Installation, Operation and Maintenance Manual

AudioCodes One Voice Operations Center

OVOC

Installation, Operation and Maintenance

Version 8.2.3000

OVOC
One Voice Operations Center

audiocodes

Notice

Date Published: June-19-2024

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
94185	Updates for Version 8.2: Updates to Sections: Managed VoIP Equipment; OVOC Server Minimum Requirements; OVOC Server Users; OVOC Software Deliverables; Viewing Process Statuses; Viewing General Info; Service Provider Cluster; HTTPS SSL TLS Security; Syslog Server Configuration; Upgrading OVOC from ISO File; Upgrading OVOC from DVD; DVD3 OVOC Server Application; Configuring OVOC Cloud Architecture Mode; Configure OVOC Server with NAT IP Address per Interface; Configuring the Firewall; Transferring Files; Static Routes; OVOC License Added Sections: Select Logs; Postgres DB Password; Creating VMware VM using ESXi Wizard; Restore Backup Data to Separate Virtual Machine Updated, Moved and Renamed Section: Setting up Multiple Ethernet Interfaces; Microsoft Teams URLs Removed Sections: all related information to Service Provider cluster (not supported in this release).
94186	Updates for Version 8.2: Updates to Sections: analytics API; OVOC Server Users; Configuring OVOC Web Interface for Tunnel Mode.
94188	Updates for Version 8.2.1000: Added Sections: Deploying Older OVOC Versions using PowerShell; Updated Sections: Managed VoIP Equipment; OVOC Server Minimum Requirements; OVOC Capacities; Voice Quality Bandwidth Requirements; OVOC Software Deliverables; Creating OVOC Virtual Machine on Microsoft Azure; Proxy Settings; Collecting Logs; Selected Logs; OVOC Server Backup

LTRT	Description
	Processes
94189	Updates to Section: Devices Syslog Configuration; Configuring Internal Azure Mail Server on Microsoft Office 365; Full Restore Added Section: Host Header Validation Configuration.
94190	Updates: Clarification of TLSv.12 as default TLS version (Section OVOC Server Manager Menu Options Summary, HTTPS SSL TLS Security and HTTP Security Settings Menu Options). Syntax corrections for instructing to press Enter after typing OVOC Server Manager menu options; Supported VoIP Equipment (MSBR Version 7.26.xx).
94191	Update for Device Manager firewall ports (Section Configuring the Firewall).
94192	Removed Section "Installing the OVOC Server on OpenStack". Installation of OVOC server on the OpenStack platform **is not supported**.
94193	Added Sections: Elastic Search DB Password; VMware Tools Updated Sections: Managed VoIP Equipment; Hardware and Software Requirements; Upgrade; Configuring the Firewall (for OVOC Device Manager ports)
94194	Updated Section: Proxy Settings
94195	Updates to the Firewall tables for Device Manager managed devices connections.
94196	Updates to Capacities table; Managing Device Connections; analytics API; Firewall diagram; Northbound Interfaces Flows table; Collect Logs Added new section Device Manager Communication and Optimization

Table of Contents

This page is intentionally left blank.

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
Generic Applications	
Fax and Auto-Attendant (IVR)	Version 2.6.200
Microsoft Teams Direct Routing SBA	
Mediant 800B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 800C DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 1000B DR-SBA	SBA Versions 1.0.1xx and later, 1.0.22 and 1.0.21 with SBC certified by Microsoft.
Mediant 2600B DR-SBA	SBA Version 1.0.1xx and later with SBC certified by Microsoft.
Mediant DR-SBA Virtual Appliance	SBA Version 1.0.1x.x and later with SBC certified by Microsoft.
AudioCodes Routing Manager (ARM)	Version 9.8
Device Management	
400HD Series Lync server	From Version 2.0.13: 420HD, 430HD 440HD

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

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

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-Linux CentOS Operating System ■ DVD3-OVOC Software Installation
VMware	DVD5-OVOC Software Installation OVA file
HyperV	■ DVD5-OVOC Software Installation 7z file
Amazon AWS	■ Create OVOC instance from Public AMI image provided by AudioCodes
Microsoft Azure	■ Create OVOC virtual machine from Azure Marketplace.
Upgrade	
Dedicated	■ DVD3-OVOC Server Application DVD OR ■ DVD3-OVOC Server Application ISO file
Microsoft HyperV	■ DVD3-OVOC Server Application ISO file
Amazon AWS	■ DVD3-OVOC Server Application ISO file

Note the following

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

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

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

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

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

Part II

OVOC Server Installation

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

5 Files Verification

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

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

Windows

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

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

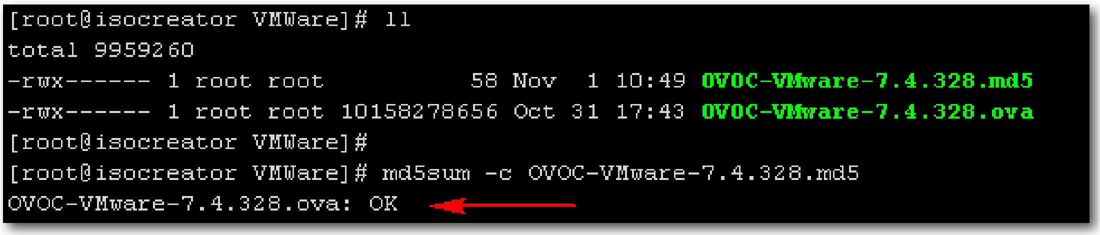
Linux

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

```
md5sum -c filename.md5
```

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

Figure 5-1: ISO File Integrity Verification



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

OVOC Server Users

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

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

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

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

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

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

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

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

Launching Public OVOC Image on Amazon Web Services (AWS)

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

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

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

Launching Public Image on AWS

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

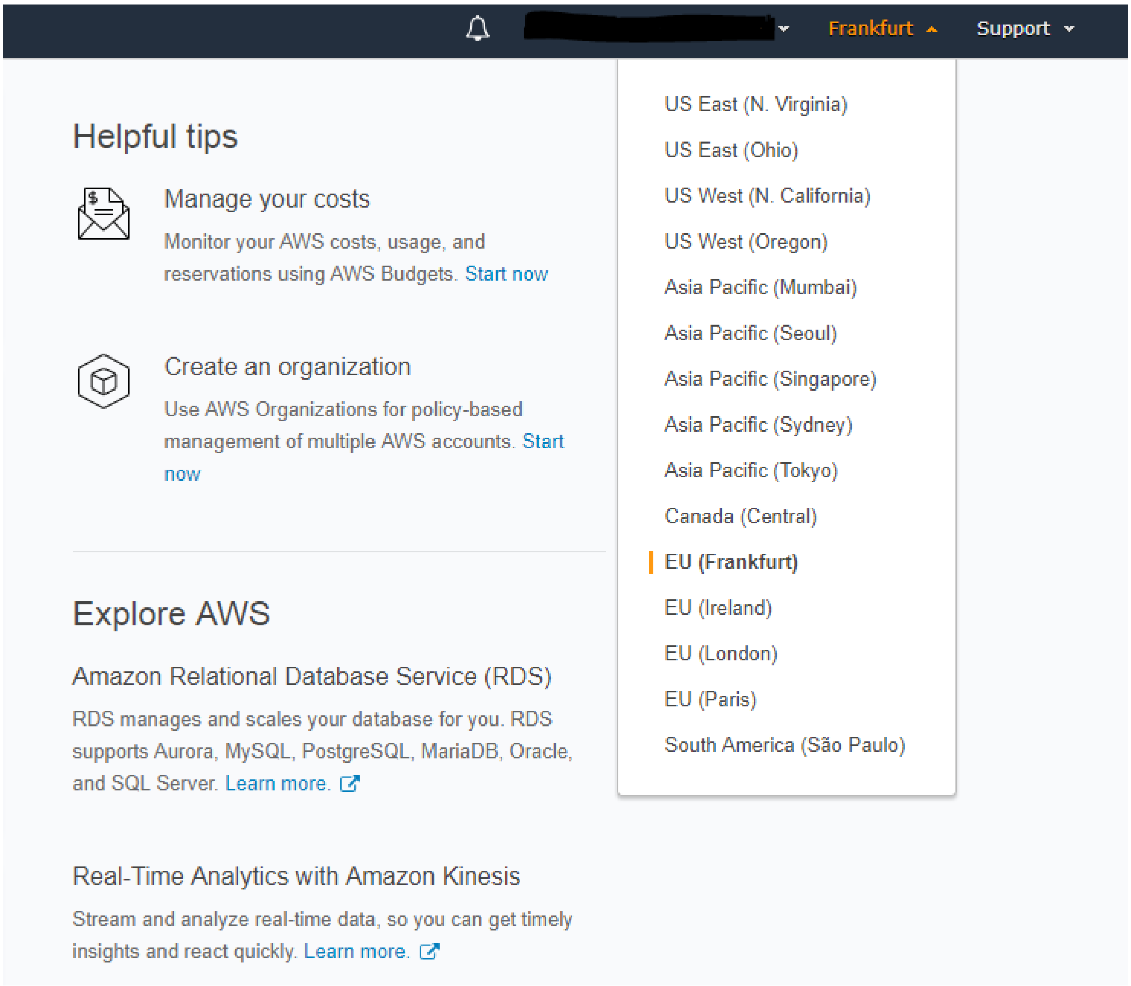
➢ **To setup and load the AWS image:**

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

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

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

Figure 6-1: Select Region



Helpful tips

Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

Amazon Relational Database Service (RDS)

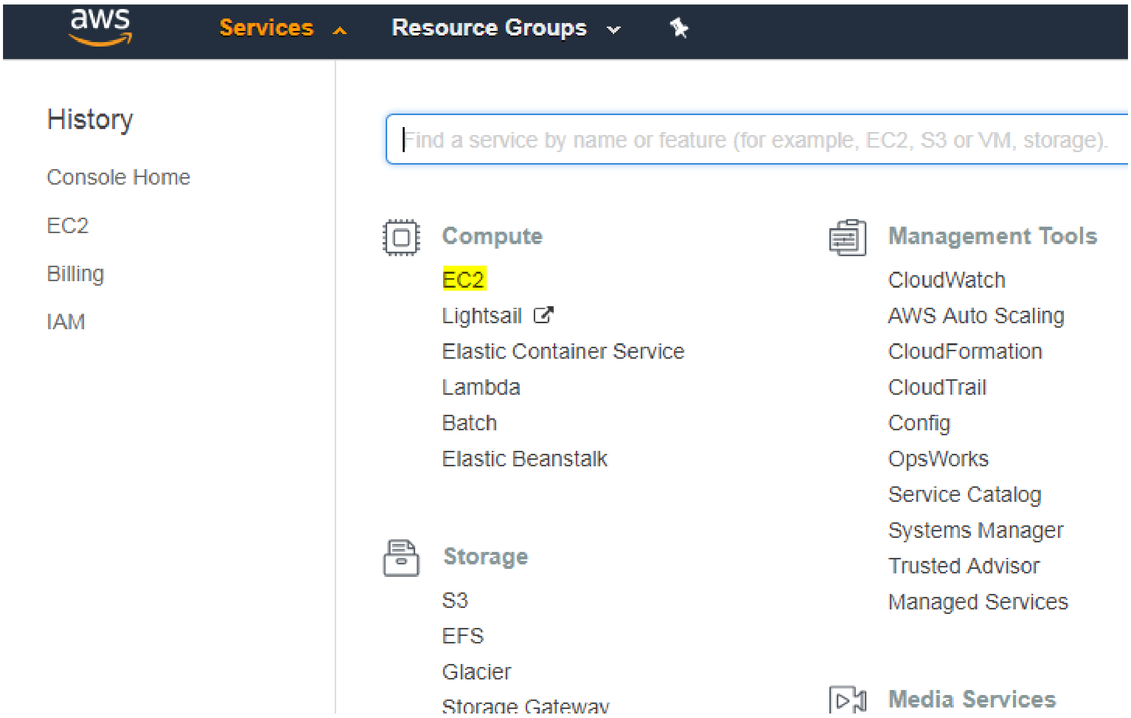
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

Real-Time Analytics with Amazon Kinesis

Stream and analyze real-time data, so you can get timely insights and react quickly. Learn more.

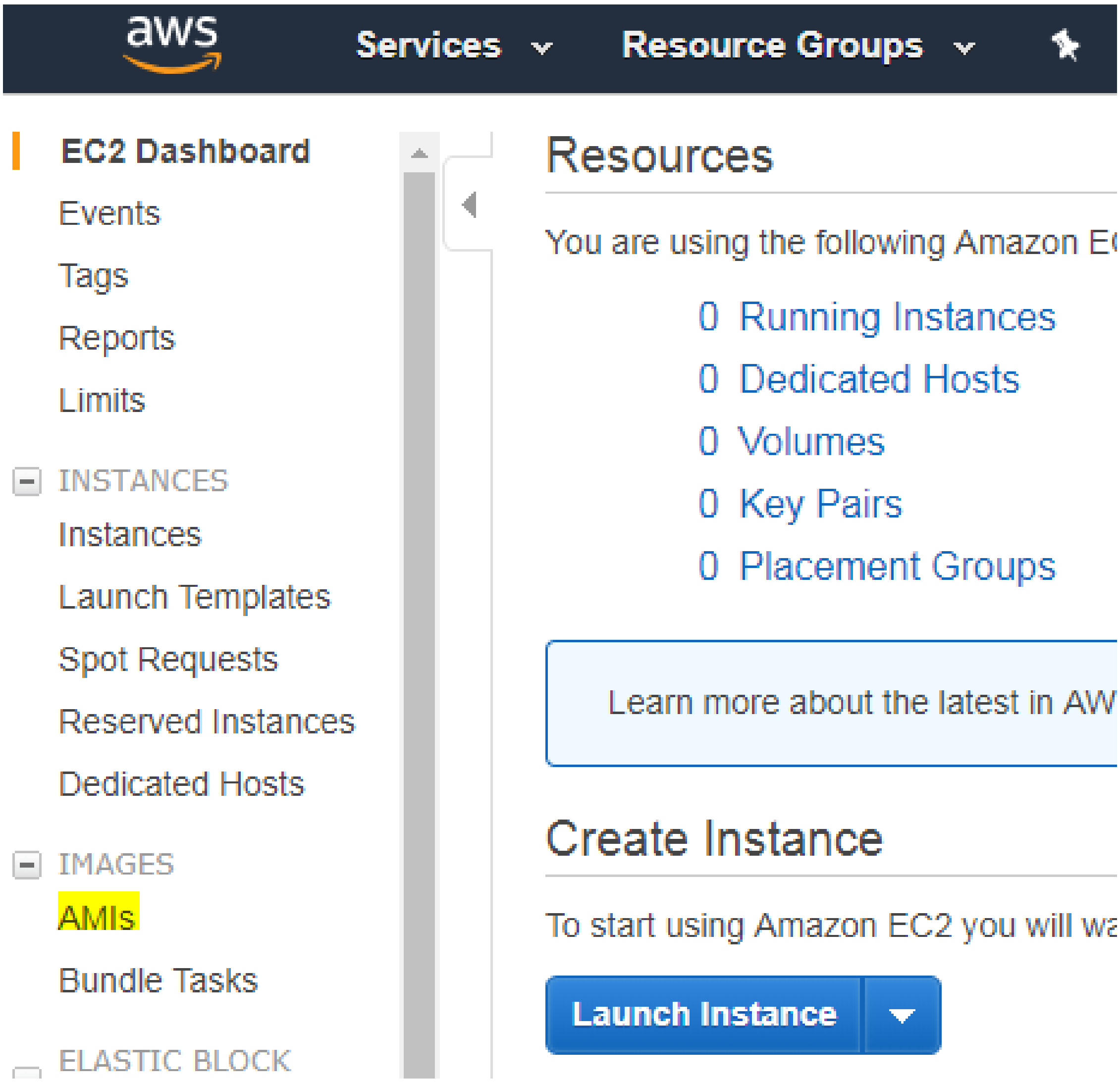
3. In the "Services" menu, choose EC2.

Figure 6-2: Services Menu - EC2



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

Figure 6-3: Images

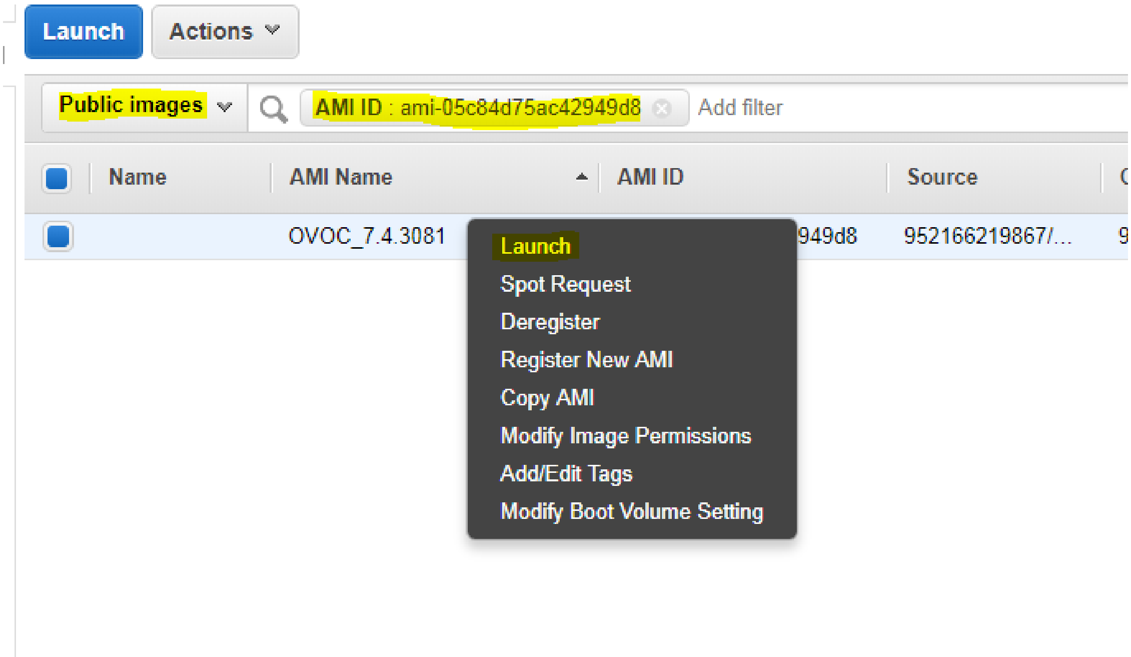


5. In the search bar, choose Public images and apply the following filter:

   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:

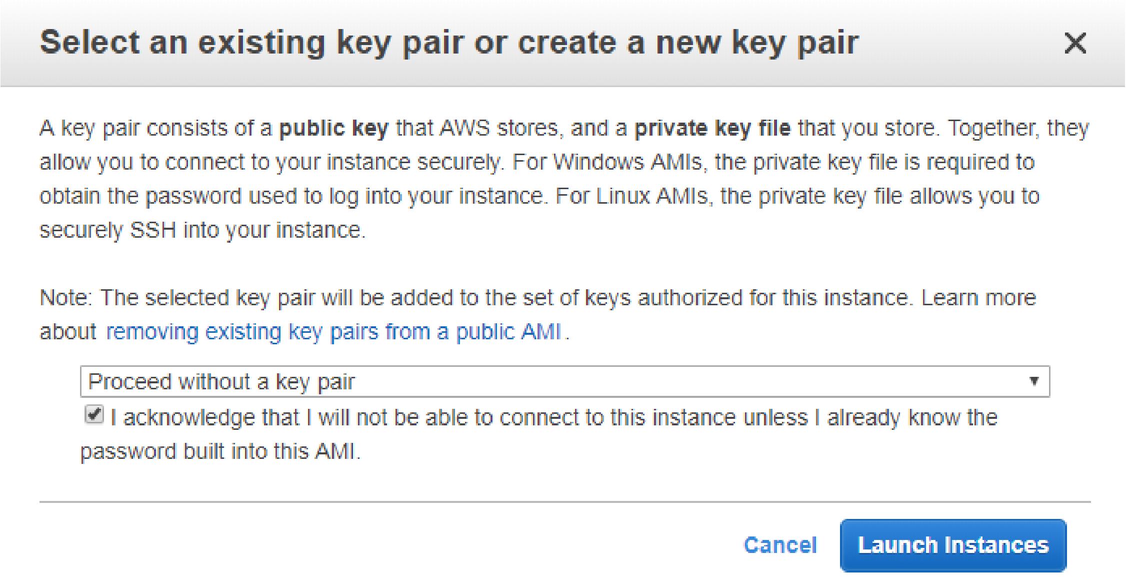
Table 6-1: Firewall for Amazon AWS

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 166

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



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

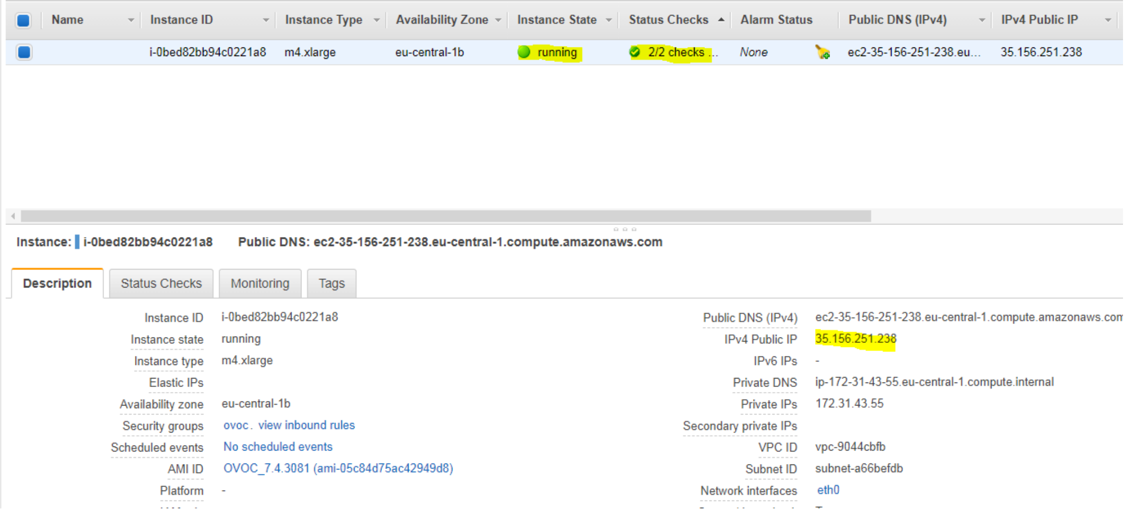
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Proceed without a key pair ▾

☑ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

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



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-0bed82bb94c0221a8	m4.xlarge	eu-central-1b	running	2/2 checks ...	None	ec2-35-156-251-238.eu...	35.156.251.238

Instance: i-0bed82bb94c0221a8 **Public DNS: ec2-35-156-251-238.eu-central-1.compute.amazonaws.com**

Instance ID	i-0bed82bb94c0221a8	Public DNS (IPv4)	ec2-35-156-251-238.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	35.156.251.238
Instance type	m4.xlarge	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-43-55.eu-central-1.compute.internal
Availability zone	eu-central-1b	Private IPs	172.31.43.55
Security groups	ovoc . view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-9044cbfb
AMI ID	OVOC_7.4.3081 (ami-05c84d75ac42949d8)	Subnet ID	subnet-a66befdb
Platform	-	Network interfaces	eth0

Note the AWS public IP address as its later configured in Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS on page 167

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

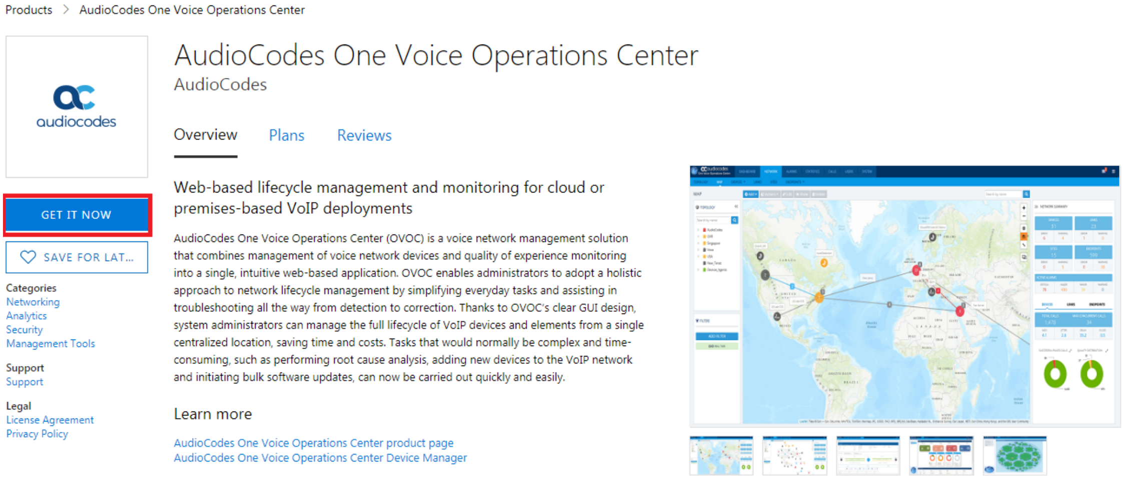
This chapter describes how to install the OVOC server on a virtual machine in a Cloud-based deployment from the Microsoft Azure Marketplace.

- 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


Products > AudioCodes One Voice Operations Center

AudioCodes One Voice Operations Center
AudioCodes

Overview Plans Reviews

GET IT NOW

SAVE FOR LAT...

Categories
Networking
Analytics
Security
Management Tools

Support
Support

Legal
License Agreement
Privacy Policy

Web-based lifecycle management and monitoring for cloud or premises-based VoIP deployments

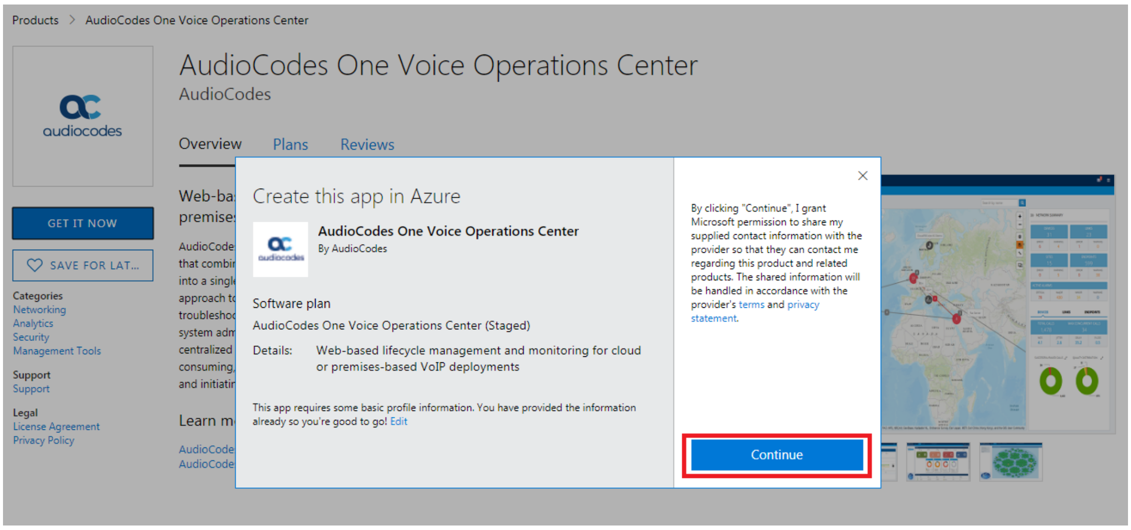
AudioCodes One Voice Operations Center (OVOC) is a voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application. OVOC enables administrators to adopt a holistic approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction. Thanks to OVOC's clear GUI design, system administrators can manage the full lifecycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks that would normally be complex and time-consuming, such as performing root cause analysis, adding new devices to the VoIP network and initiating bulk software updates, can now be carried out quickly and easily.

Learn more

AudioCodes One Voice Operations Center product page
AudioCodes One Voice Operations Center Device Manager

2. Click **Continue.**

Figure 6-8: Create this App in Azure


Create this app in Azure

AudioCodes One Voice Operations Center
By AudioCodes

Software plan
AudioCodes One Voice Operations Center (Staged)

Details: Web-based lifecycle management and monitoring for cloud or premises-based VoIP deployments

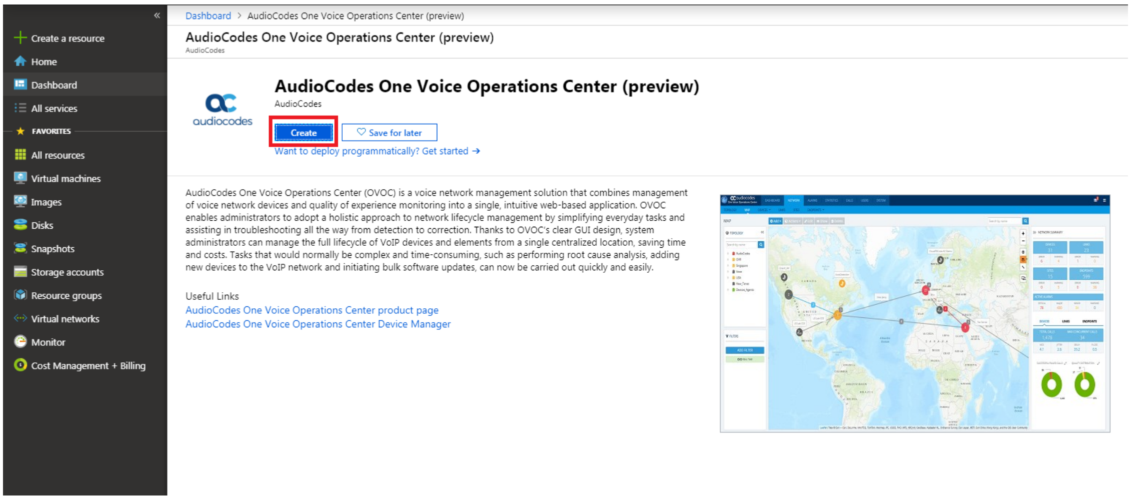
This app requires some basic profile information. You have provided the information already so you're good to go! Edit

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's terms and privacy statement.

Continue

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

Figure 6-9: Create Virtual Machine



Dashboard > AudioCodes One Voice Operations Center (preview)

AudioCodes One Voice Operations Center (preview)
AudioCodes

AudioCodes One Voice Operations Center (preview)
AudioCodes

Create Save for later
Want to deploy programmatically? Get started →

AudioCodes One Voice Operations Center (OVOC) is a voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application. OVOC enables administrators to adopt a holistic approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction. Thanks to OVOC's clear GUI design, system administrators can manage the full lifecycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks that would normally be complex and time-consuming, such as performing root cause analysis, adding new devices to the VoIP network and initiating bulk software updates, can now be carried out quickly and easily.

Useful Links
AudioCodes One Voice Operations Center product page
AudioCodes One Voice Operations Center Device Manager

4. Configure the following:

   a. Choose your Subscription.

   b. Choose your Resource Group or create a new one

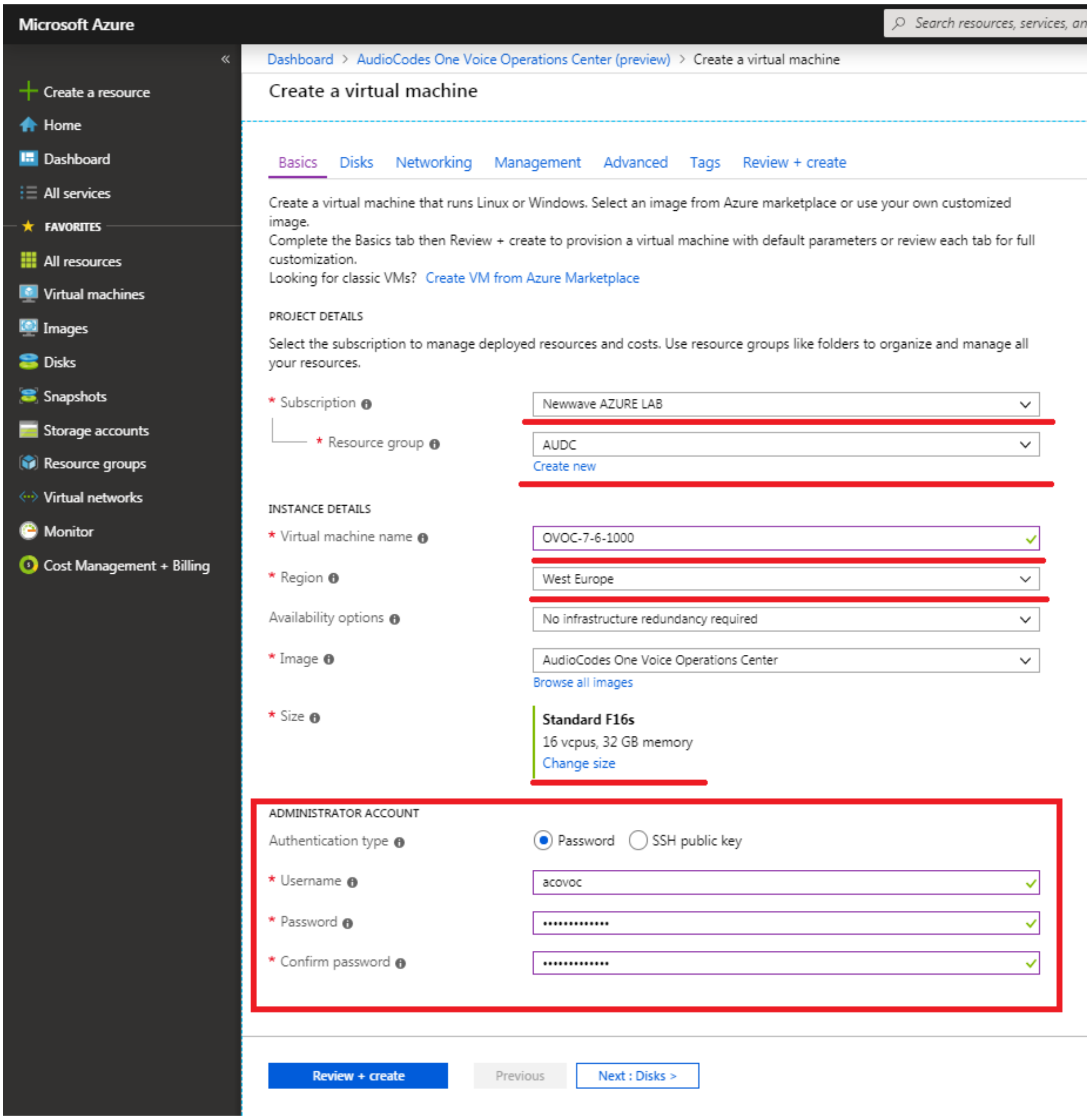
   c. Enter the name of the new Virtual Machine.

   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



Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

- * Subscription: Newwave AZURE LAB
- * Resource group: AUDC (Create new)

INSTANCE DETAILS

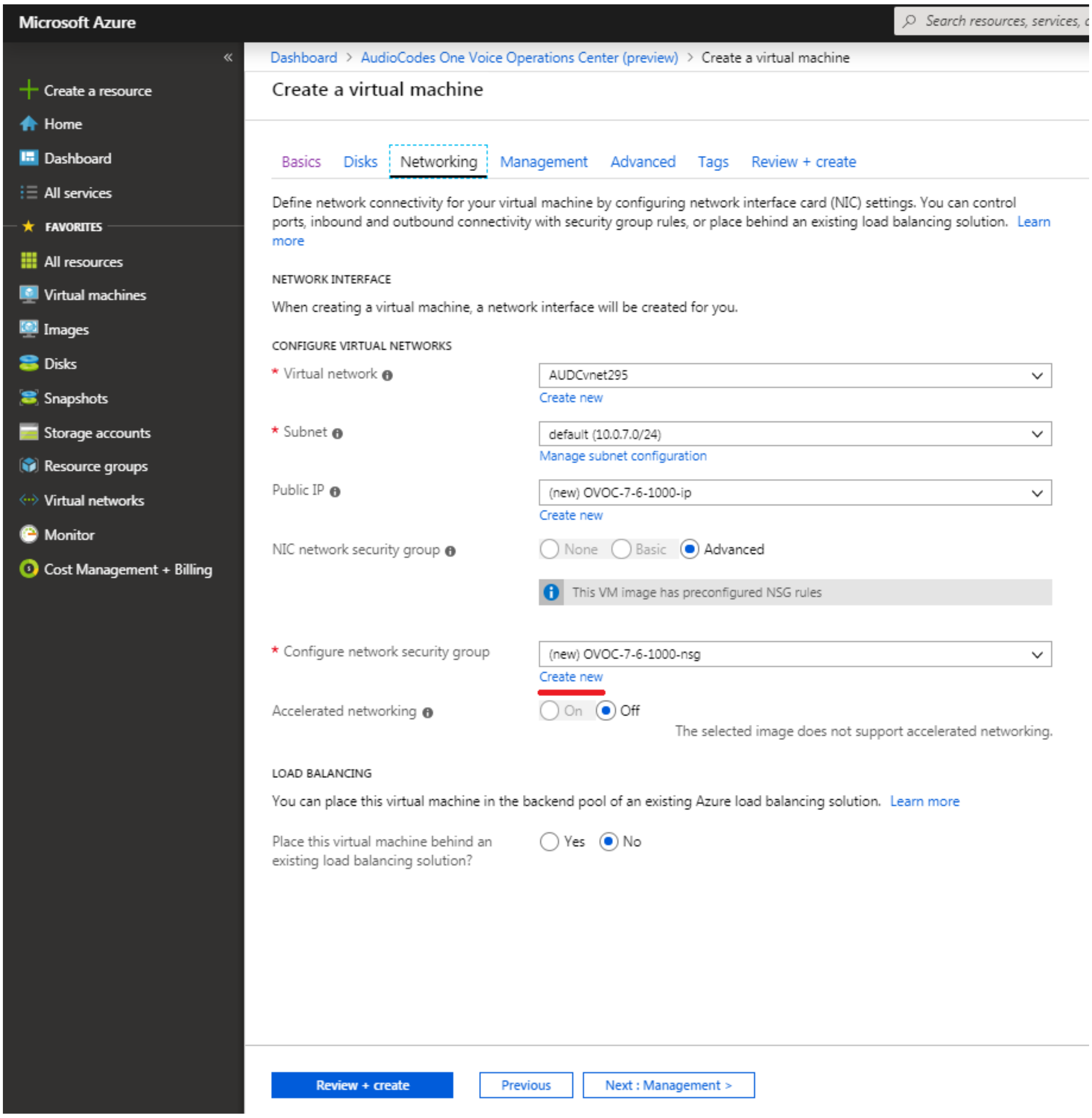
- * Virtual machine name: OVOC-7-6-1000
- * Region: West Europe
- Availability options: No infrastructure redundancy required
- * Image: AudioCodes One Voice Operations Center (Browse all images)
- * Size: **Standard F16s** 16 vcpus, 32 GB memory (Change size)

ADMINISTRATOR ACCOUNT

- Authentication type: ● Password ○ SSH public key
- * Username: acovoc
- * Password: •••••••••••••
- * Confirm password: •••••••••••••

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

Figure 6-11: Network Settings



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network: AUDCvnet295 (Create new)

* Subnet: default (10.0.7.0/24) (Manage subnet configuration)

Public IP: (new) OVOC-7-6-1000-ip (Create new)

NIC network security group: ○ None ○ Basic ● Advanced

This VM image has preconfigured NSG rules

* Configure network security group: (new) OVOC-7-6-1000-nsg (Create new)

Accelerated networking: ○ On ● Off

The selected image does not support accelerated networking.

LOAD BALANCING

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

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.

