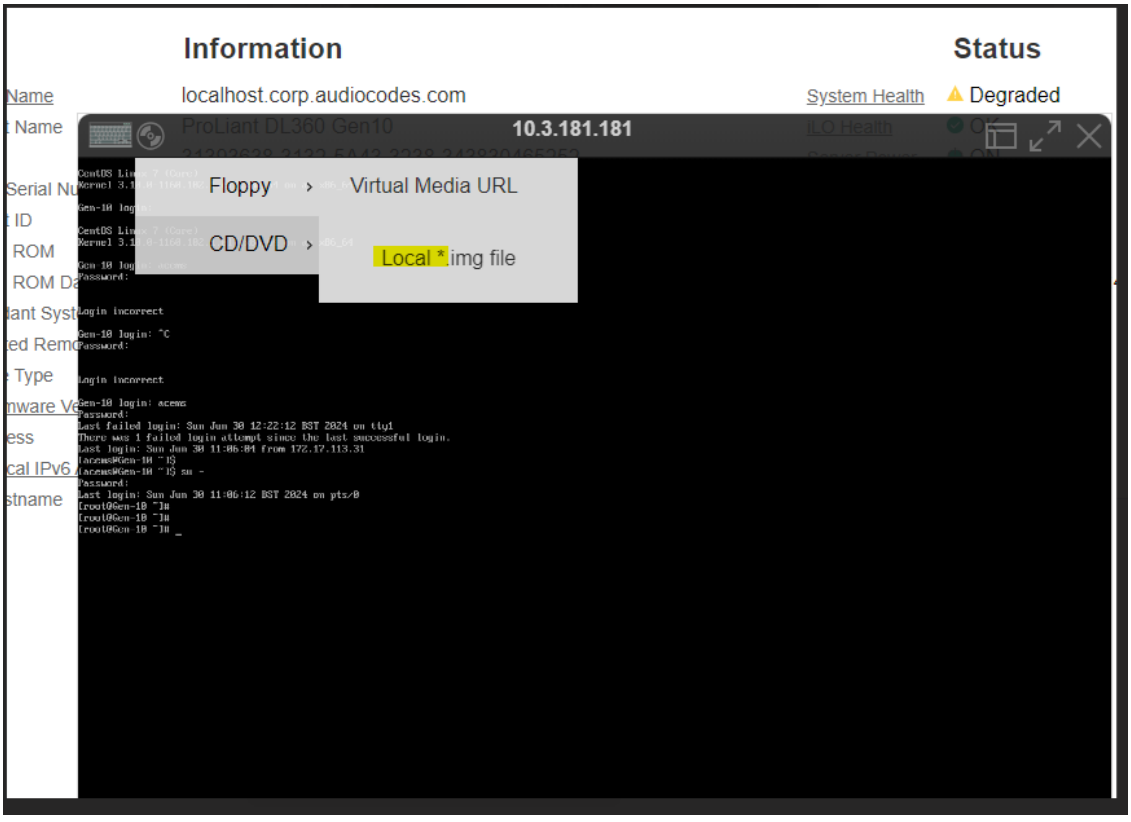
1. Download the **DVD1**.ISO file to your PC.
2. Using the WinSCP utility (see Transferring Files on page 328) transfer the **DVD1**.ISO file to the virtual machine installation platform.
3. Login to ILO 5 with “Administrator” privileges.
4. Launch the Integrated Remote Console.

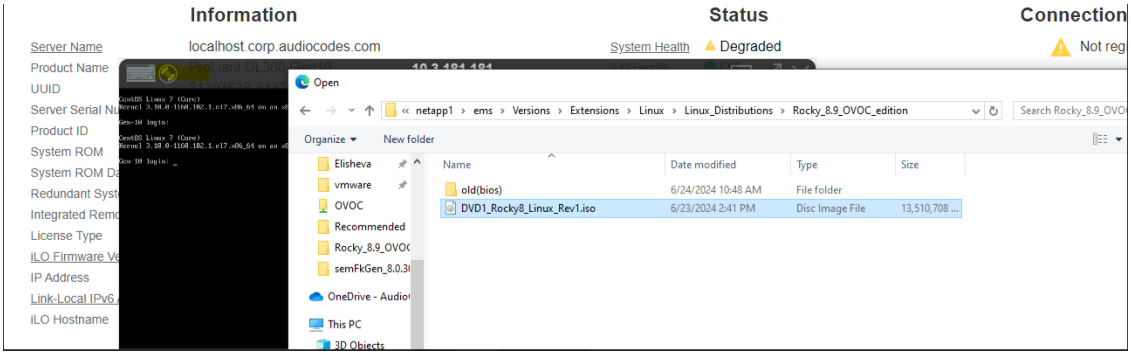
Figure 9-1: Information-iLO Overview



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

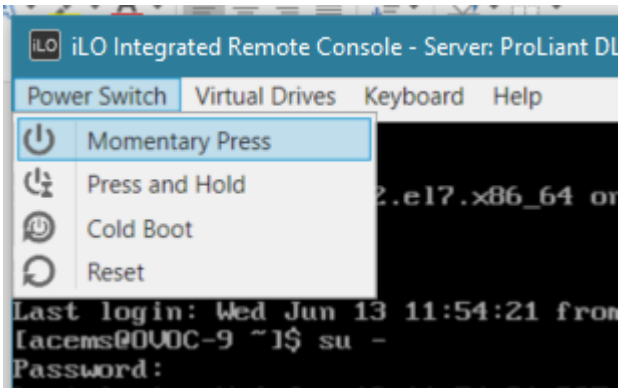
Figure 9-2: iLO Integrated Remote Console





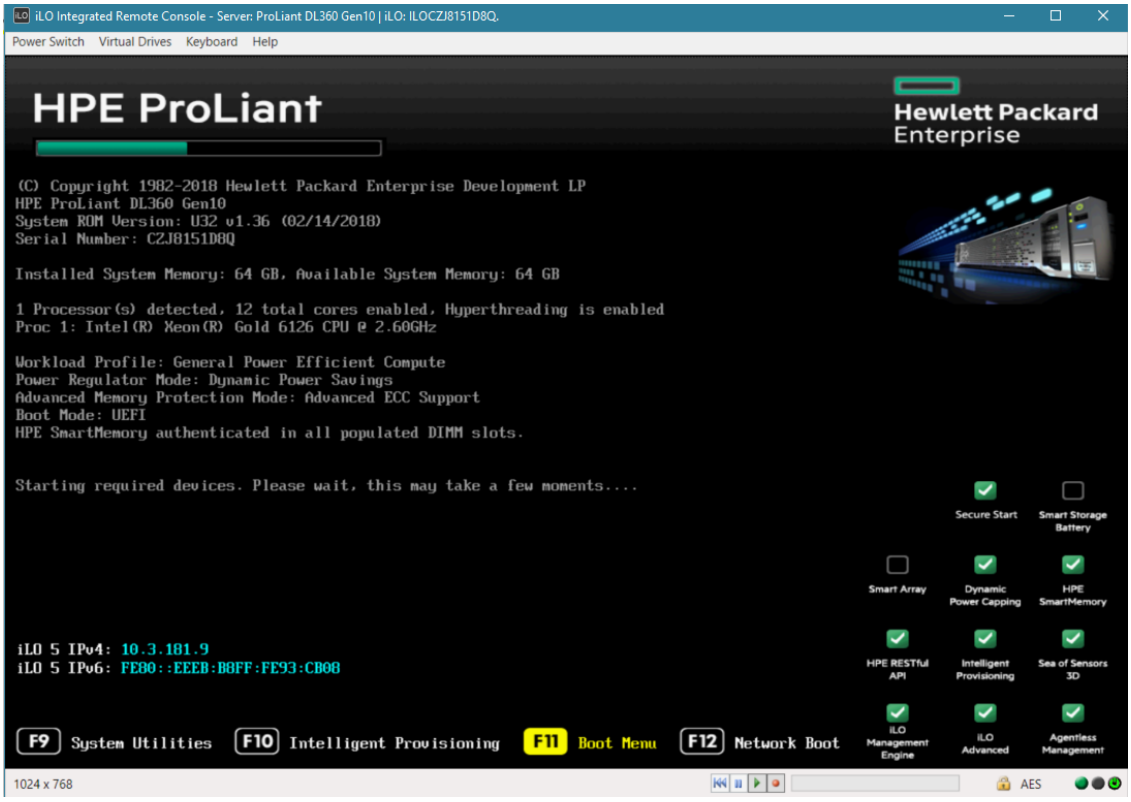
6. From Integrated Remote Console, click **Power Switch** > **Momentary Press**, the server is shutdown. Click **Momentary Press** to power the server back on.

Figure 9-3: Momentary Press



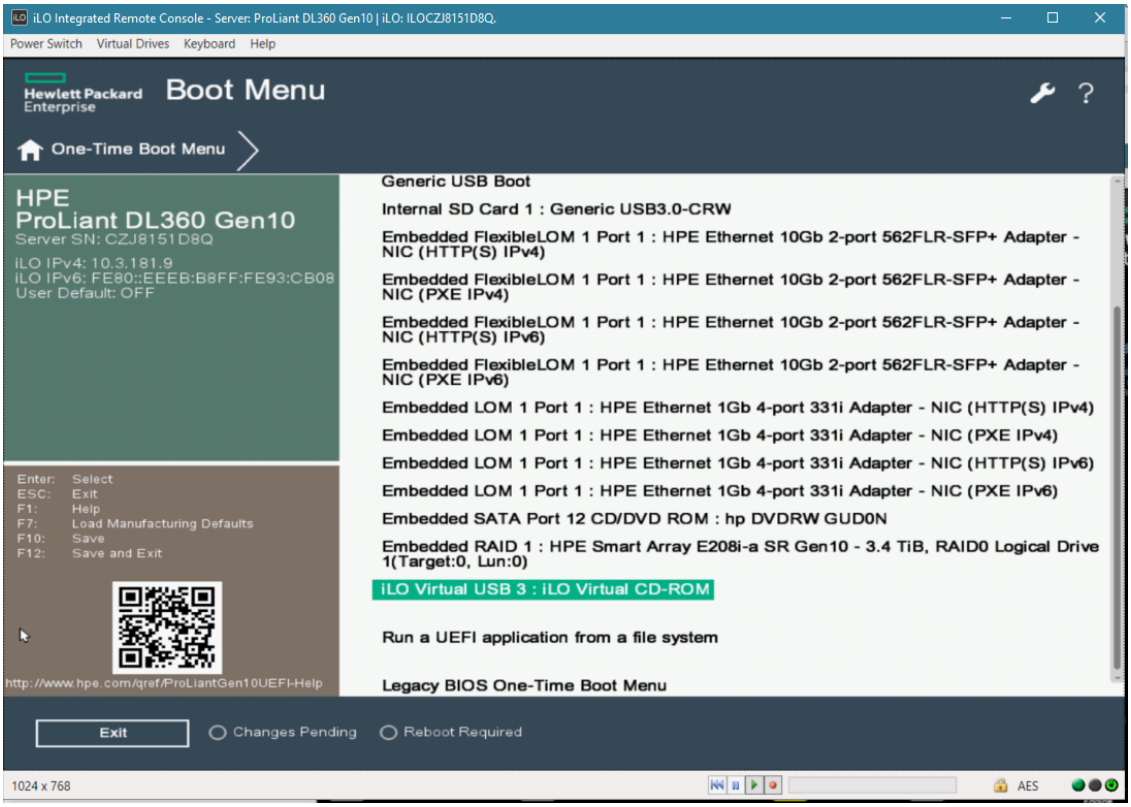
After server boot process has commenced, press F11 to enter the boot menu.

Figure 9-4: Boot Menu



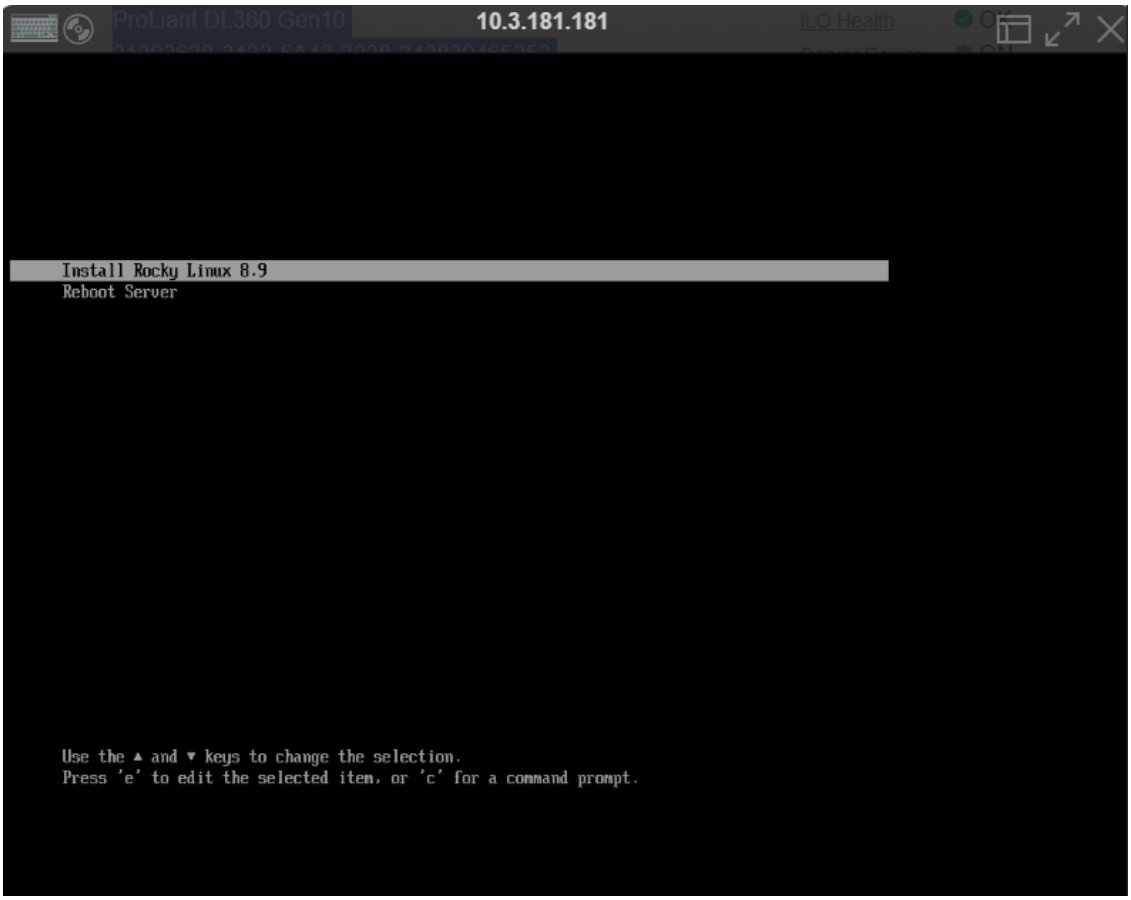
7. On boot menu, scroll down by mouse or arrows keys and select the “iLO Virtual USB 3 : iLO Virtual CD-ROM” to start the boot sequence.

Figure 9-5: Boot Sequence



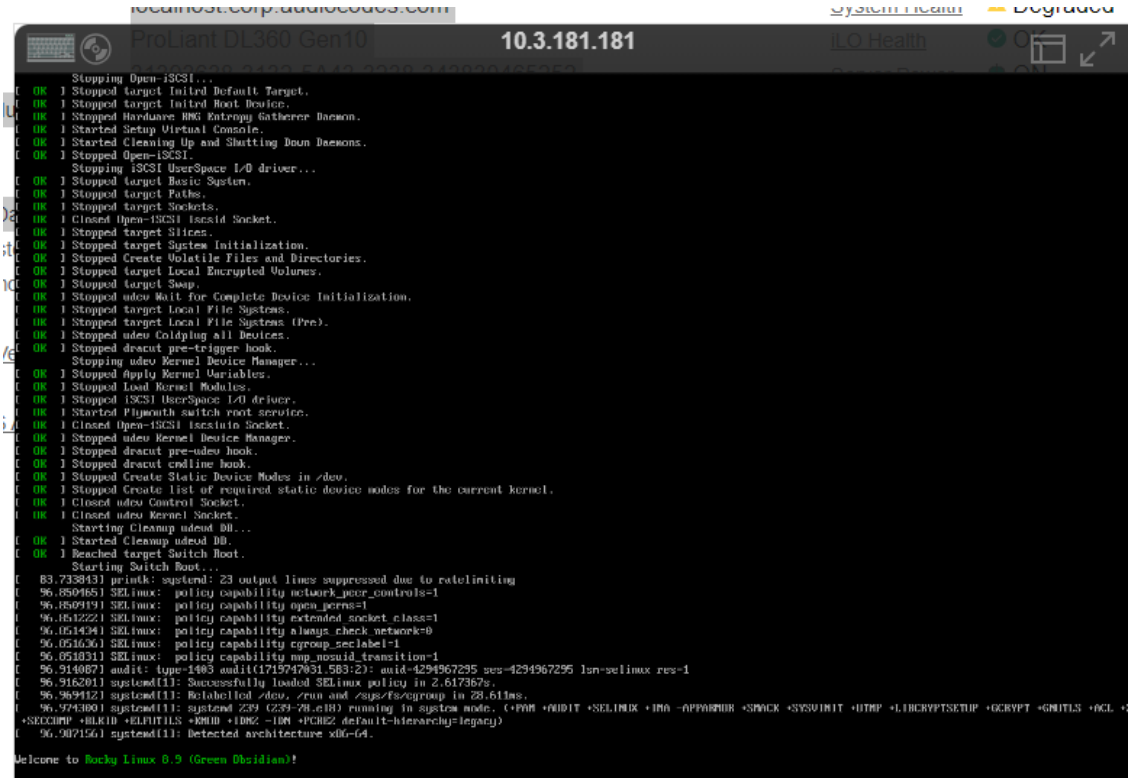
8. The following screen appears, select “Install Rocky Linux version 8.x …” and press Enter.

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



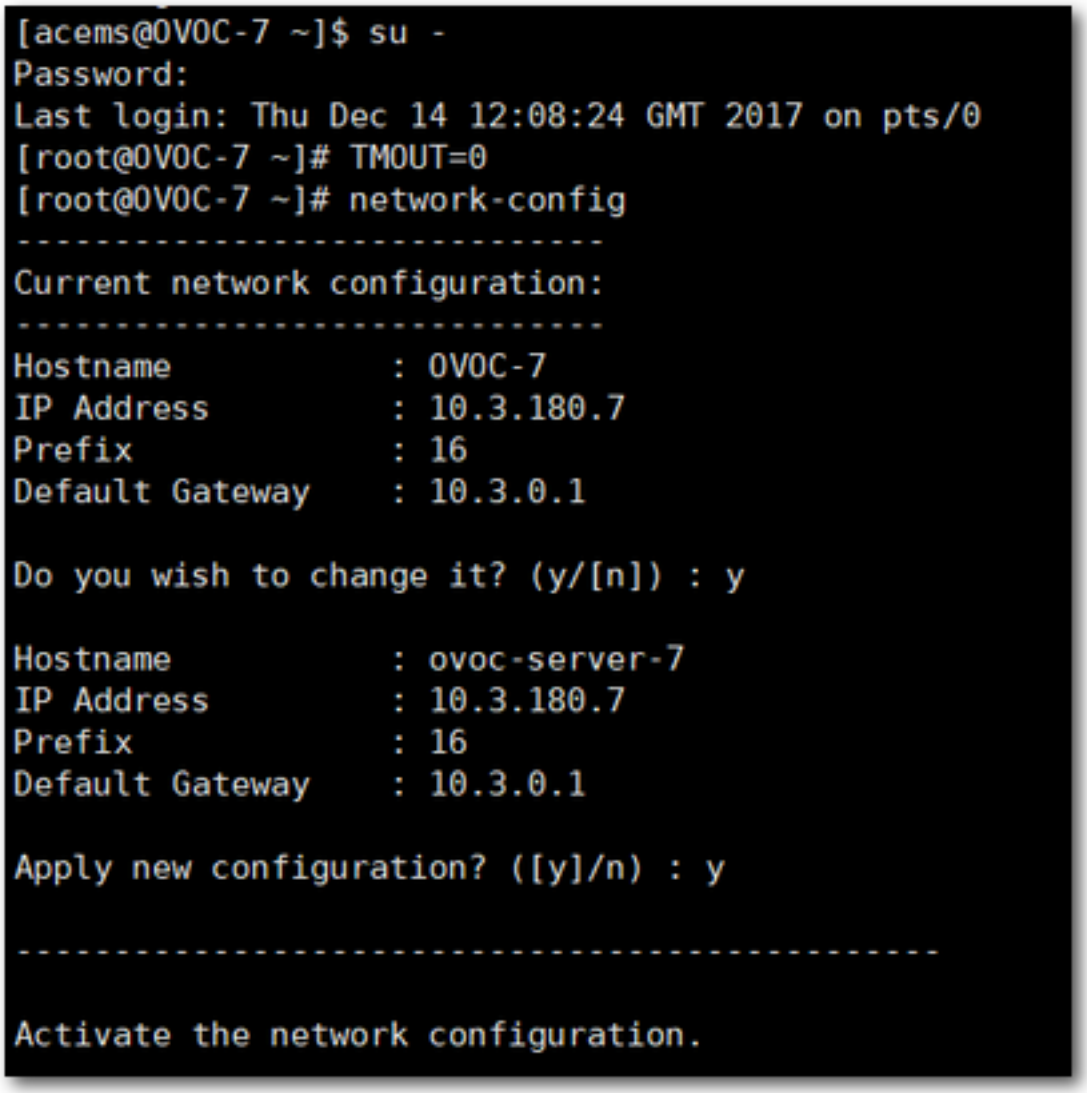
9. After a while the Rocky Linux version 8.x installation commences:

Figure 9-7: Start Rocky Linux version 8.x



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



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
```

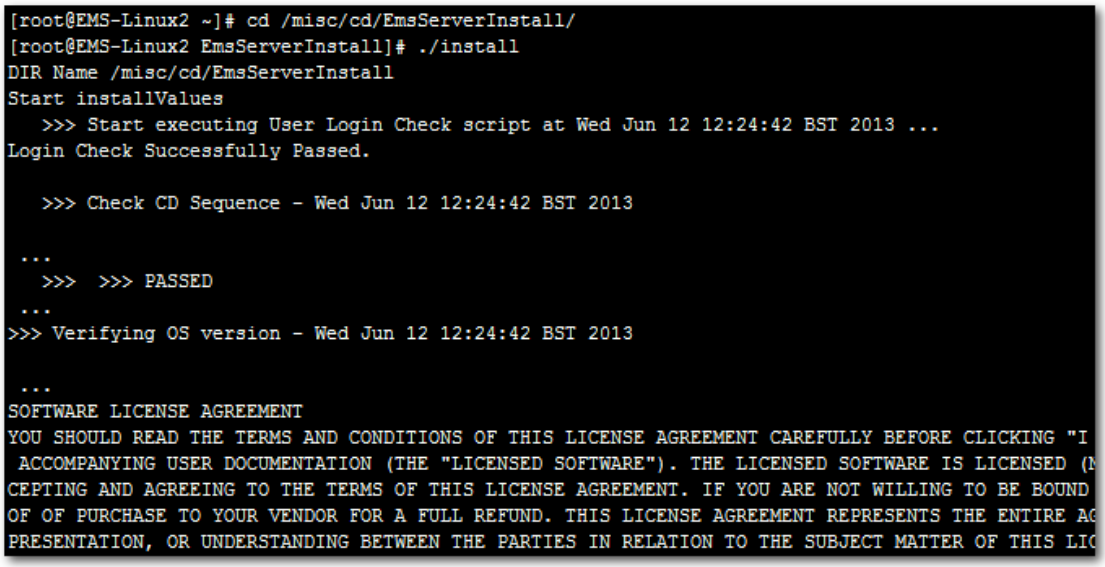
6. Change directory to the script location:

```
cd /mnt/EmsServerInstall/
```

5. Run the installation script from its location:

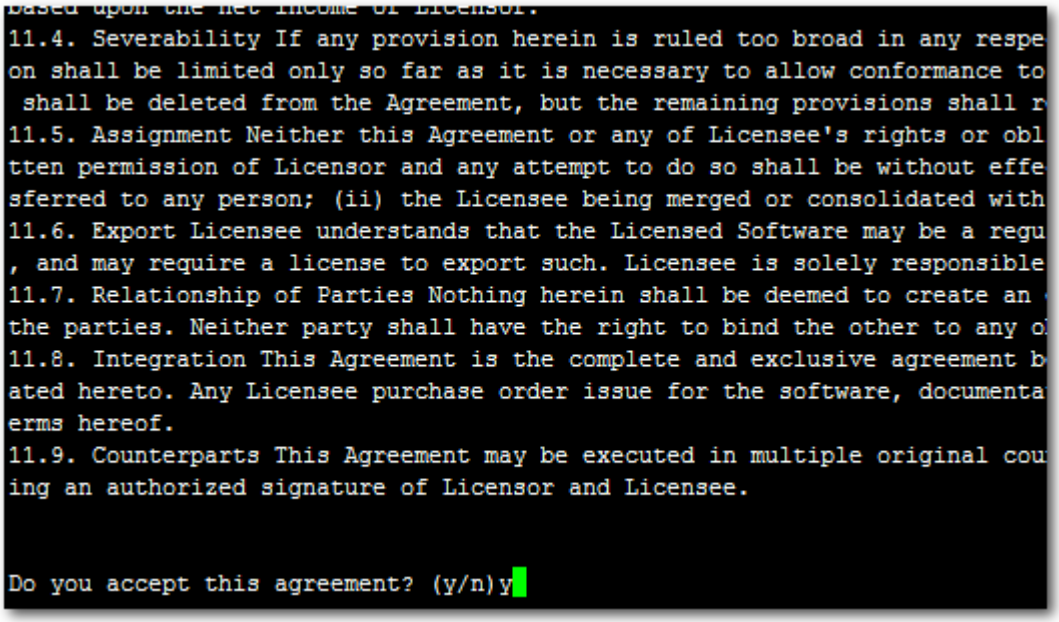
```
./install
```

Figure 9-9: OVOC server Application Installation



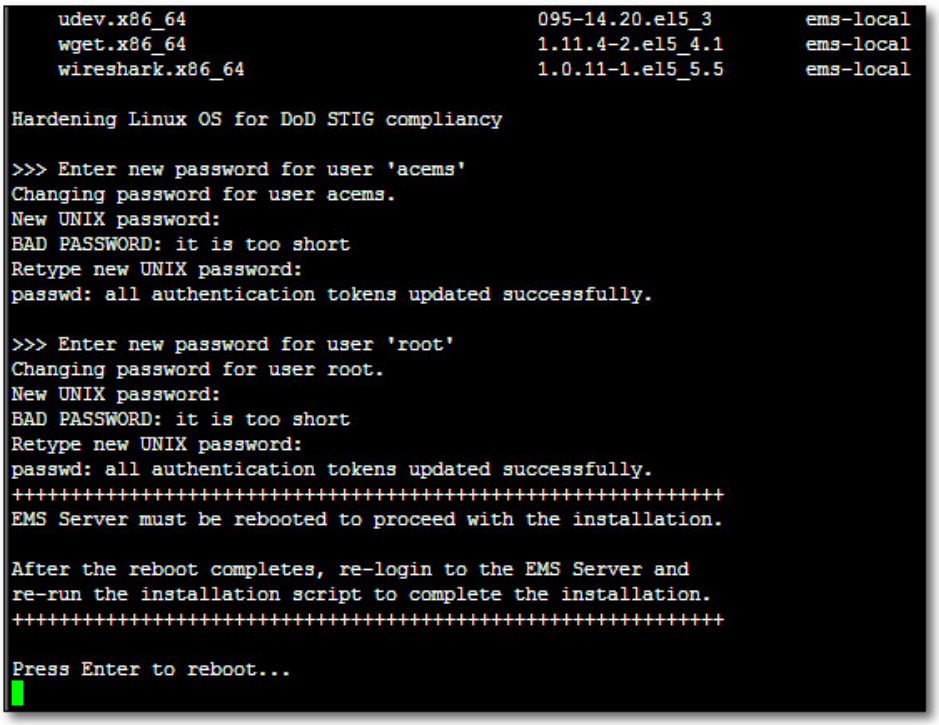
7. Enter **y**, and then press Enter to accept the License agreement.

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



8. 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.

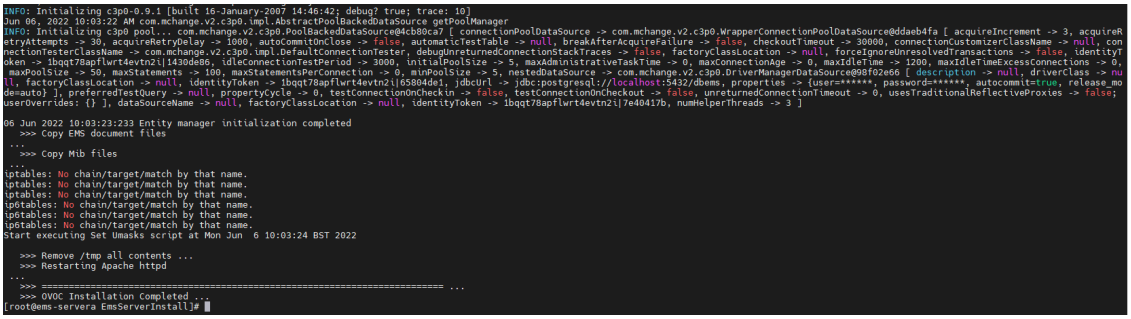
Figure 9-11: OVOC server Application Installation (cont)



9. 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:**

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 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:

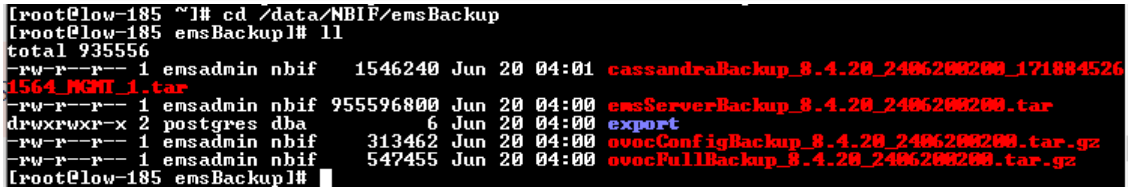
```
cd /mnt/EmsServerInstall/
```

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
```



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*):