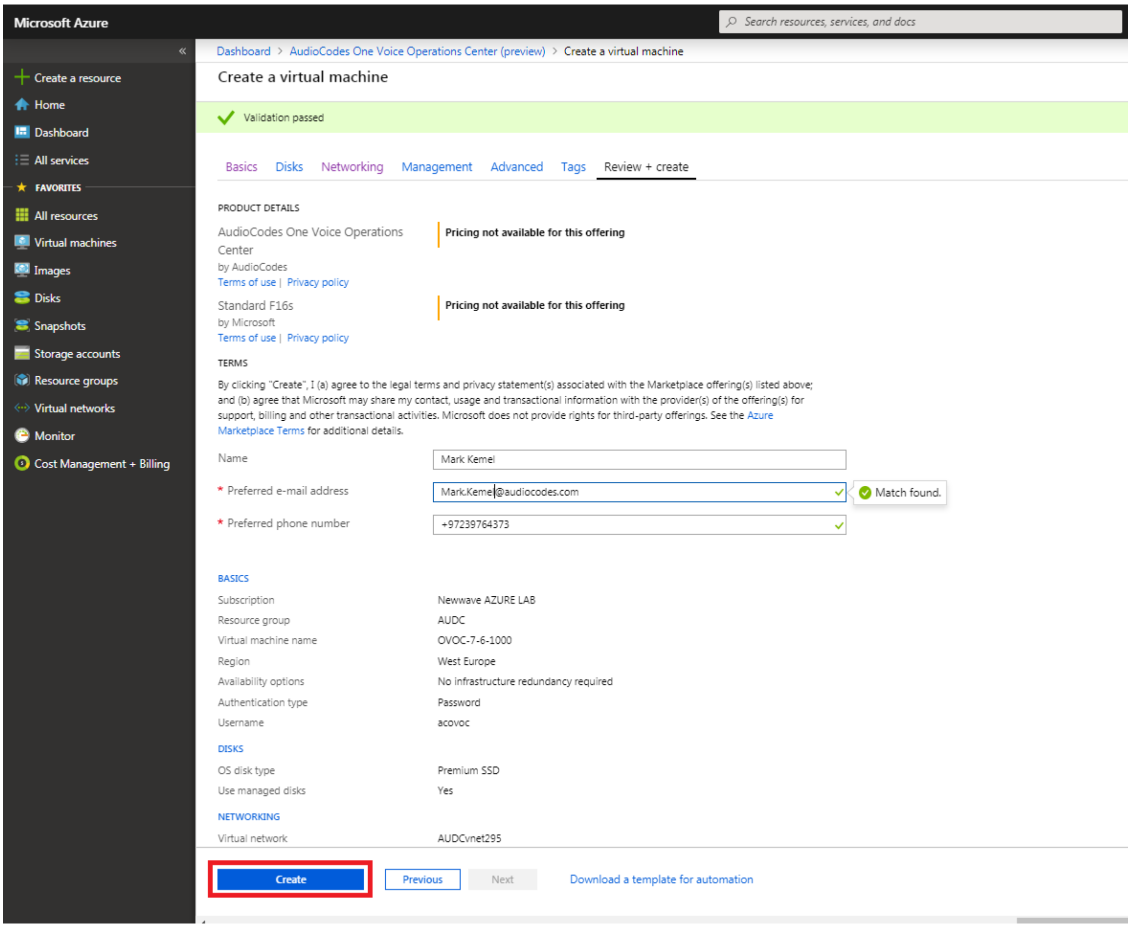
⚠ By default, only ports 22 and 443 are open for inbound traffic; open other ports for managing devices behind a NAT (outside the Azure environment) as described in the table below.

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 159
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 159
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 158

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

Figure 6-12: Review and Create



Create a virtual machine

✓ Validation passed

PRODUCT DETAILS

AudioCodes One Voice Operations Center
by AudioCodes
Terms of use | Privacy policy

Pricing not available for this offering

Standard F16s
by Microsoft
Terms of use | Privacy policy

Pricing not available for this offering

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; and (b) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

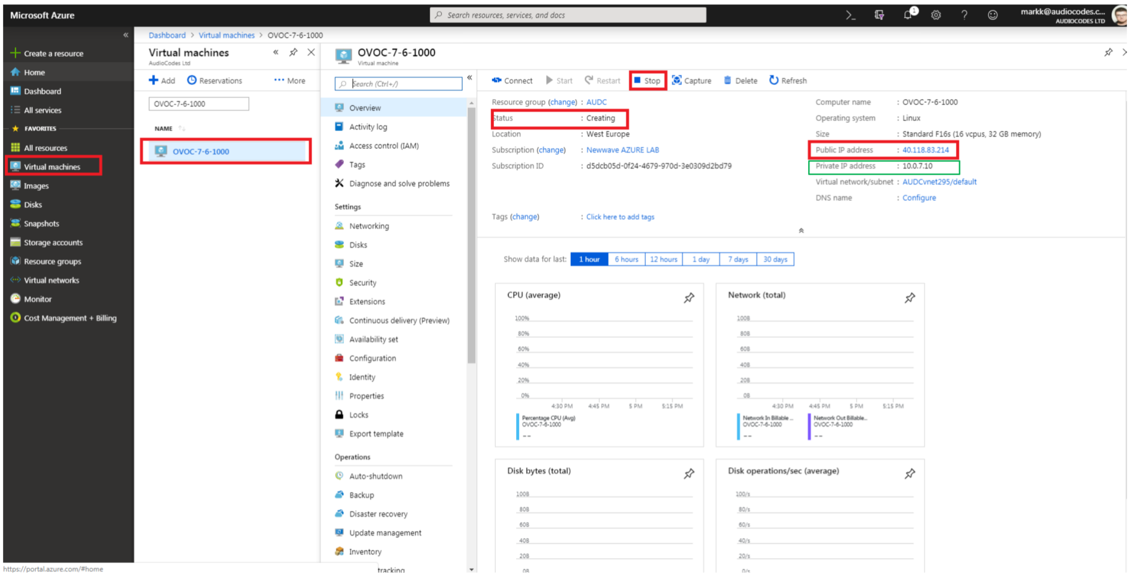
Name	Mark Kemel
* Preferred e-mail address	Mark.Kemel@audiocodes.com ✓ Match found.
* Preferred phone number	+97239764373 ✓

BASICS	
Subscription	Newwave AZURE LAB
Resource group	AUDC
Virtual machine name	OVOC-7-6-1000
Region	West Europe
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	acovoc
DISKS	
OS disk type	Premium SSD
Use managed disks	Yes
NETWORKING	
Virtual network	AUDCvnet295

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 159 and Configuring the OVOC Server Manager on Azure (Internal IP) on page 163 respectively.

Figure 6-13: Azure Deployment Process Complete



Resource group (change) : AUDC
Status : Creating
Location : West Europe
Subscription (change) : Newwave AZURE LAB
Subscription ID : d5dcb05d-0f24-4679-970d-3e0309d2bd79
Tags (change) : Click here to add tags

Computer name : OVOC-7-6-1000
Operating system : Linux
Size : Standard F16s (16 vcpus, 32 GB memory)
Public IP address : 40.118.83.214
Private IP address : 10.0.7.10
Virtual network/subnet : AUDCvnet295/default
DNS name : Configure

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

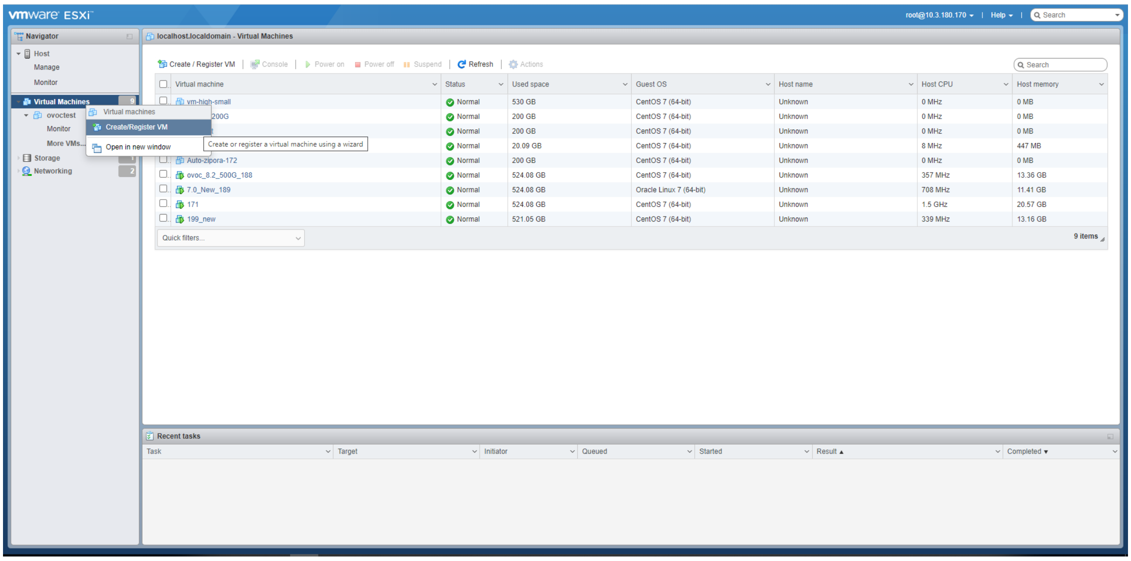
Deploying Standalone VMware VM using ESXi Wizard

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 326 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

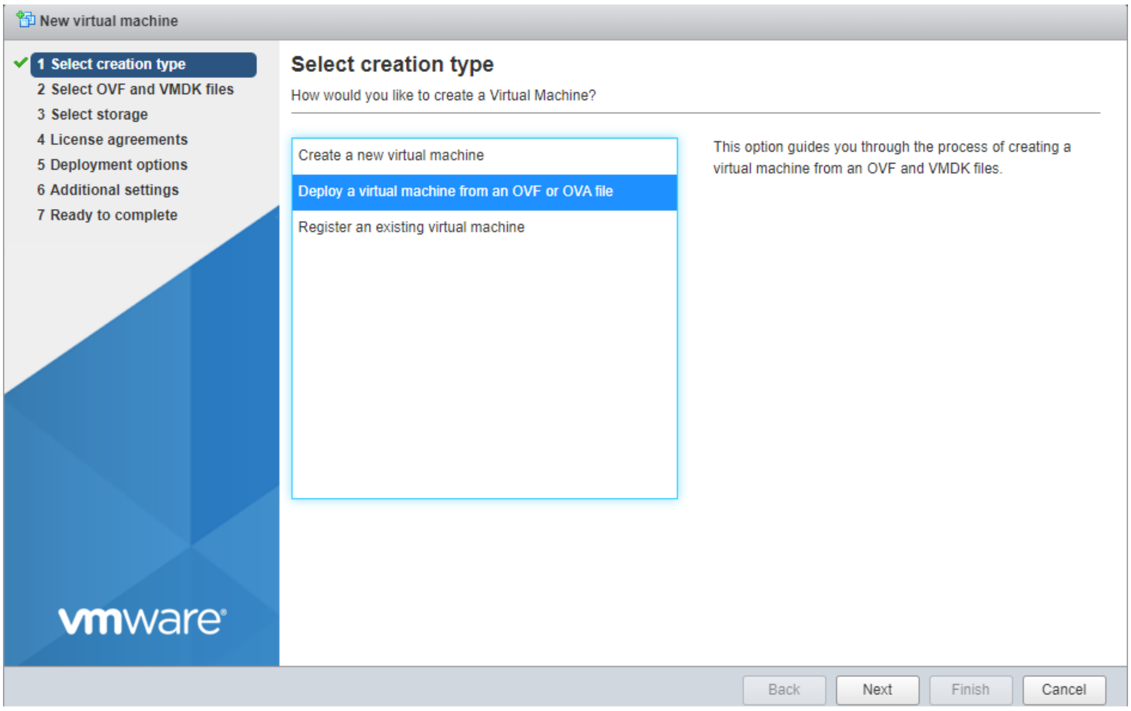


vmware ESXi
root@10.3.180.170 | Help | Search
Navigator
Host
Manage
Monitor
Virtual Machines 9
ovoctest
Monitor
More VMs...
Storage 1
Networking 2
Virtual machines
Create/Register VM
Open in new window
Create or register a virtual machine using a wizard
localhost.localdomain - Virtual Machines
Create / Register VM | Console | Power on | Power off | Suspend | Refresh | Actions
Search
Quick filters...
9 items
Recent tasks
Task | Target | Initiator | Queued | Started | Result ▲ | Completed ▼

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
vm-high-small	Normal	530 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
200G	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
t	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
	Normal	20.09 GB	CentOS 7 (64-bit)	Unknown	8 MHz	447 MB
Auto-zipora-172	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
ovoc_8.2_500G_188	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	357 MHz	13.36 GB
7.0_New_189	Normal	524.08 GB	Oracle Linux 7 (64-bit)	Unknown	708 MHz	11.41 GB
171	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	1.5 GHz	20.57 GB
199_new	Normal	521.05 GB	CentOS 7 (64-bit)	Unknown	339 MHz	13.16 GB

The New virtual machine wizard opens.

Figure 7-2: Select Creation Type



Select creation type

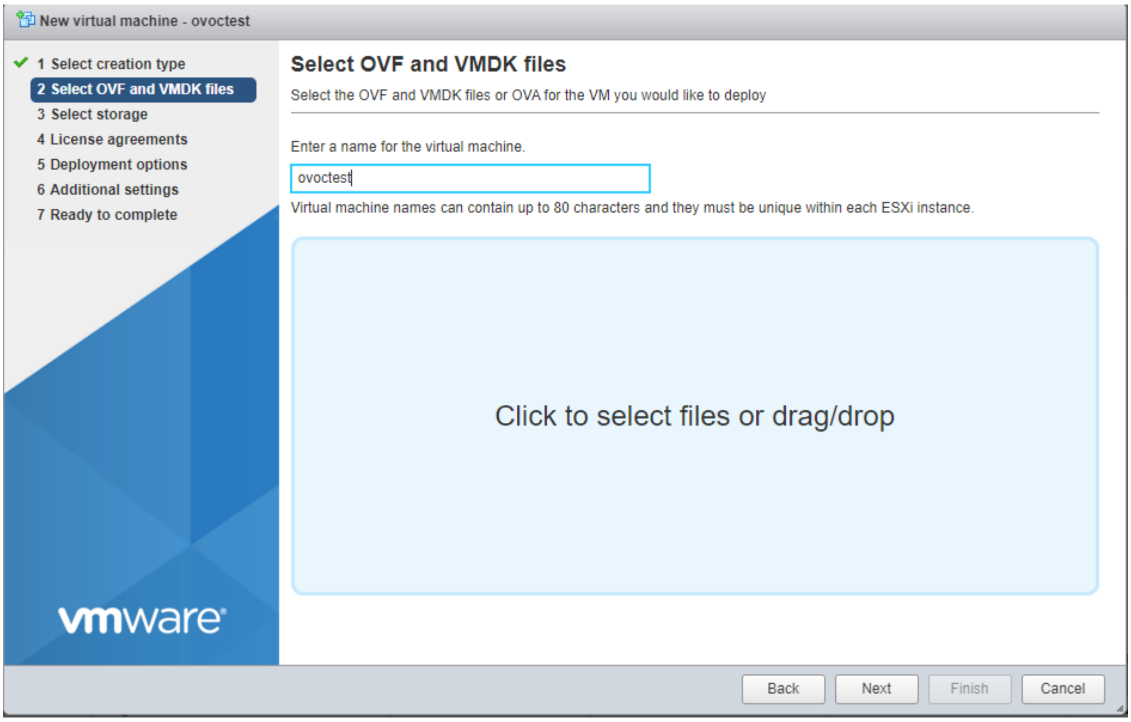
How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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

Figure 7-3: OVF and VMDK Files



New virtual machine - ovoctest

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

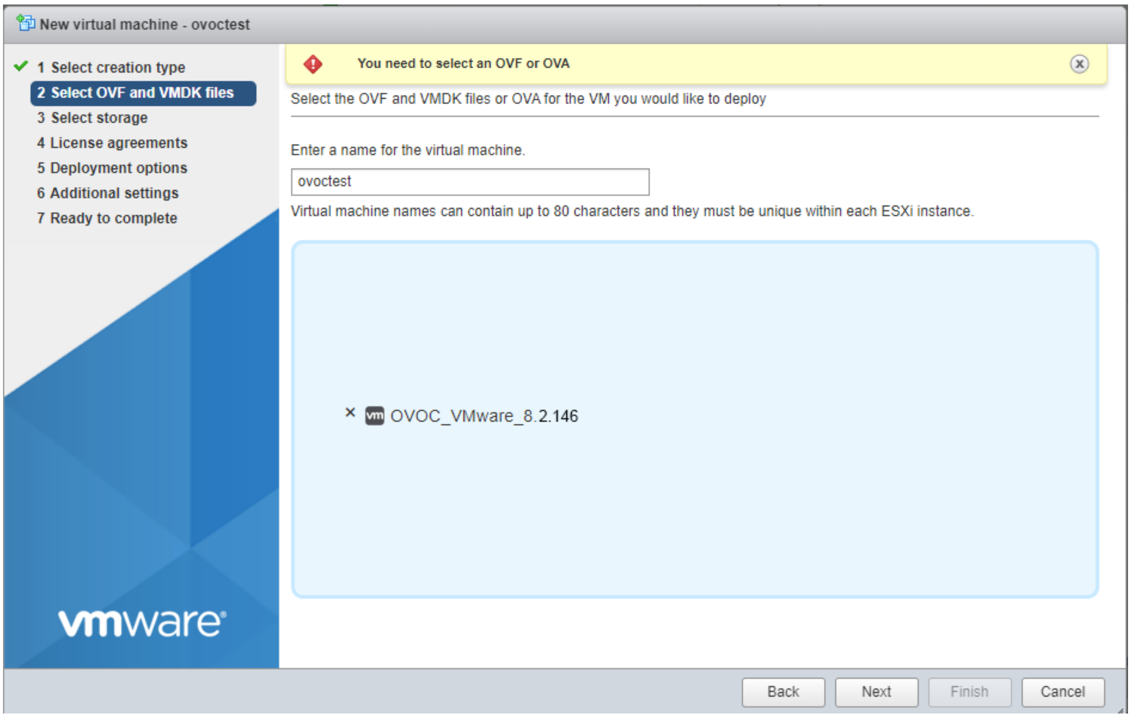
ovoctest

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Click to select files or drag/drop

5. Enter the name of the virtual machine.

Figure 7-4: Select OVF or OVA



New virtual machine - ovoctest

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

You need to select an OVF or OVA

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

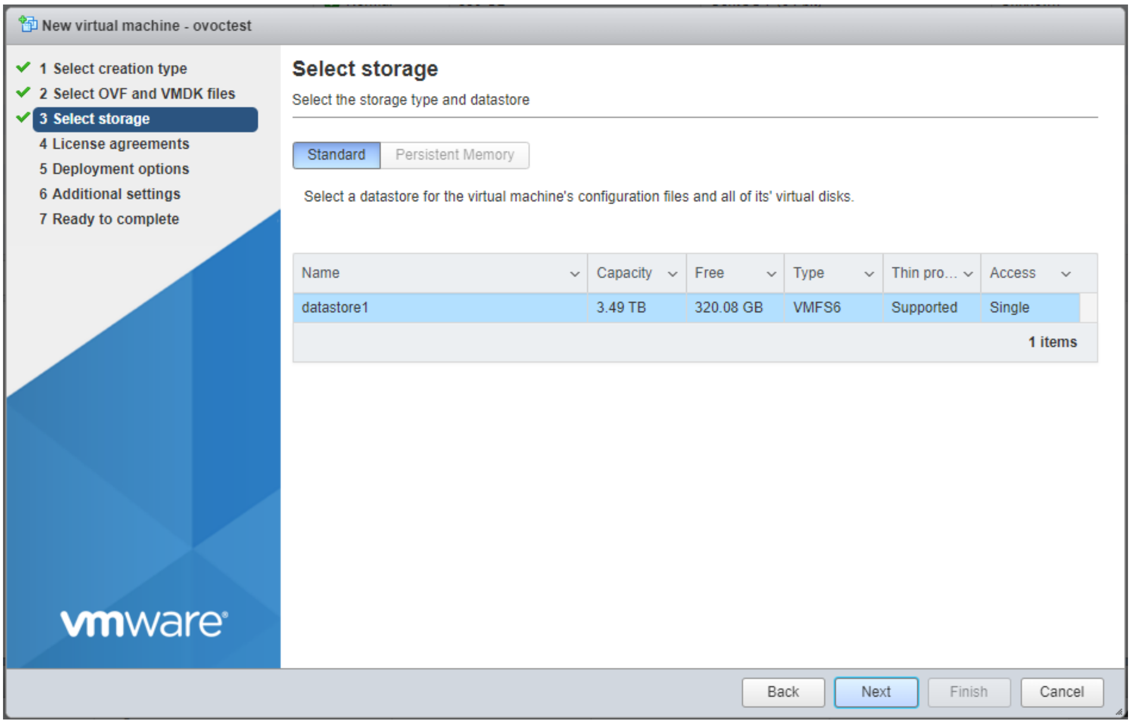
ovoctest

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× OVOC_VMware_8.2.146

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

Figure 7-5: Select storage



New virtual machine - ovoctest

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the storage type and datastore

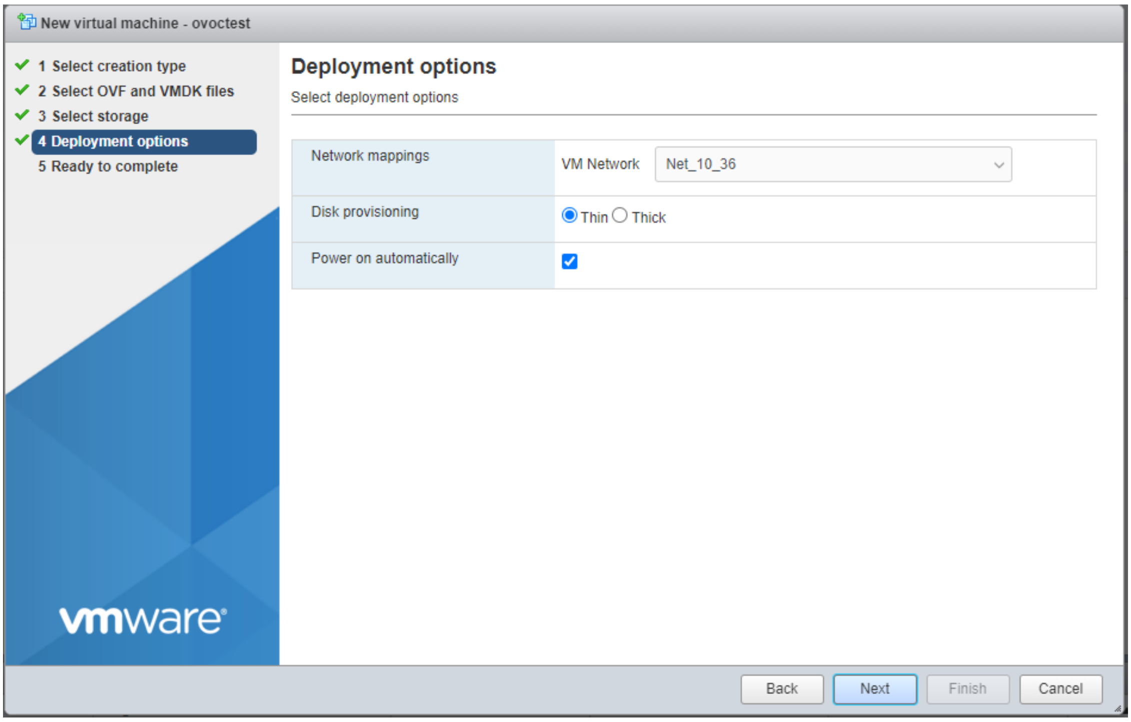
Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	3.49 TB	320.08 GB	VMFS6	Supported	Single

1 items

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

Figure 7-6: Deployment options



New virtual machine - ovoctest

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

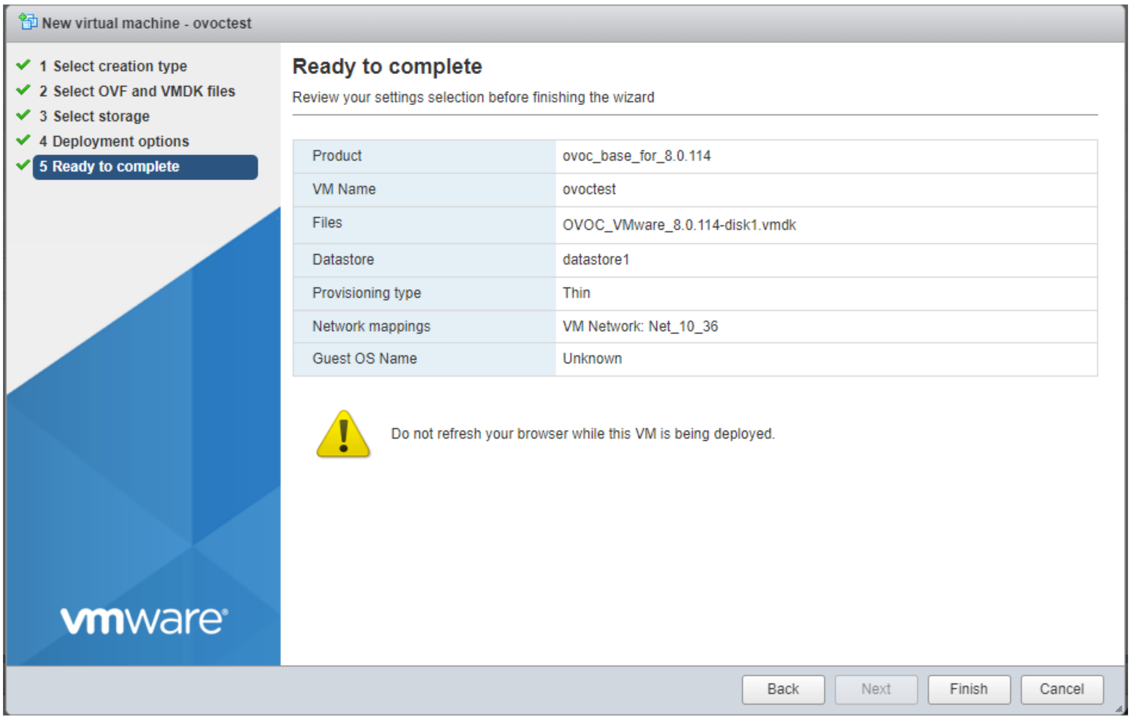
Select deployment options

Network mappings	VM Network Net_10_36
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

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



Ready to complete

Review your settings selection before finishing the wizard

Product	ovoc_base_for_8.0.114
VM Name	ovoctest
Files	OVOC_VMware_8.0.114-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: Net_10_36
Guest OS Name	Unknown

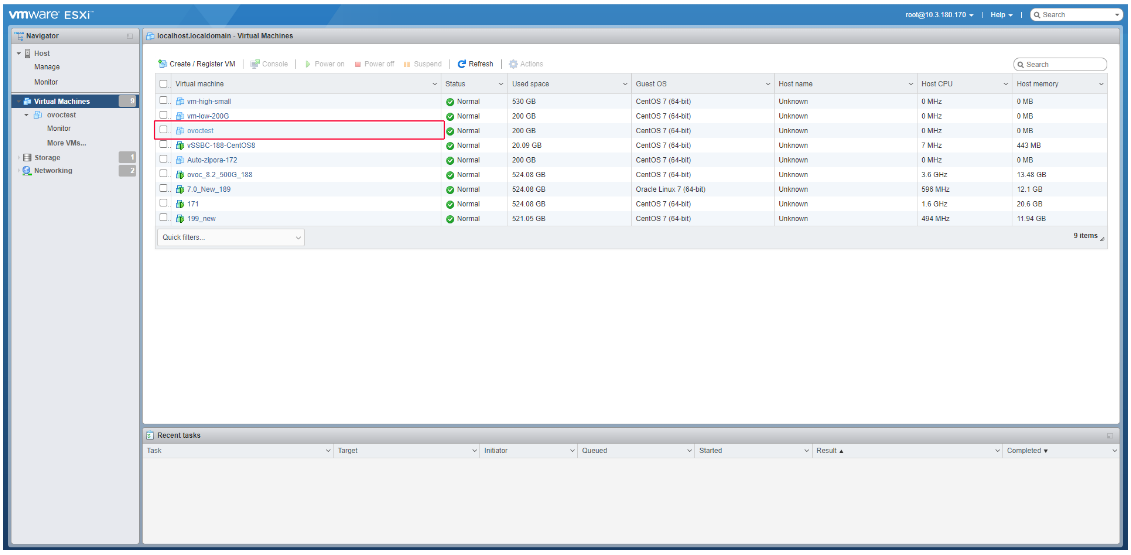
Do not refresh your browser while this VM is being deployed.

9. Click **Finish**.

   The new Virtual Machine is displayed.

Figure 7-8: New Virtual Machine Created

Figure 7-9:



Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
vm-high-small	Normal	530 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
vm-low-200G	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
ovoctest	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
vSSBC-188-CentOS8	Normal	20.09 GB	CentOS 7 (64-bit)	Unknown	7 MHz	443 MB
Auto-zipora-172	Normal	200 GB	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
ovoc_8.2_500G_188	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	3.6 GHz	13.48 GB
7.0_New_189	Normal	524.08 GB	Oracle Linux 7 (64-bit)	Unknown	596 MHz	12.1 GB
171	Normal	524.08 GB	CentOS 7 (64-bit)	Unknown	1.6 GHz	20.6 GB
199_new	Normal	521.05 GB	CentOS 7 (64-bit)	Unknown	494 MHz	11.94 GB

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼

Deploying OVOC Image with VMware vSphere Cluster

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

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

➢ To run VMware OVF tool:

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 326 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
```

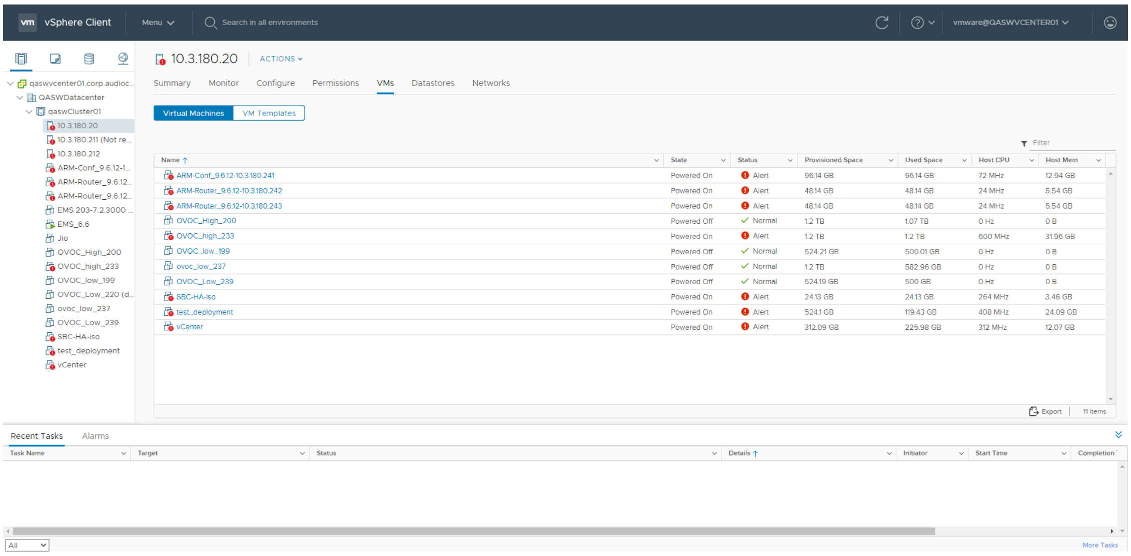
Where:

- $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 7-10: OVF Example



Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
ARM-Conf_9.6.12-10.3.180.241	Powered On	Alert	96.14 GB	96.14 GB	72 MHz	12.94 GB
ARM-Router_9.6.12-10.3.180.242	Powered On	Alert	48.14 GB	48.14 GB	24 MHz	5.54 GB
ARM-Router_9.6.12-10.3.180.243	Powered On	Alert	48.14 GB	48.14 GB	24 MHz	5.54 GB
OVOC_High_200	Powered Off	✓ Normal	1.2 TB	1.07 TB	0 Hz	0 B
OVOC_high_233	Powered On	Alert	1.2 TB	1.2 TB	600 MHz	31.96 GB
OVOC_low_199	Powered Off	✓ Normal	524.21 GB	500.01 GB	0 Hz	0 B
ovoc_low_237	Powered Off	✓ Normal	1.2 TB	582.96 GB	0 Hz	0 B
OVOC_Low_239	Powered Off	✓ Normal	524.19 GB	500 GB	0 Hz	0 B
SBC-HA-iso	Powered On	Alert	24.13 GB	24.13 GB	264 MHz	3.46 GB
test_deployment	Powered On	Alert	524.1 GB	119.43 GB	408 MHz	24.09 GB
vCenter	Powered On	Alert	312.09 GB	225.98 GB	312 MHz	12.07 GB

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.

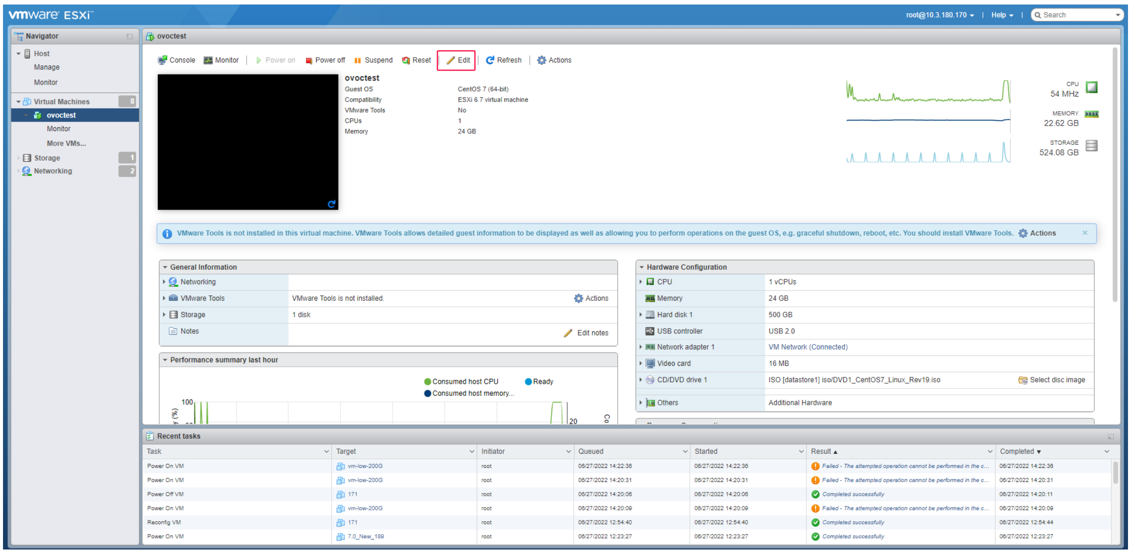
Table 7-1: Virtual Machine Configuration

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 7-11: Edit Settings option



ovoctest

Guest OS	CentOS 7 (64-bit)
Compatibility	ESXi 6.7 virtual machine
VMware Tools	No
CPUs	1
Memory	24 GB

VMware Tools is not installed in this virtual machine. VMware Tools allows detailed guest information to be displayed as well as allowing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. You should install VMware Tools. Actions

General Information

Networking	
VMware Tools	VMware Tools is not installed. Actions
Storage	1 disk
Notes	Edit notes

Performance summary last hour

Hardware Configuration

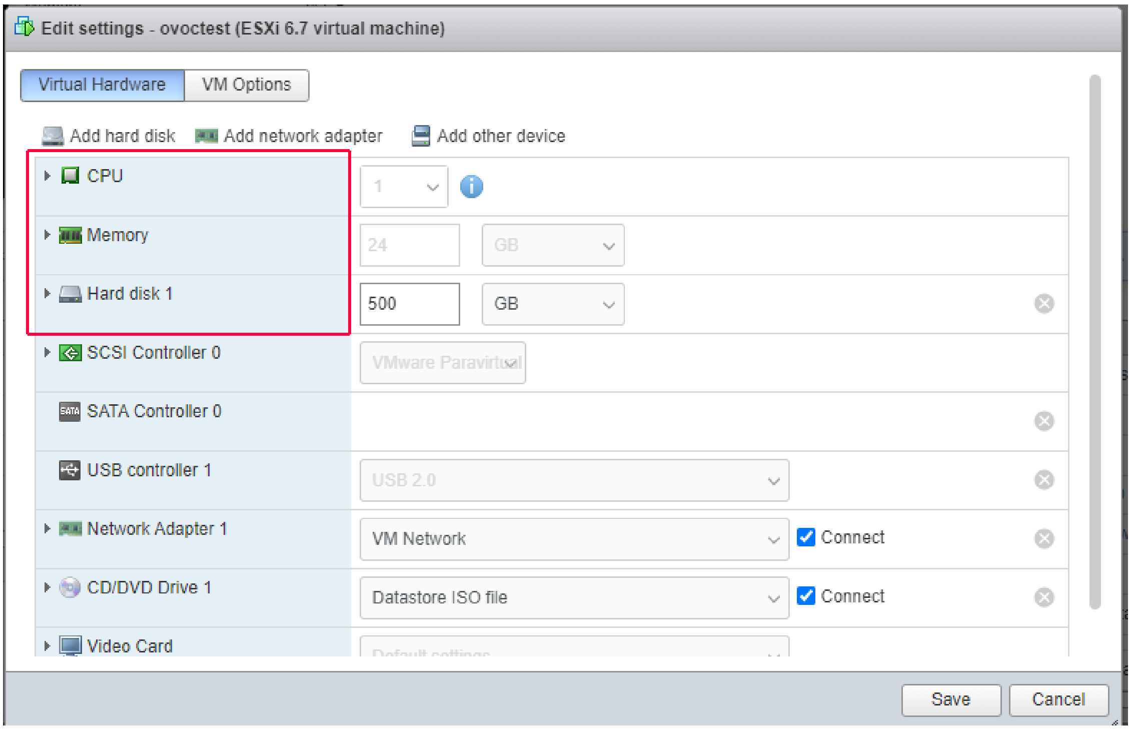
CPU	1 vCPUs
Memory	24 GB
Hard disk 1	500 GB
USB controller	USB 2.0
Network adapter 1	VM Network (Connected)
Video card	16 MB
CD/DVD drive 1	ISO [datastore1] iso/DVD1_CentOS7_Linux_Rev19.iso Select disc image
Others	Additional Hardware

Recent tasks

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Power On VM	vm-low-200G	root	06/27/2022 14:22:36	06/27/2022 14:22:36	Failed - The attempted operation cannot be performed in the c...	06/27/2022 14:22:36
Power On VM	vm-low-200G	root	06/27/2022 14:20:31	06/27/2022 14:20:31	Failed - The attempted operation cannot be performed in the c...	06/27/2022 14:20:31
Power Off VM	171	root	06/27/2022 14:20:06	06/27/2022 14:20:06	Completed successfully	06/27/2022 14:20:11
Power On VM	vm-low-200G	root	06/27/2022 14:20:09	06/27/2022 14:20:09	Failed - The attempted operation cannot be performed in the c...	06/27/2022 14:20:09
Reconfig VM	171	root	06/27/2022 12:54:40	06/27/2022 12:54:40	Completed successfully	06/27/2022 12:54:44
Power On VM	7.0_New_189	root	06/27/2022 12:23:27	06/27/2022 12:23:27	Completed successfully	06/27/2022 12:23:27

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

Figure 7-12: CPU, Memory and Hard Disk Settings



Edit settings - ovoctest (ESXi 6.7 virtual machine)

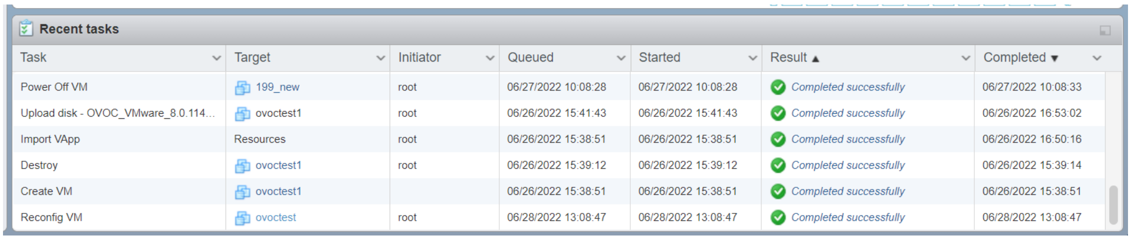
CPU	1
Memory	24 GB
Hard disk 1	500 GB
SCSI Controller 0	VMware Paravirtual
SATA Controller 0	
USB controller 1	USB 2.0
Network Adapter 1	VM Network ☑ Connect
CD/DVD Drive 1	Datastore ISO file ☑ Connect
Video Card	Default settings

- 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 7-13: Recent Tasks



Recent tasks

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

Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

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

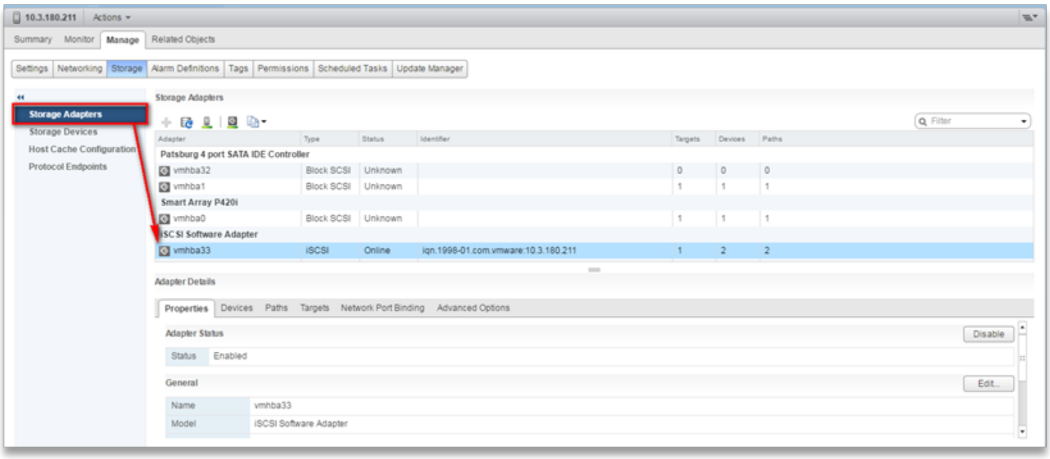
VMware Cluster Site Requirements

Ensure that your VMware cluster site meets the following requirements:

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

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

Figure 7-14: Storage Adapters



Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Patsburg 4 port SATA IDE Controller						
vmhba32	Block SCSI	Unknown		0	0	0
vmhba1	Block SCSI	Unknown		1	1	1
Smart Array P420i						
vmhba0	Block SCSI	Unknown		1	1	1
iSC SI Software Adapter						
vmhba33	iSCSI	Online	iqn.1998-01.com.vmware:10.3.180.211	1	2	2

Adapter Status

Status: Enabled

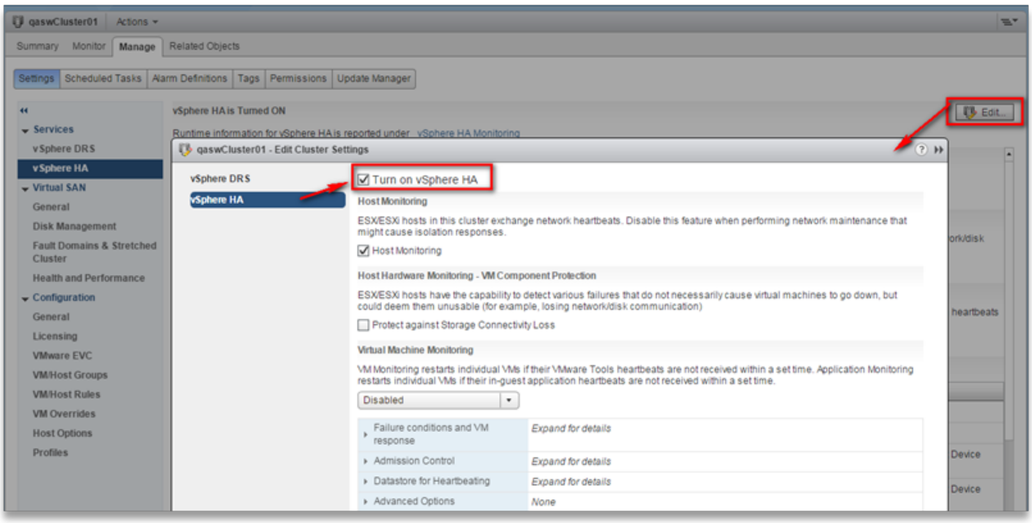
General

Name: vmhba33

Model: iSCSI Software Adapter

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

Figure 7-15: Turn On vSphere HA



vSphere HA is Turned ON

Runtime information for vSphere HA is reported under vSphere HA Monitoring

qaswCluster01 - Edit Cluster Settings

☑ Turn on vSphere HA

Host Monitoring

ESX/ESXi hosts in this cluster exchange network heartbeats. Disable this feature when performing network maintenance that might cause isolation responses.

☑ Host Monitoring

Host Hardware Monitoring - VM Component Protection

ESX/ESXi hosts have the capability to detect various failures that do not necessarily cause virtual machines to go down, but could deem them unusable (for example, losing network/disk communication)

□ Protect against Storage Connectivity Loss

Virtual Machine Monitoring

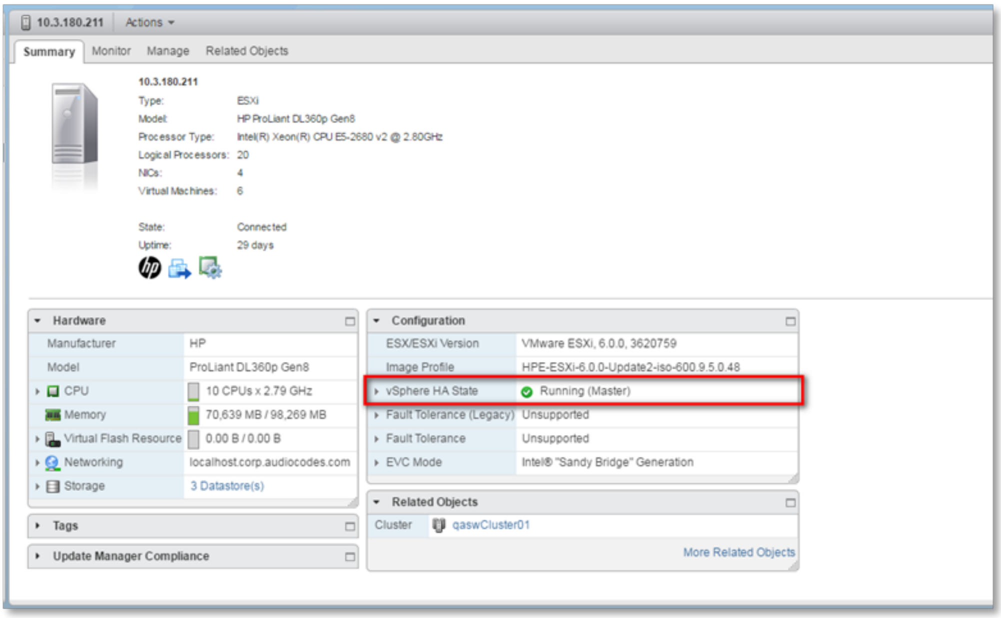
VM Monitoring restarts individual VMs if their VMware Tools heartbeats are not received within a set time. Application Monitoring restarts individual VMs if their in-guest application heartbeats are not received within a set time.

Disabled

Failure conditions and VM response	Expand for details
Admission Control	Expand for details
Datastore for Heartbeating	Expand for details
Advanced Options	None

- Ensure that HA is activated on each cluster node:

Figure 7-16: Activate HA on each Cluster Node



10.3.180.211

Type:	ESXi
Model:	HP ProLiant DL360p Gen8
Processor Type:	Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors:	20
NICs:	4
Virtual Machines:	6
State:	Connected
Uptime:	29 days

Hardware

Manufacturer	HP
Model	ProLiant DL360p Gen8
CPU	10 CPUs x 2.79 GHz
Memory	70,639 MB / 98,269 MB
Virtual Flash Resource	0.00 B / 0.00 B
Networking	localhost.corp.audiocodes.com
Storage	3 Datastore(s)

Configuration

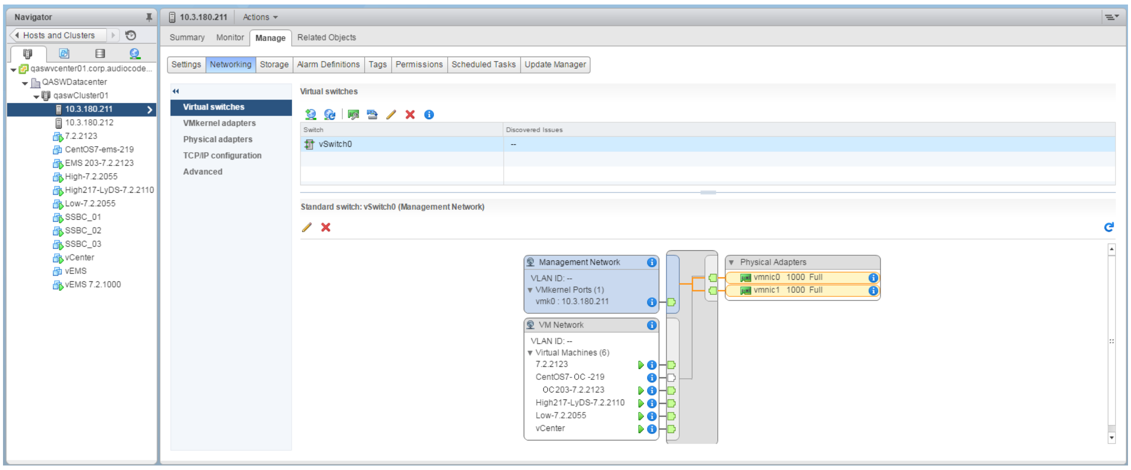
ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759
Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.0.48
vSphere HA State	✓ Running (Master)
Fault Tolerance (Legacy)	Unsupported
Fault Tolerance	Unsupported
EVC Mode	Intel® "Sandy Bridge" Generation

Related Objects

Cluster	qaswCluster01

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

Figure 7-17: Networking



Virtual switches

Switch	Discovered Issues
vSwitch0	--

Standard switch: vSwitch0 (Management Network)

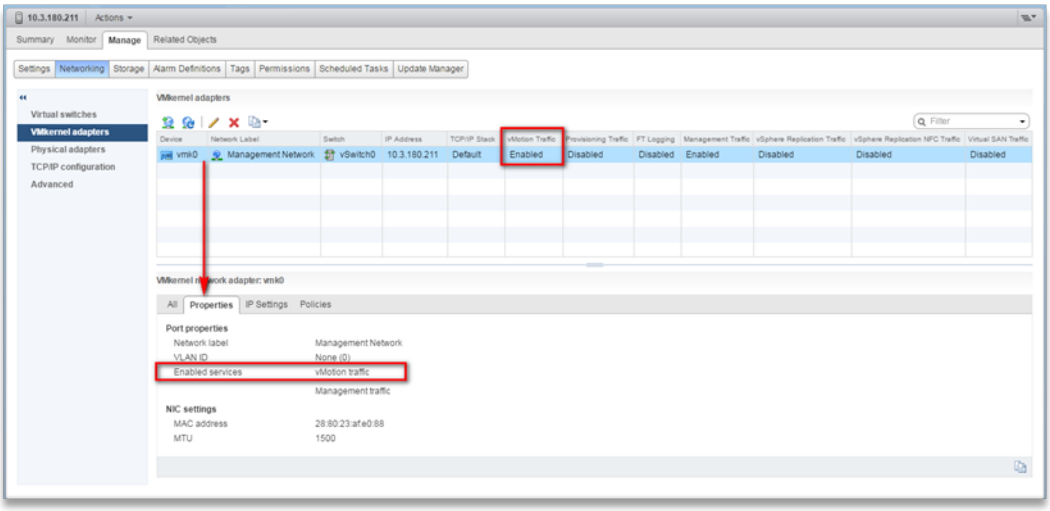
Management Network
VLAN ID: --
VMkernel Ports (1)
vmk0 : 10.3.180.211

VM Network
VLAN ID: --
Virtual Machines (6)
7.2.2123
CentOS7-OC -219
OC203-7.2.2123
High217-LyDS-7.2.2110
Low-7.2.2055
vCenter

Physical Adapters
vmnic0 1000 Full
vmnic1 1000 Full

- 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 7-18: Switch Properties



VMkernel adapters

Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion Traffic	Provisioning Traffic	FT Logging	Management Traffic	vSphere Replication Traffic	vSphere Replication NFC Traffic	Virtual SAN Traffic
vmk0	Management Network	vSwitch0	10.3.180.211	Default	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

VMkernel network adapter: vmk0

All | Properties | IP Settings | Policies

Port properties

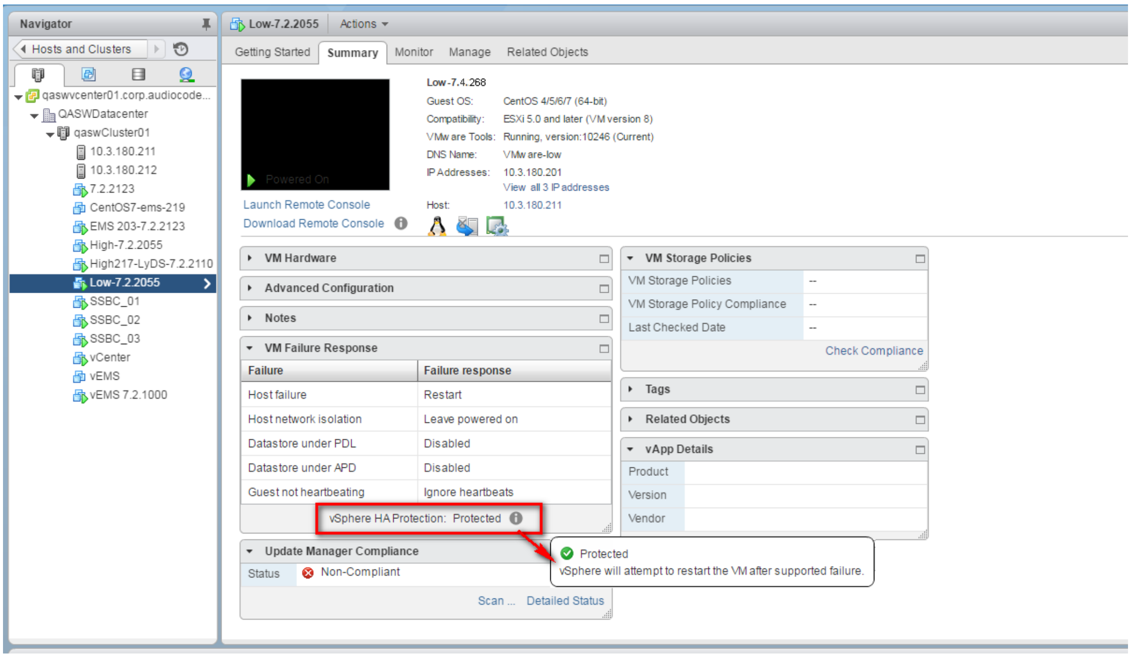
Network label	Management Network
VLAN ID	None (0)
Enabled services	vMotion traffic Management traffic

NIC settings

MAC address	28:80:23:af:e0:88
MTU	1500

- 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 7-19: Protected VM



Low-7.4.268

Guest OS: CentOS 4/5/6/7 (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Running, version:10246 (Current)
DNS Name: VMware-low
IP Addresses: 10.3.180.201
View all 3 IP addresses
Host: 10.3.180.211

VM Failure Response

Failure	Failure response
Host failure	Restart
Host network isolation	Leave powered on
Datastore under PDL	Disabled
Datastore under APD	Disabled
Guest not heartbeating	Ignore heartbeats

vSphere HA Protection: Protected

Protected
vSphere will attempt to restart the VM after supported failure.

Update Manager Compliance

Status: Non-Compliant

VM Storage Policies

VM Storage Policies	--
VM Storage Policy Compliance	--
Last Checked Date	--

vApp Details

Product	
Version	
Vendor	

If you wish to manually migrate the OVOC VMs to another cluster node, see Managing Clusters on page 308.

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.

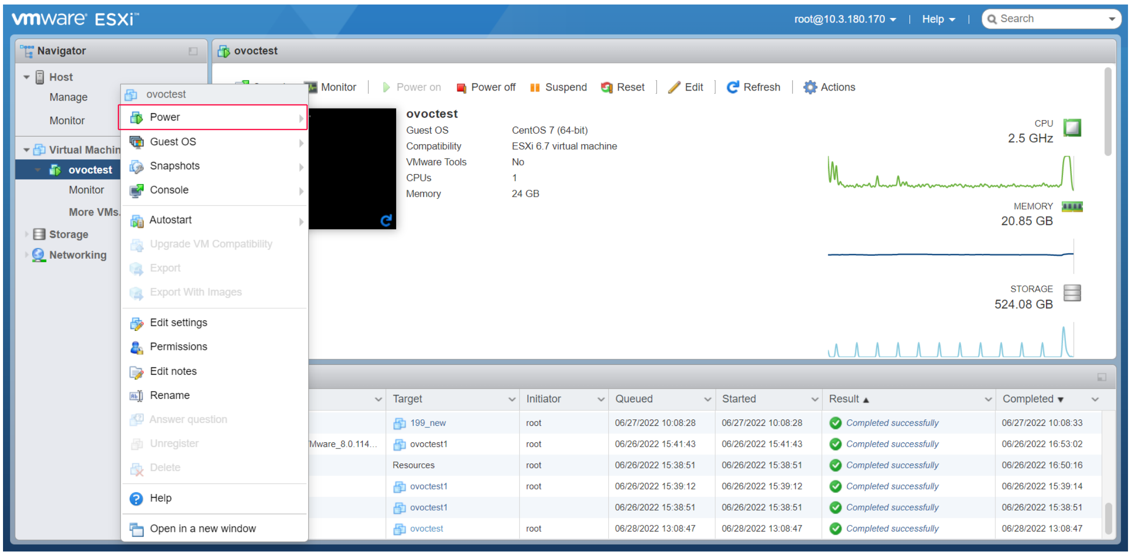
Connecting OVOC Server to Network on VMware

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 7-20: Power On



ovoctest

Guest OS	CentOS 7 (64-bit)
Compatibility	ESXi 6.7 virtual machine
VMware Tools	No
CPUs	1
Memory	24 GB

	Target	Initiator	Queued	Started	Result ▲	Completed ▼
	199_new	root	06/27/2022 10:08:28	06/27/2022 10:08:28	✓ Completed successfully	06/27/2022 10:08:33
Mware_8.0.114...	ovoctest1	root	06/26/2022 15:41:43	06/26/2022 15:41:43	✓ Completed successfully	06/26/2022 16:53:02
	Resources	root	06/26/2022 15:38:51	06/26/2022 15:38:51	✓ Completed successfully	06/26/2022 16:50:16
	ovoctest1	root	06/26/2022 15:39:12	06/26/2022 15:39:12	✓ Completed successfully	06/26/2022 15:39:14
	ovoctest1		06/26/2022 15:38:51	06/26/2022 15:38:51	✓ Completed successfully	06/26/2022 15:38:51
	ovoctest	root	06/28/2022 13:08:47	06/28/2022 13:08:47	✓ Completed successfully	06/28/2022 13:08:47

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.