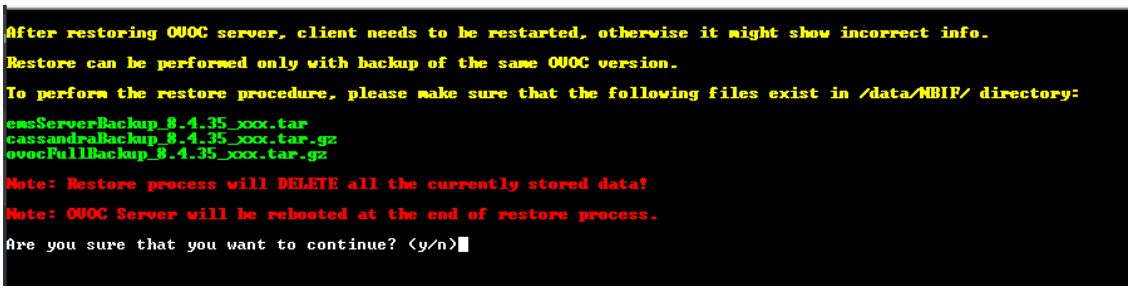
```
su - root
```

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
```

16. 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.

The restore process may take a few minutes.



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

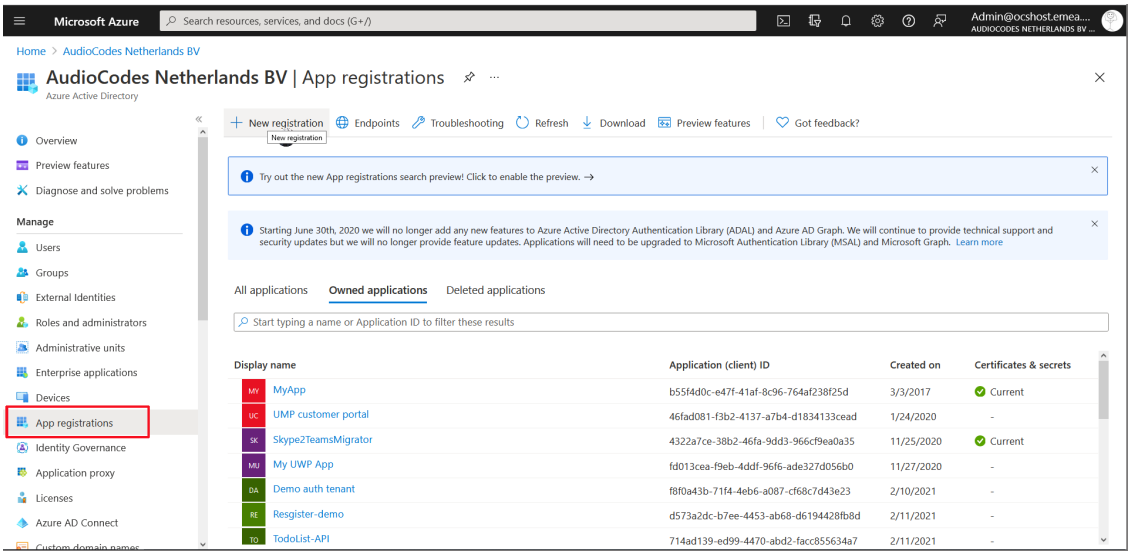
Registering Single Tenant in Organizational Directory

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:**

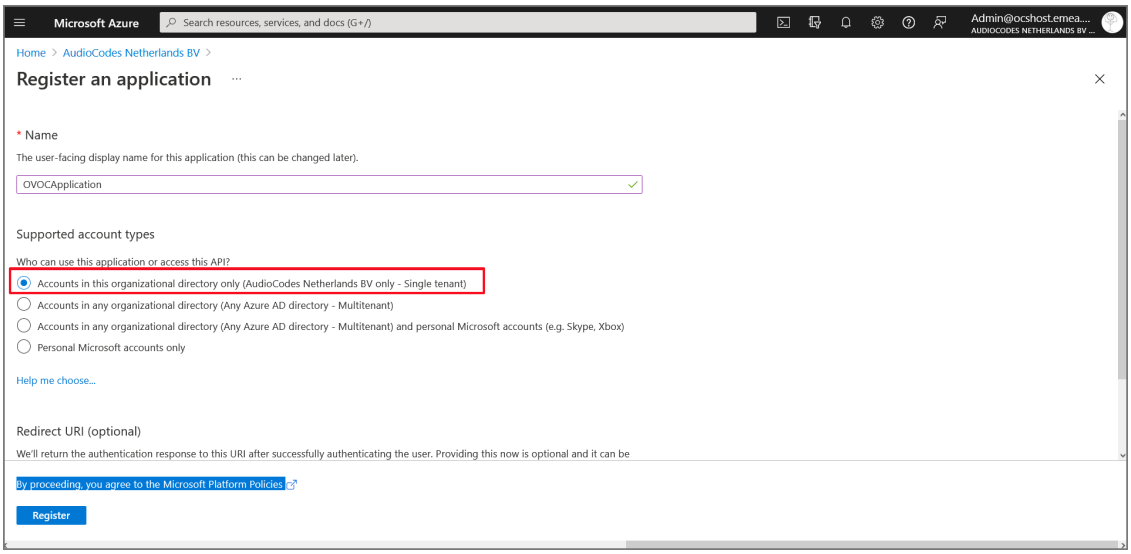
1. Login to the Azure portal with tenant admin permissions.
2. In the Navigation pane, select **App registrations** and then click **New registration**.

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)**.

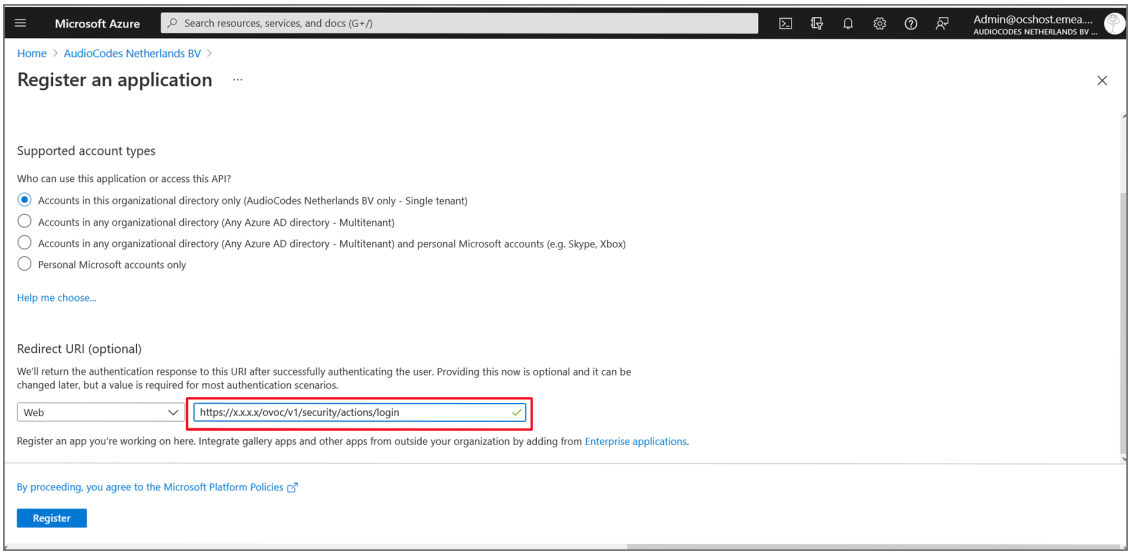
Figure 11-2: Single Organizational Tenant



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

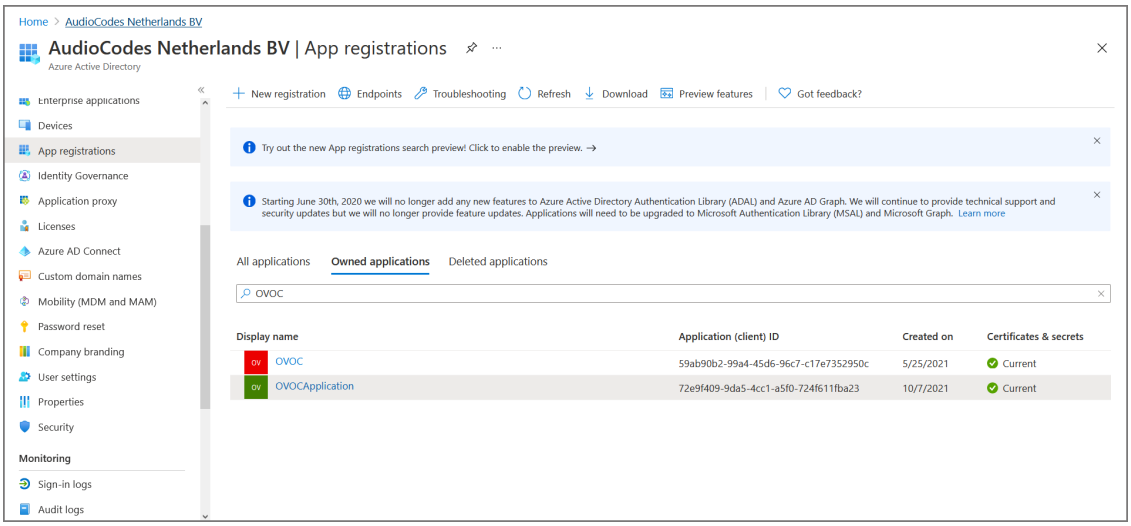
Figure 11-3: Register an application



6. Click **Register**.

   The new registered application is displayed.

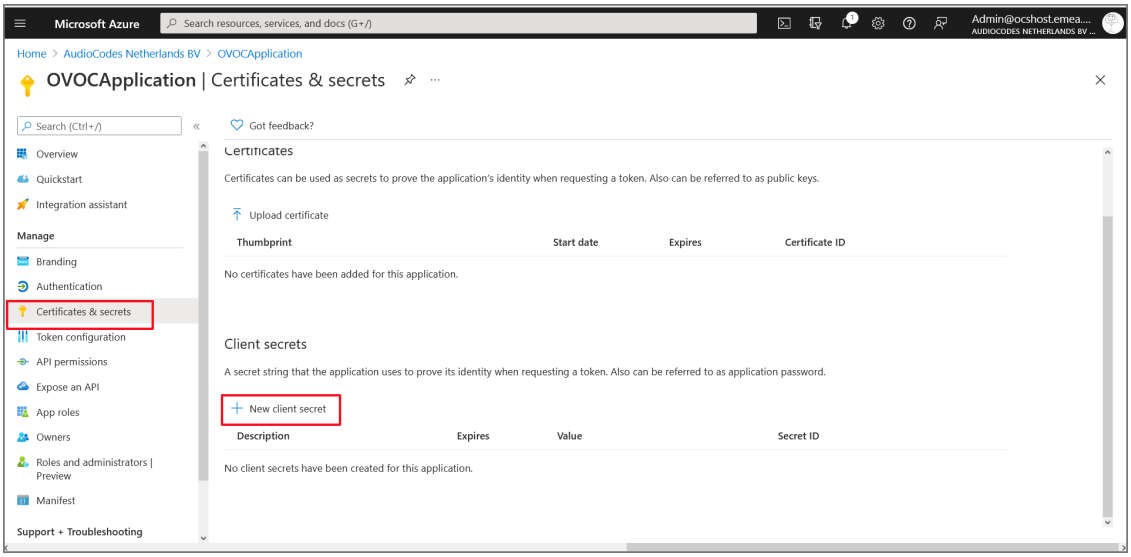
Figure 11-4: New Registered Application



7. Double-click the new application i.e. OVOCApplication (in this example) to configure it.

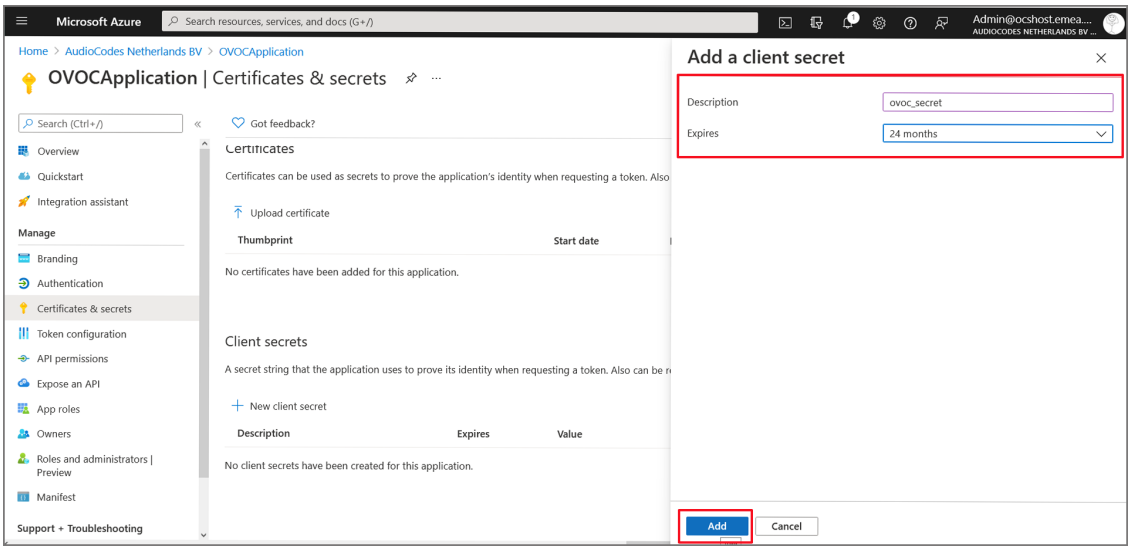
8. In the navigation pane, select **Certificates & secrets**.

Figure 11-5: Certificates & secrets



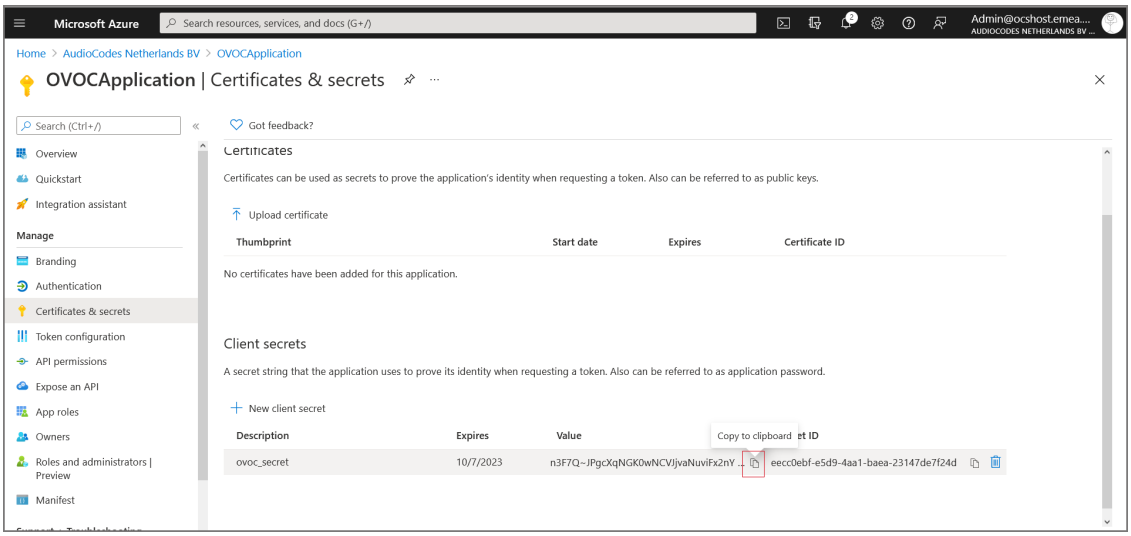
9. Click **New client secret**.

Figure 11-6: New client secret



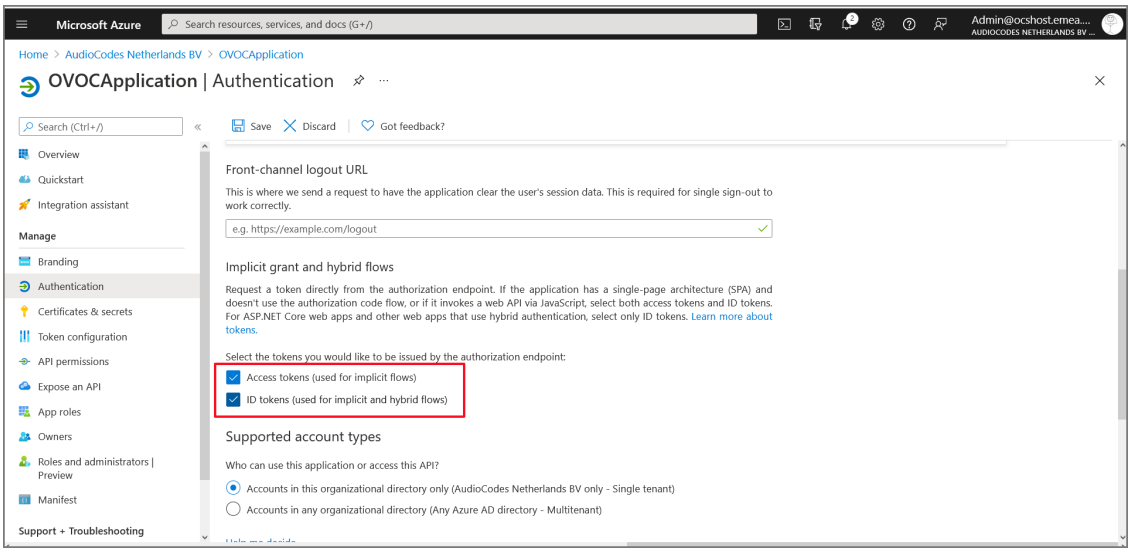
10. Enter a description and from the drop-down list select **24 months**.
11. Click **Add**.

Figure 11-7: Client Secret Generated



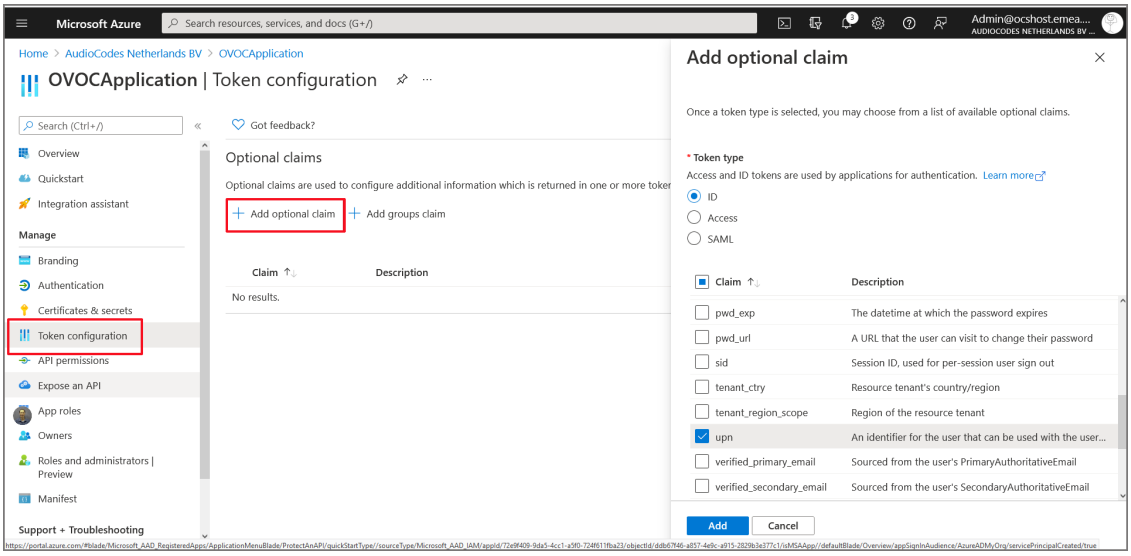
12. Copy the secret Value to clipboard as its required in later configuration and cannot be retrieved once you leave this screen.
13. In the navigation pane, select **Authentication**.

Figure 11-8: Authentication



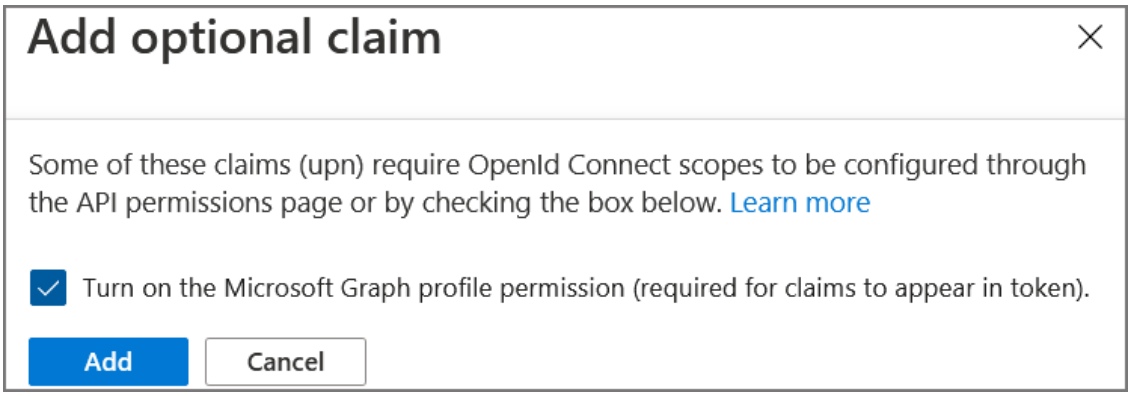
14. Under Implicit grant and hybrid flows select the following:
    - **Access tokens (used for implicit flows)**
    - **ID tokens (used for implicit and hybrid flows)**
15. Click **Save**.
16. In the navigation pane, select **Token configuration**.

Figure 11-9: Token configuration



17. Select **Add optional claim.**
18. Under Token Type, select **ID**.
19. Under Claims, select the **upn** check box.
20. Click **Add.**

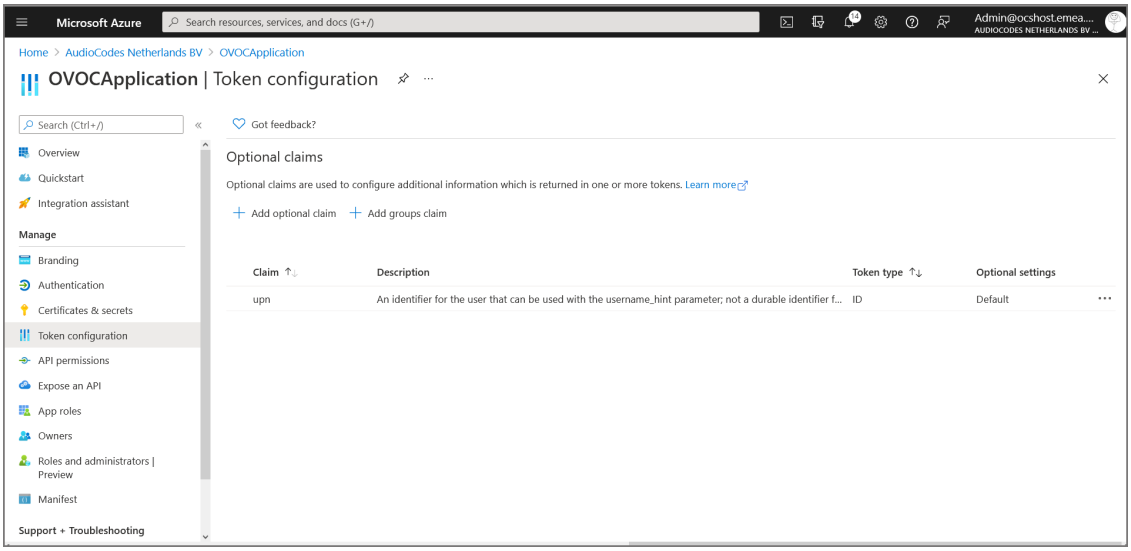
Figure 11-10: Add Optional claim



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.

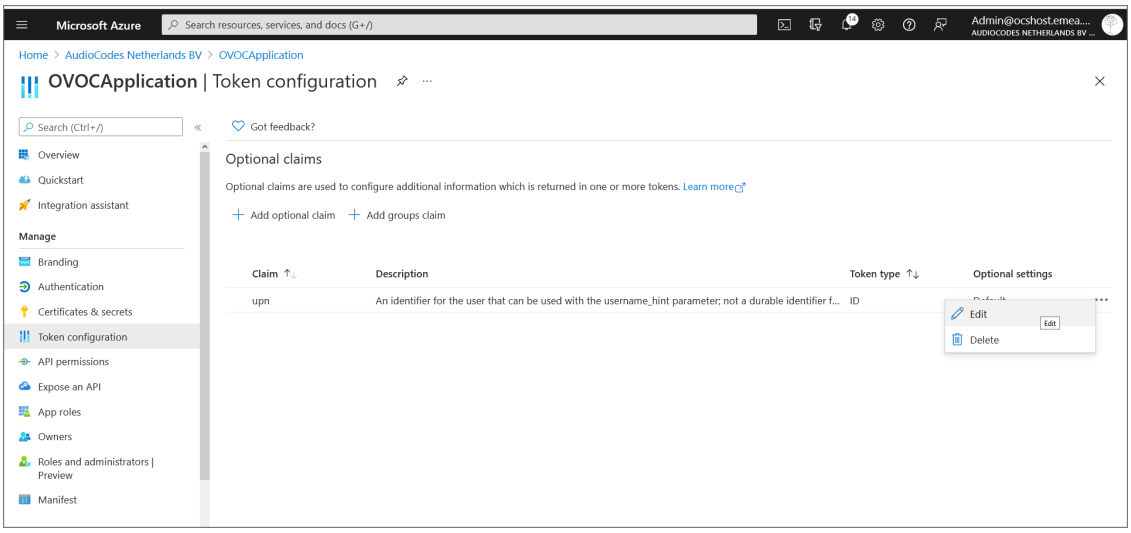
    The new claim is displayed.

Figure 11-11: New UPN Claim



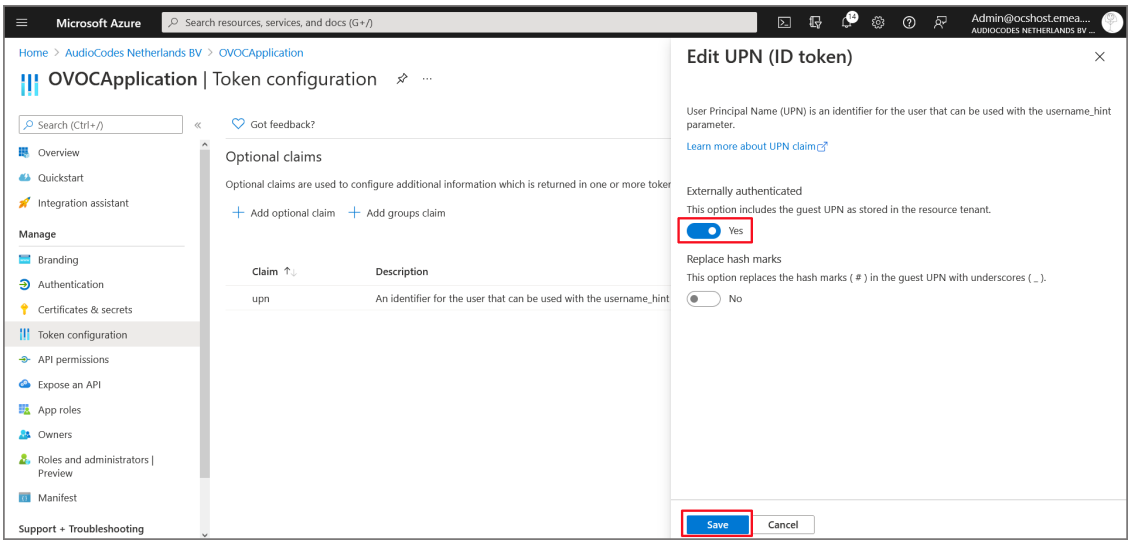
22. Right-click the newly added token and select **Edit.**

Figure 11-12: Edit Optional Claim



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).

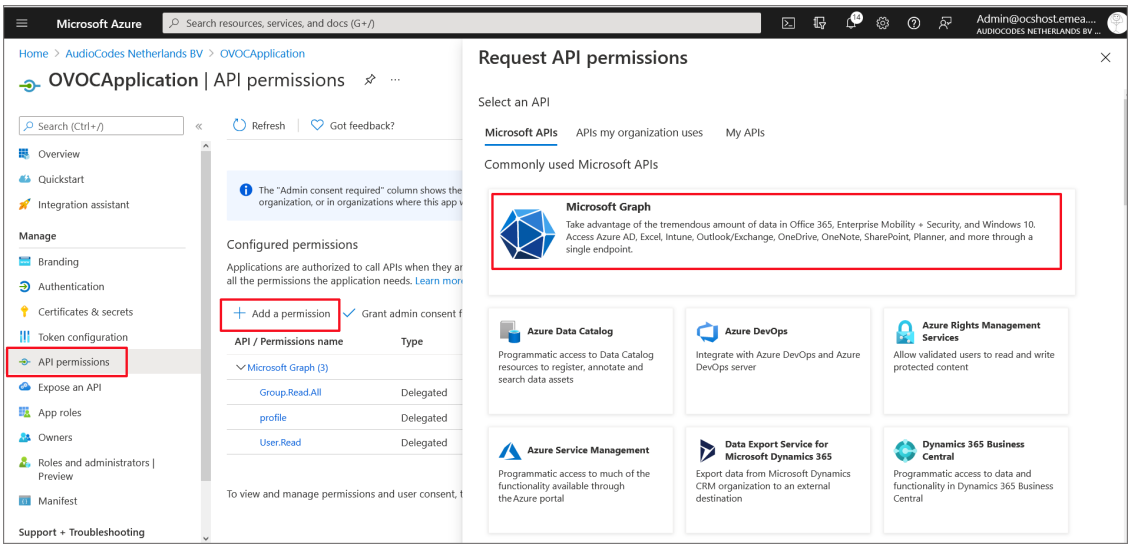
Figure 11-13: Edit UPN (ID token)



24. Click **Save**.

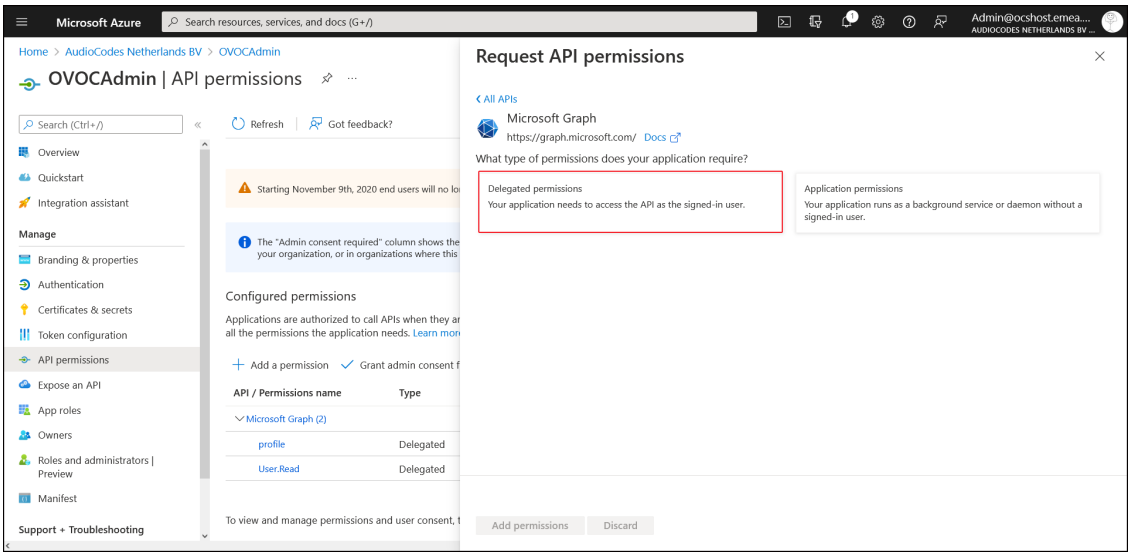
25. In the Navigation pane, select **API permissions**.

Figure 11-14: API Permissions



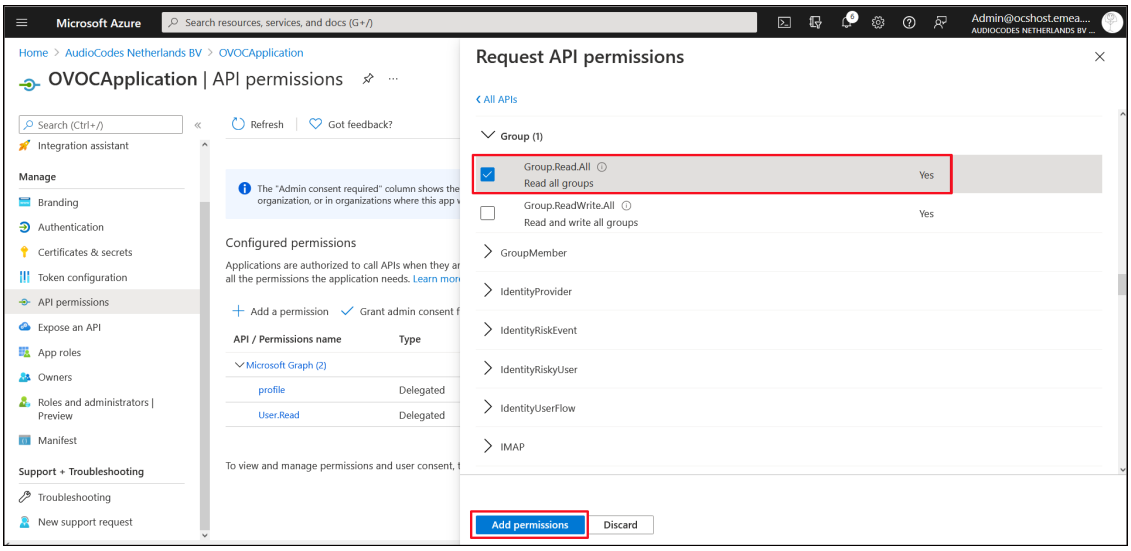
26. Click **Add a permission** and then click the **Microsoft Graph** link.

Figure 11-15: Delegated permissions



27. Click **Delegated permissions**.

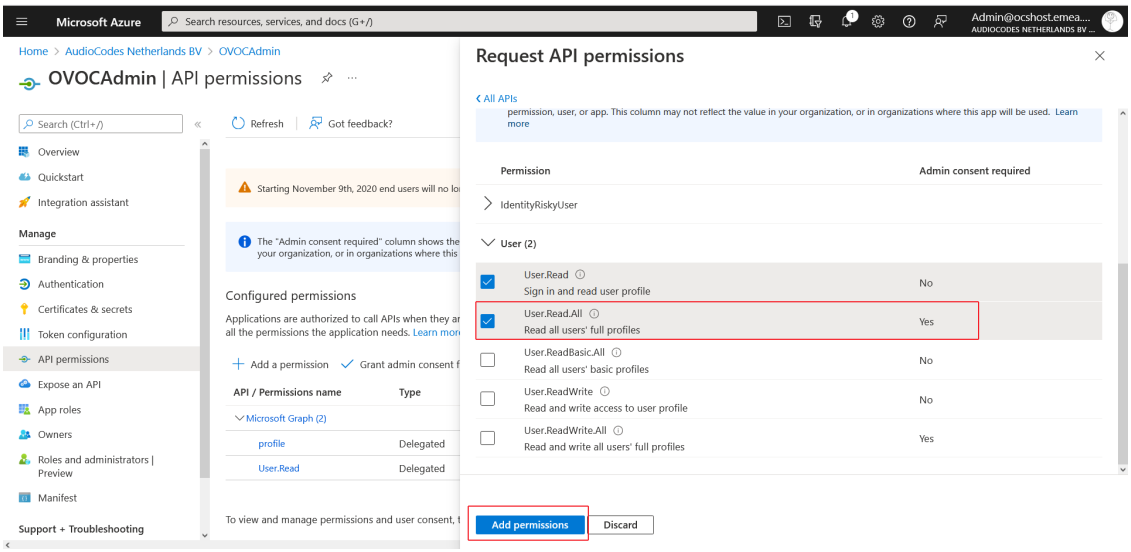
Figure 11-16: Microsoft Graph Permissions



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**.

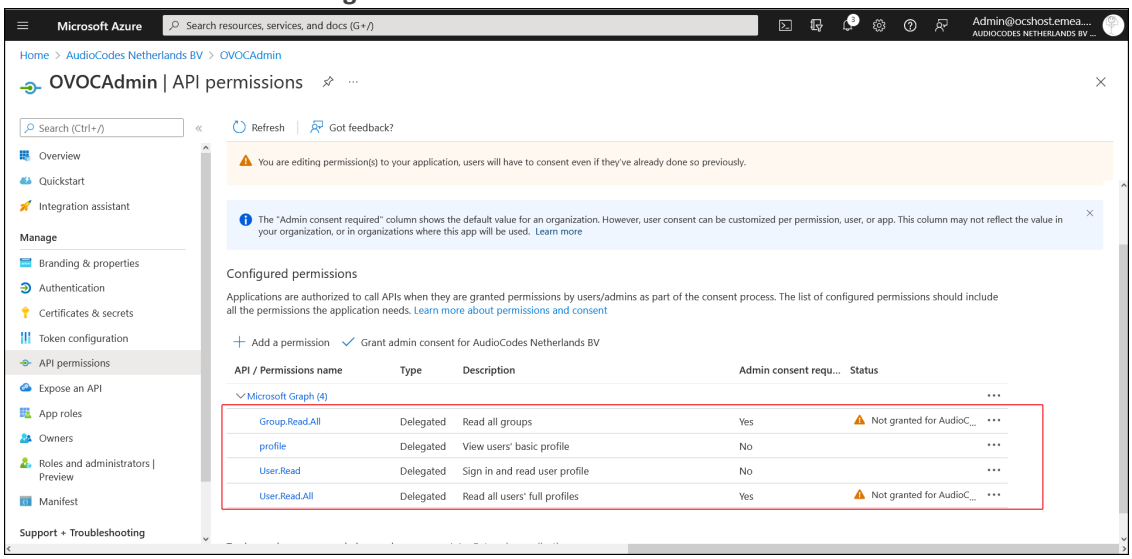
Figure 11-17: Delegated permissions



The configured API permissions are displayed.

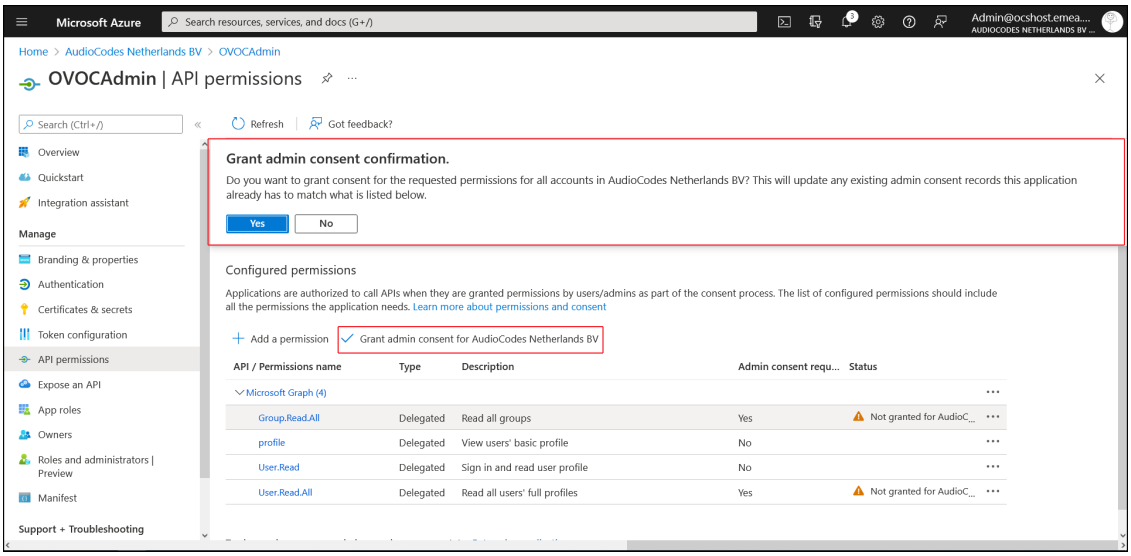
Figure 11-18: Configured API Permissions

Figure 11-19:



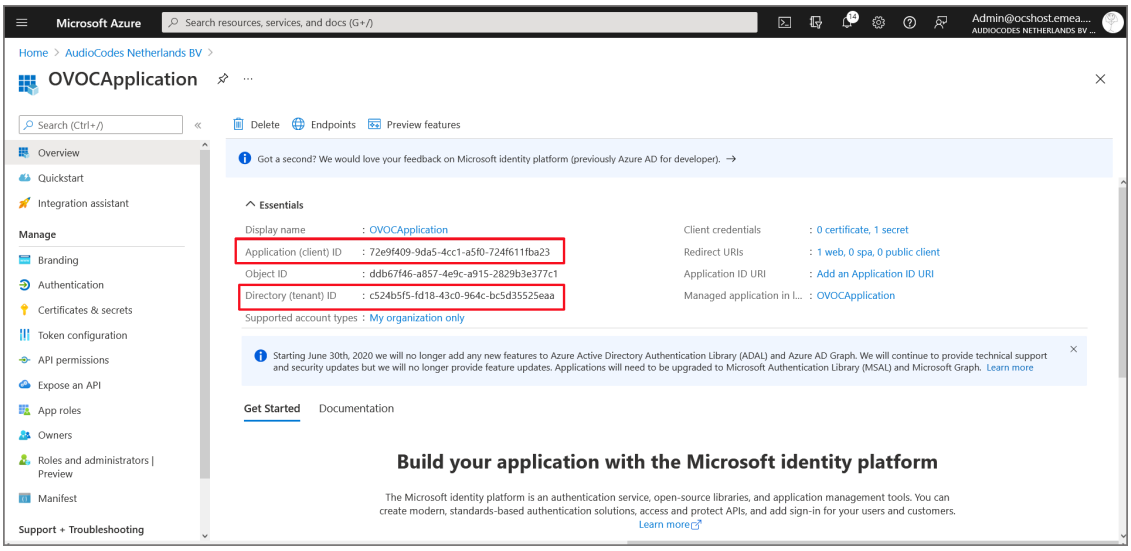
30. Click **Grant admin consent for <Tenant_Name>** link to grant consent for the requested permissions for all accounts for this tenant, and then click **Yes** to confirm.

Figure 11-20: Grant Admin Consent for all Accounts



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

Figure 11-21: Overview Page



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

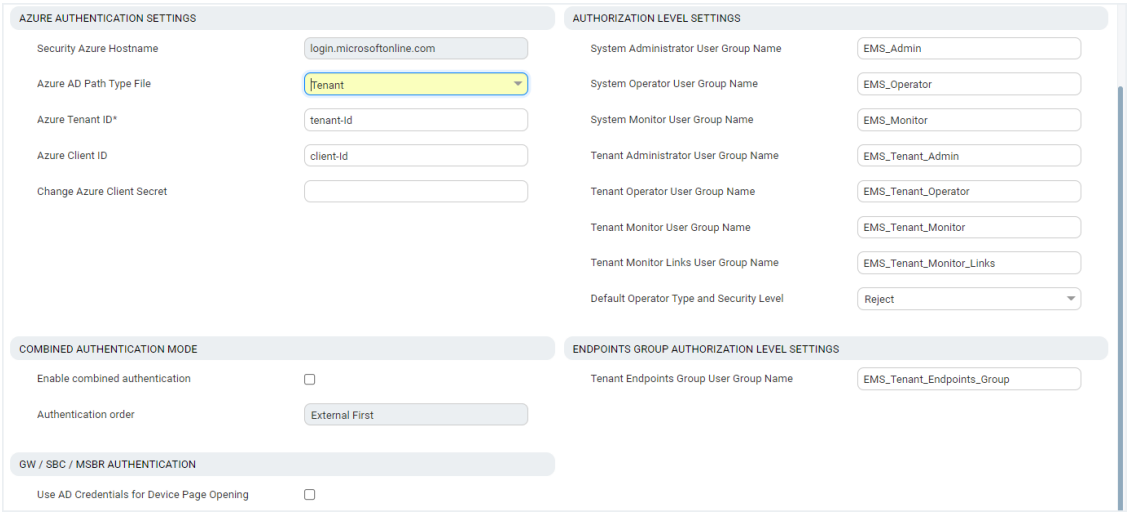
Configuring OVOC Web Azure Settings - Single Tenant Setup

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 :

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

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

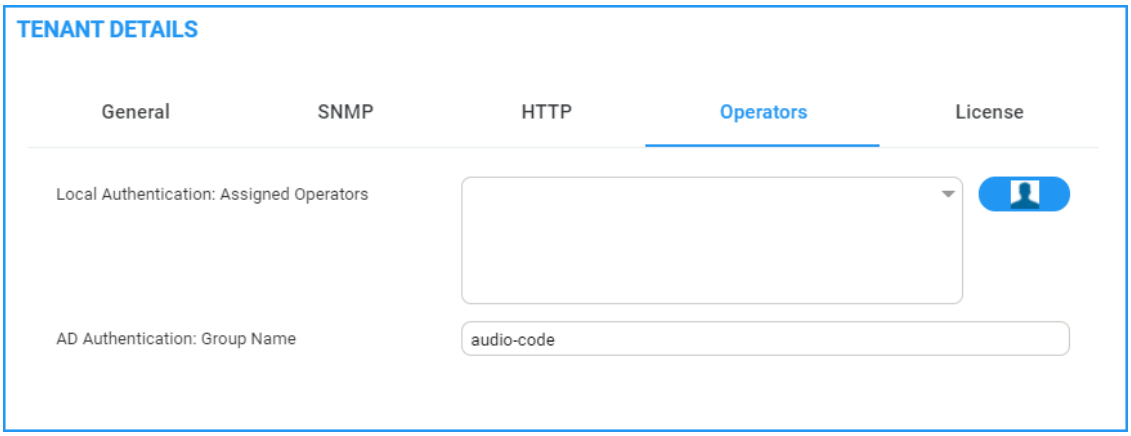
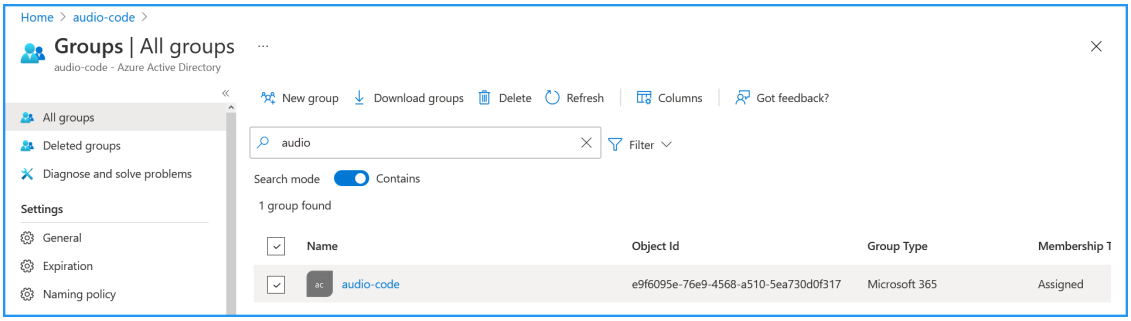


Figure 11-24: Matching Group on Azure



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.

Figure 11-25: Authorization Level Settings

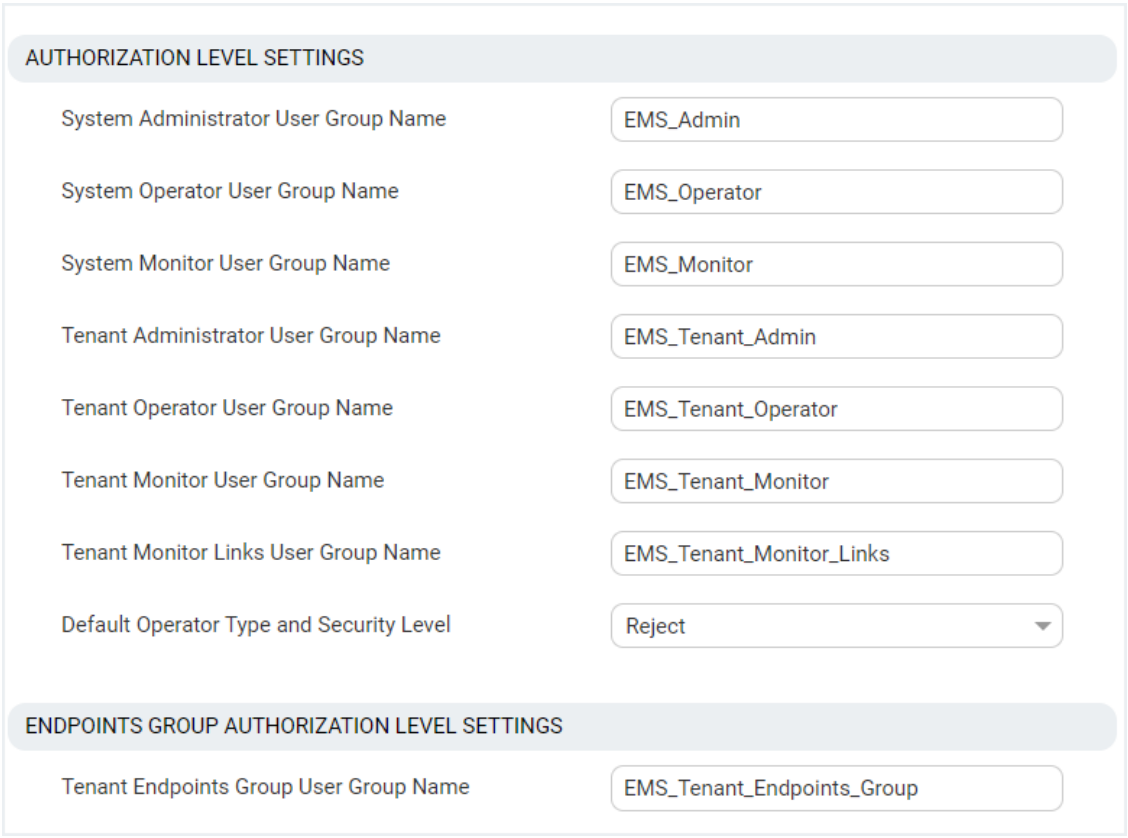
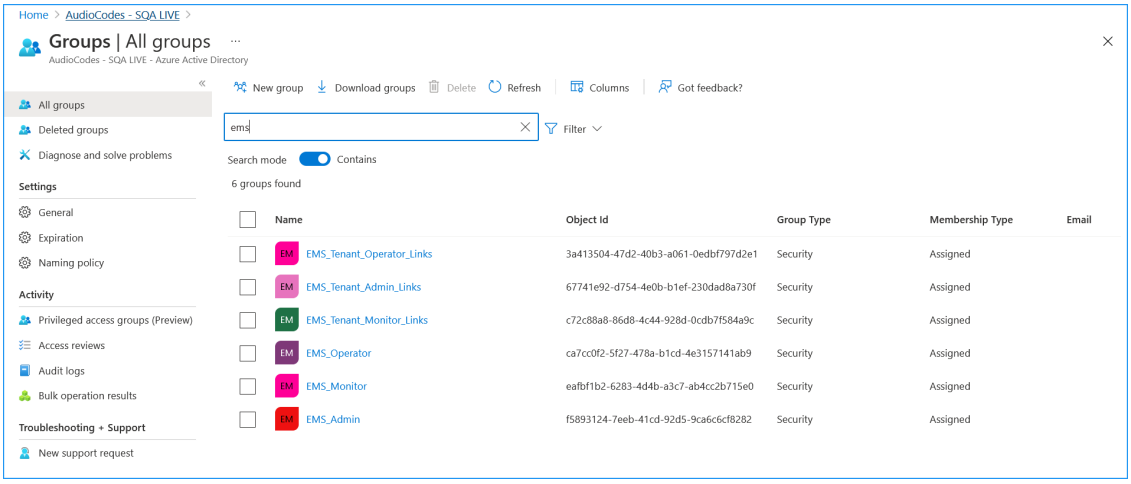


Figure 11-26: Matching Groups on Azure



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**.

Figure 11-27: App Registrations

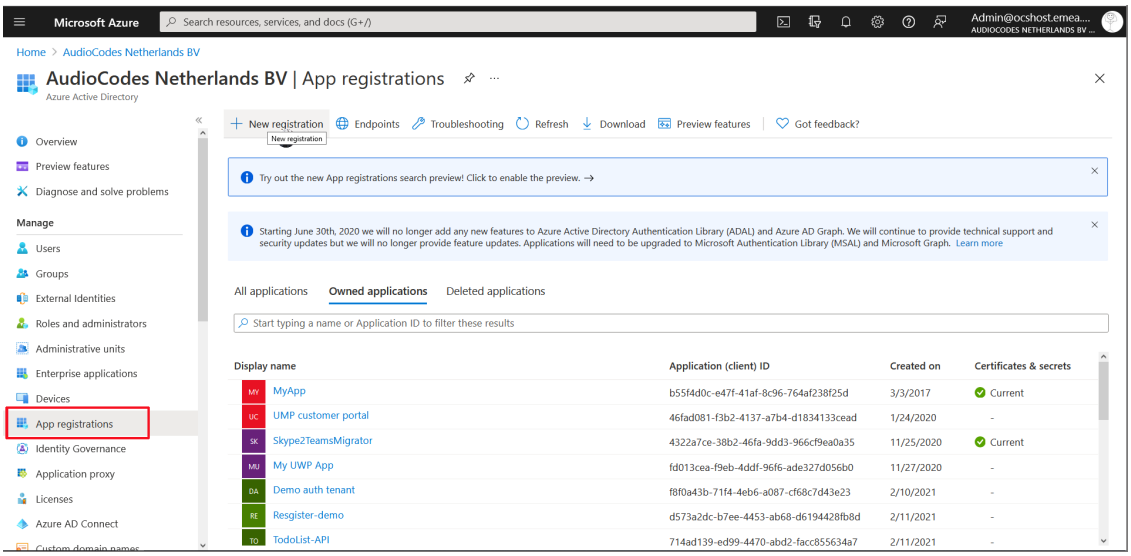
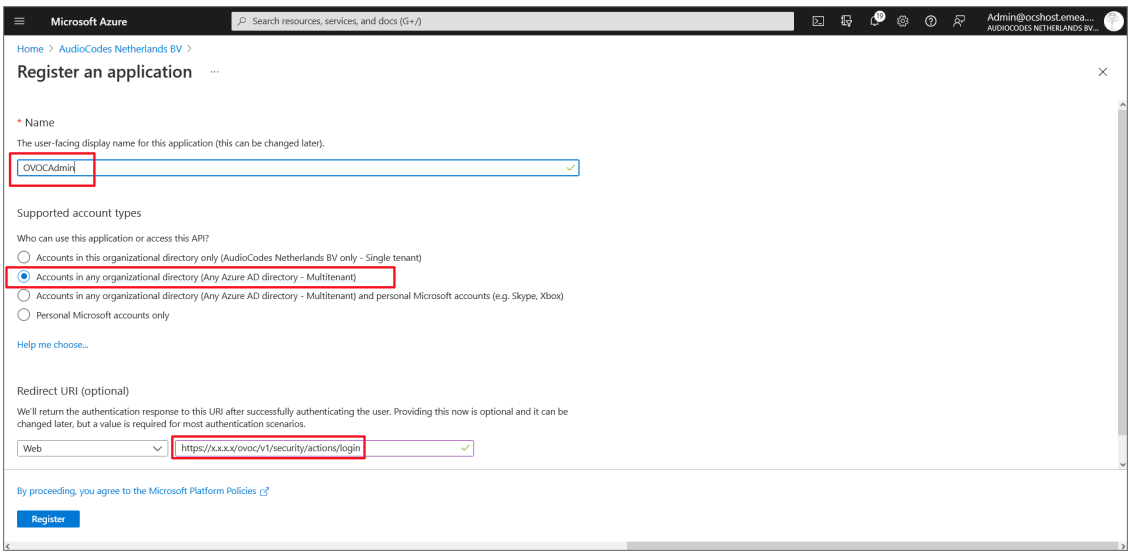


Figure 11-28: New Registration



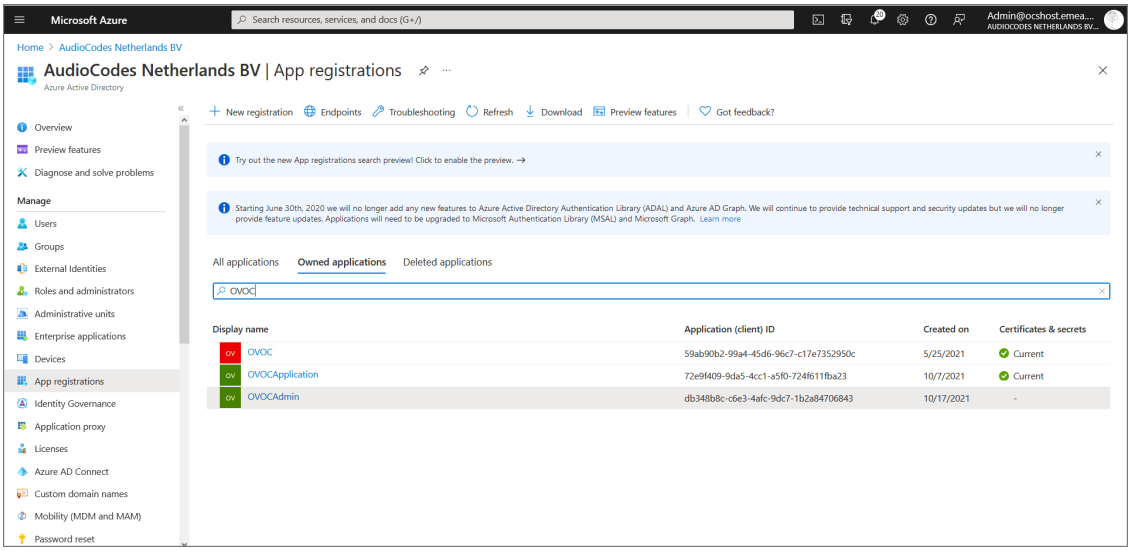
3. Enter the name of the OVOC registration tenant.

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.

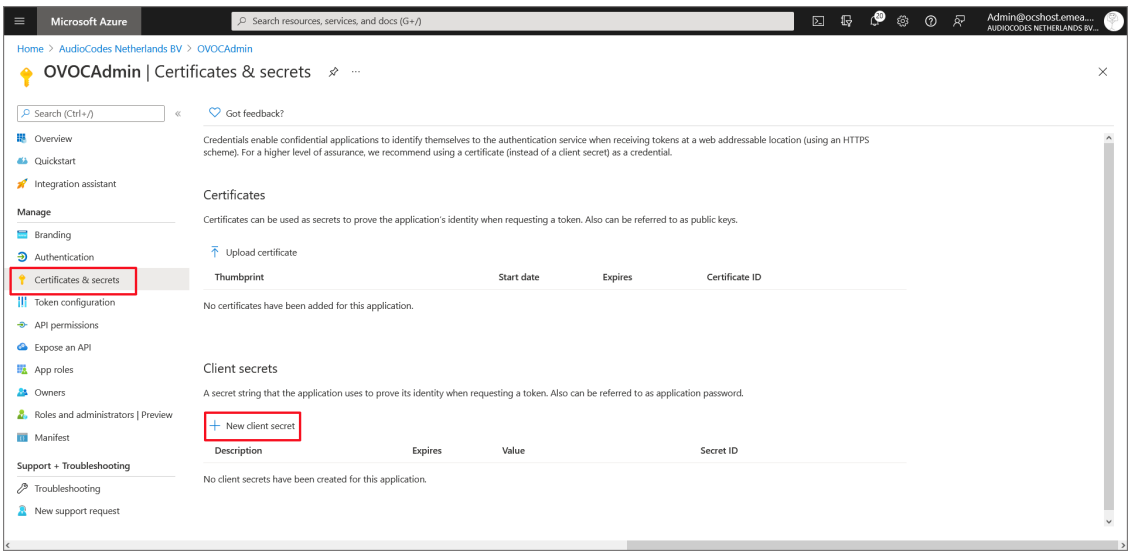
Figure 11-29: New Registered Application



6. Double-click the new application i.e. OVOCAdmin (in this example) to configure it.

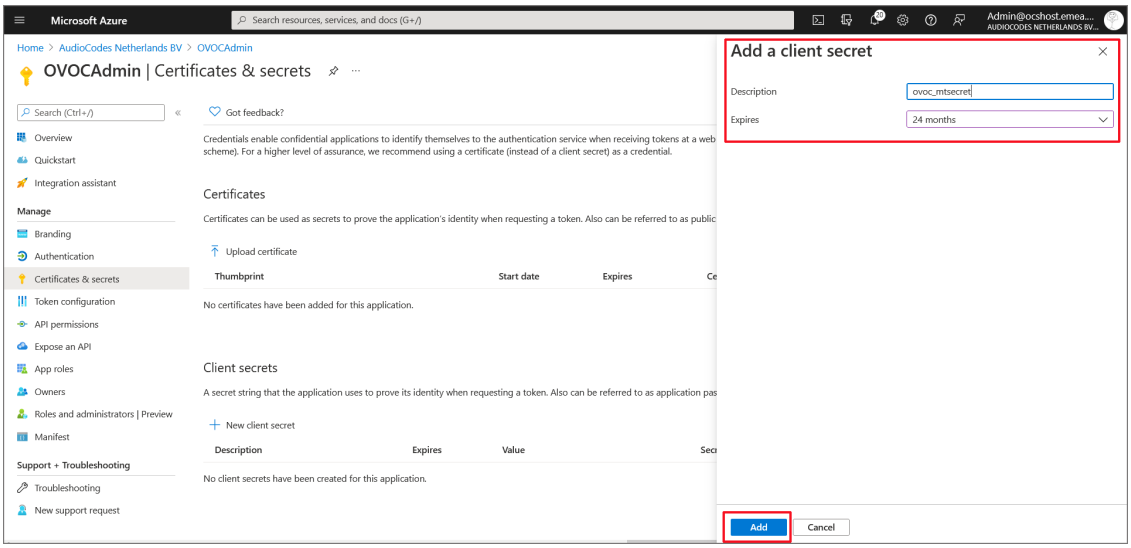
7. In the navigation pane, select **Certificates & secrets**.

Figure 11-30: Certificates & secrets



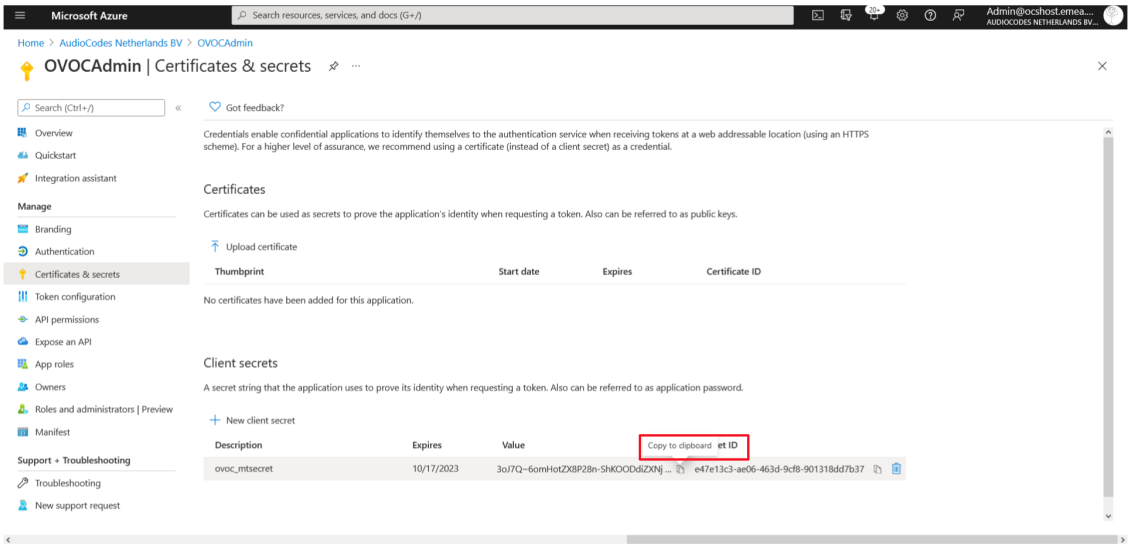
8. Click **New client secret**.

Figure 11-31: New client secret



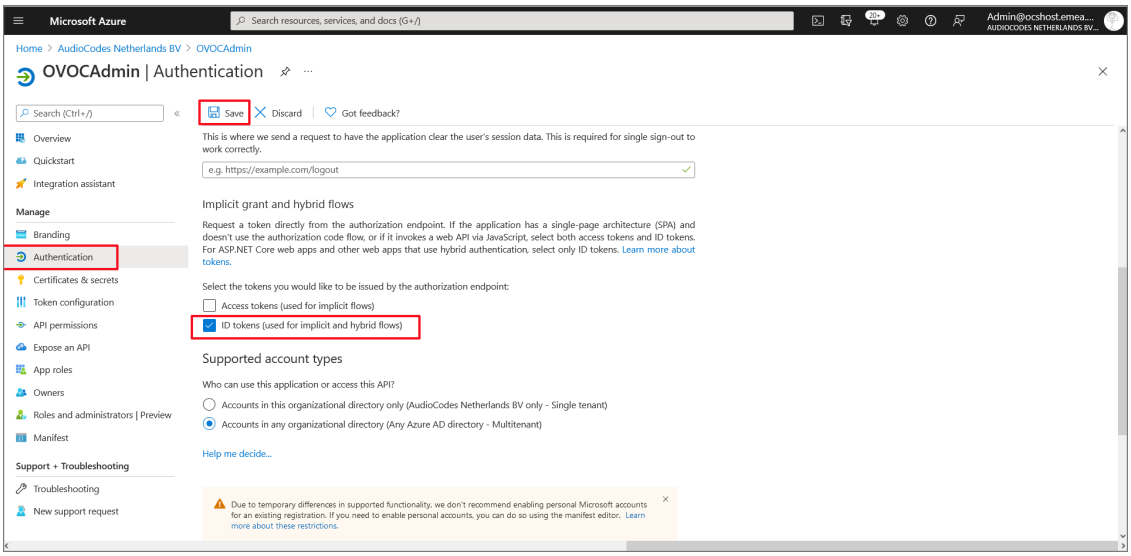
9. Enter a description and from the drop-down list select **24 months**.
10. Click **Add**.

Figure 11-32: Client Secret Generated



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

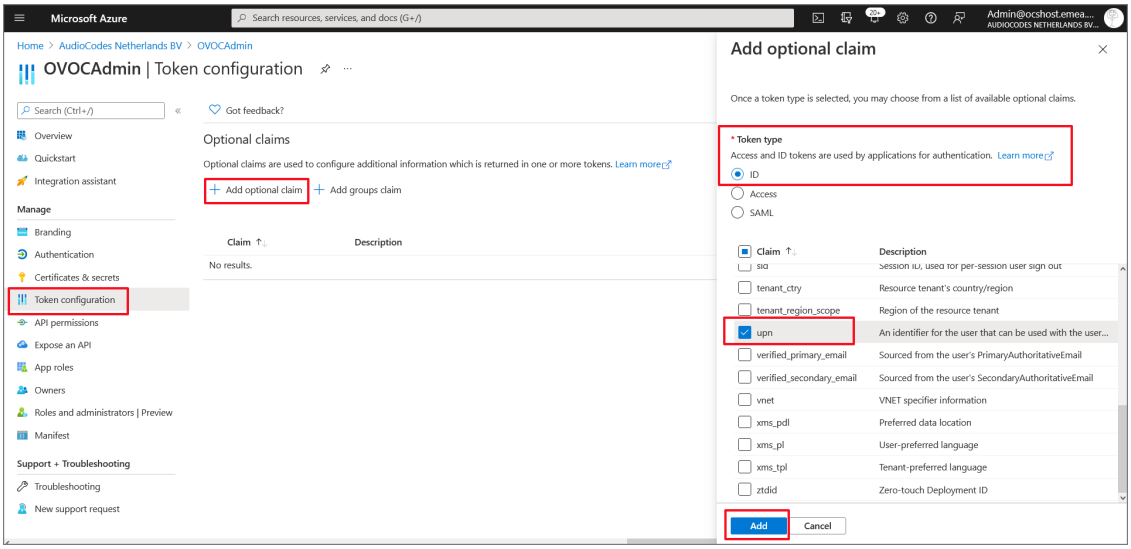


13. Under Implicit grant and hybrid flows, select "ID tokens"

14. Click **Save**.

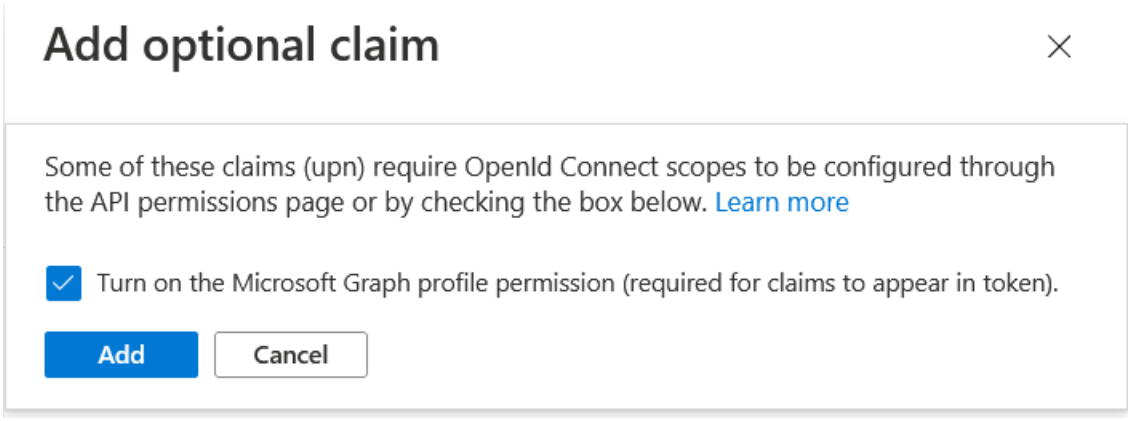
15. In the Navigation pane, select **Token configuration**

Figure 11-34: Token Configuration-Add



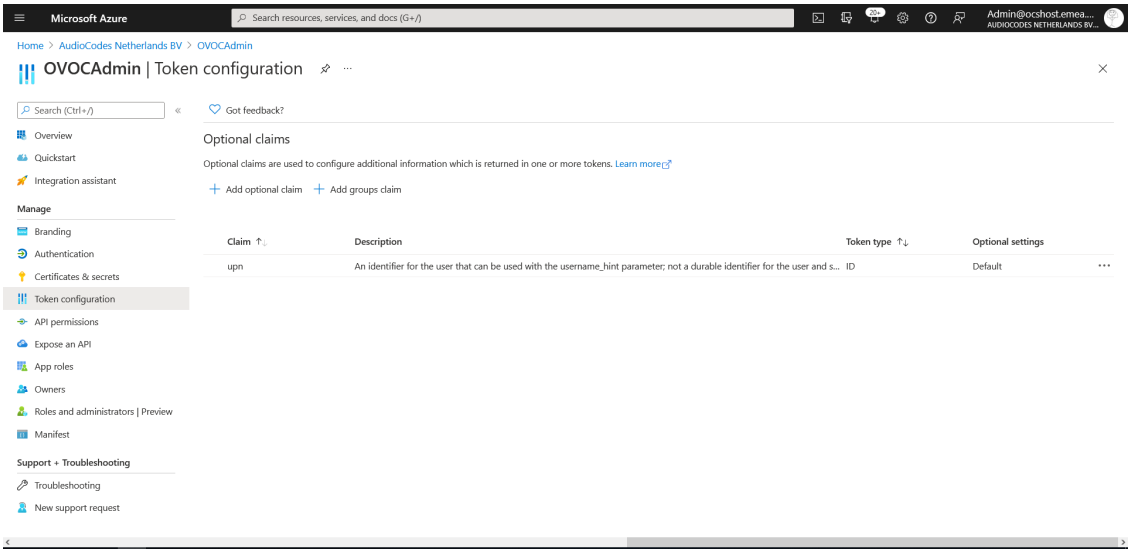
16. Click **Add optional claim**, choose **ID** type then **upn** optional claim and click **Add** to confirm.

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.

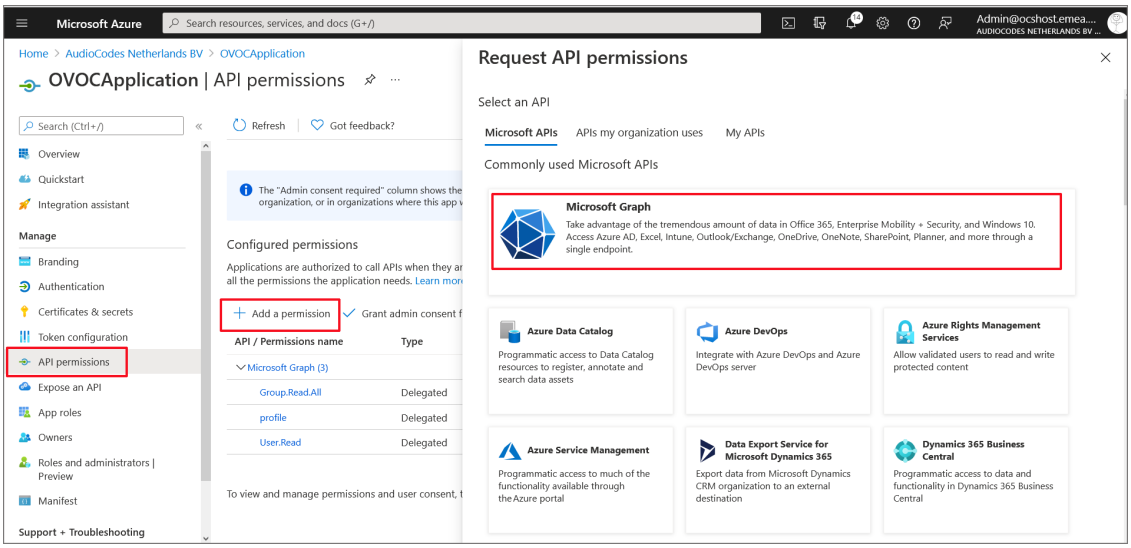
Figure 11-36: Optional claims Added



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.

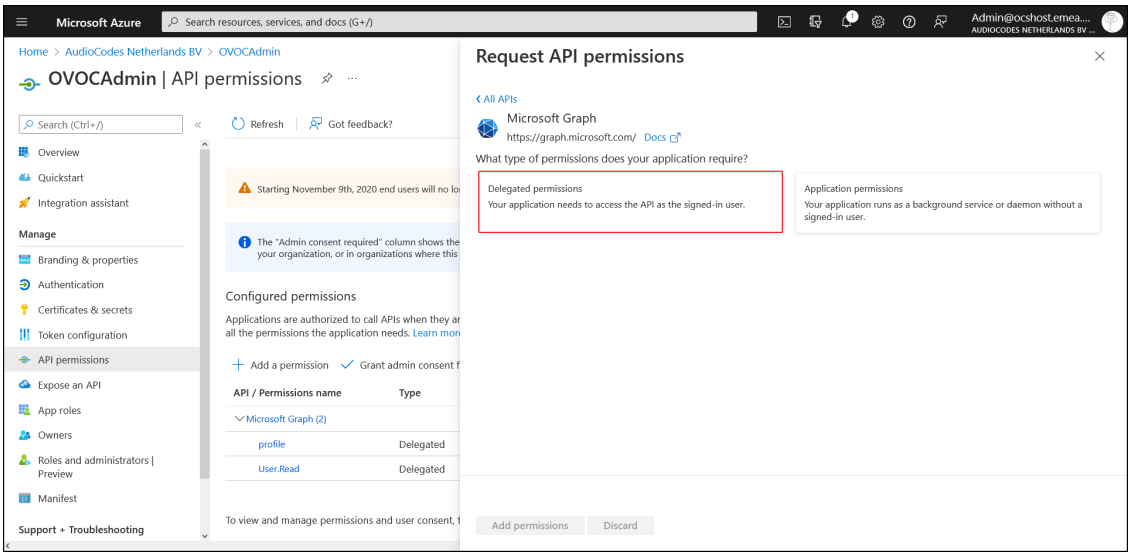
18. In the Navigation pane, select **API permissions**.

Figure 11-37: API Permissions



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

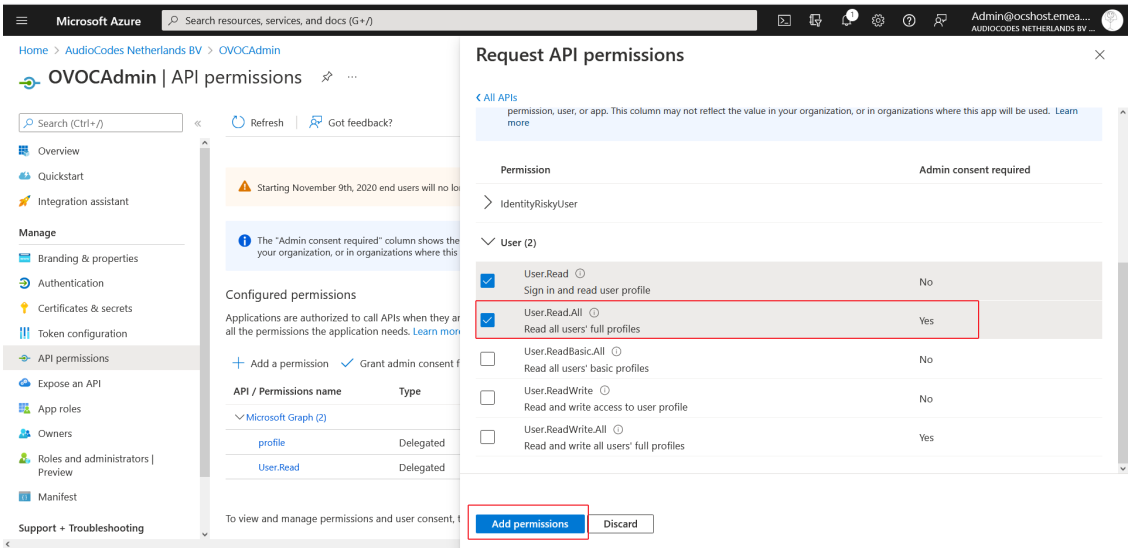
Figure 11-38: Delegated permissions



20. Click **Delegated permissions**.

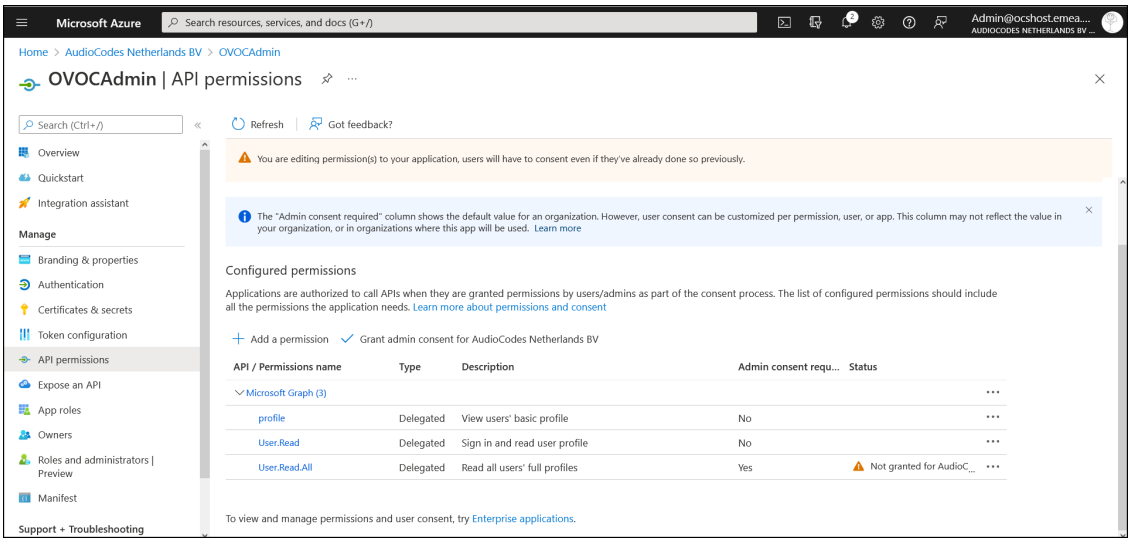
21. Select permission **User.Read.All** and then click **Add permissons**.

Figure 11-39: Delegated permissions



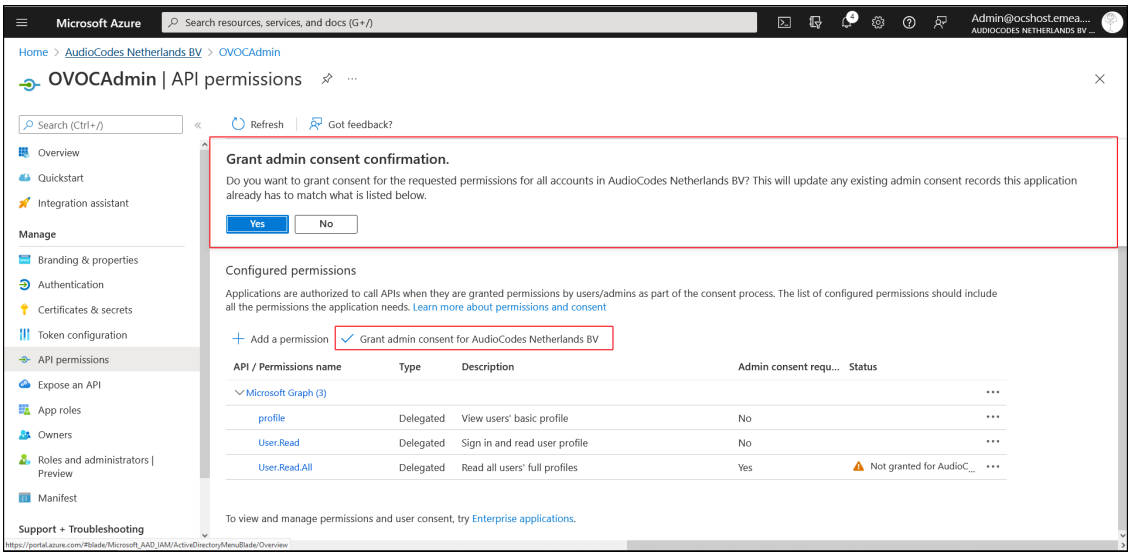
The configured API permissions are displayed.

Figure 11-40: Configured API Permissions



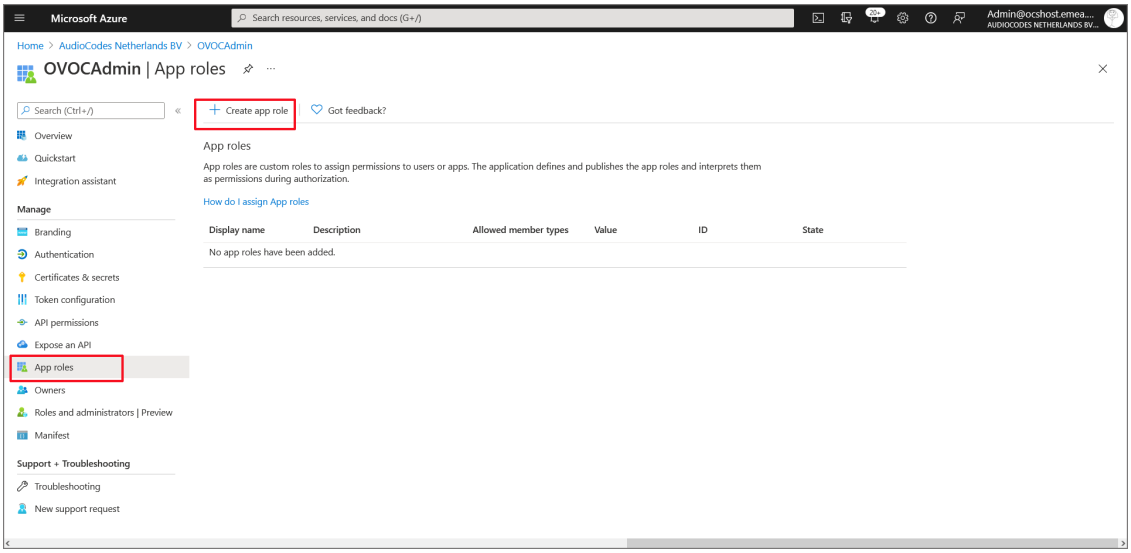
22. Click **Grant admin consent for <Tenant_Name>** link to grant consent for the requested permissions for all accounts for this tenant, and then click **Yes** to confirm.

Figure 11-41: Grant Admin Consent for all Accounts



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

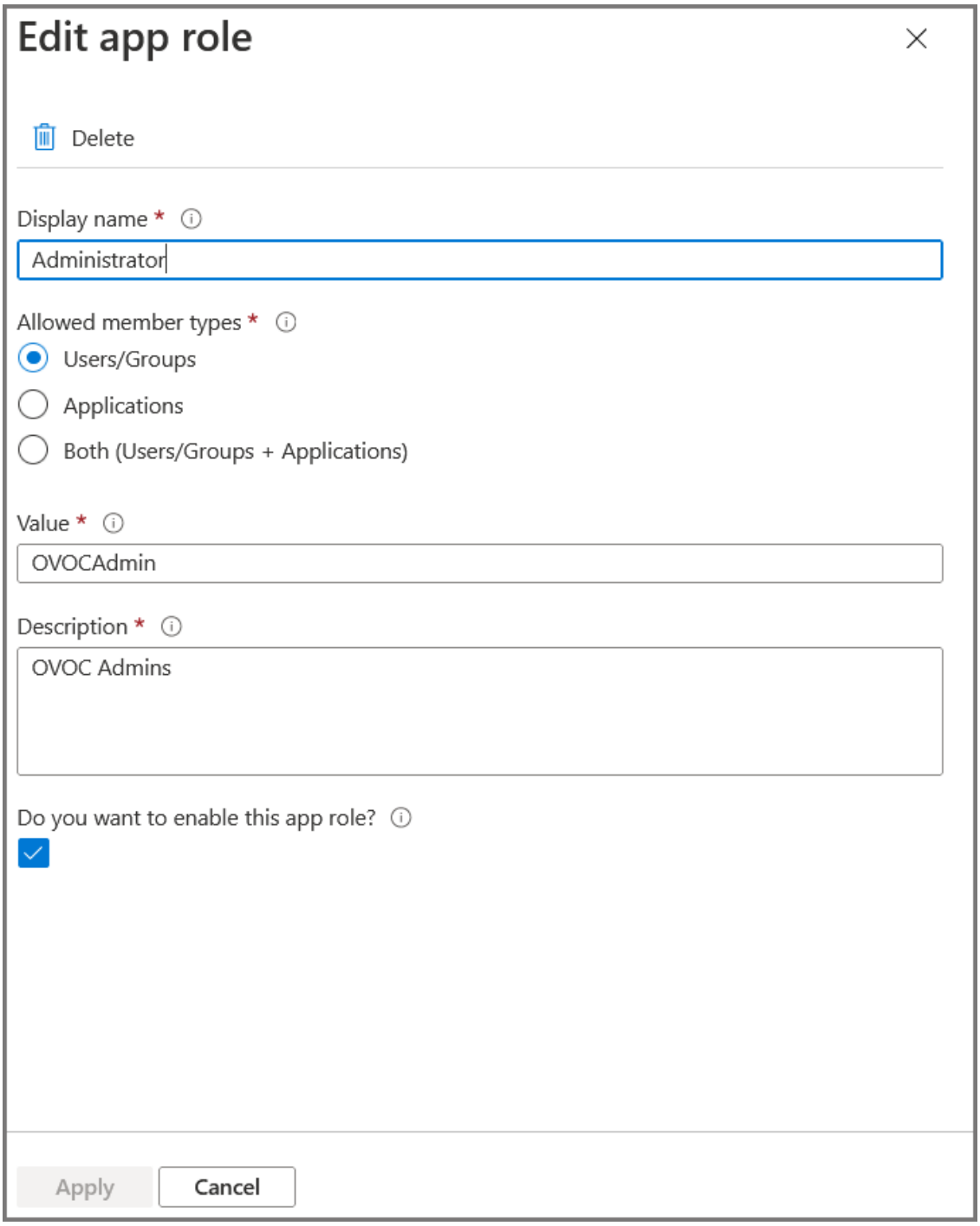
Figure 11-42: App roles



24. Create an app role with Admin permissions:

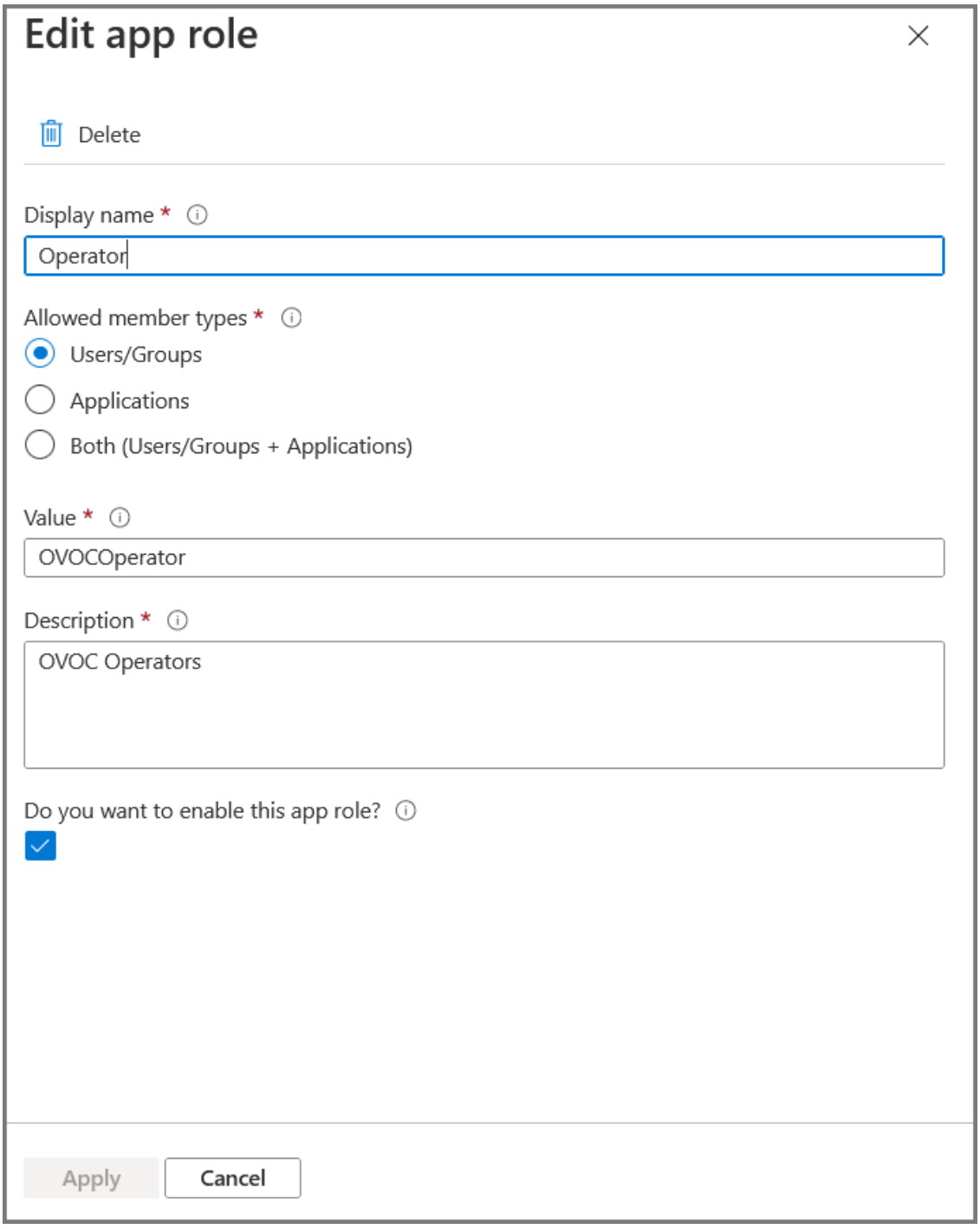
- **a.** In the Display Name field, enter "Administrators" or "Admins"
- **b.** Select Users/Groups check box.
- **c.** Enter value "OVOCAdmin"
- **d.** Select the **do you want to enable this app role** check box.
- **e.** Click **Apply**

Figure 11-43: Admin Role



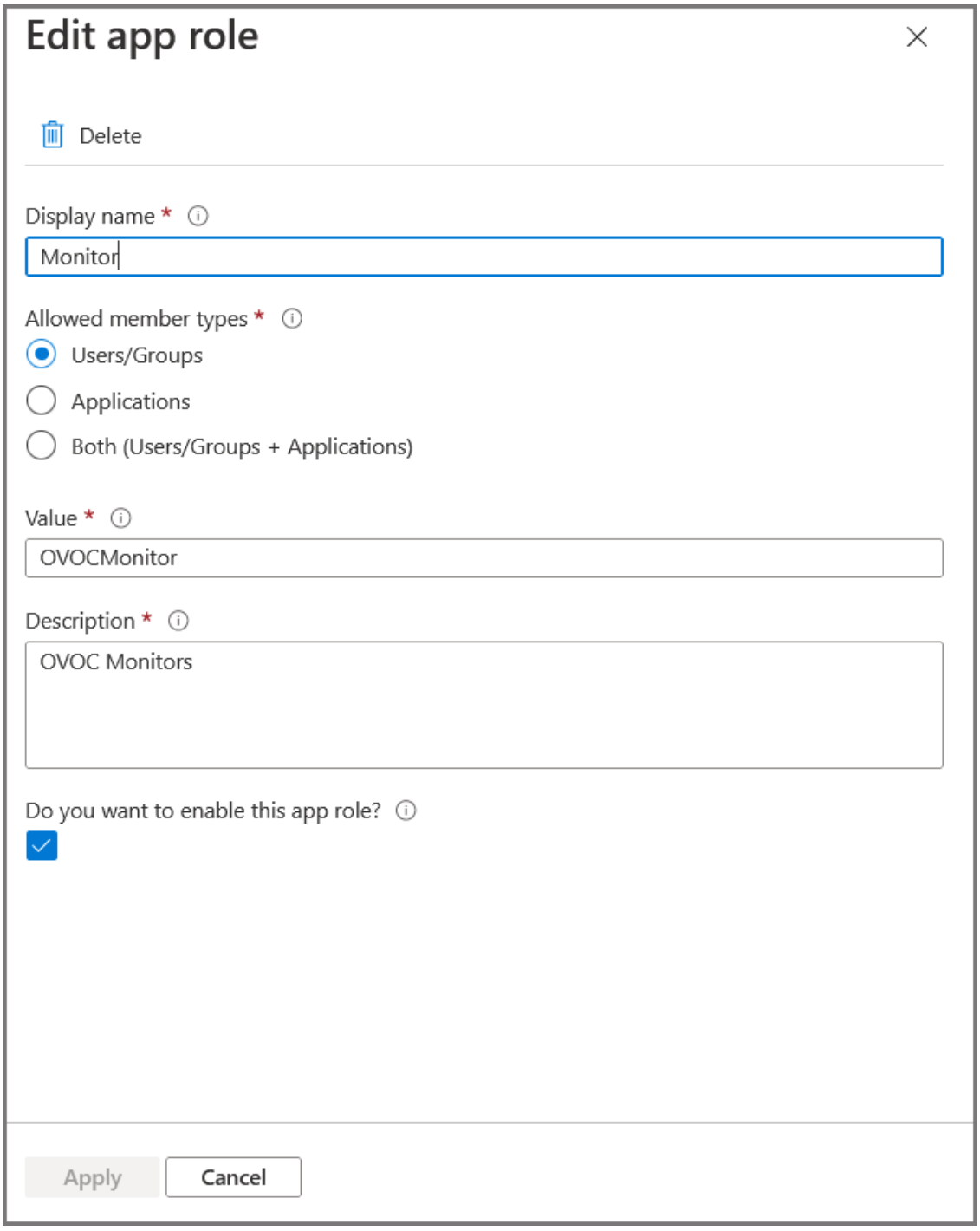
25. Repeat the above steps to create an App role with Operator permissions with value 'OVOCOperator".

Figure 11-44: Operator Role



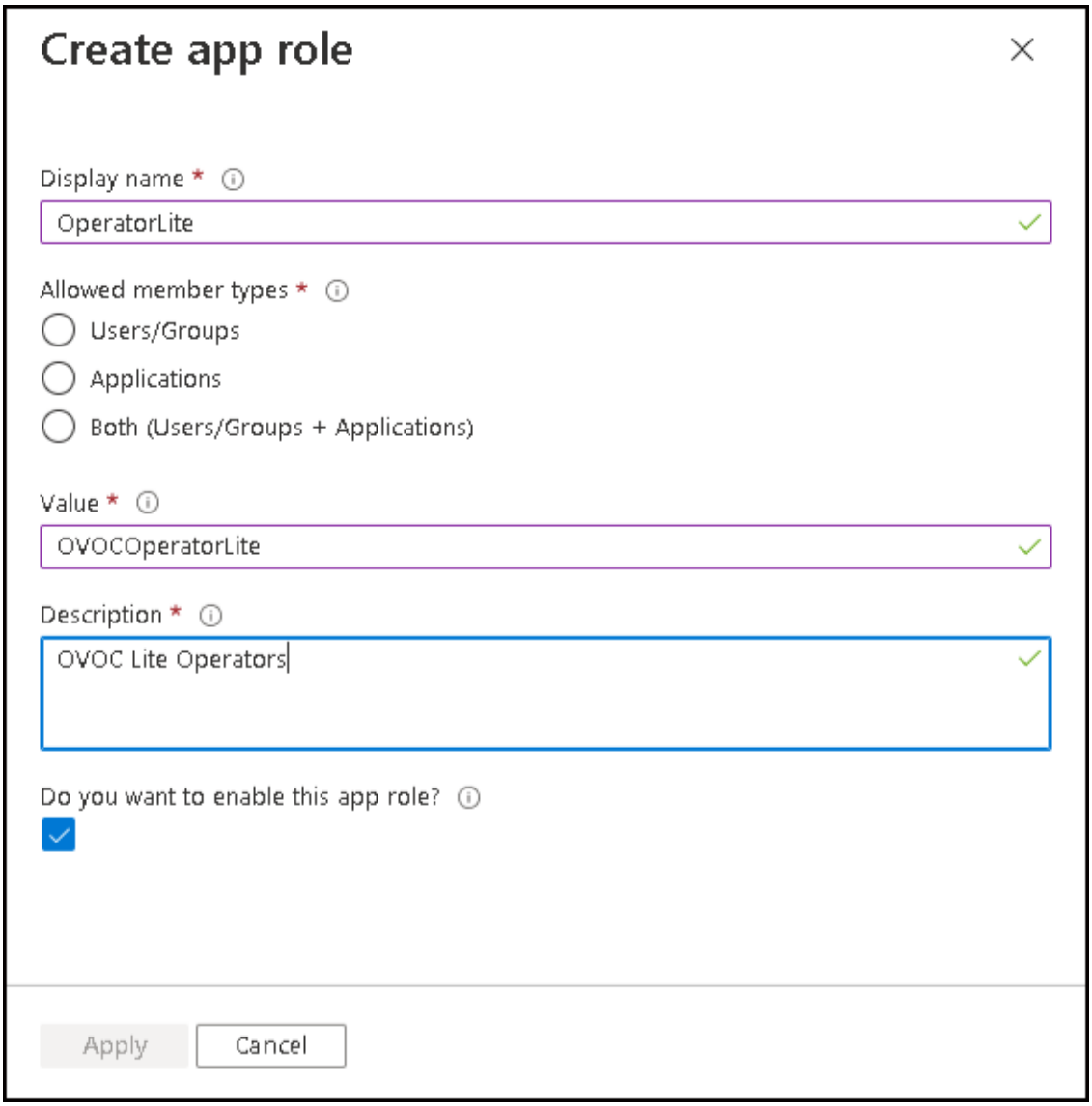
26. Repeat the steps described for adding "Admin" role above to create an app role with Monitor permissions with value "OVOCMonitor".

Figure 11-45: Operator Role



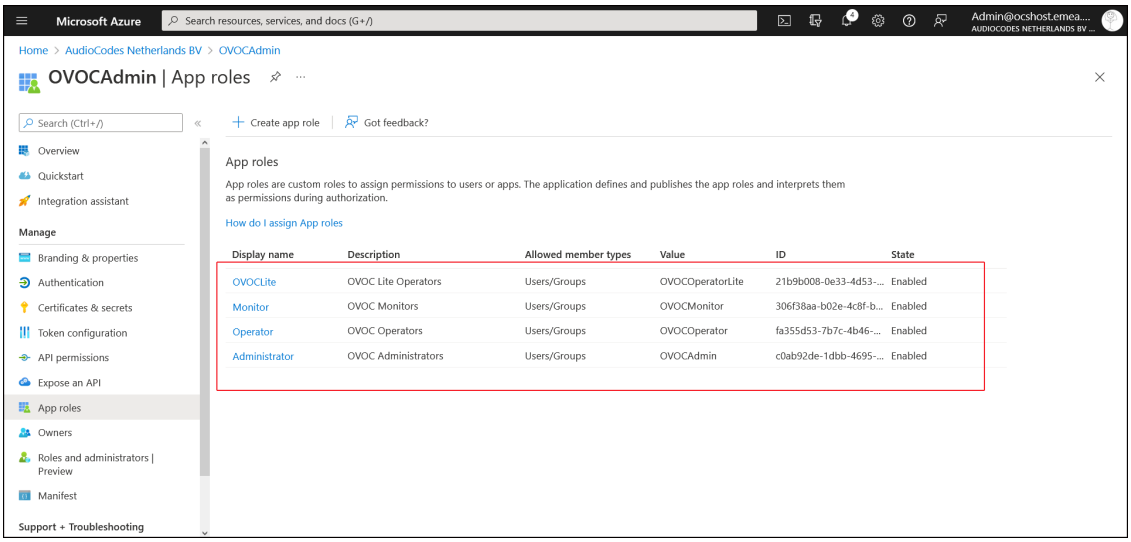
27. Repeat the steps described for adding "Admin" role above to create an app role with Monitor permissions with value "OVOCOperatorLite".

Figure 11-46: OVOC Operator Lite



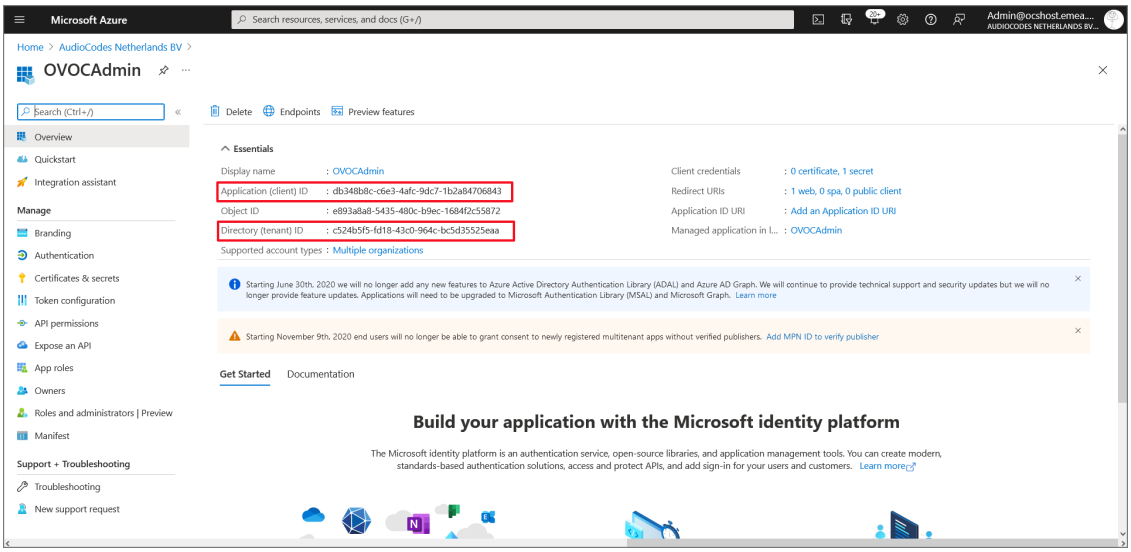
The new roles are displayed:

Figure 11-47: App roles



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

Figure 11-48: Overview Page



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

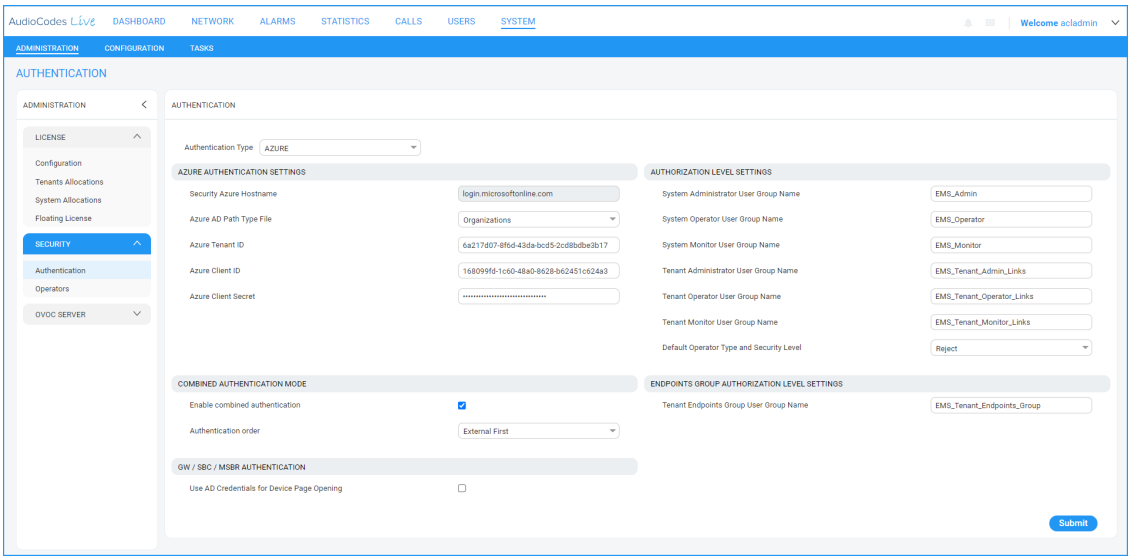
Configuring OVOC Web Azure Settings - Multitenant Setup

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:

1. 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



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

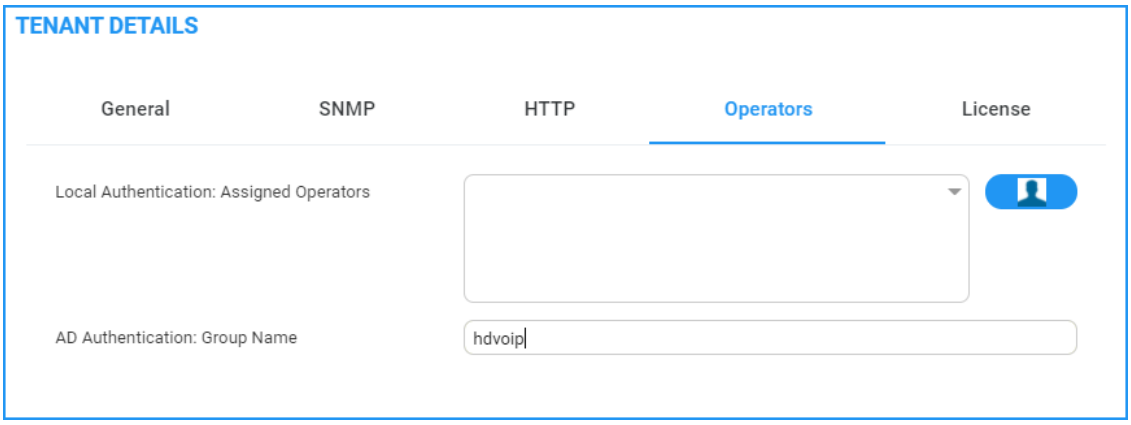
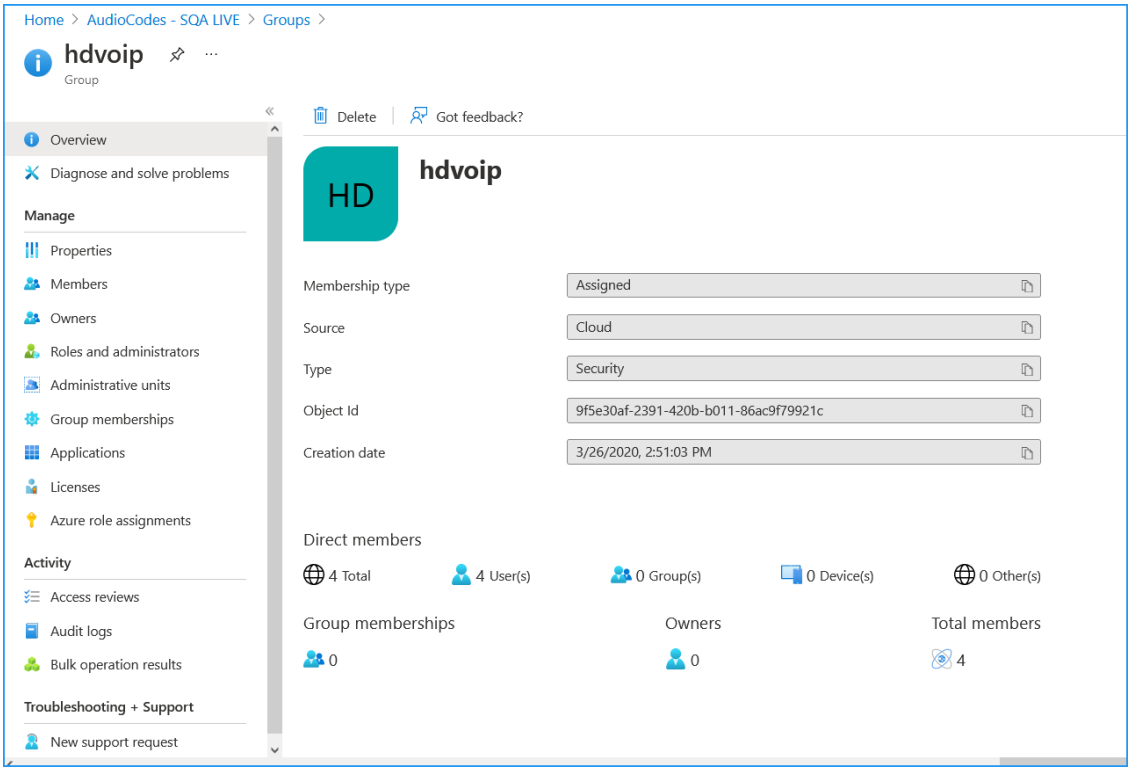


Figure 11-51: Matching Group on Azure



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.

Figure 11-52: Authorization Level Settings

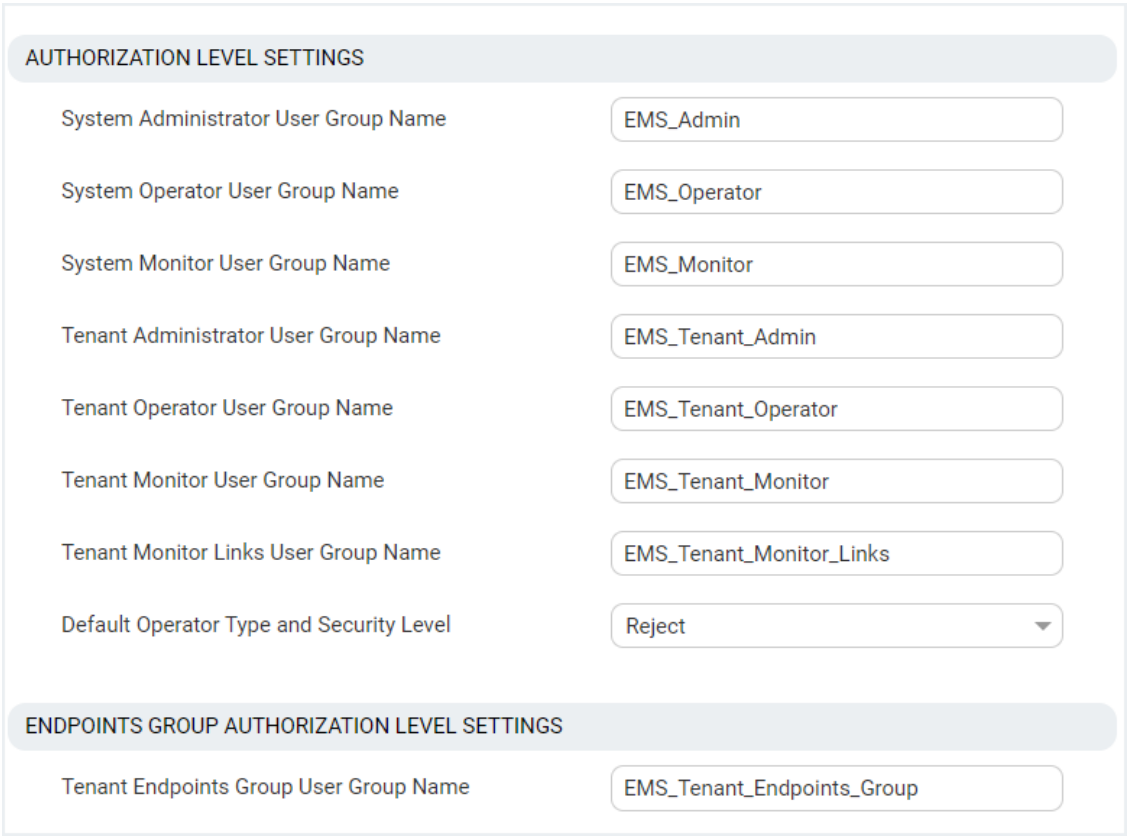
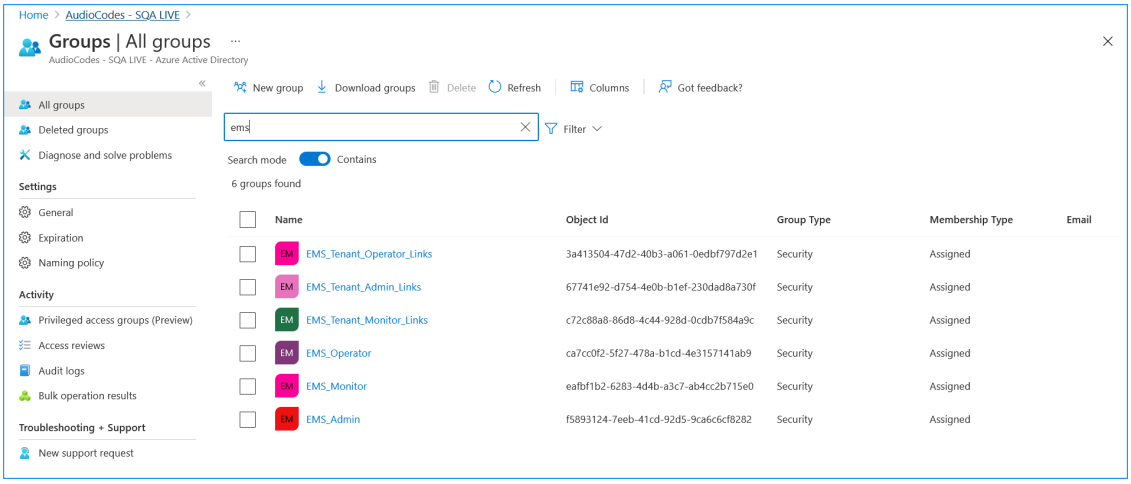
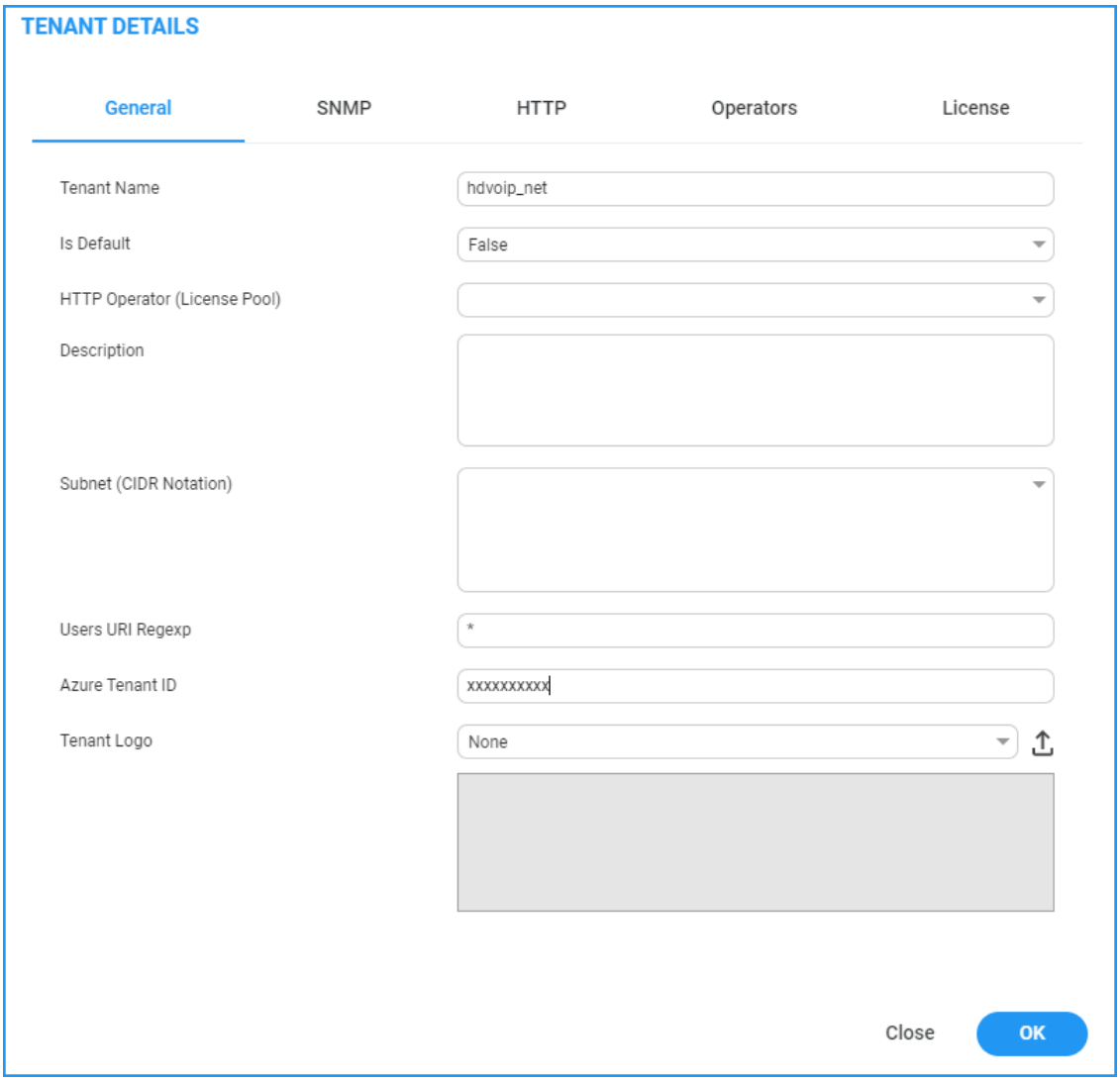


Figure 11-53: Matching Groups on Azure



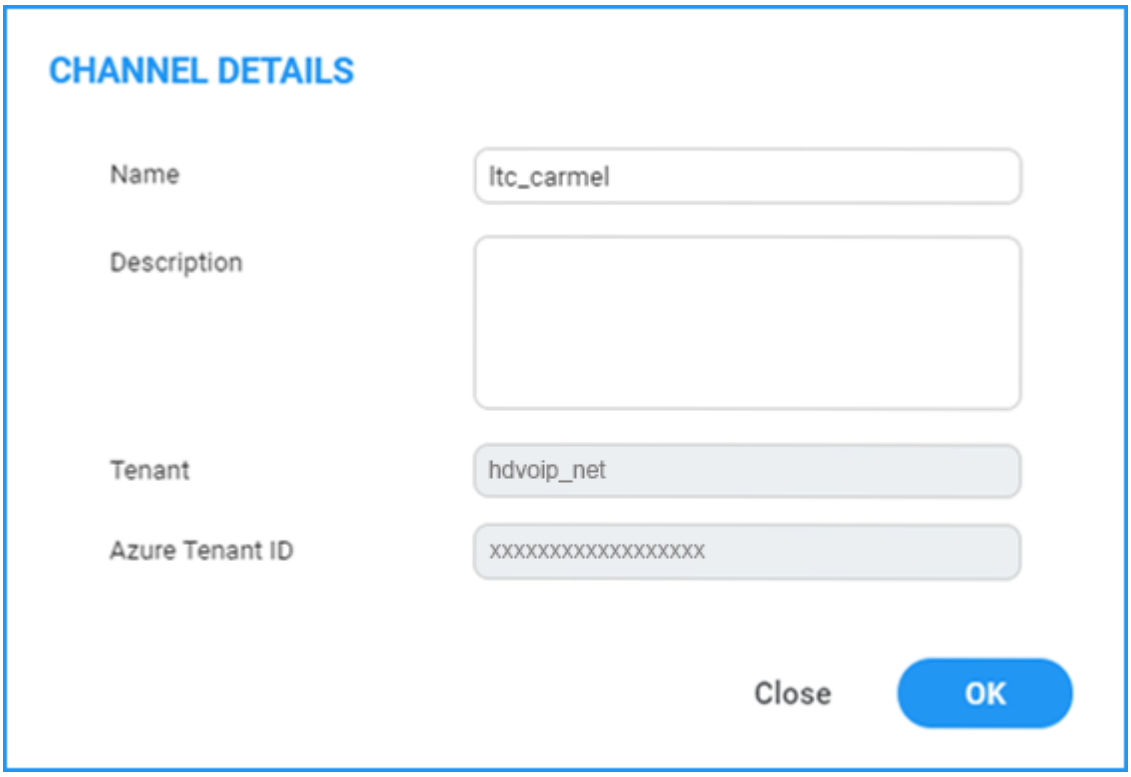
8. In the Tenant Details, enter the "Azure Tenant ID" of the **external managed tenant** as shown in the screen below.

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



Upgrading from Single Tenant to Multitenant

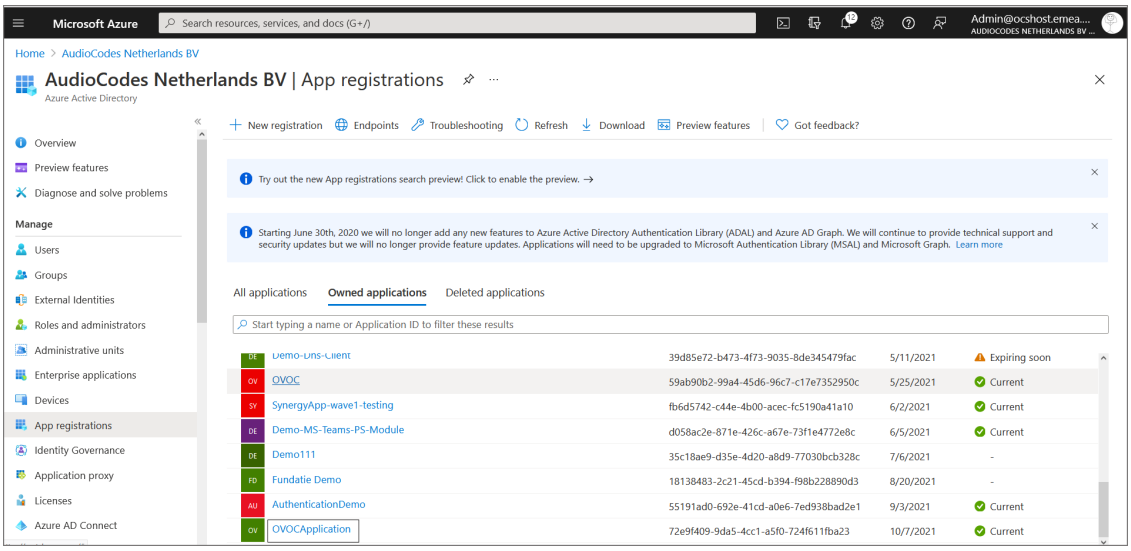
This procedure describes how to upgrade from Single tenant to Multitenant setup.

> 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



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

Figure 11-57: OVOC Application

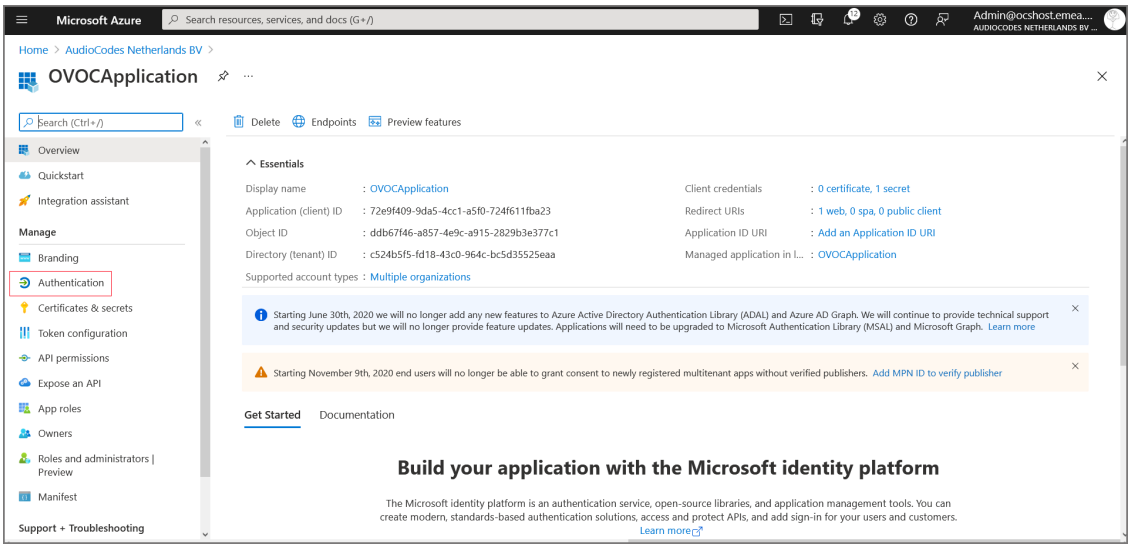
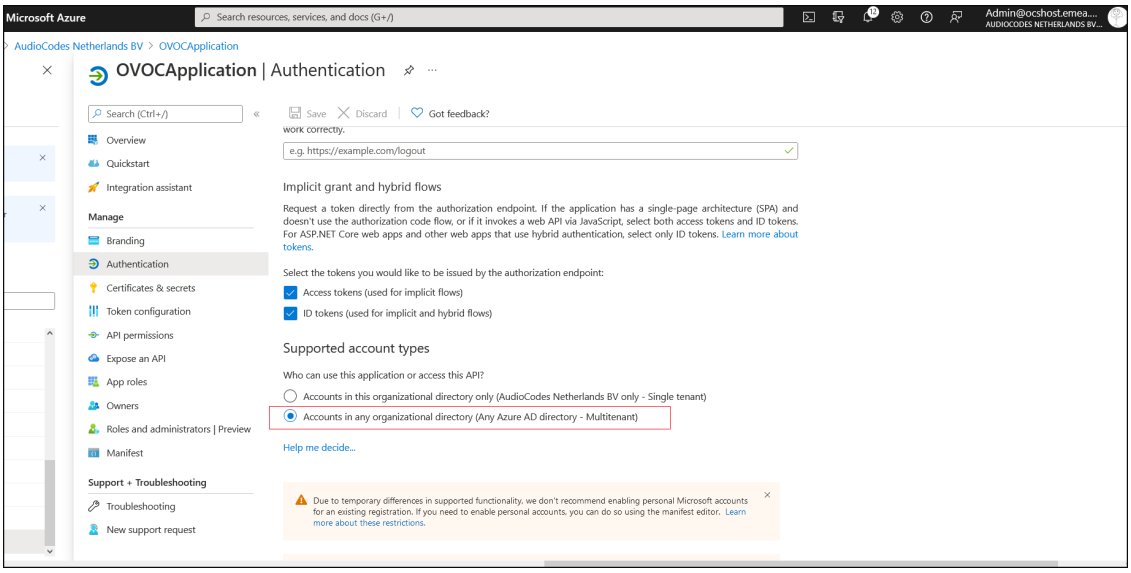


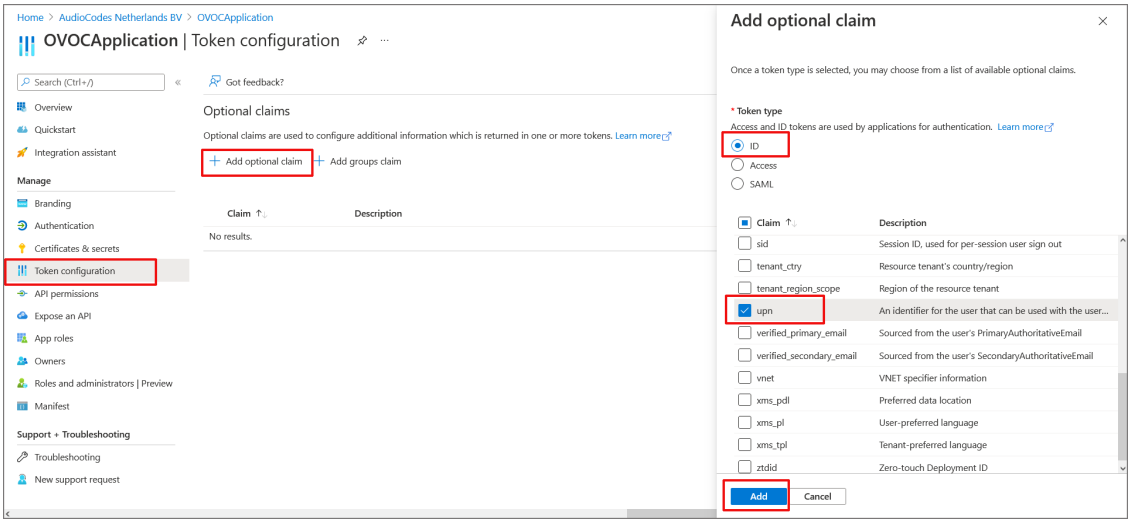
Figure 11-58: Authentication Screen



4. Under account types, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)** and then click **Save**.

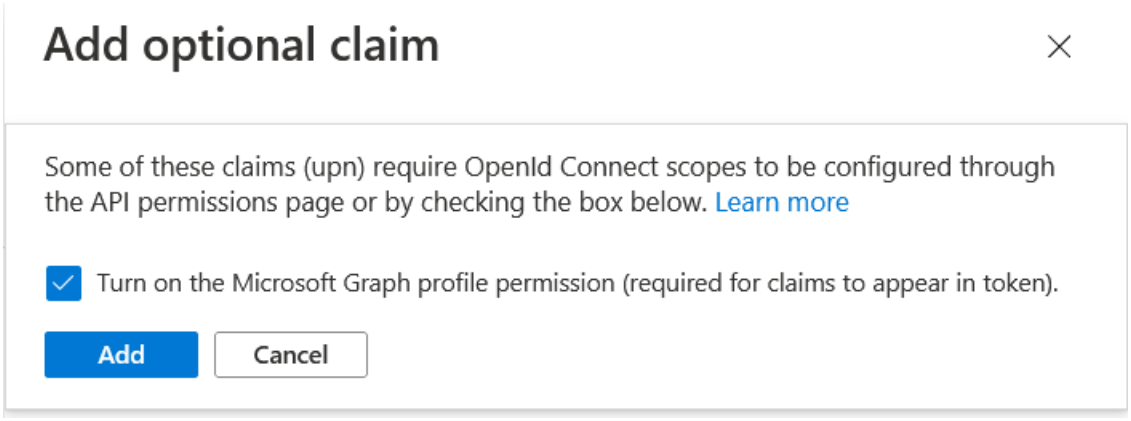
5. In the Navigation pane, select **Token configuration**

Figure 11-59: Token Configuration-Add