```
# EmsServerManager
```

7. Verify that all processes are up and running (Viewing Process Statuses on page 201) 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 225).

9. Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 196).

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.

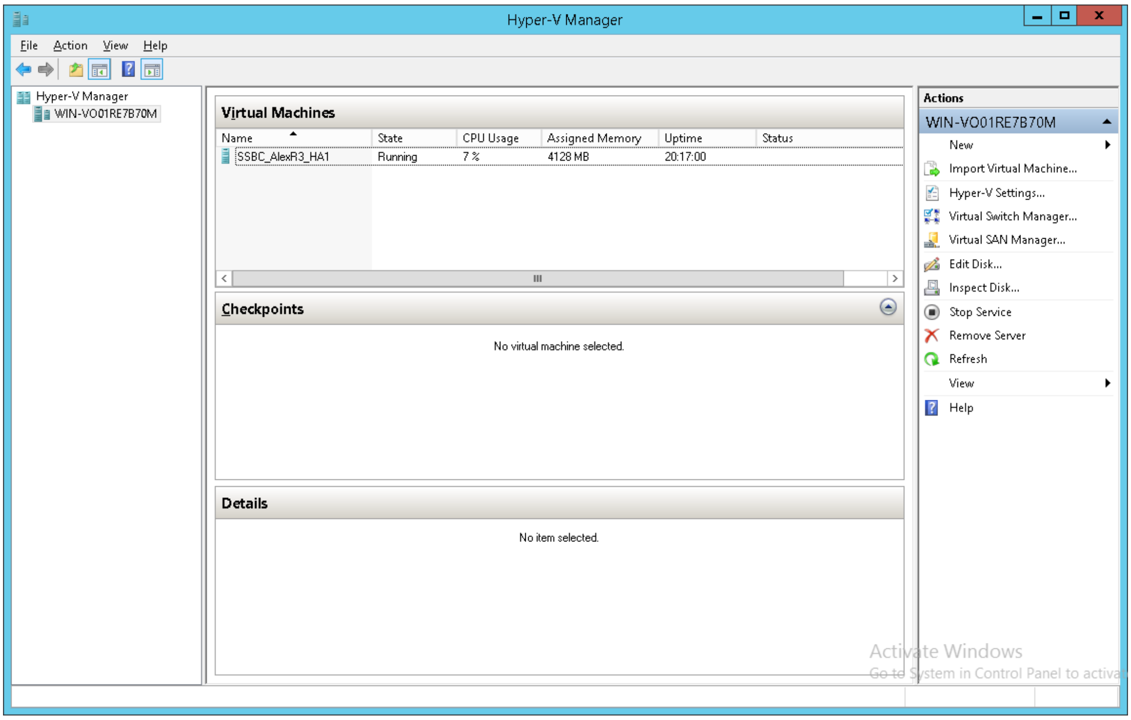
- Before proceeding, ensure that the minimum platform requirements are met (see .Hardware and Software Specifications on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see OVOC Software Deliverables on page 13
  - ✓ Note 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 326 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



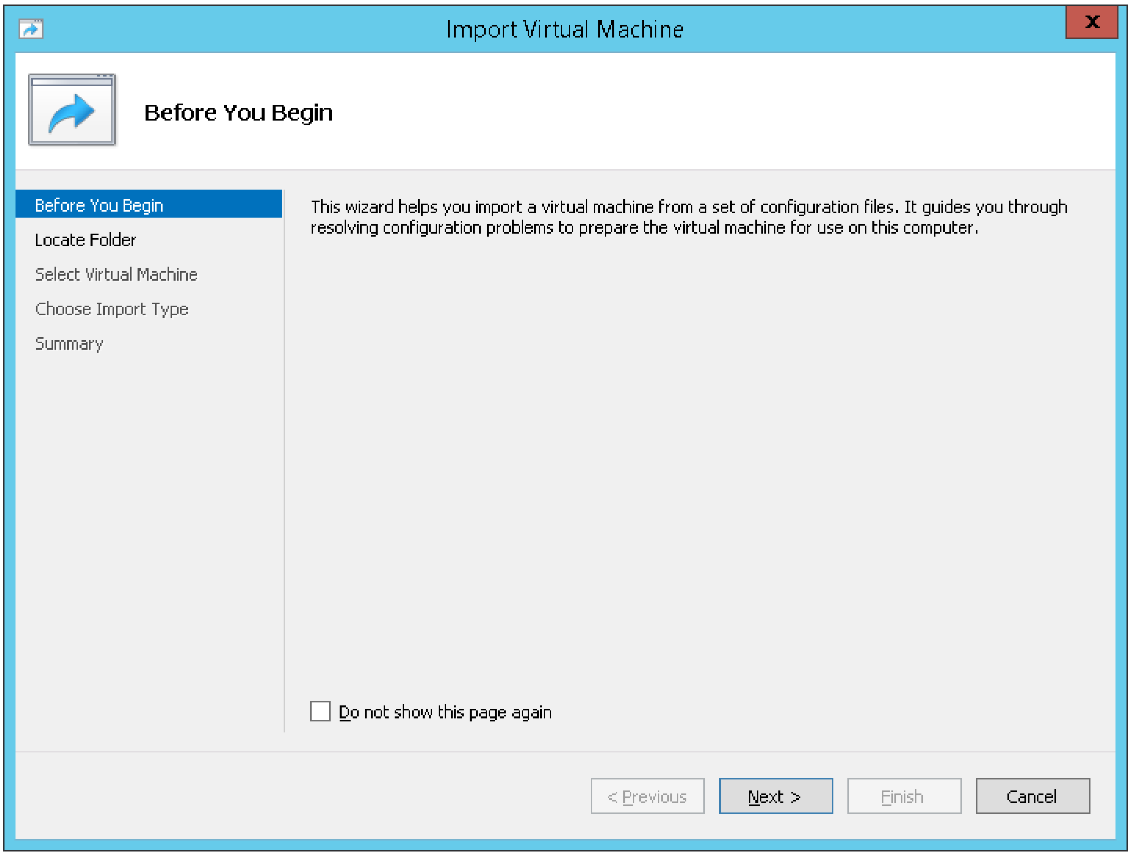
Name	State	CPU Usage	Assigned Memory	Uptime	Status
SSBC_AlexR3_HA1	Running	7 %	4128 MB	20:17:00	

No virtual machine selected.

No item selected.

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

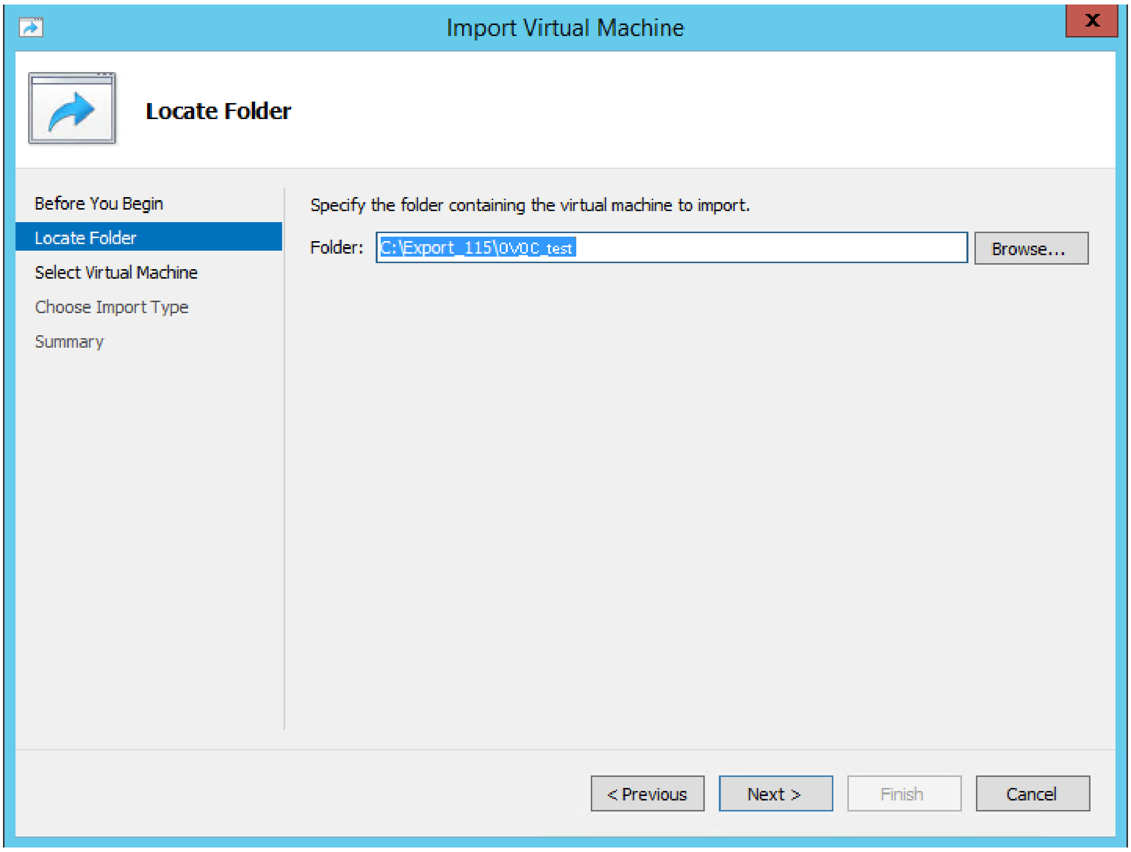


This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

☐ Do not show this page again

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

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



Import Virtual Machine

Locate Folder

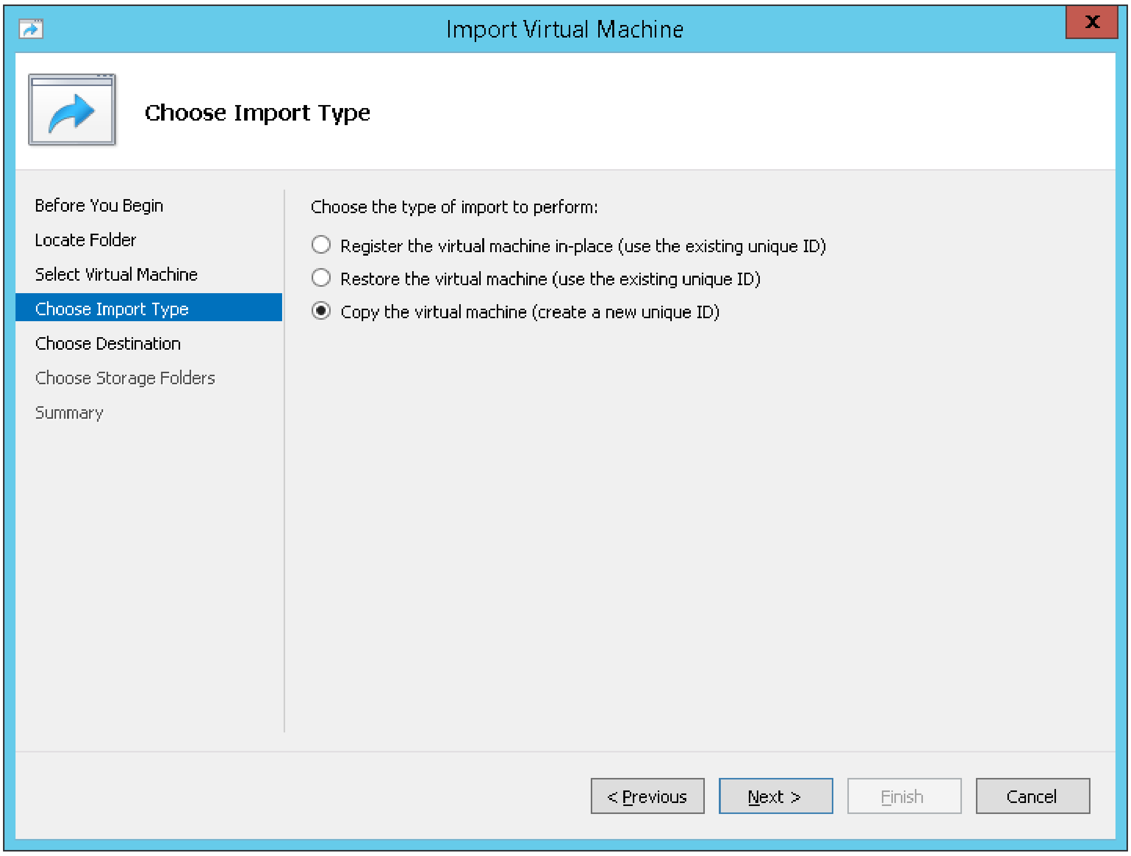
Specify the folder containing the virtual machine to import.

Folder: C:\Export_115\OVOC_test

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



Choose the type of import to perform:

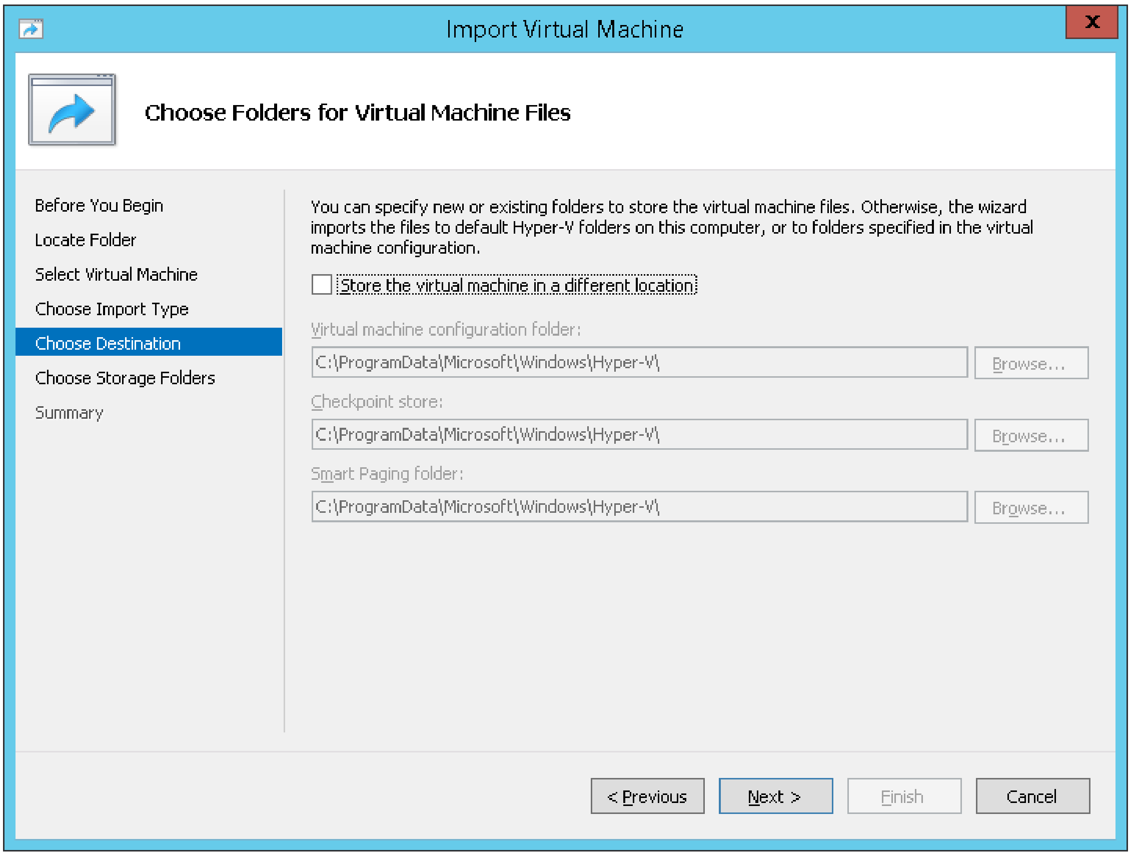
○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

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



Import Virtual Machine

Choose Folders for Virtual Machine Files

You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

□ Store the virtual machine in a different location

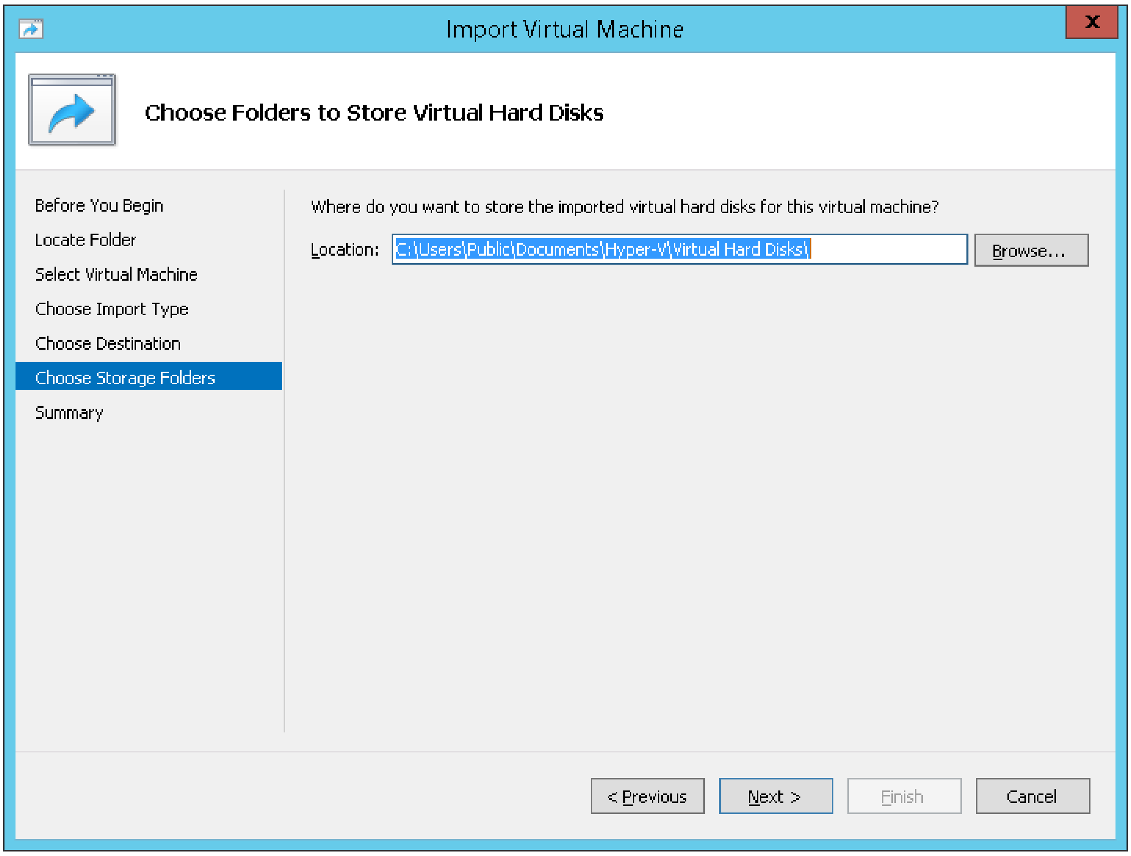
Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Checkpoint store: C:\ProgramData\Microsoft\Windows\Hyper-V\

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

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



Import Virtual Machine

Choose Folders to Store Virtual Hard Disks

Where do you want to store the imported virtual hard disks for this virtual machine?

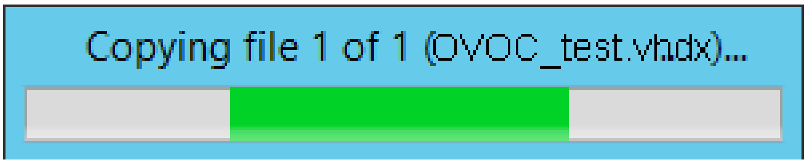
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

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.



Copying file 1 of 1 (OVOC_test.vhdx)...

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.

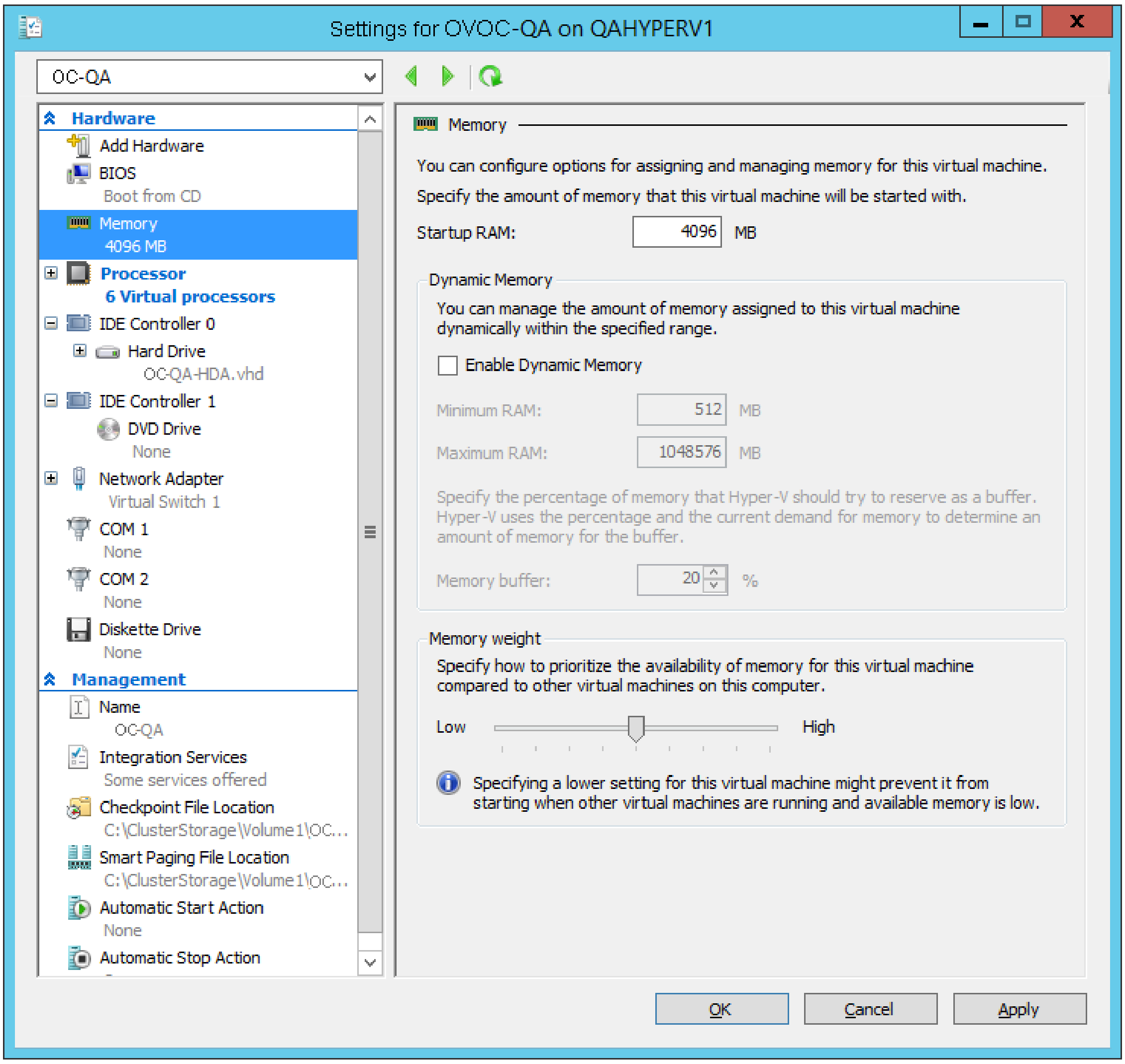
Table 8-1: Virtual Machine Configuration

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



You can configure options for assigning and managing memory for this virtual machine.

Specify the amount of memory that this virtual machine will be started with.

Startup RAM: 4096 MB

Dynamic Memory

You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

□ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight

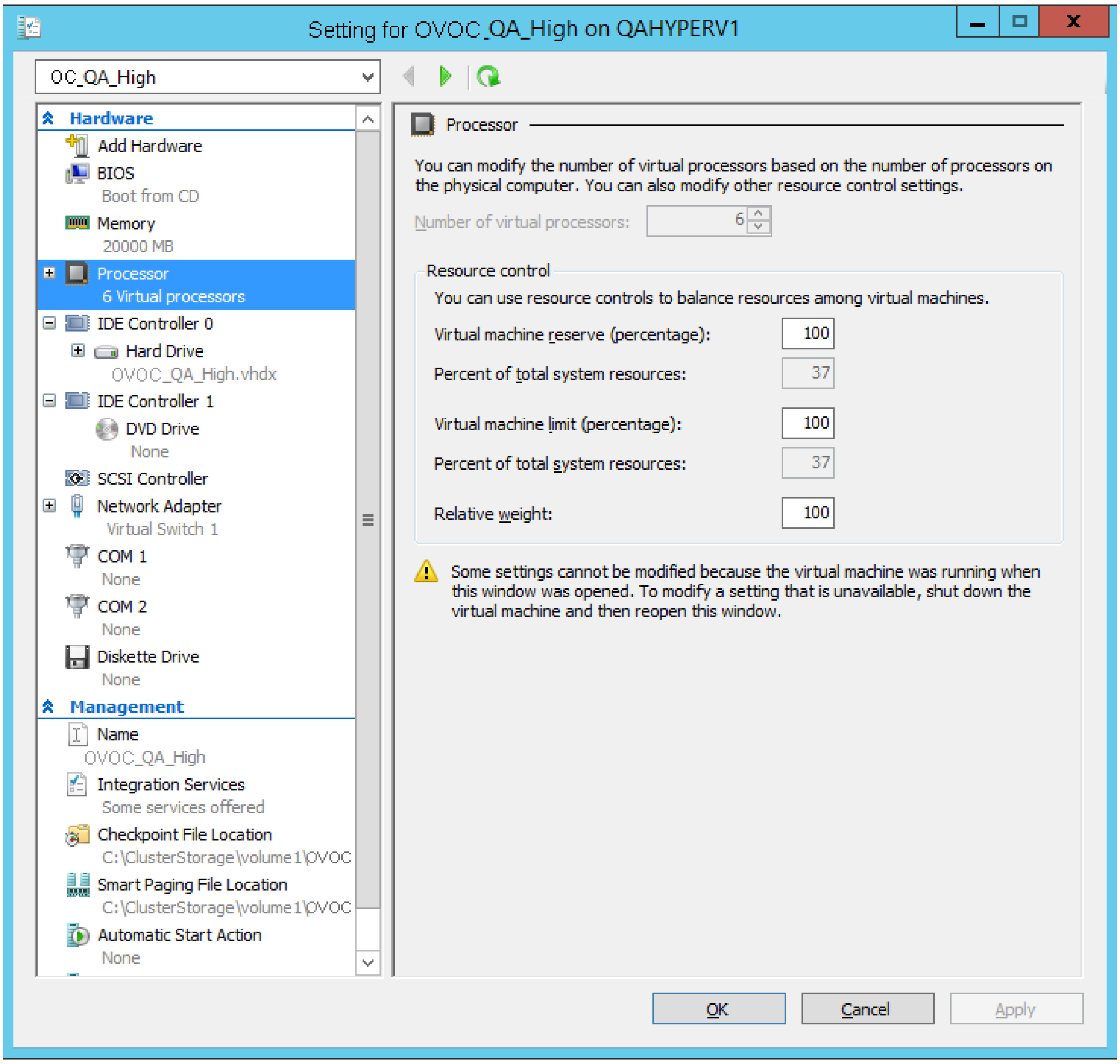
Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.

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



You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 6

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 100

Percent of total system resources: 37

Virtual machine limit (percentage): 100

Percent of total system resources: 37

Relative weight: 100

Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

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).

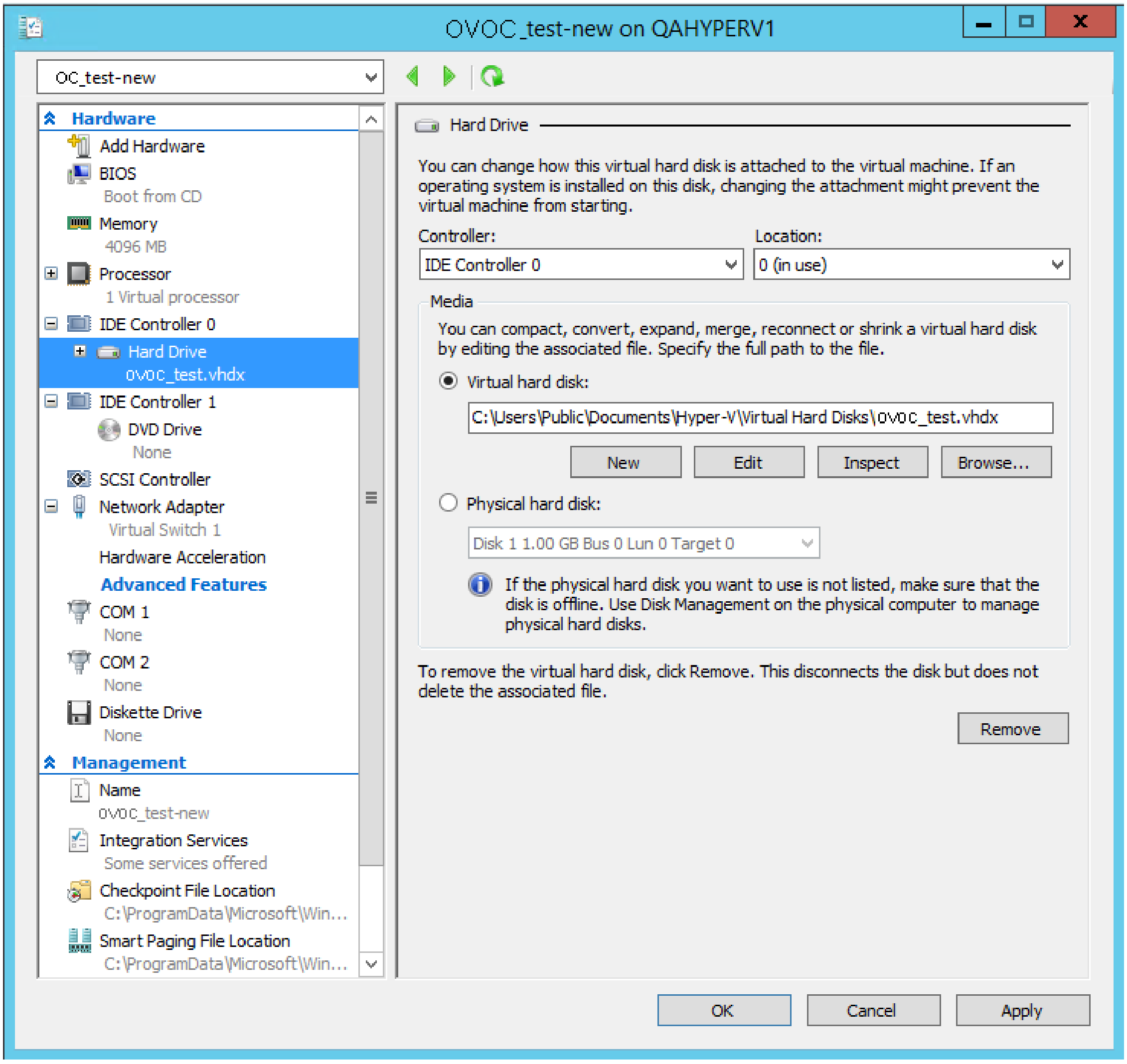
Expanding Disk Capacity

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



OVOC_test-new on QAHYPERV1

OC_test-new

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ovoc_test.vhdx

○ Physical hard disk:

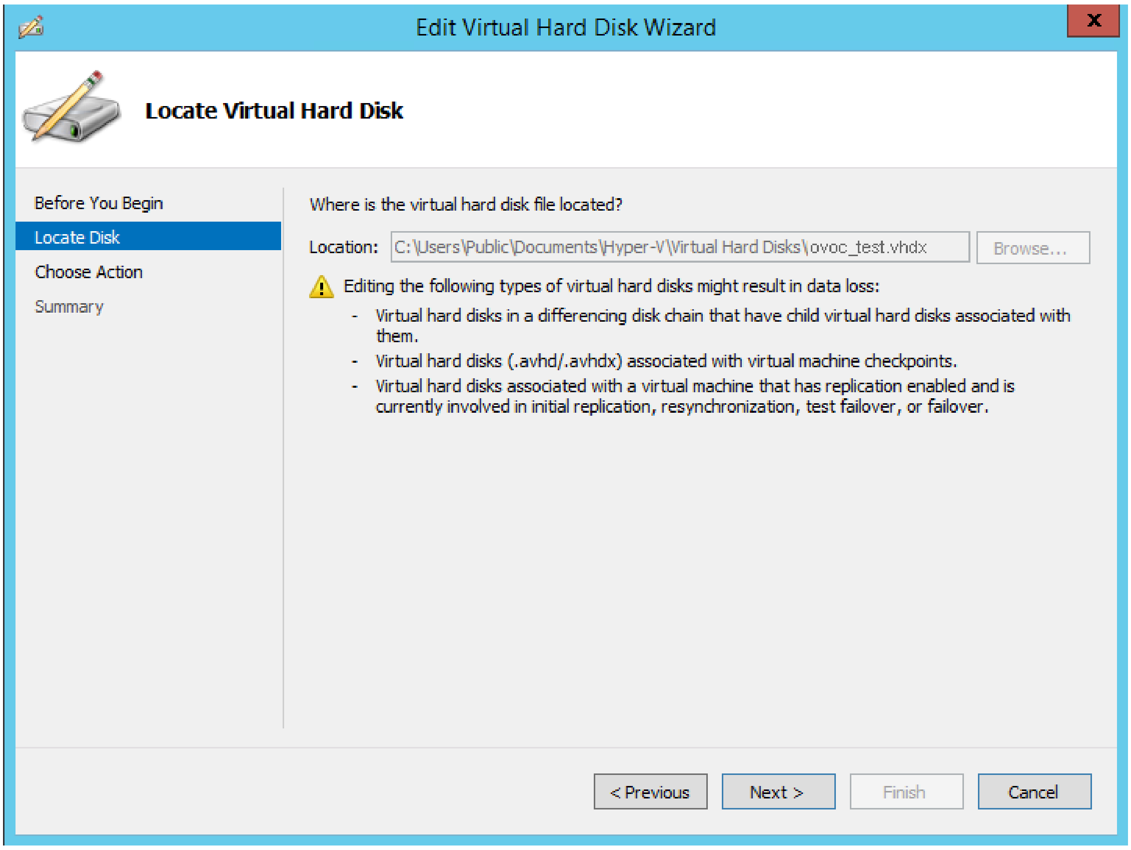
Disk 1 1.00 GB Bus 0 Lun 0 Target 0

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

The Edit Virtual Disk Wizard is displayed as shown below.

Figure 8-11: Edit Virtual Hard Disk Wizard



Where is the virtual hard disk file located?

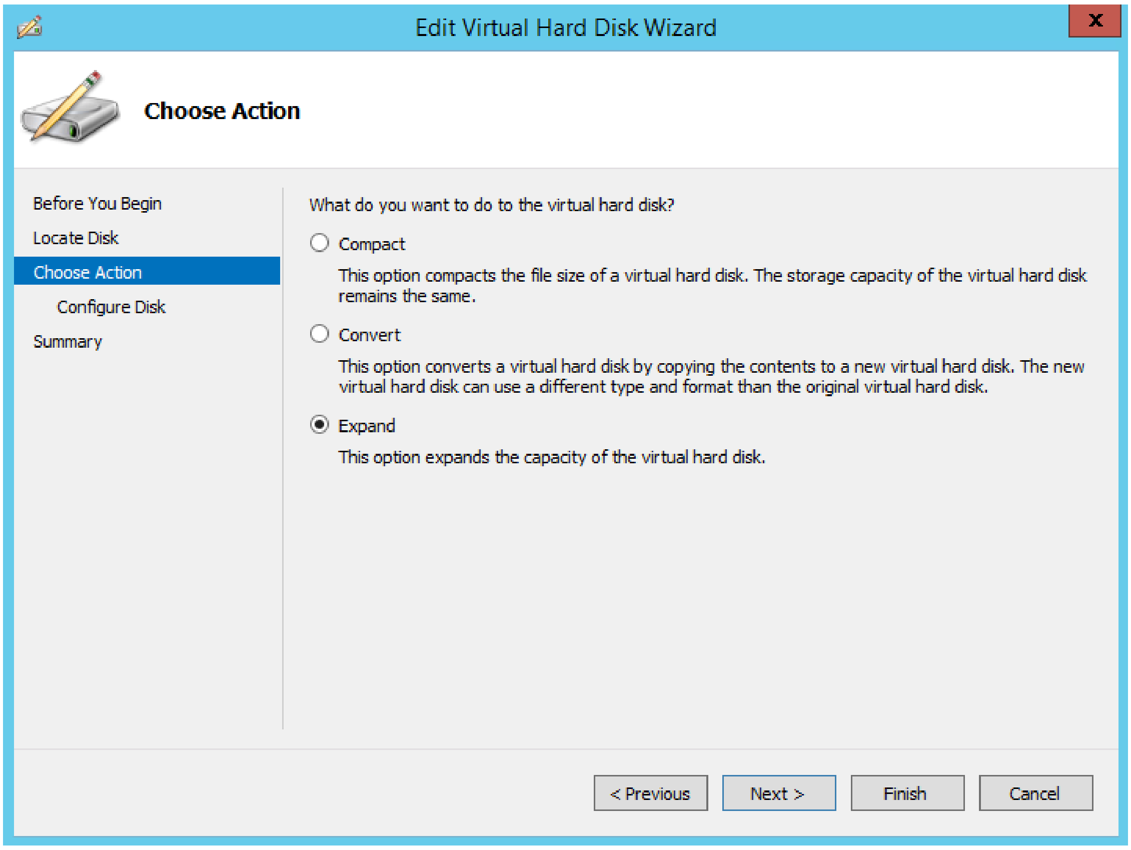
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ovoc_test.vhdx

Editing the following types of virtual hard disks might result in data loss:

- Virtual hard disks in a differencing disk chain that have child virtual hard disks associated with them.
- Virtual hard disks (.avhd/.avhdx) associated with virtual machine checkpoints.
- Virtual hard disks associated with a virtual machine that has replication enabled and is currently involved in initial replication, resynchronization, test failover, or failover.

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

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



What do you want to do to the virtual hard disk?

○ Compact

This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same.

○ Convert

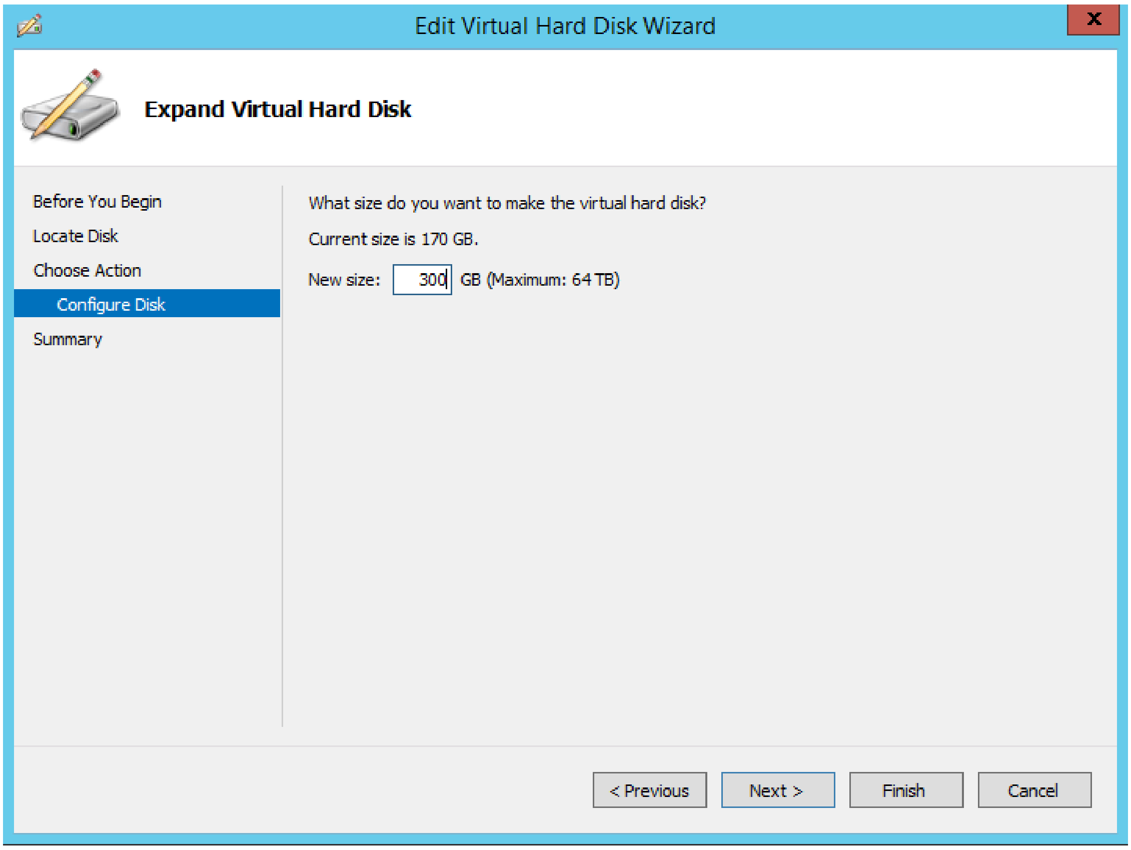
This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

● Expand

This option expands the capacity of the virtual hard disk.

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



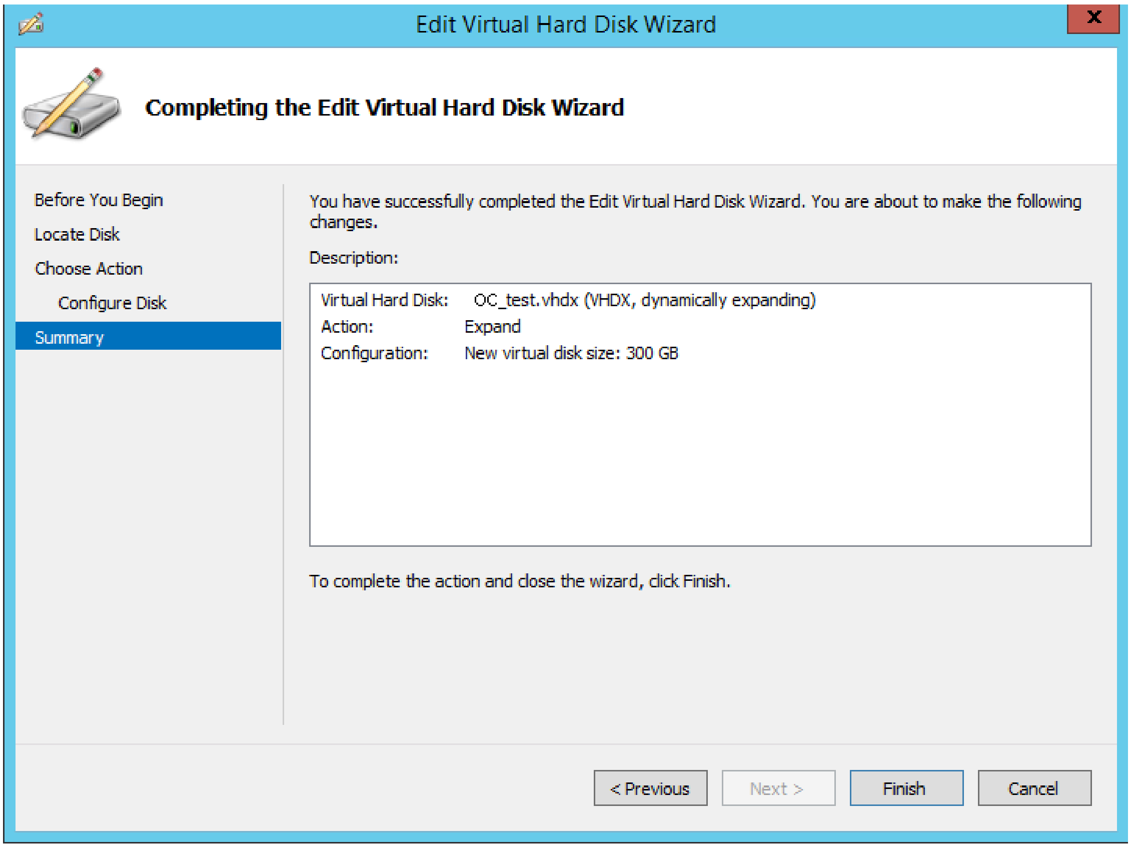
What size do you want to make the virtual hard disk?

Current size is 170 GB.

New size: 300 GB (Maximum: 64 TB)

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



You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to make the following changes.

Description:

Virtual Hard Disk: OC_test.vhdx (VHDX, dynamically expanding)
Action: Expand
Configuration: New virtual disk size: 300 GB

To complete the action and close the wizard, click Finish.

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:

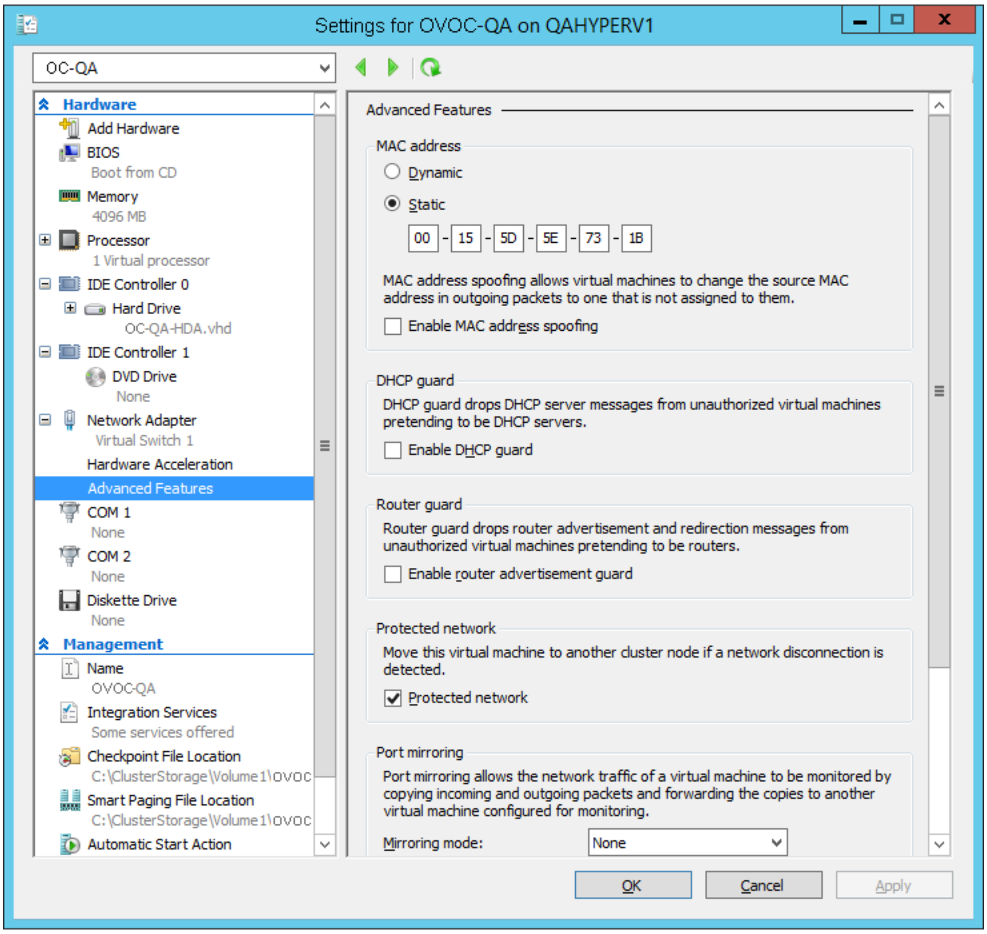
1. Shutdown the OVOC server (Shutdown the OVOC Server Machine on page 222).

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



Settings for OVOC-QA on QAHYPERV1

OC-QA

Hardware
- Add Hardware
- BIOS
  - Boot from CD
- Memory
  - 4096 MB
- Processor
  - 1 Virtual processor
- IDE Controller 0
  - Hard Drive
    - OC-QA-HDA.vhd
- IDE Controller 1
  - DVD Drive
    - None
- Network Adapter
  - Virtual Switch 1
  - Hardware Acceleration
  - Advanced Features
- COM 1
  - None
- COM 2
  - None
- Diskette Drive
  - None

Management
- Name
  - OVOC-QA
- Integration Services
  - Some services offered
- Checkpoint File Location
  - C:\ClusterStorage\Volume1\ovoc
- Smart Paging File Location
  - C:\ClusterStorage\Volume1\ovoc
- Automatic Start Action

Advanced Features

MAC address

○ Dynamic

● Static

00 - 15 - 5D - 5E - 73 - 1B

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

□ Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

□ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

□ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: None

Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster

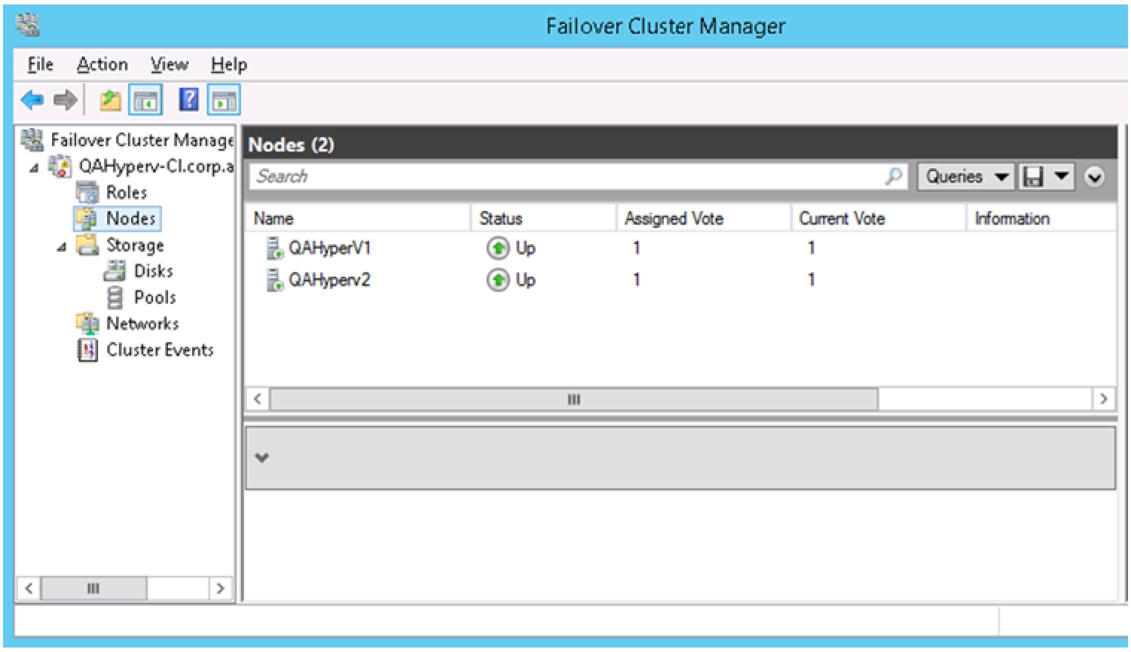
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

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



Name	Status	Assigned Vote	Current Vote	Information
QAHyperV1	Up	1	1	
QAHyperv2	Up	1	1	

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

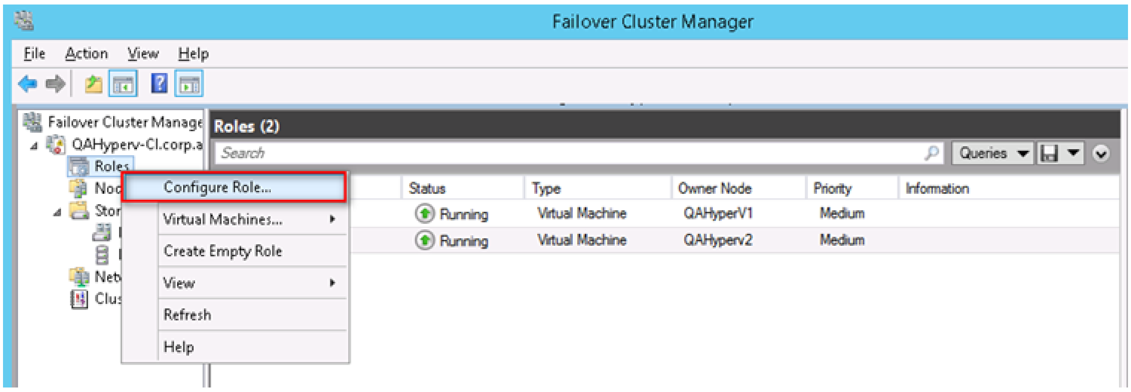
Add the OVOC VM in Failover Cluster Manager

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.**

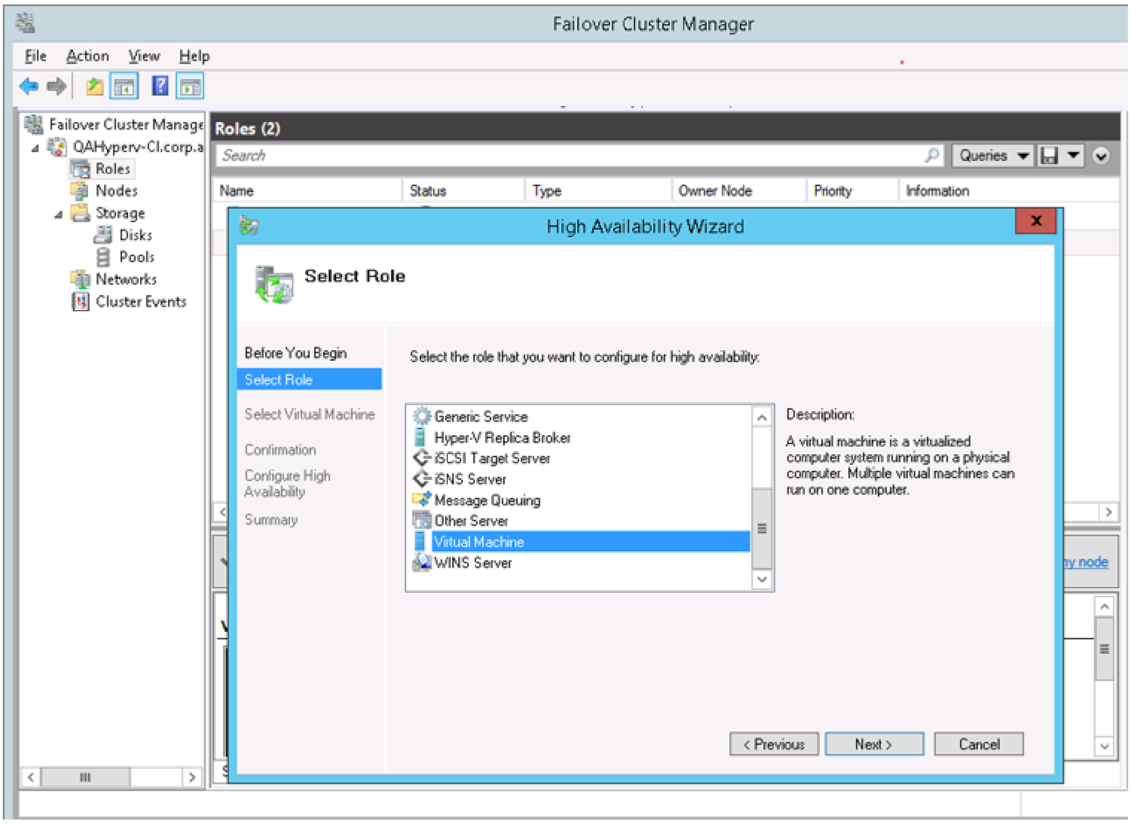
Figure 8-17: Configure Role



Status	Type	Owner Node	Priority	Information
Running	Virtual Machine	QAHyperV1	Medium	
Running	Virtual Machine	QAHyperv2	Medium	

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

Figure 8-18: Choose Virtual Machine



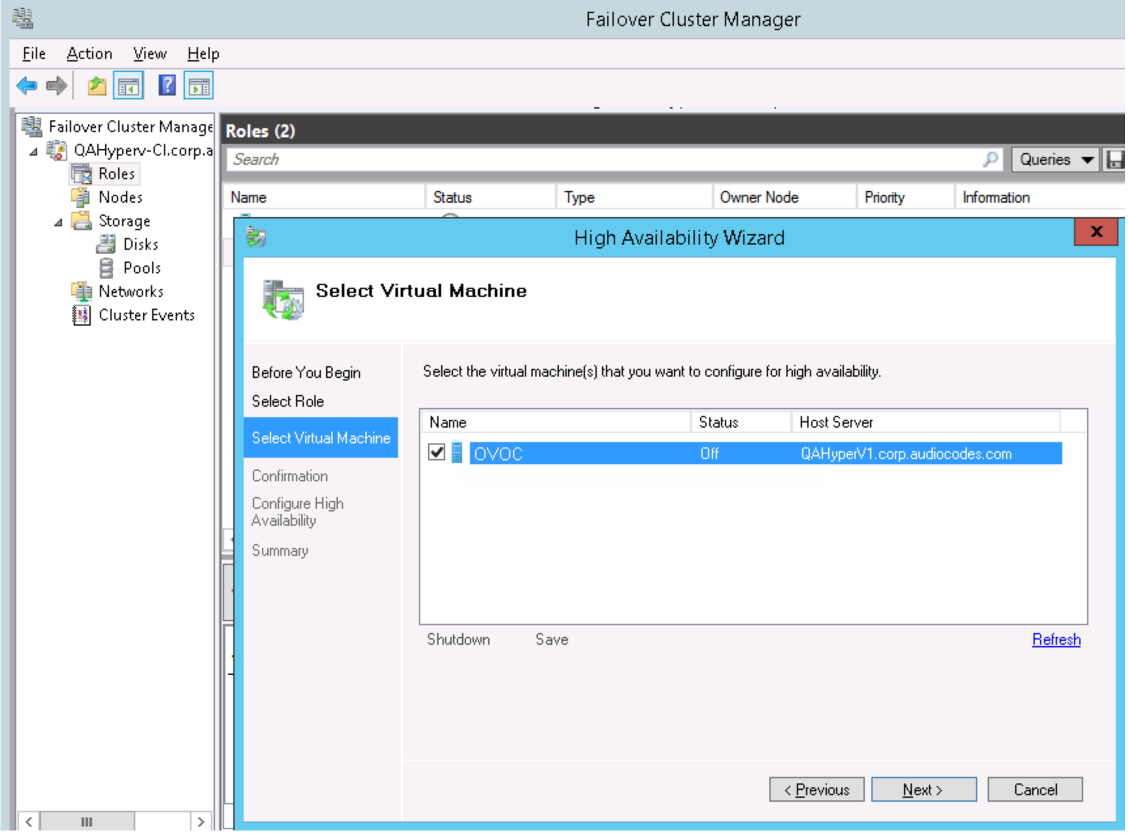
Select the role that you want to configure for high availability:

Description:

A virtual machine is a virtualized computer system running on a physical computer. Multiple virtual machines can run on one computer.

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

Figure 8-19: Confirm Virtual Machine



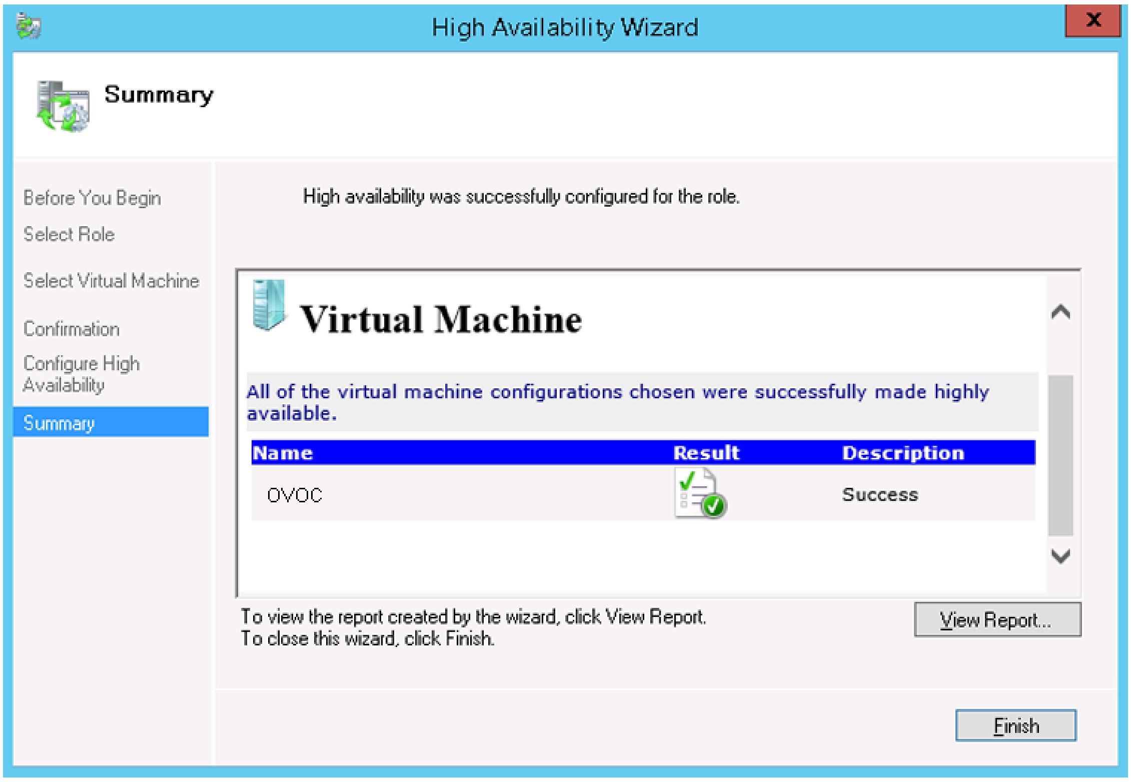
Select the virtual machine(s) that you want to configure for high availability.

	Name	Status	Host Server
☑	OVOC	Off	QAHyperV1.corp.audiocodes.com

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



High availability was successfully configured for the role.

Virtual Machine

All of the virtual machine configurations chosen were successfully made highly available.

Name	Result	Description
OVOC	✓	Success

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

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 308.

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.

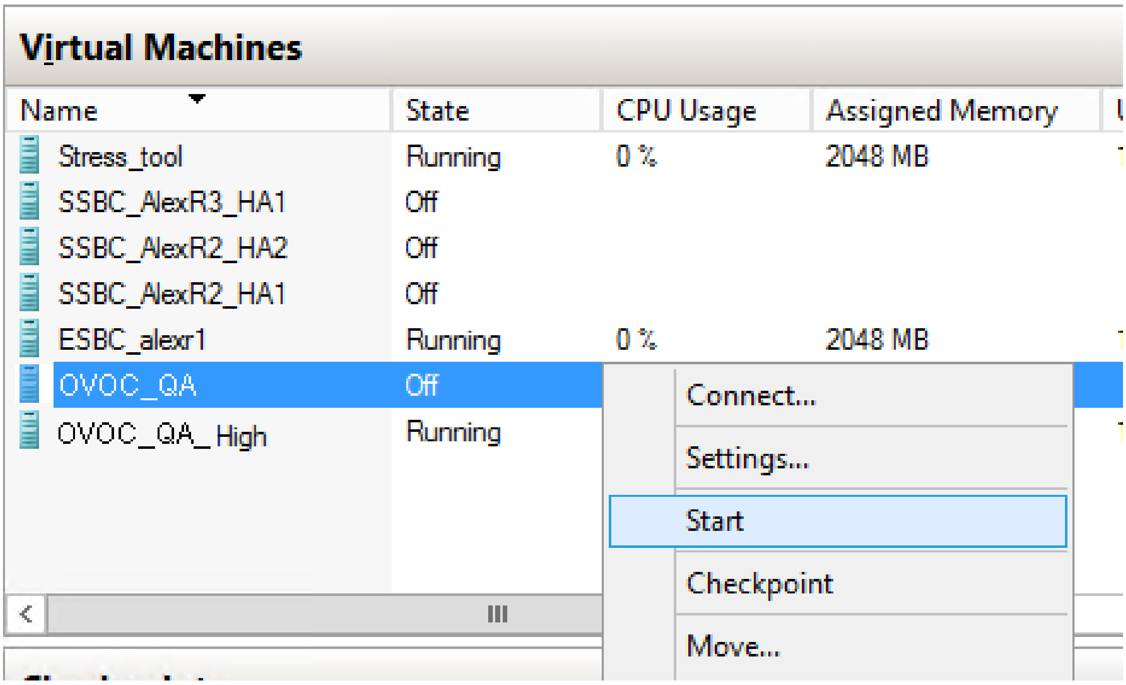
Connecting OVOC Server to Network on HyperV

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

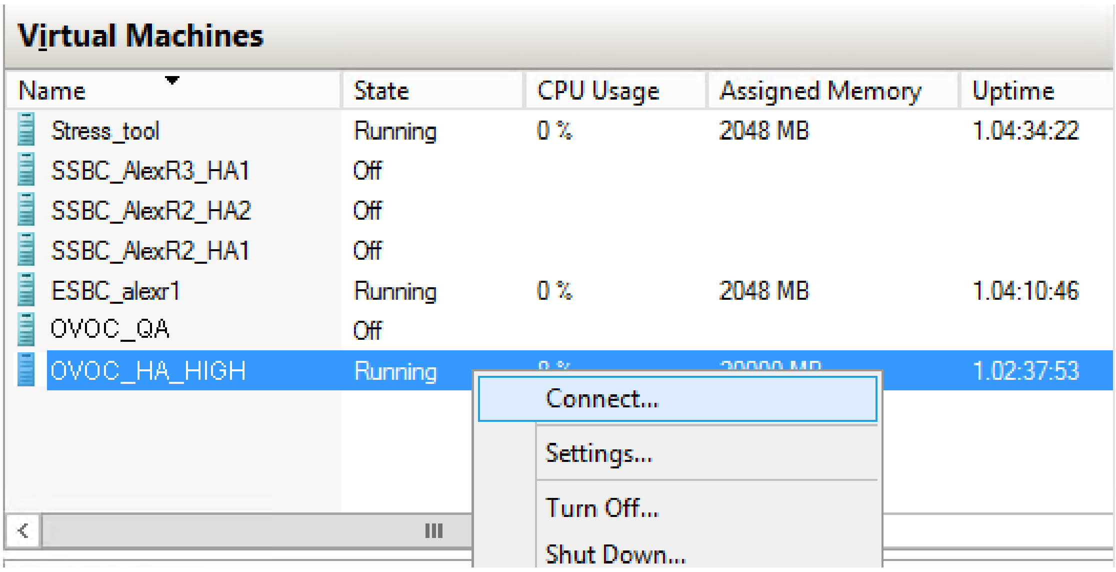


Virtual Machines

Name	State	CPU Usage	Assigned Memory	U
Stress_tool	Running	0 %	2048 MB	1
SSBC_AlexR3_HA1	Off			
SSBC_AlexR2_HA2	Off			
SSBC_AlexR2_HA1	Off			
ESBC_alexr1	Running	0 %	2048 MB	1
OVOC_QA	Off			
OVOC_QA_ High	Running			1

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

Figure 8-22: Connect to OVOC server Console



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
Stress_tool	Running	0 %	2048 MB	1.04:34:22
SSBC_AlexR3_HA1	Off			
SSBC_AlexR2_HA2	Off			
SSBC_AlexR2_HA1	Off			
ESBC_alexr1	Running	0 %	2048 MB	1.04:10:46
OVOC_QA	Off			
OVOC_HA_HIGH	Running	0 %	20000 MB	1.02:37:53

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:

```
# EmsServerManager
```

6. Verify that all processes are up and running (Viewing Process Statuses on page 201) 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 225).

8. Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 196).

9 Installing OVOC Server on Dedicated Hardware

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

- **DVD1:** OS installation: OS installation DVD
- **DVD3:** OVOC application: OVOC server application installation DVD

- 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

DVD1: Linux CentOS

The procedure below describes how to install Linux CentOS. This procedure takes approximately 20 minutes.

Before commencing the installation, you must configure RAID-0 (see Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers on page 305).

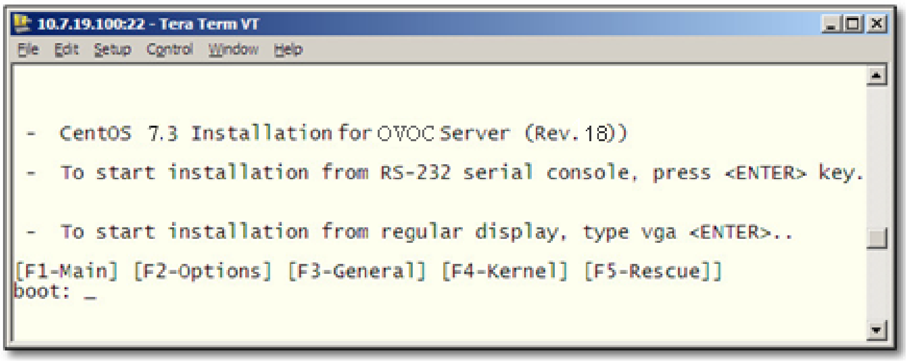
➢ **To perform DVD1 installation:**

1. Insert the **DVD1** into the DVD ROM.
2. Connect the OVOC server through the serial port with a terminal application and login with 'root' user. Default password is *root*.
3. Perform OVOC server machine reboot by specifying the following command:

```
reboot
```

4. Press Enter; you are prompted whether you which to start the installation through the RS-232 console or through the regular display.
5. Press Enter to start the installation from the RS-232 serial console or type **vga**, and then press Enter to start the installation from a regular display.

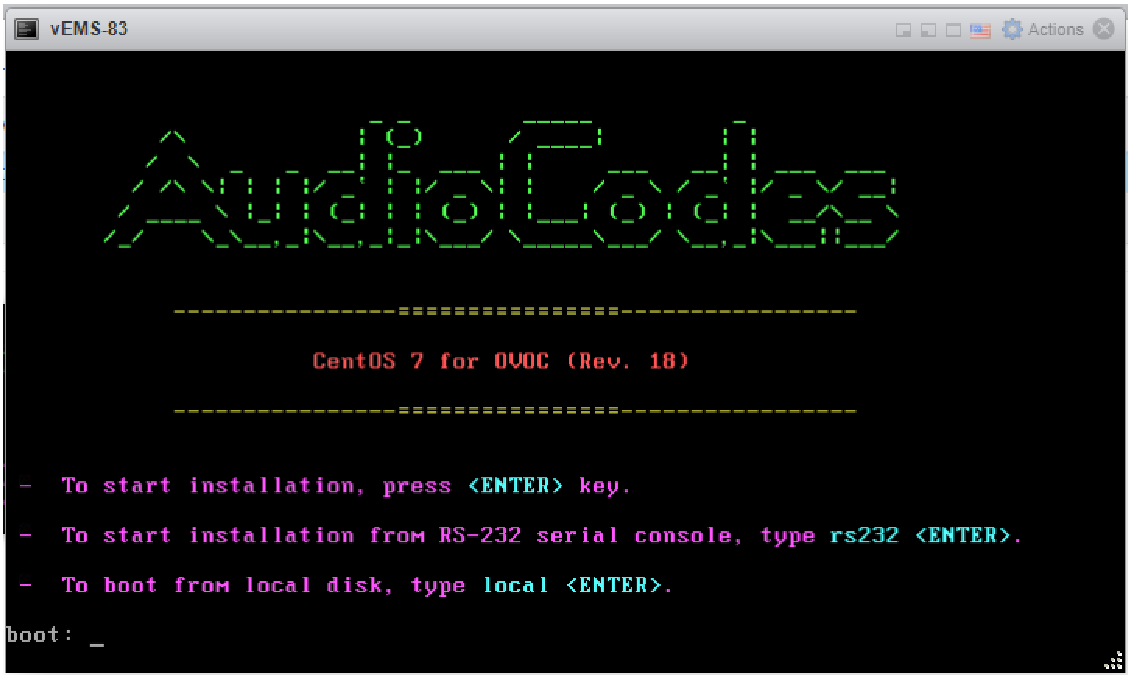
Figure 9-1: Linux CentOS Installation



10.7.19.100:22 - Tera Term VT
File Edit Setup Control Window Help

```
 -  CentOS  7.3 Installation for OVOC Server  (Rev. 18))
 -  To start installation from RS-232 serial console, press <ENTER> key.

 -  To start installation from regular display, type vga <ENTER>..
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]]
boot: _
```

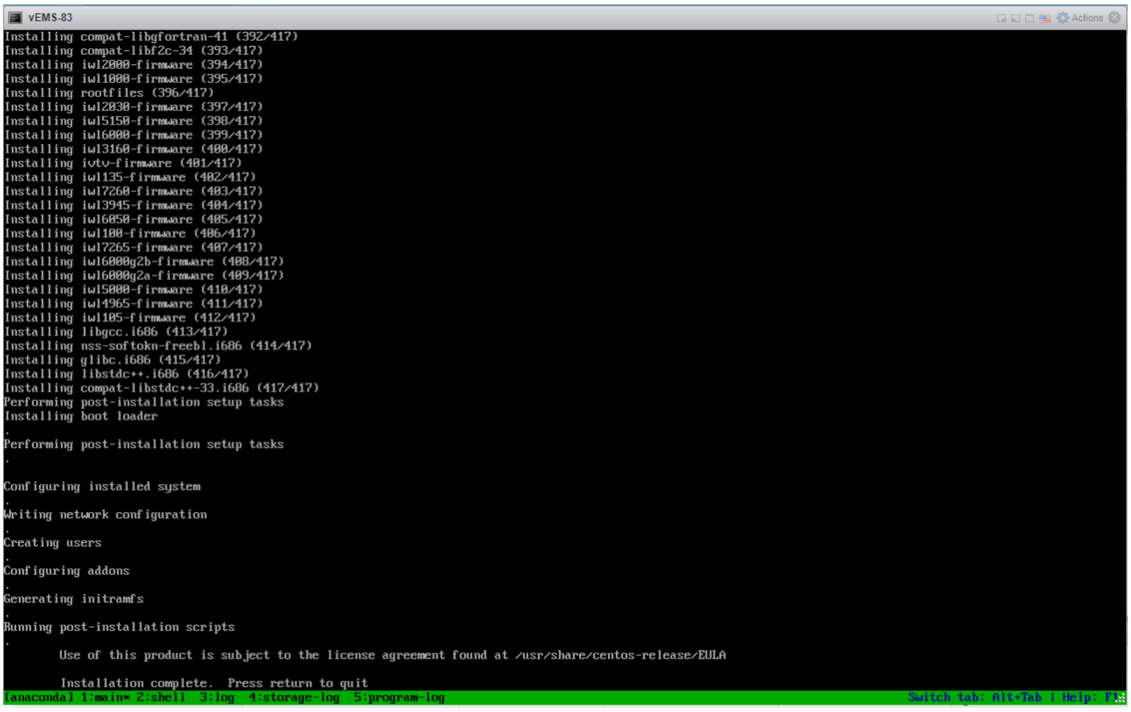
Figure 9-2: CentOS



```
                -----------------================----------------

                           CentOS 7 for OVOC (Rev. 18)

                -----------------================----------------

 -  To start installation, press <ENTER> key.

 -  To start installation from RS-232 serial console, type rs232 <ENTER>.

 -  To boot from local disk, type local <ENTER>.

boot: _
```

6. Wait for the installation to complete.

Figure 9-3: CentOS Installation

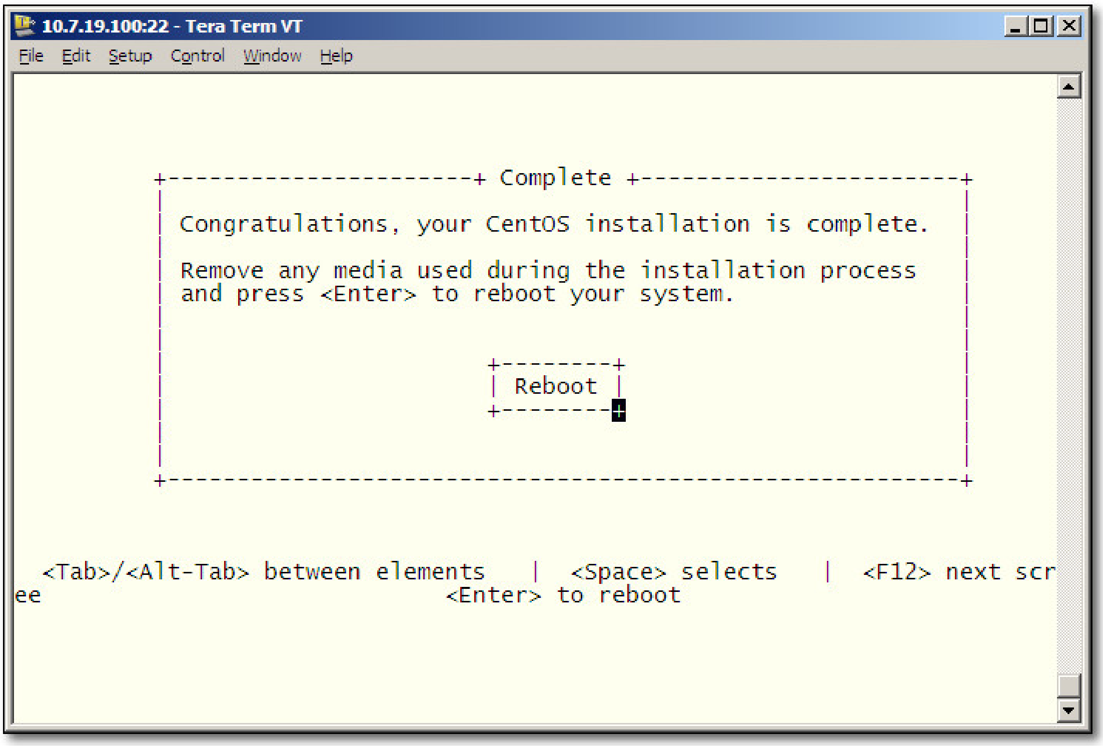


```
Installing compat-libgfortran-41 (392/417)
Installing compat-libf2c-34 (393/417)
Installing iwl2000-firmware (394/417)
Installing iwl1000-firmware (395/417)
Installing rootfiles (396/417)
Installing iwl2030-firmware (397/417)
Installing iwl5150-firmware (398/417)
Installing iwl6000-firmware (399/417)
Installing iwl3160-firmware (400/417)
Installing ivtv-firmware (401/417)
Installing iwl135-firmware (402/417)
Installing iwl7260-firmware (403/417)
Installing iwl3945-firmware (404/417)
Installing iwl6050-firmware (405/417)
Installing iwl100-firmware (406/417)
Installing iwl7265-firmware (407/417)
Installing iwl6000g2b-firmware (408/417)
Installing iwl6000g2a-firmware (409/417)
Installing iwl5000-firmware (410/417)
Installing iwl4965-firmware (411/417)
Installing iwl105-firmware (412/417)
Installing libgcc.i686 (413/417)
Installing nss-softokn-freebl.i686 (414/417)
Installing glibc.i686 (415/417)
Installing libstdc++.i686 (416/417)
Installing compat-libstdc++-33.i686 (417/417)
Performing post-installation setup tasks
Installing boot loader
.
Performing post-installation setup tasks
.

Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
        Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

        Installation complete.  Press return to quit
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log                    Switch tab: Alt+Tab | Help: F1
```

7. Reboot your machine by pressing **Enter**.

> Do not forget to remove the Linux installation DVD from the DVD-ROM before rebooting your machine.

Figure 9-4: Linux CentOS Installation Complete

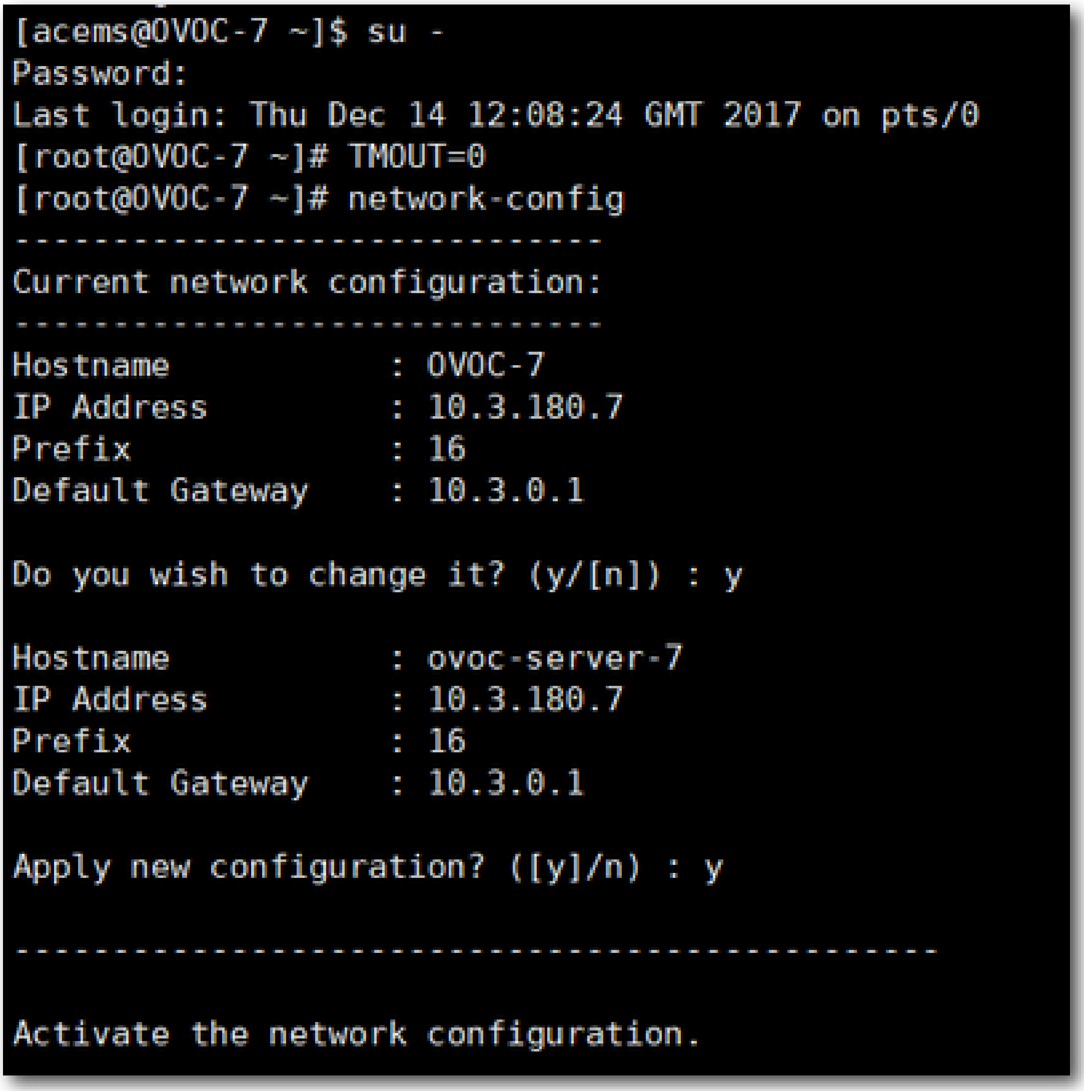


```
          +----------------------+ Complete +-----------------------+
          |                                                         |
          | Congratulations, your CentOS installation is complete.  |
          |                                                         |
          | Remove any media used during the installation process   |
          | and press <Enter> to reboot your system.                |
          |                                                         |
          |                                                         |
          |                        +--------+                       |
          |                        | Reboot |                       |
          |                        +--------+                       |
          |                                                         |
          |                                                         |
          +---------------------------------------------------------+


  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next scr
ee                              <Enter> to reboot
```

8. Login as 'root' user with password *root*.

9. Type **network-config**, and then press Enter; the current configuration is displayed:

Figure 9-5: Linux CentOS Network Configuration



```
[acems@OVOC-7 ~]$ su -
Password:
Last login: Thu Dec 14 12:08:24 GMT 2017 on pts/0
[root@OVOC-7 ~]# TMOUT=0
[root@OVOC-7 ~]# network-config
------------------------------
Current network configuration:
------------------------------
Hostname              : OVOC-7
IP Address            : 10.3.180.7
Prefix                : 16
Default Gateway       : 10.3.0.1

Do you wish to change it? (y/[n]) : y

Hostname              : ovoc-server-7
IP Address            : 10.3.180.7
Prefix                : 16
Default Gateway       : 10.3.0.1

Apply new configuration? ([y]/n) : y

-----------------------------------------------

Activate the network configuration.
```

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

10. You are prompted to change the configuration; enter **y**.

11. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.

12. Confirm the changes; enter **y**.

13. You are prompted to reboot; enter **y**.

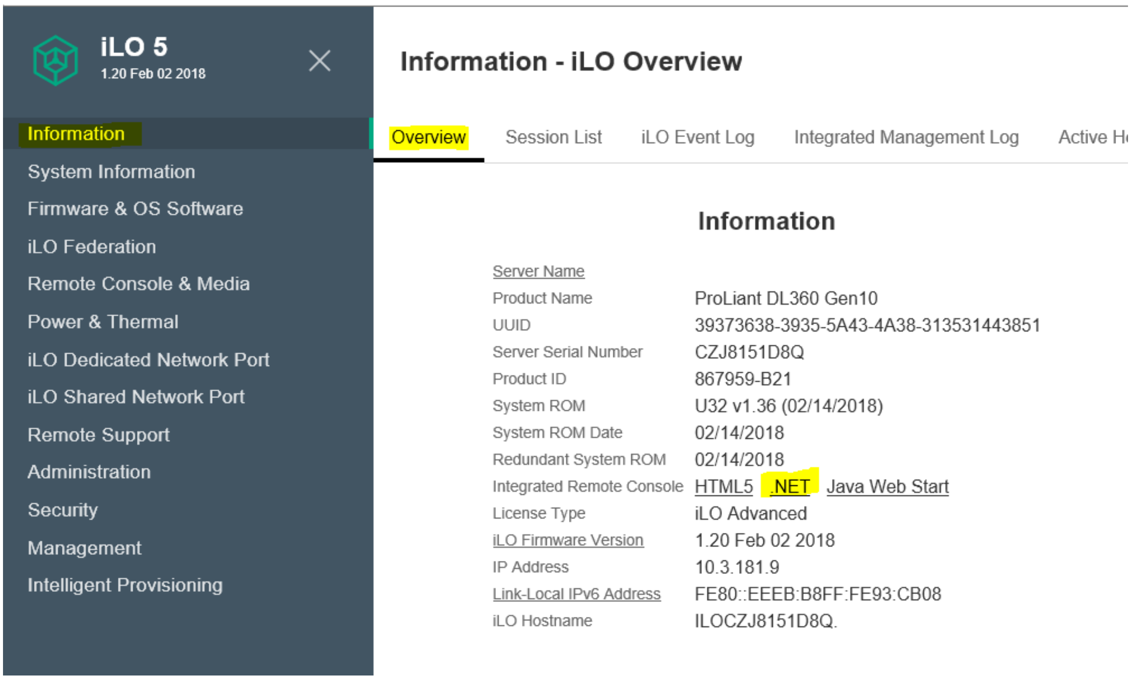
Installing DVD1 without a CD-ROM

This section describes how to install DVD1 without a CD-ROM.

➢ To install DVD1 without a DVD:

1. Login to ILO 5 with “Administrator” privileges.
2. Launch the Integrated Remote Console.

Figure 9-6: Information-iLO Overview



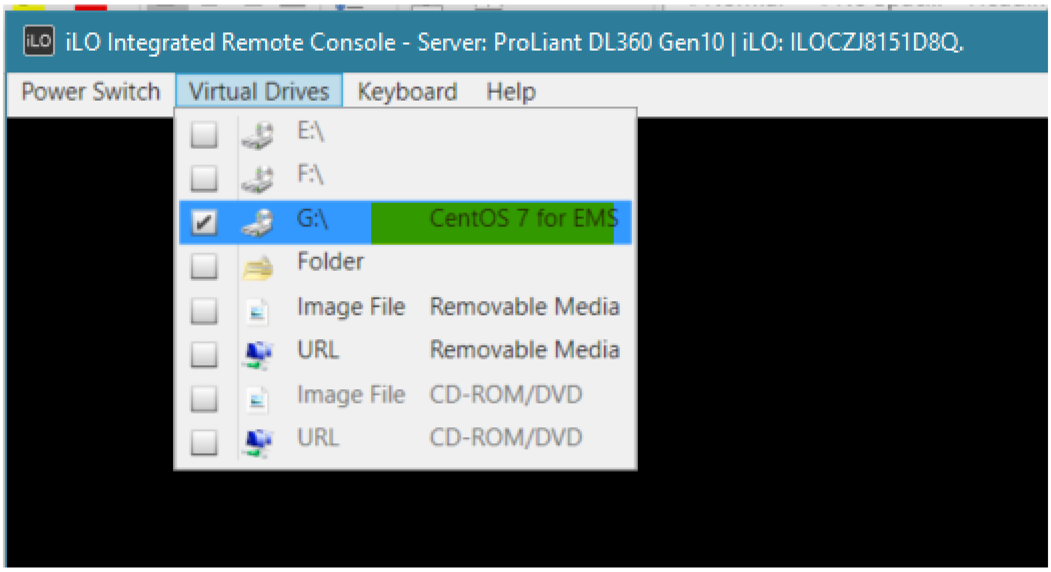
Information - iLO Overview

Information

Server Name	
Product Name	ProLiant DL360 Gen10
UUID	39373638-3935-5A43-4A38-313531443851
Server Serial Number	CZJ8151D8Q
Product ID	867959-B21
System ROM	U32 v1.36 (02/14/2018)
System ROM Date	02/14/2018
Redundant System ROM	02/14/2018
Integrated Remote Console	HTML5 .NET Java Web Start
License Type	iLO Advanced
iLO Firmware Version	1.20 Feb 02 2018
IP Address	10.3.181.9
Link-Local IPv6 Address	FE80::EEEB:B8FF:FE93:CB08
iLO Hostname	ILOCZJ8151D8Q.

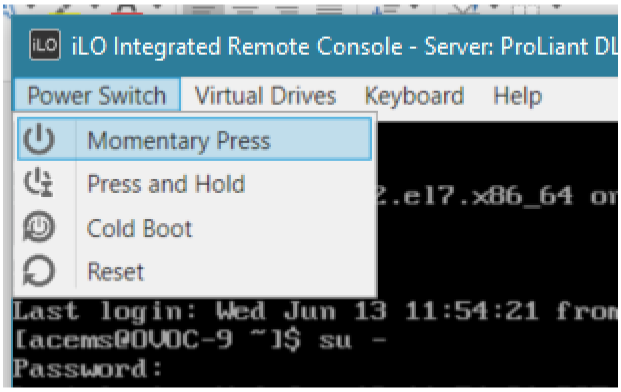
3. On your PC insert the OVOC DVD1 to the drive and note the drive letter.
4. From Integrated Remote Console, click Virtual Drives and select the appropriate drive letter.

Figure 9-7: iLO Integrated Remote Console



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

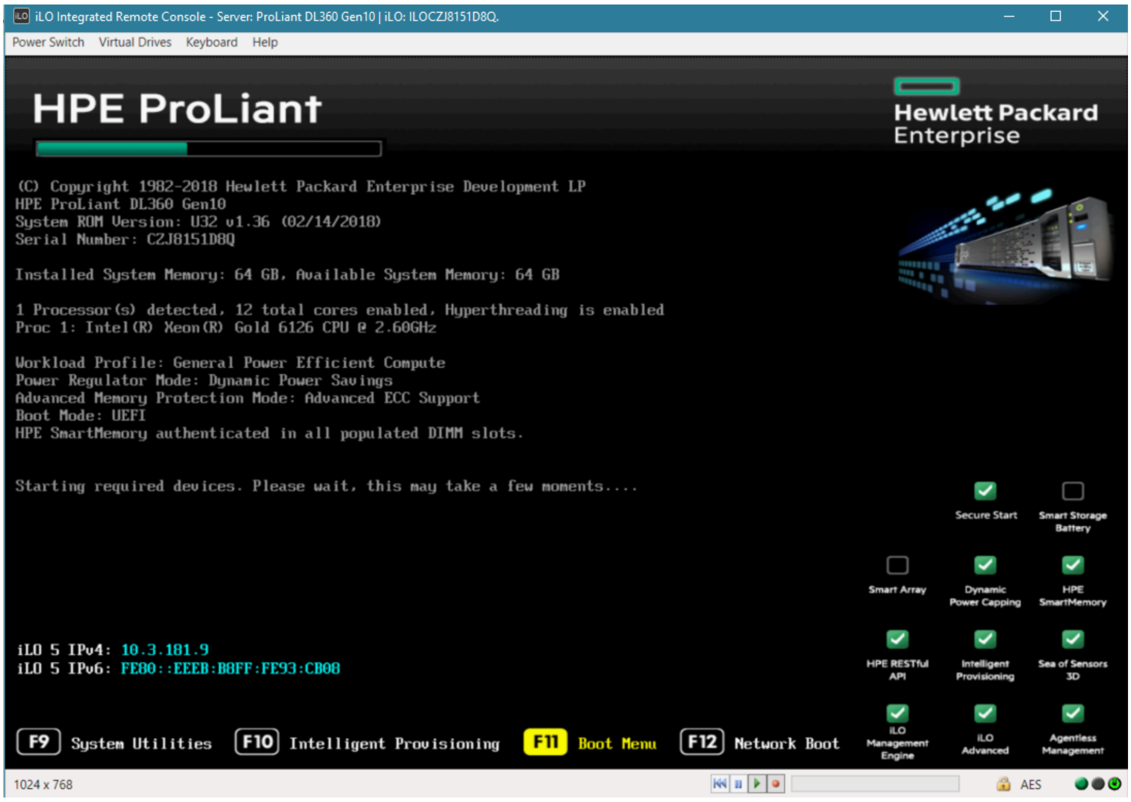
Figure 9-8: Momentary Press



```
2.el7.x86_64 on
Last login: Wed Jun 13 11:54:21 from
[acems@OVOC-9 ~]$ su -
Password:
```

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

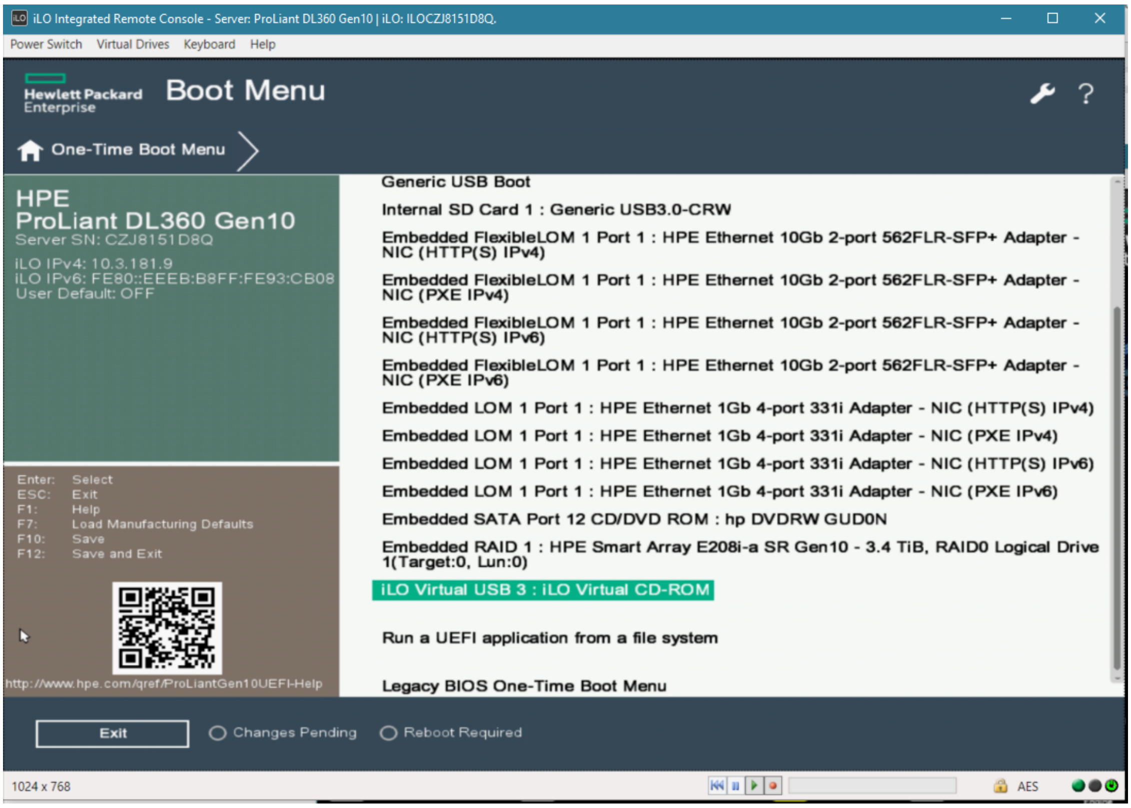
Figure 9-9: Boot Menu



```
(C) Copyright 1982-2018 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v1.36 (02/14/2018)
Serial Number: CZJ8151D8Q

Installed System Memory: 64 GB, Available System Memory: 64 GB

1 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz

Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI
HPE SmartMemory authenticated in all populated DIMM slots.