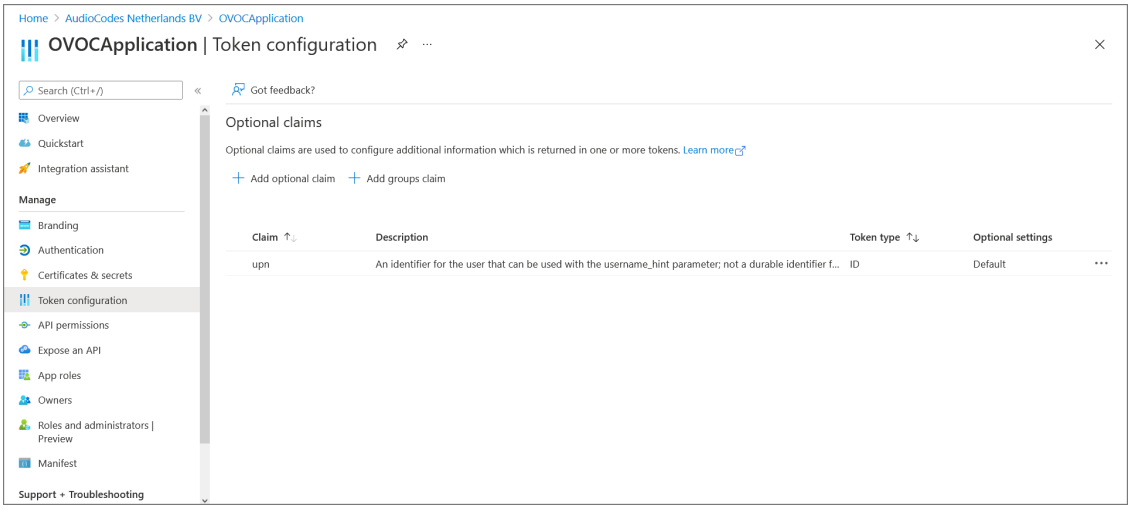
6. Click **Add optional claim**, choose **ID** type then **upn** optional claim and click **Add** to confirm.

Figure 11-60: Turn on Profile Permission



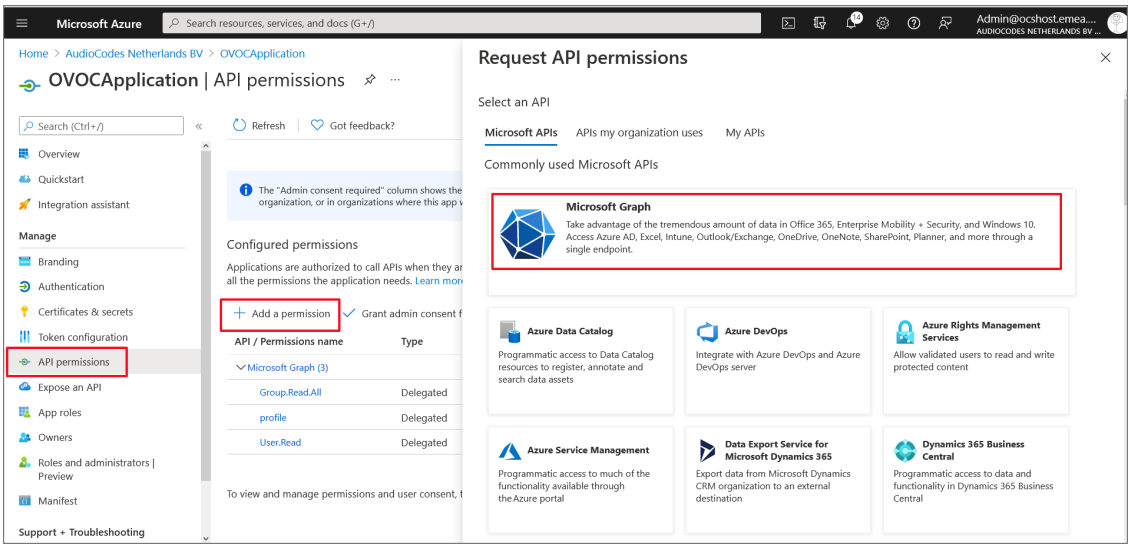
7. Select the **Turn on the Microsoft Graph profile permission** check box and then click **Add**. This adds the Profile permission to the API permissions list.

Figure 11-61: Optional claims Added



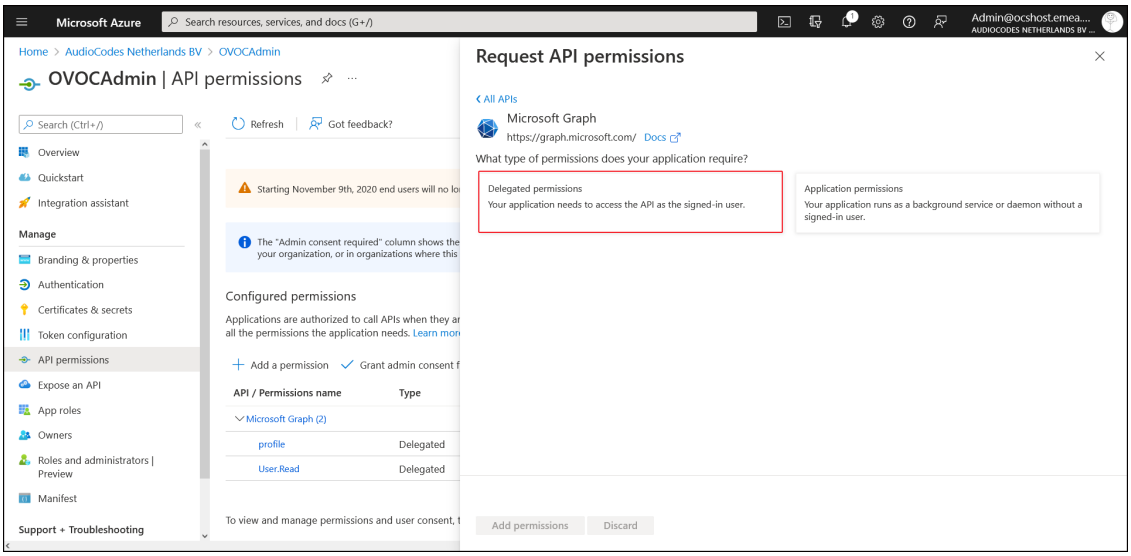
8. In the Navigation pane, select **API permissions**.

Figure 11-62: API Permissions



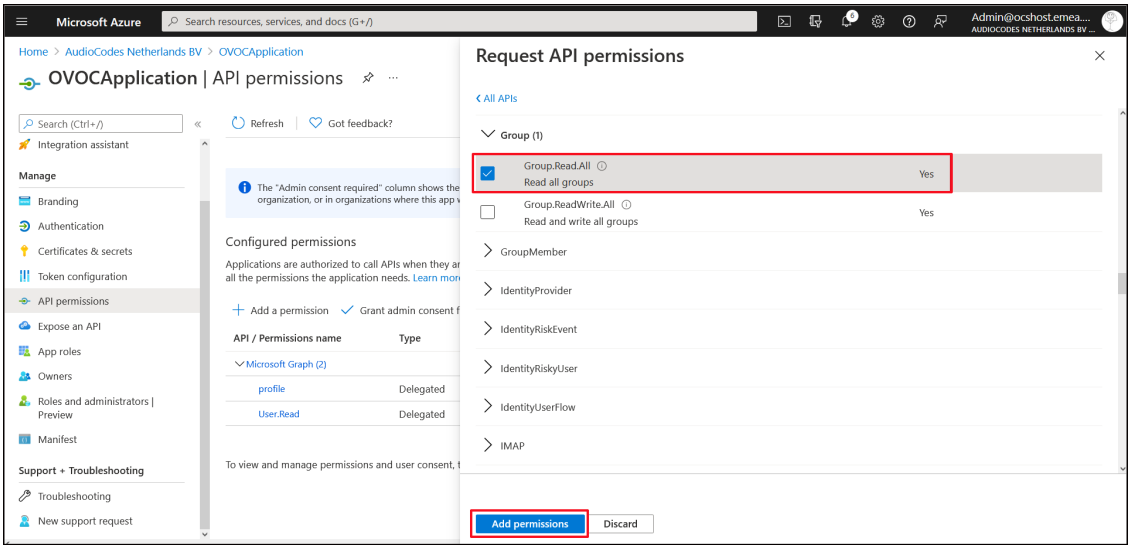
9. Click **Add a permission** and then click the **Microsoft Graph** link.

Figure 11-63: Delegated permissions



10. Click **Delegated permissions.**

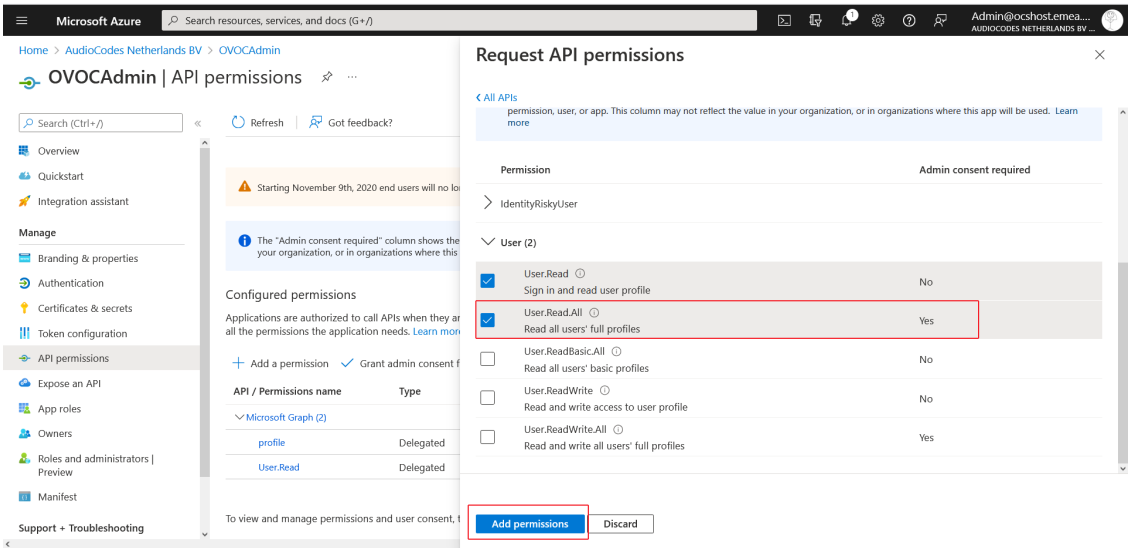
Figure 11-64: Microsoft Graph Permissions



11. Select permission **Group.Read.All** and then click **Add permission**.

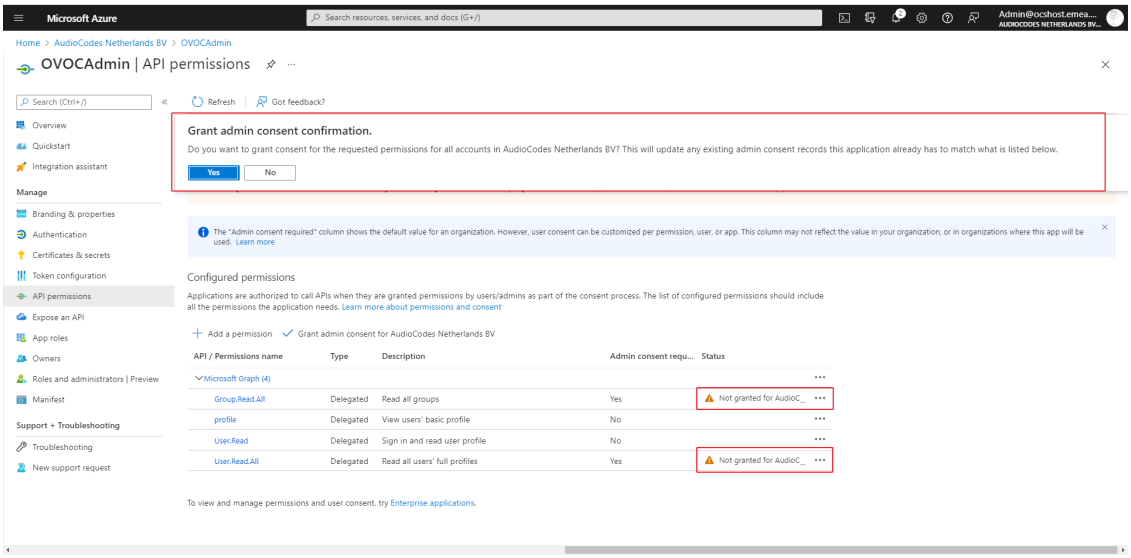
12. Add another Delegated permission **User.Read.All** and then click **Add permissons**.

Figure 11-65: Delegated permissions



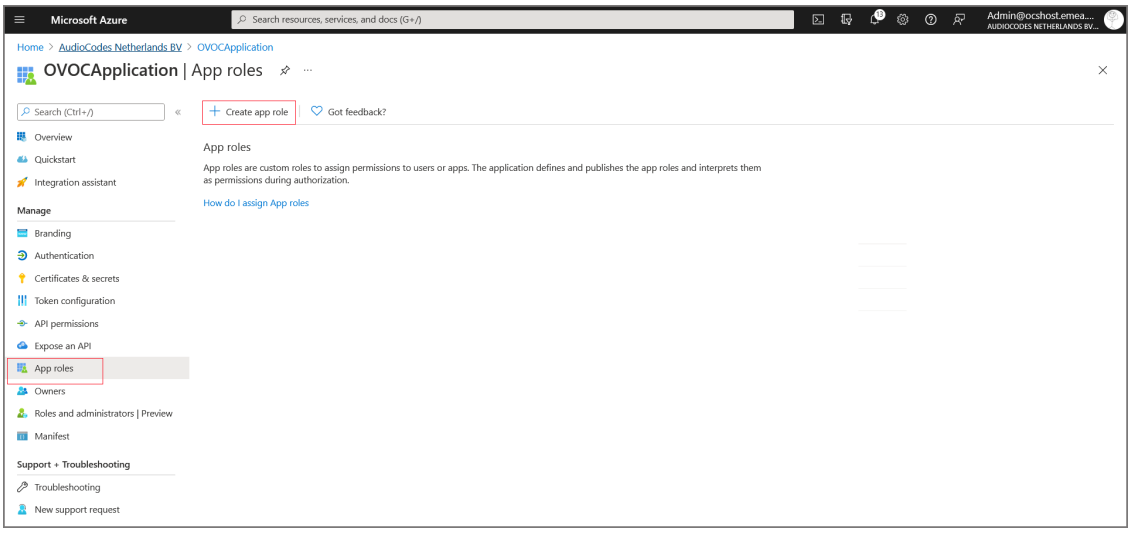
13. Click **Grant admin consent for <Tenant_Name>** link to grant consent for the requested permissions for all accounts for this tenant, and then click **Yes** to confirm.

Figure 11-66: Grant Admin Consent for all Accounts



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

Figure 11-67: Create App Roles



15. Create an app role with Admin permissions:

    a. In the Display Name field, enter "Administrators" or "Admins"

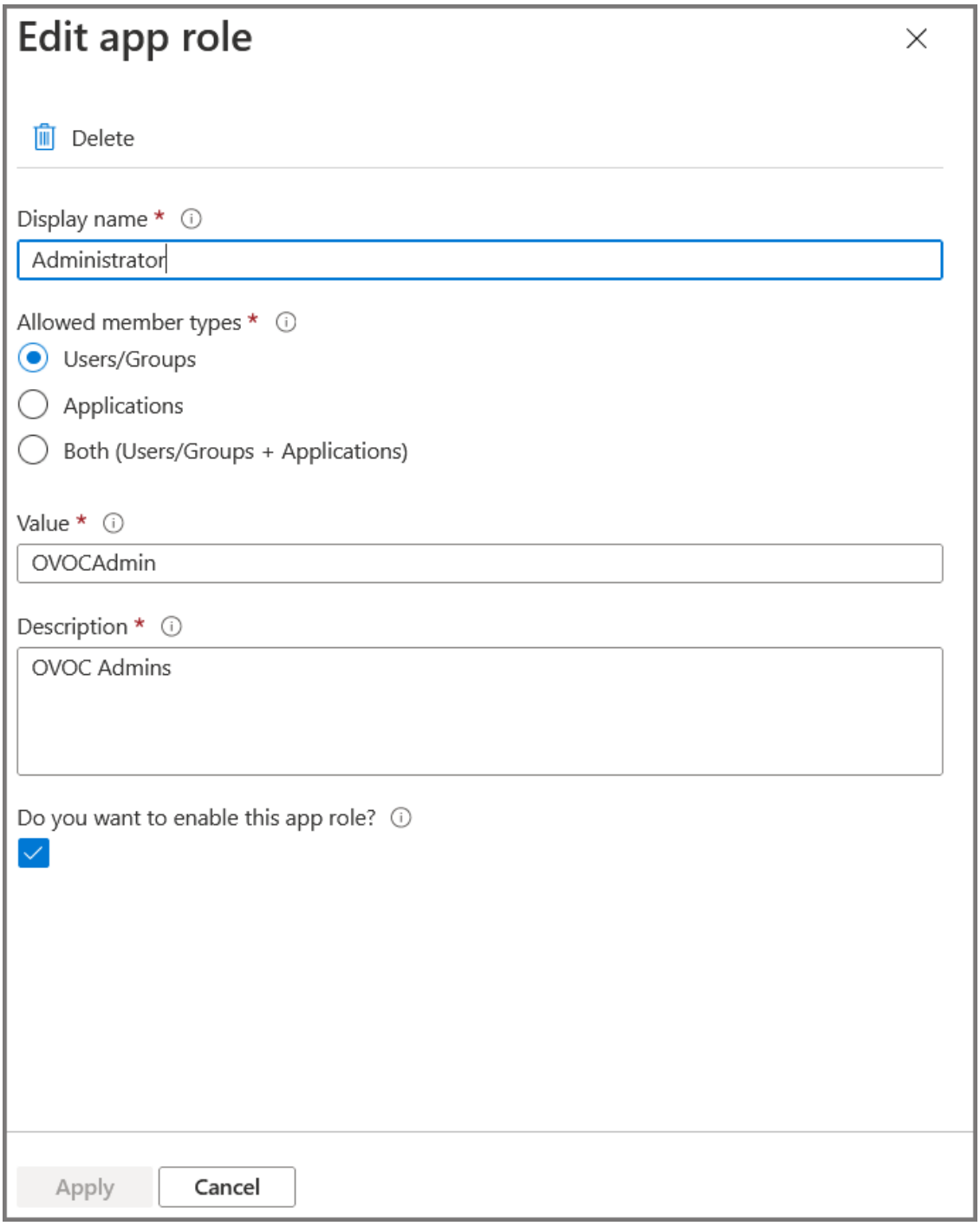
    b. Select Users/Groups check box

    c. Enter value "OVOCAdmin"

    d. Select the **do you want to enable this app role** check box.

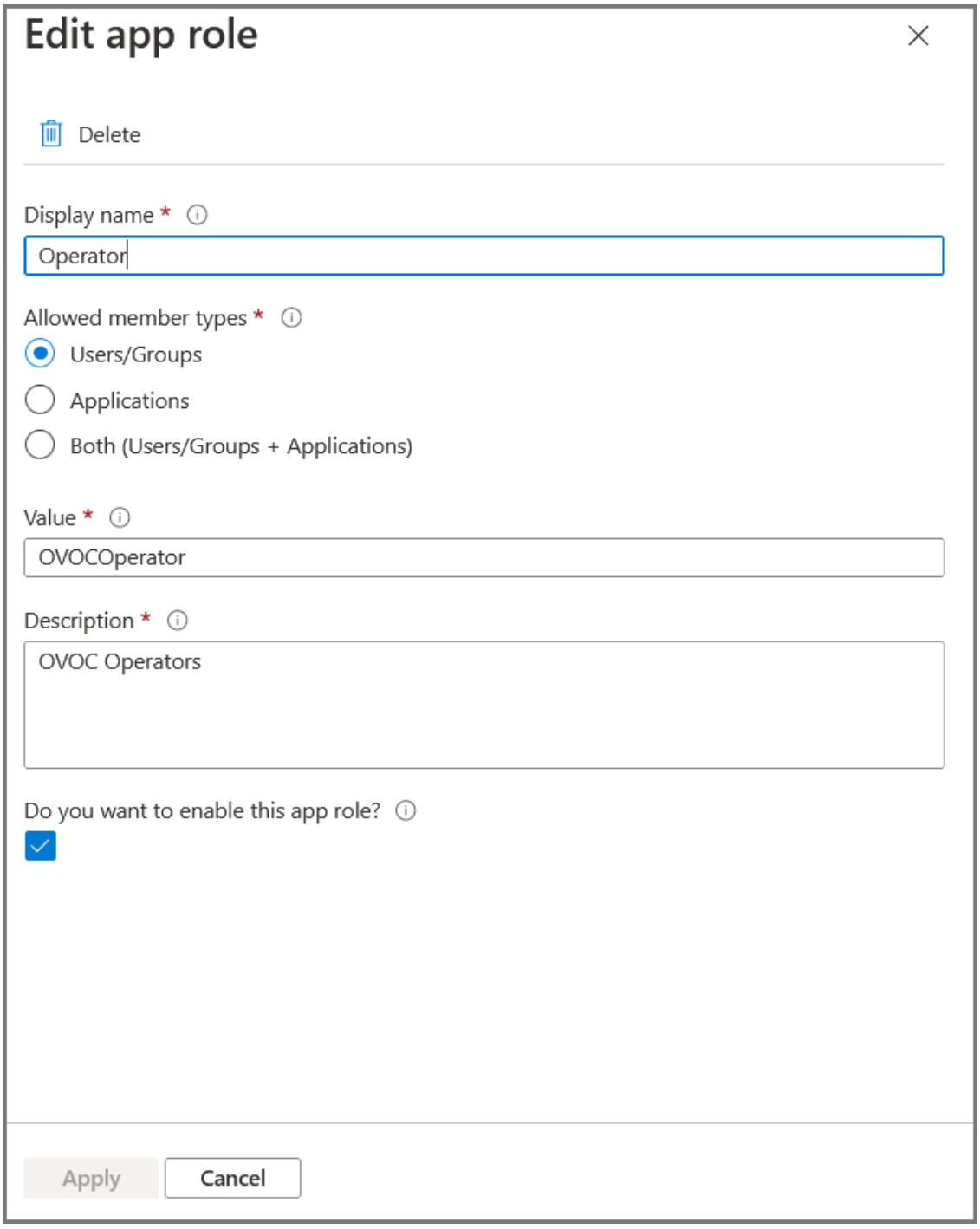
    e. Click **Apply**

Figure 11-68: Admin Role



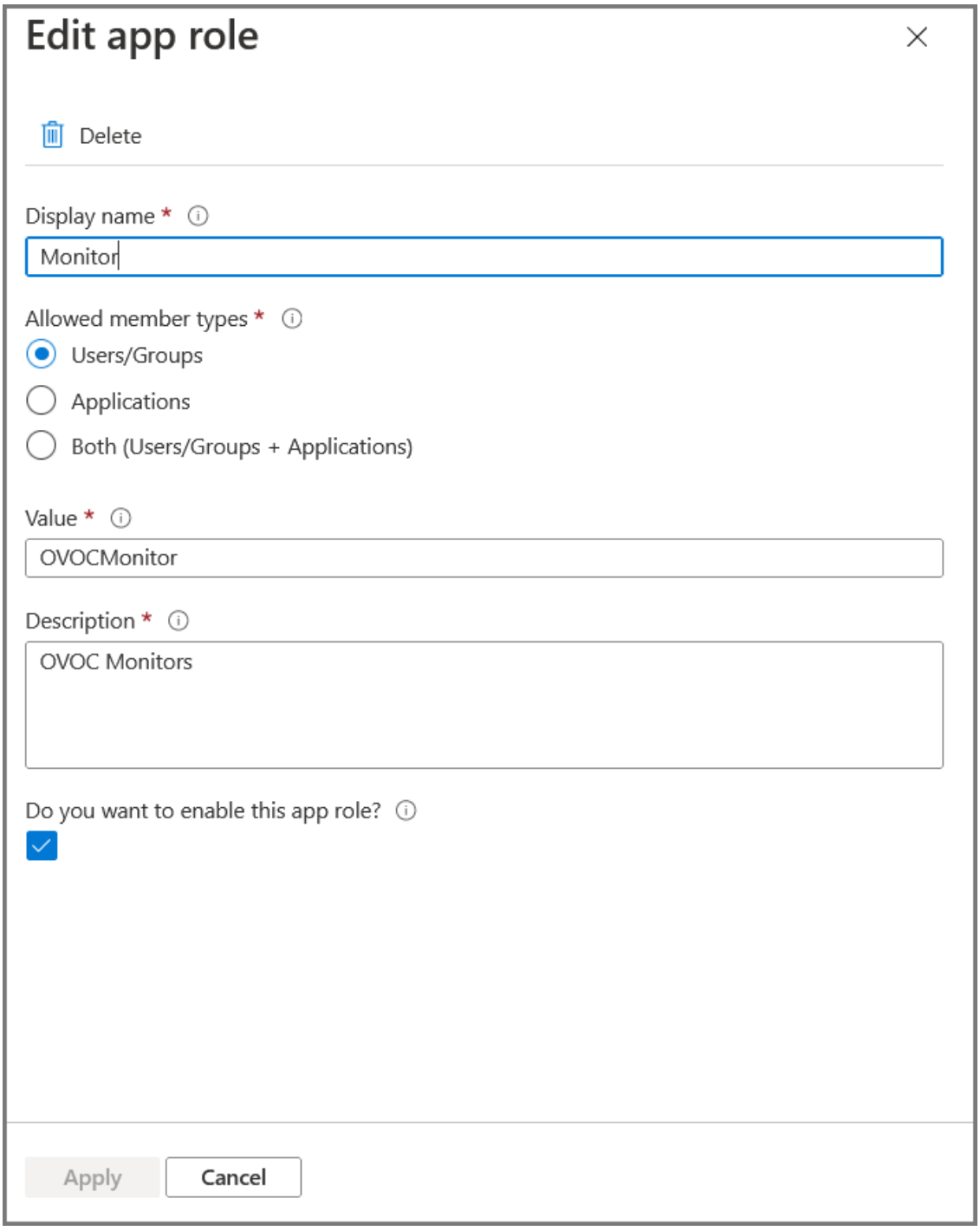
16. Repeat the above steps to create an App role with Operator permissions with value 'OVOCOperator".

Figure 11-69: Operator Role



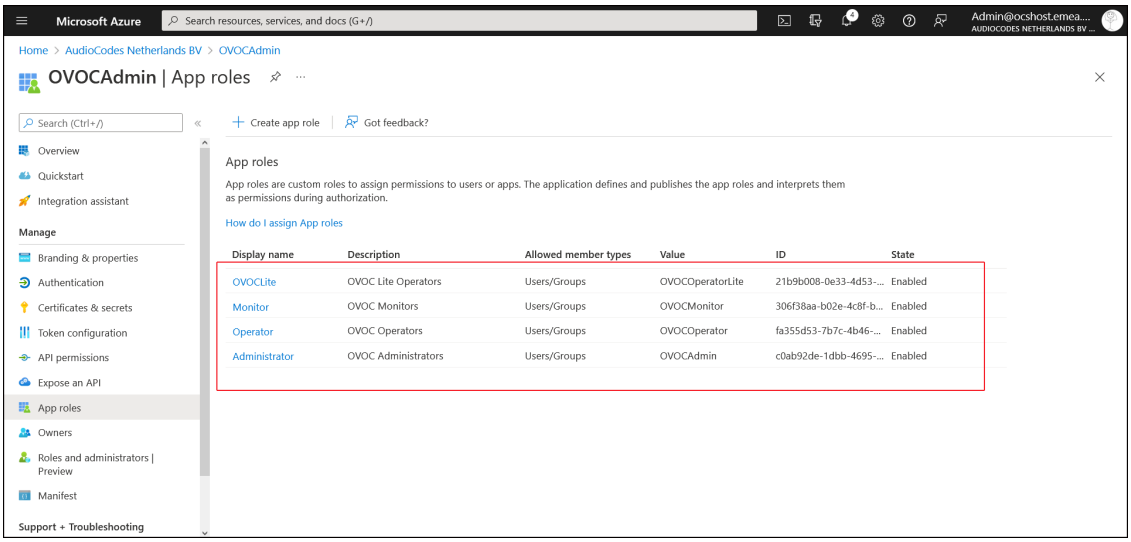
17. Repeat the steps described for creating "Admin" role above to create an app role with Monitor permissions with value "OVOCMonitor".

Figure 11-70: Operator Role



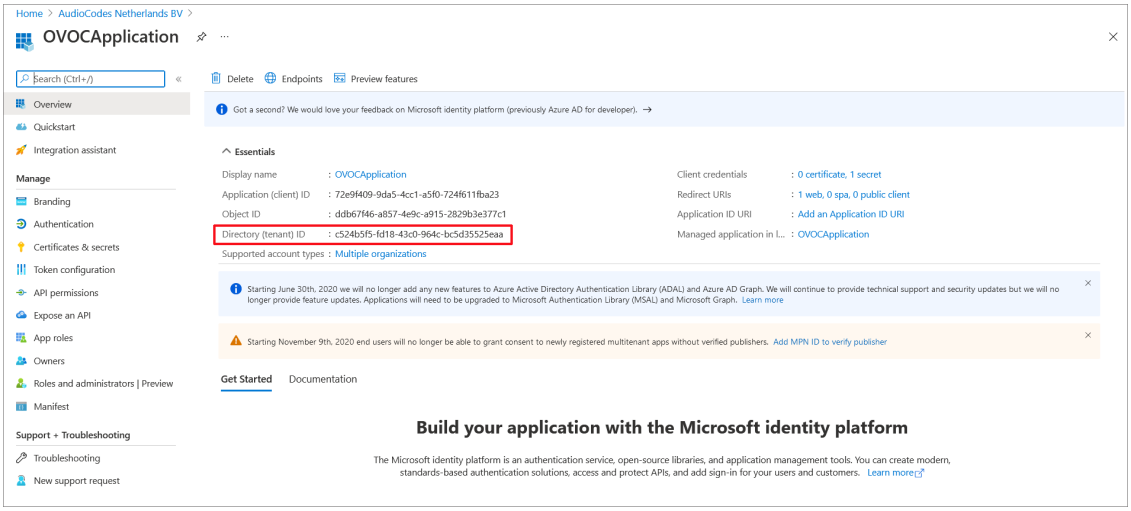
The new roles are displayed:

Figure 11-71: App roles Configured



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

Figure 11-72: Overview Page



19. Note the Directory (tenant) ID value as it must later be configured inConfiguring OVOC Web Azure Settings - Multitenant Upgrade below
20. 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

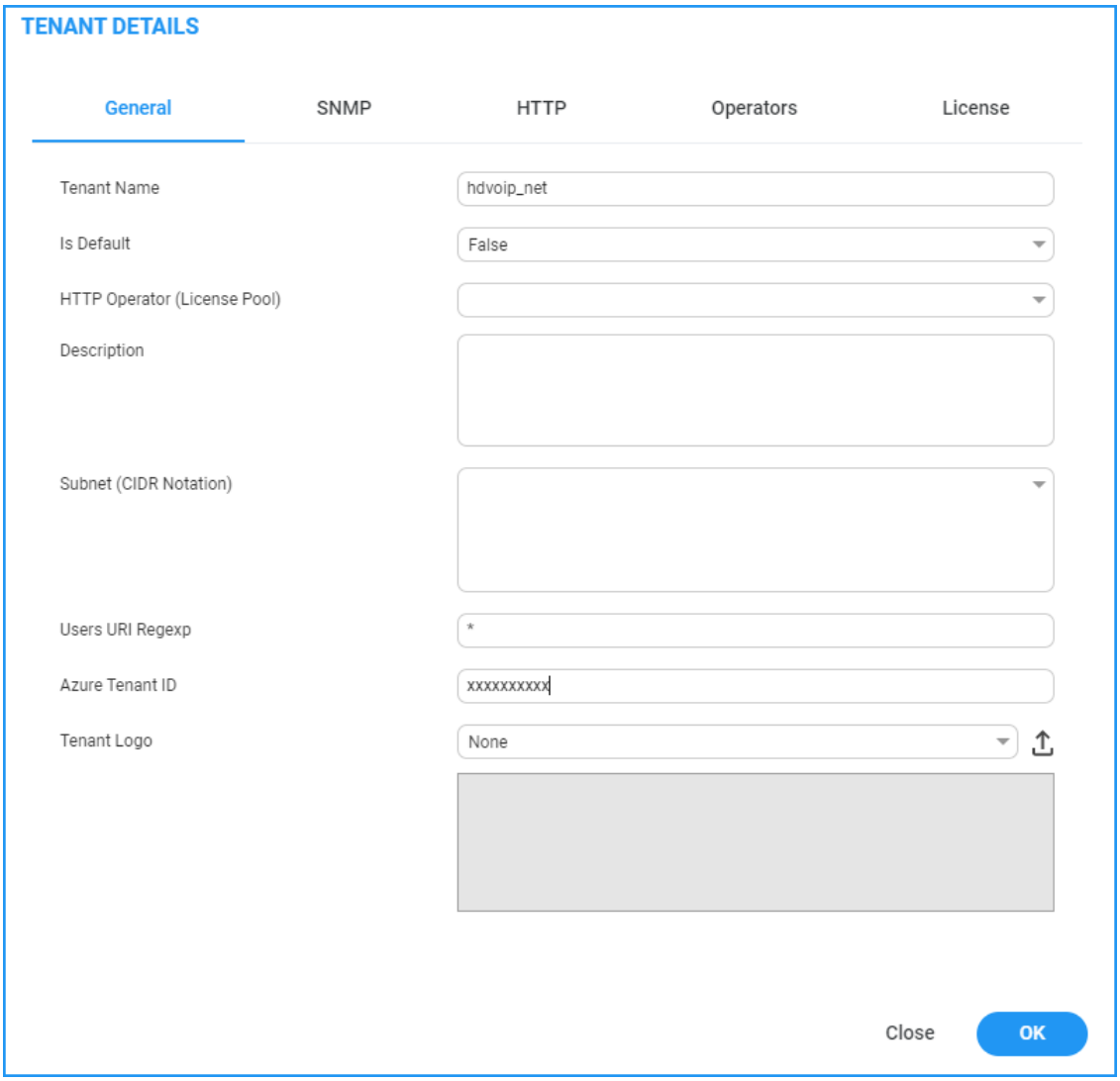
Configuring OVOC Web Azure Settings - Multitenant Upgrade

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:**

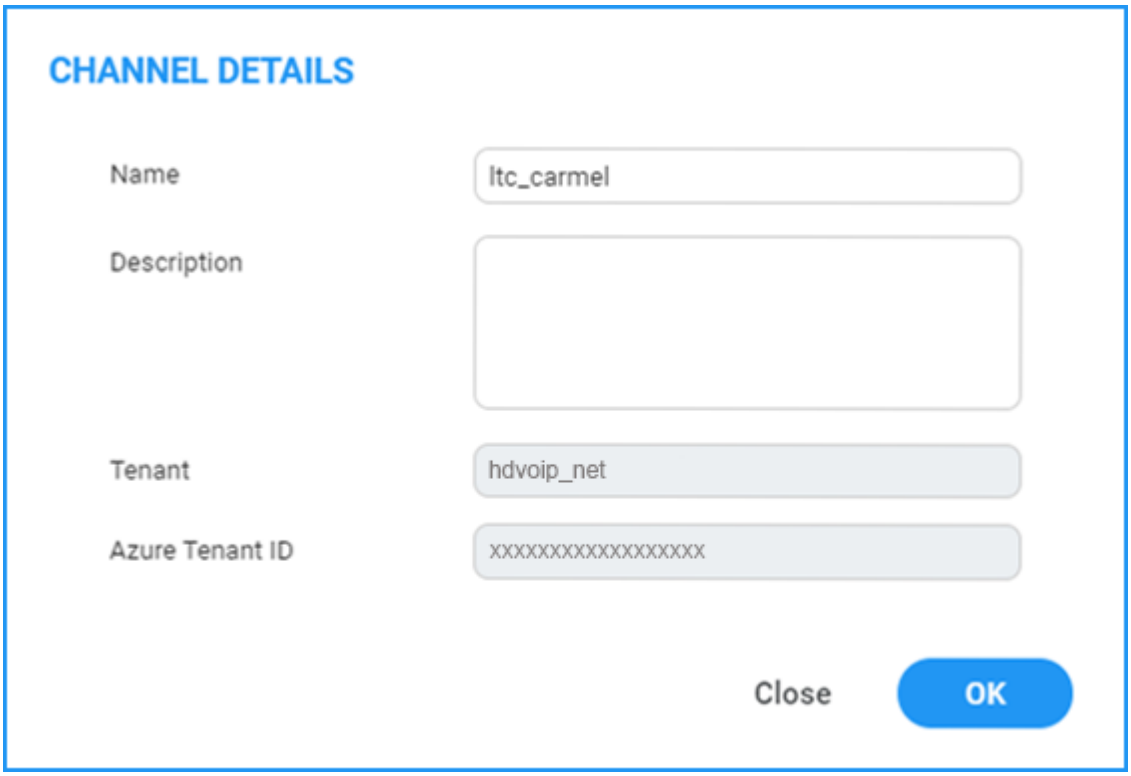
1. In the Tenant Details, enter the "Azure Tenant ID" of the **external managed tenant** as shown in the screen below.

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



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.

Table 11-1: OVOC Security Groups

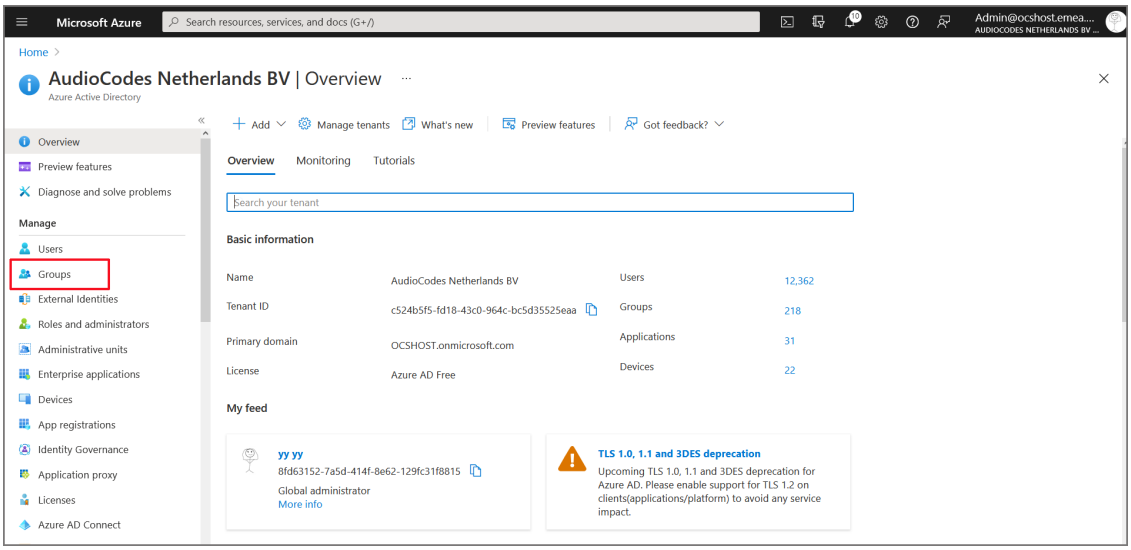
Security Group OVOC (Parameter Name)	Description
System Administrator User Group Name	The name of the User Group of the 'System' type operator whose security level is 'Administrator'.
System Operator User Group Name	The name of the User Group of the 'System' type operator whose security level is 'Operator'.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

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:

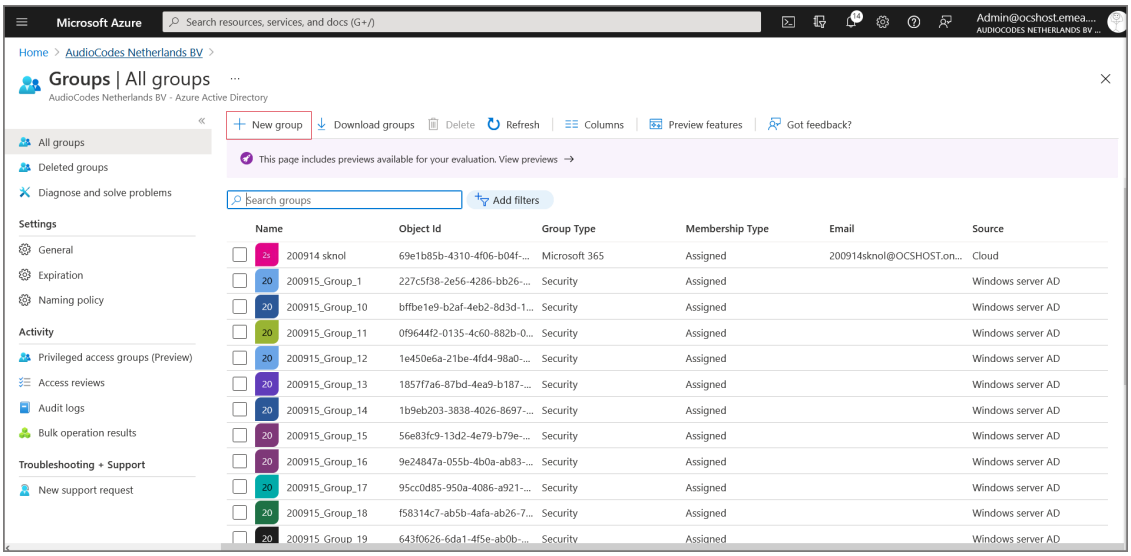
1. Login to the Azure portal as Global Administrator.
2. Navigate to the Tenant Overview page.

Figure 11-75: Tenant Overview Page



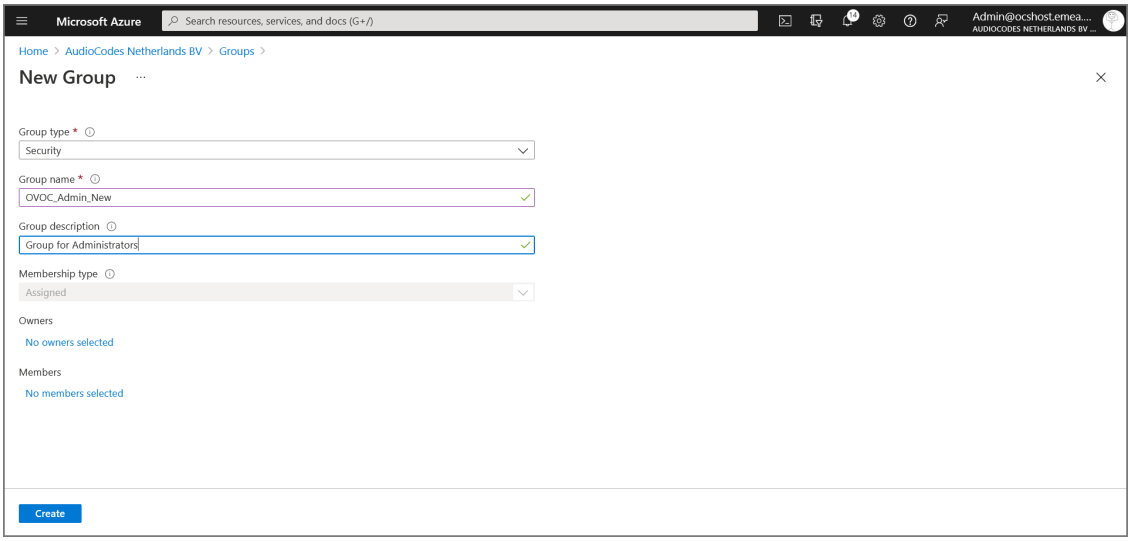
3. In the Navigation pane, select **Groups.**

Figure 11-76: Create New Group



4. Click **New group**.

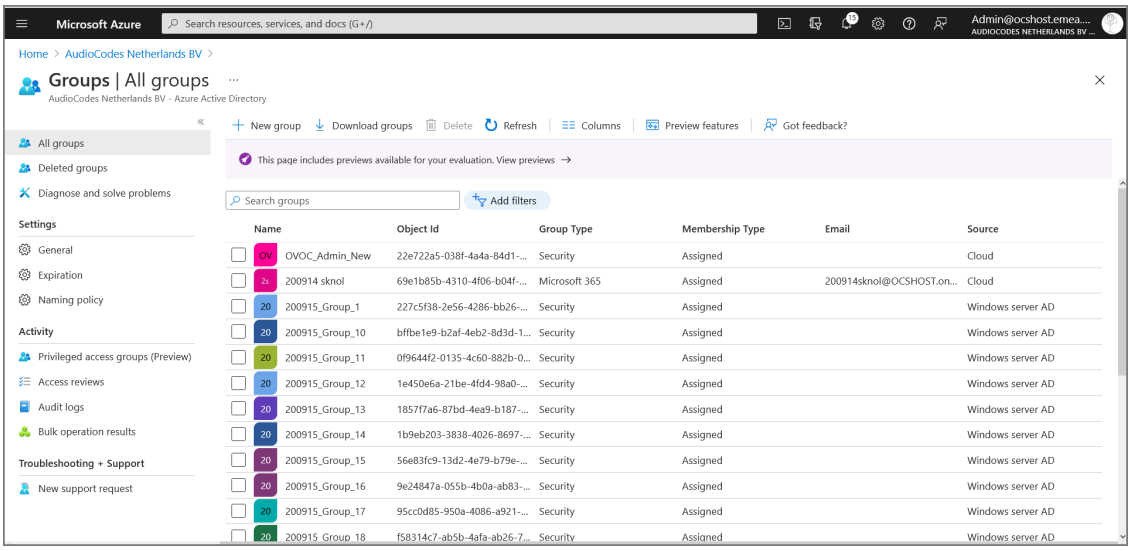
Figure 11-77: New Group



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)

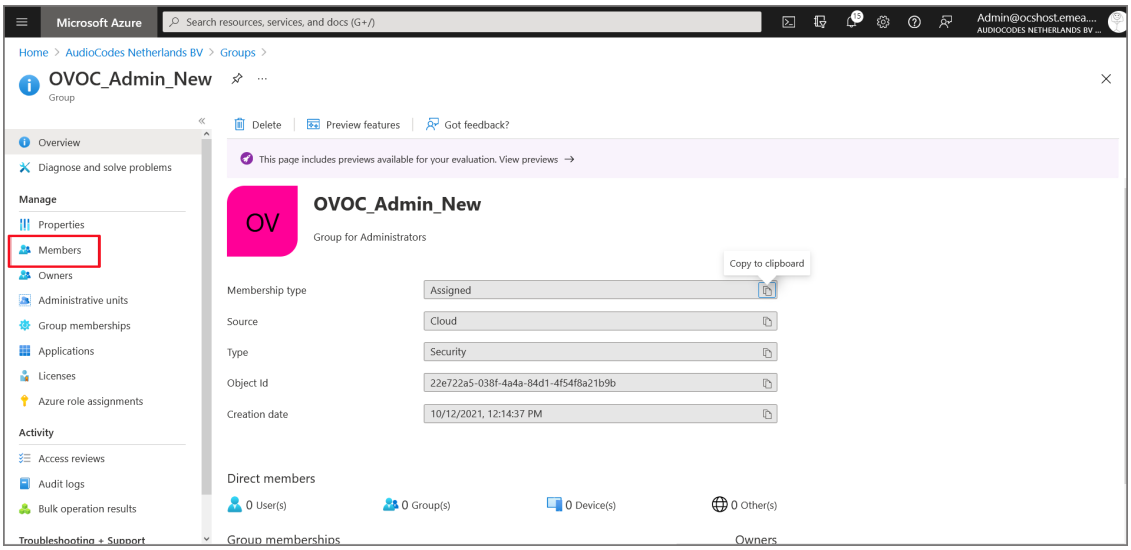
Figure 11-78: Created Group



6. Select the new group.

7. In the Navigation pane, select **Members**.

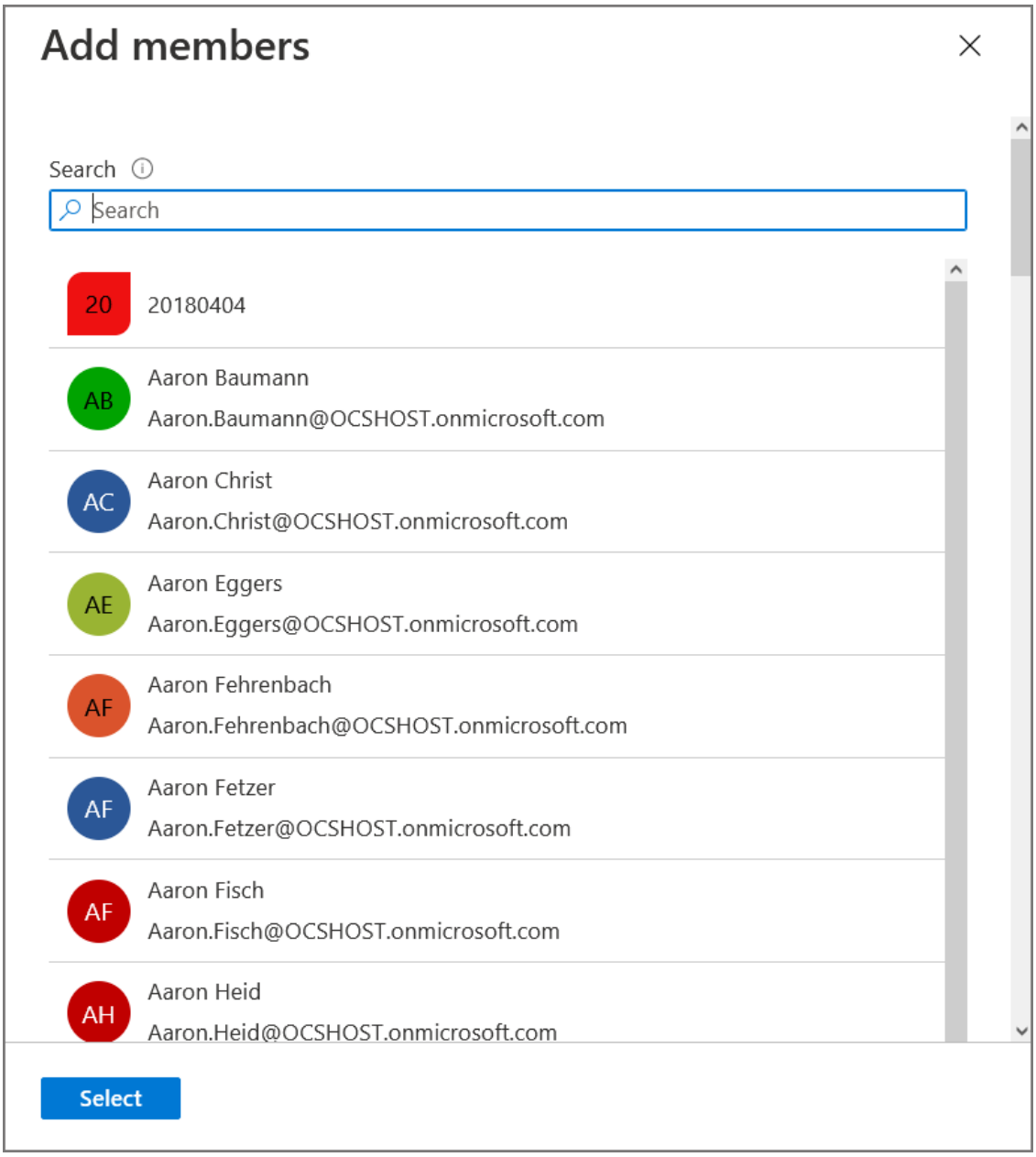
Figure 11-79: Add Members to Group



8. Click **Add members** to add new members to the group.

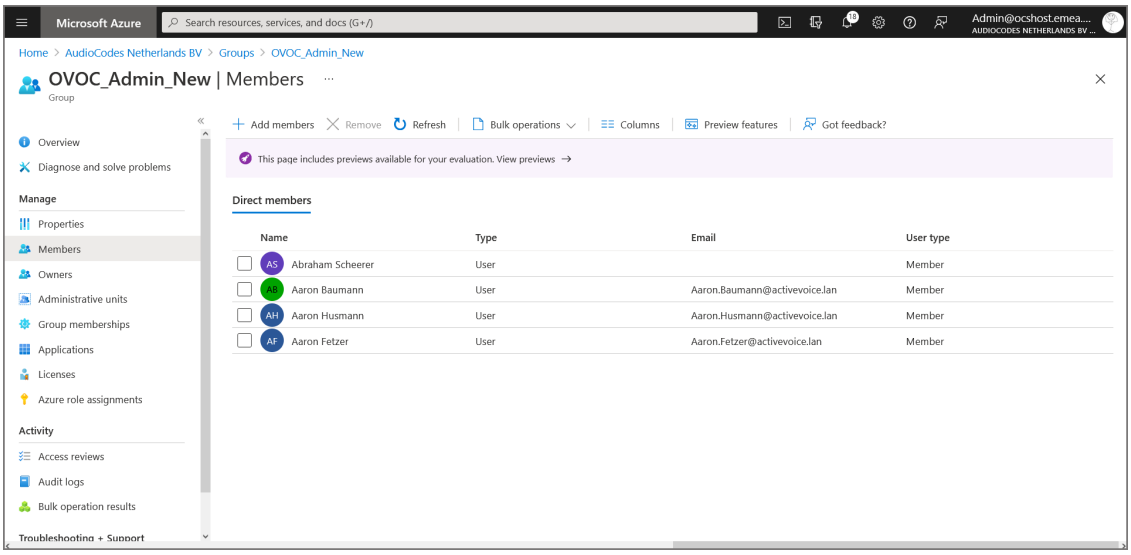
9. Select the members to add to the Group.

Figure 11-80: Select Group Members



The new members are added to the group.

Figure 11-81: New Group Members



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

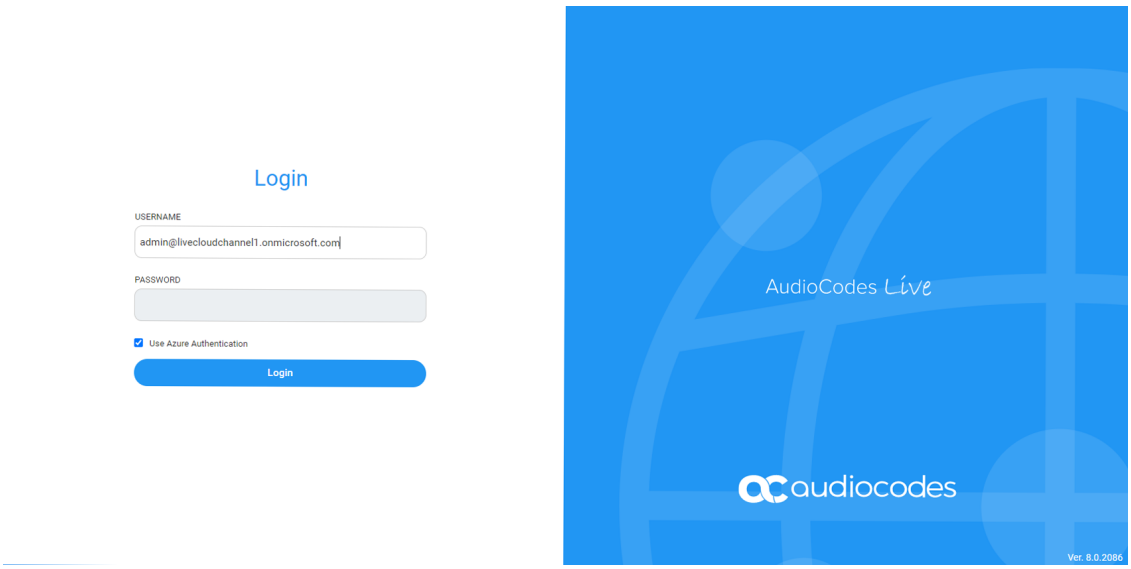
Add External Tenant Operators and Assign Roles

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:

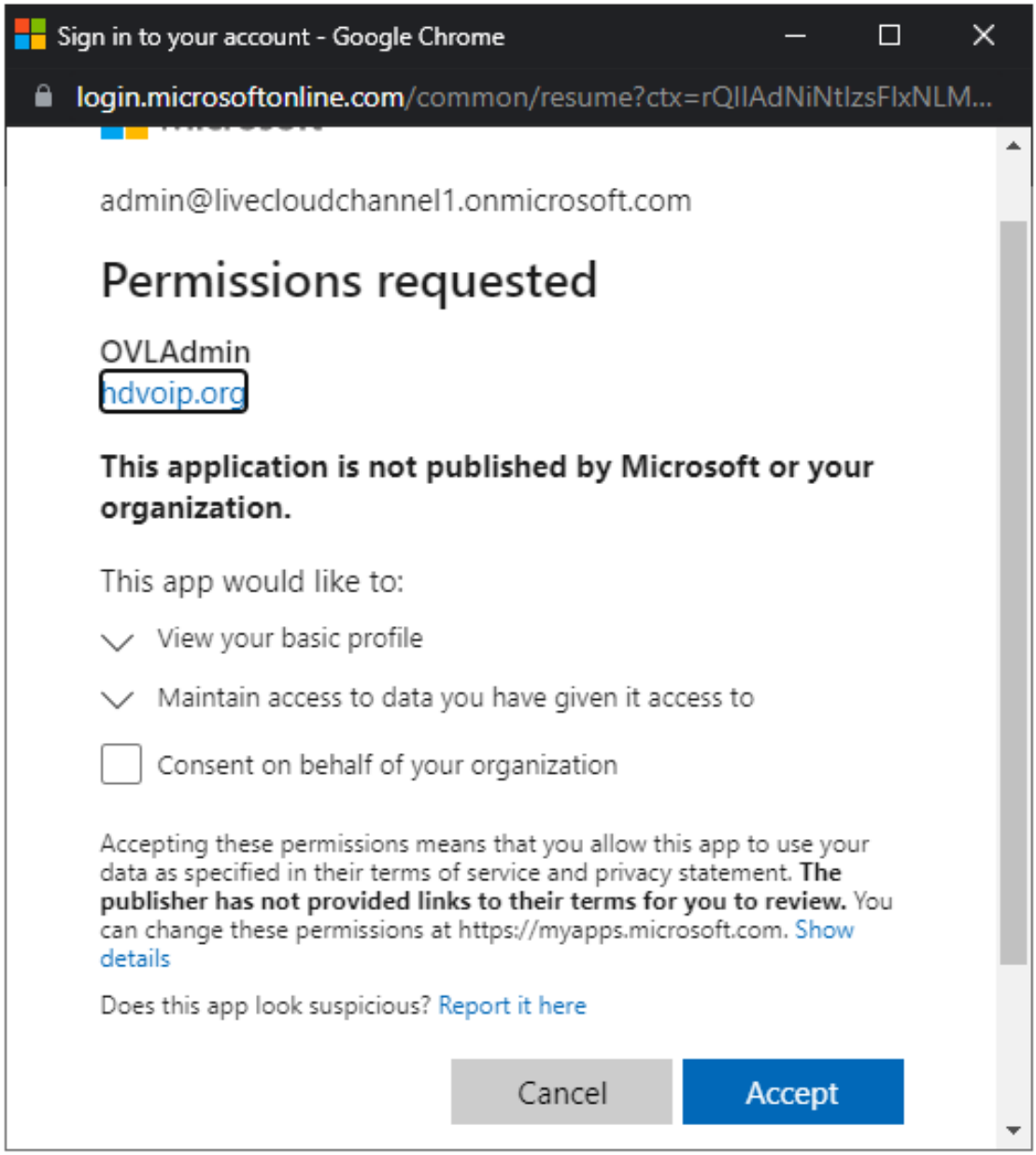
1. Login to OVOC interface with the appropriate Admin permissions for the Azure tenant (login with Admin operators that you defined in Create Azure Groups and Assign Members on page 124.

Figure 11-82: Initial Operator Login



The Azure authentication and Permissions request dialog is displayed:

Figure 11-83: Permissions requested

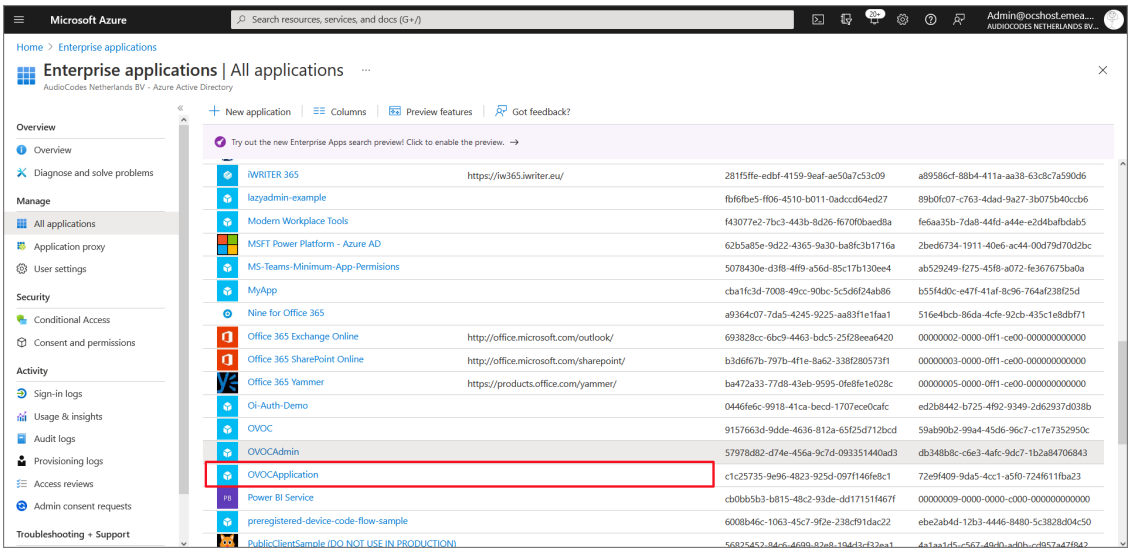


2. Select the **Consent on behalf of your organization** check box and then click **Accept**.

> 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.

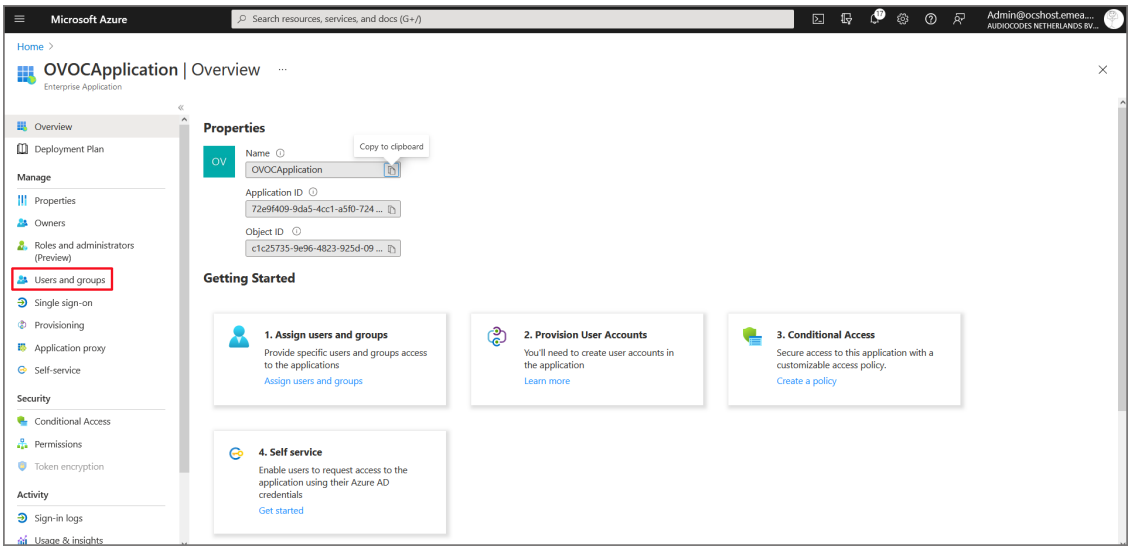
3. Login to the Azure portal with Tenant 'Admin' permissions and navigate to the newly created OVOC application (**Enterprise applications** > **OVOCApplication**).

Figure 11-84: OVOC Application



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

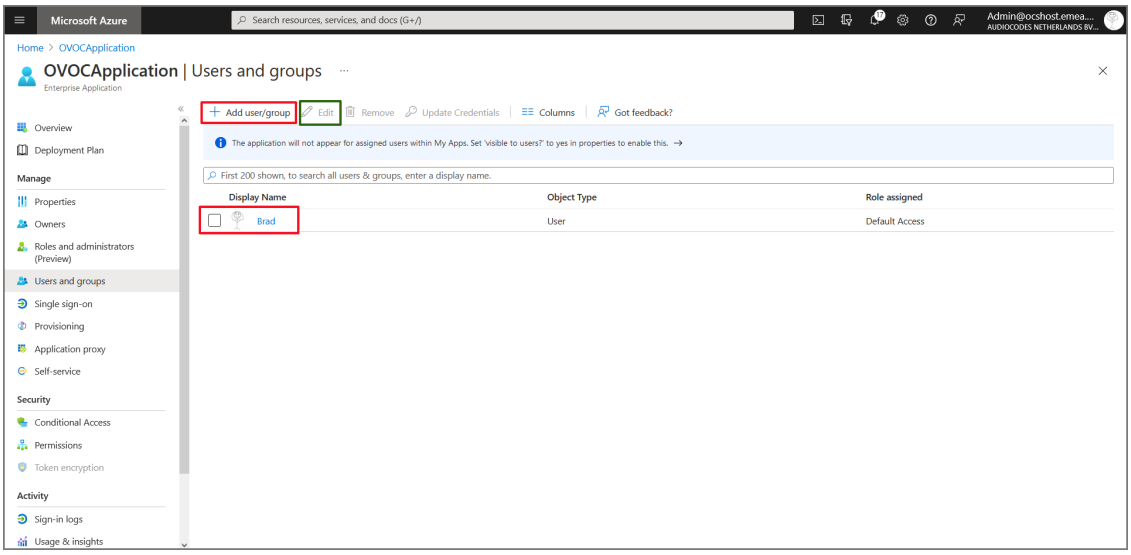
Figure 11-85: Users and Groups



5. Do one of the following:

- Assign role to a new user
- Assign role to existing user

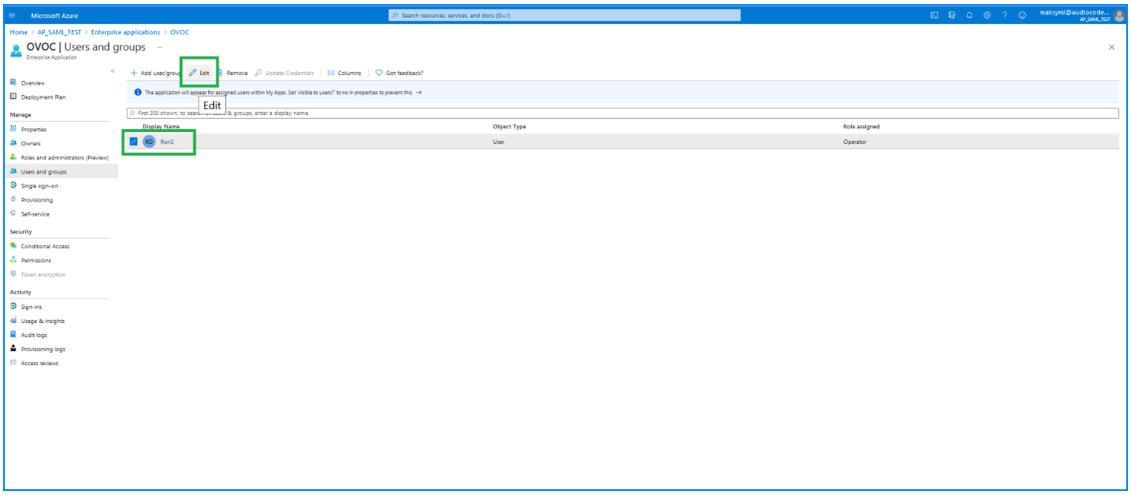
Figure 11-86: Assign Role to New User /Existing User



➢ To assign a role to an existing user:

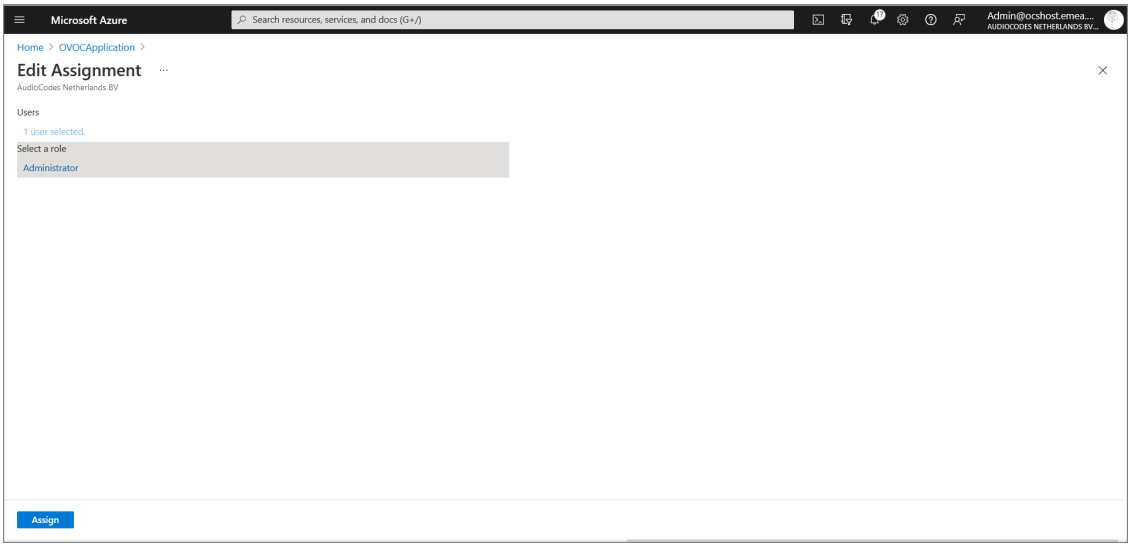
1. Choose a particular user in the list and then click **Edit.**

Figure 11-87: Edit Assignment



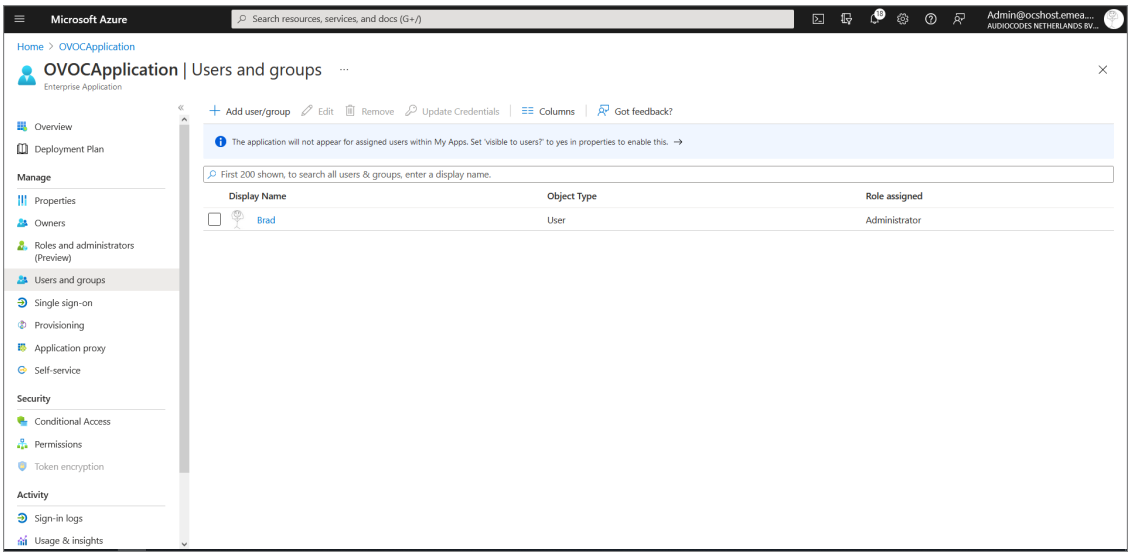
2. In the left pane, under "Select a role" click **None Selected**.
3. In the right pane, choose the relevant role and then click **Select**.

Figure 11-88: Add Assignment



4. Confirm by clicking **Assign.**

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**.

Figure 11-90: Choose User

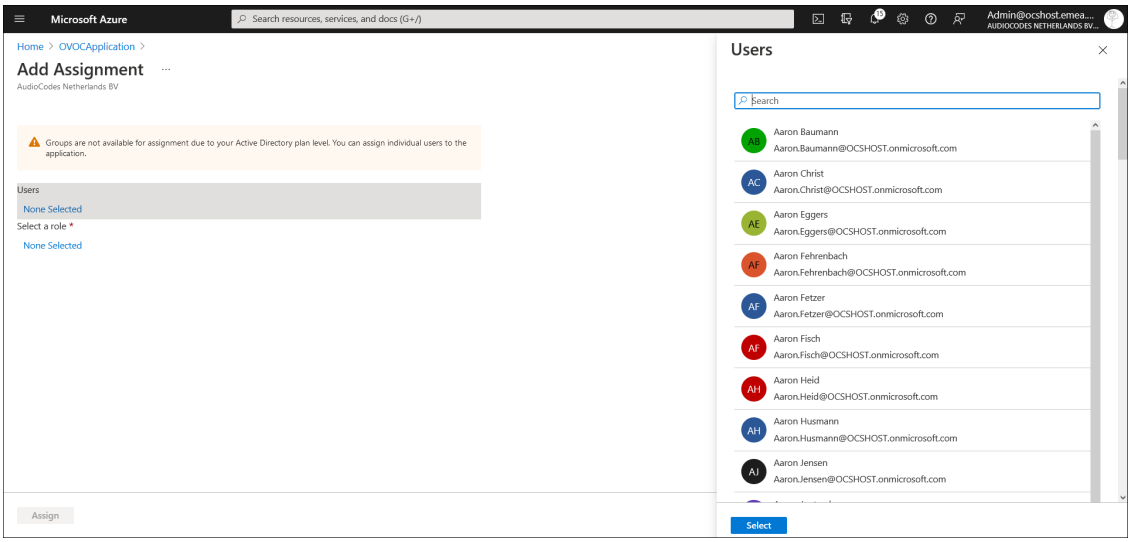
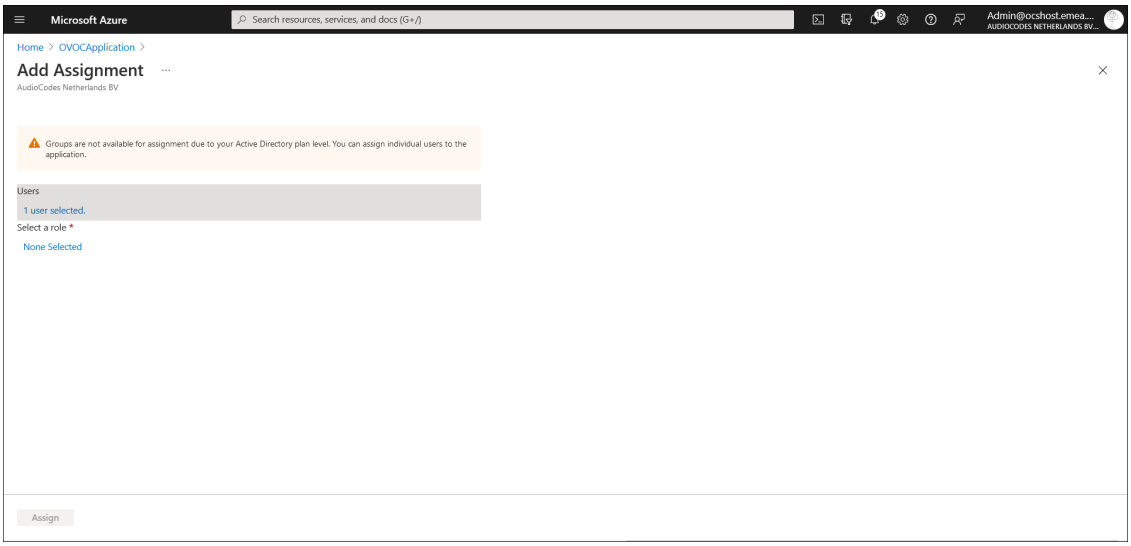
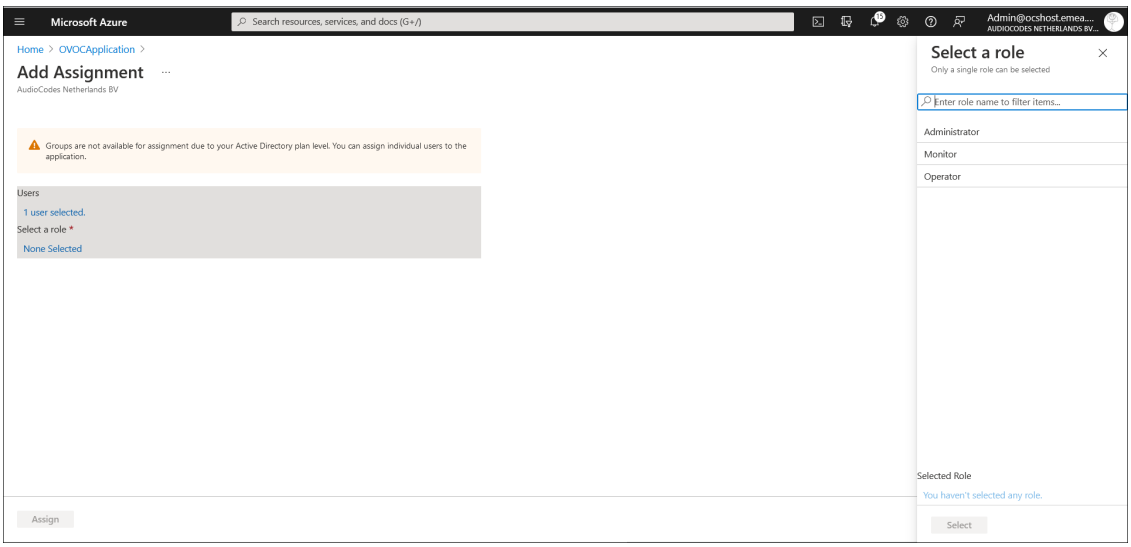


Figure 11-91: User Selected



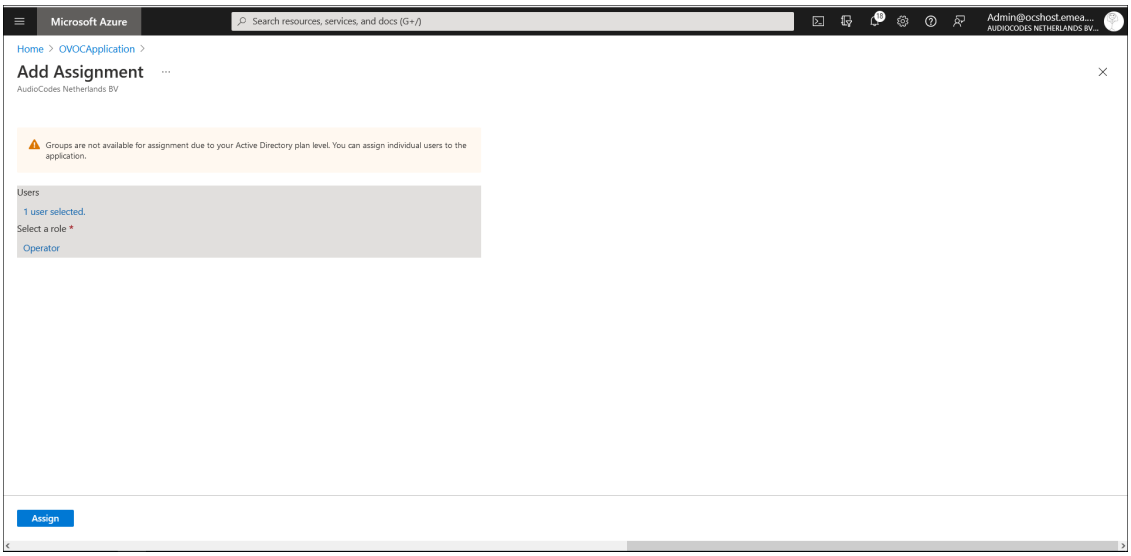
3. In the left pane under Select a role, click **None Selected**.

Figure 11-92: Select a Role



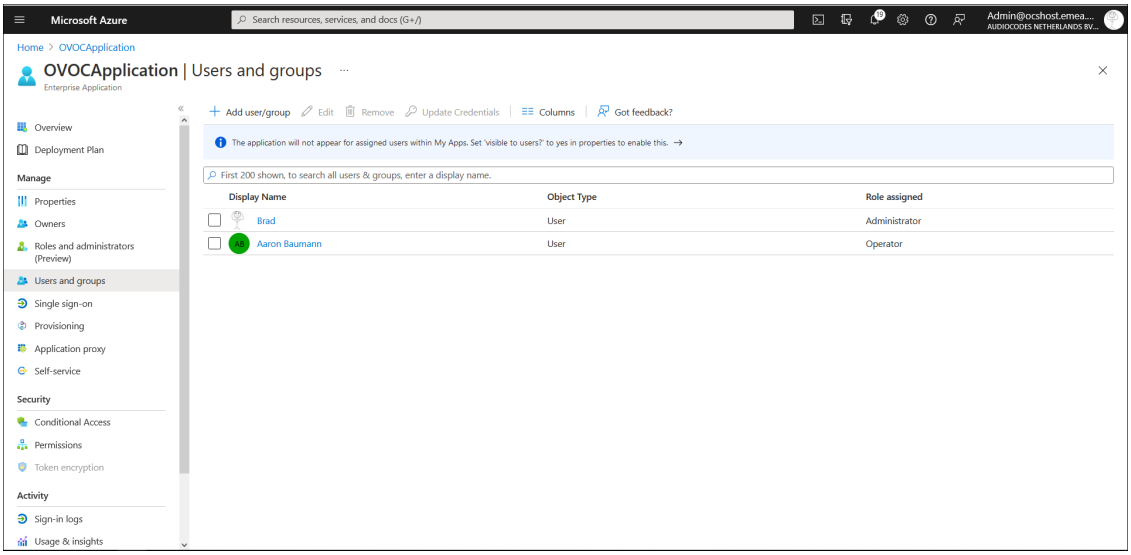
4. In the right pane, choose the relevant role and then click **Select**.

Figure 11-93: Assign Role to New User



5. Confirm by clicking **Assign**.

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



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

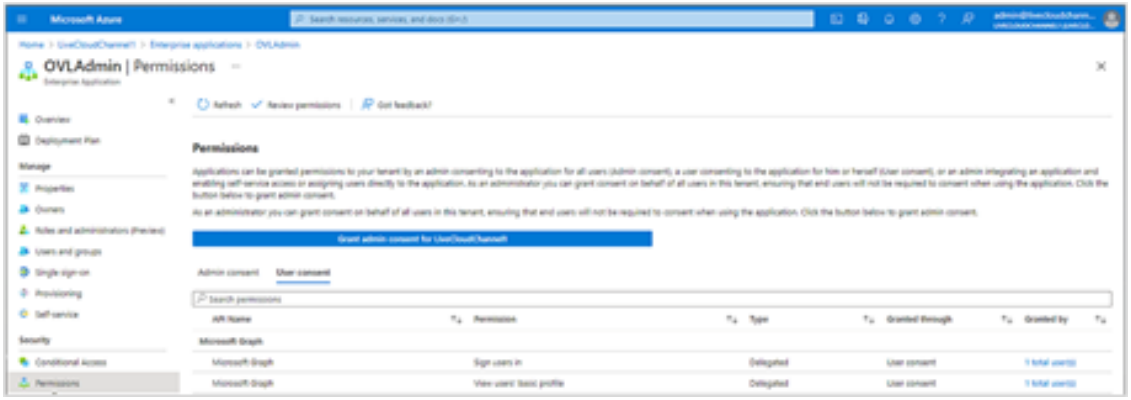
Troubleshooting - Granting Admin Consent

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

➢ To grant admin consent:

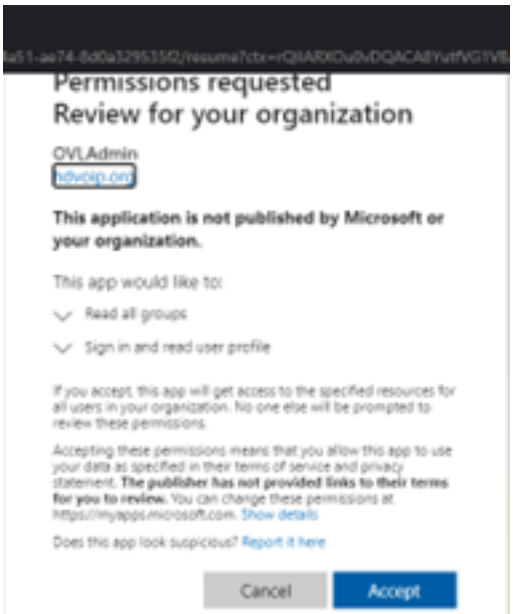
1. Login to Azure portal with "admin" of Azure channel tenant.
2. In the Navigation pane, select **Active Directory** > **Enterprise applications** > **OVOC Application**
3. Select **Security** > **Permissions**.

Figure 11-95: Permissions



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

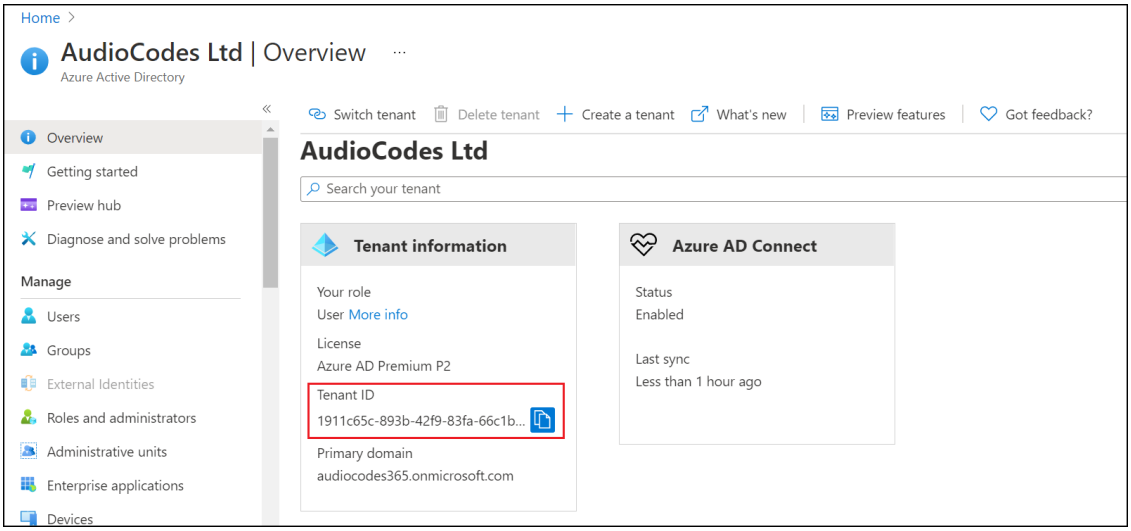
Register Microsoft Teams Application

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:

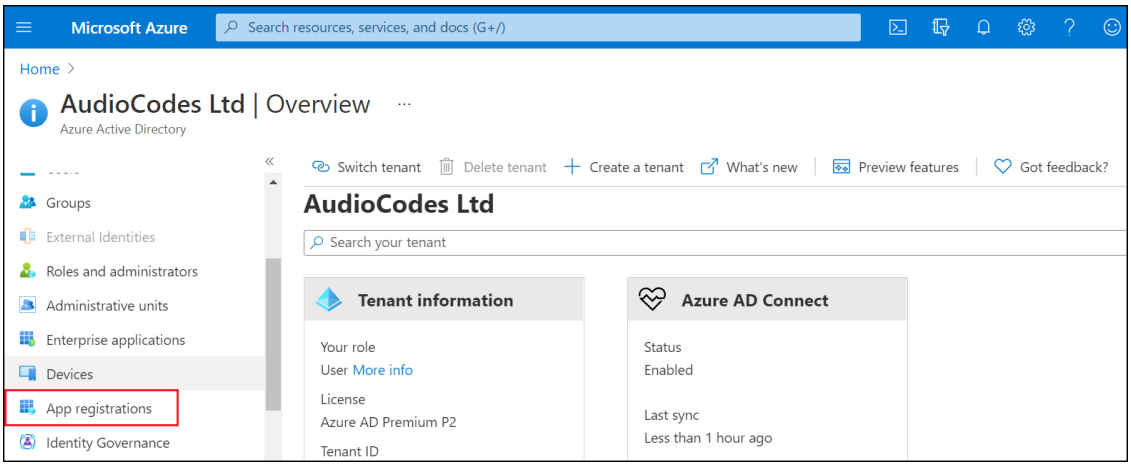
1. Open the Azure Portal, the Overview page is displayed with the Tenant ID of the managed Teams tenant.

Figure 12-1: Tenant ID



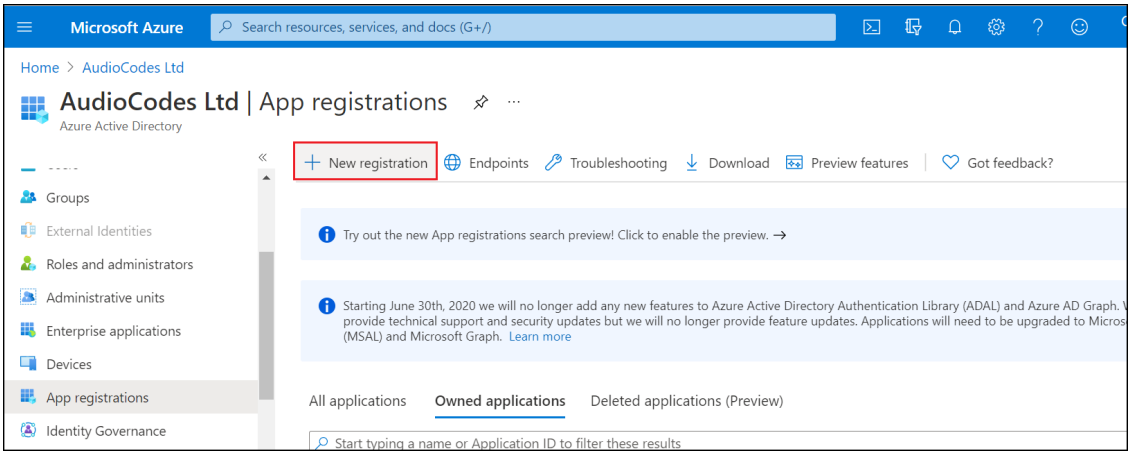
2. In the Navigation pane, select **App registrations.**

Figure 12-2: App Registrations



3. Click **New registration.**

Figure 12-3: New registration



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

Figure 12-4: Name the application

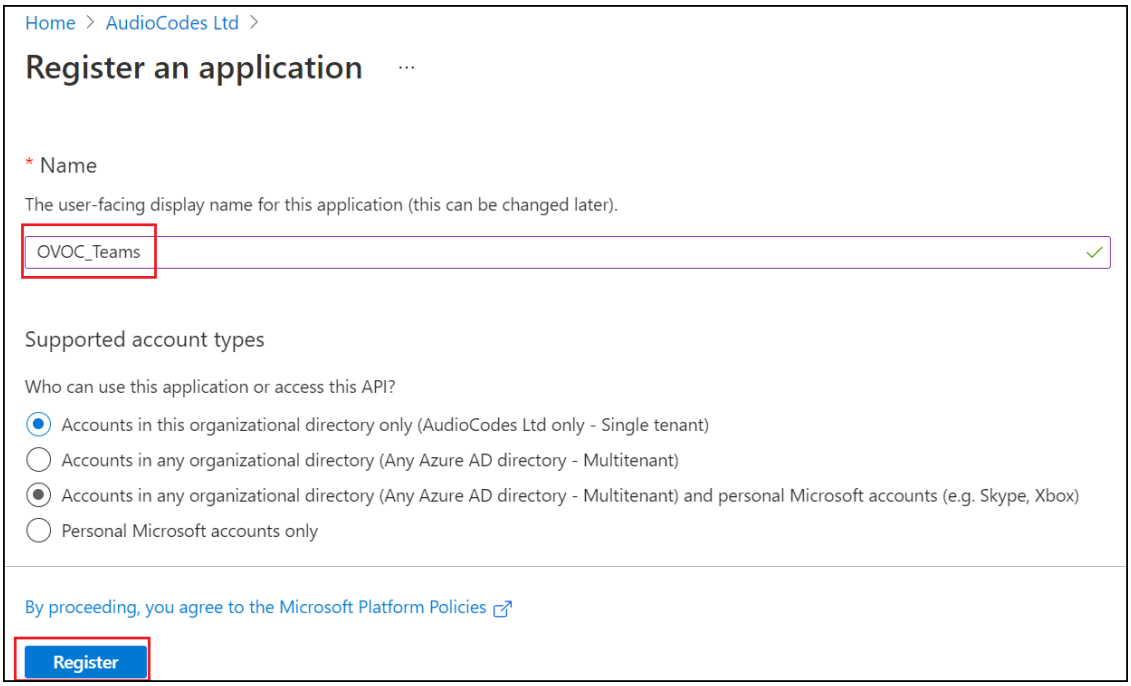
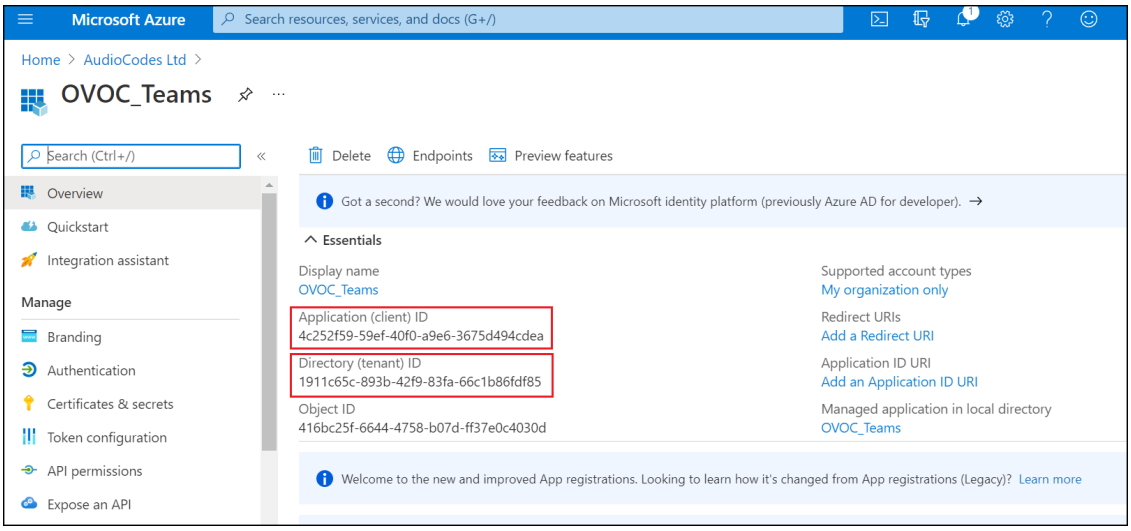
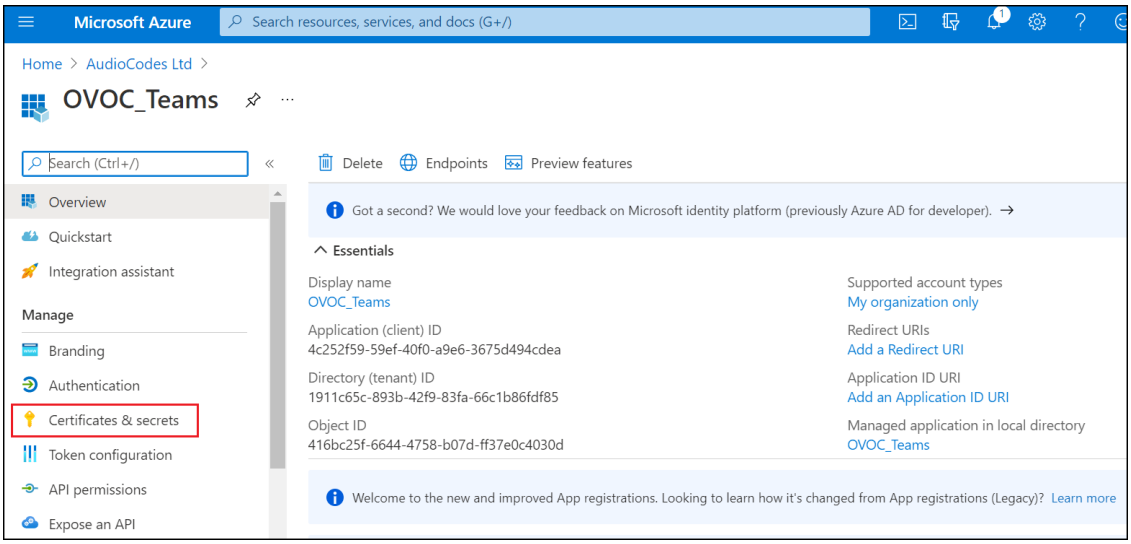


Figure 12-5: Successful Registration



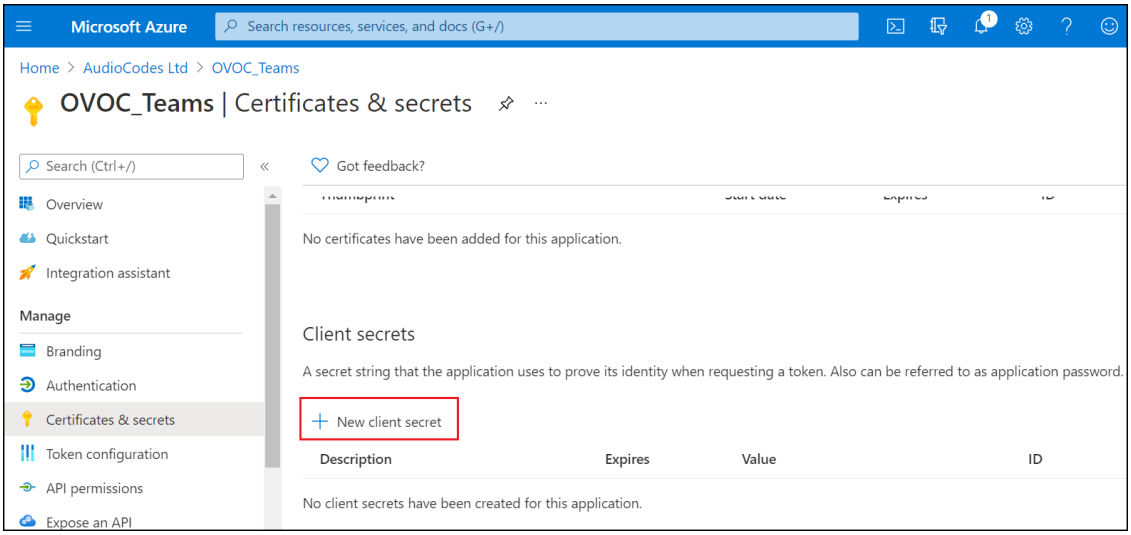
5. In the Navigation pane select **Certificate & Secrets.**

Figure 12-6: Certificate & Secrets



6. Click **New client secret**.

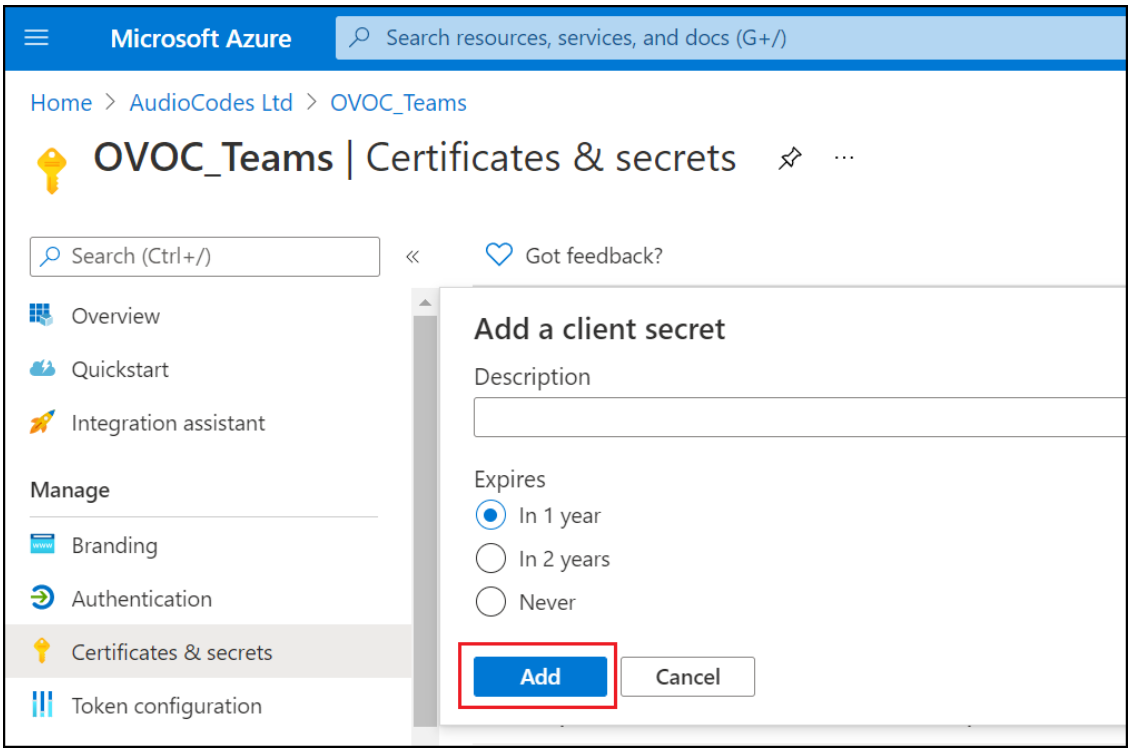
Figure 12-7: New Client Secret



7. Click **Add**.

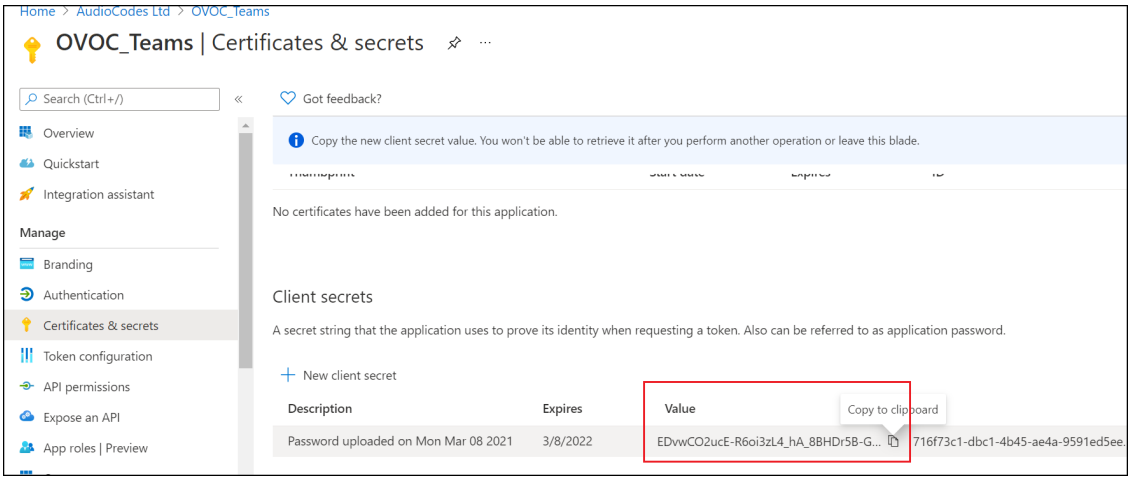
The newly added client secret is added as shown in the figure below.

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 Certificates & Secrets



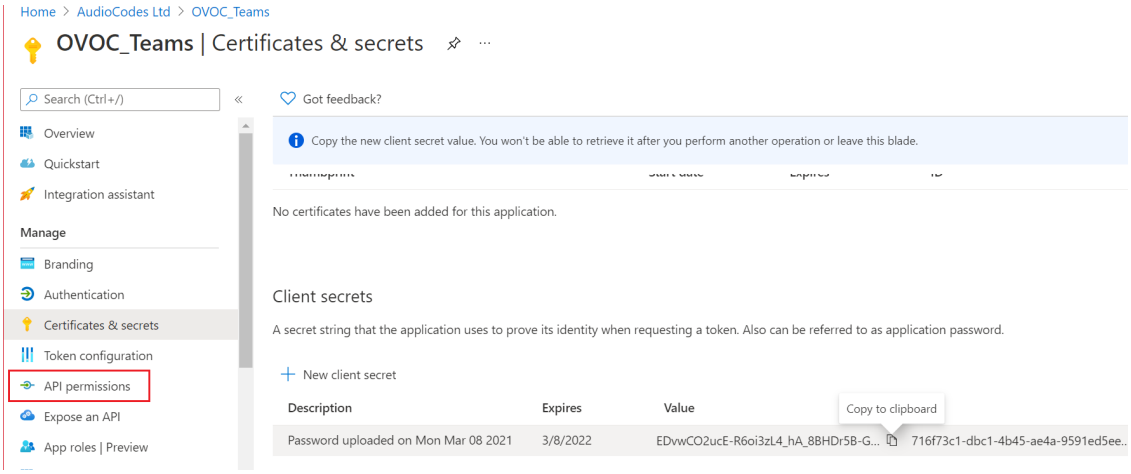
Configure Microsoft Graph API Permissions

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.

➢ **To configure Microsoft Graph permissions:**

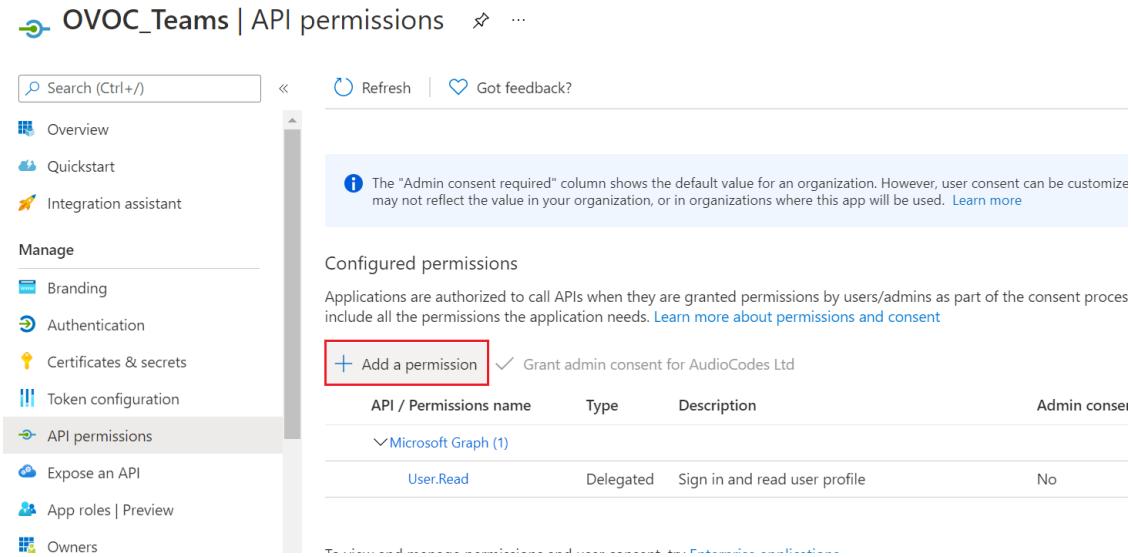
1. In the Navigation pane, select **API permissions**.

Figure 12-10: API Permissions



2. Click **Add a permission.**

Figure 12-11: Add a permission

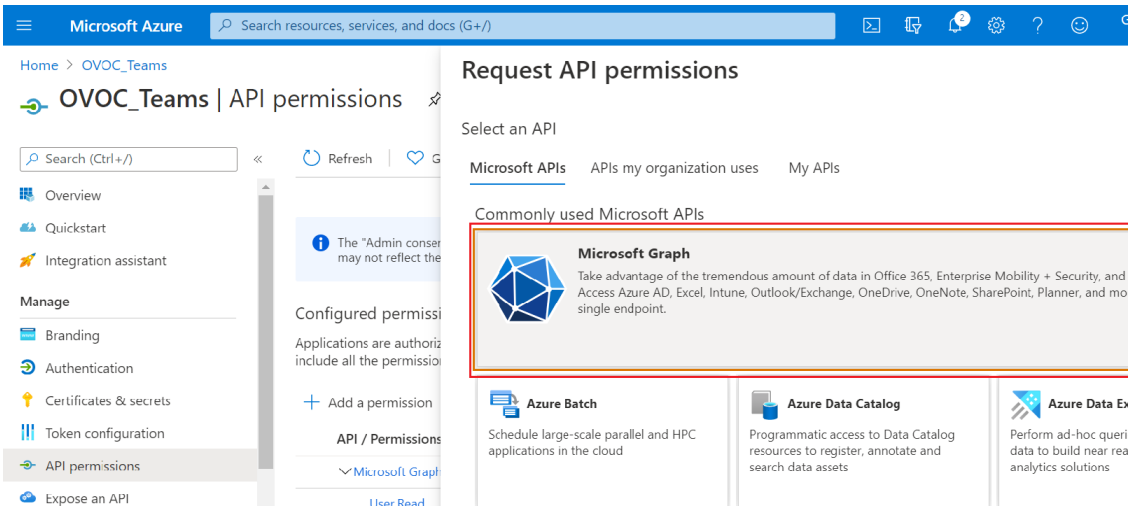


3. Select **Grant Admin Consent for** .... and select **Yes**.

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

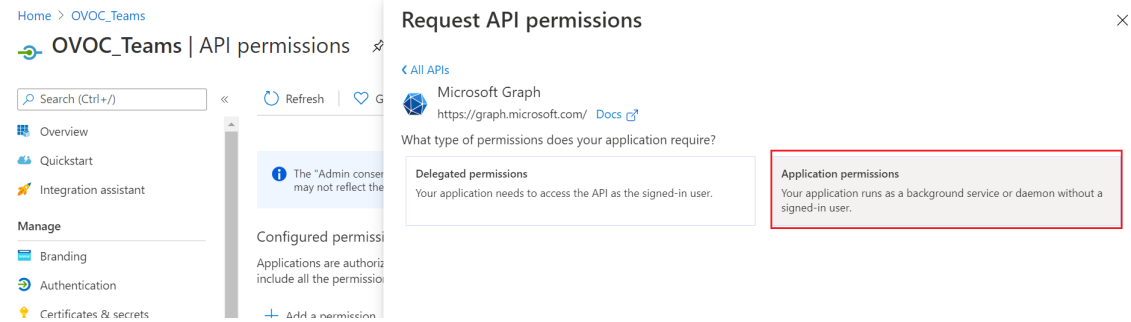
4. Select **Microsoft Graph**.

Figure 12-12: Request API Permissions



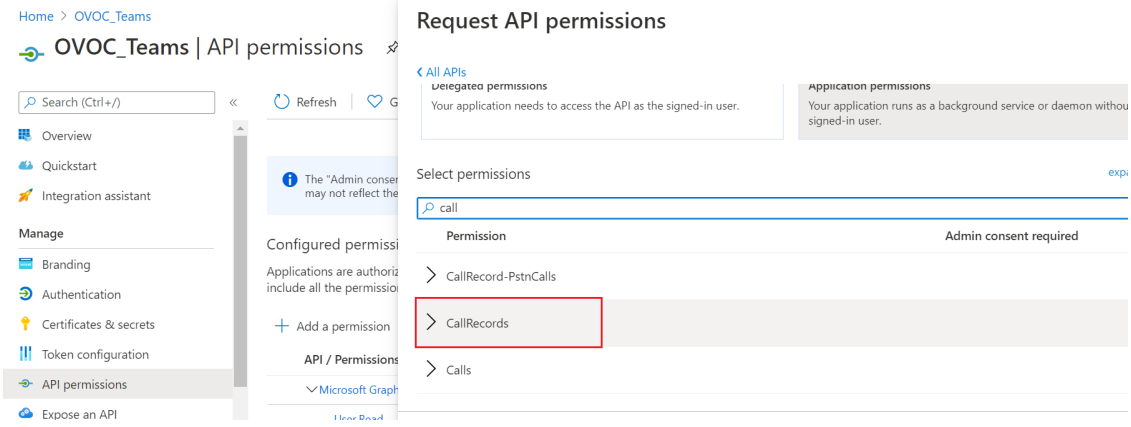
5. Select **Application permissions**.

Figure 12-13: Application permissions



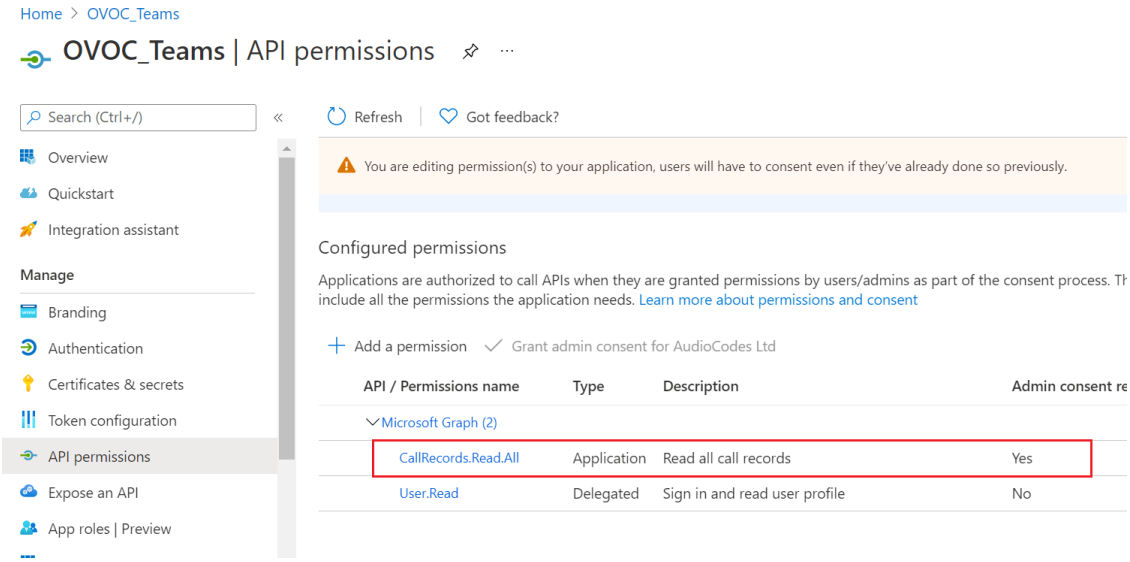
6. Search for Permission **Call Records**.

Figure 12-14: Call Records



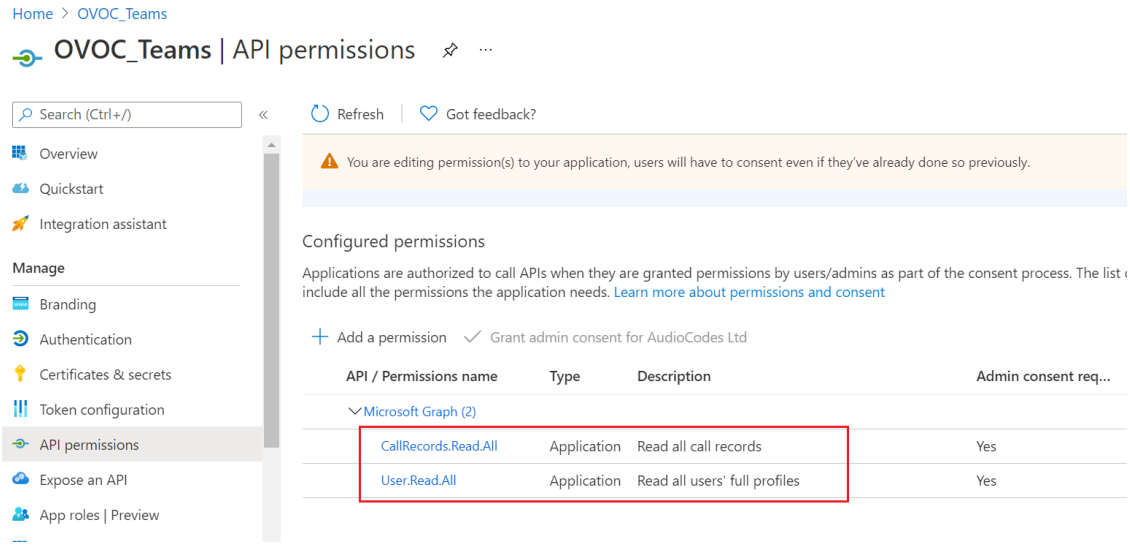
7. Set permission **CallRecords.Read.All** to enable access to retrieved call notifications.

Figure 12-15: API Permissions



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

Figure 12-16: User Read Permissions



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.

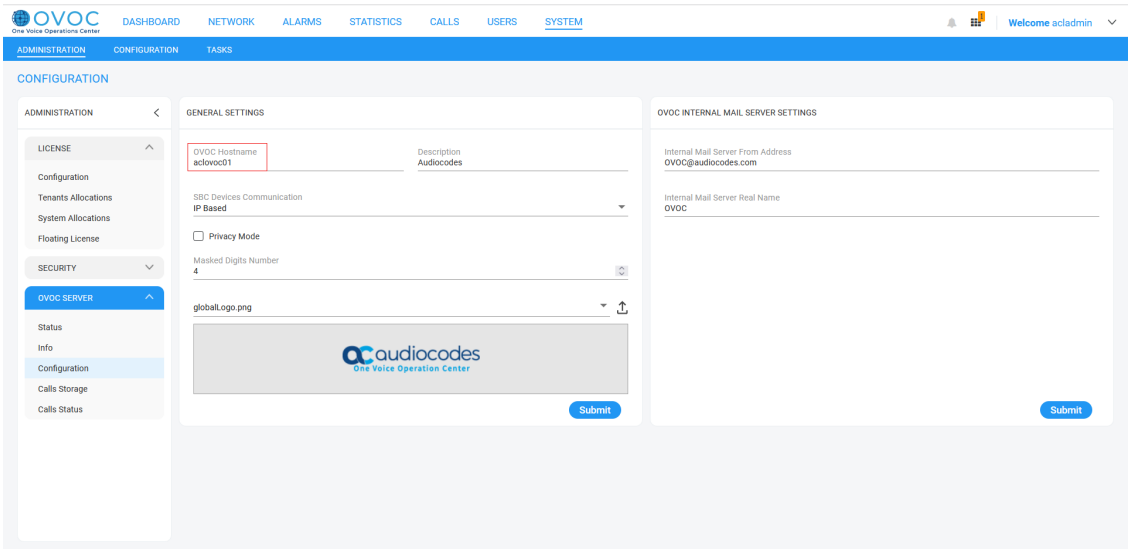
➢ **Do the following:**

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

```
C:\Users\enterprise1user>nslookup
www.google.com

Server:  tlc-ovoc.trunkpack.com

Address:  10.1.1.10

Non-authoritative answer:

Name:    www.google.com

Addresses:  2a00:1450:4006:801::2004

172.217.18.36
```

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

Figure 12-17: OVOC Server Configuration



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.

Table 13-1: Device Connection Scenarios

Configuration Option/Deployment Scenario	OVOC				Devices		
	AWS	Azure	On-Premises	Public Network	AWS	Azure	On-Premises
AudioCodes SBC Devices							
Cloud Architecture Mode	√	√		-	√	√	√
OVOC Server Configured with Public IP	√	√	√	√	√	√	√

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.

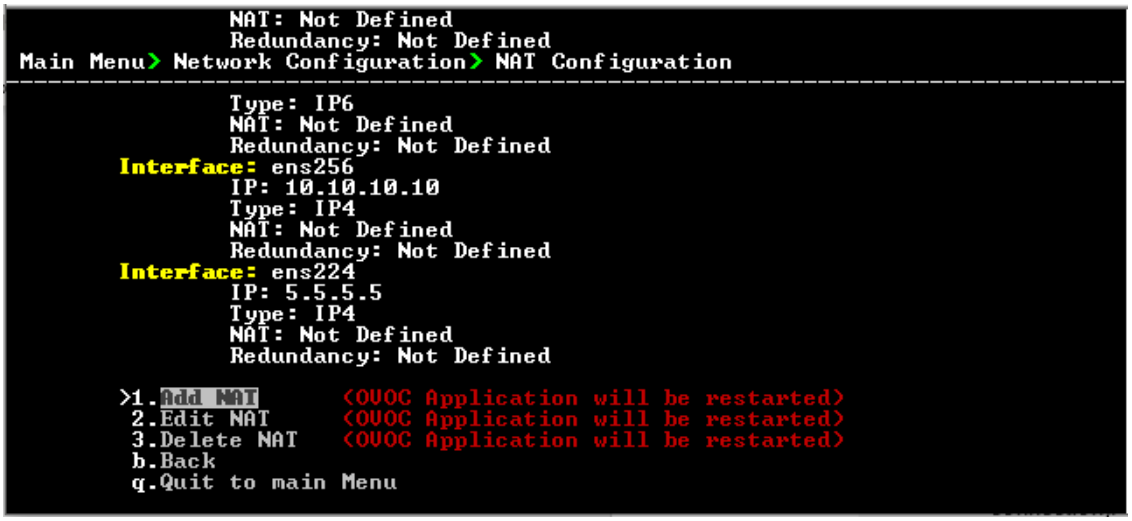
➢ To configure OVOC Server with Public IP address:

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

Figure 13-1: Configure NAT IP

2. Choose option **NAT Per Interface Configuration**.

Figure 13-2: NAT Per Interface Configuration



➢ 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

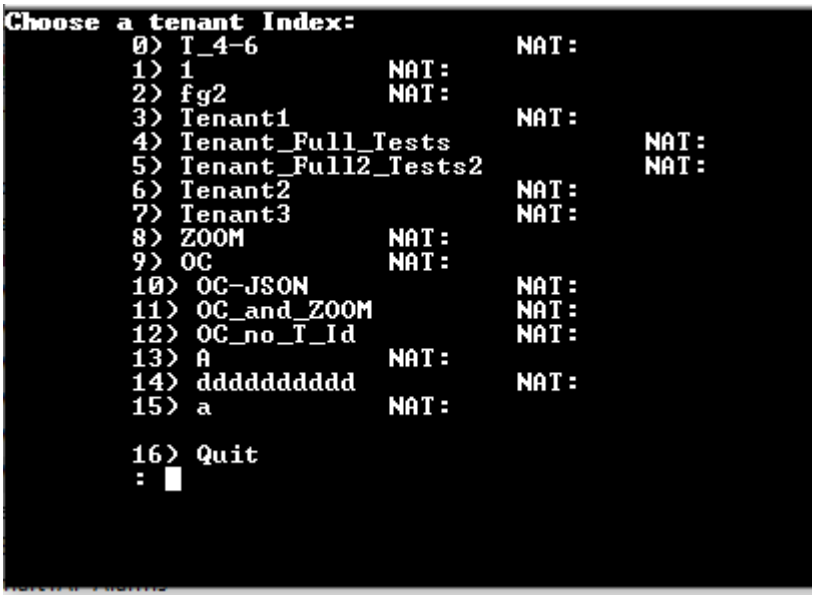
This option can be configured when OVOC is deployed behind a different NAT to customer tenants. It allows the configuration of an applicative level NAT interface for each tenant domain; Devices' incoming communication like SNMP traps, license reports and file upload/download will communicate via the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

2. Choose option **NAT Per Tenant Configuration**.

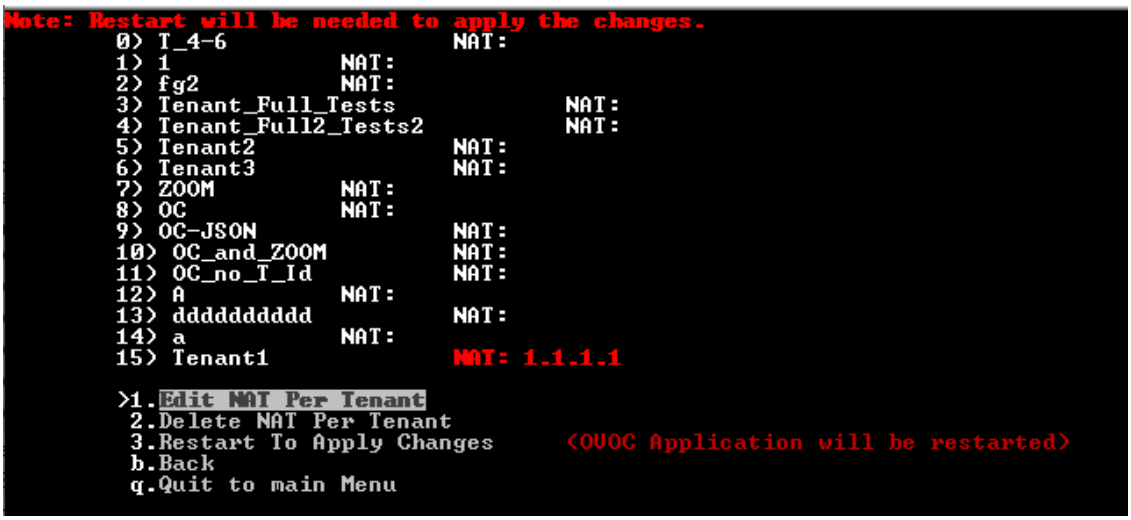


3. Enter the number corresponding to the tenant that you wish to configure.

Figure 13-5: NAT IP Address

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

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

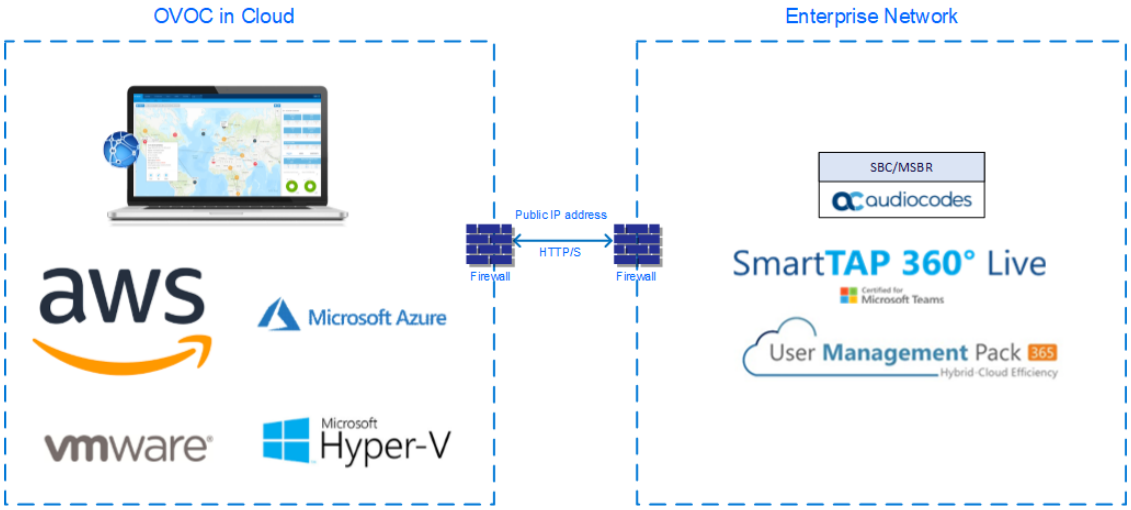
the devices and automatically determines their firmware version and subnet. Devices are then added to the appropriate tenant/region according to the best match for subnet address. When a default tenant exists, devices that cannot be successfully matched with a subnet are added to an automatically created 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.

Figure 13-7: 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)

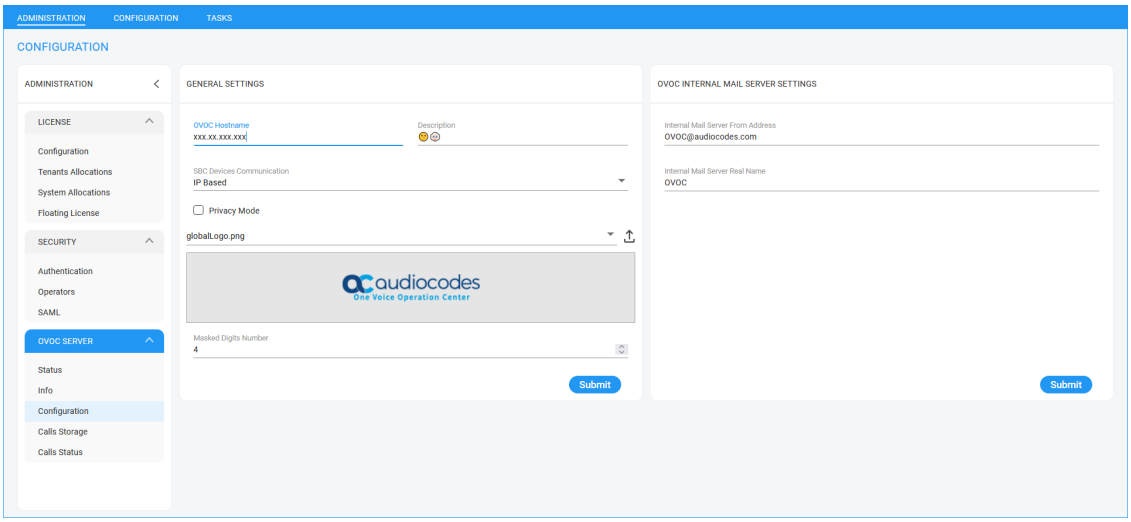
Configuring OVOC Web Interface for Tunnel Mode

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

➢ **To configure SBC devices communication:**

1. Open the OVOC Server Configuration screen.

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

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

The OVOC server is restarted.

> 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

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

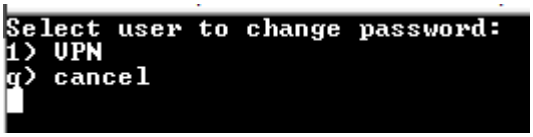
Change the Cloud Architecture Mode Service Password

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
```

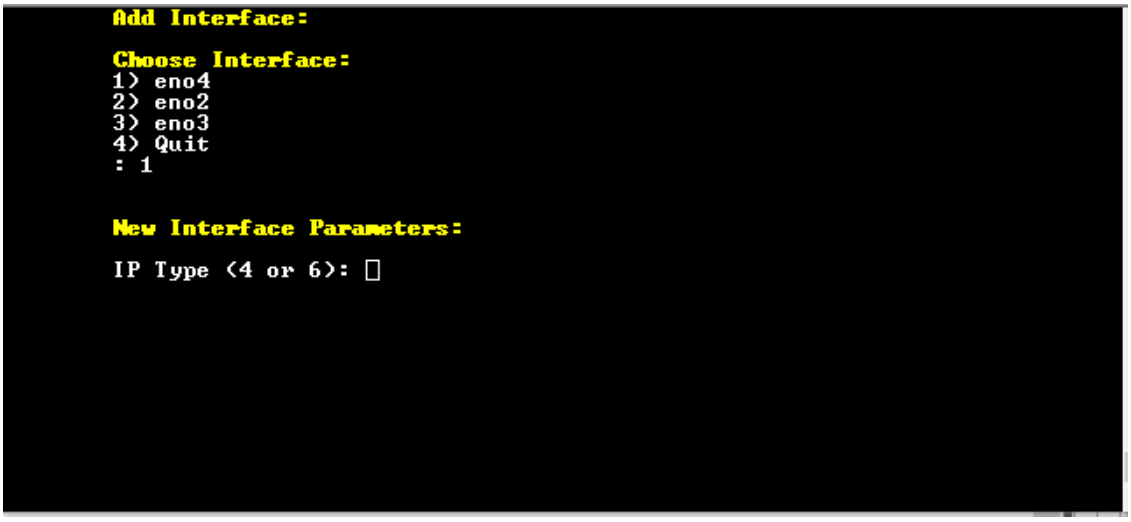
In the output it can be seen that ens160 is used for this IP address. Only one interface can be selected from all interfaces on the server to be use for routing this IP address.