Starting required devices. Please wait, this may take a few moments....



iLO 5 IPv4: 10.3.181.9
iLO 5 IPv6: FE80::EEEB:B8FF:FE93:CB08

F9 System Utilities   F10 Intelligent Provisioning   F11 Boot Menu   F12 Network Boot
```

6. 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 9-10: Boot Sequence


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch Virtual Drives Keyboard Help
Hewlett Packard Enterprise
Boot Menu
One-Time Boot Menu
Exit
○ Changes Pending
○ Reboot Required
1024 x 768
AES

HPE
ProLiant DL360 Gen10
Server SN: CZJ8151D8Q
iLO IPv4: 10.3.181.9
iLO IPv6: FE80::EEEB:B8FF:FE93:CB08
User Default: OFF

Enter: Select
ESC: Exit
F1: Help
F7: Load Manufacturing Defaults
F10: Save
F12: Save and Exit

http://www.hpe.com/qref/ProLiantGen10UEFI-Help

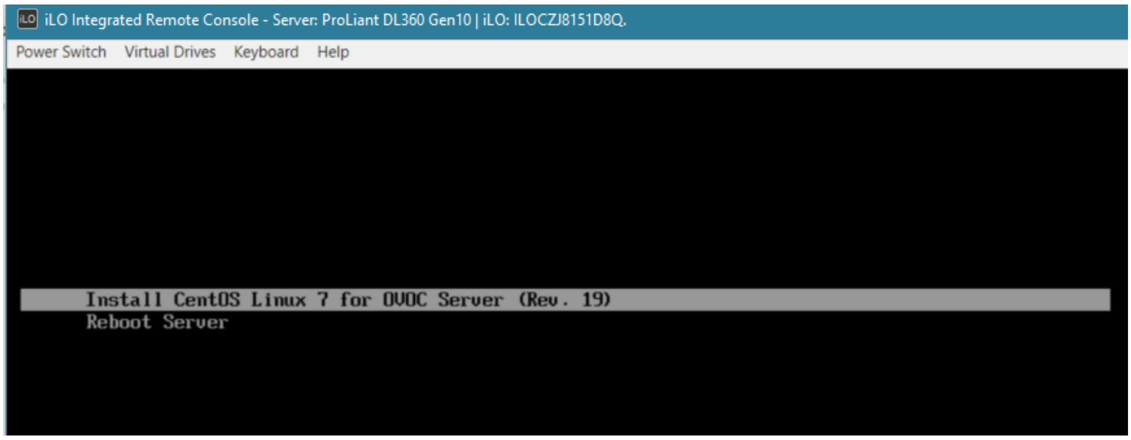
Generic USB Boot
Internal SD Card 1 : Generic USB3.0-CRW
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv6)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv6)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv4)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv4)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv6)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv6)
Embedded SATA Port 12 CD/DVD ROM : hp DVDRW GUD0N
Embedded RAID 1 : HPE Smart Array E208i-a SR Gen10 - 3.4 TiB, RAID0 Logical Drive 1(Target:0, Lun:0)
iLO Virtual USB 3 : iLO Virtual CD-ROM

Run a UEFI application from a file system

Legacy BIOS One-Time Boot Menu

7. The following screen appears, select “Install CentOS …” and press Enter.

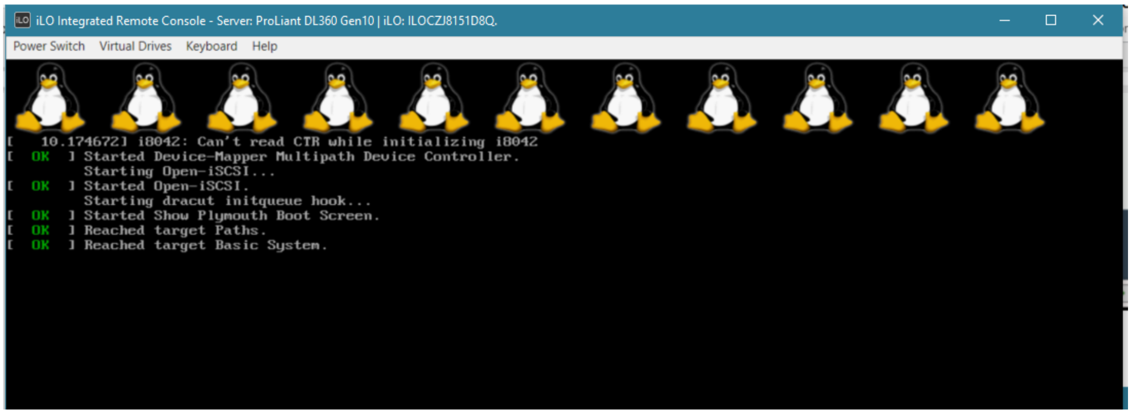
Figure 9-11: Install CentOS


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch Virtual Drives Keyboard Help

```
Install CentOS Linux 7 for OVOC Server (Rev. 19)
Reboot Server
```

8. After a while the CentOS installation commences:

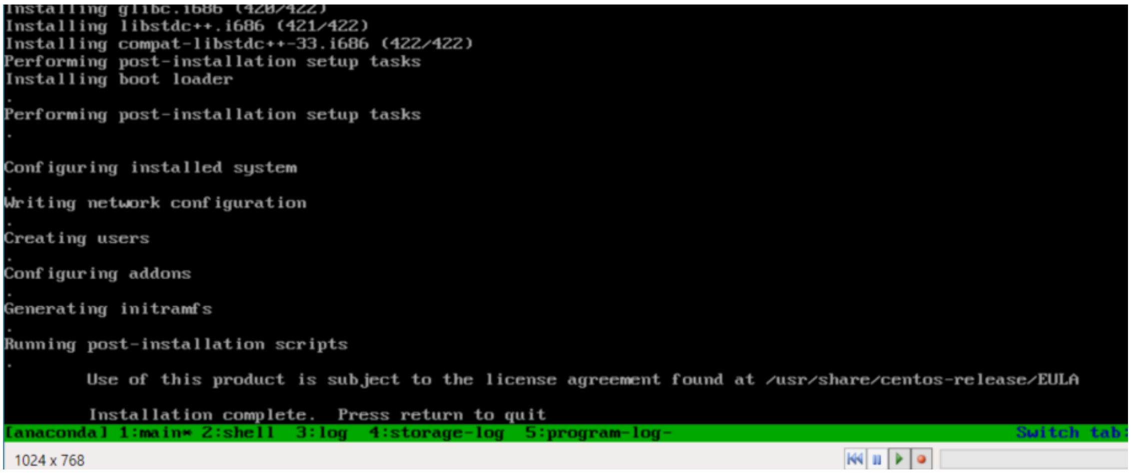
Figure 9-12: Start CentOS


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch
Virtual Drives
Keyboard
Help

```
[   10.174672] i8042: Can't read CTR while initializing i8042
[  OK  ] Started Device-Mapper Multipath Device Controller.
         Starting Open-iSCSI...
[  OK  ] Started Open-iSCSI.
         Starting dracut initqueue hook...
[  OK  ] Started Show Plymouth Boot Screen.
[  OK  ] Reached target Paths.
[  OK  ] Reached target Basic System.
```

9. Wait for the installation to finish, from “Virtual Drives” menu deselect the selected drive and press Enter, the server is rebooted.

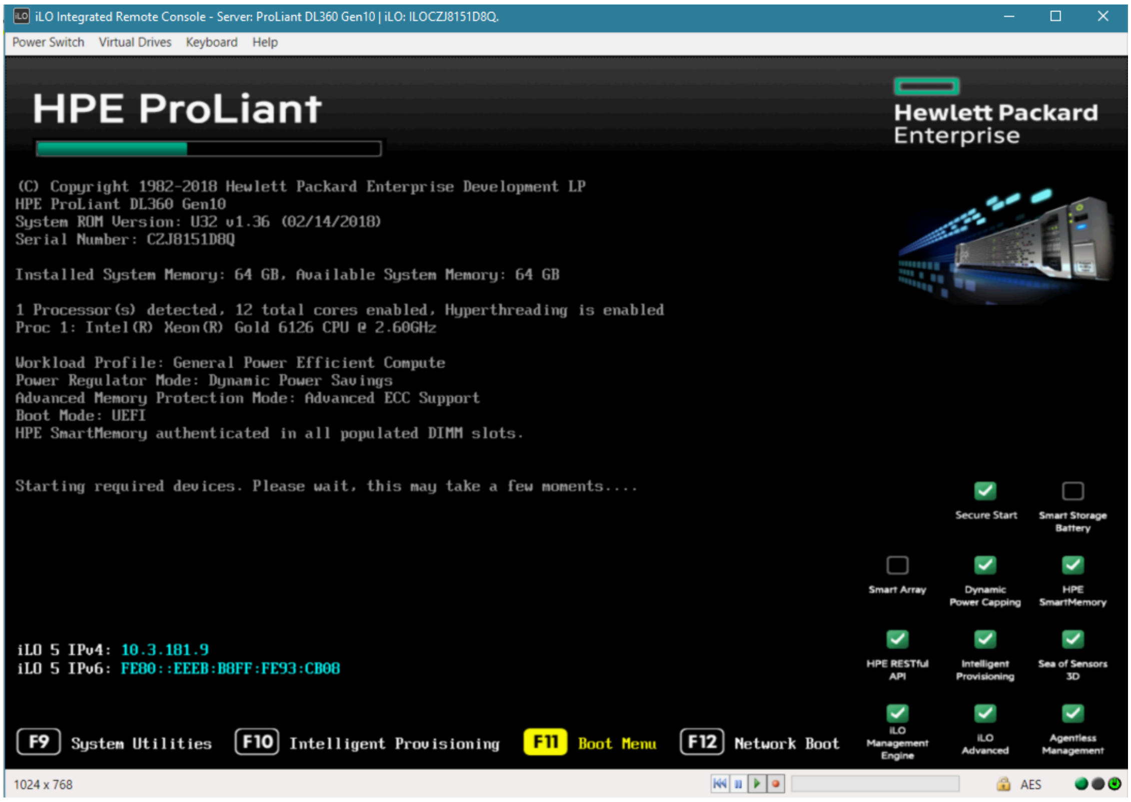
Figure 9-13: Server Rebooted



```
Installing glibc.i686 (420/422)
Installing libstdc++.i686 (421/422)
Installing compat-libstdc++-33.i686 (422/422)
Performing post-installation setup tasks
Installing boot loader

Performing post-installation setup tasks
.
Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
        Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

        Installation complete.  Press return to quit
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log-                              Switch tab:
```

10. After server has restarted, press F11 to enter boot menu.

Figure 9-14: Boot Menu



```
(C) Copyright 1982-2018 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v1.36 (02/14/2018)
Serial Number: CZJ8151D8Q

Installed System Memory: 64 GB, Available System Memory: 64 GB

1 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz

Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI
HPE SmartMemory authenticated in all populated DIMM slots.

Starting required devices. Please wait, this may take a few moments....

iLO 5 IPv4: 10.3.181.9
iLO 5 IPv6: FE80::EEEB:B8FF:FE93:CB08

F9 System Utilities   F10 Intelligent Provisioning   F11 Boot Menu   F12 Network Boot
```

DVD3: OVOC Server Application Installation

The procedure below describes how to install the OVOC server application including the installation of the Postgre SQL database. This procedure takes approximately 20 minutes.

➢ To perform DVD3 installation:

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

```
su - root
```

4. Mount the DVDROM to make it available:

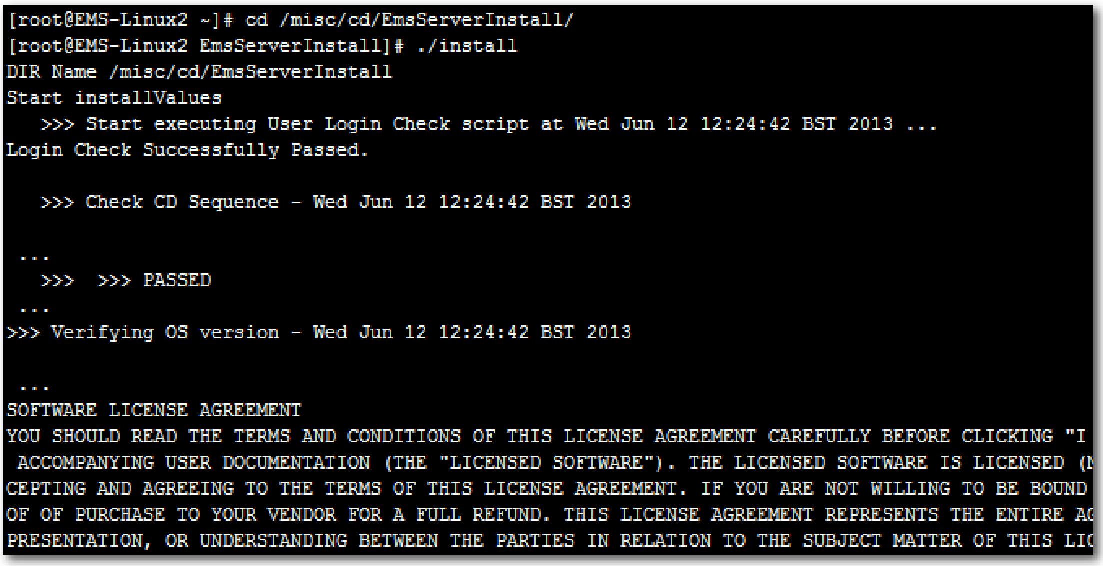
```
mount /home/acems/DVD3_EMS_.iso /mnt/EmsServerInstall/
```

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

5. Run the installation script from its location:

```
./install
```

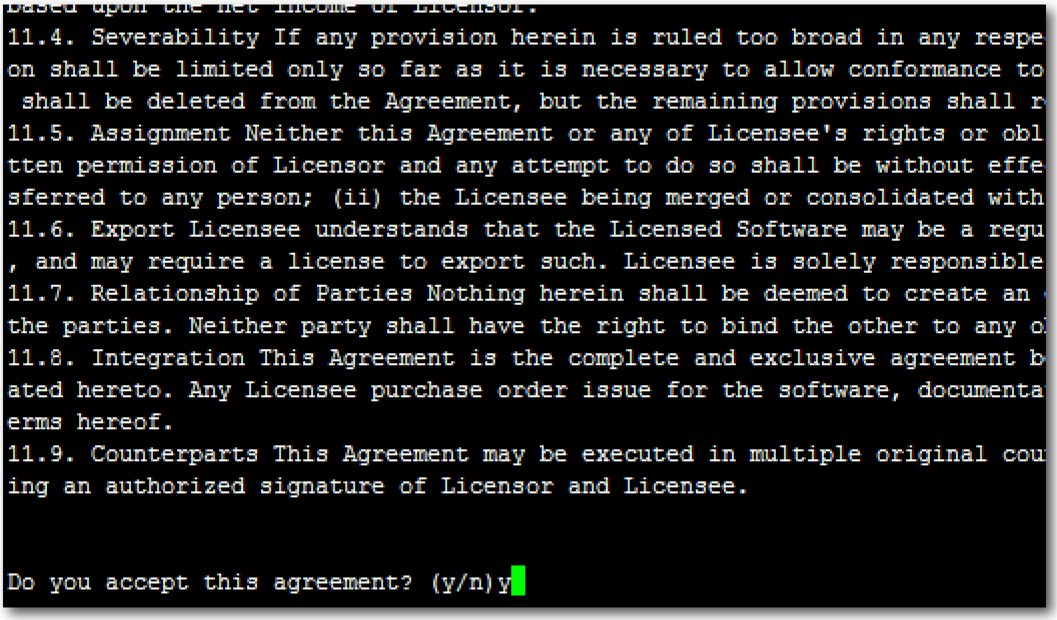
Figure 9-15: OVOC server Application Installation



```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/
[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
   >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

   >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

 ...
   >>>  >>> PASSED
 ...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

 ...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
 ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

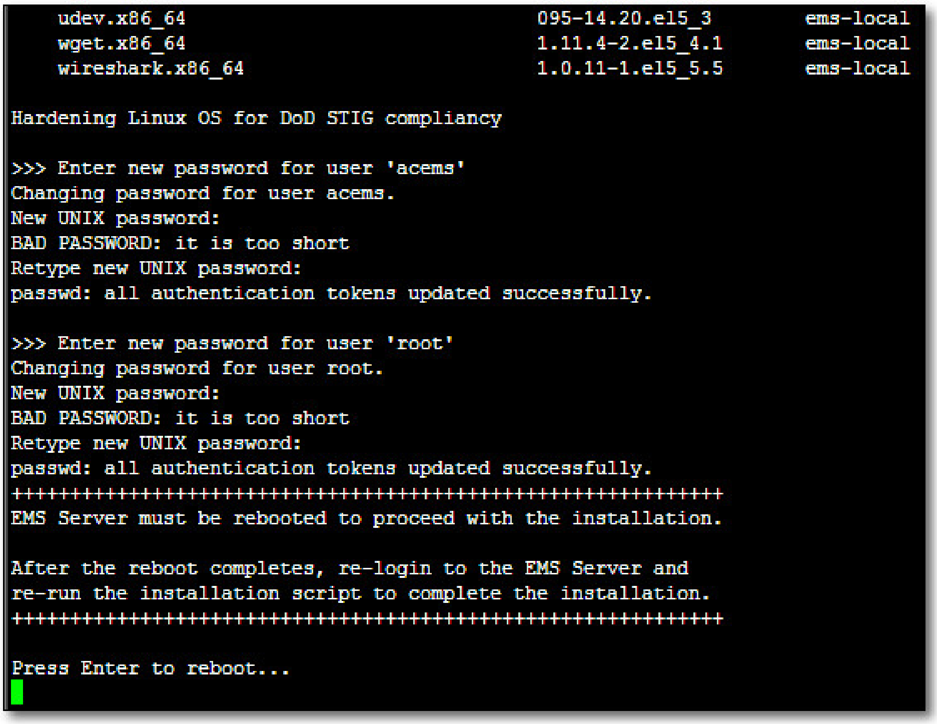
Figure 9-16: OVOC server Application Installation – License Agreement



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


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

7. 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 9-17: OVOC server Application Installation (cont)



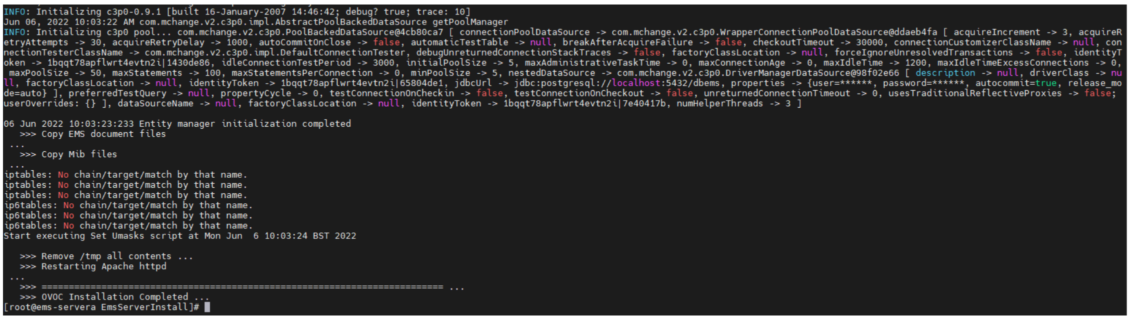
```
    udev.x86_64                             095-14.20.el5_3        ems-local
    wget.x86_64                             1.11.4-2.el5_4.1       ems-local
    wireshark.x86_64                        1.0.11-1.el5_5.5       ems-local

Hardening Linux OS for DoD STIG compliancy

>>> Enter new password for user 'acems'
Changing password for user acems.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

>>> Enter new password for user 'root'
Changing password for user root.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
EMS Server must be rebooted to proceed with the installation.

After the reboot completes, re-login to the EMS Server and
re-run the installation script to complete the installation.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Press Enter to reboot...
```

8. The installation process verifies whether CentOS 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 180 to Enter y, and then press Enter to accept the License agreement. on page 181

Figure 9-18: OVOC Server Installation Complete



```
INFO: Initializing c3p0-0.9.1 [built 16-January-2007 14:46:42; debug? true; trace: 10]
Jun 06, 2022 10:03:22 AM com.mchange.v2.c3p0.impl.AbstractPoolBackedDataSource getPoolManager
INFO: Initializing c3p0 pool... com.mchange.v2.c3p0.PoolBackedDataSource@4cb80ca7 [ connectionPoolDataSource -> com.mchange.v2.c3p0.WrapperConnectionPoolDataSource@ddaeb4fa [ acquireIncrement -> 3, acquireR
etryAttempts -> 30, acquireRetryDelay -> 1000, autoCommitOnClose -> false, automaticTestTable -> null, breakAfterAcquireFailure -> false, checkoutTimeout -> 30000, connectionCustomizerClassName -> null, con
nectionTesterClassName -> com.mchange.v2.c3p0.impl.DefaultConnectionTester, debugUnreturnedConnectionStackTraces -> false, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, identityT
oken -> 1bqqt78apflwrt4evtn2i|1430de86, idleConnectionTestPeriod -> 3000, initialPoolSize -> 5, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 1200, maxIdleTimeExcessConnections -> 0,
 maxPoolSize -> 50, maxStatements -> 100, maxStatementsPerConnection -> 0, minPoolSize -> 5, nestedDataSource -> com.mchange.v2.c3p0.DriverManagerDataSource@98f02e66 [ description -> null, driverClass -> nu
ll, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|65804de1, jdbcUrl -> jdbc:postgresql://localhost:5432/dbems, properties -> {user=******, password=******, autocommit=true, release_mo
de=auto} ], preferredTestQuery -> null, propertyCycle -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, usesTraditionalReflectiveProxies -> false;
userOverrides: {} ], dataSourceName -> null, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|7e40417b, numHelperThreads -> 3 ]

06 Jun 2022 10:03:23:233 Entity manager initialization completed
   >>> Copy EMS document files
 ...
   >>> Copy Mib files
 ...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
Start executing Set Umasks script at Mon Jun  6 10:03:24 BST 2022

   >>> Remove /tmp all contents ...
   >>> Restarting Apache httpd
 ...
   >>> ======================================================================== ...
   >>> OVOC Installation Completed ...
[root@ems-servera EmsServerInstall]#
```

9. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.

10. When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems.*

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

    ```
    su - root
    ```

12. Type the following command:

    ```
    # EmsServerManager
    ```

13. Verify that all processes are up and running (Viewing Process Statuses on page 201) and verify login to the OVOC Web client is successful.

14. Verify that the Date and Time are set correctly (Date and Time Settings on page 245).

15. Configure other settings as required (Getting Started on page 196).

Part III

Post Installation

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

10 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 93).
- Upgrade from Single Organization tenant to Multitenant (Upgrading from Single Tenant to Multitenant on page 111

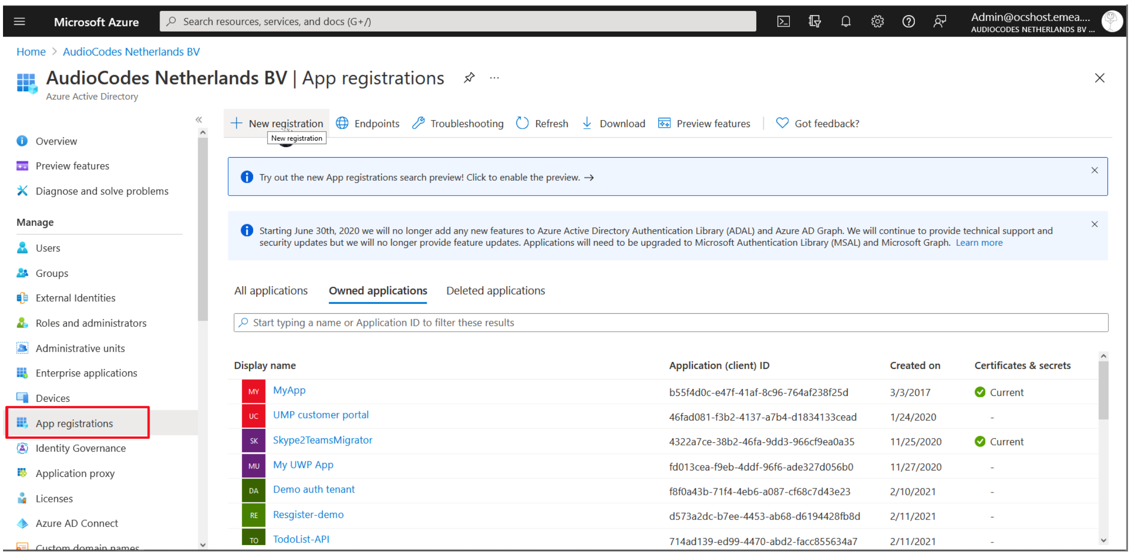
Registering Single Tenant in Organizational Directory

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 123). 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 10-1: App registrations



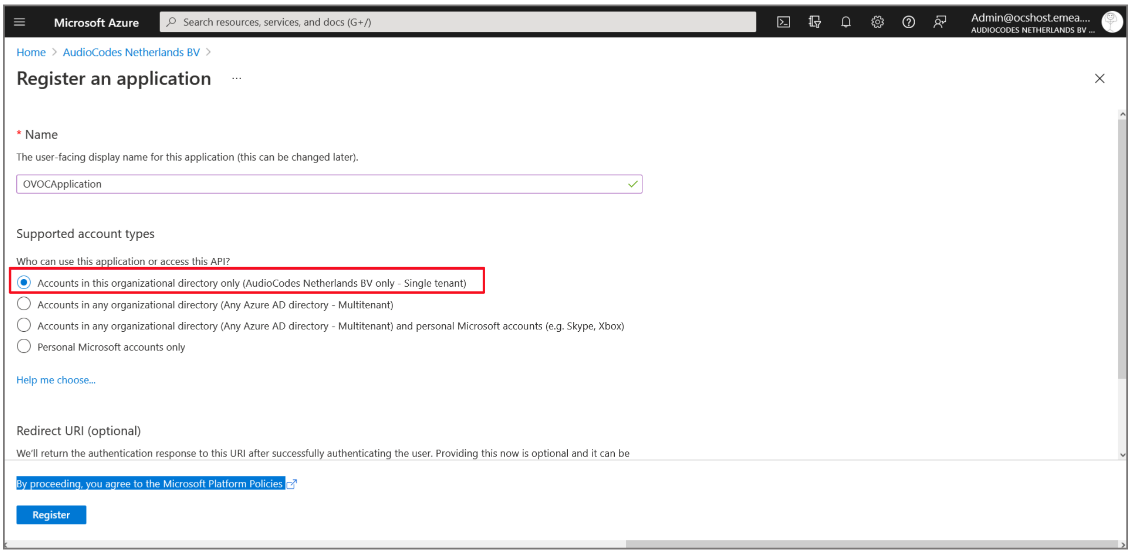
Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Display name	Application (client) ID	Created on	Certificates & secrets
MY MyApp	b55f4d0c-e47f-41af-8c96-764af238f25d	3/3/2017	✓ Current
UC UMP customer portal	46fad081-f3b2-4137-a7b4-d1834133cead	1/24/2020	-
SK Skype2TeamsMigrator	4322a7ce-38b2-46fa-9dd3-966cf9ea0a35	11/25/2020	✓ Current
MU My UWP App	fd013cea-f9eb-4ddf-96f6-ade327d056b0	11/27/2020	-
DA Demo auth tenant	f8f0a43b-71f4-4eb6-a087-cf68c7d43e23	2/10/2021	-
RE Resgister-demo	d573a2dc-b7ee-4453-ab68-d6194428fb8d	2/11/2021	-
TO TodoList-API	714ad139-ed99-4470-abd2-facc855634a7	2/11/2021	-

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

Figure 10-2: Single Organizational Tenant



Home > AudioCodes Netherlands BV >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

OVOCApplication

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be

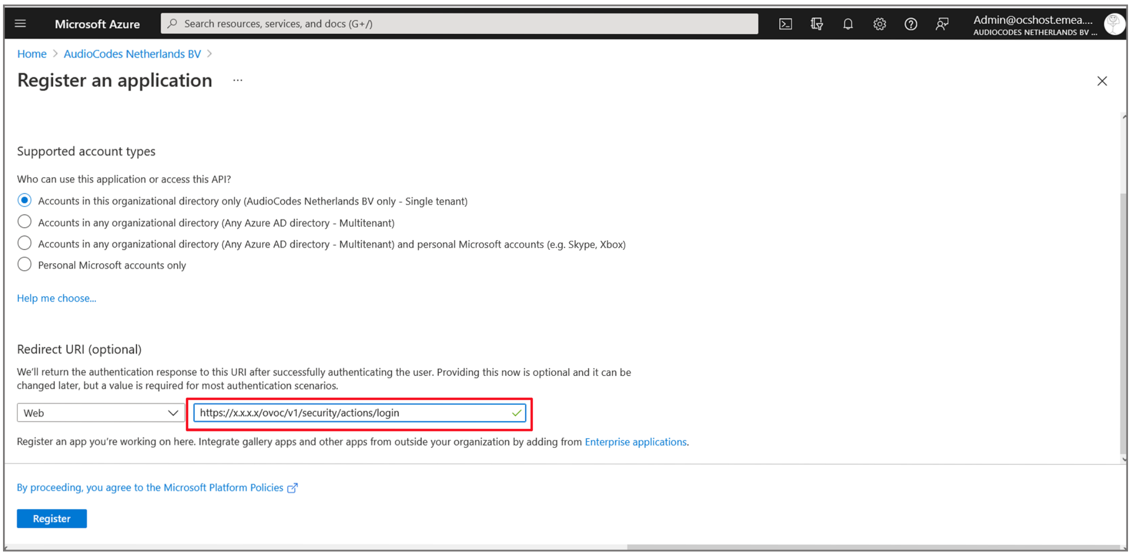
By proceeding, you agree to the Microsoft Platform Policies

Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Register

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

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

Figure 10-3: Register an application



Home > AudioCodes Netherlands BV >

Register an application

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

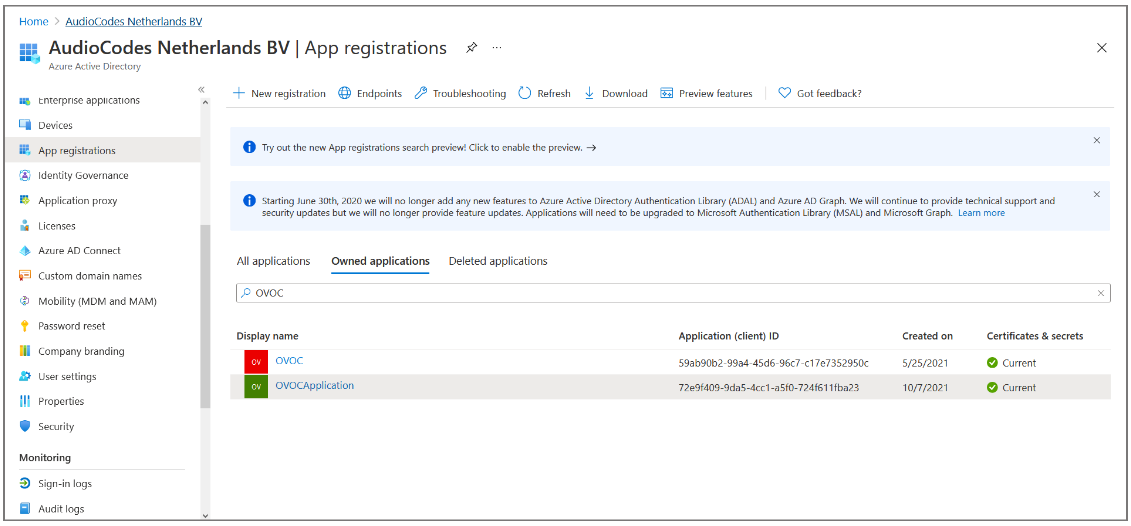
By proceeding, you agree to the Microsoft Platform Policies

Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Register

6. Click **Register**.

   The new registered application is displayed.

Figure 10-4: New Registered Application



Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

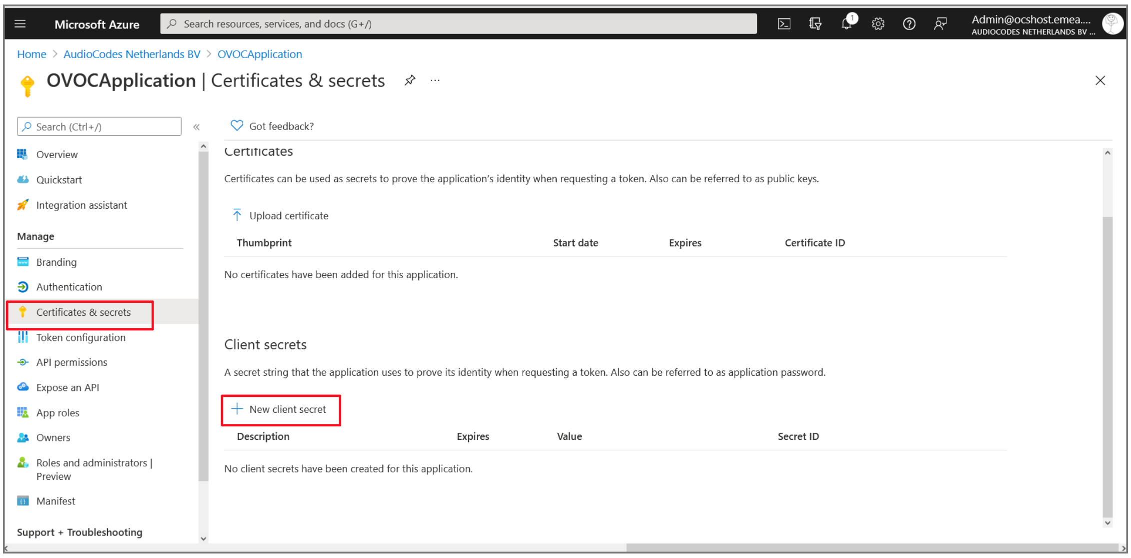
OVOC

Display name	Application (client) ID	Created on	Certificates & secrets
OV OVOC	59ab90b2-99a4-45d6-96c7-c17e7352950c	5/25/2021	✓ Current
OV OVOCApplication	72e9f409-9da5-4cc1-a5f0-724f611fba23	10/7/2021	✓ Current

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

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

Figure 10-5: Certificates & secrets



Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

Client secrets

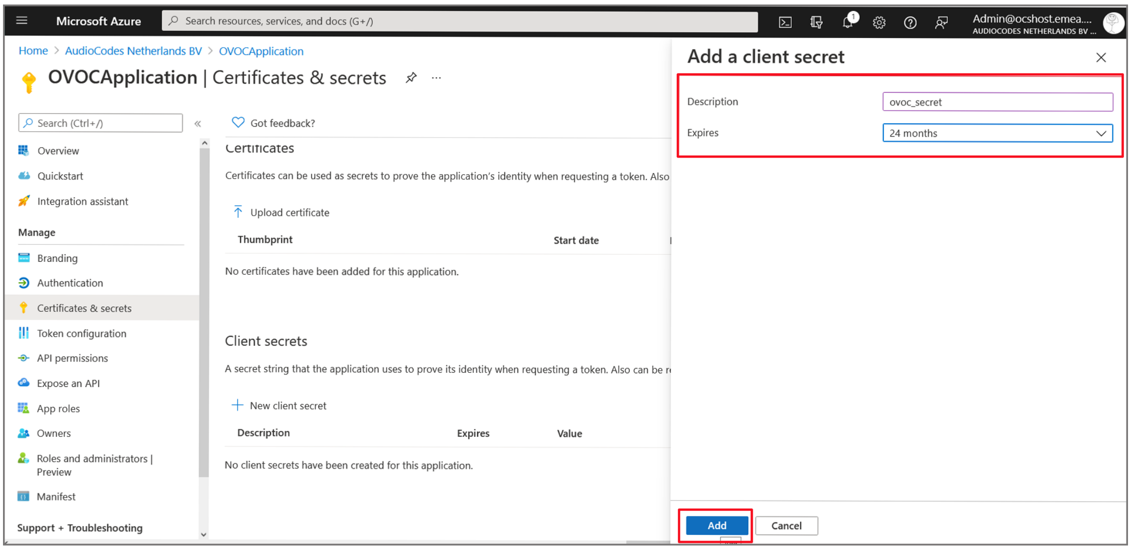
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

9. Click **New client secret**.

Figure 10-6: New client secret



Home > AudioCodes Netherlands BV > OVOCApplication

OVOCApplication | Certificates & secrets

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also

Upload certificate

Thumbprint	Start date

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be r

New client secret

Description	Expires	Value

No client secrets have been created for this application.

Add a client secret

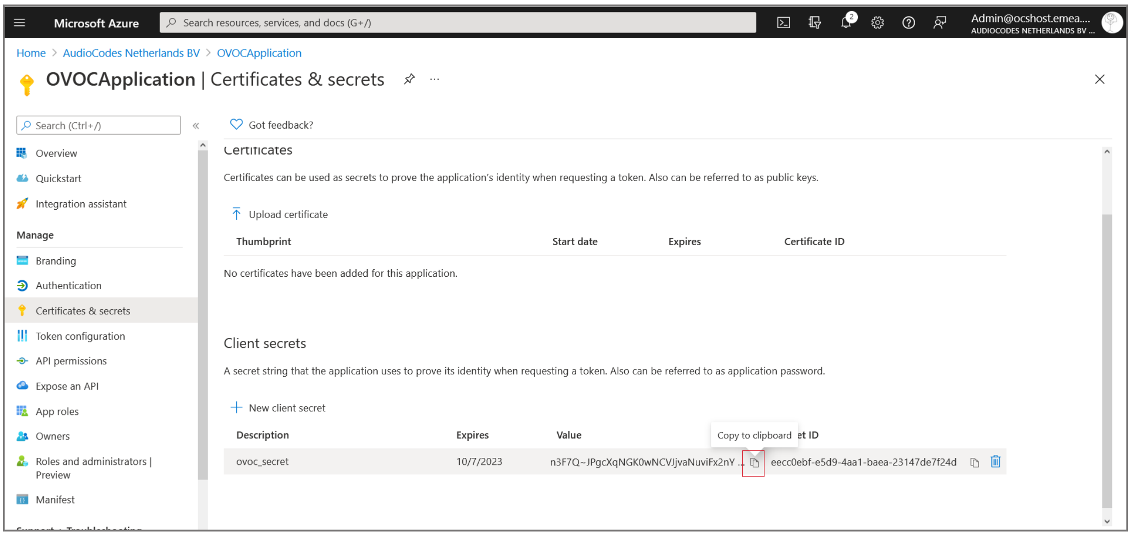
Description: ovoc_secret

Expires: 24 months

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

11. Click **Add**.

Figure 10-7: Client Secret Generated



Home > AudioCodes Netherlands BV > OVOCApplication

OVOCApplication | Certificates & secrets

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

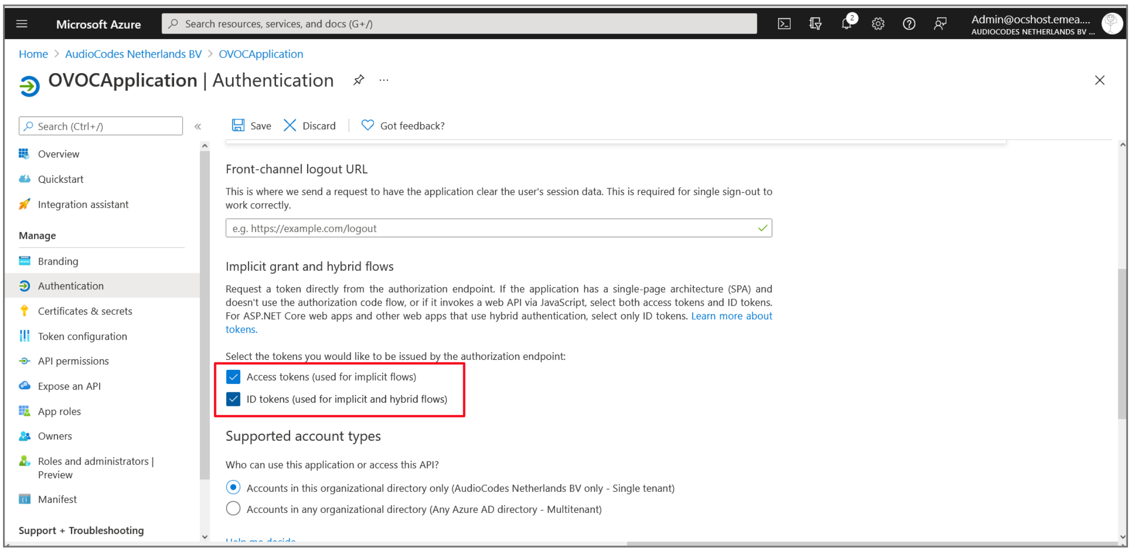
New client secret

Description	Expires	Value	Secret ID
ovoc_secret	10/7/2023	n3F7Q~JPgcXqNGK0wNCVJjvaNuviFx2nY ...	eecc0ebf-e5d9-4aa1-baea-23147de7f24d

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 10-8: Authentication



Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

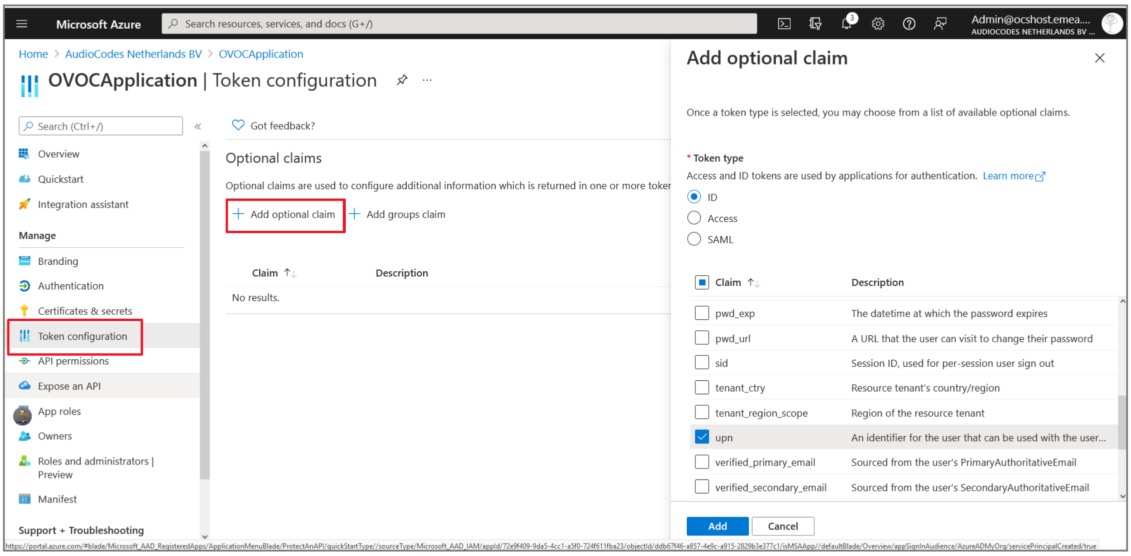
Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

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 10-9: Token configuration



Optional claims

Optional claims are used to configure additional information which is returned in one or more toker

Claim ↑↓	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

● ID

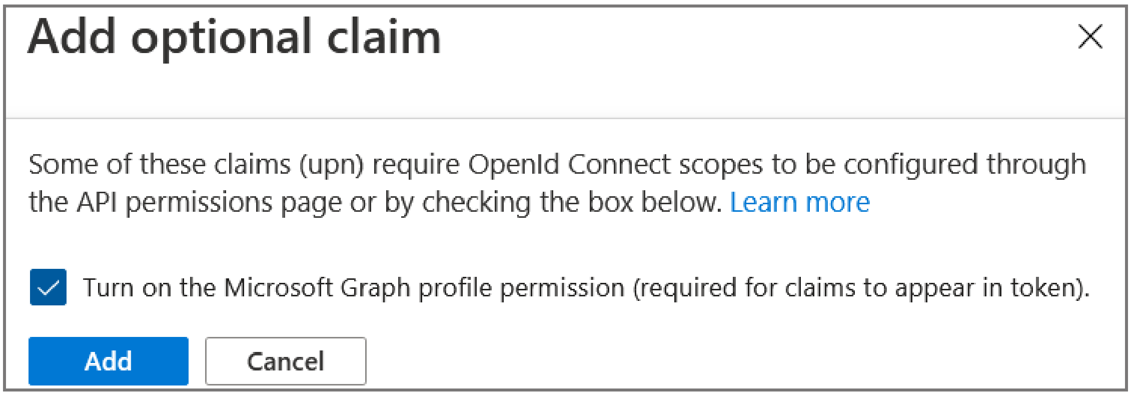
○ Access

○ SAML

	Claim ↑↓	Description
□	pwd_exp	The datetime at which the password expires
□	pwd_url	A URL that the user can visit to change their password
□	sid	Session ID, used for per-session user sign out
□	tenant_ctry	Resource tenant's country/region
□	tenant_region_scope	Region of the resource tenant
☑	upn	An identifier for the user that can be used with the user...
□	verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
□	verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail

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

Figure 10-10: Add Optional claim



Add optional claim

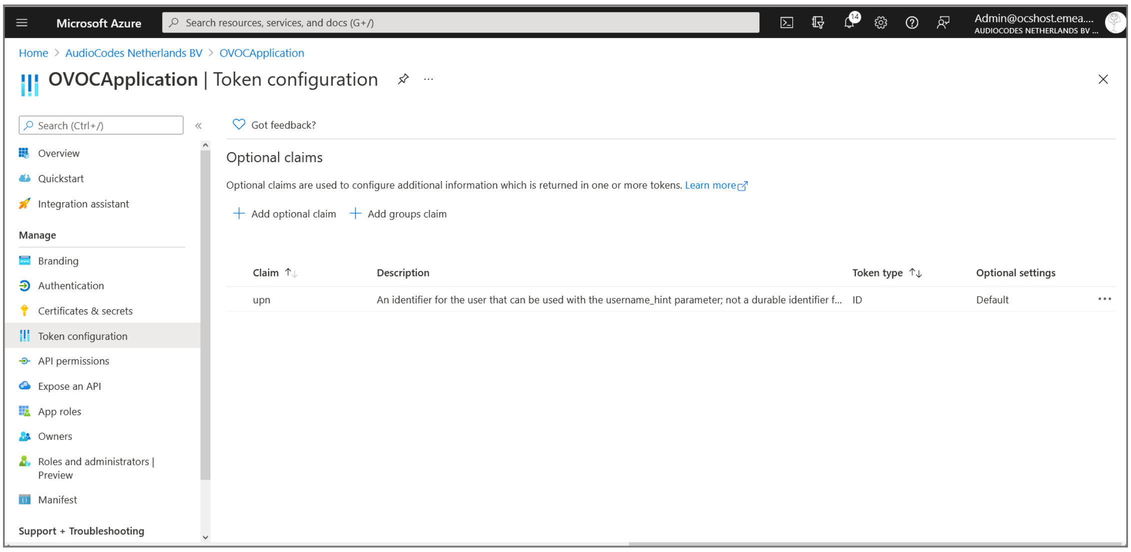
Some of these claims (upn) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph profile permission (required for claims to appear in token).

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 10-11: New UPN Claim



OVOCApplication | Token configuration

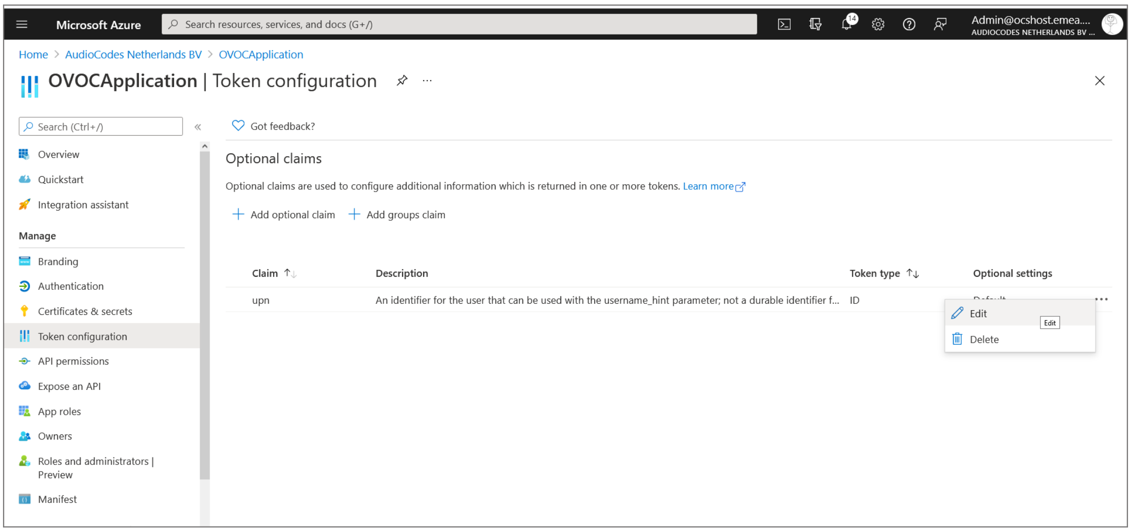
Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description	Token type	Optional settings
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier f...	ID	Default

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

Figure 10-12: Edit Optional Claim



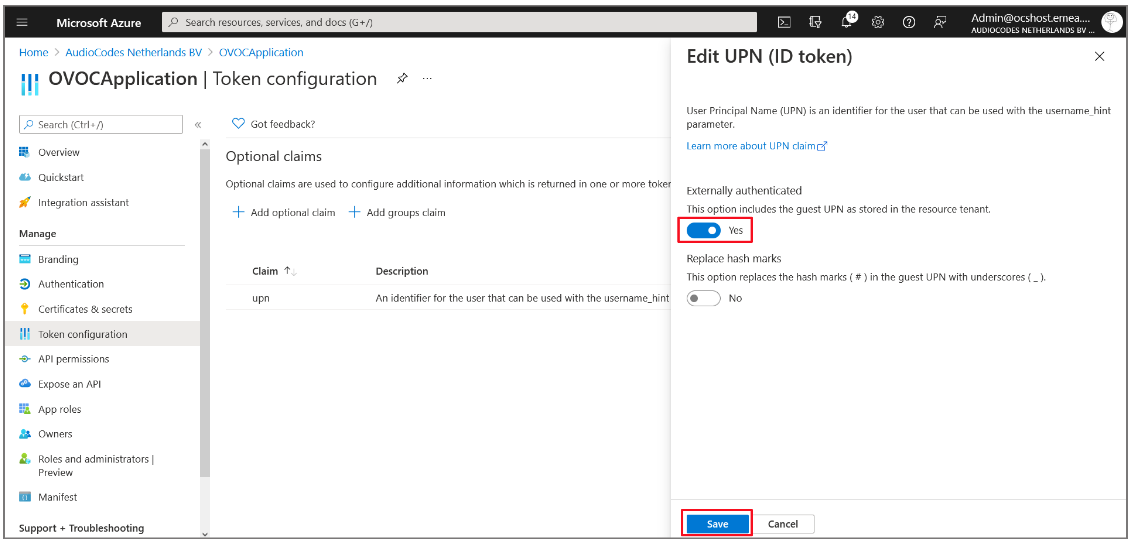
Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description	Token type	Optional settings
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier f...	ID	Default

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 10-13: Edit UPN (ID token)



Optional claims

Optional claims are used to configure additional information which is returned in one or more toker

Claim	Description
upn	An identifier for the user that can be used with the username_hint

Edit UPN (ID token)

User Principal Name (UPN) is an identifier for the user that can be used with the username_hint parameter.

Learn more about UPN claim

Externally authenticated

This option includes the guest UPN as stored in the resource tenant.

● Yes

Replace hash marks

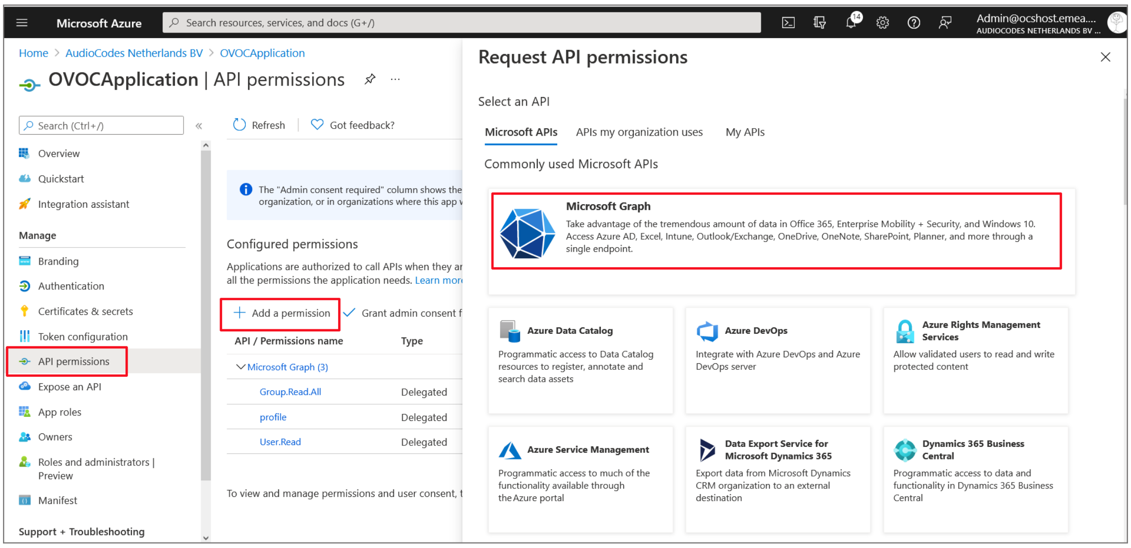
This option replaces the hash marks (#) in the guest UPN with underscores (_).

○ No

24. Click **Save**.

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

Figure 10-14: API Permissions



The "Admin consent required" column shows the organization, or in organizations where this app w

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (3)	
Group.Read.All	Delegated
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog: Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps: Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services: Allow validated users to read and write protected content

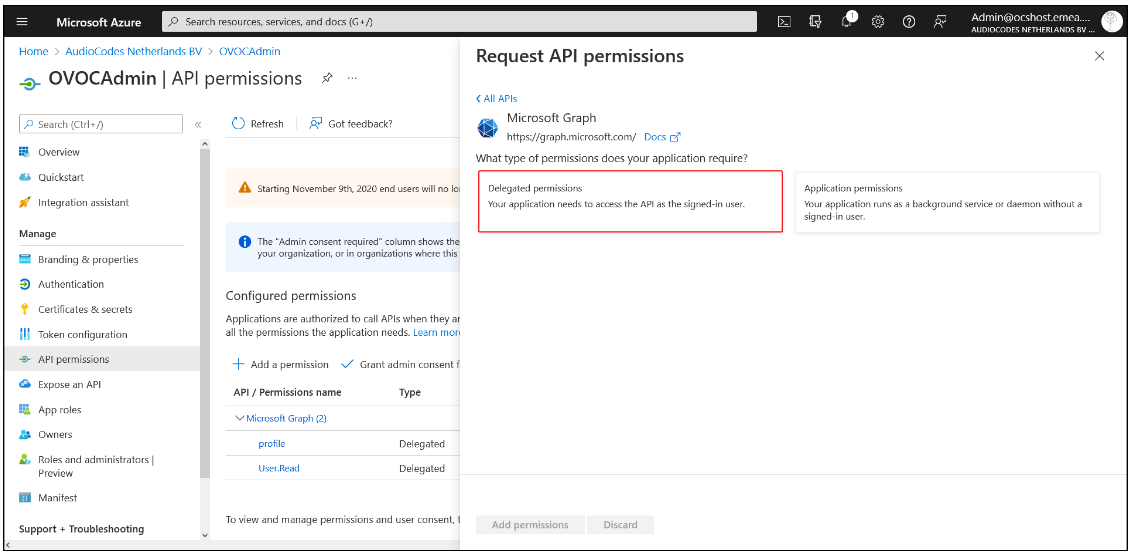
Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365: Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central

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

Figure 10-15: Delegated permissions



Starting November 9th, 2020 end users will no lo

The "Admin consent required" column shows the your organization, or in organizations where this

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

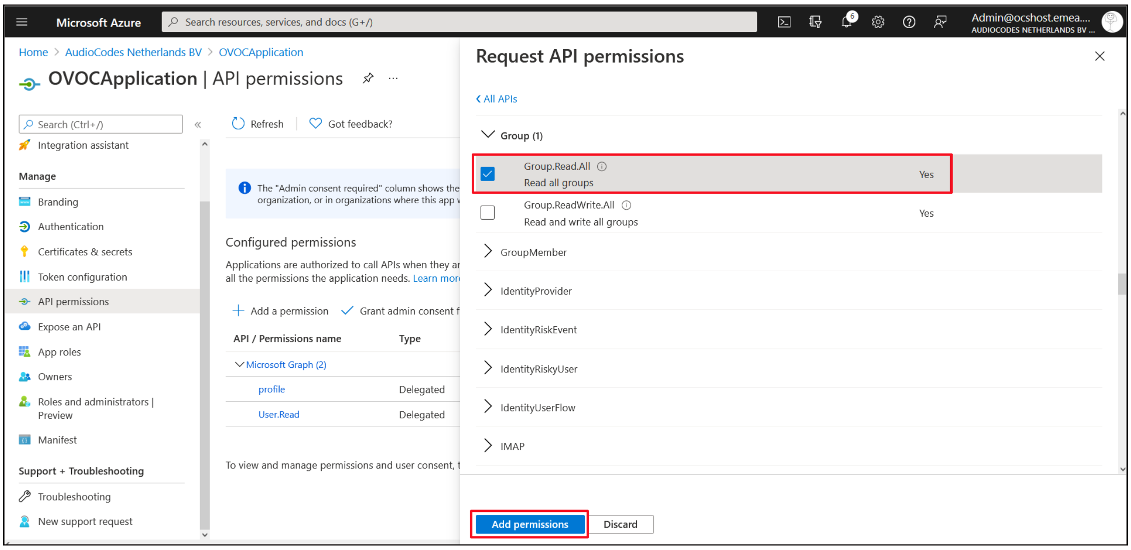
What type of permissions does your application require?

Delegated permissions: Your application needs to access the API as the signed-in user.

Application permissions: Your application runs as a background service or daemon without a signed-in user.

27. Click **Delegated permissions**.

Figure 10-16: Microsoft Graph Permissions



Request API permissions

< All APIs

Group (1)

	Permission	Admin consent required
☑	Group.Read.All Read all groups	Yes
☐	Group.ReadWrite.All Read and write all groups	Yes

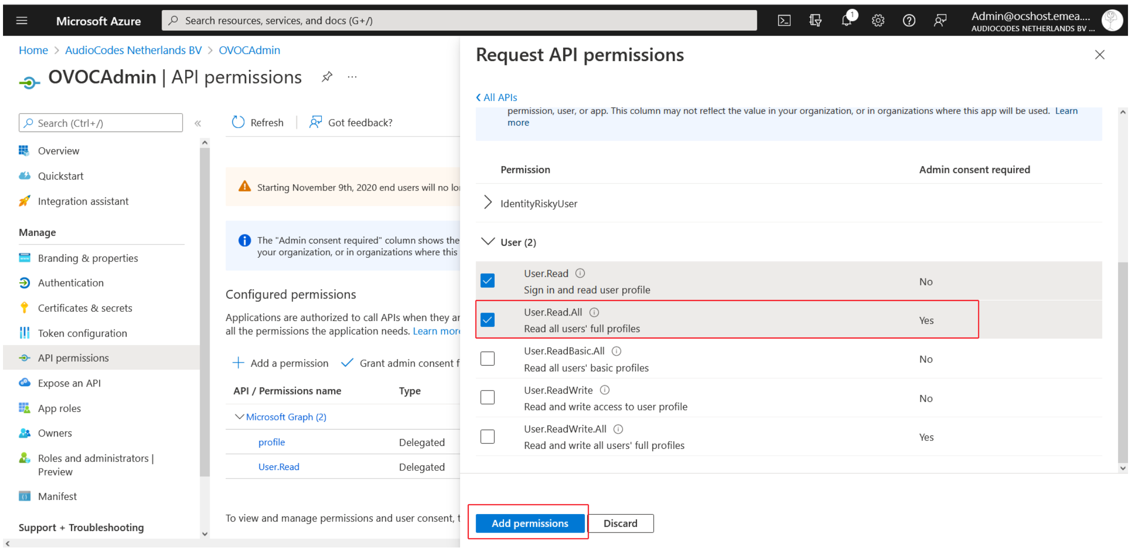
> GroupMember
> IdentityProvider
> IdentityRiskEvent
> IdentityRiskyUser
> IdentityUserFlow
> IMAP

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

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 10-17: Delegated permissions



Request API permissions

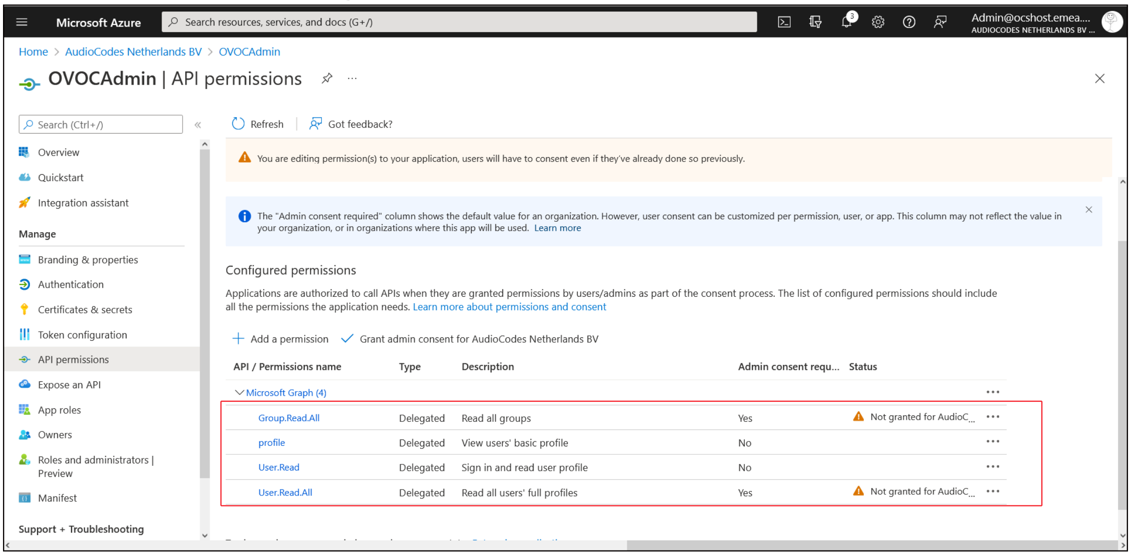
< All APIs

	Permission	Admin consent required
>	IdentityRiskyUser	
	User (2)	
☑	User.Read Sign in and read user profile	No
☑	User.Read.All Read all users' full profiles	Yes
☐	User.ReadBasic.All Read all users' basic profiles	No
☐	User.ReadWrite Read and write access to user profile	No
☐	User.ReadWrite.All Read and write all users' full profiles	Yes

The configured API permissions are displayed.

Figure 10-18: Configured API Permissions

Figure 10-19:



OVOCAdmin | API permissions

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

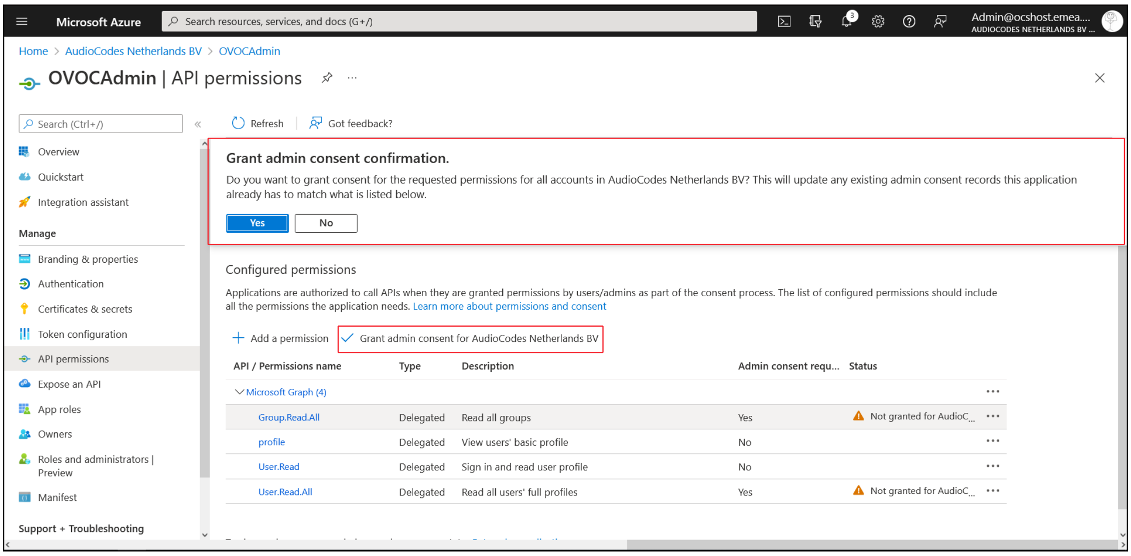
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for AudioCodes Netherlands BV

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Group.Read.All	Delegated	Read all groups	Yes	Not granted for AudioC...
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for AudioC...

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 10-20: Grant Admin Consent for all Accounts



OVOCAdmin | API permissions

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in AudioCodes Netherlands BV? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

Configured permissions

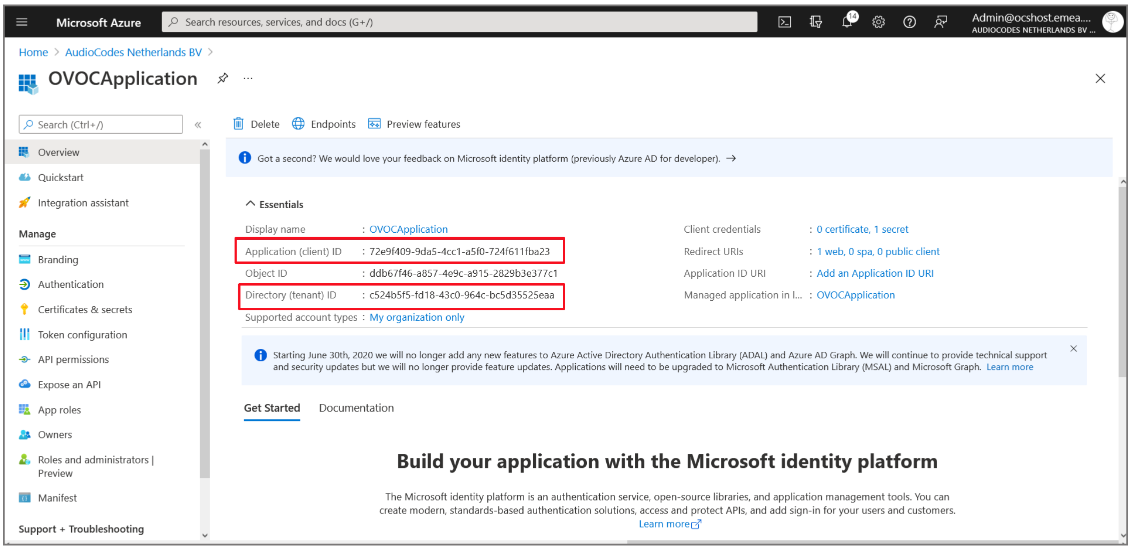
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for AudioCodes Netherlands BV

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Group.Read.All	Delegated	Read all groups	Yes	Not granted for AudioC...
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for AudioC...

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

Figure 10-21: Overview Page



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : OVOCApplication

Application (client) ID : 72e9f409-9da5-4cc1-a5f0-724f611fba23

Object ID : ddb67f46-a857-4e9c-a915-2829b3e377c1

Directory (tenant) ID : c524b5f5-fd18-43c0-964c-bc5d35525eaa

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in l... : OVOCApplication

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers.
Learn more

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 123

34. Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings - Single Tenant Setup below

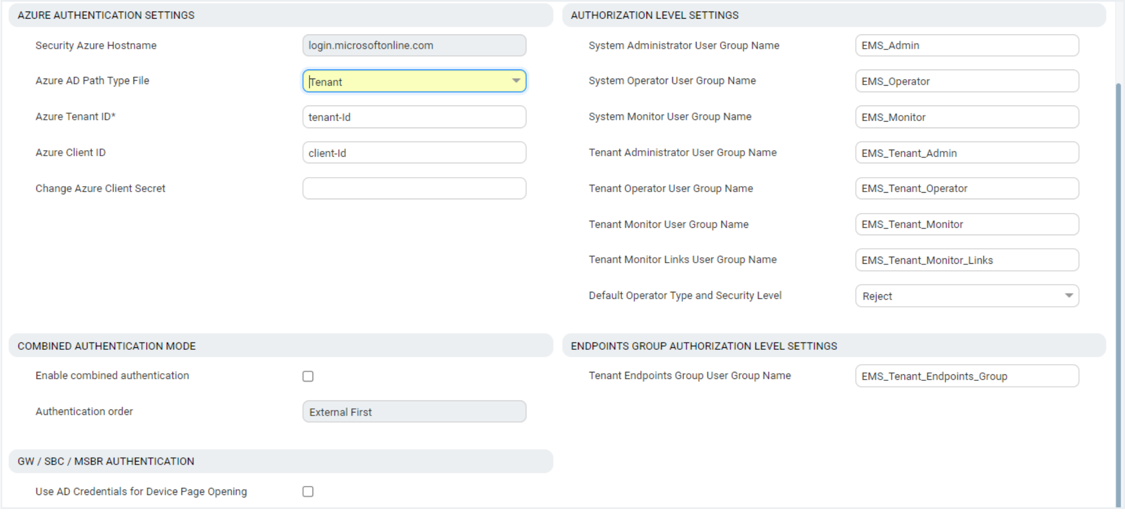
Configuring OVOC Web Azure Settings - Single Tenant Setup

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 10-22: Azure Main Tenant Authentication Settings



AZURE AUTHENTICATION SETTINGS

Security Azure Hostname	login.microsoftonline.com
Azure AD Path Type File	Tenant
Azure Tenant ID*	tenant-Id
Azure Client ID	client-Id
Change Azure Client Secret	

AUTHORIZATION LEVEL SETTINGS

System Administrator User Group Name	EMS_Admin
System Operator User Group Name	EMS_Operator
System Monitor User Group Name	EMS_Monitor
Tenant Administrator User Group Name	EMS_Tenant_Admin
Tenant Operator User Group Name	EMS_Tenant_Operator
Tenant Monitor User Group Name	EMS_Tenant_Monitor
Tenant Monitor Links User Group Name	EMS_Tenant_Monitor_Links
Default Operator Type and Security Level	Reject

COMBINED AUTHENTICATION MODE

Enable combined authentication	□
Authentication order	External First

ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS

Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group

GW / SBC / MSBR AUTHENTICATION

Use AD Credentials for Device Page Opening	□

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**.

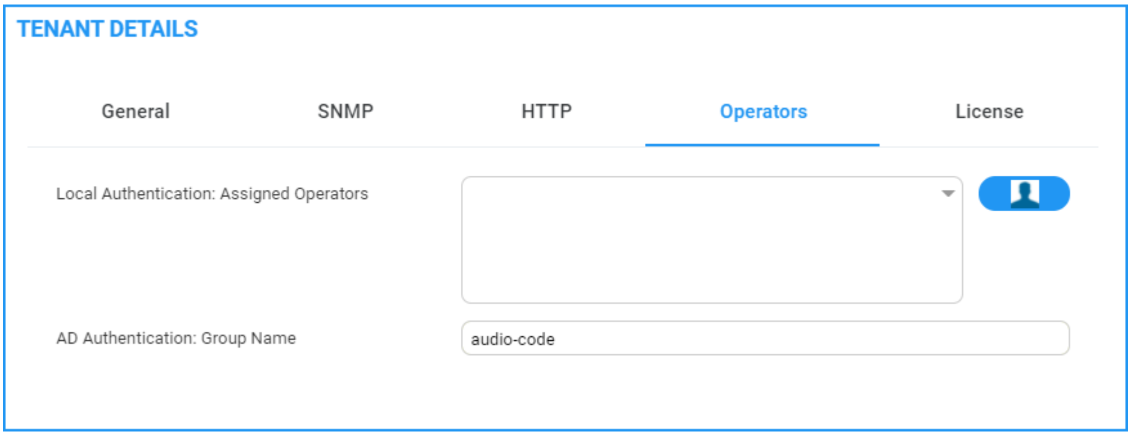
6. In the screen section 'GW / SBC / MSBR Authentication', select the option 'Use AD Credentials for Device Page Opening' for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to OVOC. The AudioCodes device will then perform authentication with the Azure 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 10-23: AD Authentication Group Name

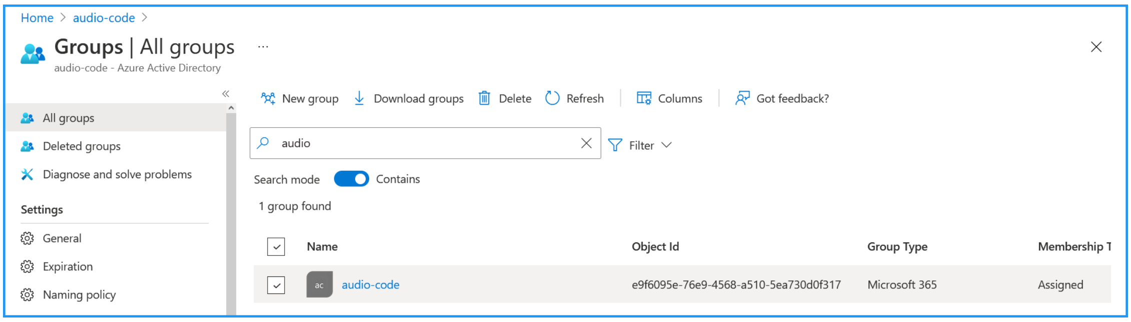


TENANT DETAILS

Local Authentication: Assigned Operators

AD Authentication: Group Name: audio-code

Figure 10-24: Matching Group on Azure



Home > audio-code >

Groups | All groups

audio-code - Azure Active Directory

audio

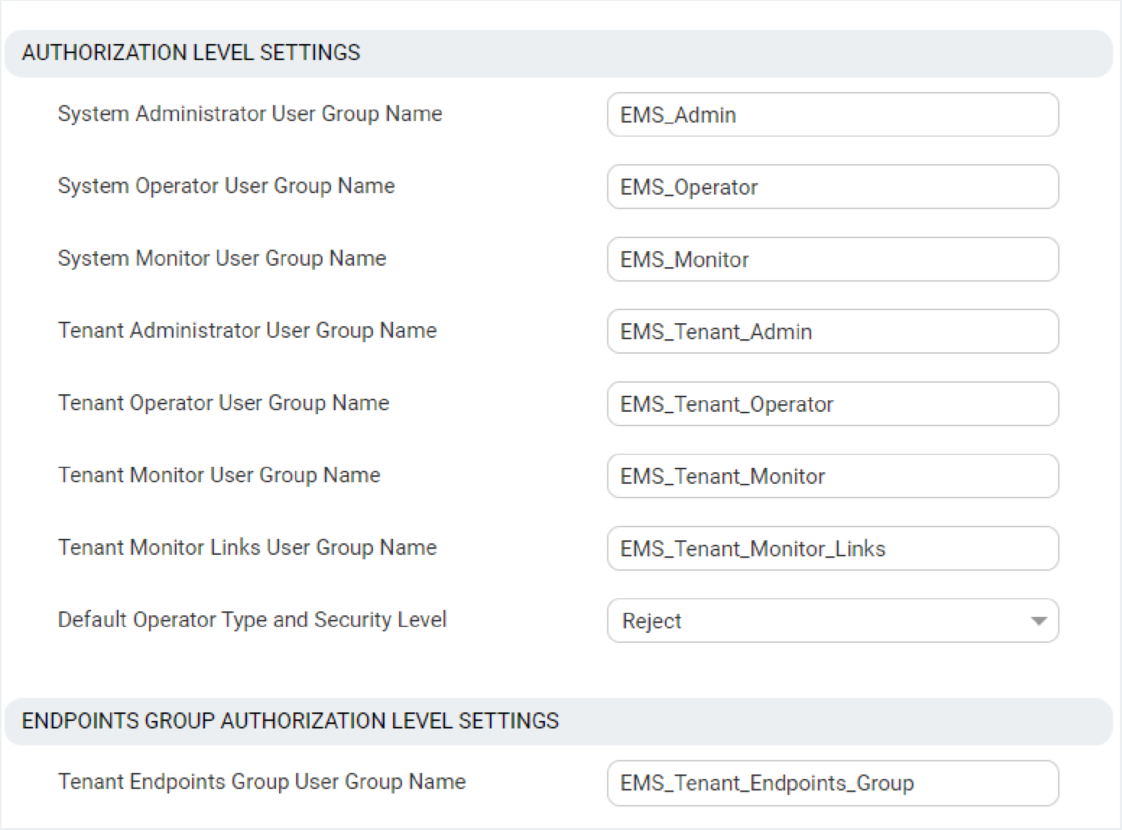
Search mode: Contains

1 group found

☑	Name	Object Id	Group Type	Membership T
☑	ac audio-code	e9f6095e-76e9-4568-a510-5ea730d0f317	Microsoft 365	Assigned

7. In the screen section Authorization Level Settings, configure the user group names exactly as defined on Azure in Create Azure Groups and Assign Members on page 123. When an operator is not assigned to a group on Azure, the parameter 'Default Operator Type and Security Level' is applied.

Figure 10-25: Authorization Level Settings



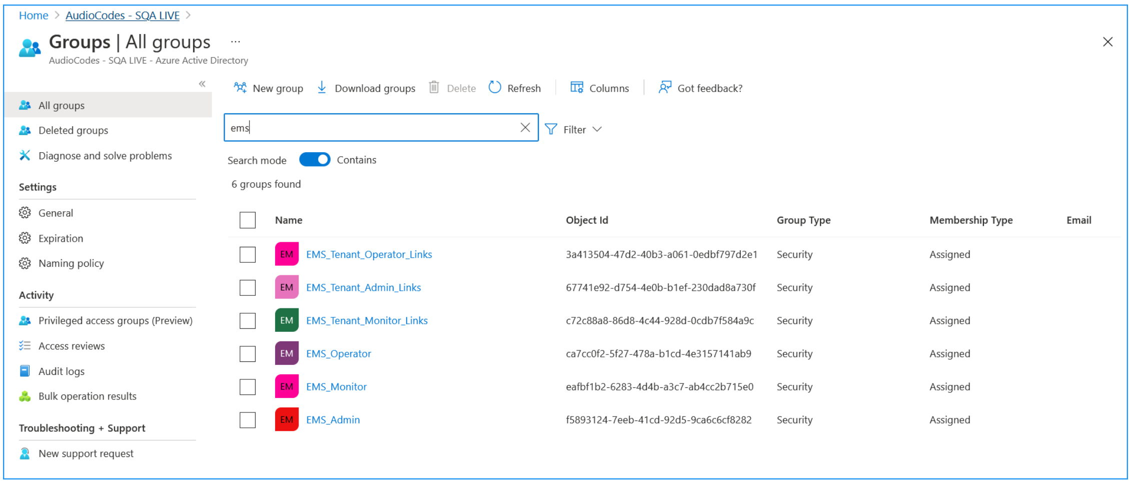
AUTHORIZATION LEVEL SETTINGS

System Administrator User Group Name	EMS_Admin
System Operator User Group Name	EMS_Operator
System Monitor User Group Name	EMS_Monitor
Tenant Administrator User Group Name	EMS_Tenant_Admin
Tenant Operator User Group Name	EMS_Tenant_Operator
Tenant Monitor User Group Name	EMS_Tenant_Monitor
Tenant Monitor Links User Group Name	EMS_Tenant_Monitor_Links
Default Operator Type and Security Level	Reject

ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS

Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group

Figure 10-26: Matching Groups on Azure



ems

Search mode Contains

6 groups found

□	Name	Object Id	Group Type	Membership Type	Email
□	EM EMS_Tenant_Operator_Links	3a413504-47d2-40b3-a061-0edbf797d2e1	Security	Assigned	
□	EM EMS_Tenant_Admin_Links	67741e92-d754-4e0b-b1ef-230dad8a730f	Security	Assigned	
□	EM EMS_Tenant_Monitor_Links	c72c88a8-86d8-4c44-928d-0cdb7f584a9c	Security	Assigned	
□	EM EMS_Operator	ca7cc0f2-5f27-478a-b1cd-4e3157141ab9	Security	Assigned	
□	EM EMS_Monitor	eafbf1b2-6283-4d4b-a3c7-ab4cc2b715e0	Security	Assigned	
□	EM EMS_Admin	f5893124-7eeb-41cd-92d5-9ca6c6cf8282	Security	Assigned	

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 128):

- Registered Service Provider Tenants

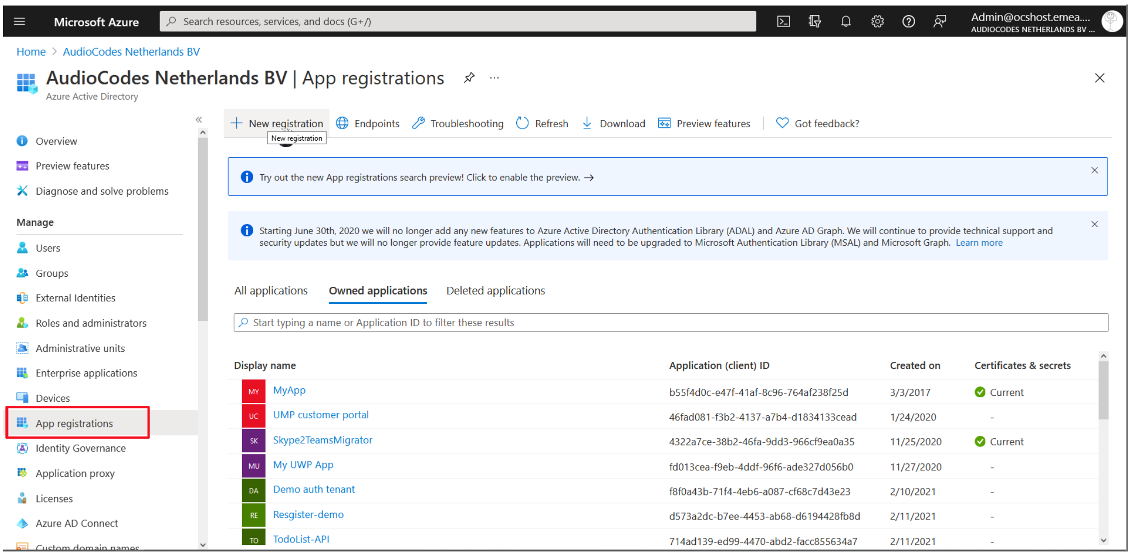
- Registered Channels
- Registered Customers

> ⚠ 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 10-27: App Registrations

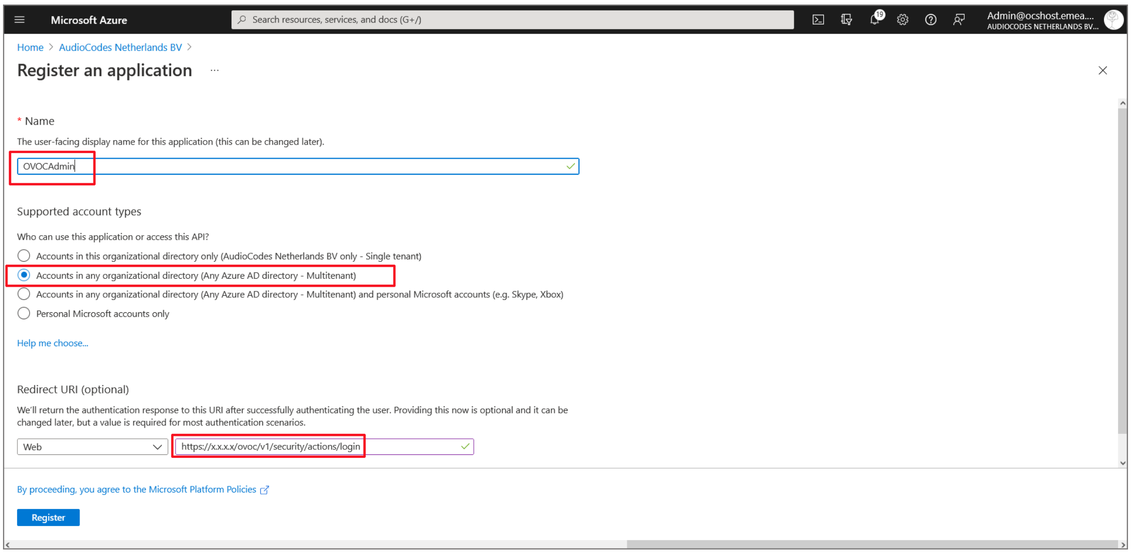


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Display name	Application (client) ID	Created on	Certificates & secrets
MY MyApp	b55f4d0c-e47f-41af-8c96-764af238f25d	3/3/2017	✓ Current
UC UMP customer portal	46fad081-f3b2-4137-a7b4-d1834133cead	1/24/2020	-
SK Skype2TeamsMigrator	4322a7ce-38b2-46fa-9dd3-966cf9ea0a35	11/25/2020	✓ Current
MU My UWP App	fd013cea-f9eb-4ddf-96f6-ade327d056b0	11/27/2020	-
DA Demo auth tenant	f8f0a43b-71f4-4eb6-a087-cf68c7d43e23	2/10/2021	-
RE Resgister-demo	d573a2dc-b7ee-4453-ab68-d6194428fb8d	2/11/2021	-
TO TodoList-API	714ad139-ed99-4470-abd2-facc855634a7	2/11/2021	-

Figure 10-28: New Registration


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV...
Home > AudioCodes Netherlands BV >
Register an application
Help me choose...
Register

* Name

The user-facing display name for this application (this can be changed later).