> 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:

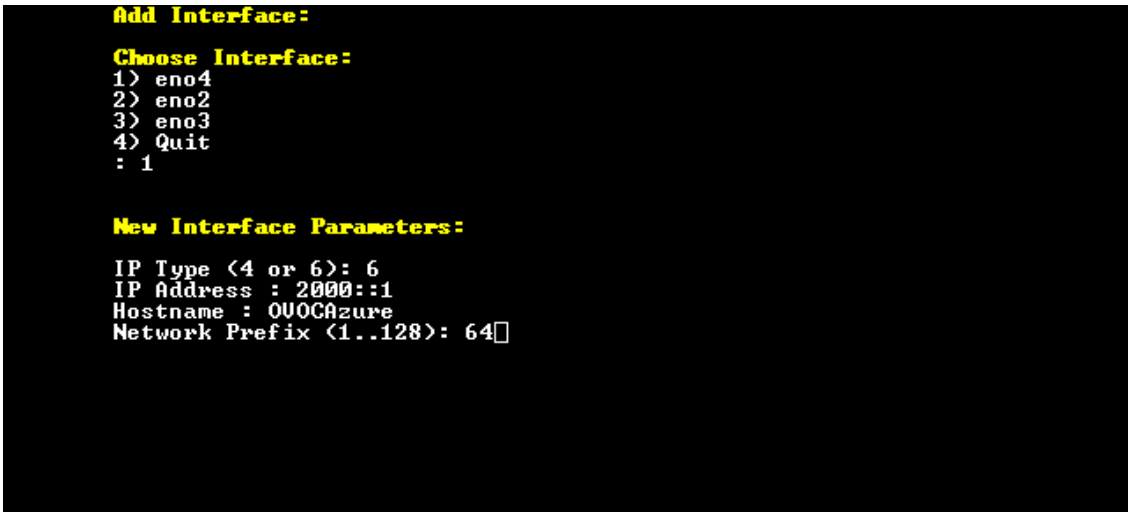
1. From the Ethernet Interfaces menu, choose option **1**; a list of currently available interfaces (not yet configured) is displayed.

Figure 13-13: Add Interface



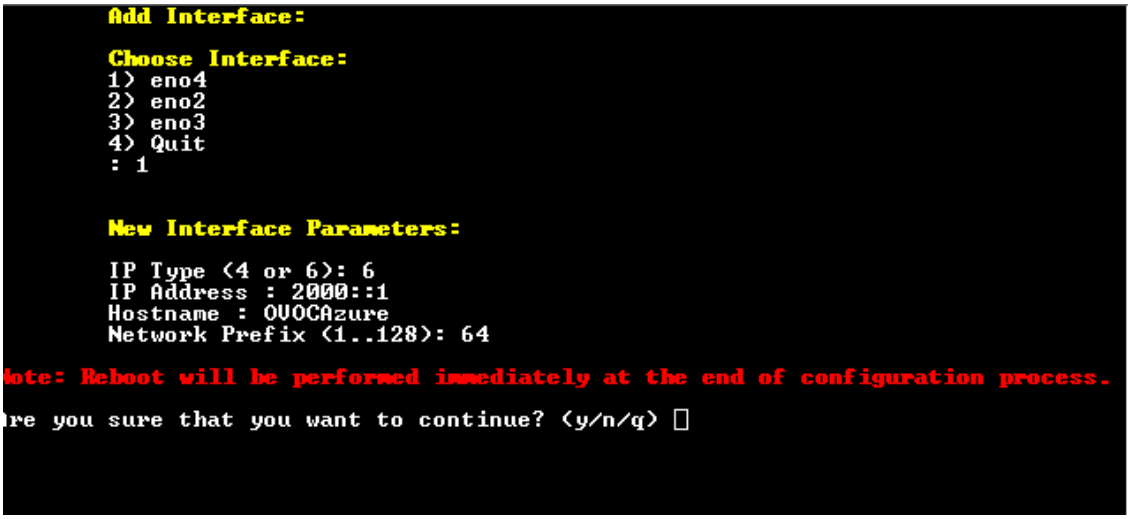
2. Enter the number of the IP interface that you wish to modify (on HP machines the interfaces are called 'eno1', 'eno2', etc) and then press Enter.
3. Choose the IP interface type and then press Enter:
   - Enter 4 for IPv4
   - Enter 6 for IPv6

Figure 13-14: Add Interface



4. 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:

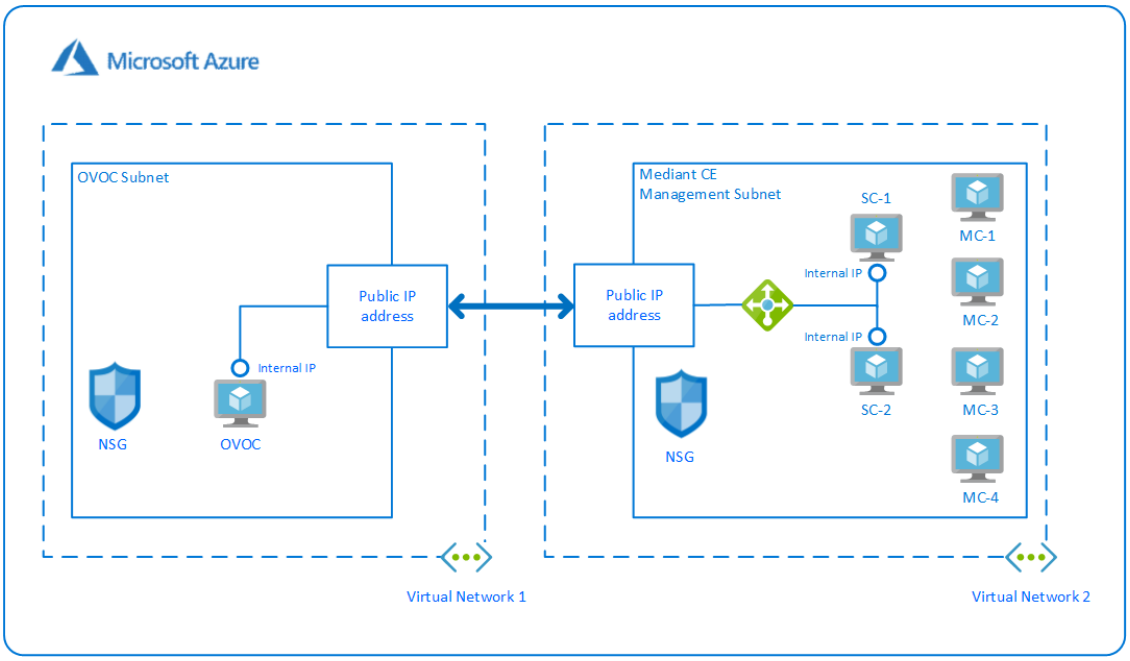
- Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on the next page
- Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address on page 163

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*.

Figure 13-16: Microsoft Azure Topology



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:**

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 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
5. 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

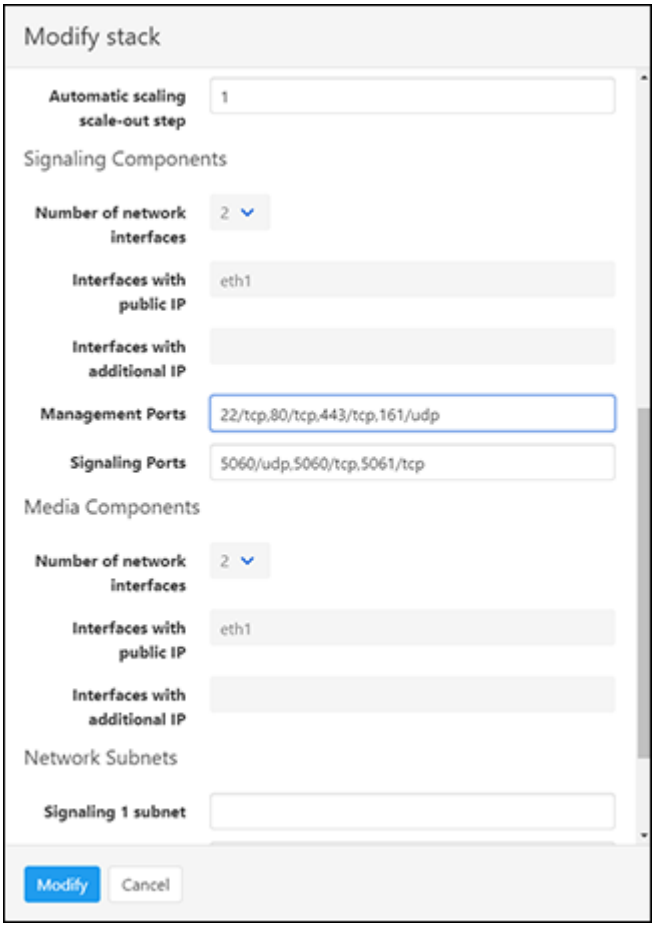
Configuring Mediant CE SNMP Public IP Connection using Stack Manager

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".
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 13-17: 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.
2. 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.
5. 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.
7. 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>
```

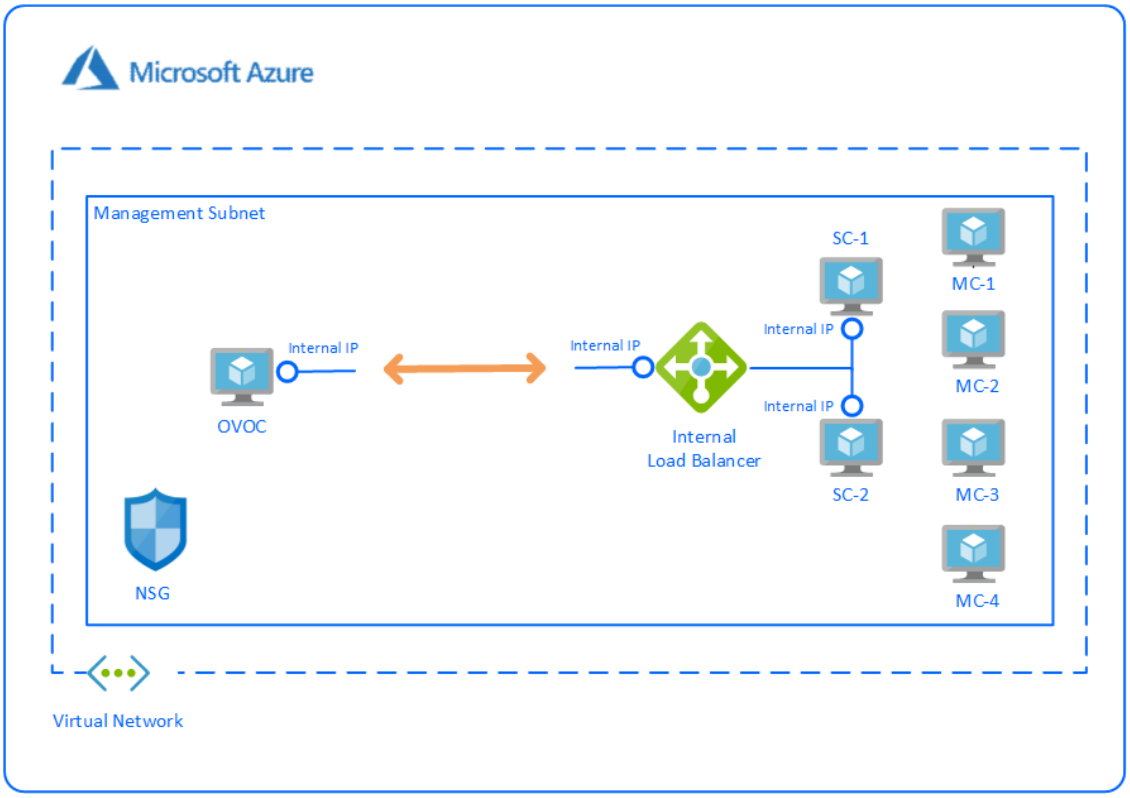
11. Reset the device for your settings to take effect (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

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.
5. 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

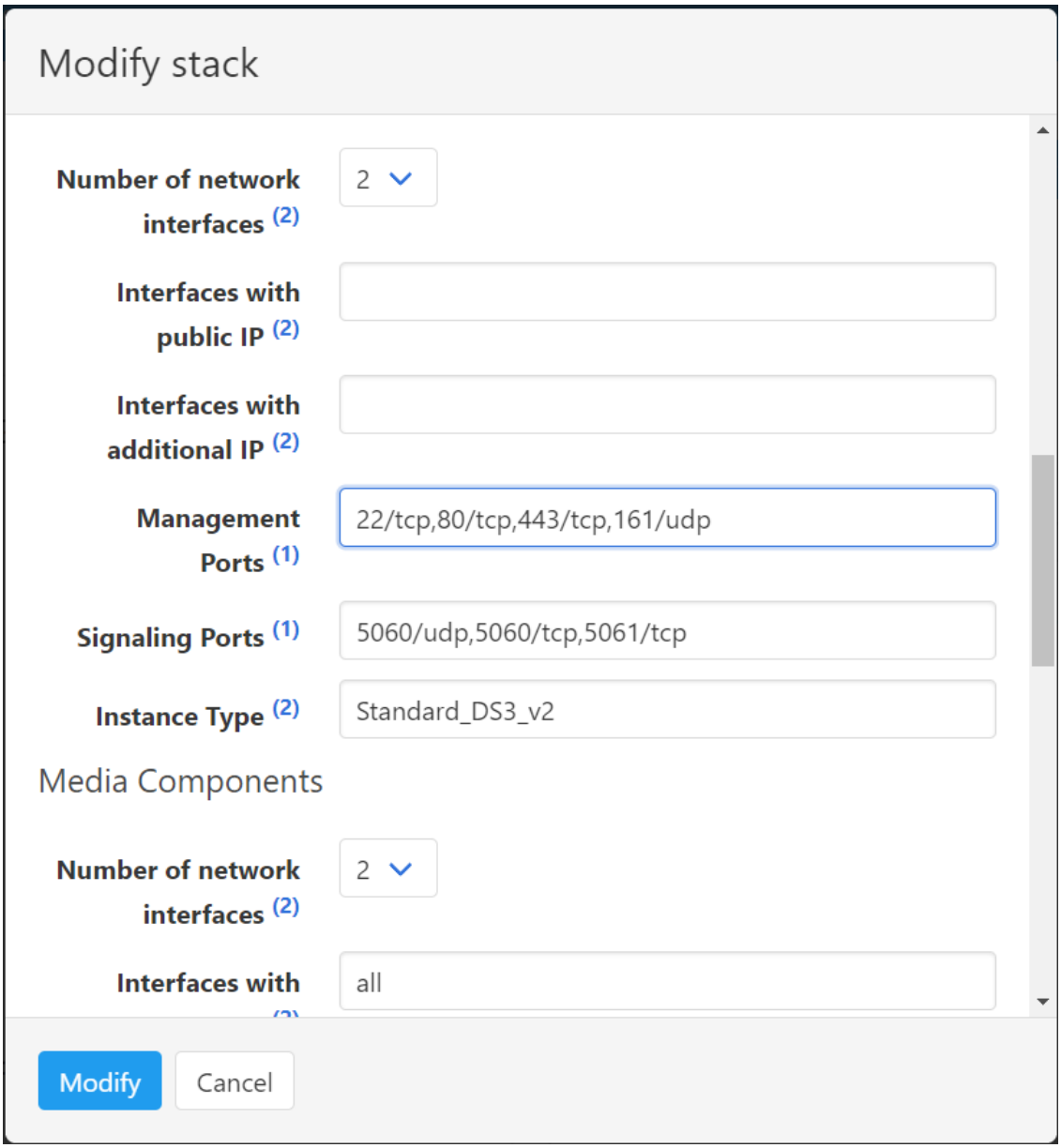
Configuring Mediant CE SNMP Internal IP Connection with OVOC using Stack Manager

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".
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 13-19: Modify Stack



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.
2. 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.
4. 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>
```

8. 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.
5. 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

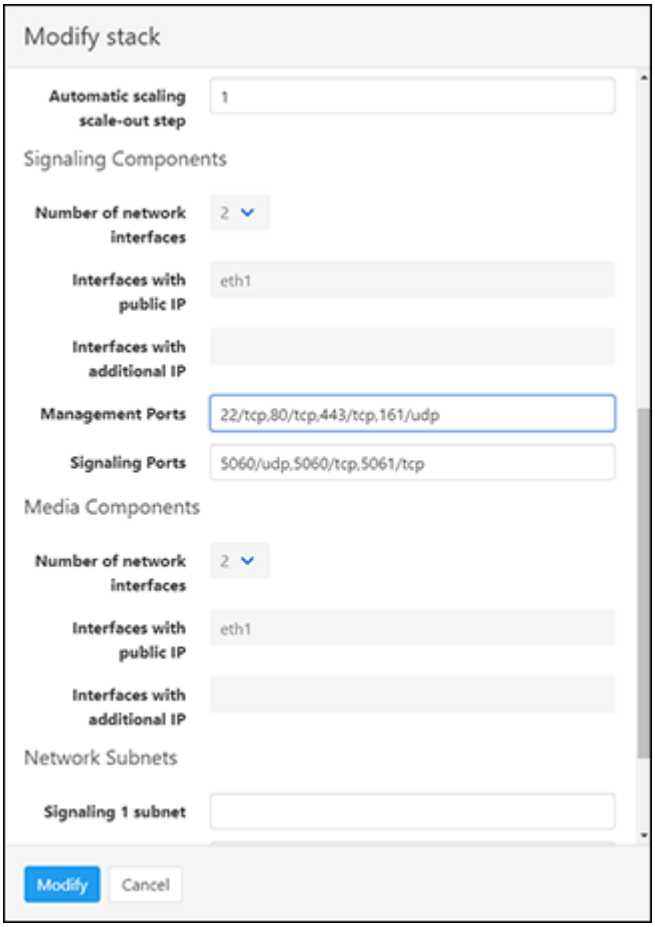
Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager

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



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.
2. 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.
5. 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.
7. 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>
```

11. 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:

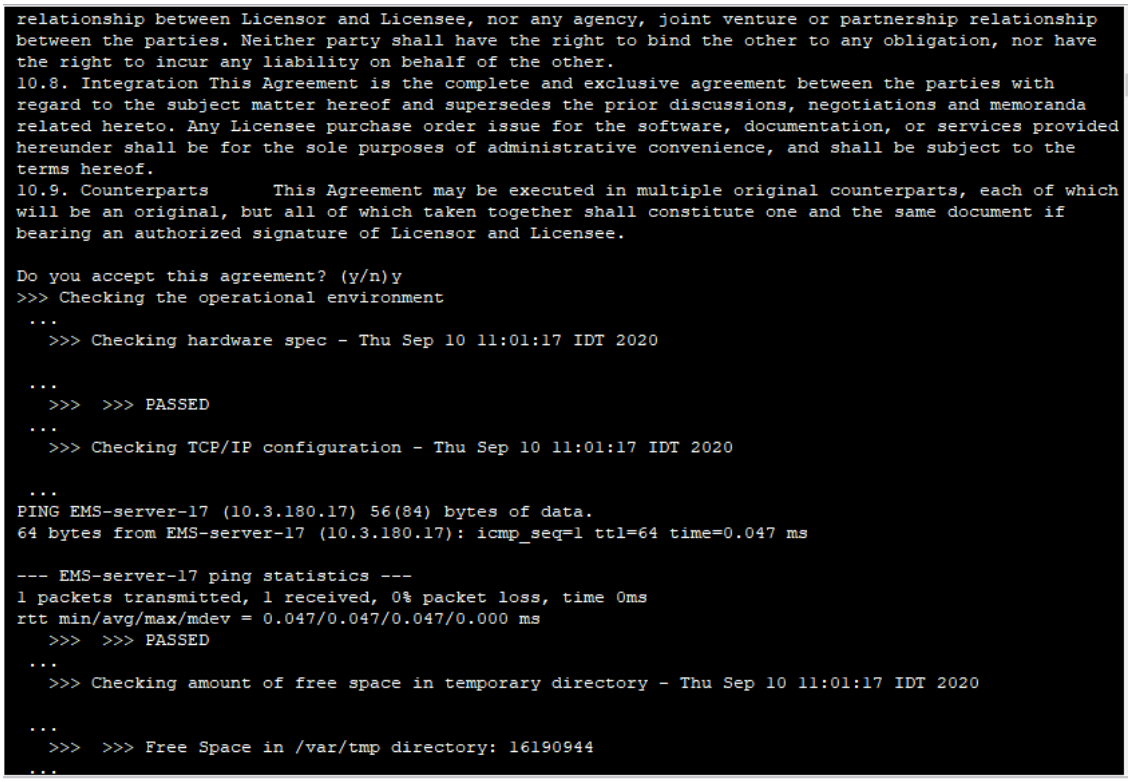
```
./install
```

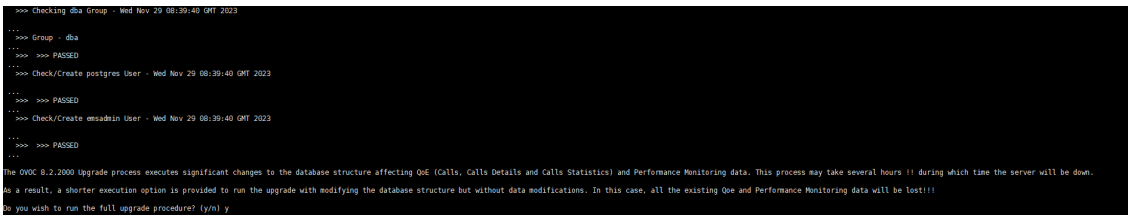
Figure 14-1: OVOC server Installation Script

```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Start executing User Login Check script at Thu Sep 10 11:01:16 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Thu Sep 10 11:01:16 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 14-2: OVOC server Upgrade – License Agreement





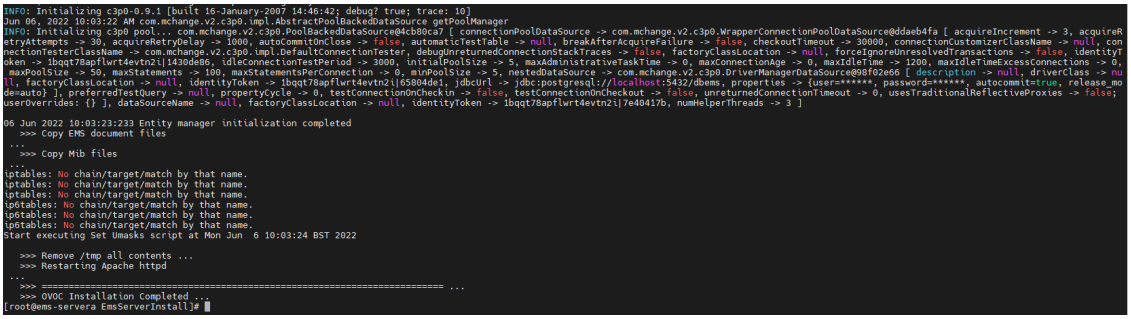
9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter **y** to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



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:

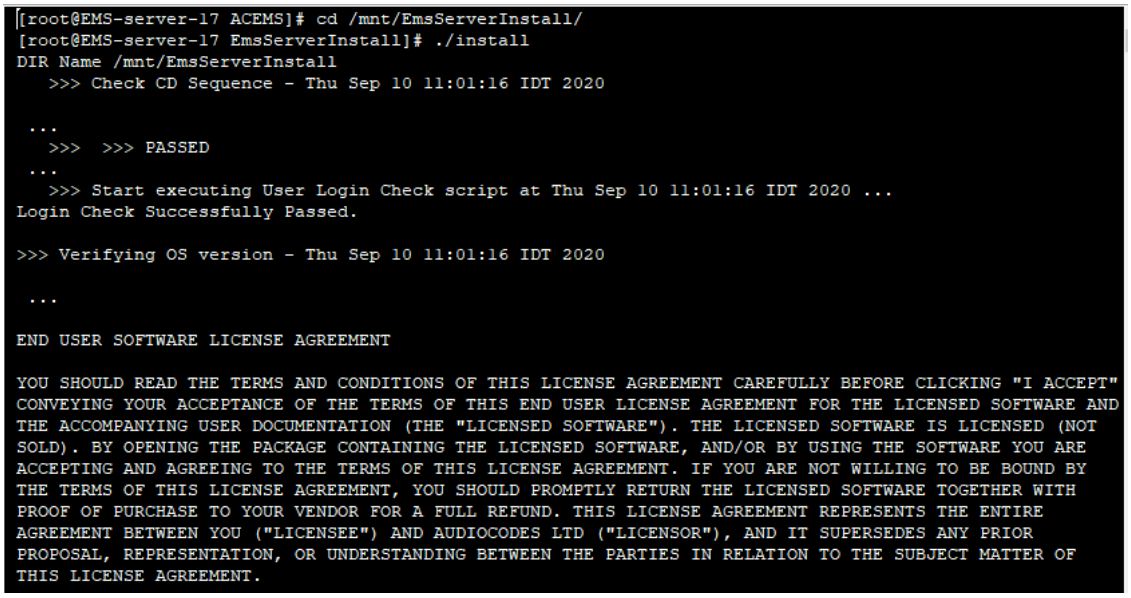
```
mount /home/acems/DVD3_OVOC_ 8.4.45.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

7. Run the installation script from its location:

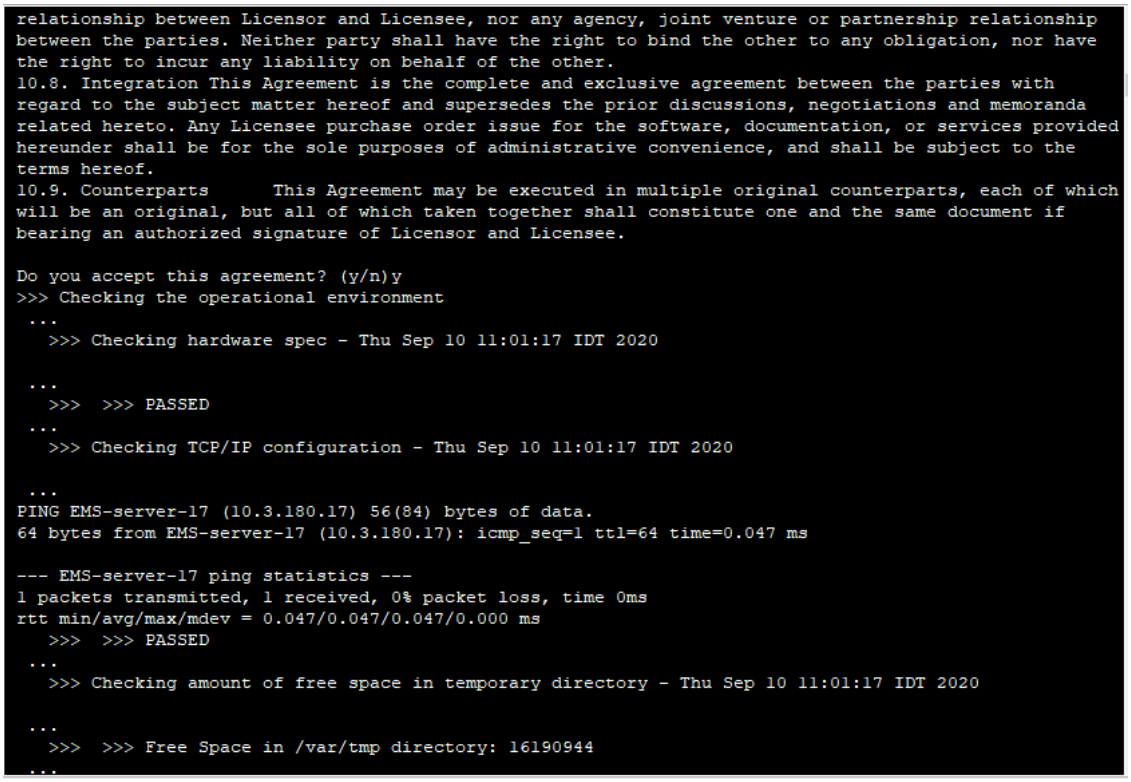
```
./install
```

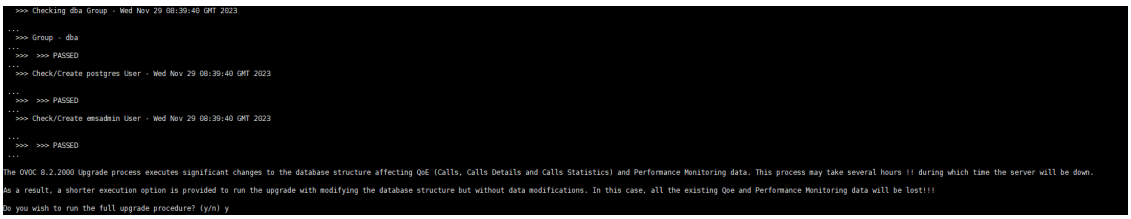
Figure 15-1: OVOC server Installation Script



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

Figure 15-2: OVOC server Upgrade – License Agreement





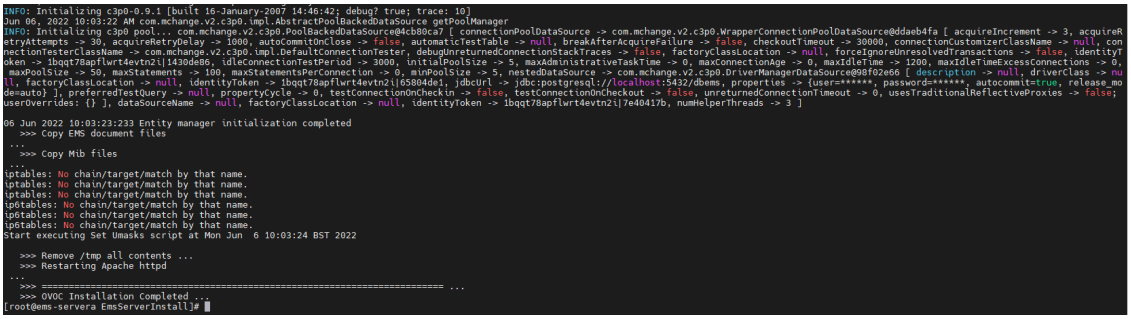
9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter **y** to 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 15-3: OVOC Server Installation Complete



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.
2. 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):

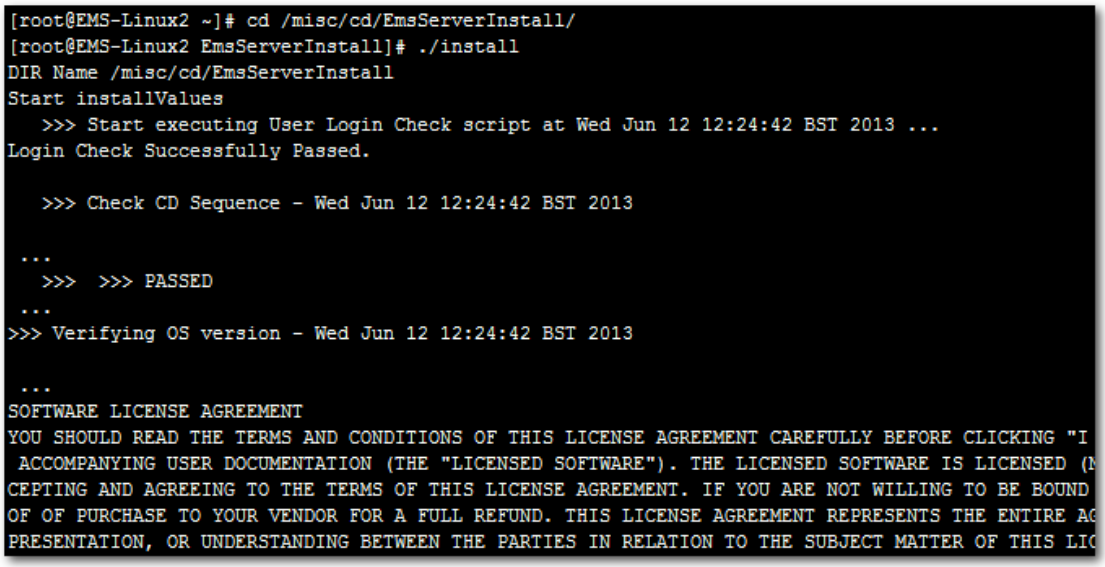
```
mount /home/acems/DVD3_OVOC_/mnt
```

5. Run the installation script from its location:

```
cd /misc/cd/EmsServerInstall/
```

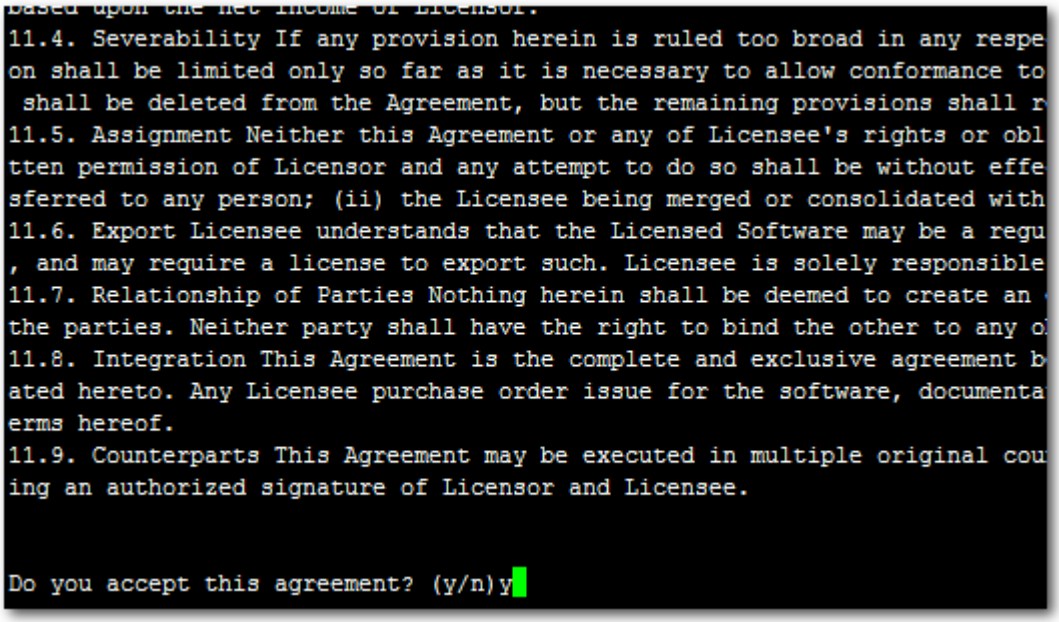
```
./install
```

Figure 16-1: OVOC server Upgrade



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

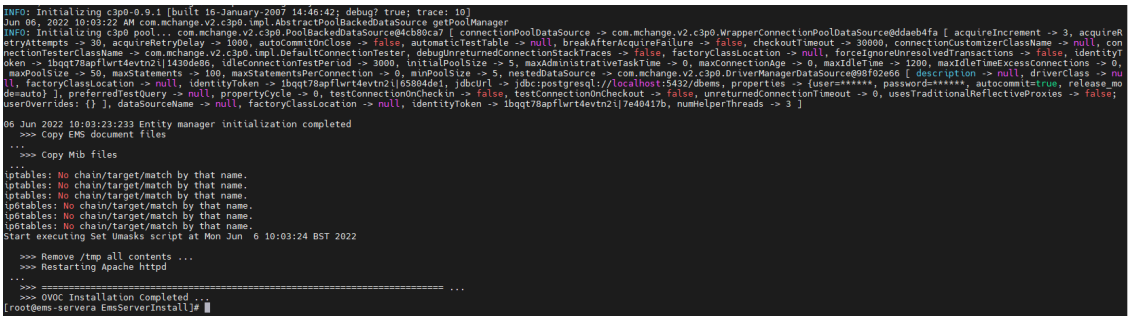
Figure 16-2: OVOC server Upgrade – License Agreement



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, 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

Figure 16-3: OVOC server Installation Complete



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).
2. 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:

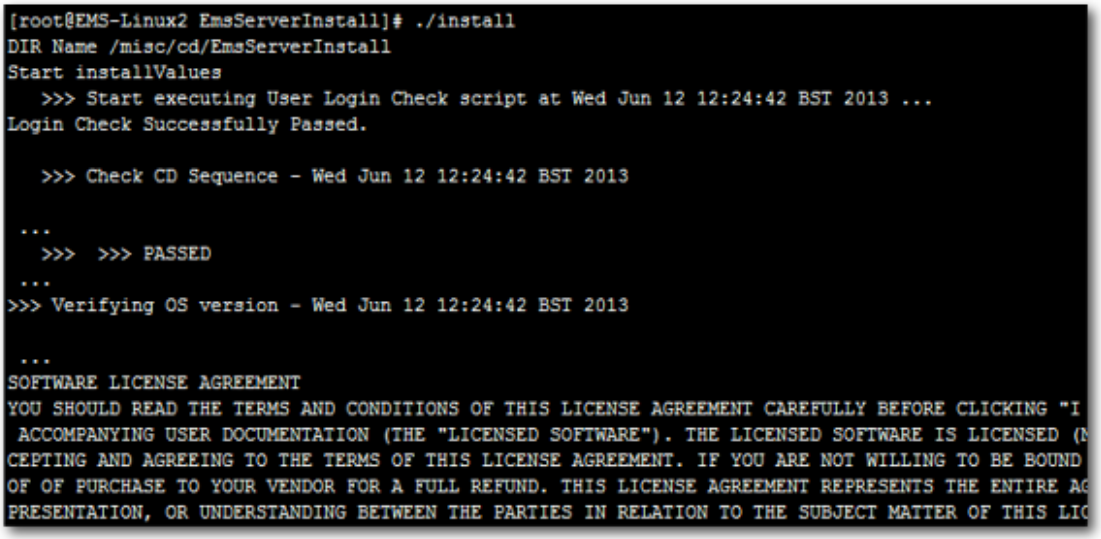
```
mount /home/acems/DVD3_OVOC_ 8.4.45.iso /mnt
```

```
cd /mnt/EmsServerInstall
```

5. Run the installation script from its location:

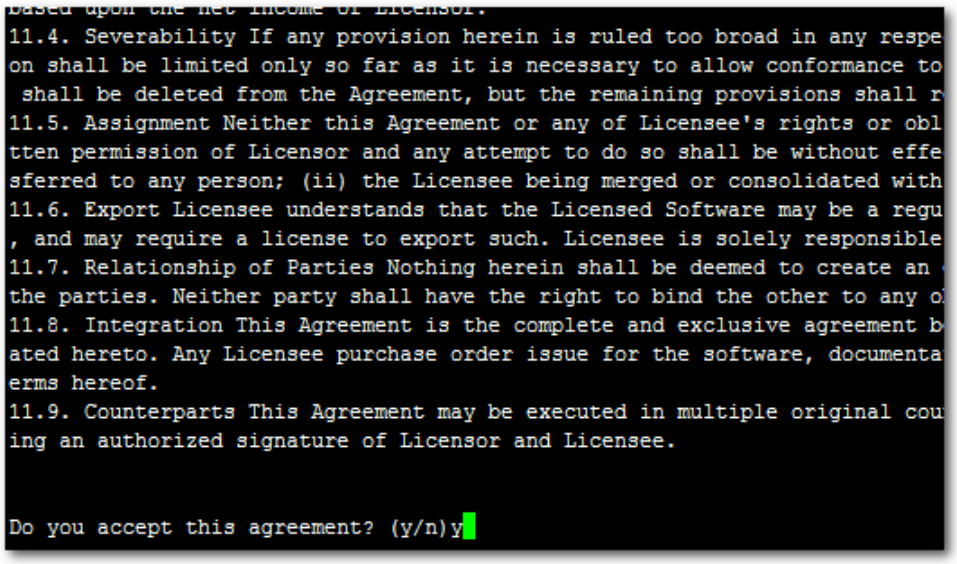
```
./install
```

Figure 16-4: OVOC server Upgrade



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

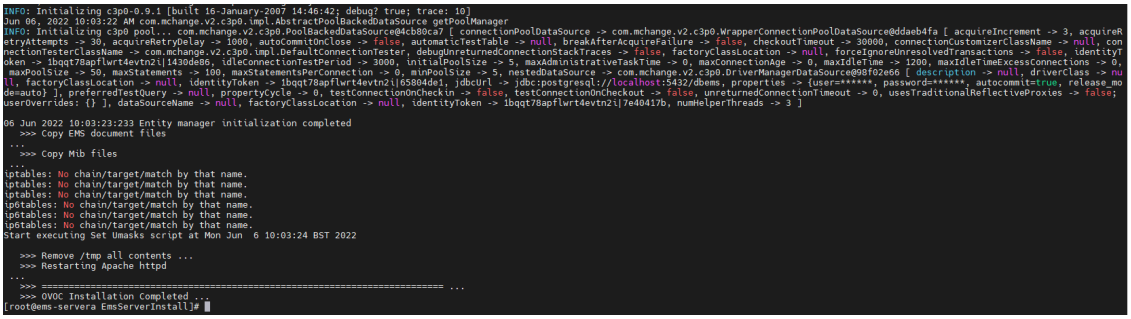
Figure 16-5: OVOC server Upgrade– License Agreement



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



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
```

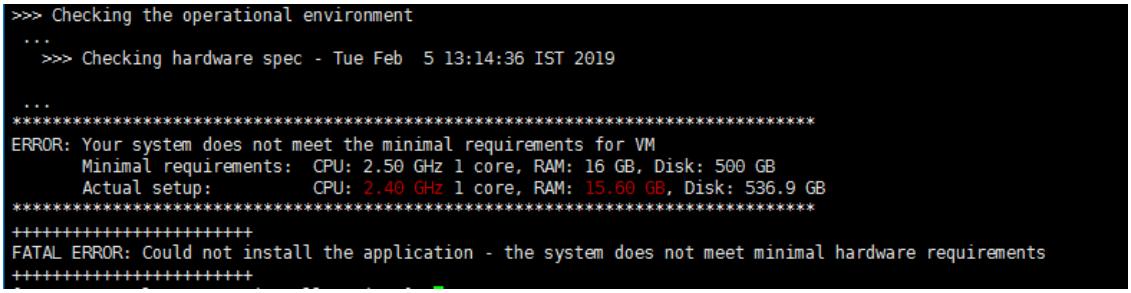
12. Verify that all processes are up and running (Viewing Process Statuses on page 203) and verify that login to OVOC Web client is successful.

17 Installation and Upgrade Troubleshooting of the Operational Environment

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

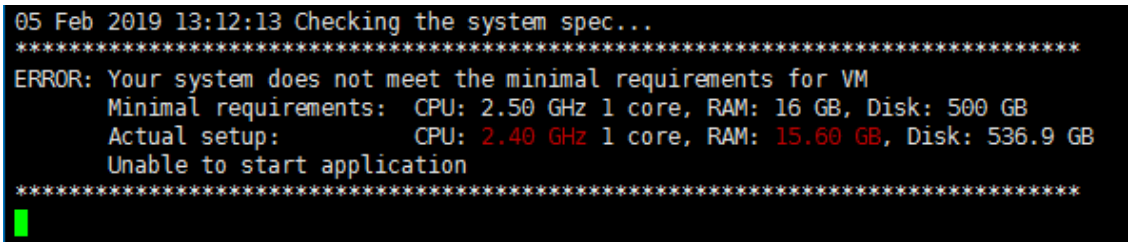
- If you attempted to upgrade and your system did not meet the minimum hardware requirements, the following message is displayed:

Figure 17-1: Minimum Hardware Requirements Upgrade



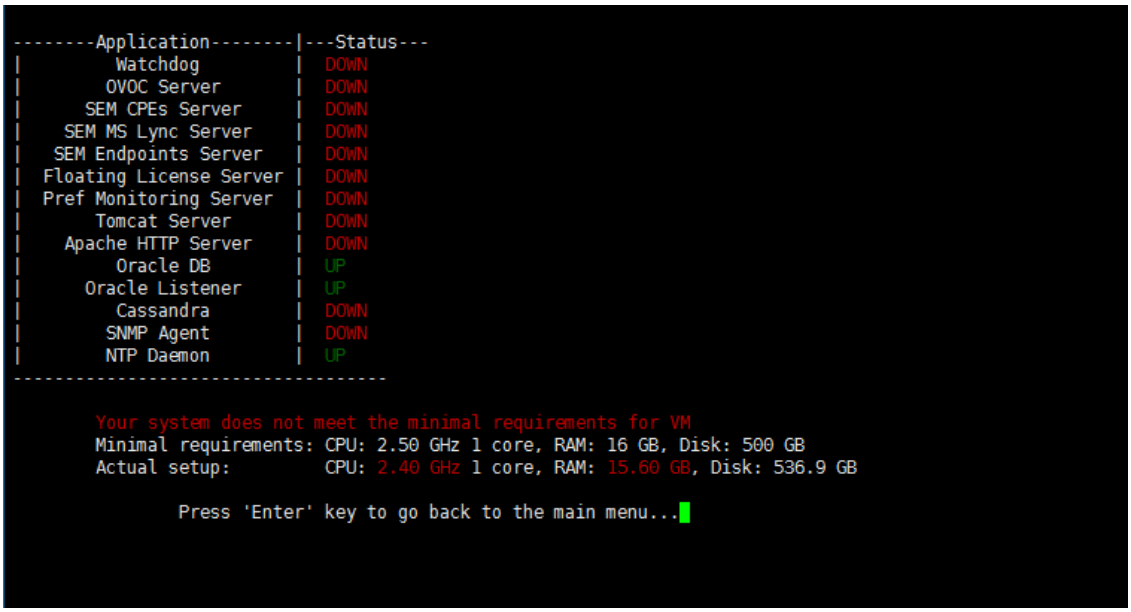
- If the OVOC server hardware configuration is changed and then the server is restarted, the following message is displayed in the /var/log/ems/nohup.out file.

Figure 17-2: Minimum Hardware Requirements System Error



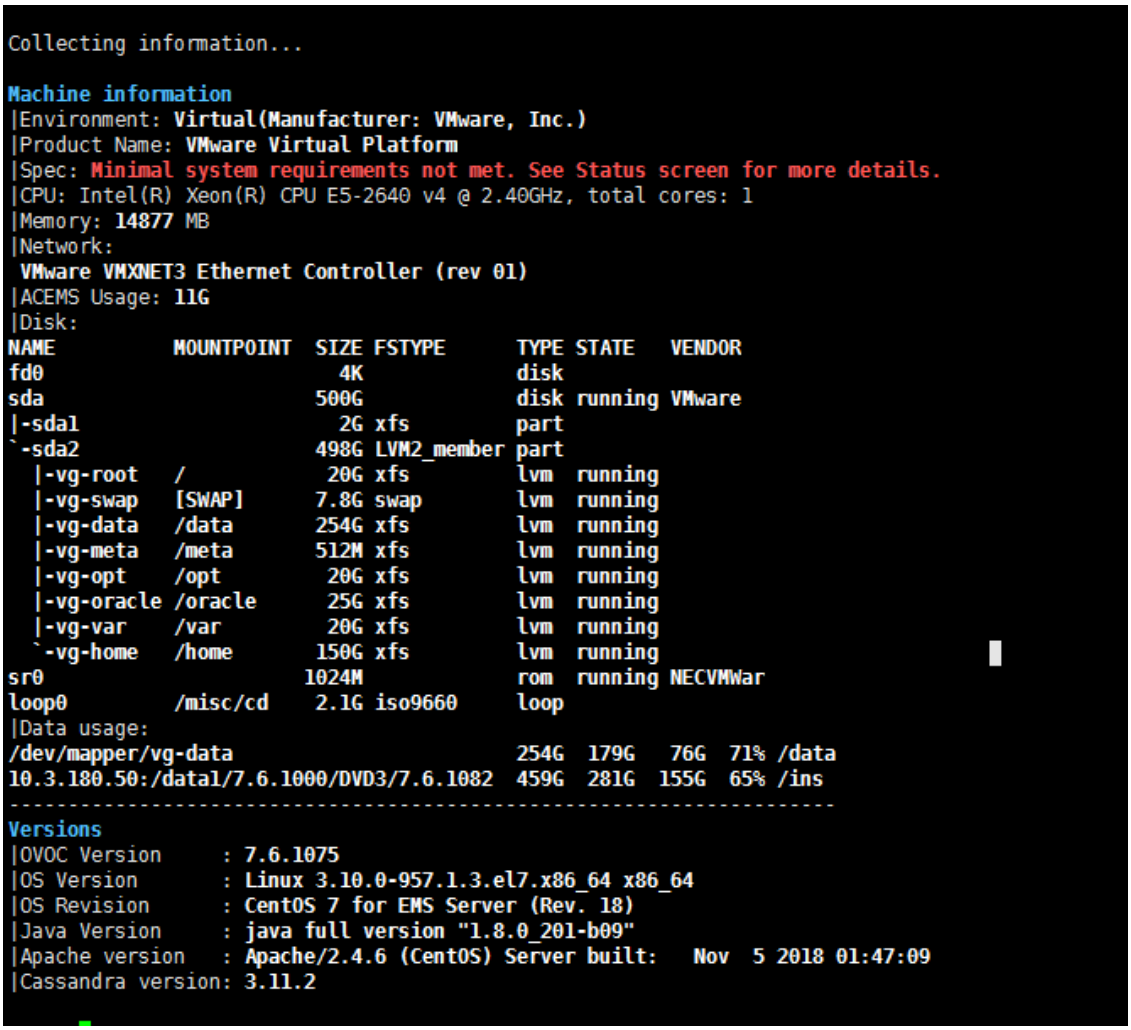
- Whenever an upgrade or clean installation is performed, and then the hardware settings are changed, which results in the minimum requirements not being met, the following message is displayed in the OVOC Server ManagerStatus screen :

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



Part V

OVOC Server Machine Backup and Restore

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

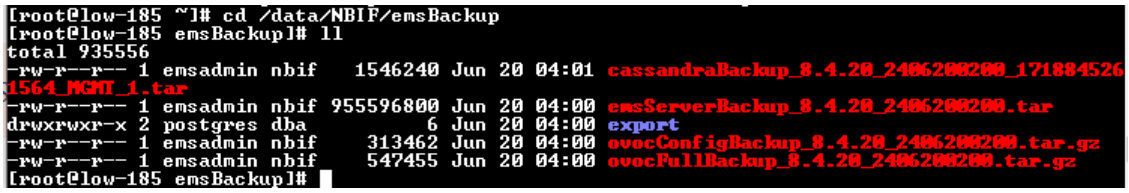
18 OVOC Server Backup Processes

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



➢ **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

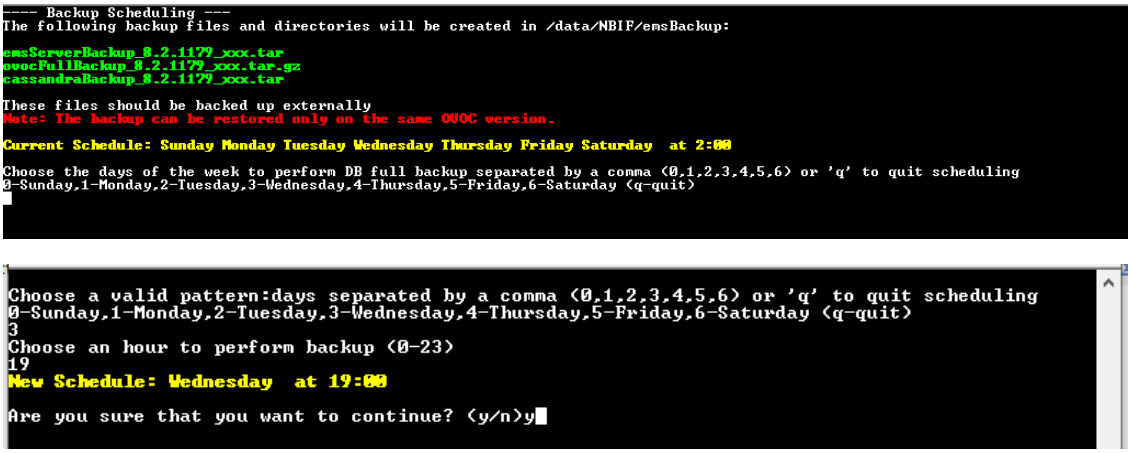
This step describes how to reschedule the time to run the automatic backup of the files described in OVOC Server Backup Processes above. By default, the backup is run daily at 2:00

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



3. Type **y** to confirm.

19 OVOC Server Restore

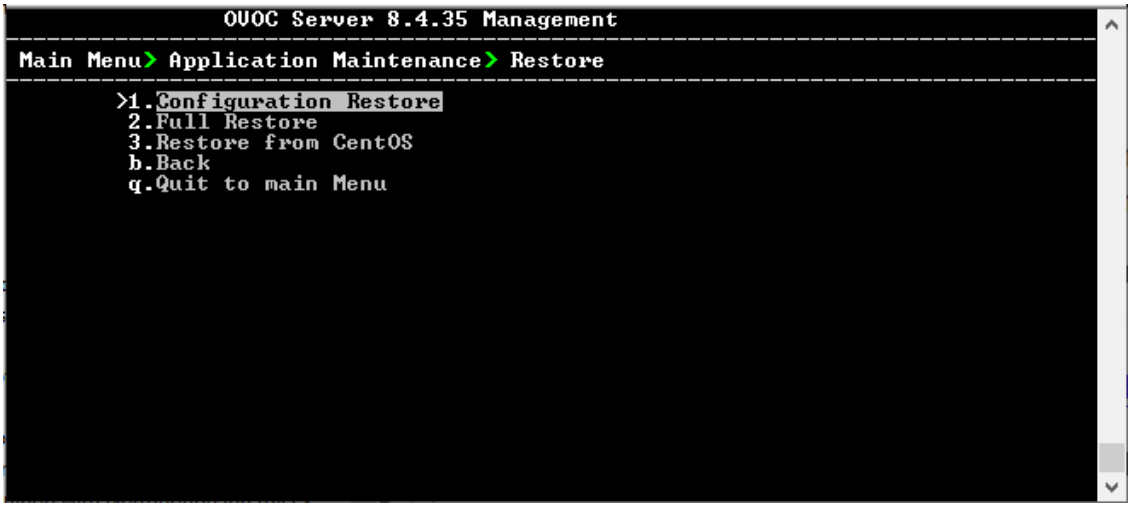
The OVOC server can be restored from the original machine where the backup files were created or from any other machine.

- 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.
5. 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:

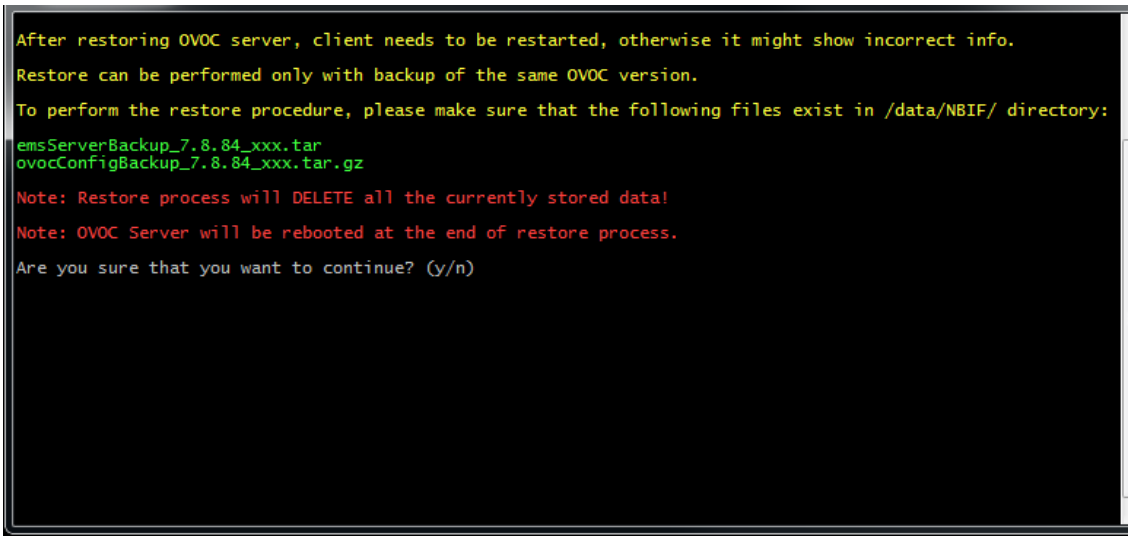
- emsServerBackup_<version>_<time&date>.tar
- ovocConfigBackup_<version>_<time&date>.tar.gz

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:**

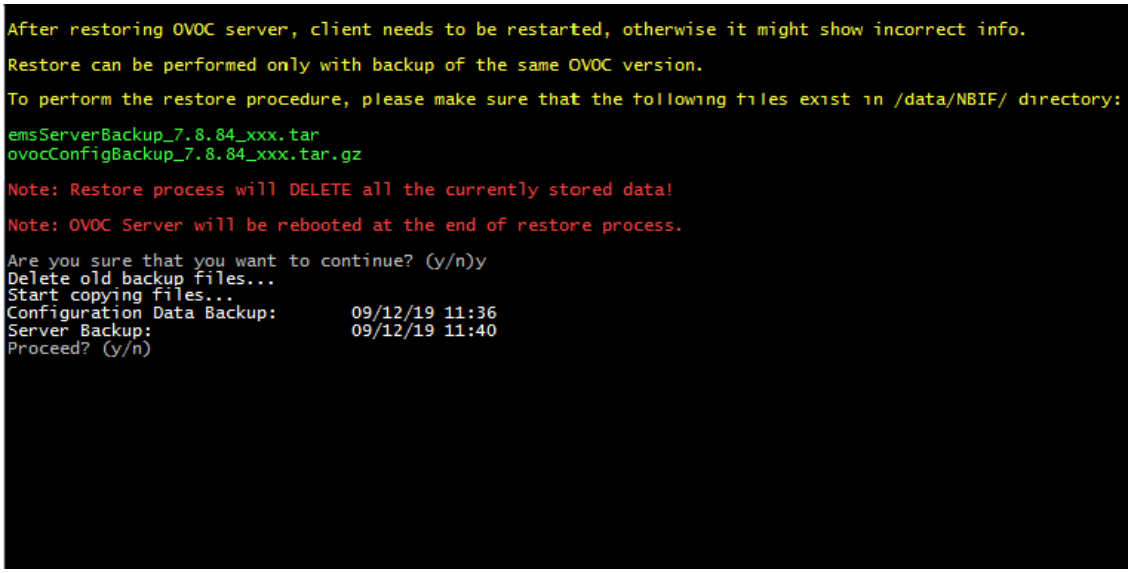
1. Select option **Configuration Restore**. A screen similar to the following is displayed:

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

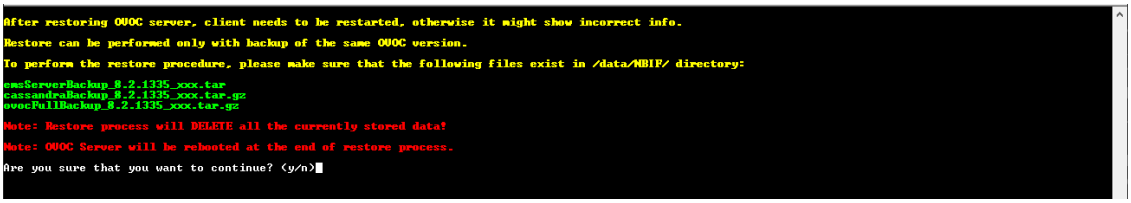
- ovocFullBackup_<version>_<time&date>.tar.gz

> 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



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).

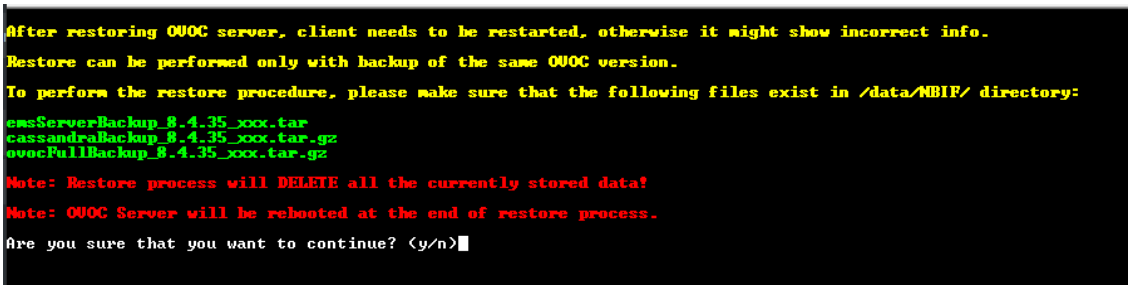
> During startup, calls older than one year are deleted. If the customer wishes to retrieve data older than one year, change the server time to the time of the backup prior to the restore.

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
```

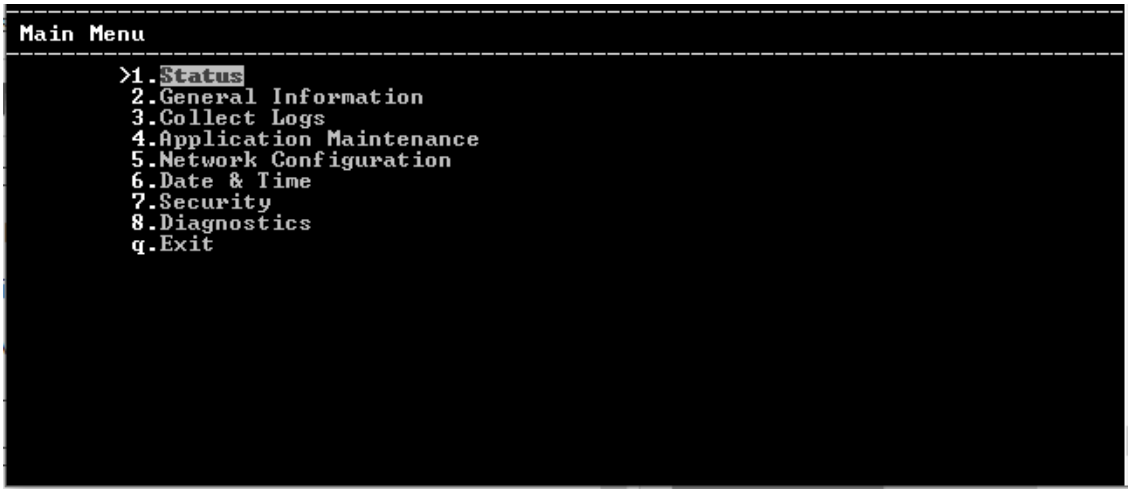
3. Type the following command:

```
# 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

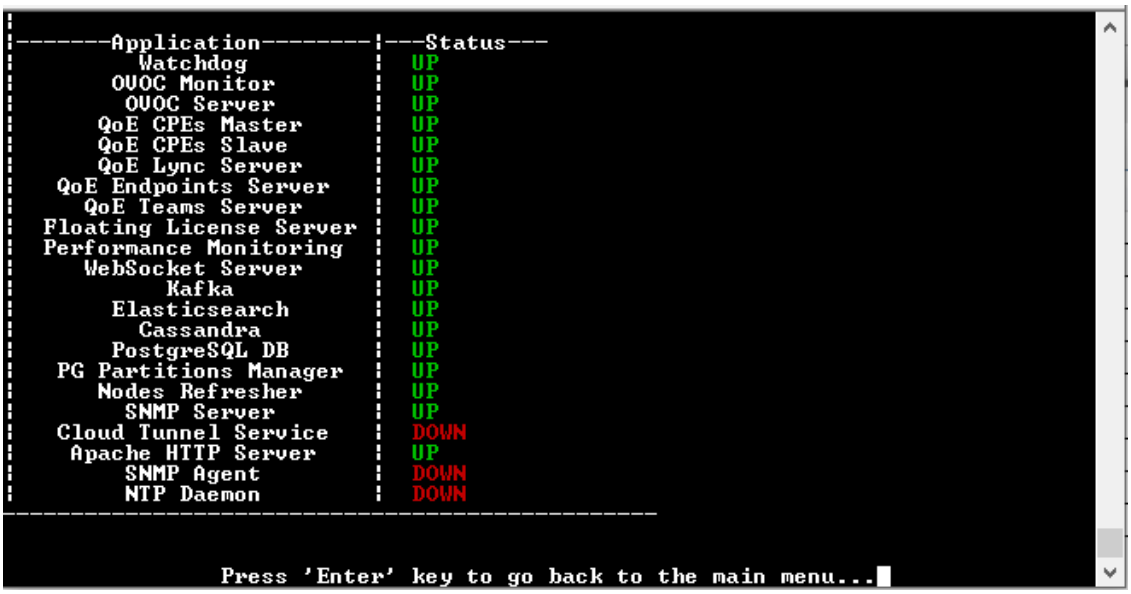
21 Viewing Process Statuses

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



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

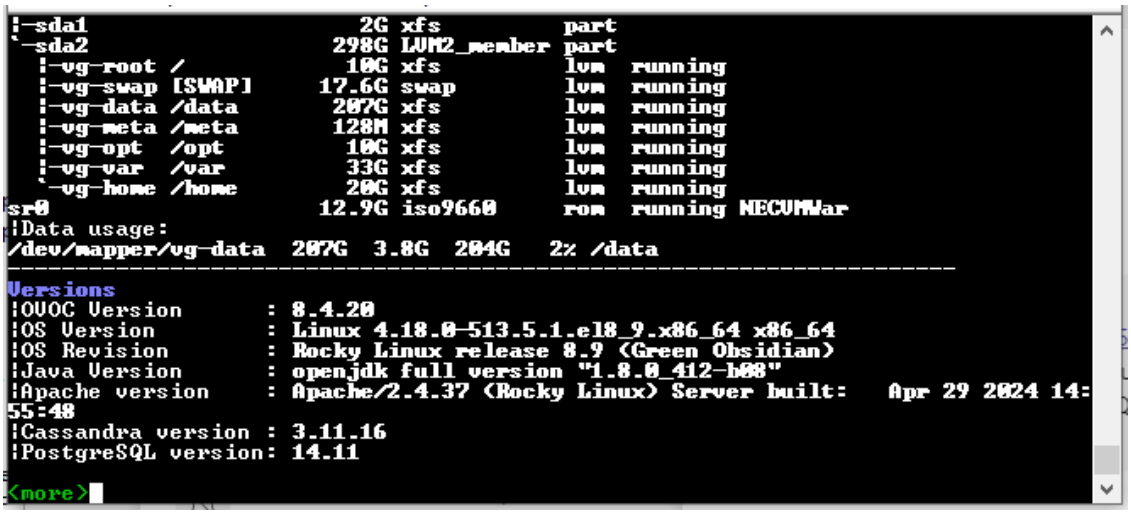
This section describes the General Information and Logs collection options. The General Information option provides detailed information about the OVOC server configuration and current status variables. The following information is provided:

- 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:

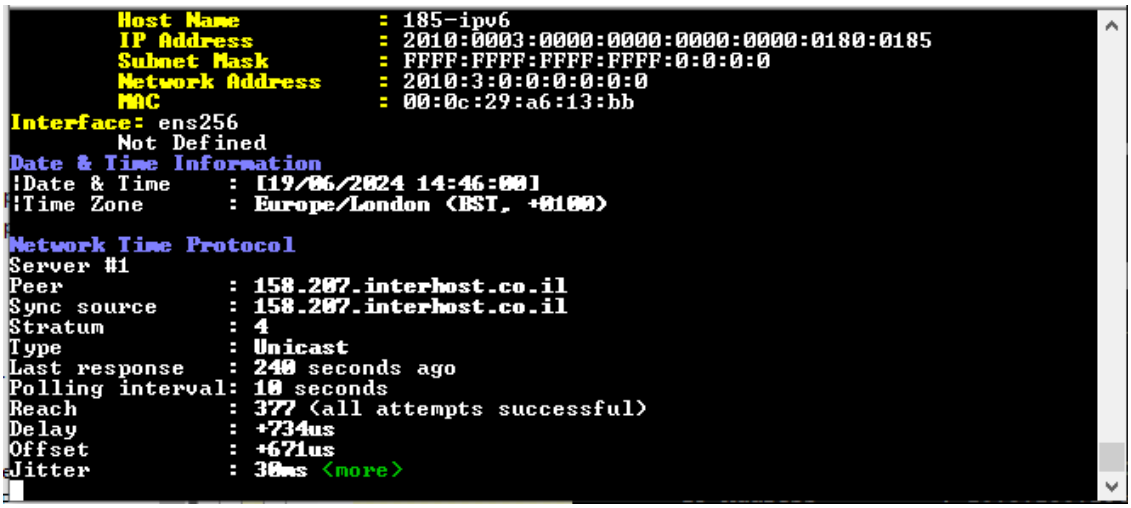
1. From the OVOC Server Manager root menu, choose **General Information**, and then press Enter.

Figure 22-1: General Information

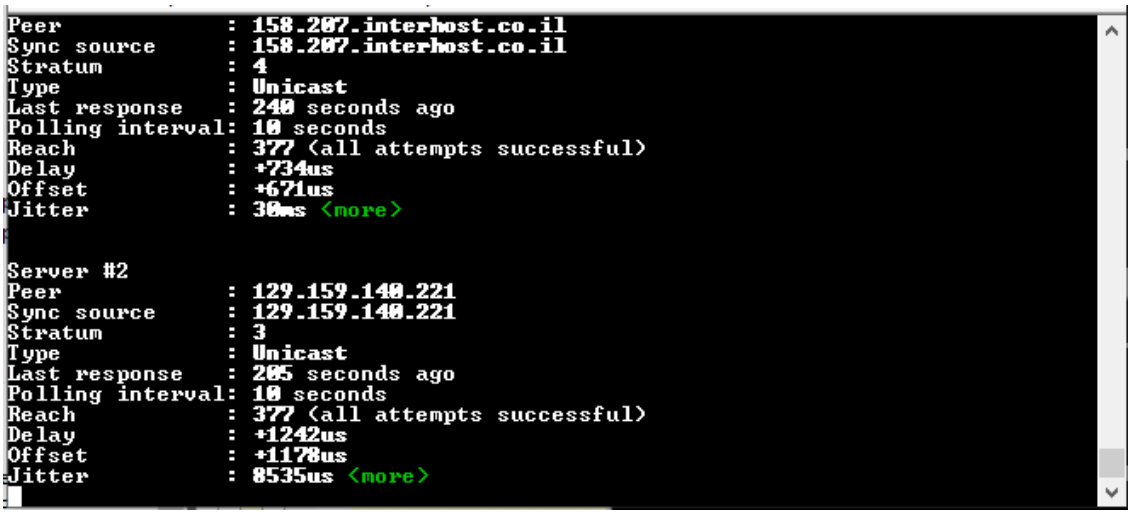


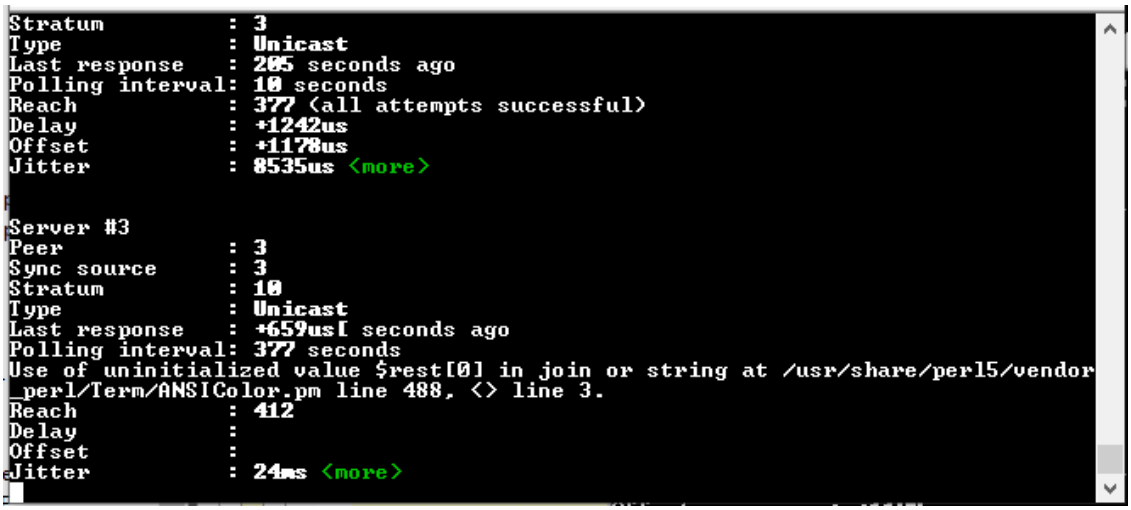
2. Press **<more>** to view more information; the following is displayed:

Figure 22-2: General Information 1



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





```
Last response    : +659us[ seconds ago
Polling interval: 377 seconds
Use of uninitialized value $rest[0] in join or string at /usr/share/perl5/vendor
_perl/Term/ANSIColor.pm line 488, <> line 3.
Reach            : 412
Delay            :
Offset           :
Jitter           : 24ms <more>


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/perl5/vendor
_perl/Term/ANSIColor.pm line 488, <> line 4.
Reach            : 68
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/perl5/vendor
_perl/Term/ANSIColor.pm line 488, <> line 4.
Reach            : 68
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/perl5/vendor
_perl/Term/ANSIColor.pm line 488, <> line 5.
Reach            : +6573us[+6573us]
Delay            :
Offset           :
Jitter           : 4 <more>
```

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.

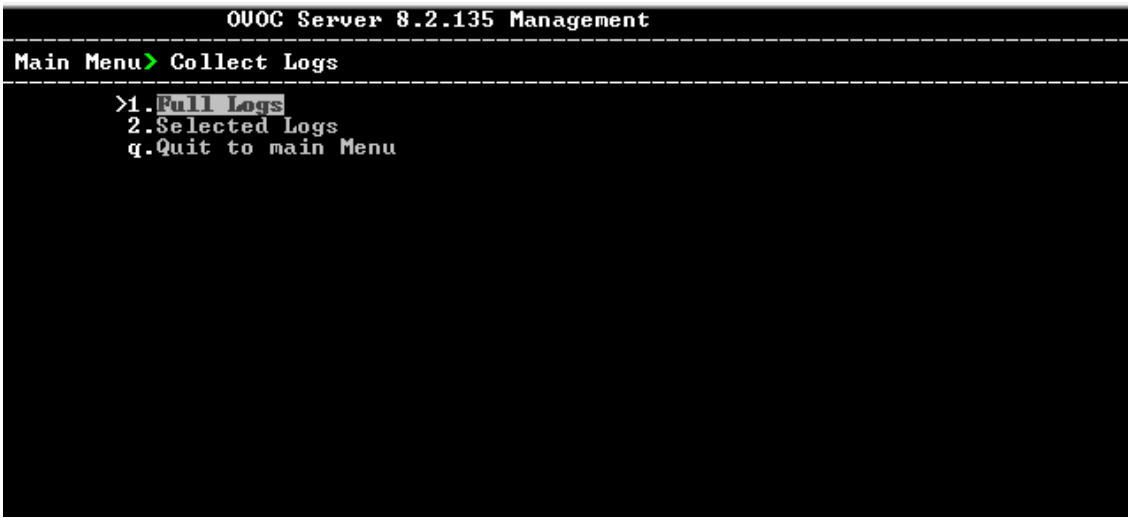
The following log files are collected:

- 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:**

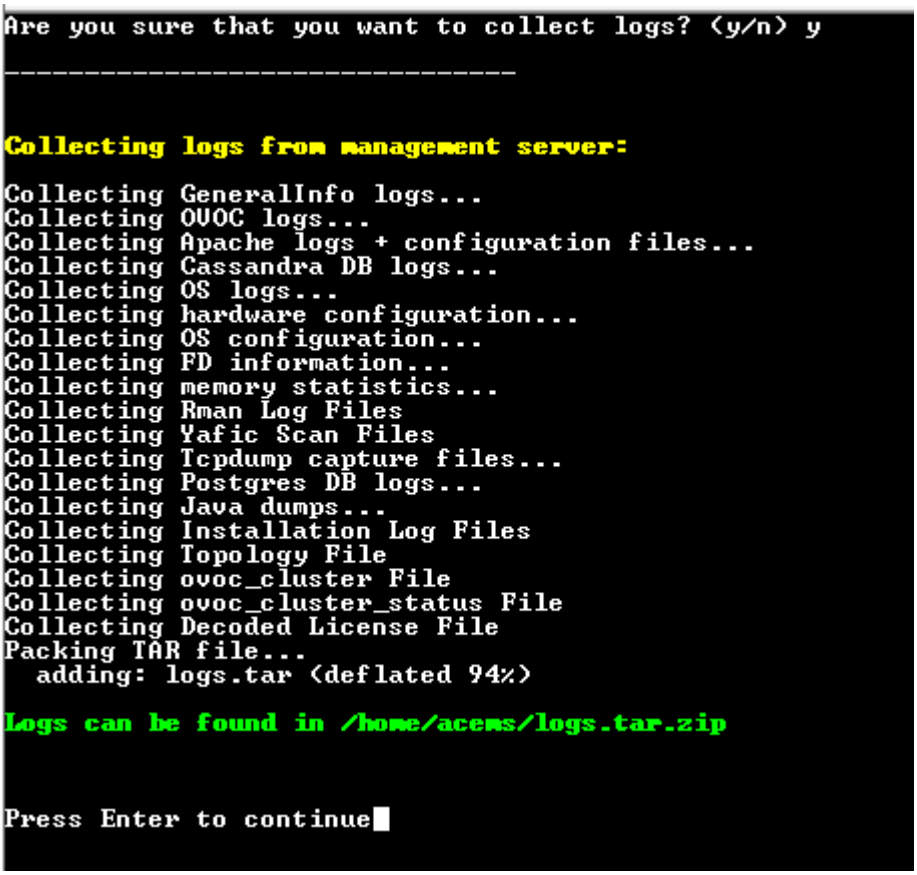
1. From the OVOC server Management root menu, choose **Collect Logs**, and then press Enter.

Figure 23-1: Collect Logs



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.

Figure 23-2: Collecting Logs

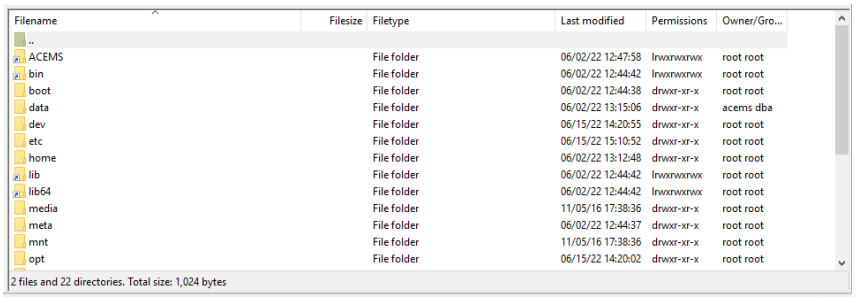
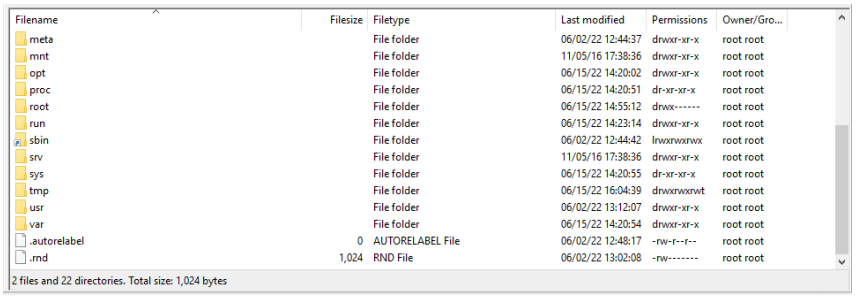
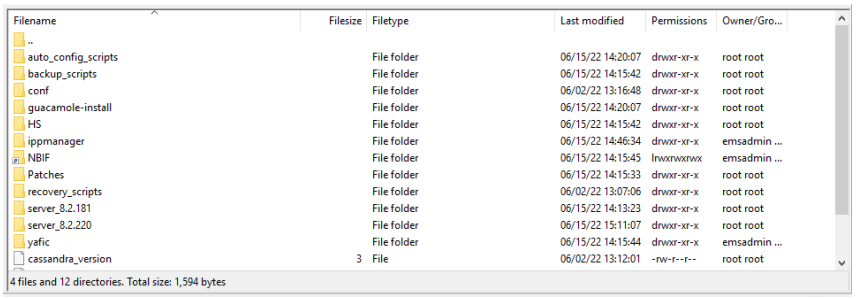


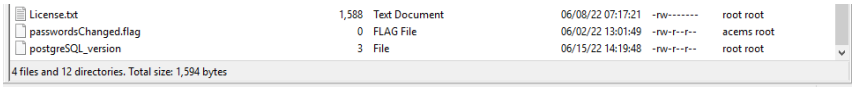
Selected Logs

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.

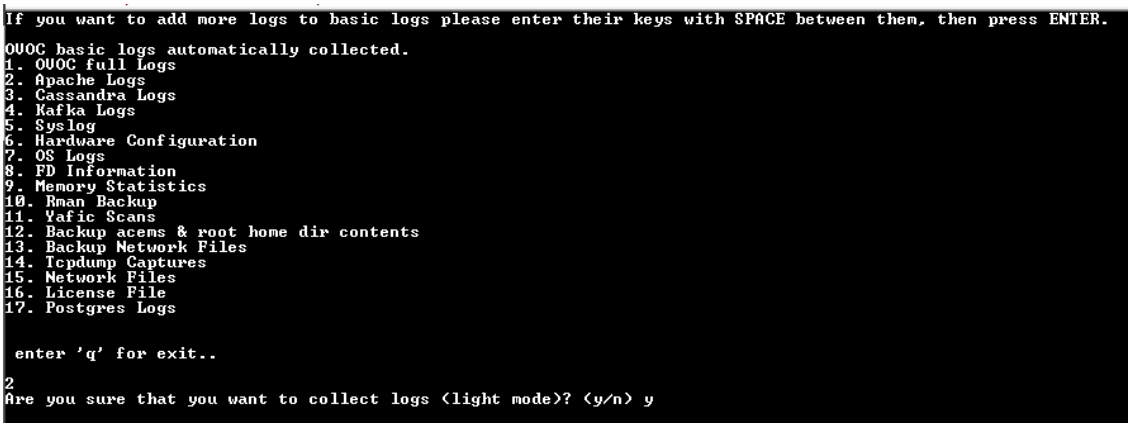
Log Type	Description
Kafka Logs	Kafka logs for managing alarms retrieved from the VQM and PM servers.
Syslog	Operating system syslog files (see also Diagnostics on page 282).
Hardware Configuration	OS dmidecode output.
FD Information	OS File Descriptors summary.
Memory Statistics	OS Memory information.
Yafic Scans	OS Yafic scan results.
acems & Root dirt contents	Output of the contents of all folders under "root" and "acems" directory root directory contents:   acems directory contents: 

Log Type	Description
	
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.

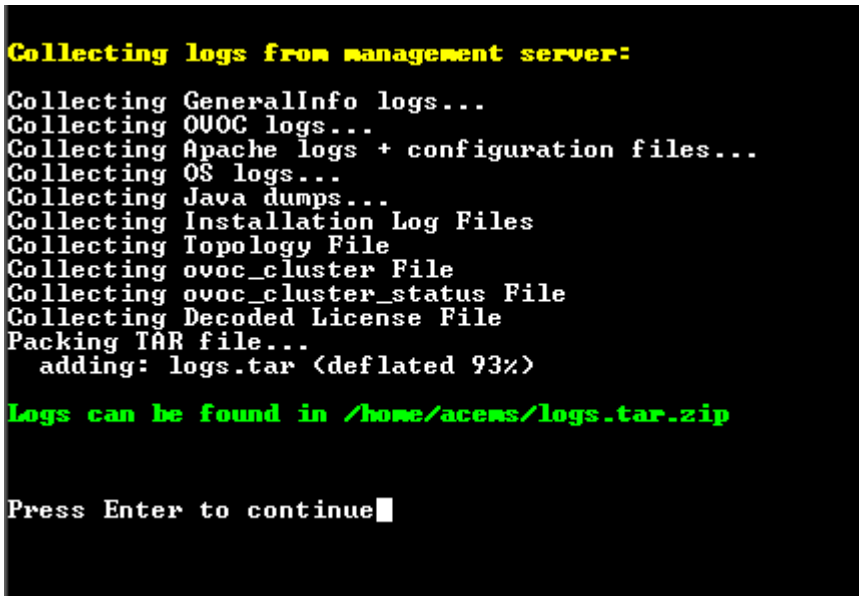
Figure 23-3: Select Logs



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.

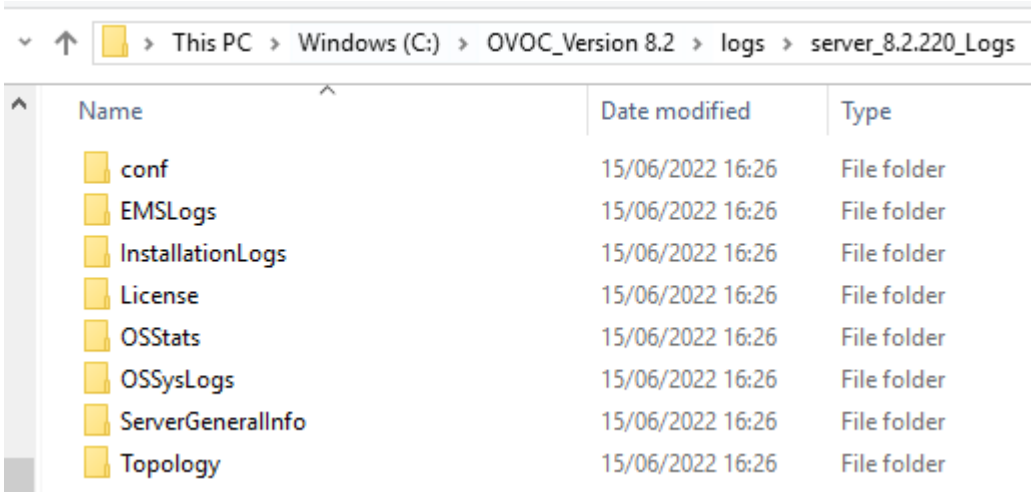
Figure 23-4: Log Directory



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:

Figure 23-5: OVOC "Full Logs"



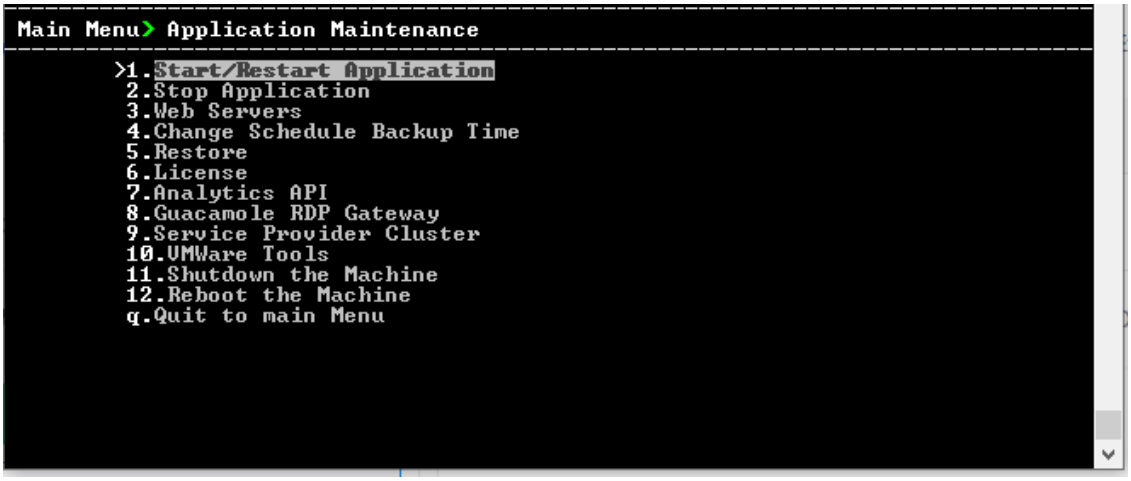
24 Application Maintenance

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**.

Figure 24-1: 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

3. Type **1** to stop the OVOC server.

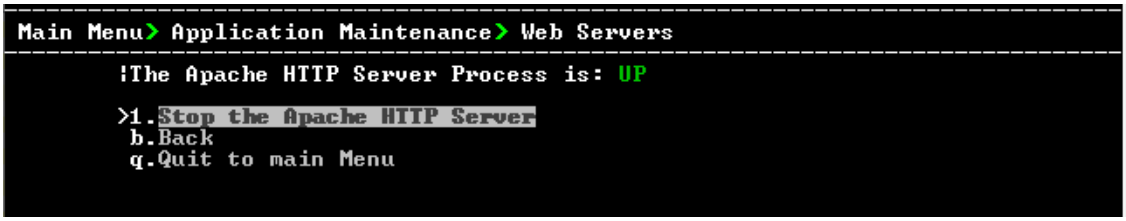
Web Servers

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



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 htttp://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:

Figure 24-5: License Manager

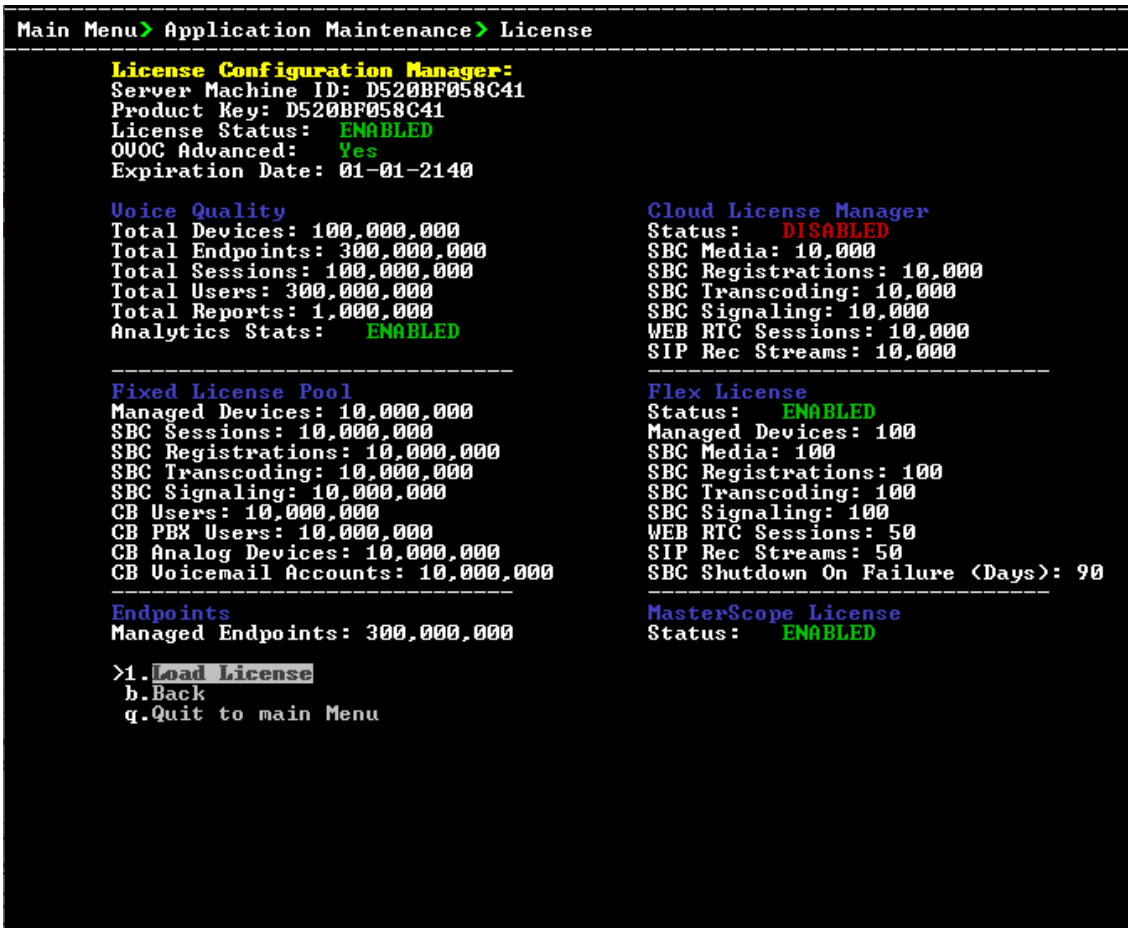


Table 24-1: License Pool Parameters

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 Manager	
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 Pool	
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.

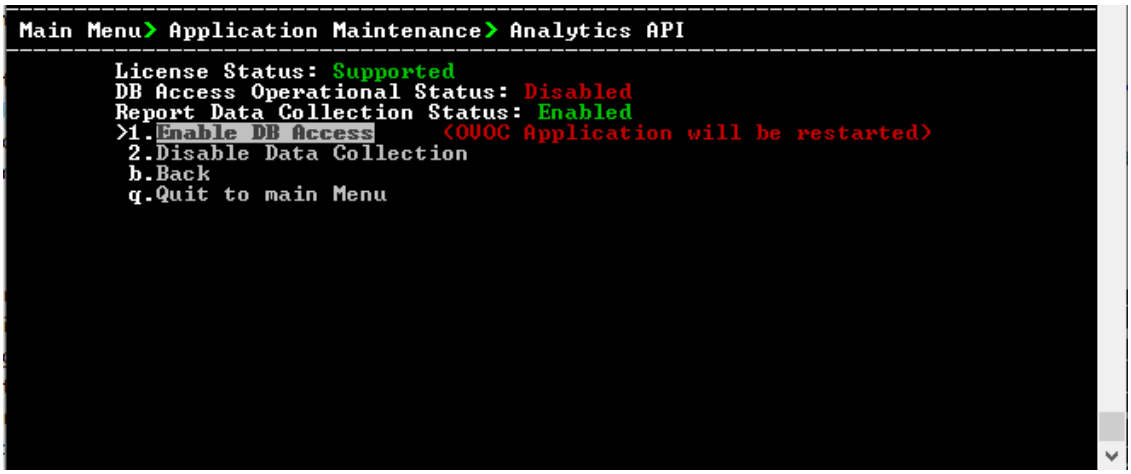
For more information, refer to OVOC Northbound Integration Guide.

➢ **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.

Figure 24-6: analytics API



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.

> The connector PostgreSQL driver must be used.

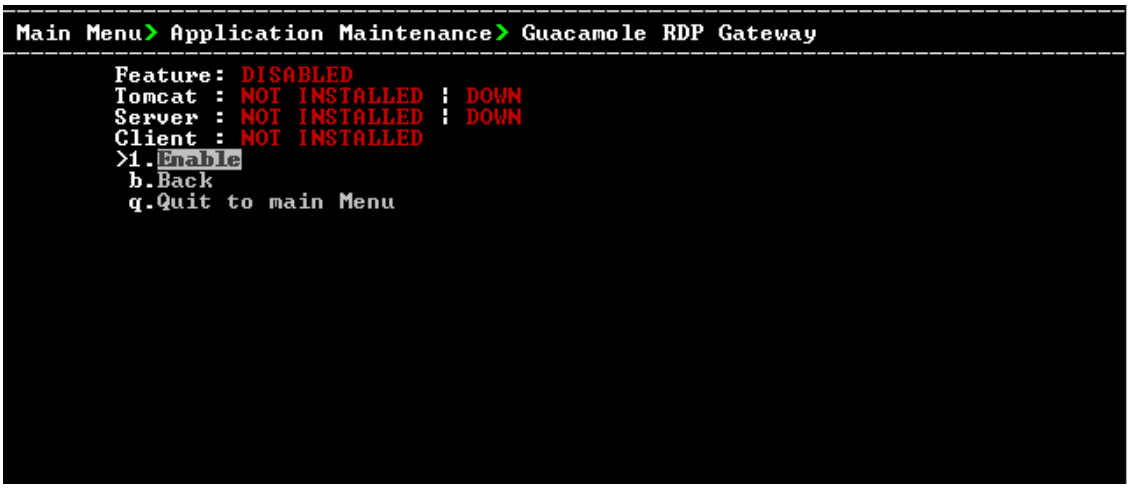
Guacamole RDP Gateway

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.

Figure 24-8: Building and Installing RDP Gateway

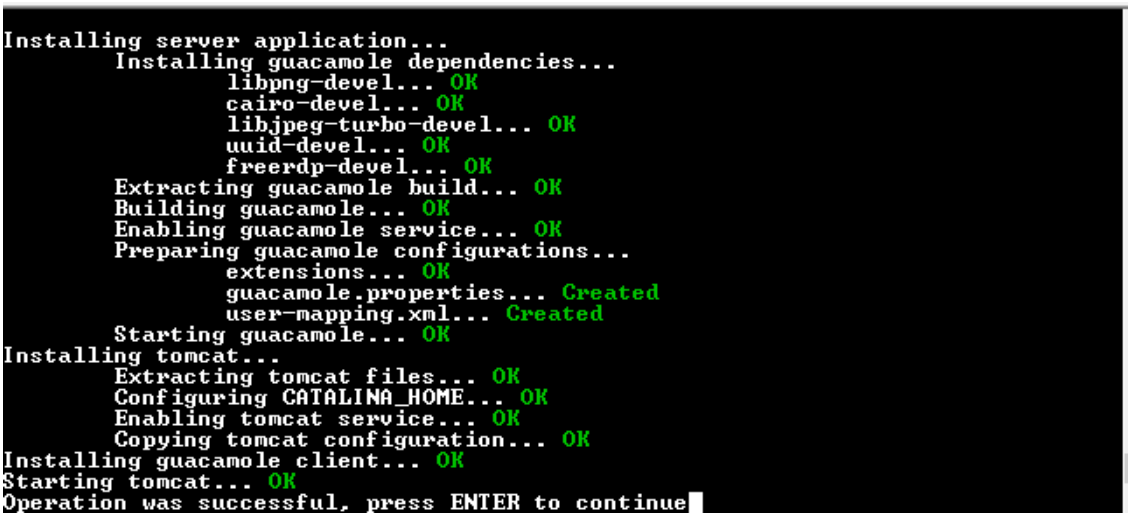
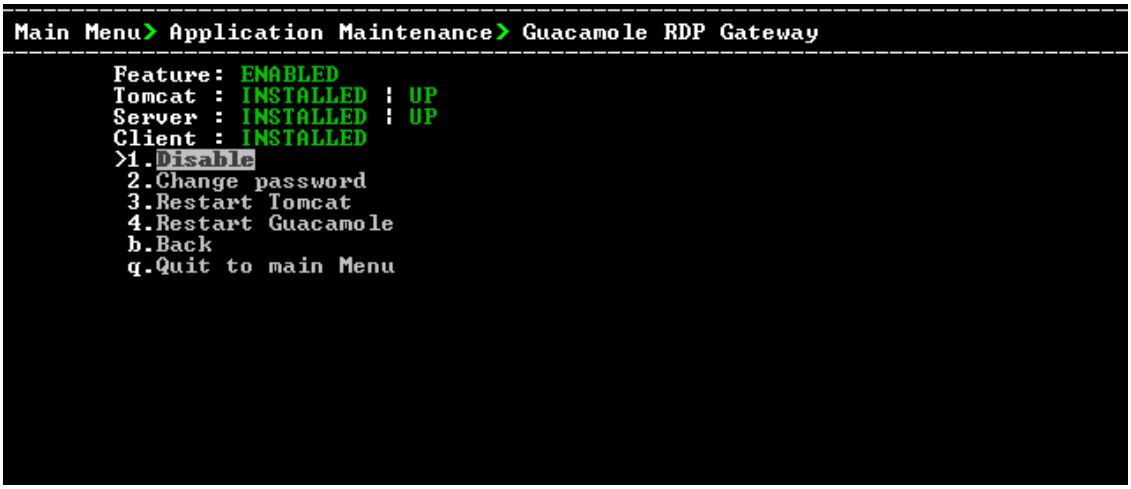


Figure 24-9: Enabled Guacamole RDP Gateway



3. Do one of the following:

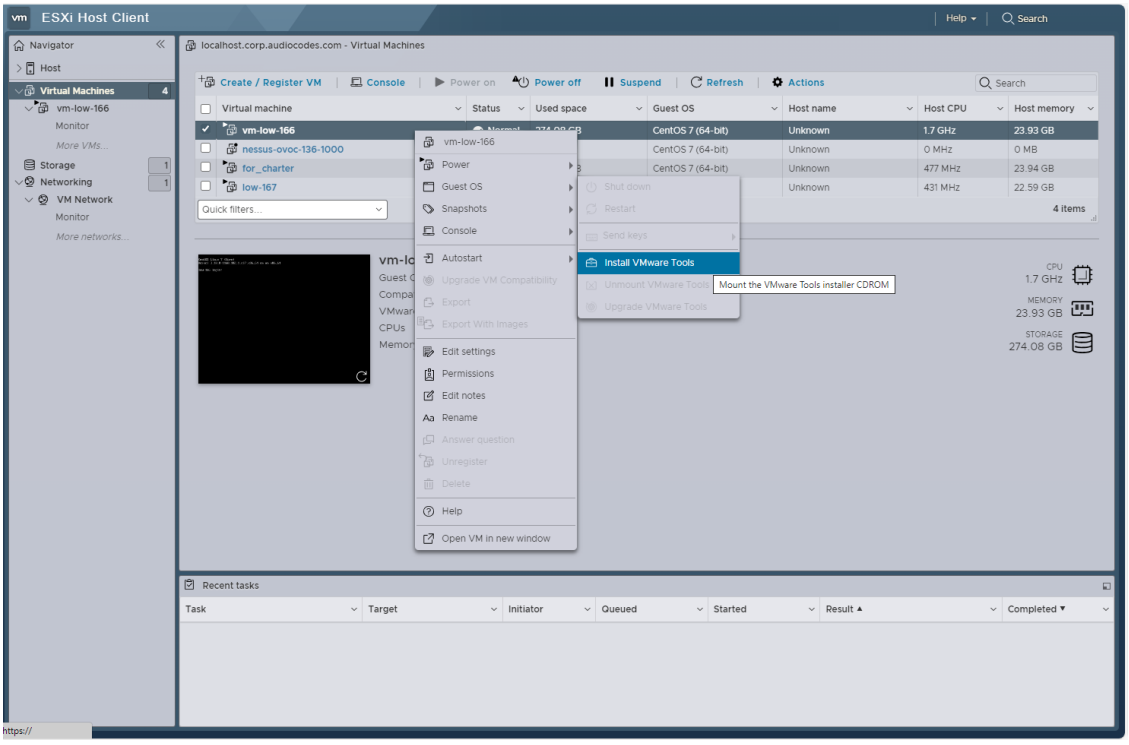
- **Change password:** Select Option **2**, enter the current password, enter new password and confirm (default username *umpman*, default password: *umppass*)
- **Restart Tomcat:** Select Option **3** and confirm.
- **Restart Guacomole:** Select Option **4** and confirm.

VMware Tools

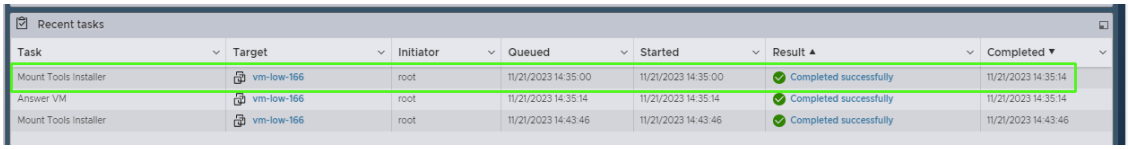
This option installs VMware Tools on the OVOC Server file system. This feature requires the pre-mounting of the VMware installer CD-ROM on the Host machine. OVOC Server verifies the existence of the Tools package and then mounts the tool to OVOC Server file system.

➢ To install VMware tools:

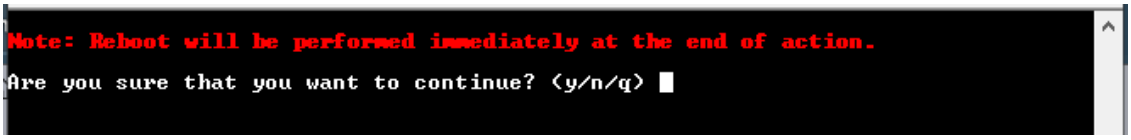
1. On the VMware Host machine, select the relevant OVOC Virtual Machine.
2. Select the Right-click menu, choose **Guest OS** > **Install VMware Tools**.



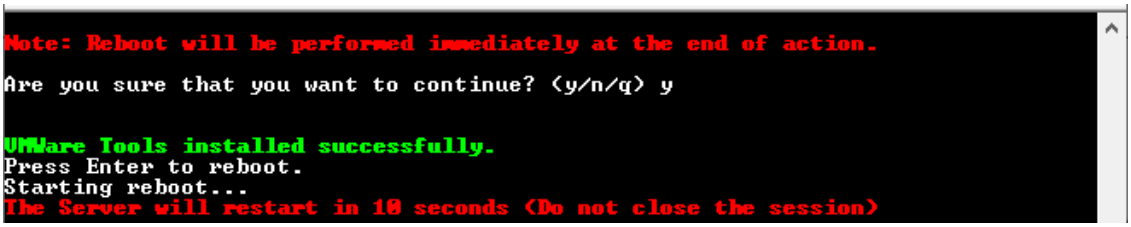
The Completed Successfully indication is displayed in the Task pane:



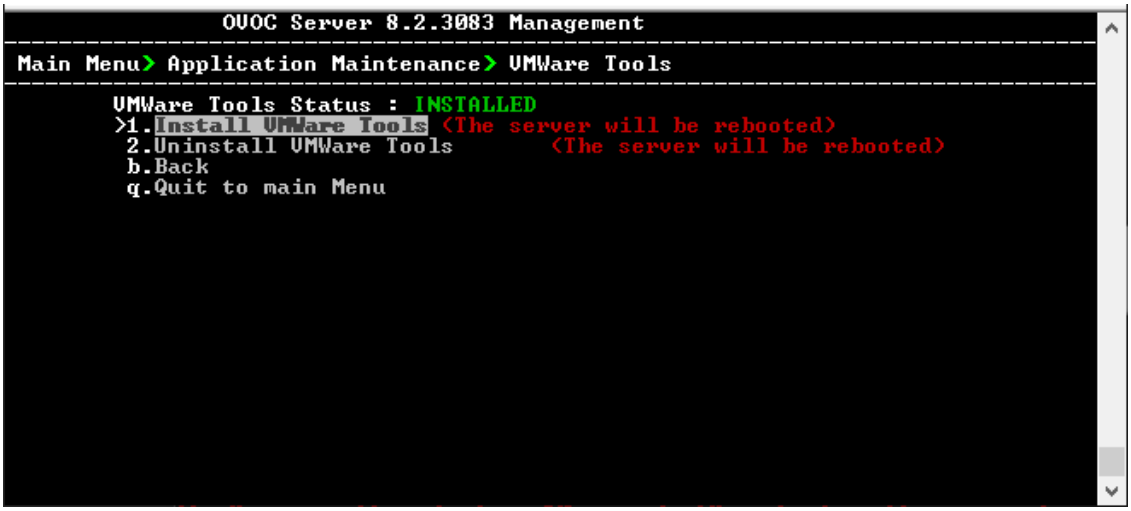
3. Open Server Manager Application Maintenance menu, choose **VMware Tools**, and then press Enter.



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.

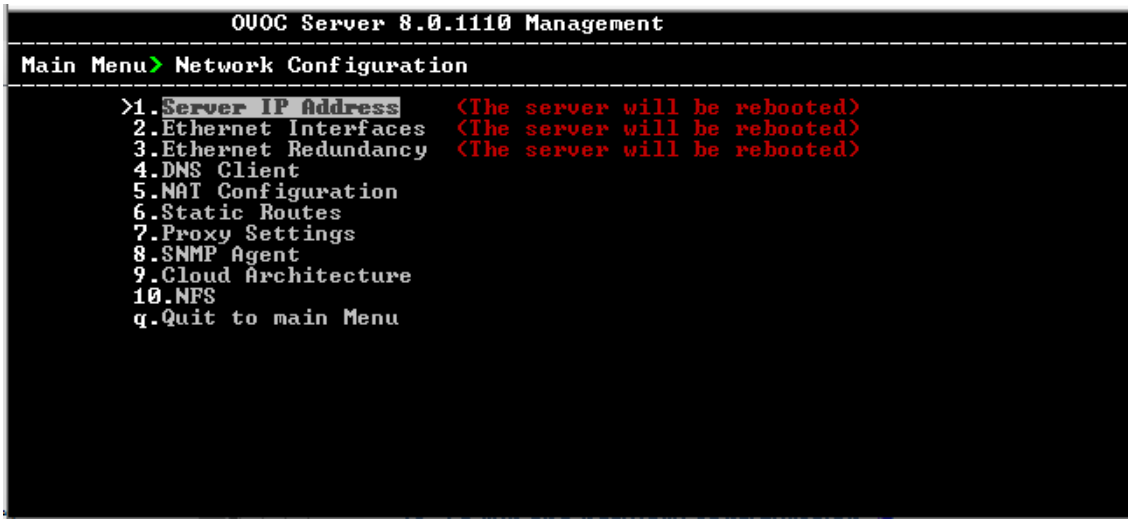
25 Network Configuration

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



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

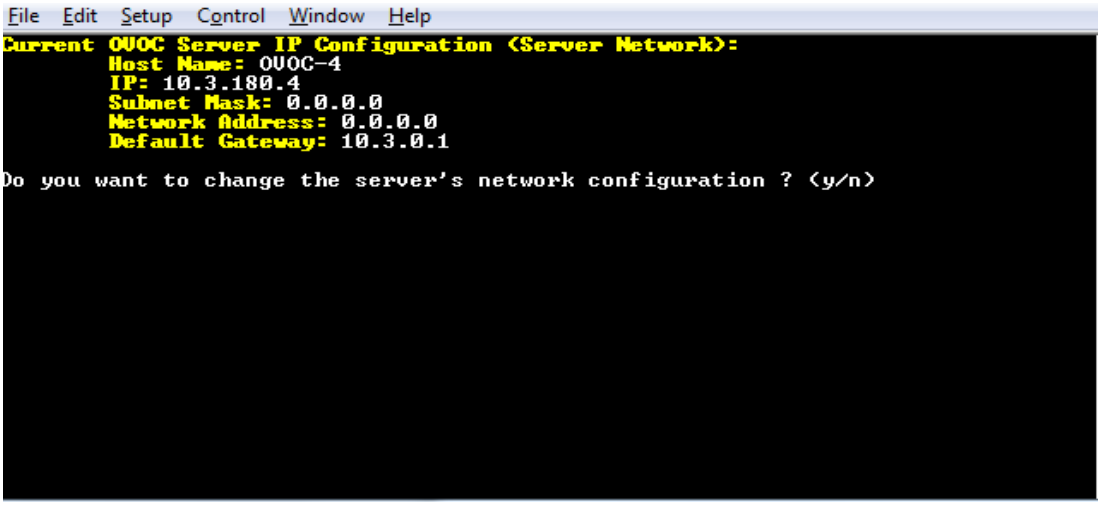
This option enables you to update the OVOC server's IP address. This option also enables you to modify the OVOC server host name.

- 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

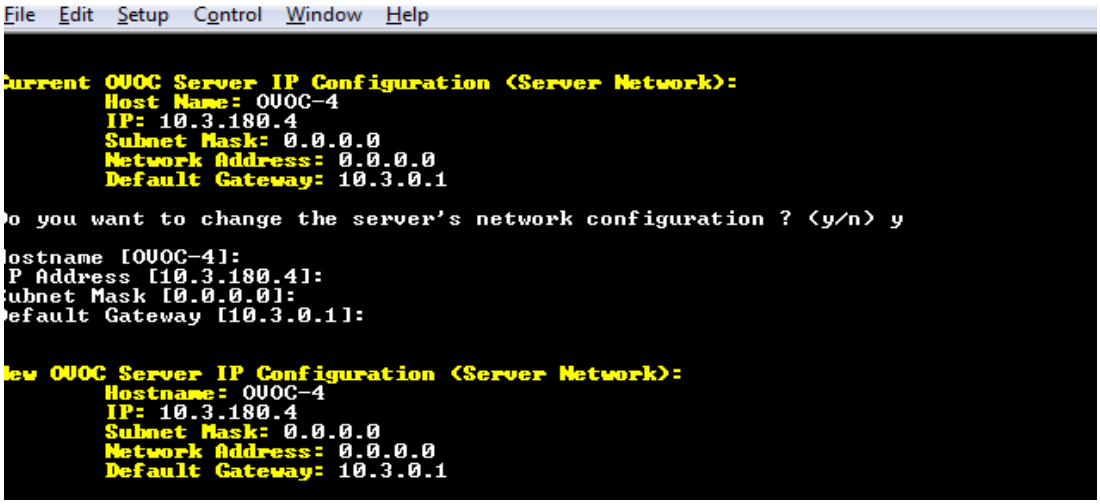


2. Configure IP configuration parameters as desired.

   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.

Figure 25-3: IP Configuration Complete



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.

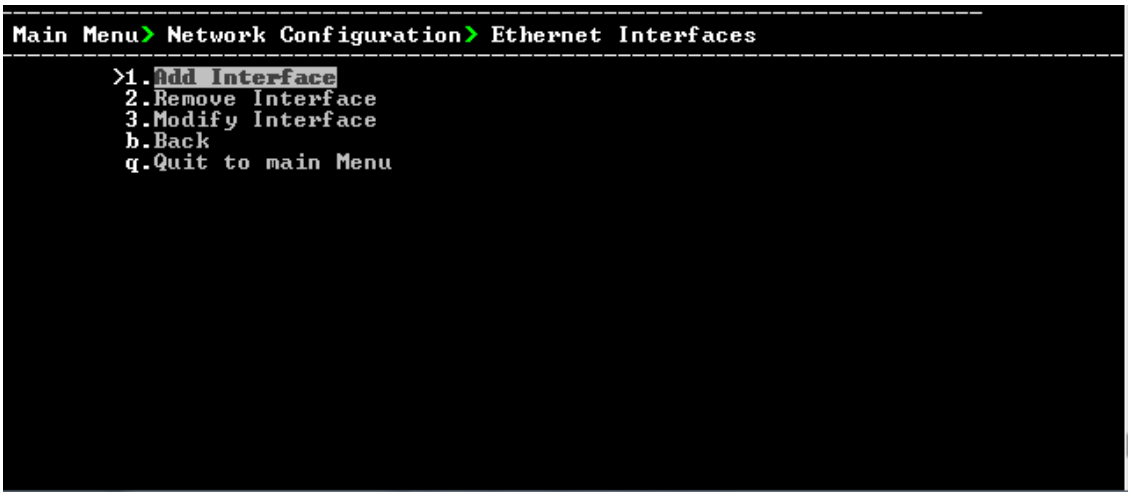
- The OVOC Main Management interface only supports IPv4.
- Each IPv4 interface can be configured for NAT and one of the IPv4 interfaces can be configured to work in the Cloud Architecture mode.

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, 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).

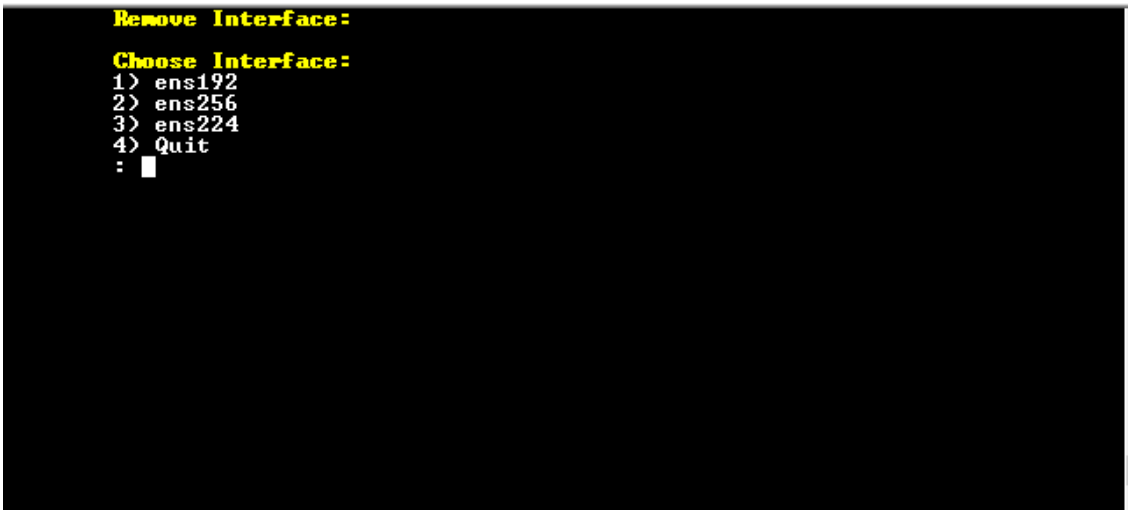
Remove Interface

This section describes how to remove an Ethernet Interface.

➢ **To remove an existing interface:**

1. From the Ethernet Interfaces menu, choose option **2**.

Figure 25-5: Remove Ethernet Interface



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.

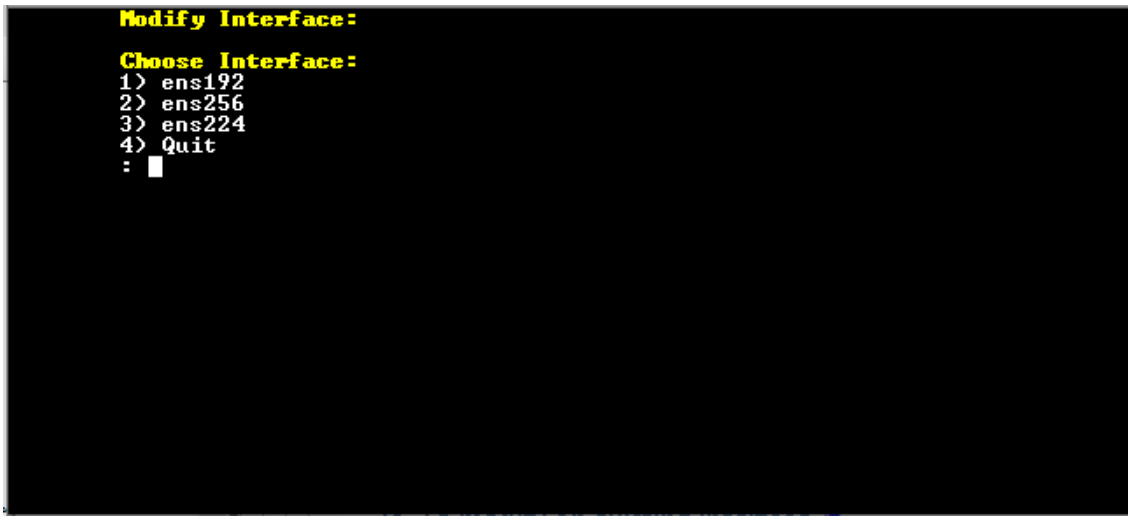
Modify Interface

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

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.

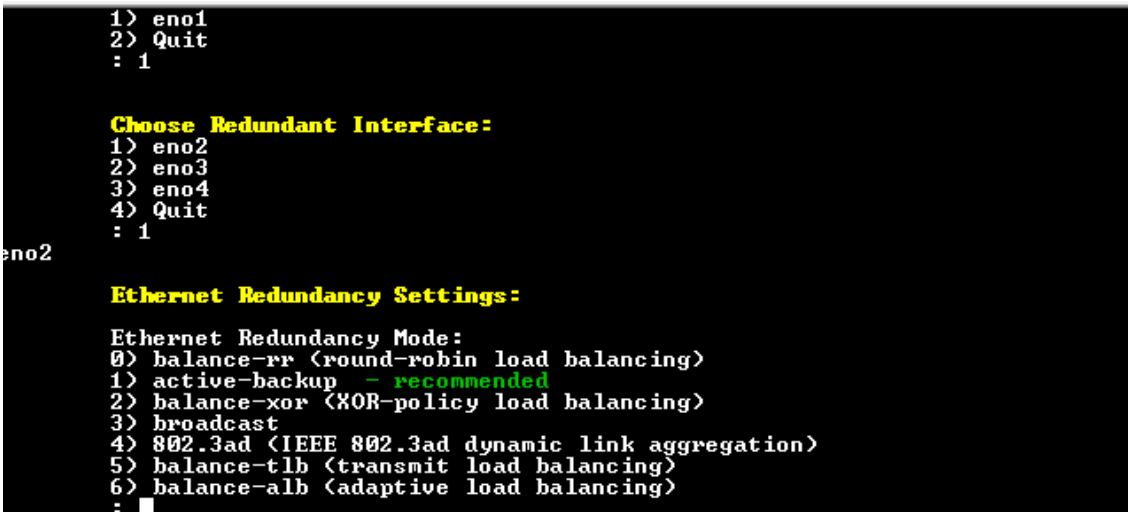
➢ **To add a redundant interface:**

1. From the Ethernet Redundancy menu, choose option **1**, and then press Enter.

Figure 25-8: Add Redundant Interface

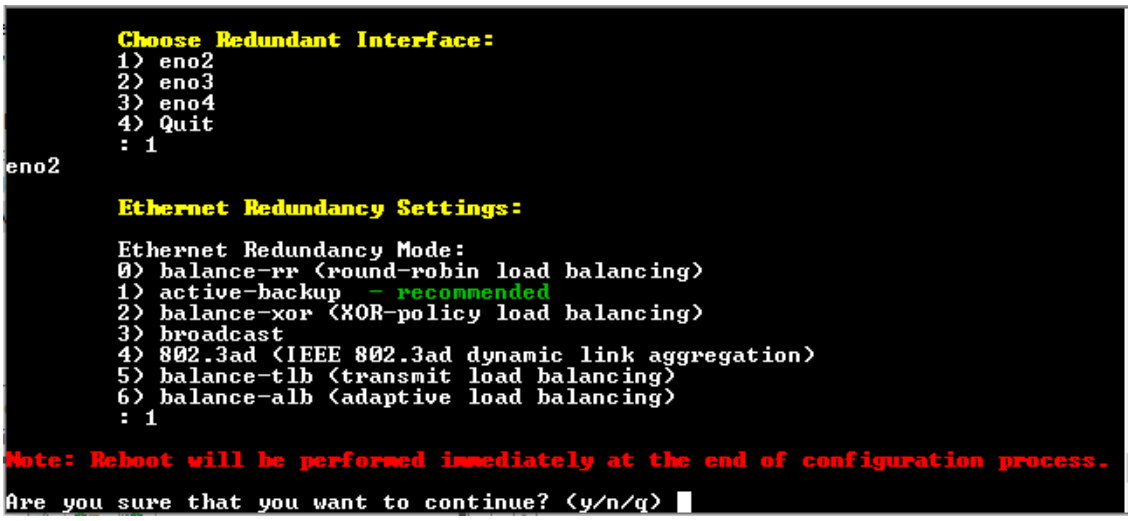
2. Choose the Master Interface for which to create a new redundant interface (for example, 'OVOC Client-Server Network'), and then press Enter.

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.

Figure 25-10: Confirm Ethernet Redundancy Update



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

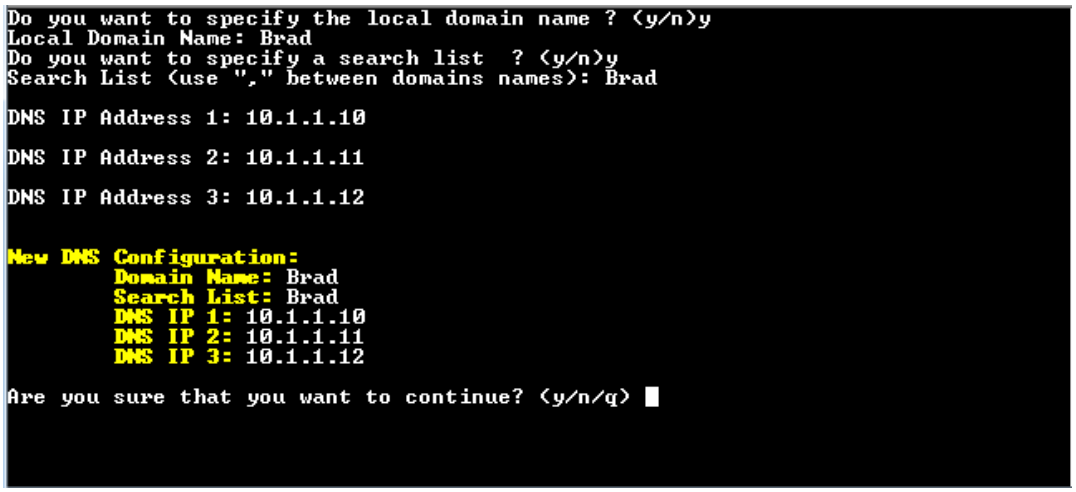
Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

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.

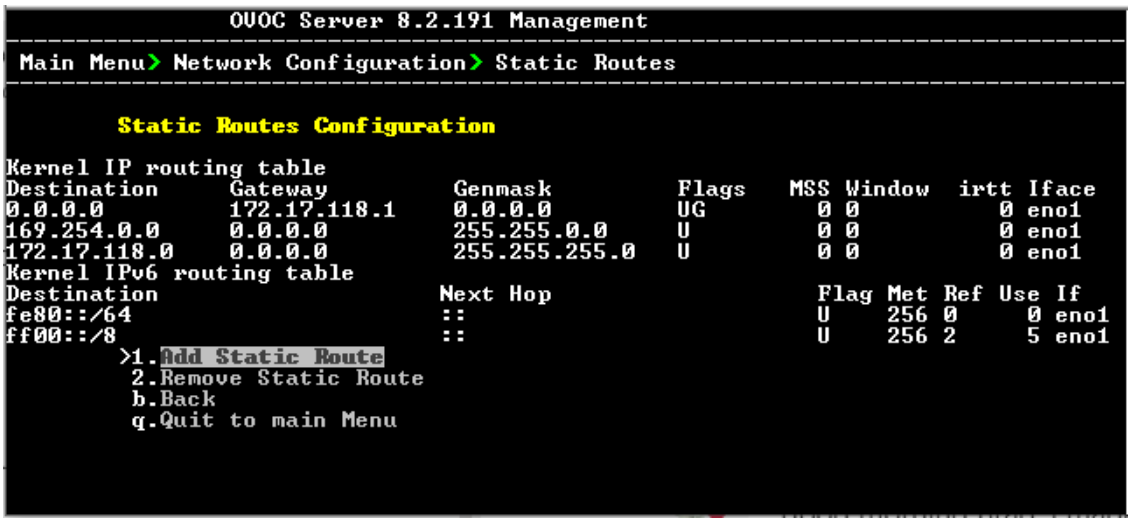
Static Routes

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.

Figure 25-12: Routing Table and Menu

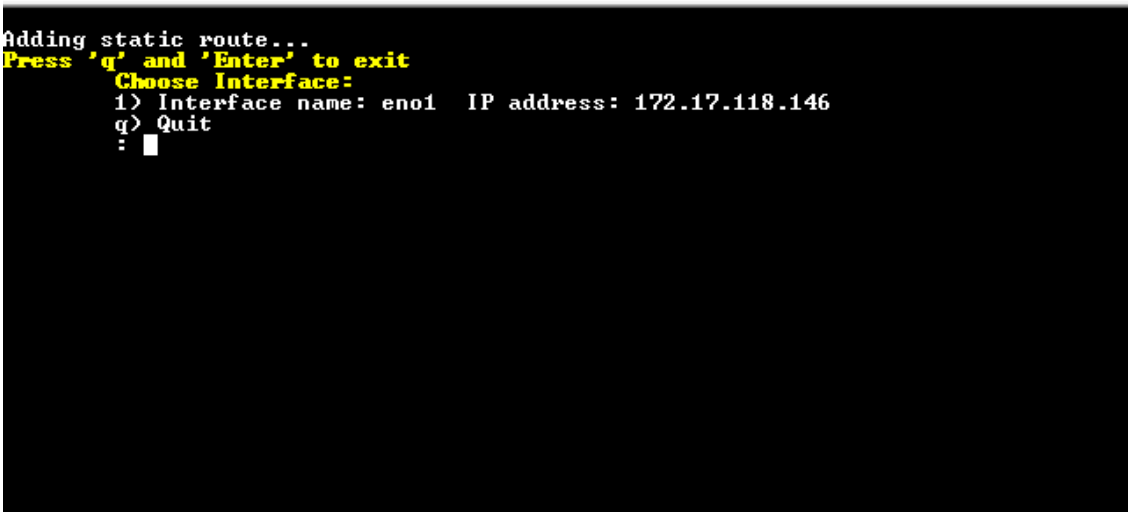


2. From the Static Routes configuration screen, choose one of the following options:
   - Add a Static Route
   - Remove a Static Route

➢ **To add a static route:**

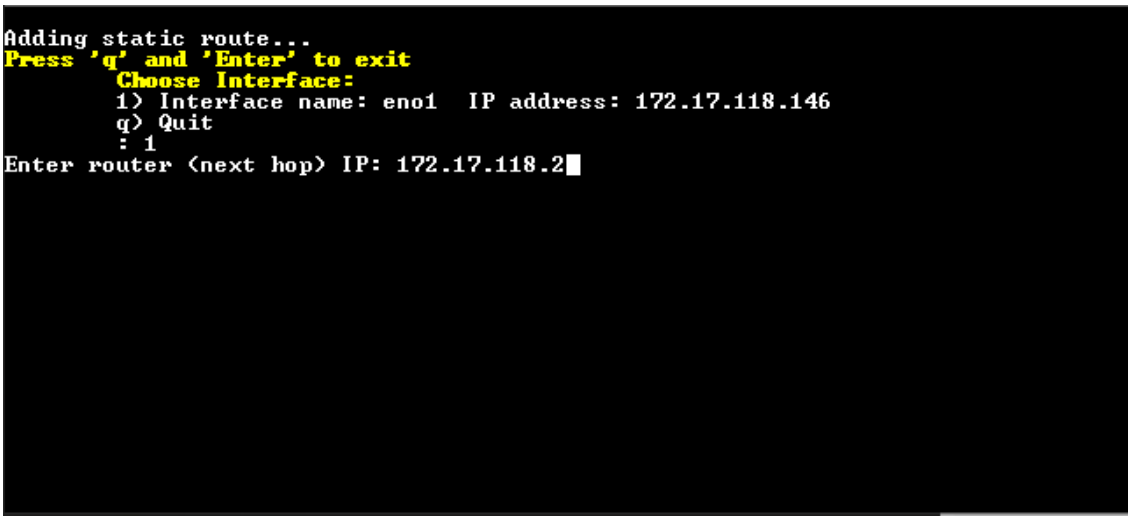
1. From the Static Routes menu, choose option **1**, and then press Enter.

Figure 25-13: Select Interface



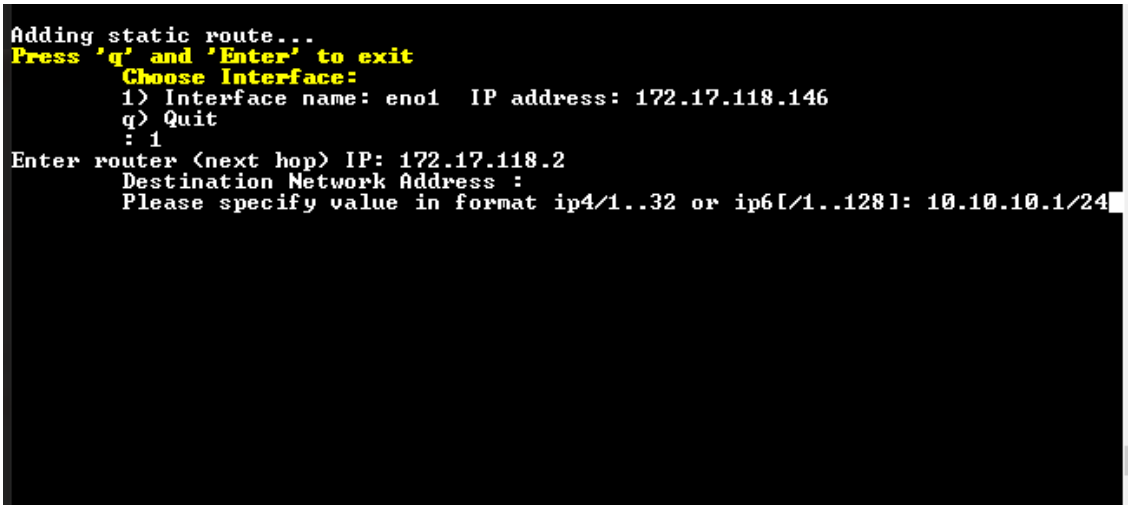
2. Enter the number corresponding to the desired interface, and then press Enter.

Figure 25-14: Enter Router (next hop)



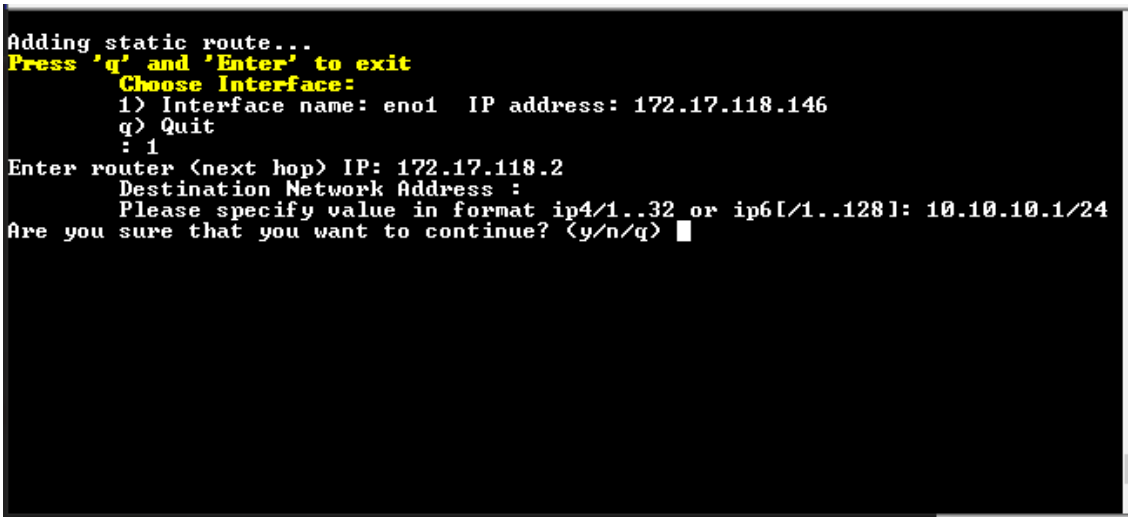
3. Enter the Router IP address, and then press Enter.

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

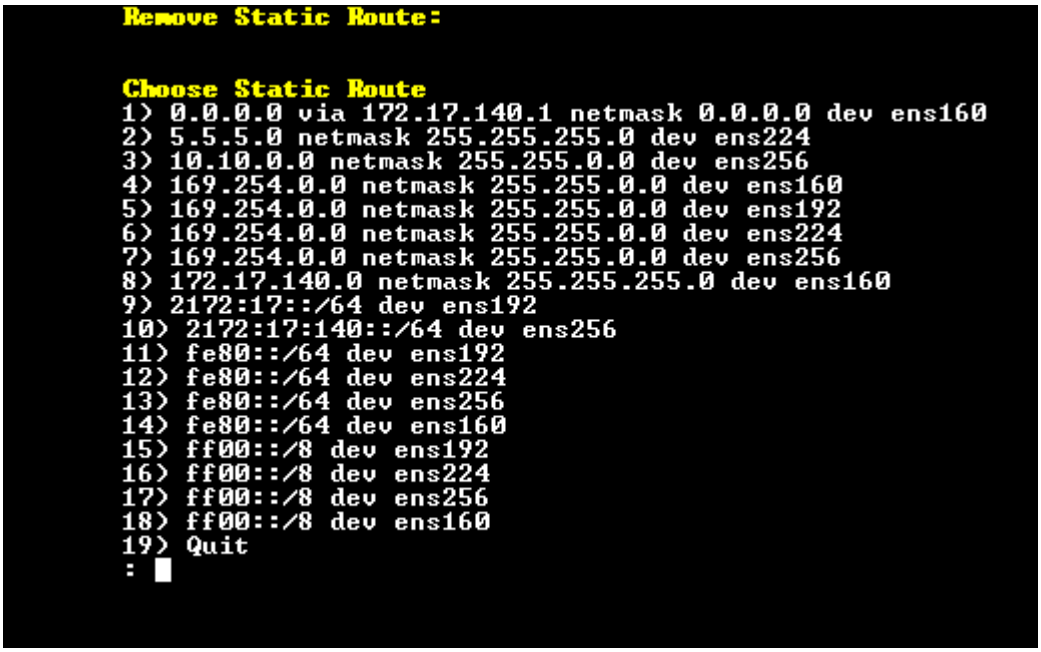


5. Enter **y** to confirm the new IP address, and then press Enter.

➢ **To remove a static route:**

1. From the Static Routes menu, choose option **2**, and then press Enter.

Figure 25-17: Remove Static Route



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.

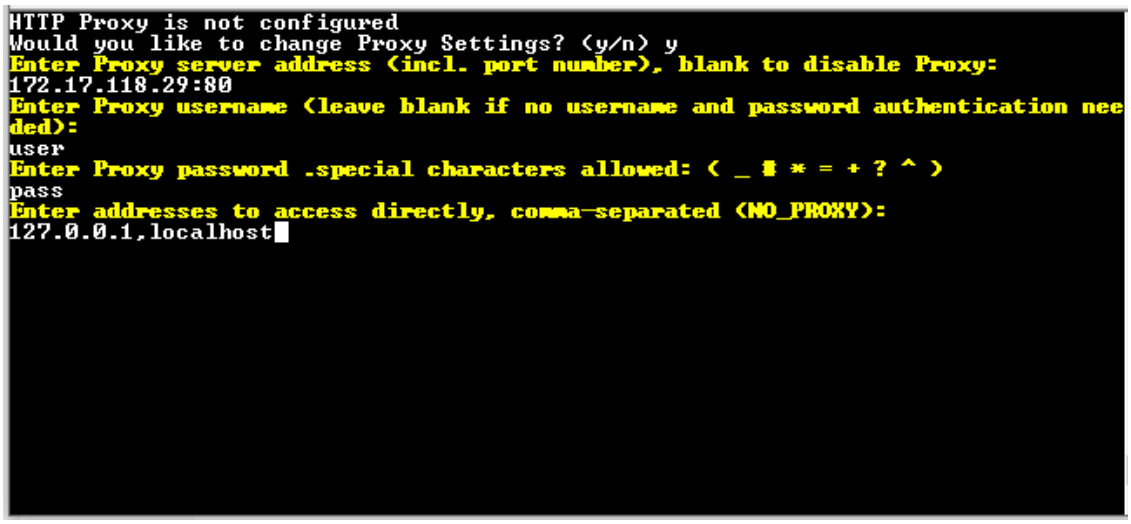
➢ **To configure proxy settings:**

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

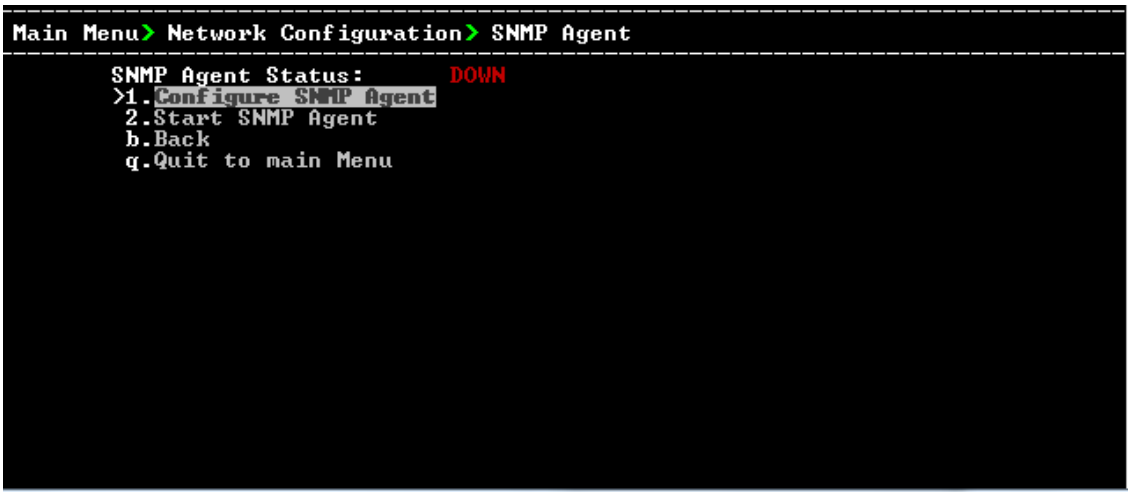
The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP). This agent serves OVOC, NMS, or higher-level management system synchronization. This menu includes the 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



The SNMP Agent status is displayed.

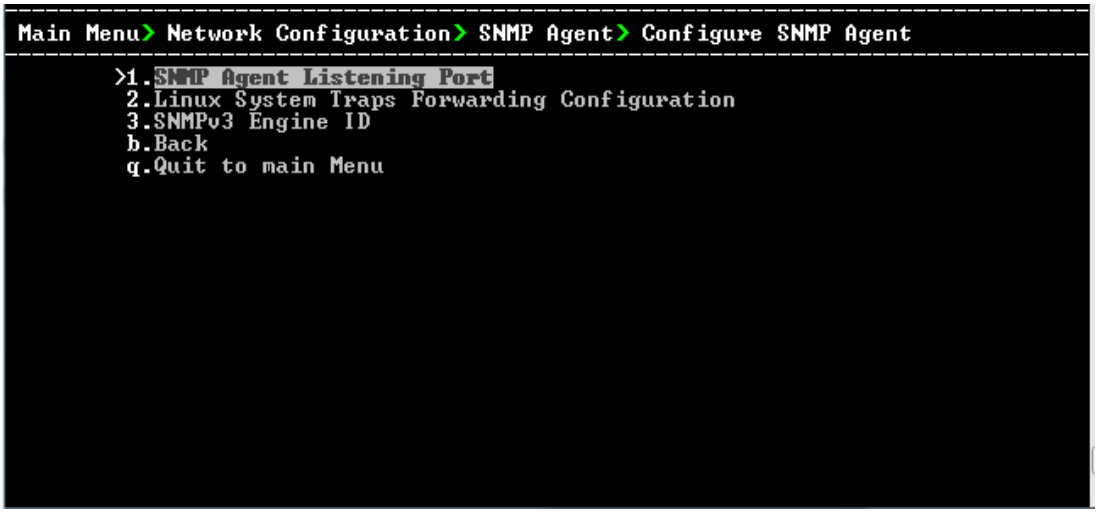
➢ **To start the SNMP Agent:**

- Choose option **2**

➢ **To configure SNMP Agent:**

1. Choose option **1**, and then press Enter.

Figure 25-20: Configure SNMP Agent



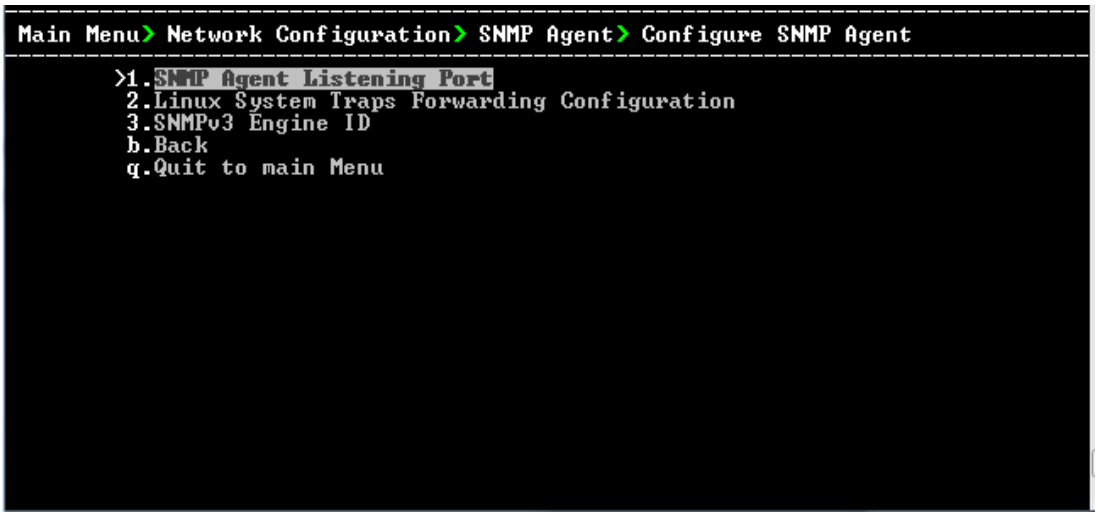
SNMP Agent Listening Port

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.

Figure 25-21: SNMP Agent Listening Port



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.

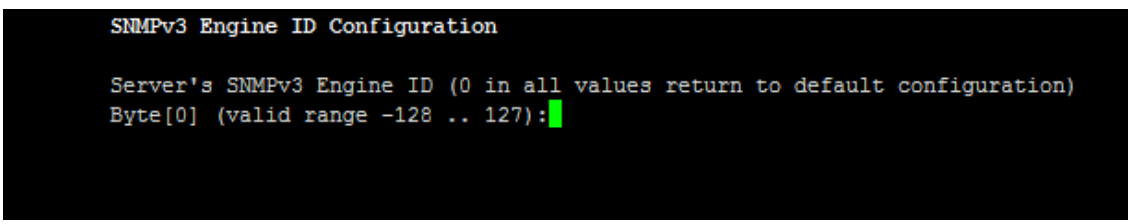
Server SNMPv3 Engine ID

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:**

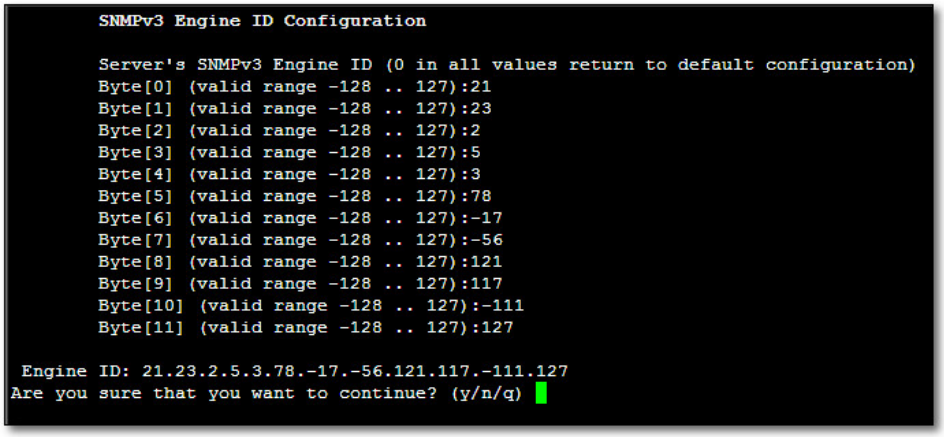
1. From the Network Configuration menu, choose **SNMPv3 Engine ID**, and then press Enter.

Figure 25-22: OVOC Server Manager – Configure SNMPv3 Engine ID



2. 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.

Figure 25-23: SNMPv3 Engine ID Configuration – Complete Configuration



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.

Figure 25-24: Network File System (NFS)

2. Select **Enable NFS Utils**, and then press Enter. You are prompted to enable the package, enter **Y**, and then press Enter.

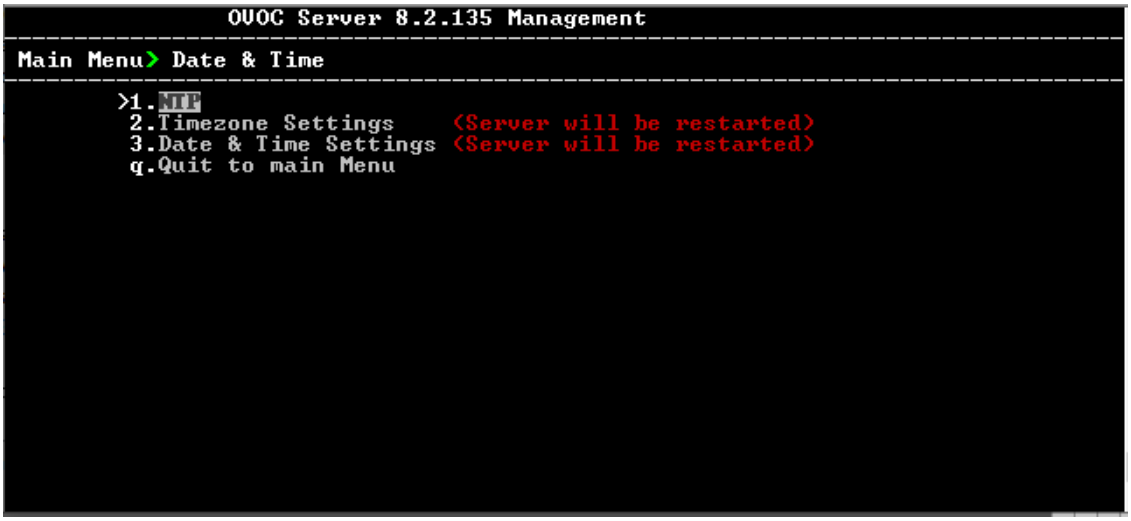
26 NTP & Clock Settings

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.

Figure 26-1: Date & Time Settings



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:

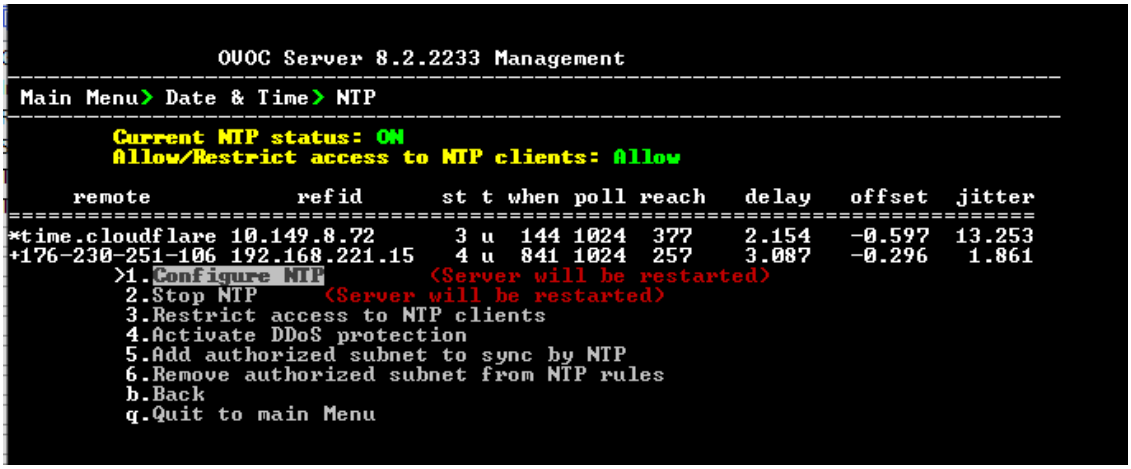
- Configure the OVOC server to obtain its clock from an external NTP clock source. Other devices that are connected to the OVOC server in the IP network can synchronize with this clock source. These devices may be any device containing an NTP server or client.
- Configure the OVOC server as the NTP server 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:

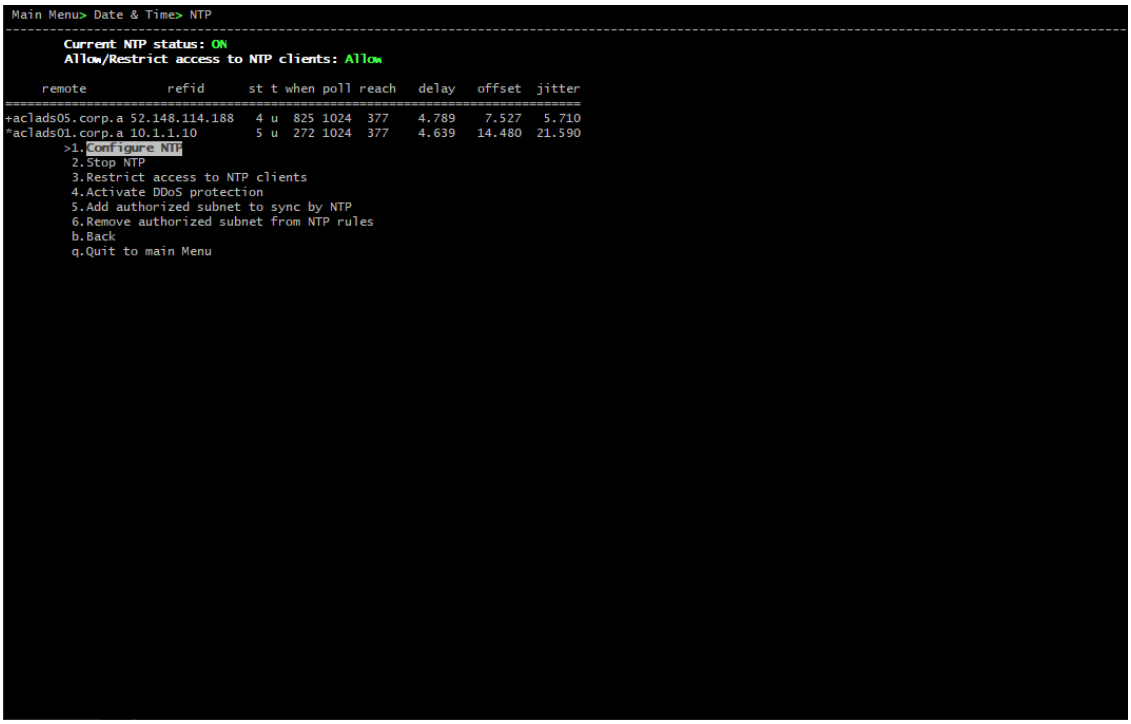
1. From the Date & Time menu, choose **NTP**, and then press Enter.

Figure 26-2: OVOC Server Manager - Configure NTP



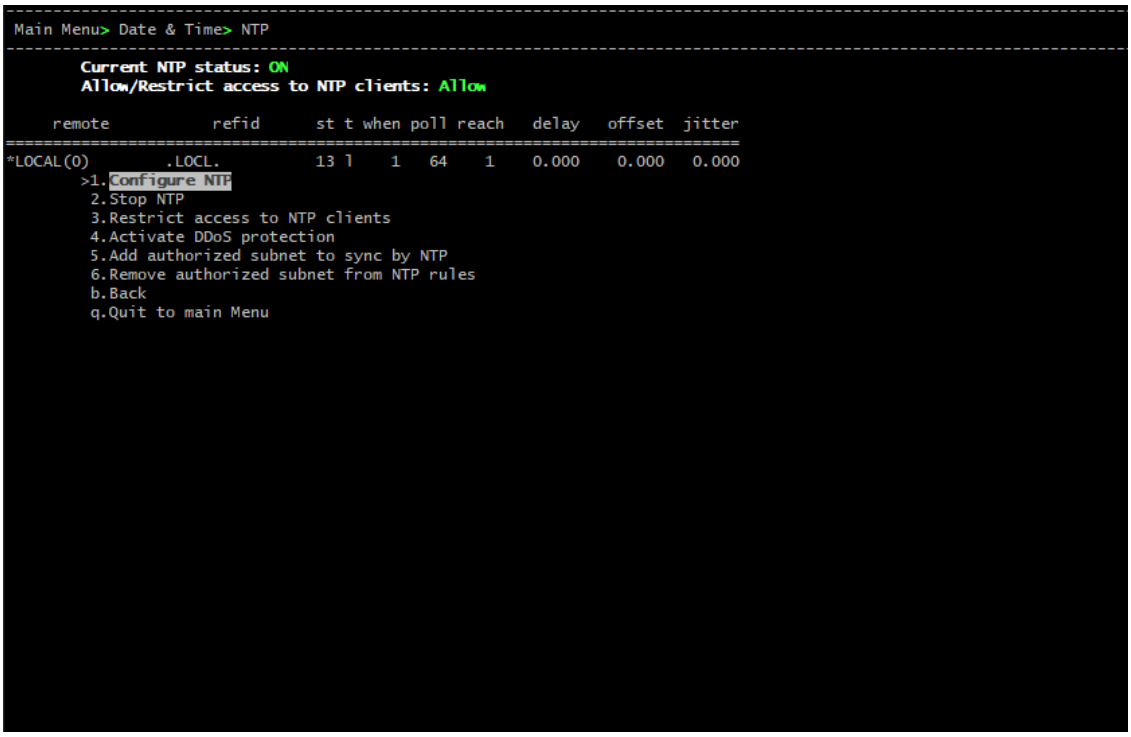
2. From the NTP menu, choose **Configure NTP**, and then press Enter.
3. At the prompt, do one of the following:
   - Type **y** for the OVOC server to act as both the NTP server and NTP client, and then press Enter. Enter the IP address or domain name of the NTP servers to serve as the clock reference 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.

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.

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.

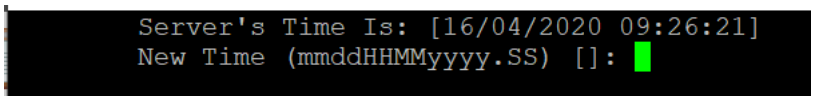
Date and Time Settings

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.

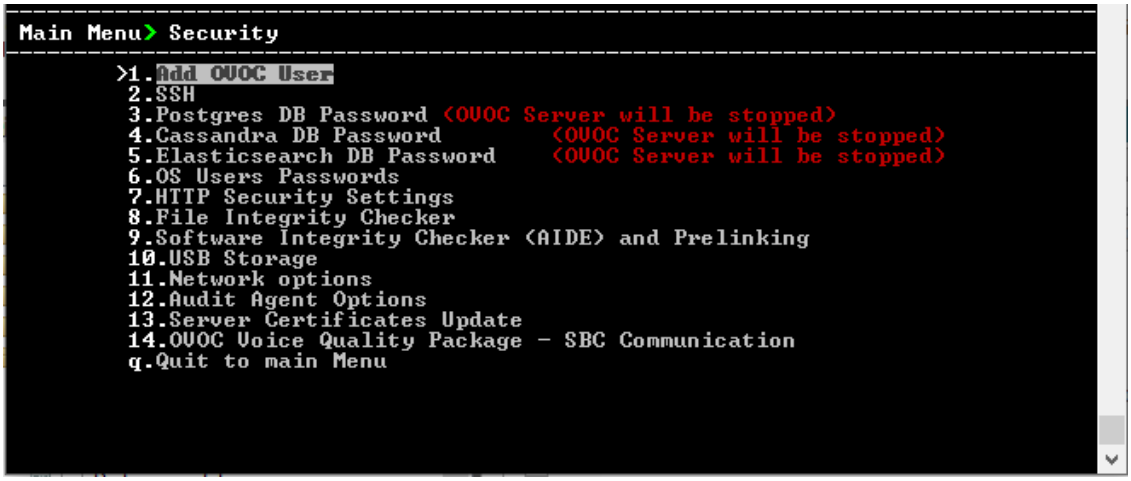
28 Security

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



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

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.

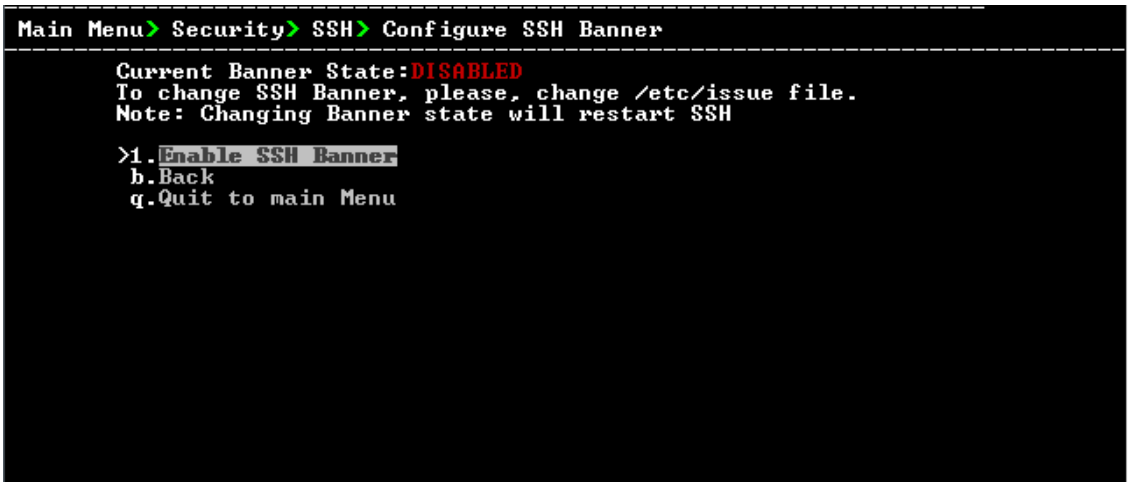
SSH Banner

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.

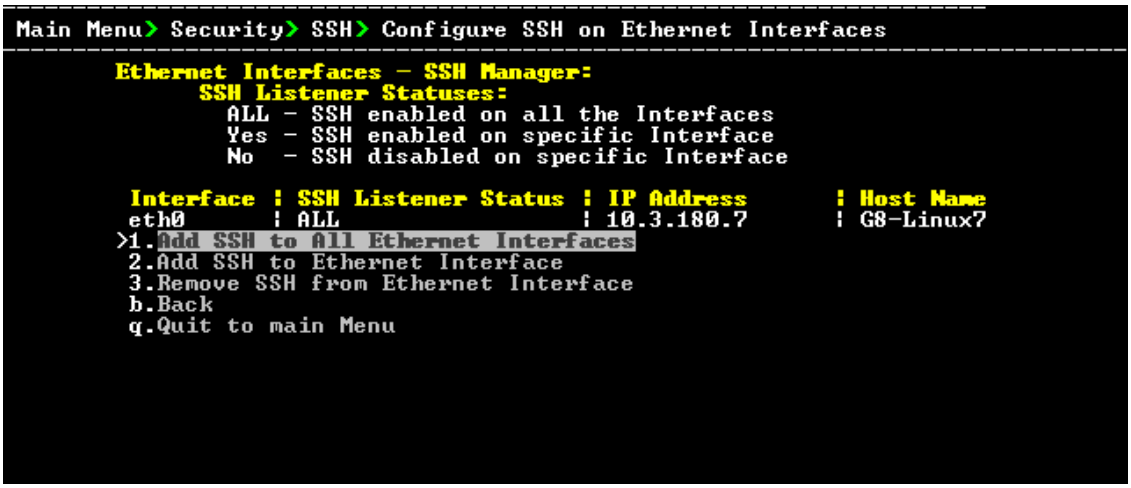
SSH on Ethernet Interfaces

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



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.

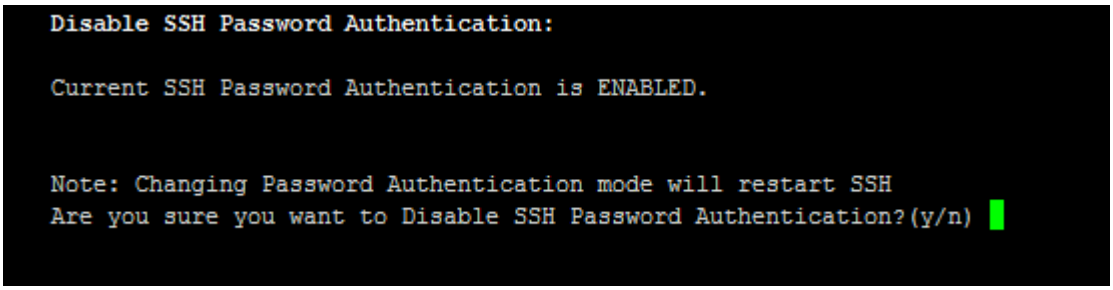
Enable/Disable SSH Password Authentication

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



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.

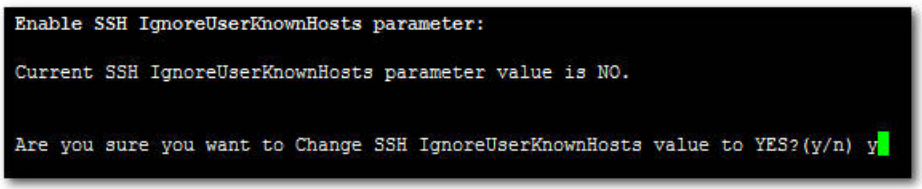
Enable SSH Ignore User Known Hosts Parameter

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.

Figure 28-7: SSH Ignore User Know Hosts Parameter - Confirm



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.

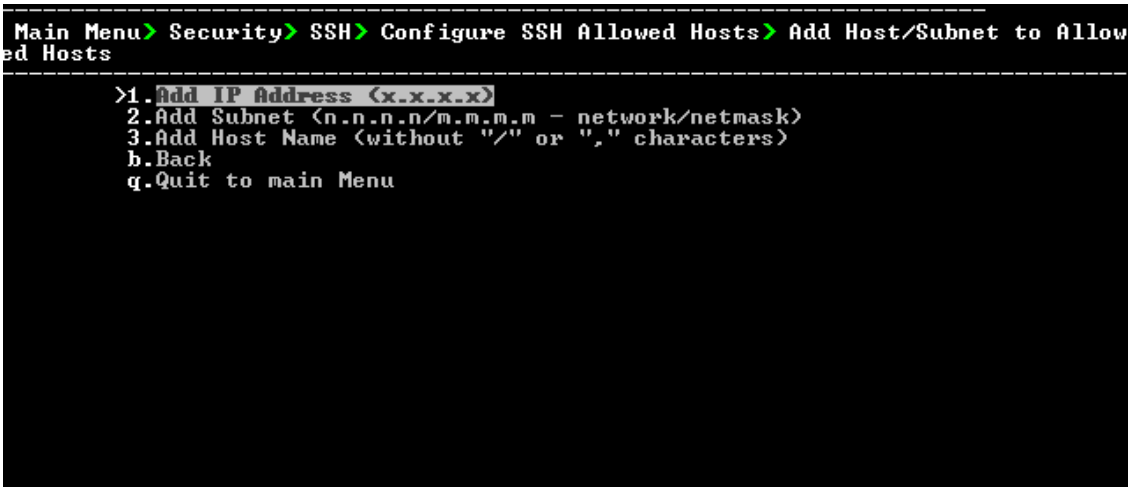
Add Hosts to Allowed Hosts

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.

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.

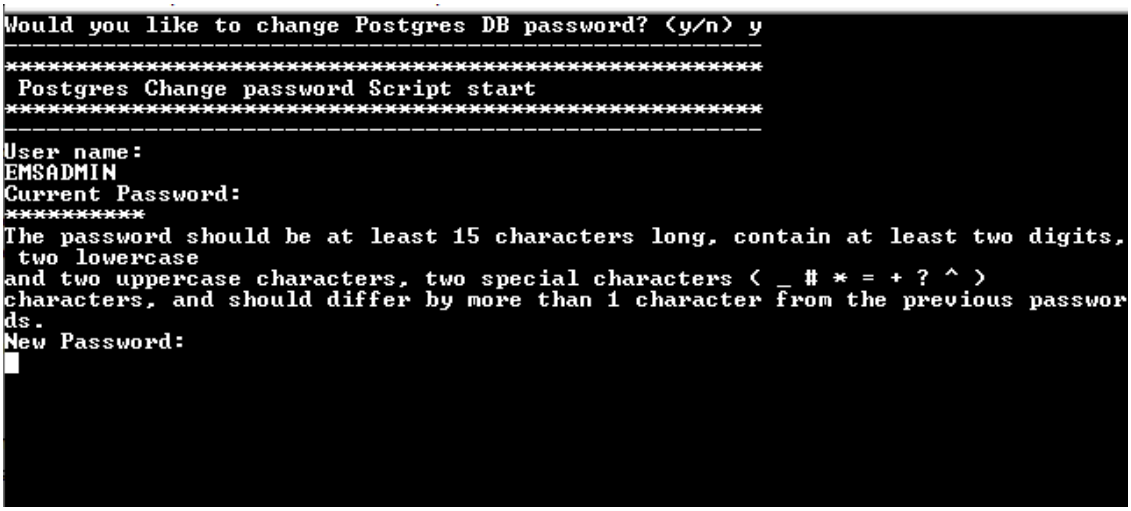
Figure 28-11: Postgre DB Password

2. Type **y** to change the password.

Figure 28-12: Current Password

3. Enter the current password.

Figure 28-13: New Password



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.

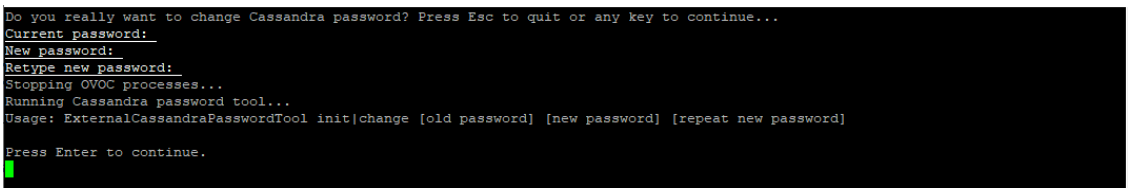
Cassandra Password

This section describes how to change the Cassandra password.

➢ **To change the Cassandra Password:**

1. 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.

Figure 28-15: Elastic Search DB Password

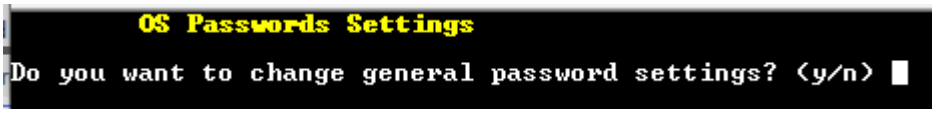
3. Enter the new password and confirm.

OS Users Passwords

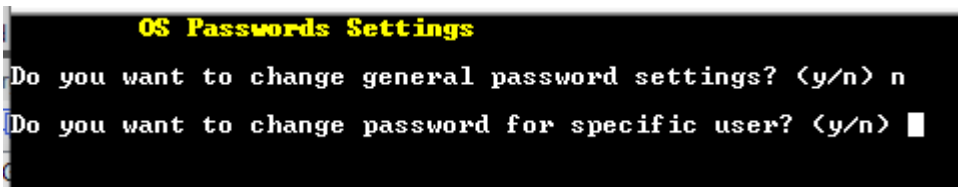
This section describes how to change the OS password settings.

➢ **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]:

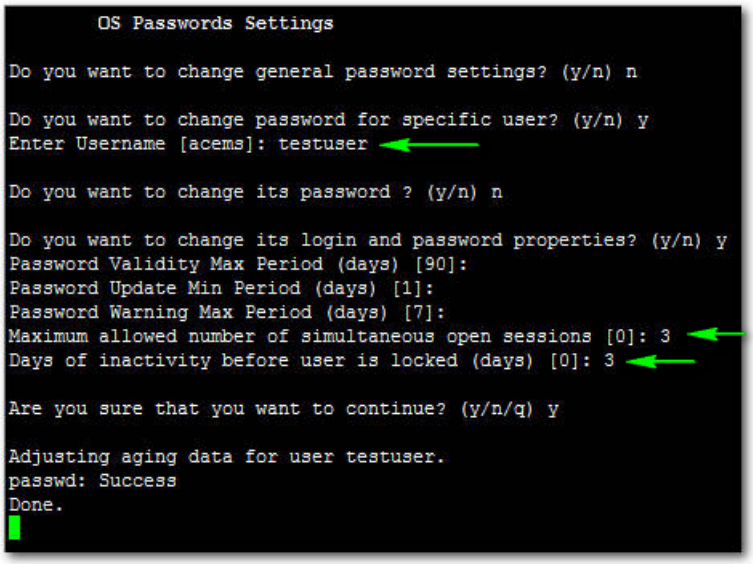
9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user, and then press Enter.

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



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.

Figure 28-17: Maximum Active SSH Sessions

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

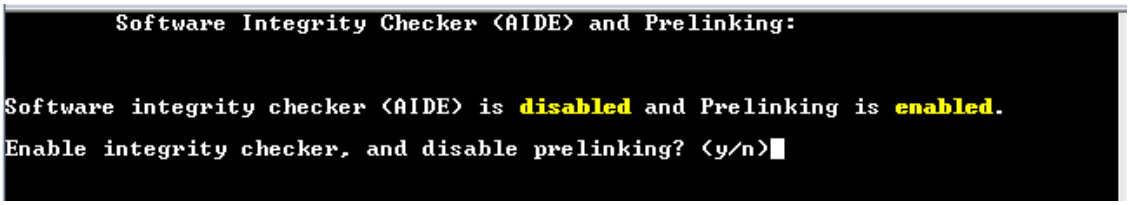
AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

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



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.

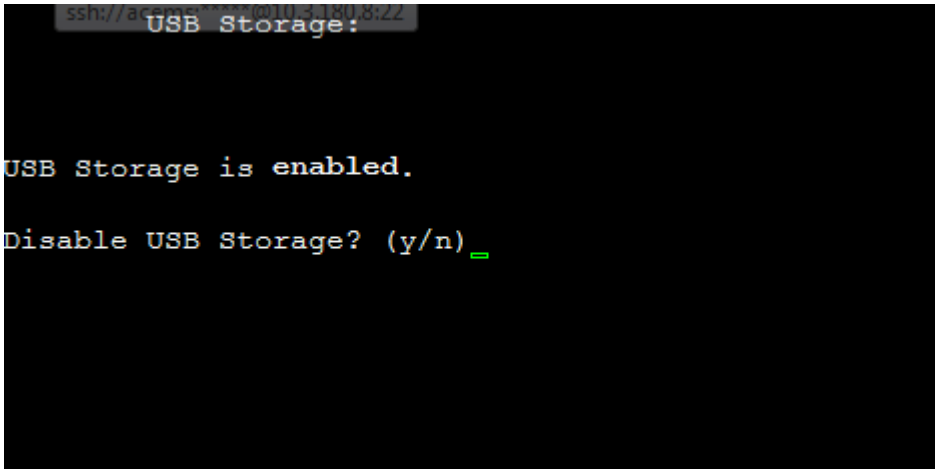
USB Storage

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.

Figure 28-19: USB Storage



2. Enable or disable USB storage as required.

Network Options

This menu option provides the following options to enhance network security:

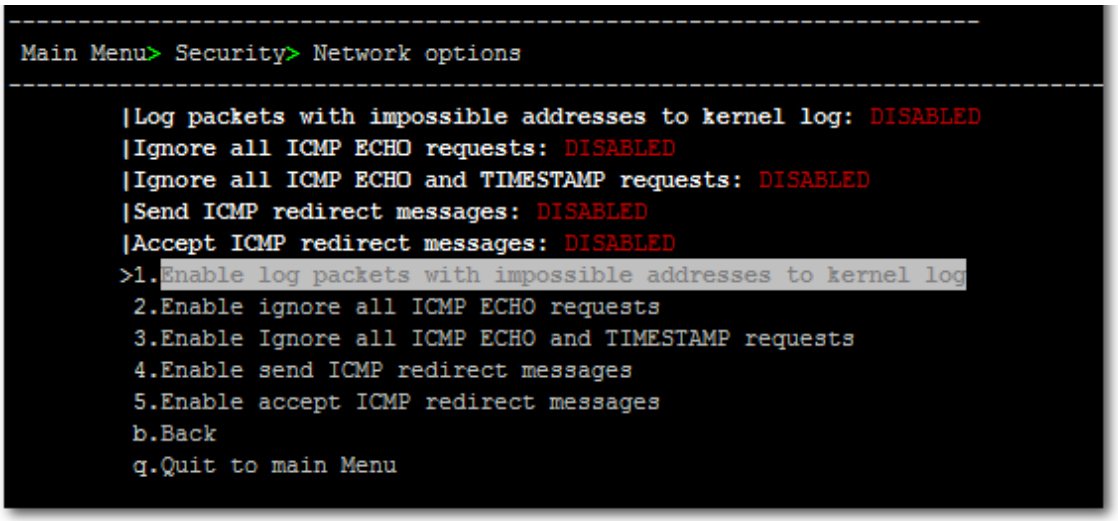
- **Ignore Internet Control Message Protocol (ICMP) Echo requests**: This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.
- **Ignore ICMP Echo and Timestamp requests:** 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



2. Set the required network options.

Auditd Agent Options

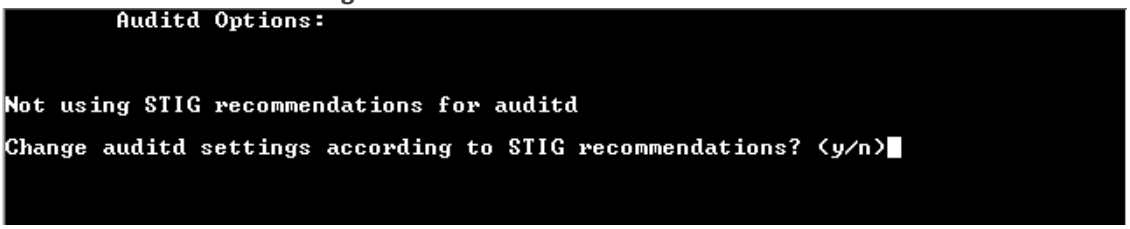
Auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk. Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

➢ **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:



2. Type **y** to enable auditd settings according to STIG recommendations.

   Audit records are saved in the following /var/log/audit/ directory.

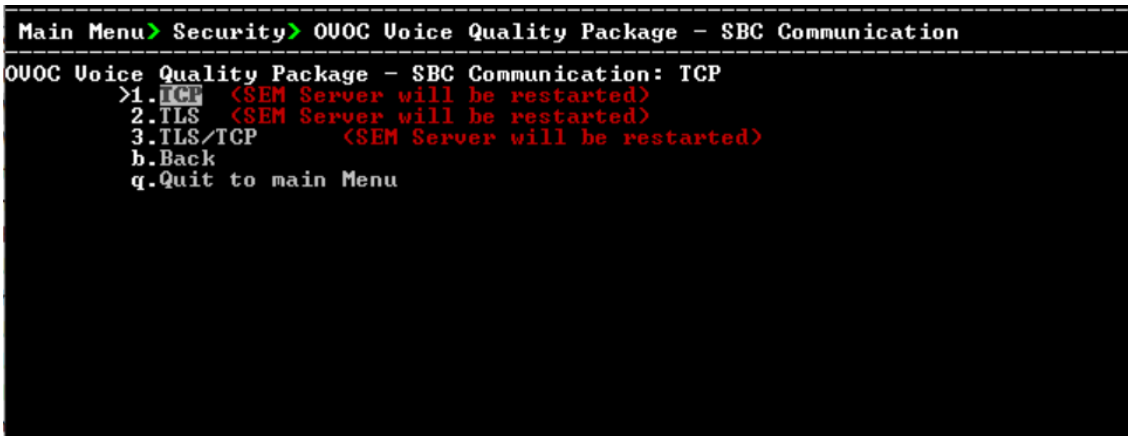
OVOC Voice Quality Package - SBC Communication

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

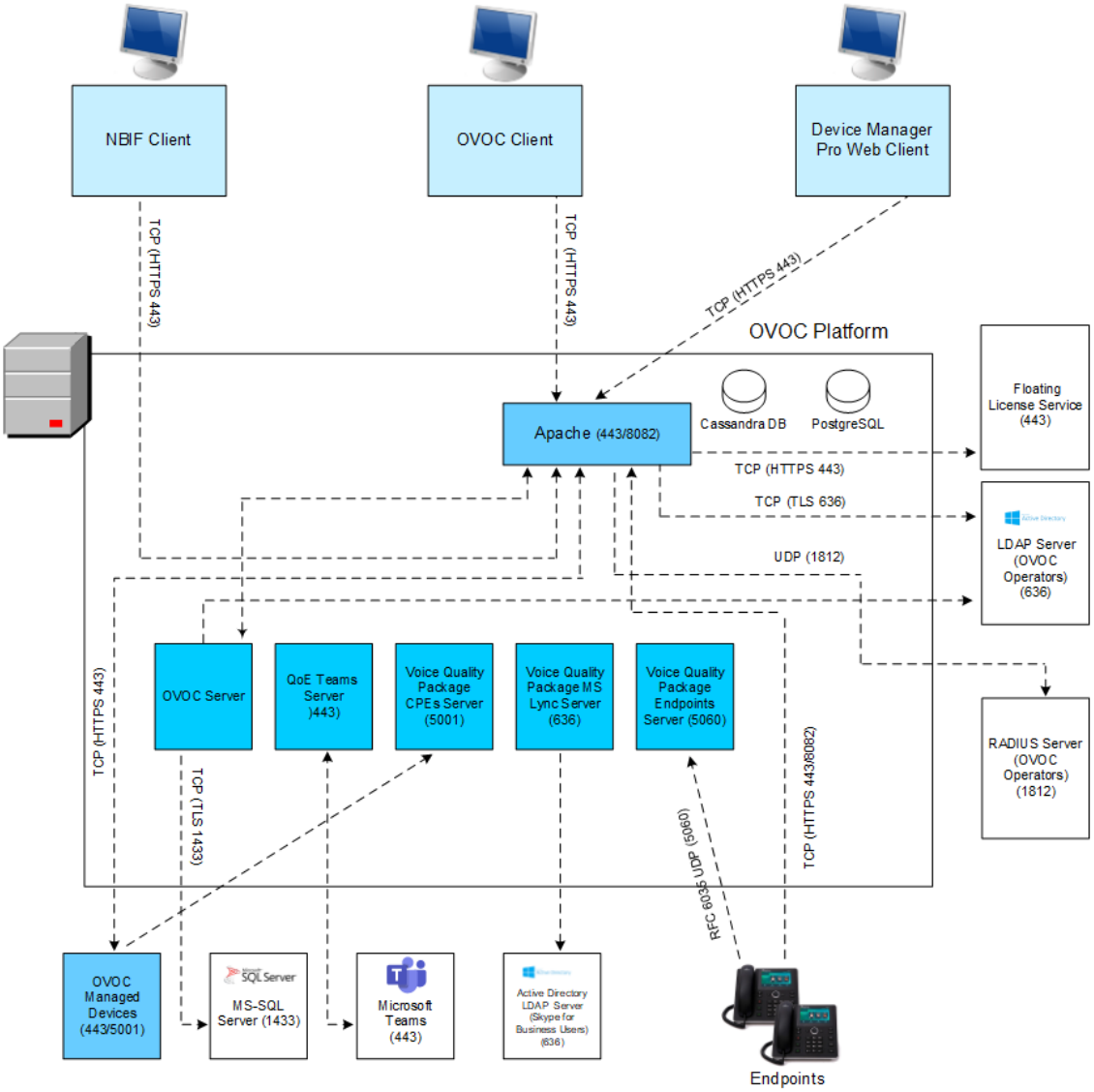


2. Choose one of the following transport types, and then press Enter:
   - TCP (opens port 5000)
   - TLS (opens port 5001)
   - TLS/TCP (this setting opens both ports 5000 and 5001).

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.

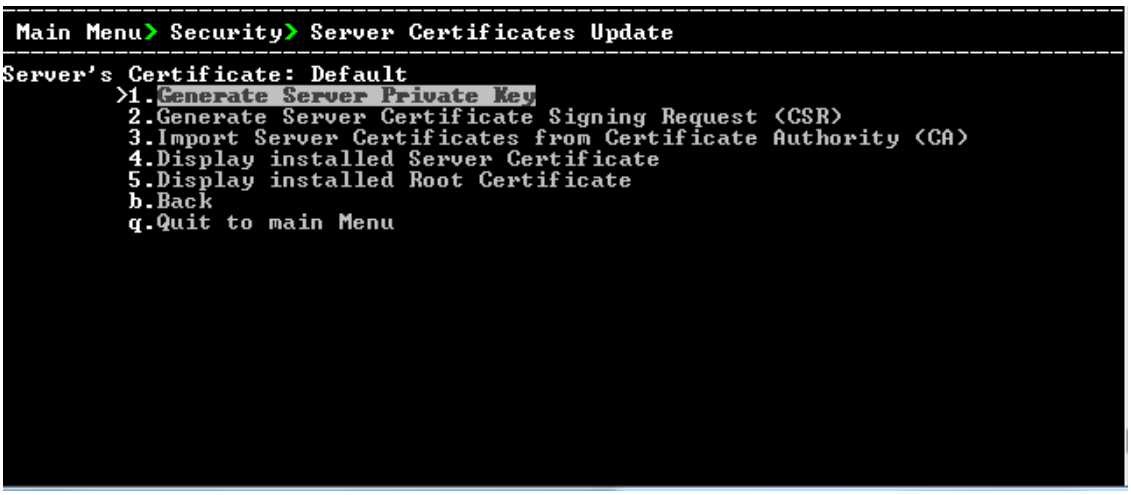
➢ **The procedure for server certificates update consists of the following steps:**

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

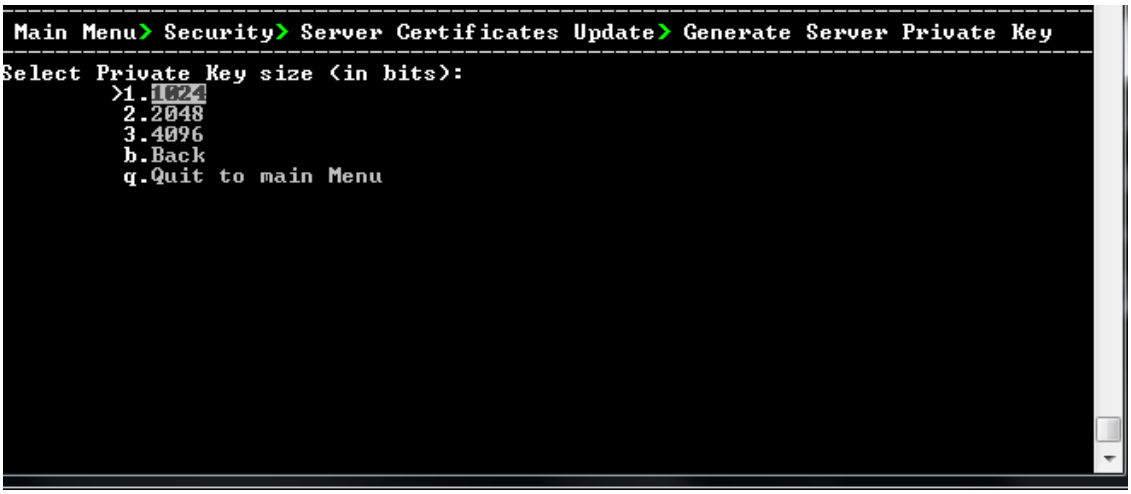


Information on the currently installed certificate is displayed (the currently installed certificate is the installation default).

➢ **Step 1: Generate a server private key:**

1. Select option **1**, and then press Enter. The following screen is displayed:

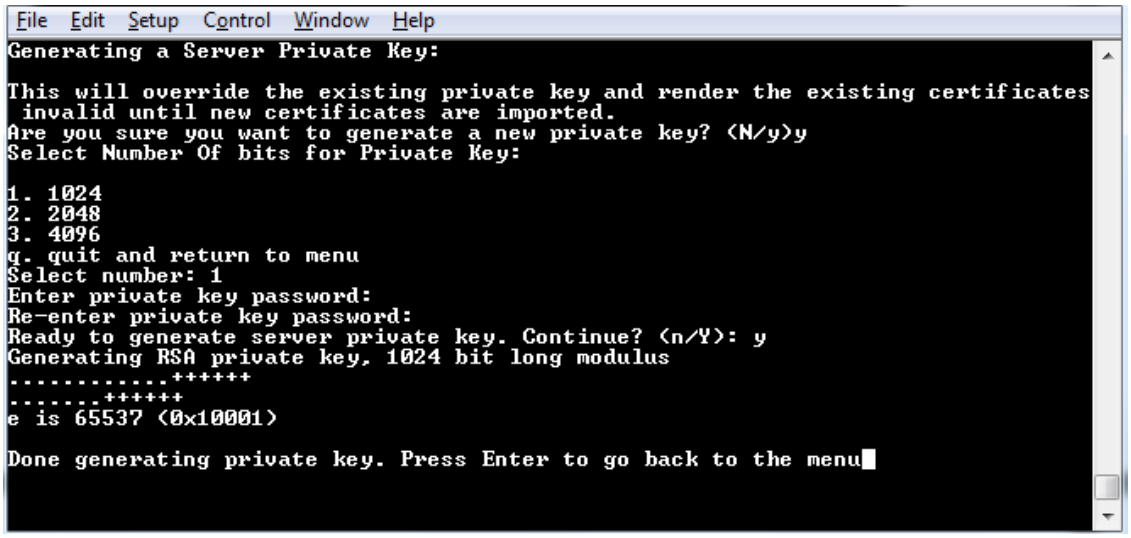
Figure 28-26: Generate Server Private Key



2. Select the number of bits required for the server private key, and then press Enter.
3. Enter and reenter the server private key password, type **y** to continue, and then press Enter.

   The private key is generated.

Figure 28-27: Server Private Key Generated

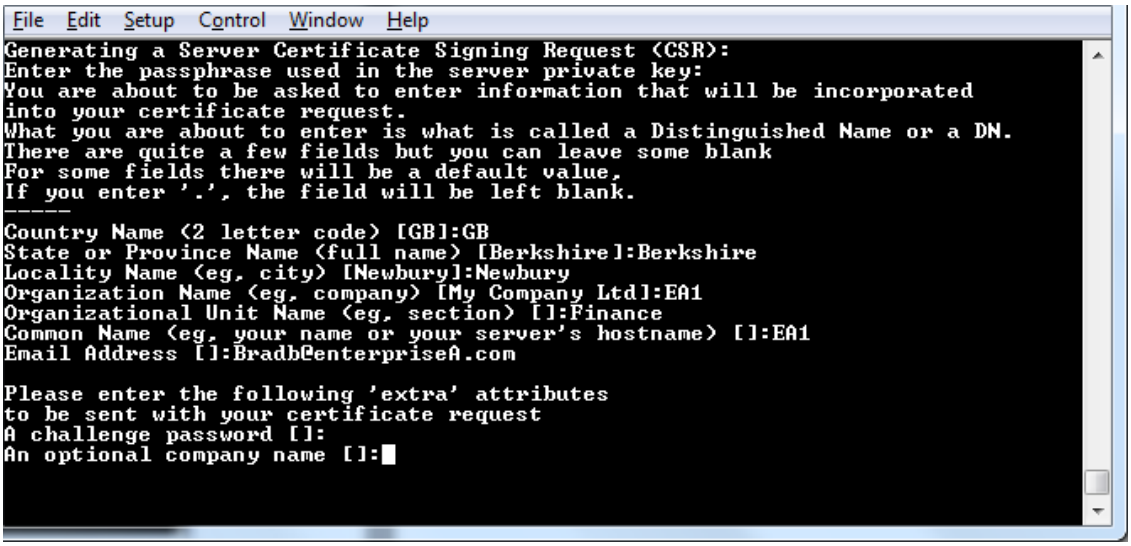


➢ Step 2: Generate a CSR for the server:

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.

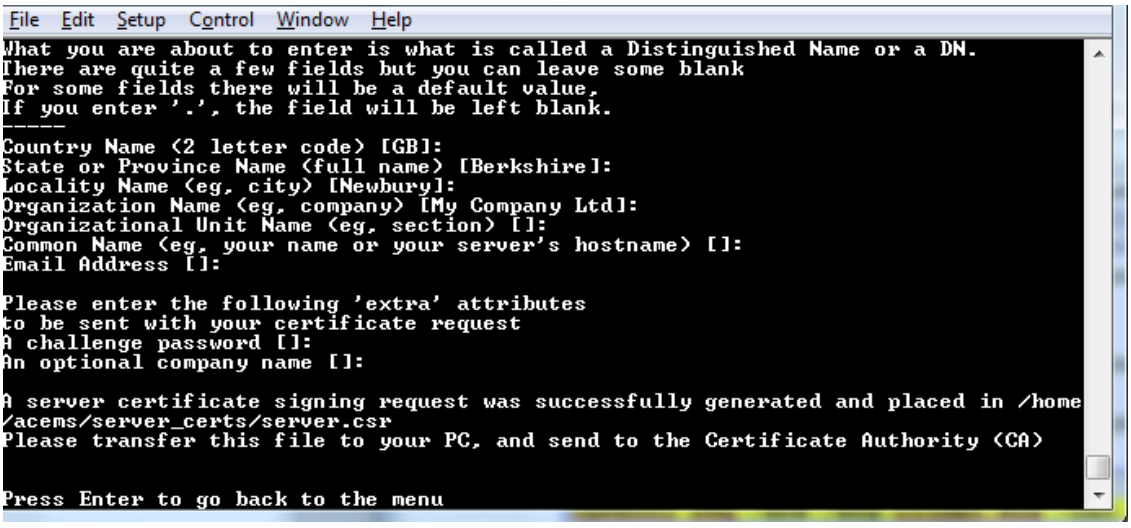
Figure 28-28: Generating a Server Certificate Signing Request (CSR)



➢ 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.

Figure 28-29: Transfer CSR File to PC



➢ 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.

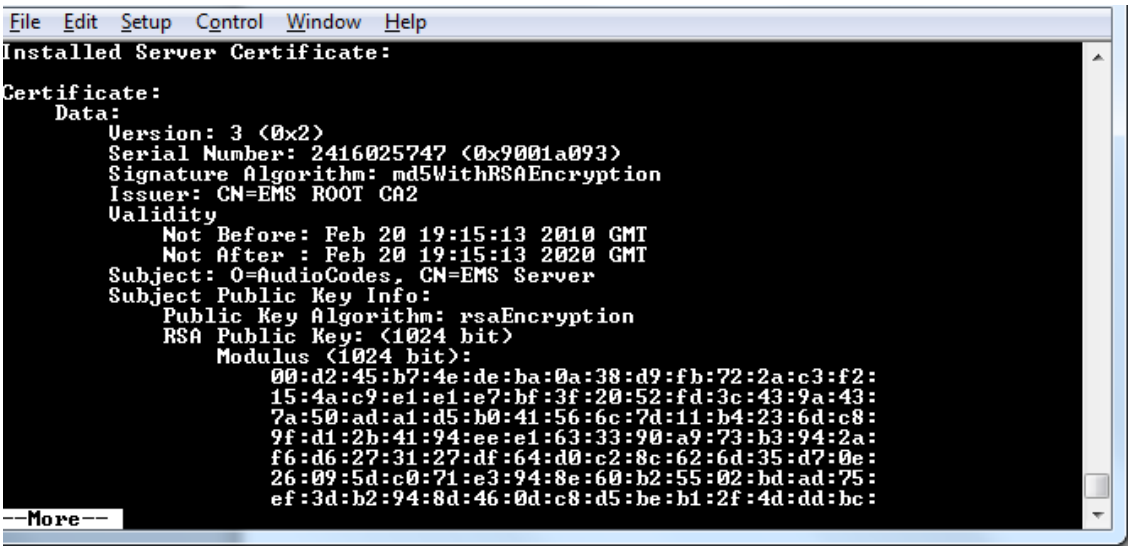
- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format and appear as follows (see Verifying and Converting Certificates on page 329 for information on converting files):

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1
UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0
MFowKjET
Tl6vqn5l27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0
L6V8lzUYOfHrEiq/6g==--
---END CERTIFICATE-----
```

➢ Step 6: Verify the installed server certificate:

■ Select option **4** ,and then press Enter. The installed server certificate is displayed:

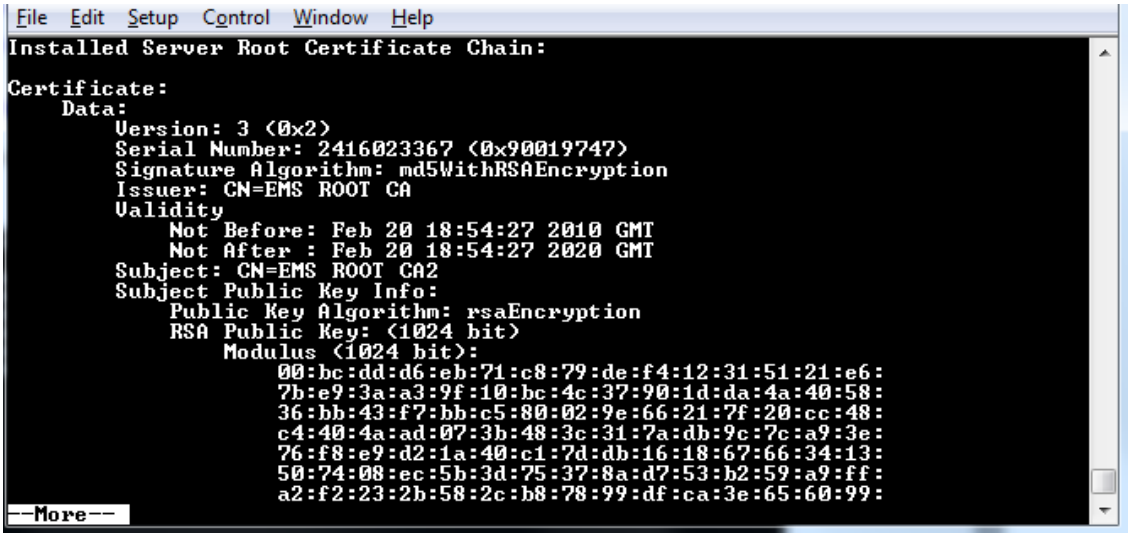
Figure 28-30: Installed Server Certificate



➢ **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



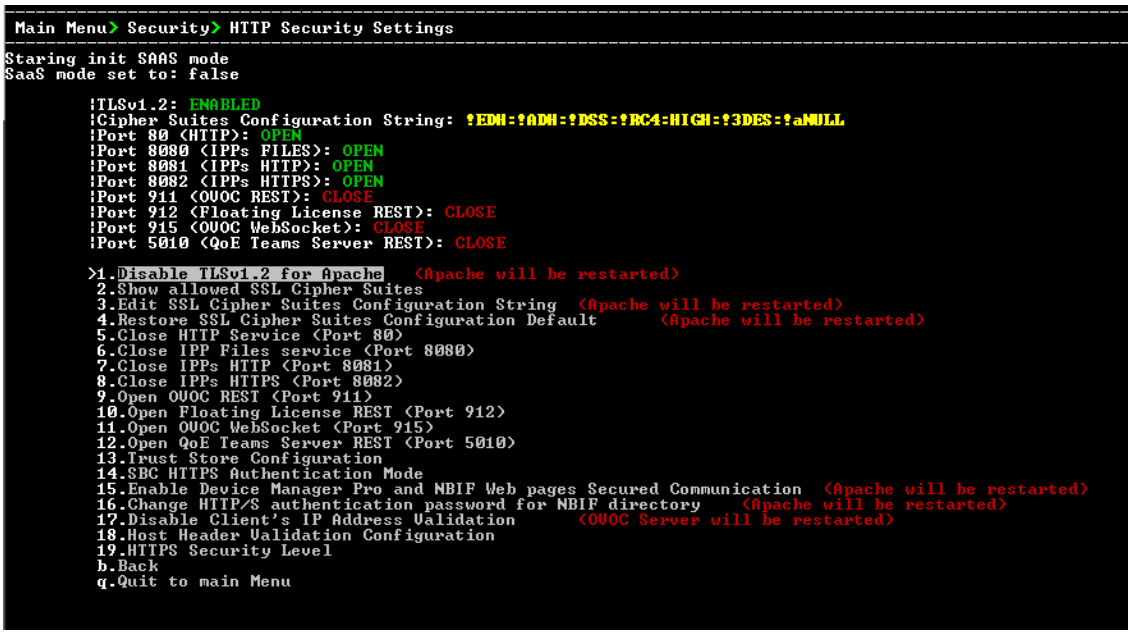
➢ **Step 8: Install device certificates and perform supplementary procedures**

- 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

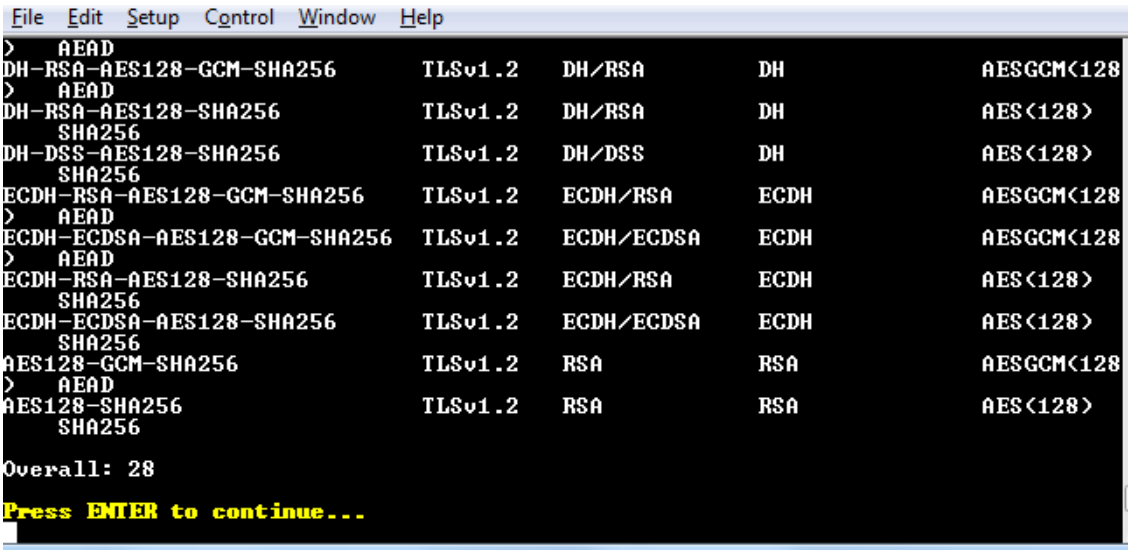
This option allows you to view the currently configured SSL cipher suites.

➢ **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



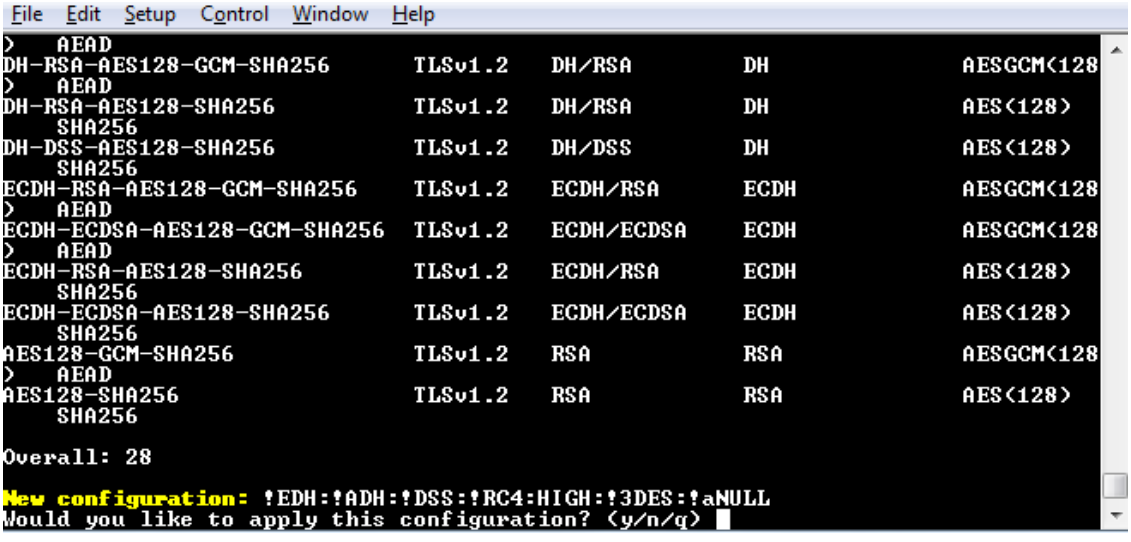
Edit SSL Cipher Suites Configuration String

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: Show SSL Cipher Suites Configuration



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:**

1. 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:**

1. 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

2. Select option **Add Trusted Root Certificate**.
3. 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:

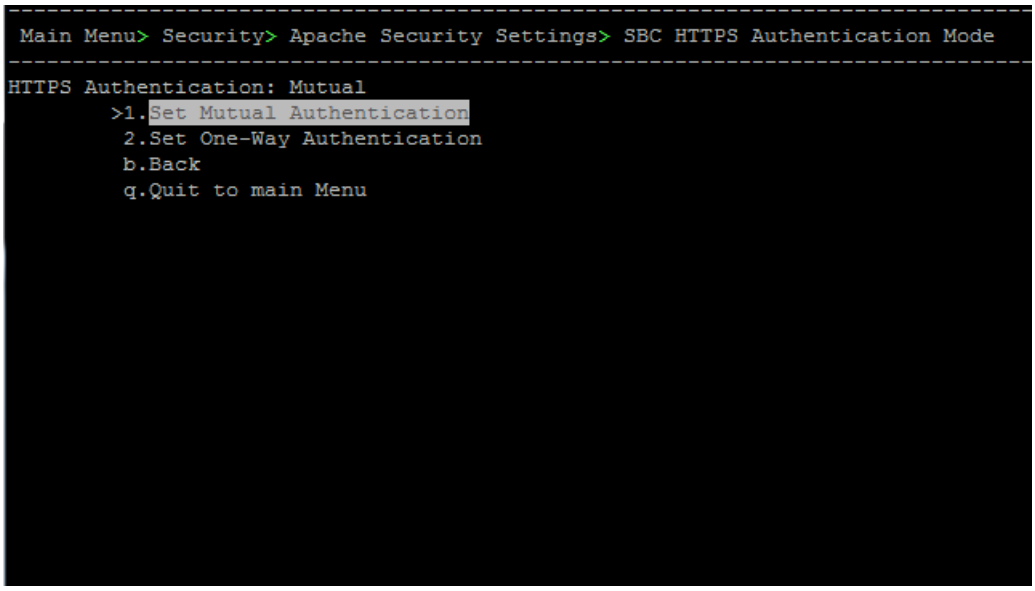
- **Mutual Authentication:** the OVOC authenticates the device connection request using certificates and the device authenticates the OVOC connection request using certificates. When this option is configured:
  - The same root CA must sign the certificate that is loaded to the device and certificate 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.

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 I**P Phone Manager and NBIF Web pages Secured Communication**, and then press Enter; the connection is secured.

Change HTTP/S Authentication Password for NBIF Directory

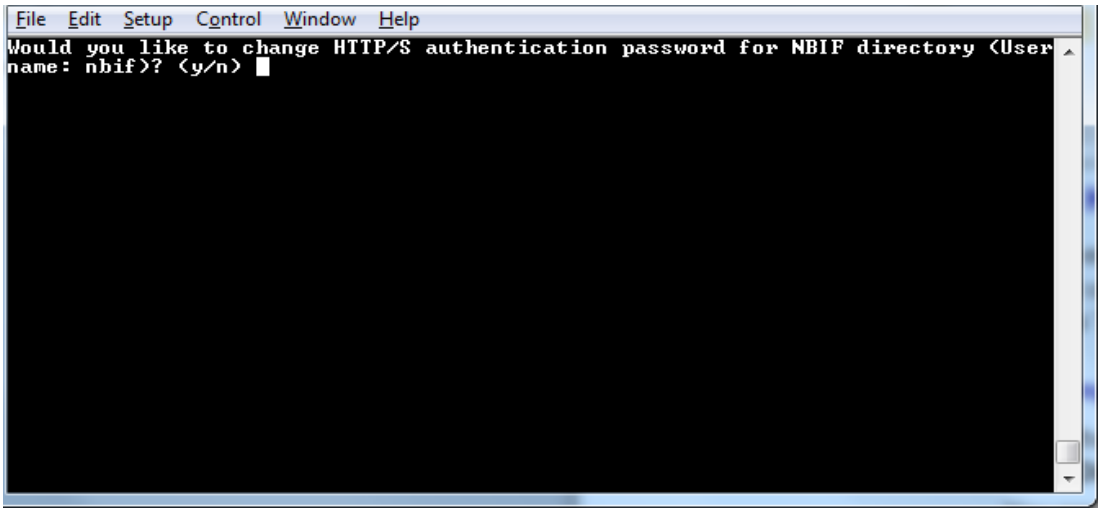
This option enables you to change the password for logging to the OVOC client from a NBIF client over an HTTP/S connection. The default user name is “nbif” and default password is “pass_1234”.

➢ **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.

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

2. Enter y to confirm update. The OVOC Server is restarted.

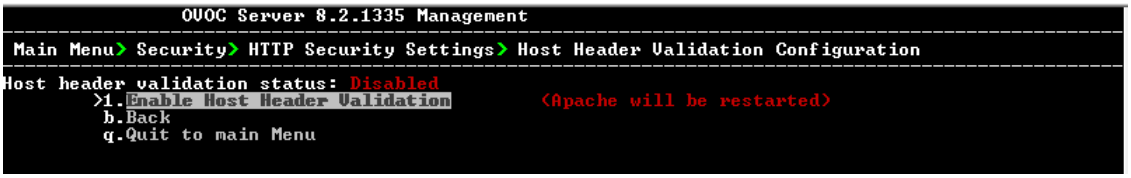
Host Header Validation Configuration

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.

Figure 28-39: Host Header Validation



2. Choose option **1** and then press Enter.

3. Enter the IP address of the host to add.

You are prompted to restart the Apache server.

29 Diagnostics

This section describes the diagnostics procedures provided by the OVOC Server Manager.

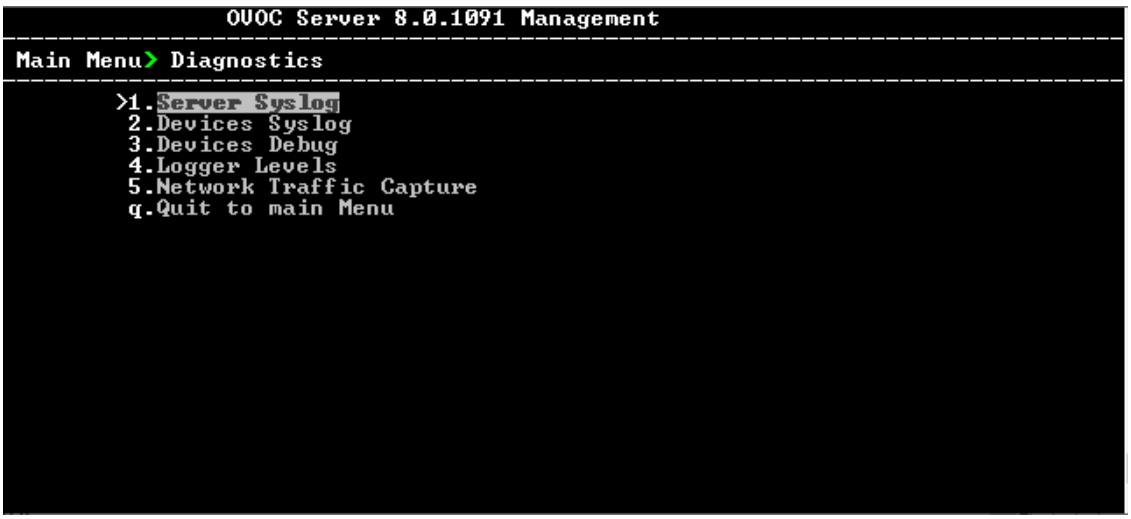
An IPv6 address can be configured for the following:

- 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.

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

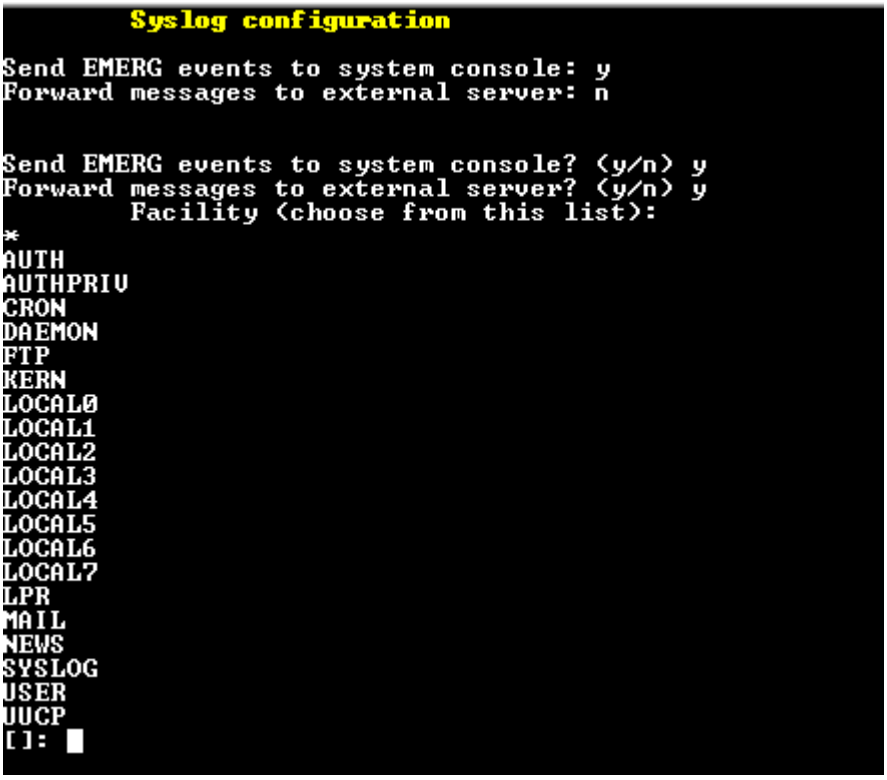
This section describes how to send OVOC server Operating System (OS)-related syslog EMERG events to the system console and other OVOC server OS related messages to a designated external server.

➢ **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.

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
   - **lpr:** 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:

Figure 29-3: Syslog Severities

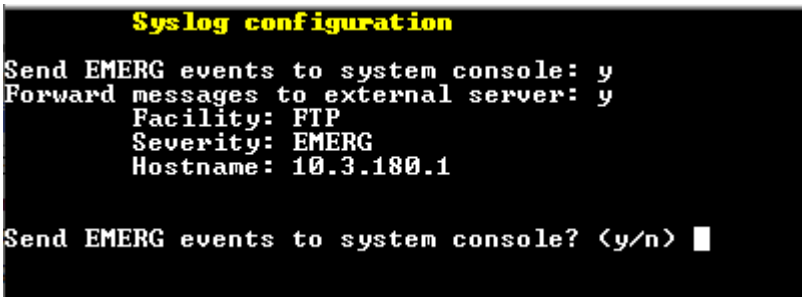
For the selected facilities, indicates one of the following:

- **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.

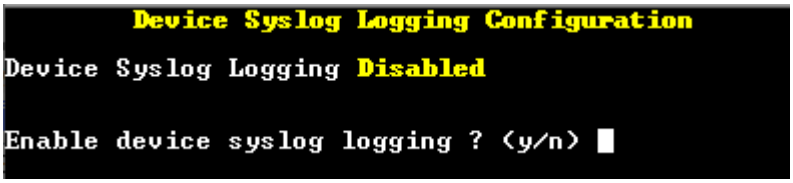
The syslog log file 'syslog' is located in the following OVOC server directory:

/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

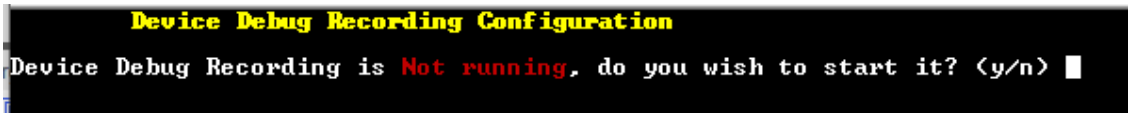
The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close; if the file reaches 10MB in less 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).

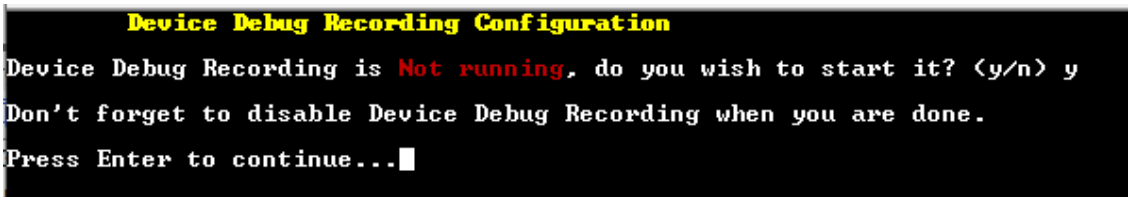
➢ **To enable or disable devices debug:**

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.



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.

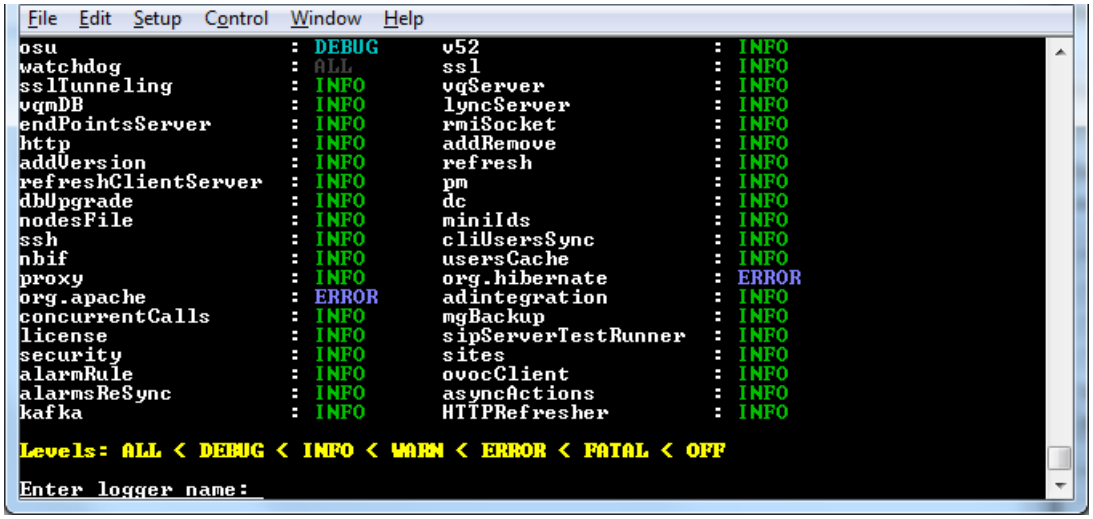
Server Logger Levels

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.

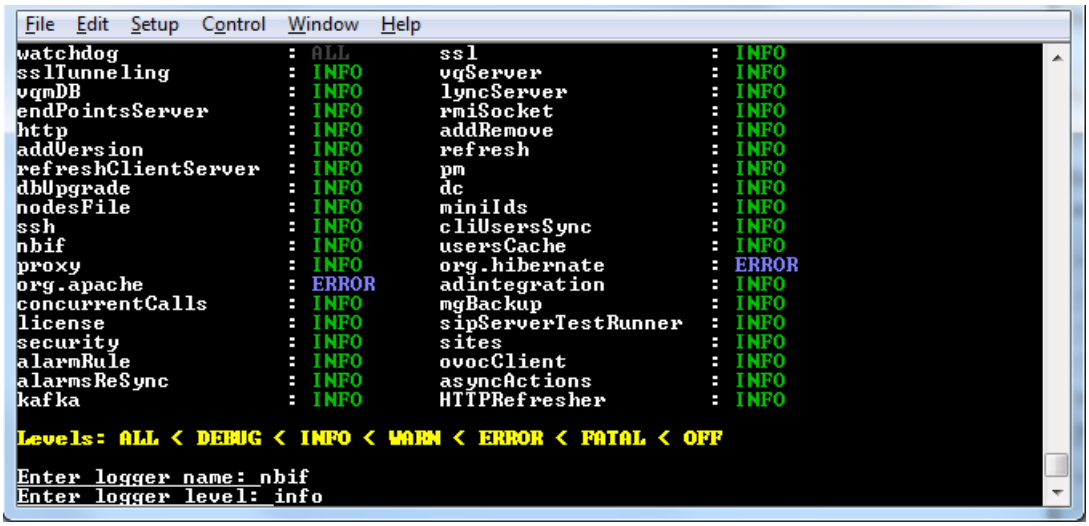
➢ **To change the <tc> server logger level:**

1. From the Diagnostics menu, choose **Logger Levels**.



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.

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.

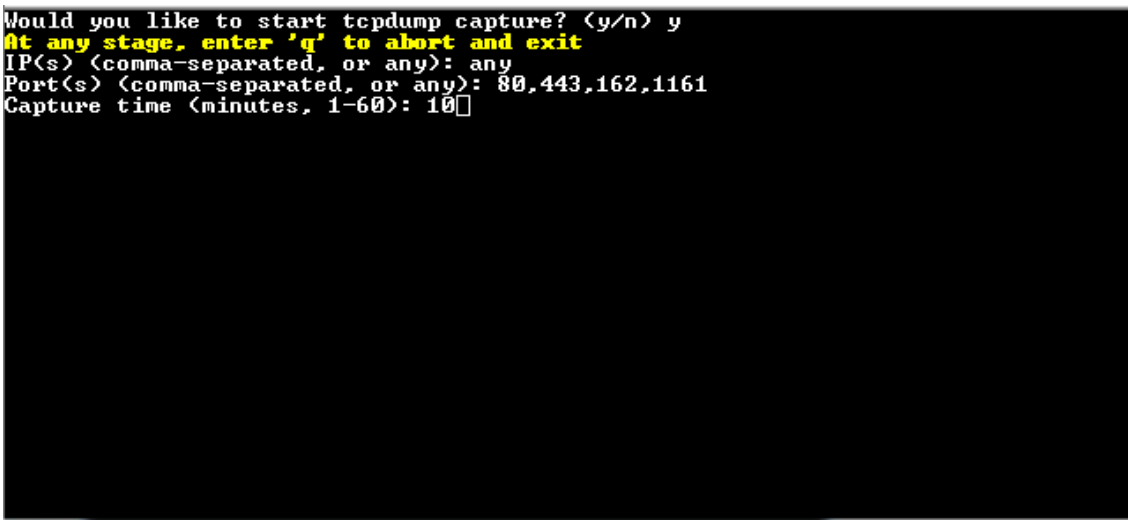
➢ **To capture TCP traffic:**

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.

Figure 29-7: TCP Dump

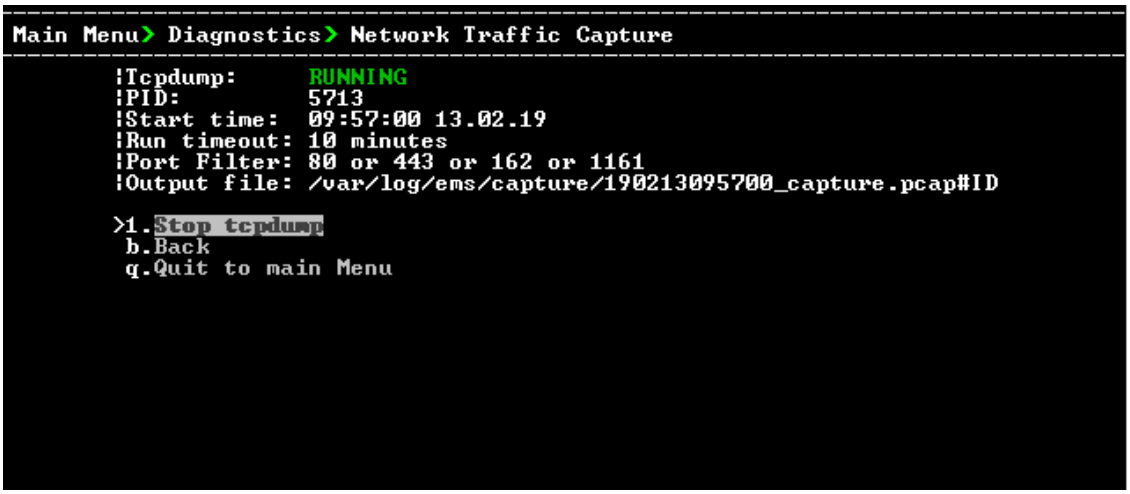


4. Enter comma separated IP address (es) or accept the default "any" IP address.
5. Enter comma separated port (s) or accept the default "any".
6. Enter the capture time (in minutes). Default: network traffic for the last ten minutes is captured.

Figure 29-8: Starting TCP Dump

7. Select **y** to proceed.

Figure 29-9: TCP Dump Running



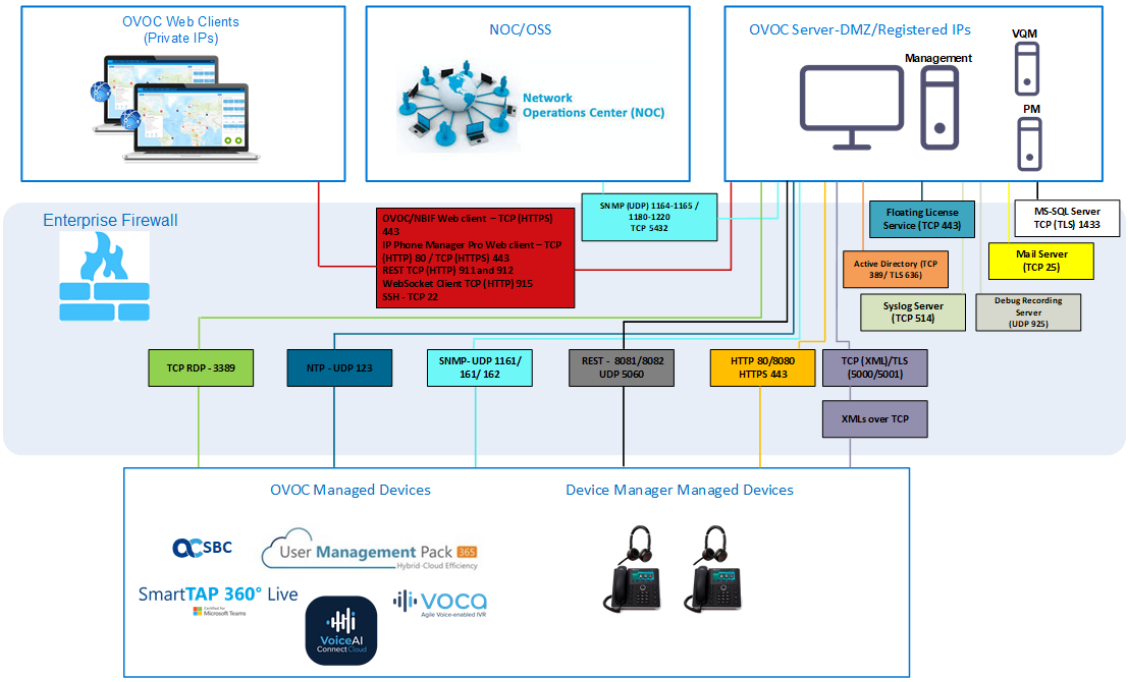
Part VII

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 ↔ OVOC server	TCP	√	22	SSH communication between OVOC server and TCP/IP client. ■ Initiator: client PC	OVOC server side / Bi-directional.
HTTPS/NBIF Clients ↔ OVOC server	TCP (HTTPS)	√	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)	√	5010	Internal	OVOC server side / Receive only
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	√	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 ↔ OVOC server (SNMP)	UDP	√	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	√	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	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)	×	80	HTTP connection for files transfer and REST communication. ■ Initiator: Both sides can initiate an HTTP connection	OVOC server side / Bi-directional
	TCP (HTTPS)	√	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)	√	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 Manager					
Endpoints ↔ OVOC Device Manager	TCP (HTTP)	×	80	HTTP connection between the Endpoints and the OVOC Device Manager. ■ Initiator: Endpoints	OVOC Device Manager side/ Bi-Directional
				HTTP connection that is used by endpoints for downloading firmware and configuration files . ■ Initiator: Endpoints	
Endpoints ↔ OVOC Device Manager	TCP (HTTPS)	√	443	HTTPS connection between the Endpoints and the OVOC Device Manager. ■ Initiator: Endpoints	OVOC Device Manager side / Bi-Directional
				HTTPS connection that is used by endpoints for downloading firmware and configuration files . ■ Initiator: Endpoints	
OVOC Device Manager ↔ ShareFile	TCP (HTTPS)	√	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 Connection	Port Number	Purpose	Port side / 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	TCP	×	5000	XML based communication for control, media data reports and SIP call flow messages. ■ Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	√	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	TCP	√	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					
Voice Quality Package ↔ Active Directory LDAP server (Skype for Business user authentication)	TCP	×	389	Connection between the Voice Quality Package server and the Active Directory LDAP server. ■ Initiator: OVOC server	Active Directory server side/ Bi-directional
	TCP (TLS)	√	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)	TCP	×	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 ↔ RADIUS server	TCP	×	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	TCP	√	443	HTTPS for OVOC/ Cloud Service ■ Initiator: OVOC REST client	OVOC REST client side / Bi-directional
External Server Connections					
OVOC server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server ■ Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	×	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	√	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. ■ Initiator: Endpoint	SEM server / Bi-directional

Table 30-2: Northbound Interfaces Flows: NOC/OSS → OVOC

Source IP Address Range	Destination IP Address Range	Protocol	Secure	Source Port Range	Destination Port Range
NOC/OSS	OVOC	SFTP	√	1024 - 65535	20
		FTP	×	1024 - 65535	21
		SSH	√	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

Table 30-3: OAM Flows: OVOC → NOC/OSS

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 Active alarms Resync feature.	×	1164 - 1174	-
		SNMP (UDP) port for alarm forwarding.	×	1180-1220	-

Figure 30-1: Firewall Configuration Schema

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	OVOC Device Manager side / Bi-Directional
		HTTPS connection that is used by endpoints for downloading firmware and configuration files from the OVOC Device Manager. ■ Initiator: Endpoints	
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.

Table 30-4: Enterprise Firewall

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC clients and OVOC server					
HTTPS/NBIF Clients ↔ OVOC server	TCP (HTTPS)	√	443	Connection for OVOC/ NBIF clients. ■ Initiator: Client	OVOC server side / Bi-directional
Microsoft Teams↔ OVOC Communication	TCP (HTTPS)	√	443	Connection to Microsoft Teams ■ Initiator: Microsoft Teams	Bi-directional
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	√	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 ↔ OVOC server (SNMP)	UDP	√	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	√	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 ↔ OVOC server	TCP (HTTP)	×	80	HTTP connection for files transfer and REST communication. ■ Initiator: Both sides can initiate an HTTP connection	OVOC server side / Bi-directional
	TCP (HTTPS)	√	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)	√	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 Manager					
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)	√	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 Server and Devices					
Media Gateways ↔ Voice Quality Package	TCP	×	5000	XML based communication for control, media data reports and SIP call flow messages. ■ Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	√	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					
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	TCP	×	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 Service					
OVOC server ↔AudioCodes Floating License Service	TCP	√	443	HTTPS for OVOC/ Cloud Service ■ Initiator: OVOC REST client	OVOC REST client side / Bi-directional
External Servers					
OVOC server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server ■ Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	×	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	√	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. ■ Initiator: Endpoint	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
```

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:

```
begin authenticators
```

```
    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_xxxxxxxx@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
```

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*.

Figure 32-1: SATA DS 1.92 TB SSD Disks

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.
6. 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:**

1. In the left-hand pane, select **HPE Smart Array E208i-a SR Gen10**, and then click **Set Bootable Logical Drive/Volume.**
2. 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.

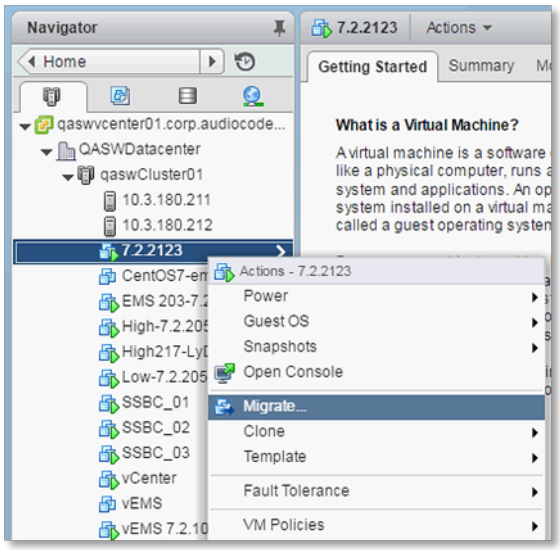
Migrating OVOC Virtual Machines in a VMware Cluster

This section describes how to migrate your OVOC Virtual machine from one ESXi host to another.

➢ **To migrate your OVOC virtual machine:**

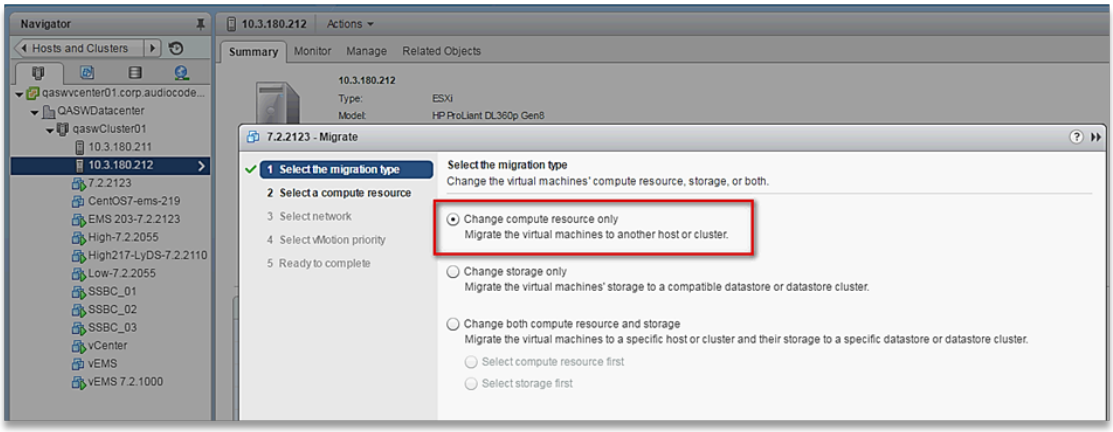
1. Select the OVOC virtual machine that you wish to migrate and then choose the **Migrate** option.

Figure 33-1: Migration



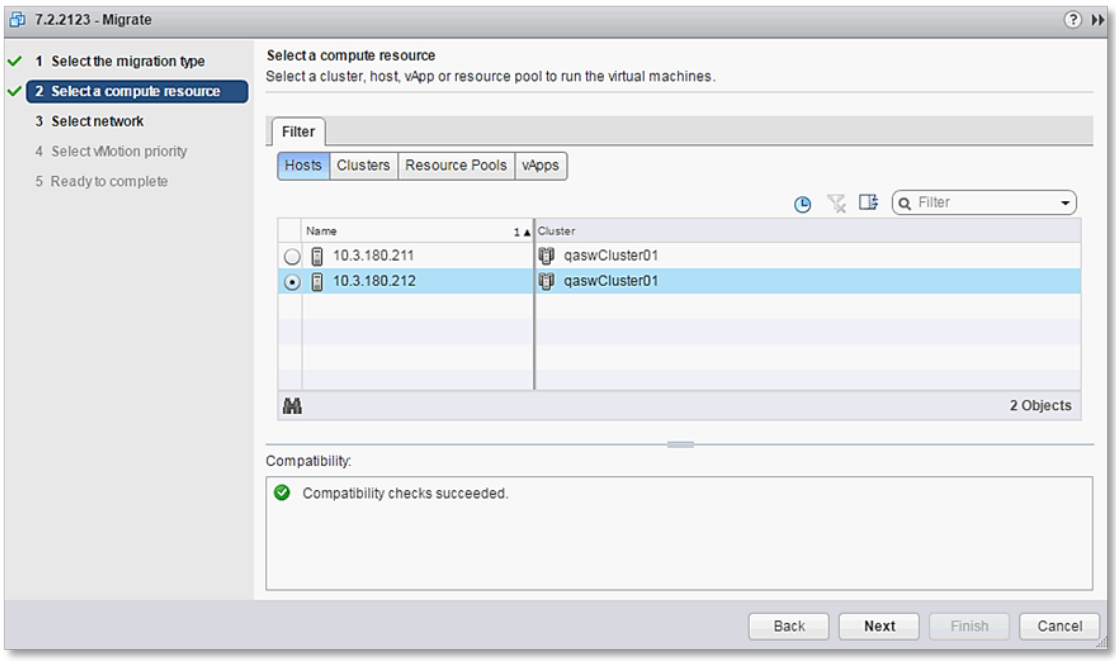
2. Change a cluster host for migration.

Figure 33-2: Change Host



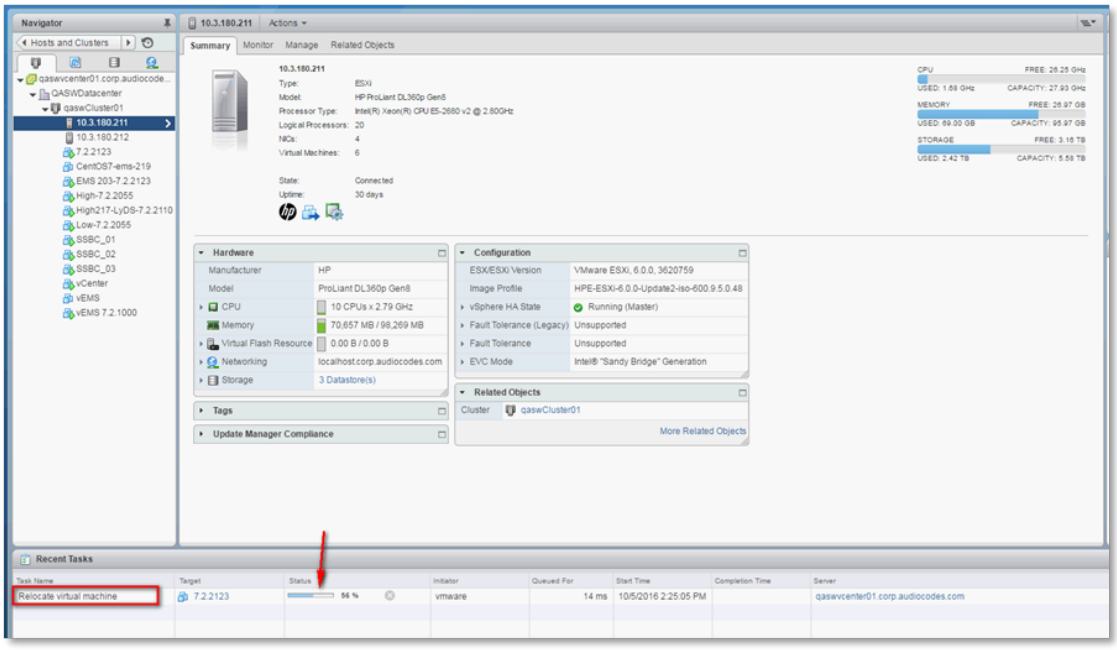
3. Choose the target host for migration.

Figure 33-3: Target Host for Migration



The migration process commences.

Figure 33-4: Migration Process Started



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

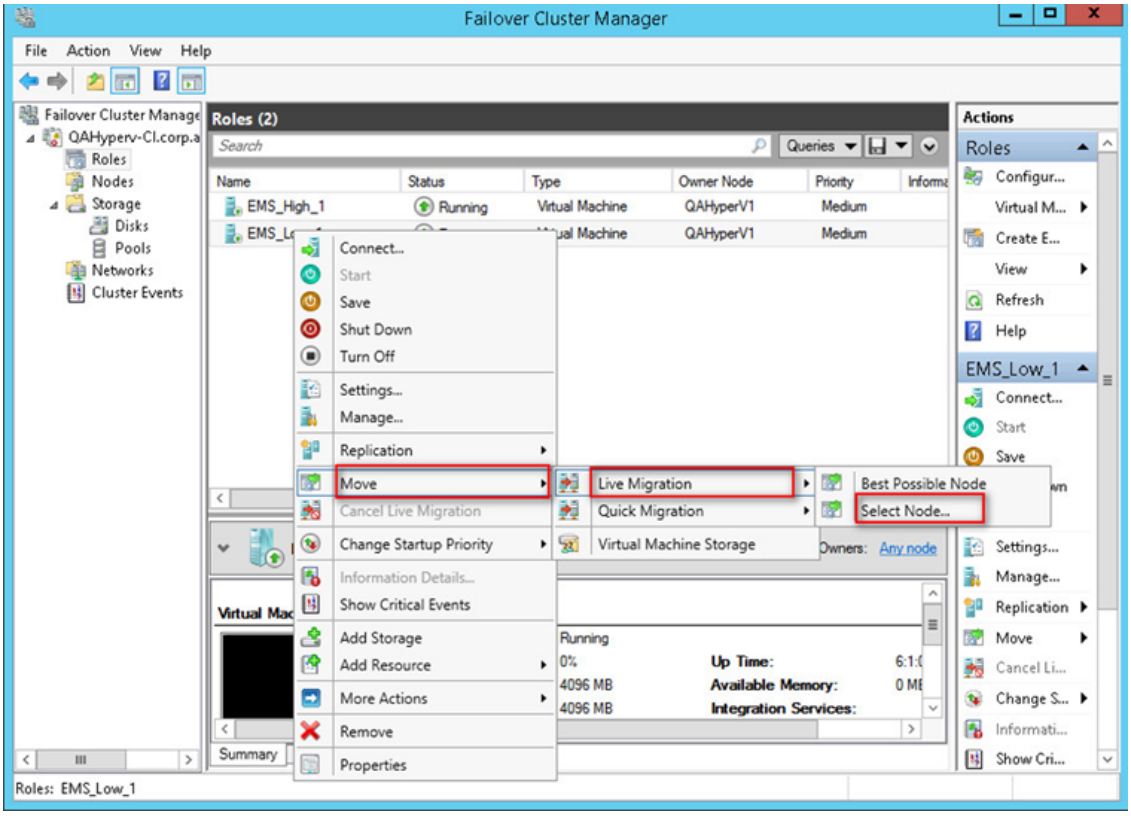
Moving OVOC VMs in a Hyper-V Cluster

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:

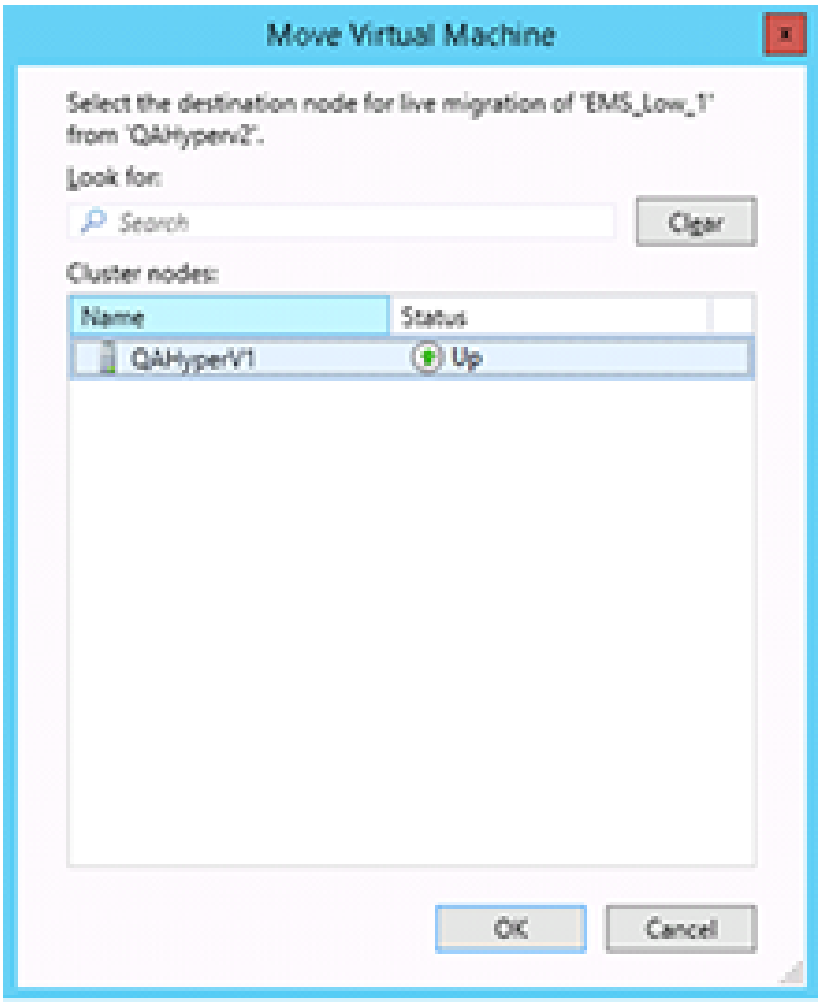
1. Select the Virtual Machine, right-click and from the menu, choose **Move** > **Live Migration** > **Select Node**.

Figure 33-5: Hyper-V Live Migration



The following screen is displayed:

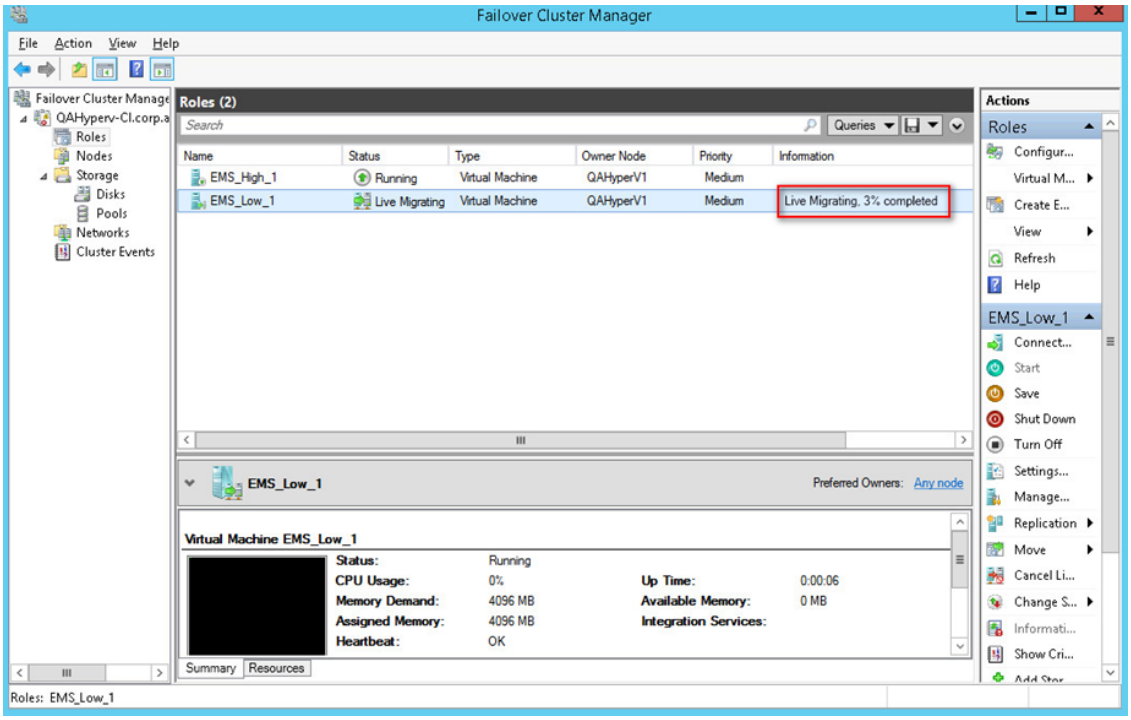
Figure 33-6: Move Virtual Machine



2. Select the relevant node and click **OK**.

   The migration process starts.

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.**

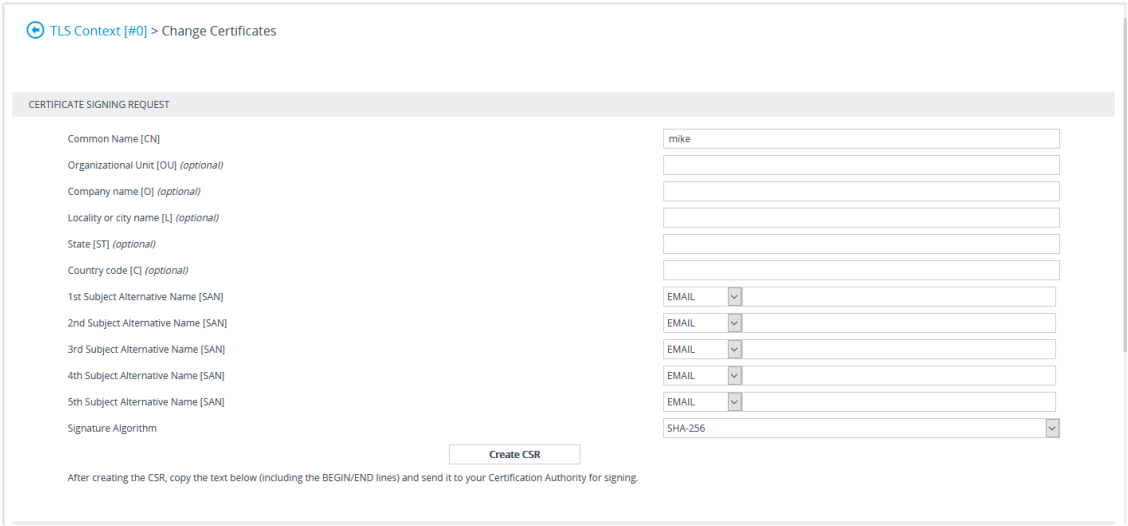
Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➢ To generate certificate signing request:

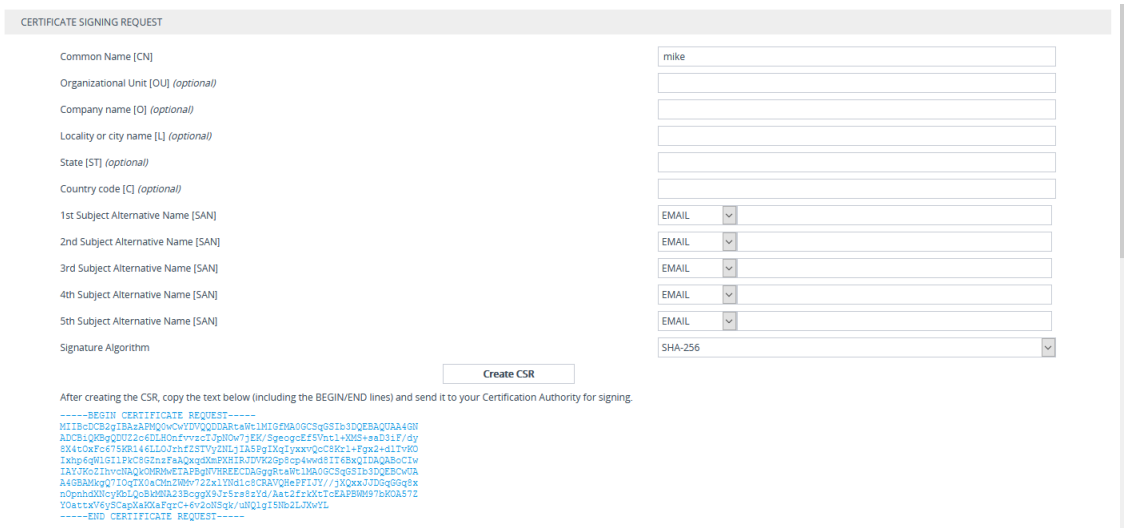
1. Login to the device's Web server.
2. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
3. In the table, select the **TLS Context Index #0**, and then click the **TLS Context Certificate** button, located below the table; the Context Certificates page appears.

Figure 34-1: Context Certificates



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:

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-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UEAxMM
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.

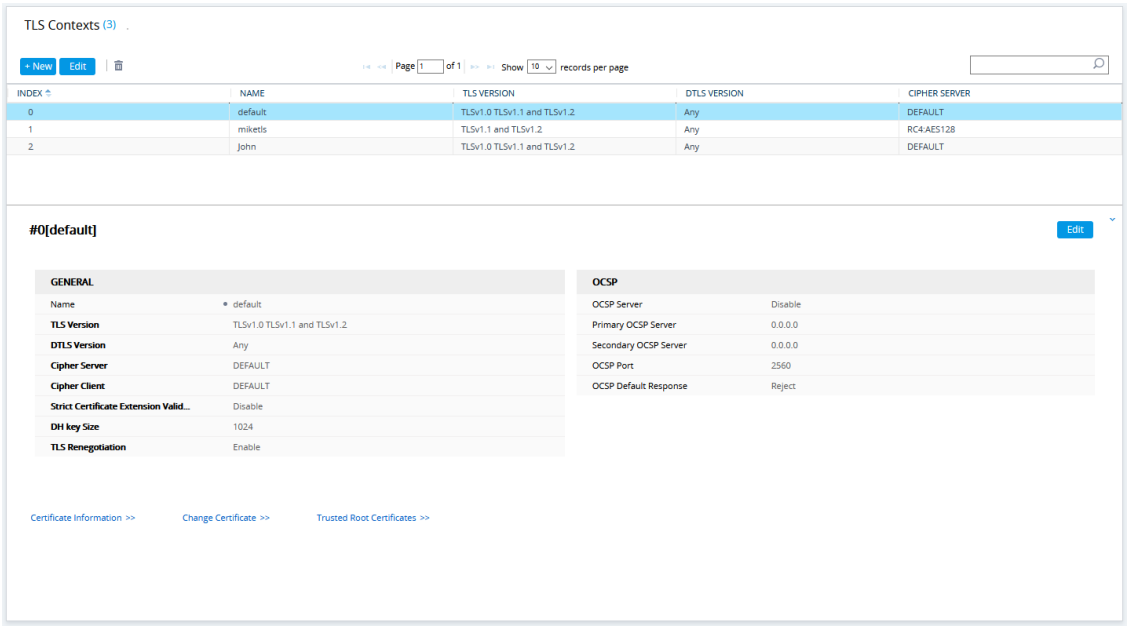
Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

➢ **To update device with new certificate:**

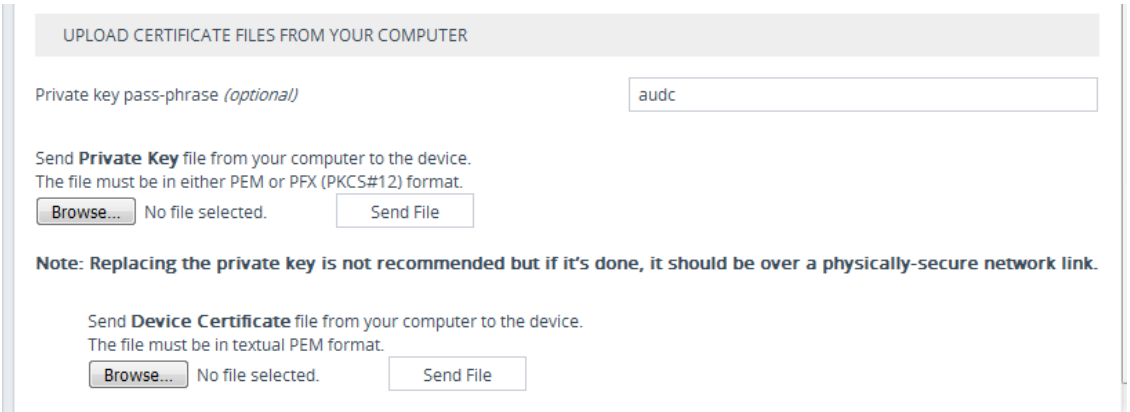
1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the table, select **TLS Context #0**, and then click the **Change Certificate** button, located below the table; the Context Certificates page appears.

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



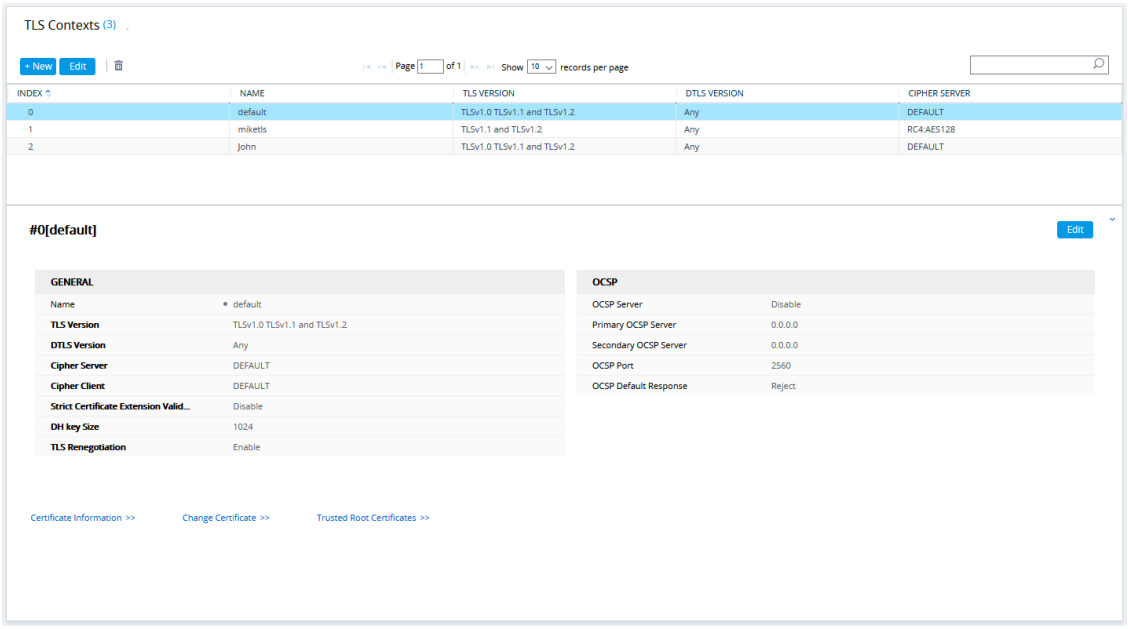
Step 4: Update Device's Trusted Certificate Store

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.

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

4. 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

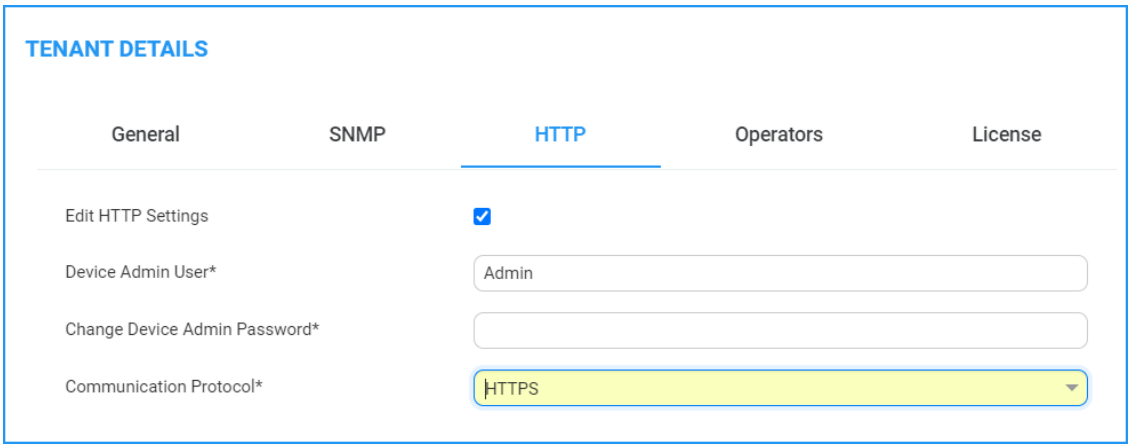
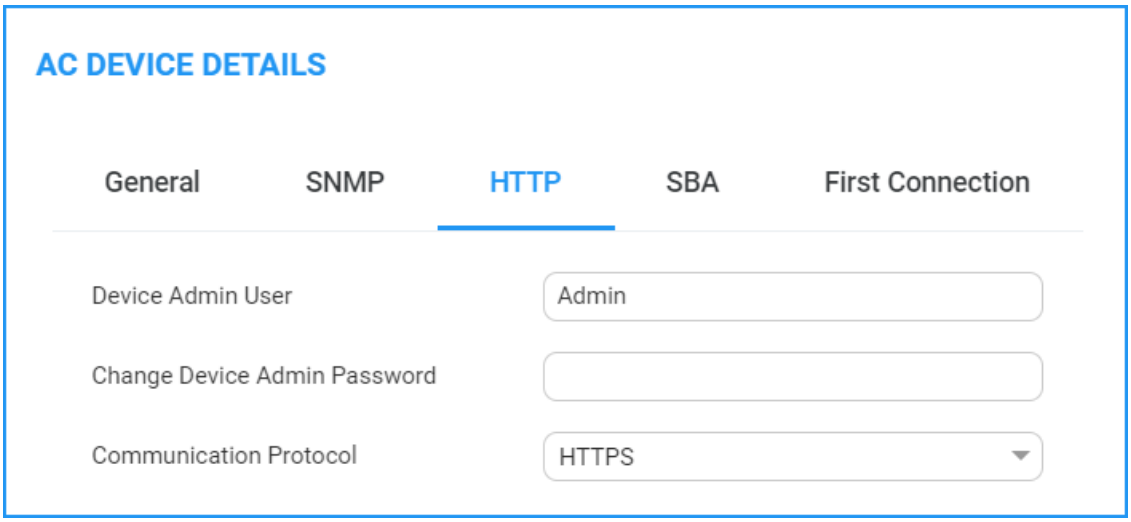


Figure 34-8: Device Details (Default HTTPS)



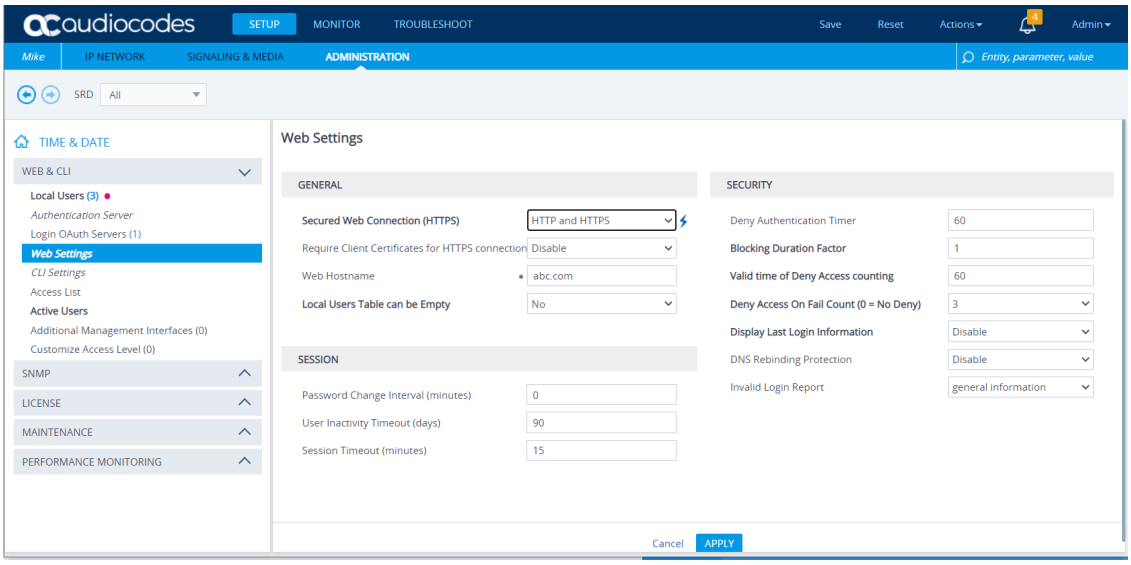
2. Create a new text file using a text-based editor (e.g., Notepad).
3. Enable mutual authentication on the device. This configuration instructs the Automatic Update mechanism to verify the TLS certificate received from the OVOC server.
   - For Media Gateway and SBC devices:

     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.
5. 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 Web Settings Page



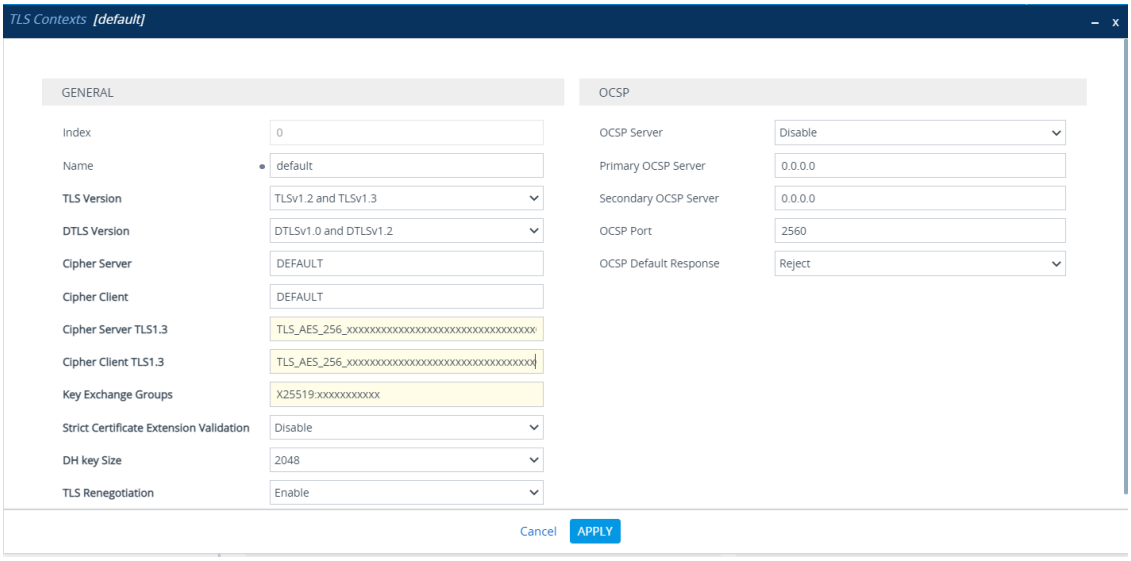
7. If you configured the SBC Devices Communication parameter to **Hostname-Based** in the OVOC Web, you must configure the parameter "Verify Certificate SubjectName" on the managed device (**Setup** Menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience Settings**).

Figure 34-10: Quality of Experience Settings

8. 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:

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:**

1. 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*.

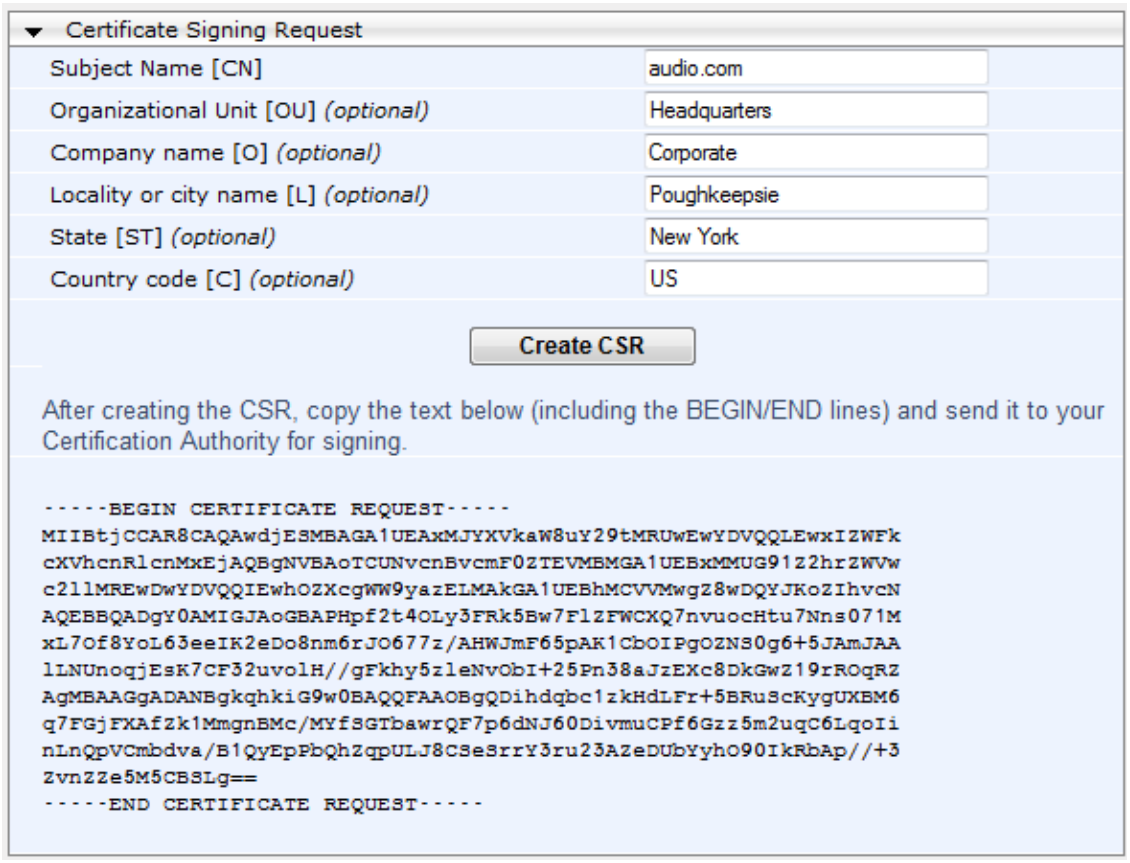
Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➢ **To generate a CSR:**

1. 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.
4. 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:

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
MDAwMFowPzELMAkGA1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpcG9zdGUxG
zAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZIhvcNAQE
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:**

1. 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
```

```
MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNfQ0EyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggwnlQiUYhOK
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/
0fmXKHWlPIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4yk
ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu
5B6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI
hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM
BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNV
HSMEQjBAgBThf6GbMQbO5b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM
MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcg
TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+
CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhlCq
hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO
RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V
XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBlO+np/O8F+P551uH0iOYA6Cc
Cj6oHGLq8RIndA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
```

```
MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhnUQrS
667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+7/q
ebESJyW8pTLTszGQns2E214+U18sKHItpUZvs1dVUIX6xQiSYFDG1CDIPR5/70pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOIp6LR72Ta9HMJFJ4gyxJPUQA
jV3Led2Y4JObvBTNlka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPUf1wRjDWgl4G
BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9lXI/HQkKRSTf8CAwEAAaN6MHgw
DAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAIYwSQYD
VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBAoTA0FD
TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggEBAHqkg4F6
wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFCz1q4QVpQNYAwdBdEAKENznZttoP3aPZE
3EOx1C8Mw2wU4pOxD7B6pH0XO+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:**

1. 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

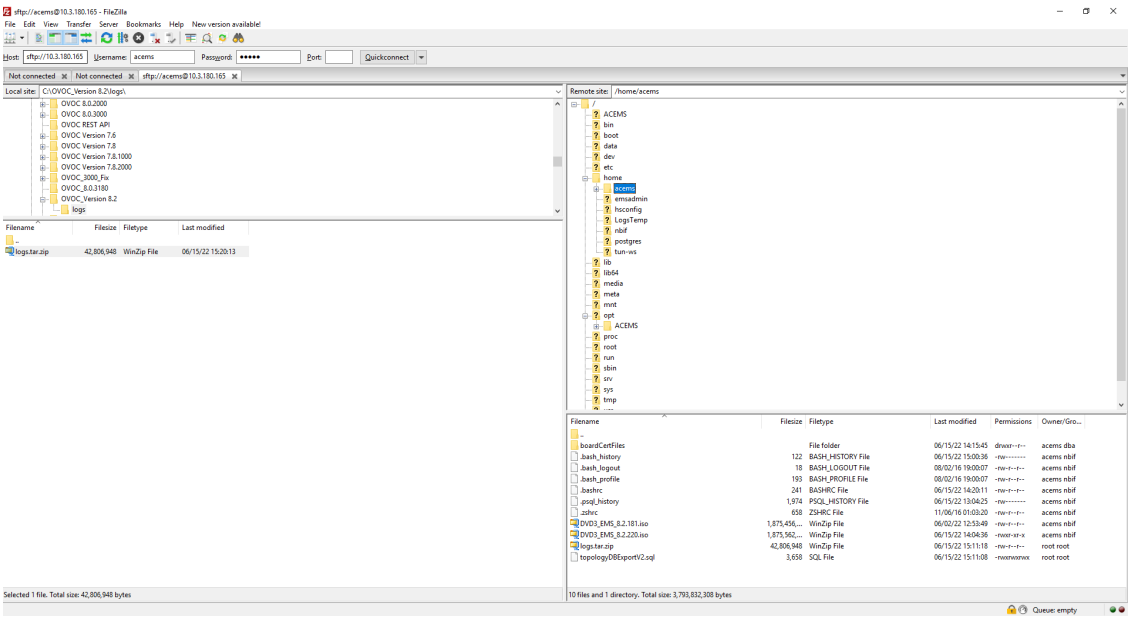
This appendix describes how to transfer files to and from the OVOC server using any SFTP/SCP file transfer application.

FTP by default is disabled on the OVOC server.

➢ 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

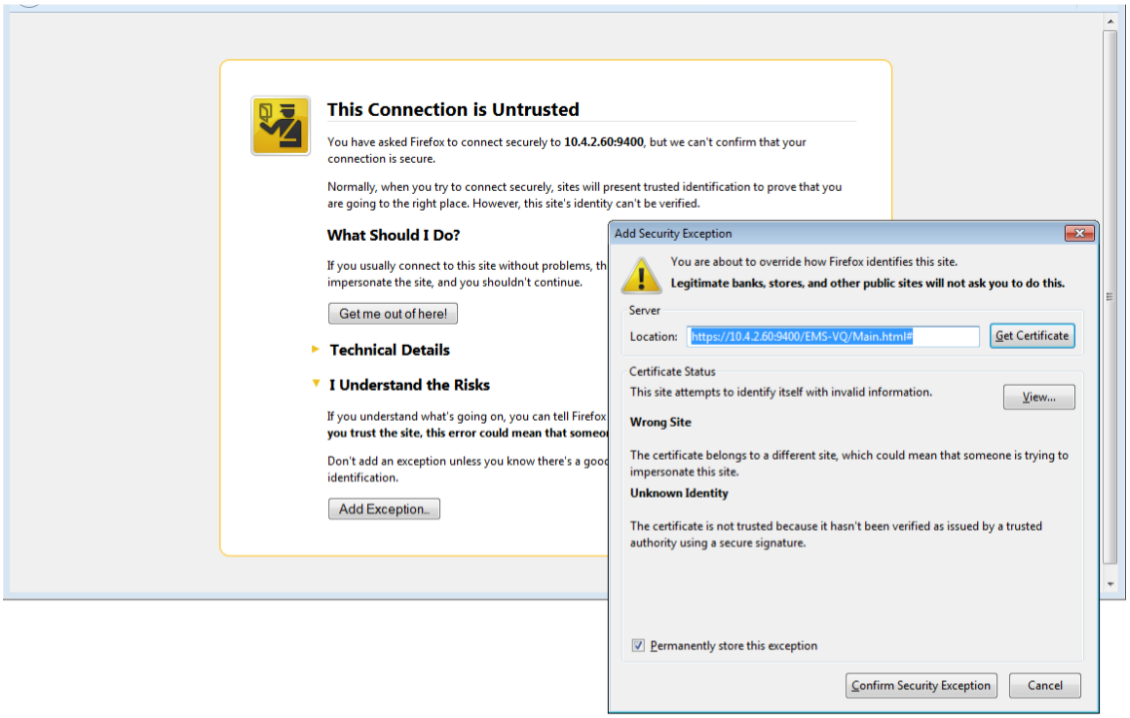
When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

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

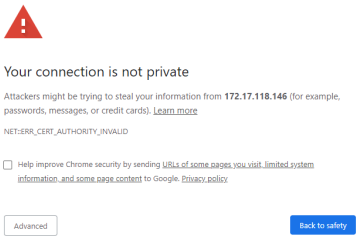


Google Chrome

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 37-2: Chrome Browser Settings



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

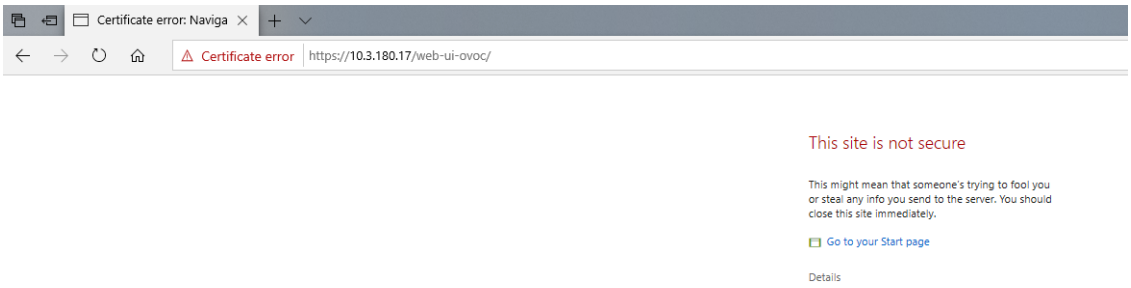
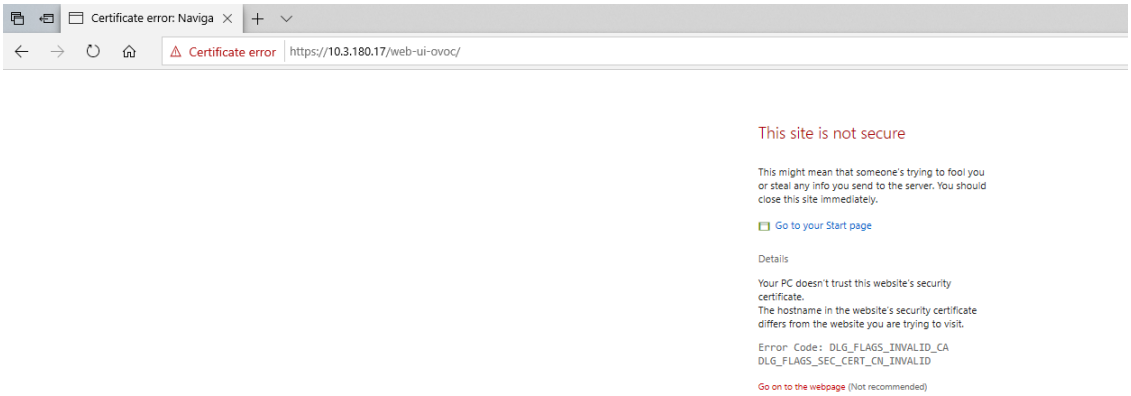


Figure 37-4: Go on to the Web Page



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.

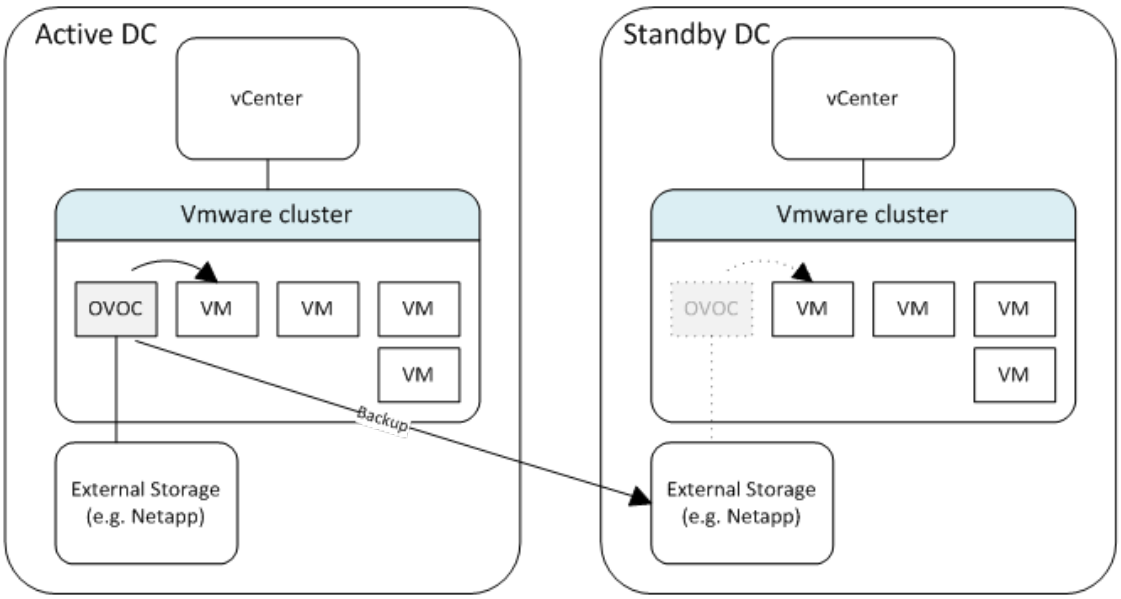
> Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

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.
6. 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.
11. 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

Document #: LTRT-94200