OVOCAdmin

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)
● Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

By proceeding, you agree to the Microsoft Platform Policies

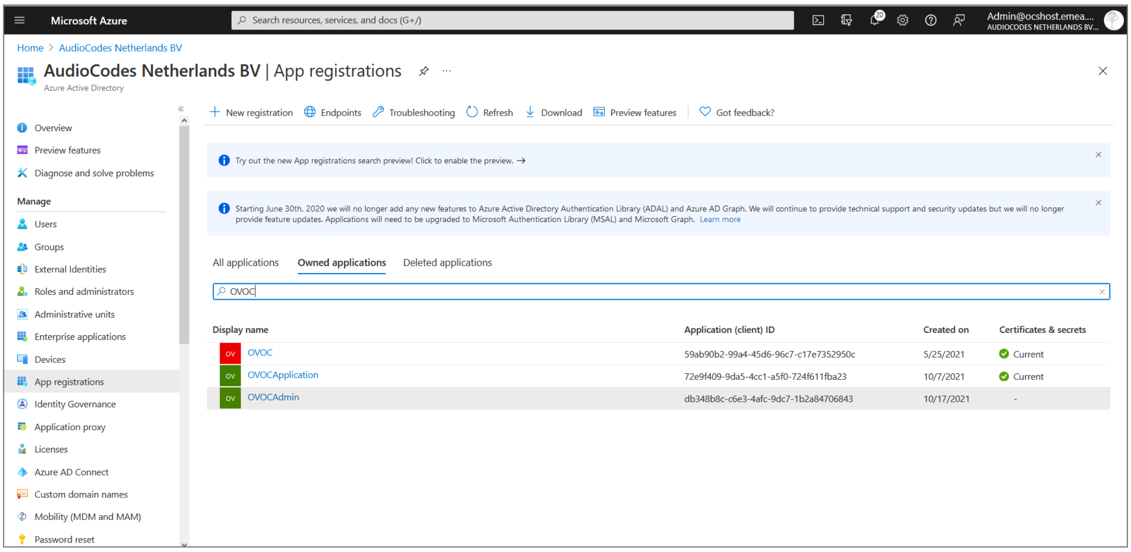
3. Enter the name of the OVOC registration tenant.

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 10-29: New Registered Application



Try out the new App registrations search preview! Click to enable the preview. →

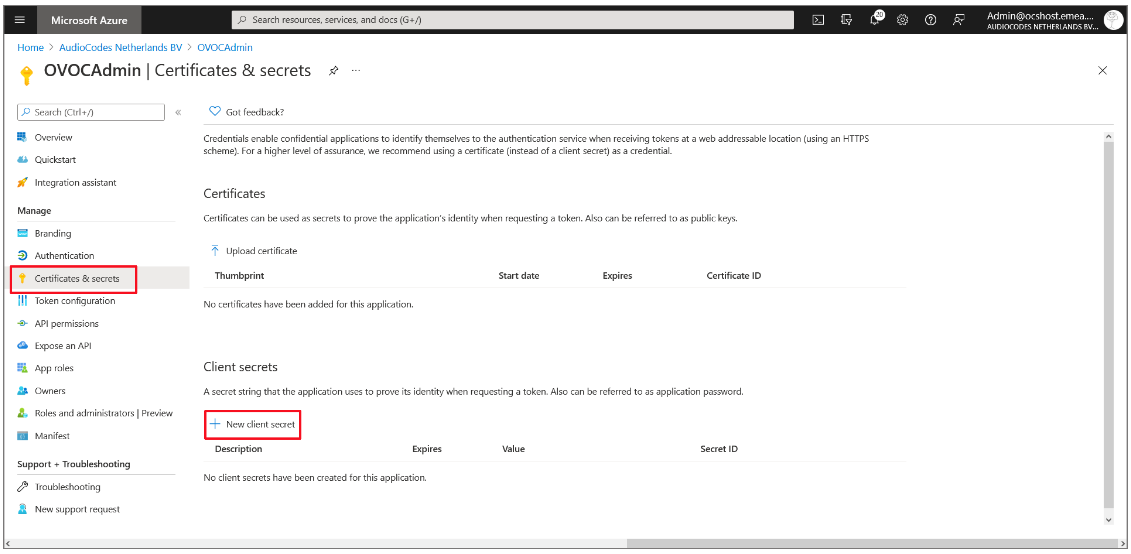
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Display name	Application (client) ID	Created on	Certificates & secrets
OV OVOC	59ab90b2-99a4-45d6-96c7-c17e7352950c	5/25/2021	✓ Current
OV OVOCApplication	72e9f409-9da5-4cc1-a5f0-724f611fba23	10/7/2021	✓ Current
OV OVOCAdmin	db348b8c-c6e3-4afc-9dc7-1b2a84706843	10/17/2021	-

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

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

Figure 10-30: Certificates & secrets



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

Client secrets

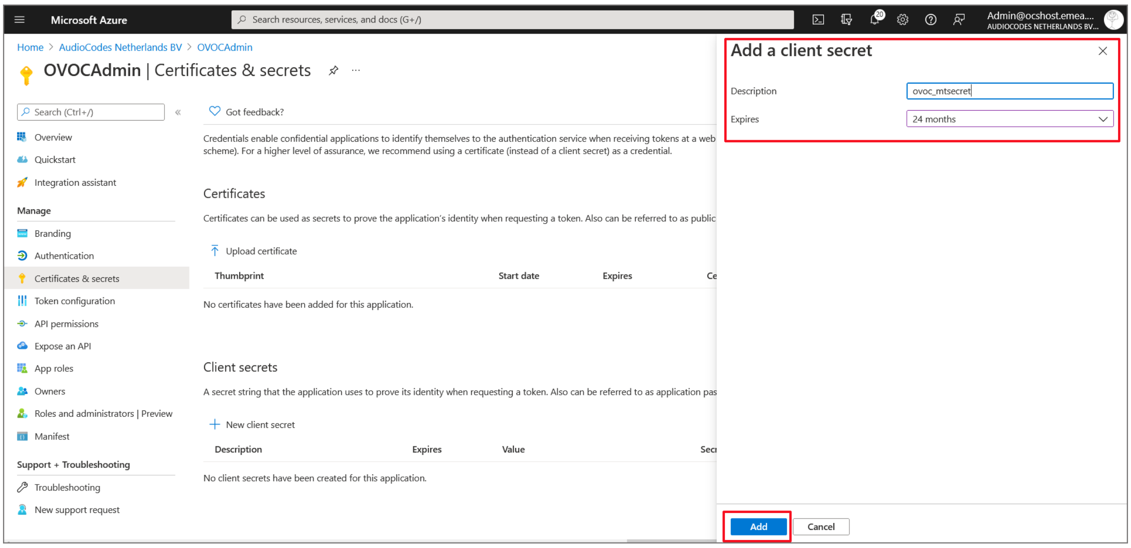
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

8. Click **New client secret**.

Figure 10-31: New client secret



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public

Thumbprint	Start date	Expires	Ce

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application pas

Description	Expires	Value	Secr

No client secrets have been created for this application.

Add a client secret

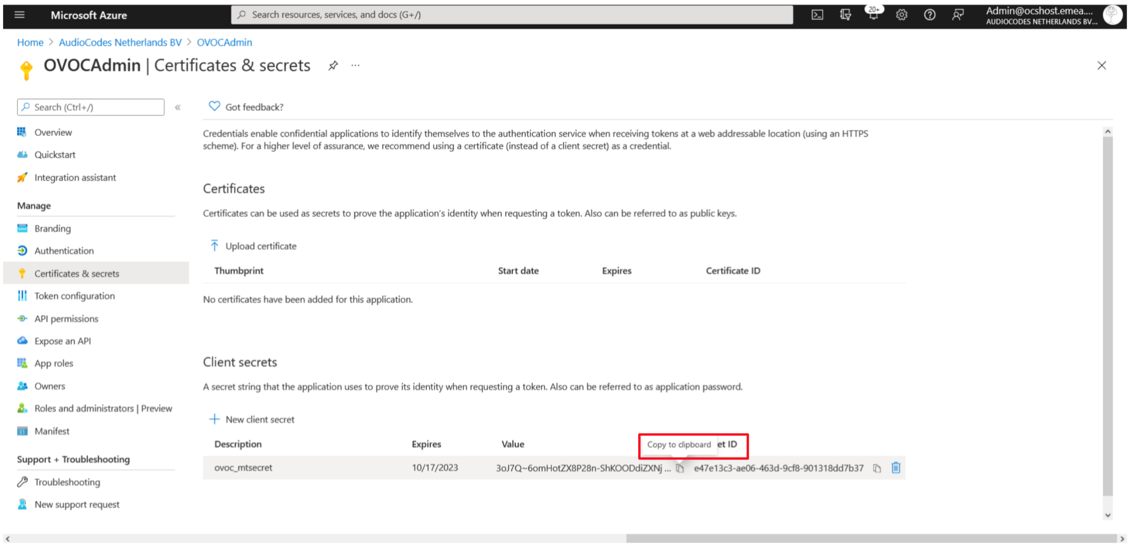
Description: ovoc_mtsecret

Expires: 24 months

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

10. Click **Add**.

Figure 10-32: Client Secret Generated



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

Client secrets

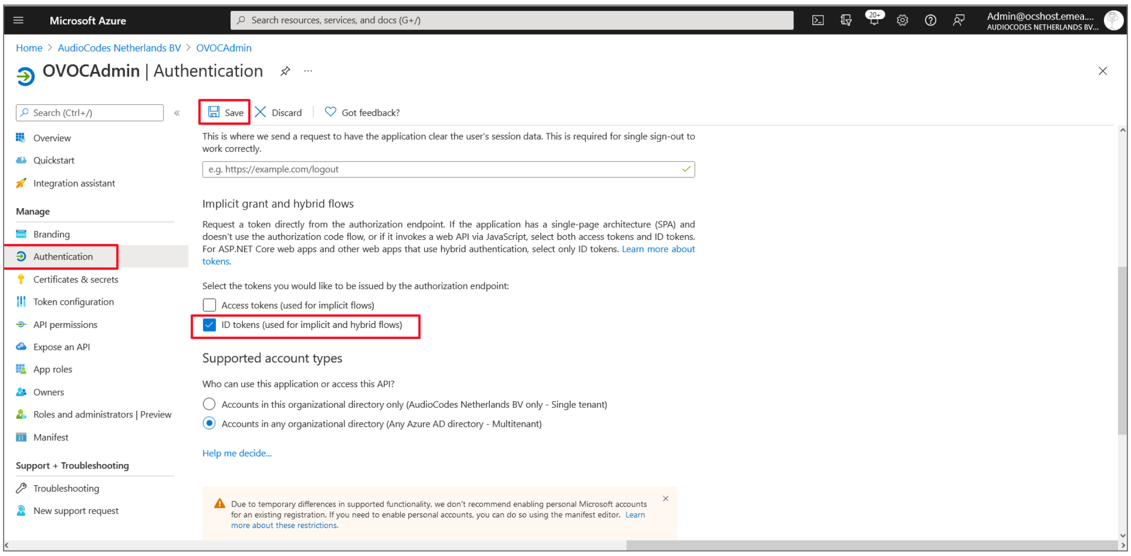
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	et ID
ovoc_mtsecret	10/17/2023	3oJ7Q~6omHotZX8P28n-ShKOODdiZXNj ...	e47e13c3-ae06-463d-9cf8-901318dd7b37

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 10-33: Authentication



This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

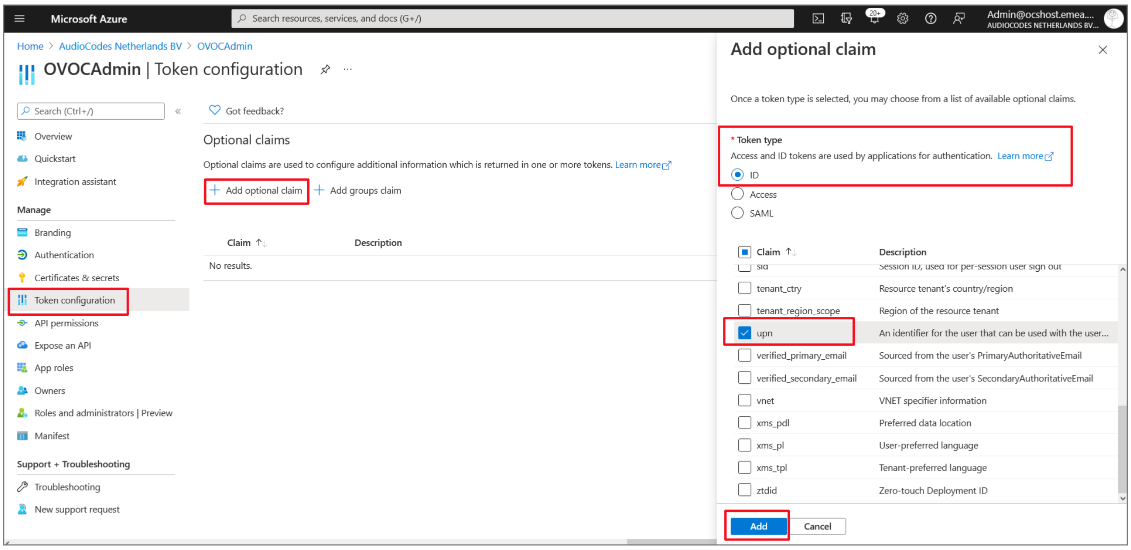
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

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

14. Click **Save**.

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

Figure 10-34: Token Configuration-Add



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

● ID

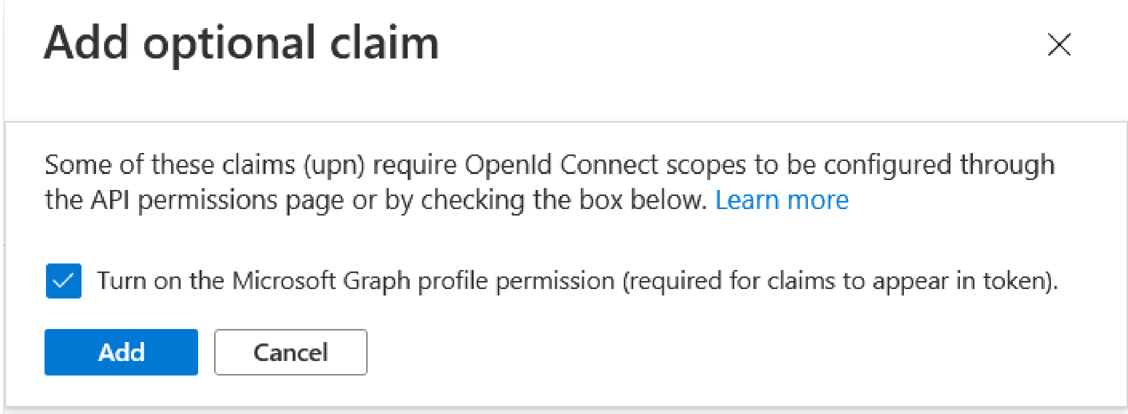
○ Access

○ SAML

	Claim ↑↓	Description
☐	sid	Session ID, used for per-session user sign out
☐	tenant_ctry	Resource tenant's country/region
☐	tenant_region_scope	Region of the resource tenant
☑	upn	An identifier for the user that can be used with the user...
☐	verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
☐	verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail
☐	vnet	VNET specifier information
☐	xms_pdl	Preferred data location
☐	xms_pl	User-preferred language
☐	xms_tpl	Tenant-preferred language
☐	ztdid	Zero-touch Deployment ID

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

Figure 10-35: Turn on Profile Permission



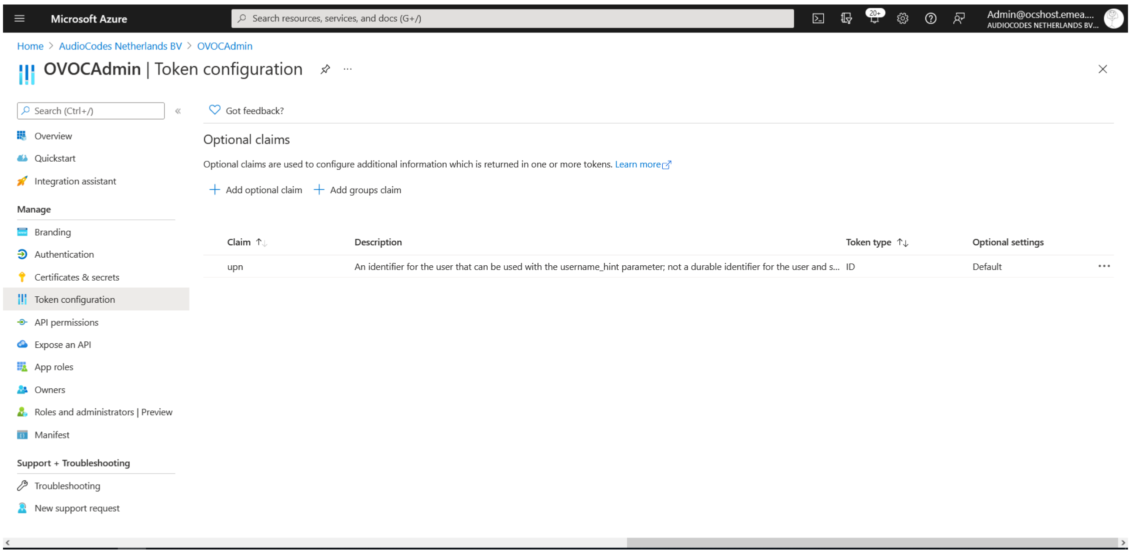
Add optional claim

Some of these claims (upn) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph profile permission (required for claims to appear in token).

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 10-36: Optional claims Added



Optional claims

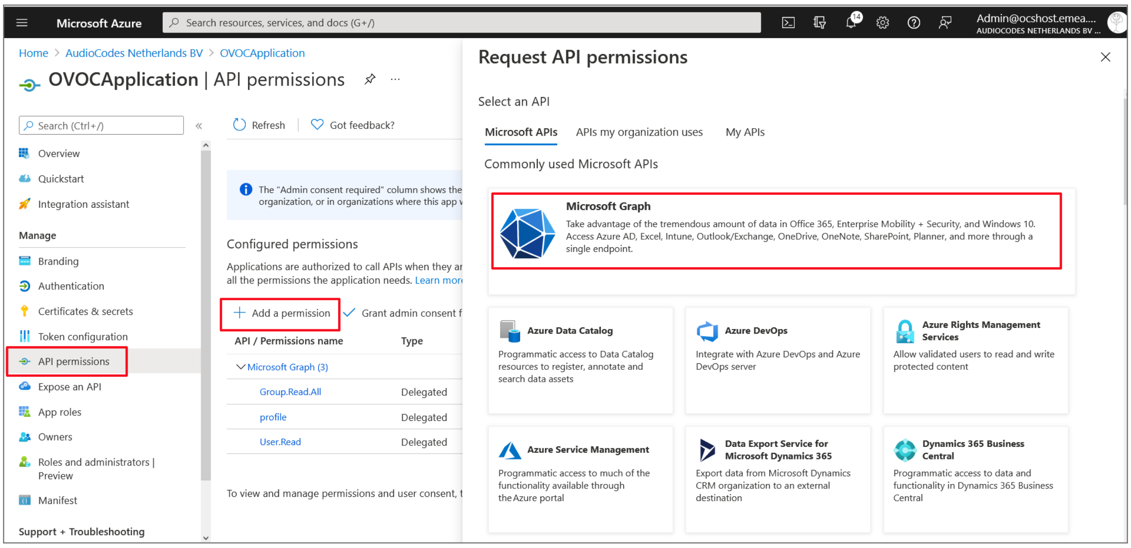
Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description	Token type ↑↓	Optional settings
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and s...	ID	Default

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 10-37: API Permissions



The "Admin consent required" column shows the ... organization, or in organizations where this app v

Configured permissions

Applications are authorized to call APIs when they ar ... all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (3)	
Group.Read.All	Delegated
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

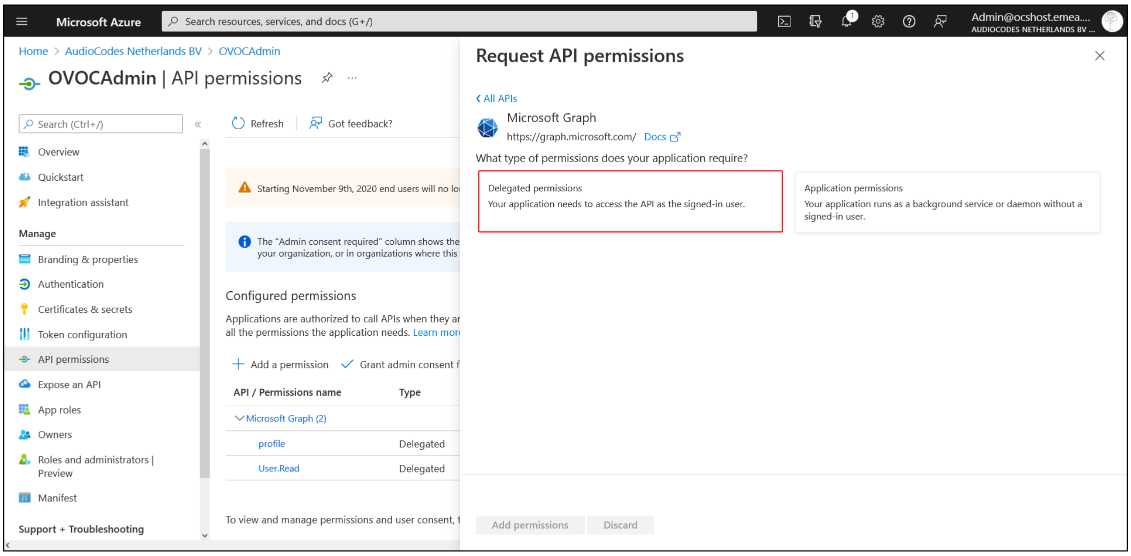
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

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

Figure 10-38: Delegated permissions



Starting November 9th, 2020 end users will no lo

The "Admin consent required" column shows the ... your organization, or in organizations where this

Configured permissions

Applications are authorized to call APIs when they ar ... all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

What type of permissions does your application require?

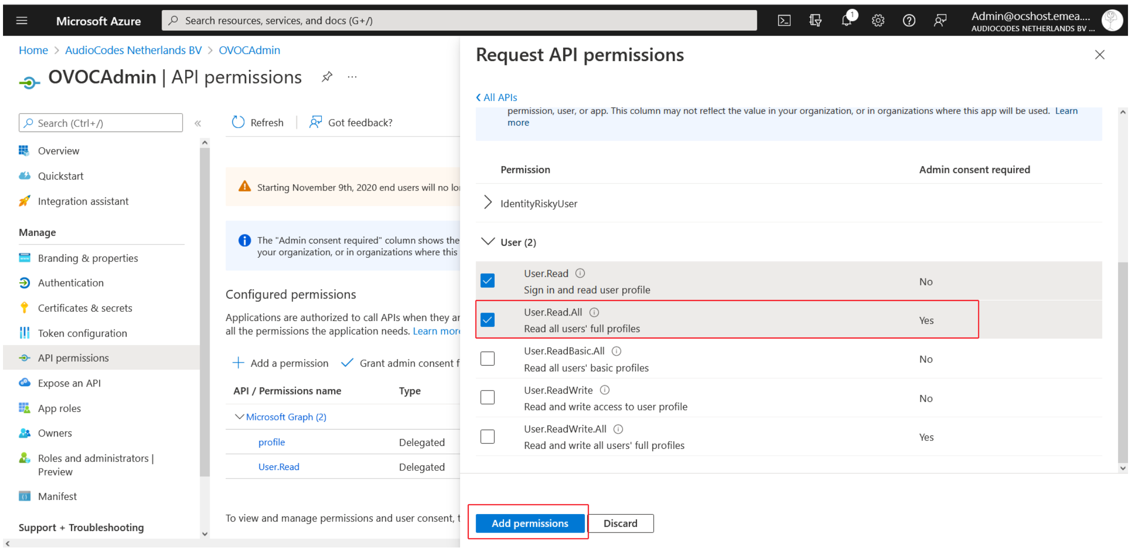
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

20. Click **Delegated permissions**.

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

Figure 10-39: Delegated permissions



Starting November 9th, 2020 end users will no lo

The "Admin consent required" column shows the your organization, or in organizations where this

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn more

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

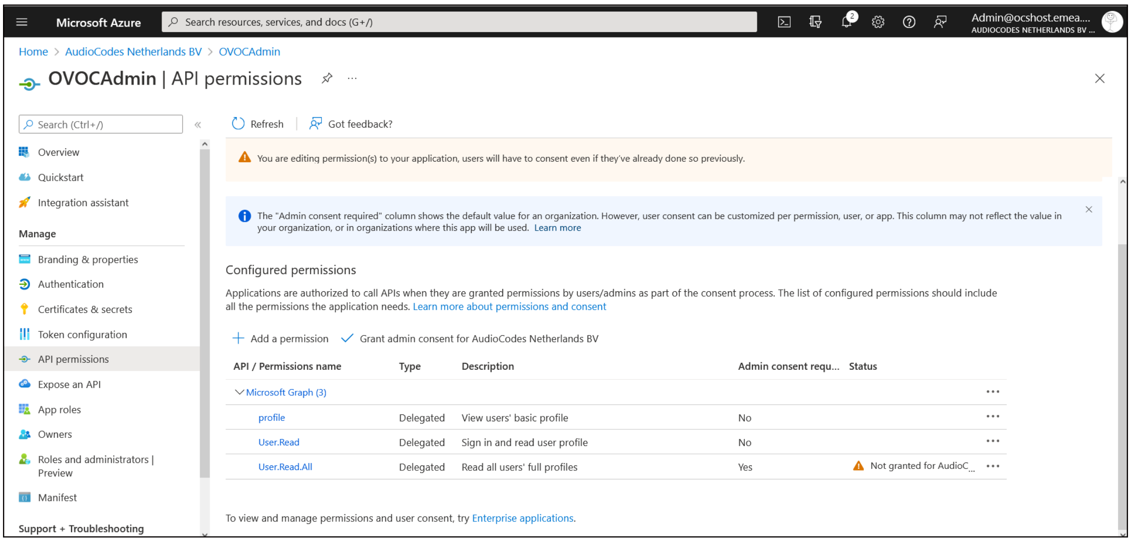
To view and manage permissions and user consent, t

permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

	Permission	Admin consent required
	IdentityRiskyUser	
	User (2)	
☑	User.Read Sign in and read user profile	No
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadBasic.All Read all users' basic profiles	No
□	User.ReadWrite Read and write access to user profile	No
□	User.ReadWrite.All Read and write all users' full profiles	Yes

The configured API permissions are displayed.

Figure 10-40: Configured API Permissions



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

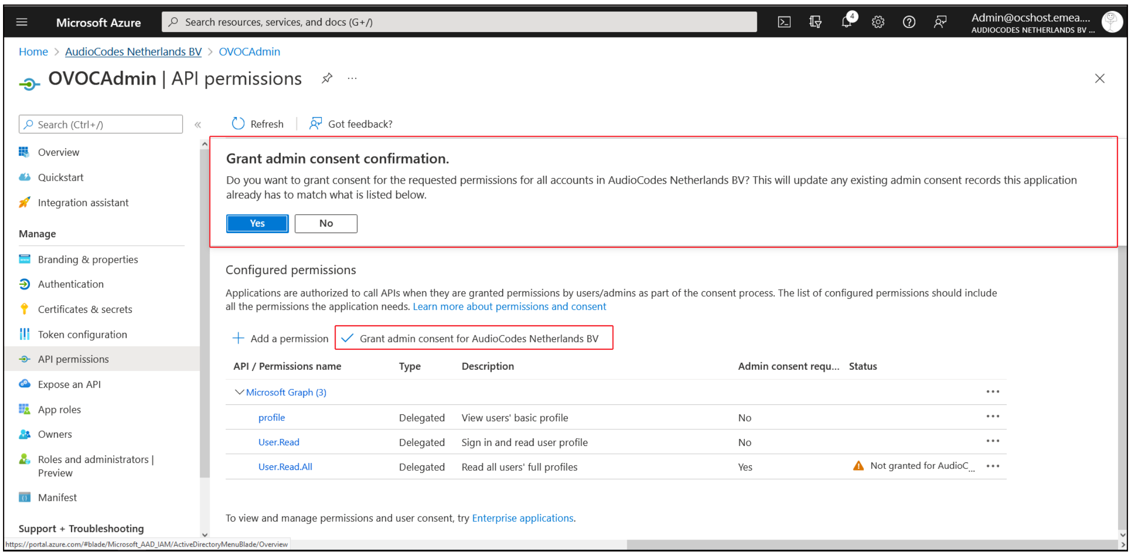
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for AudioC...

To view and manage permissions and user consent, try Enterprise applications.

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

Figure 10-41: Grant Admin Consent for all Accounts


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Home > AudioCodes Netherlands BV > OVOCAdmin
OVOCAdmin | API permissions
Search (Ctrl+/)
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Refresh
Got feedback?
Yes
No
Add a permission
Grant admin consent for AudioCodes Netherlands BV
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in AudioCodes Netherlands BV? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions

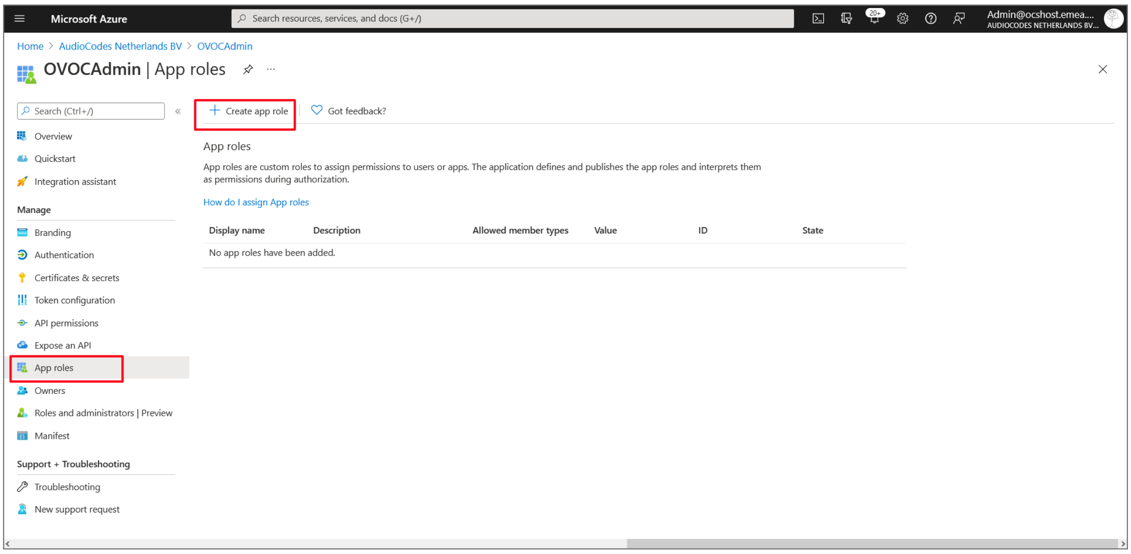
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for AudioC...

To view and manage permissions and user consent, try Enterprise applications.

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

Figure 10-42: App roles



App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
No app roles have been added.					

24. Create an app role with Admin permissions:

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

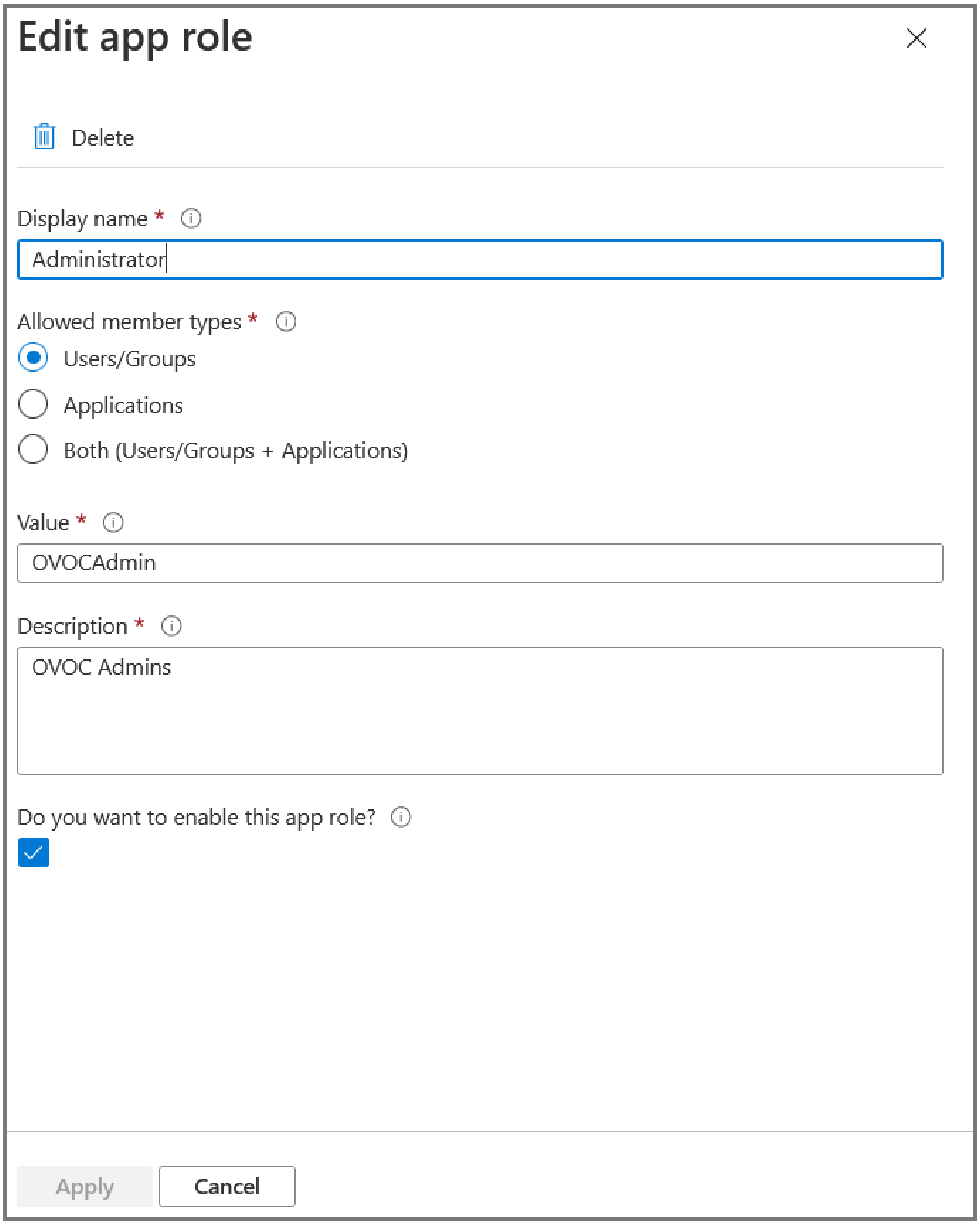
b. Select Users/Groups check box.

c. Enter value "OVOCAdmin"

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

e. Click **Apply**

Figure 10-43: Admin Role



Edit app role

Delete

Display name * : Administrator

Allowed member types *

● Users/Groups

○ Applications

○ Both (Users/Groups + Applications)

Value * : OVOCAdmin

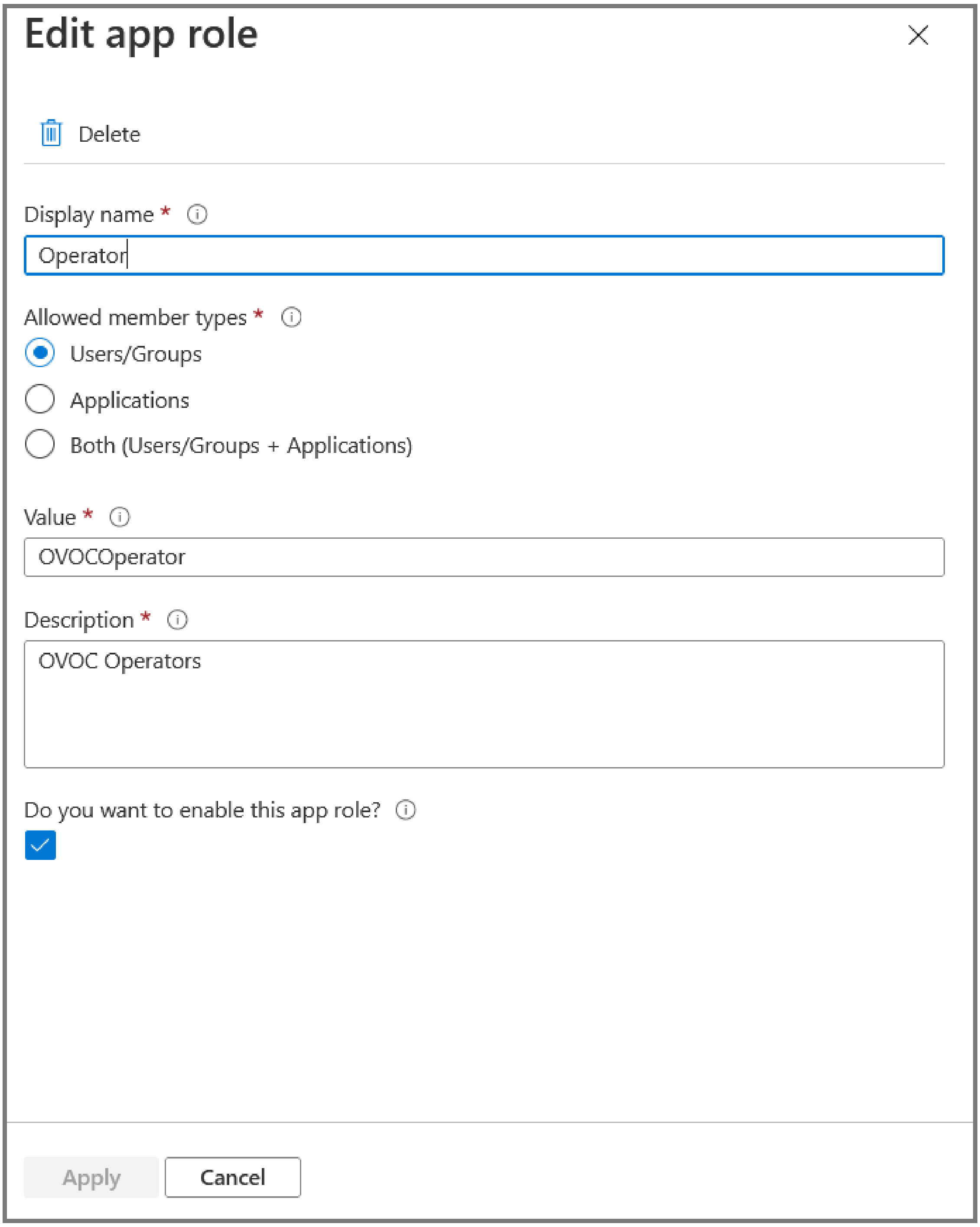
Description * : OVOC Admins

Do you want to enable this app role?

☑

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

Figure 10-44: Operator Role



Edit app role

Display name * Operator

Allowed member types *
● Users/Groups
○ Applications
○ Both (Users/Groups + Applications)

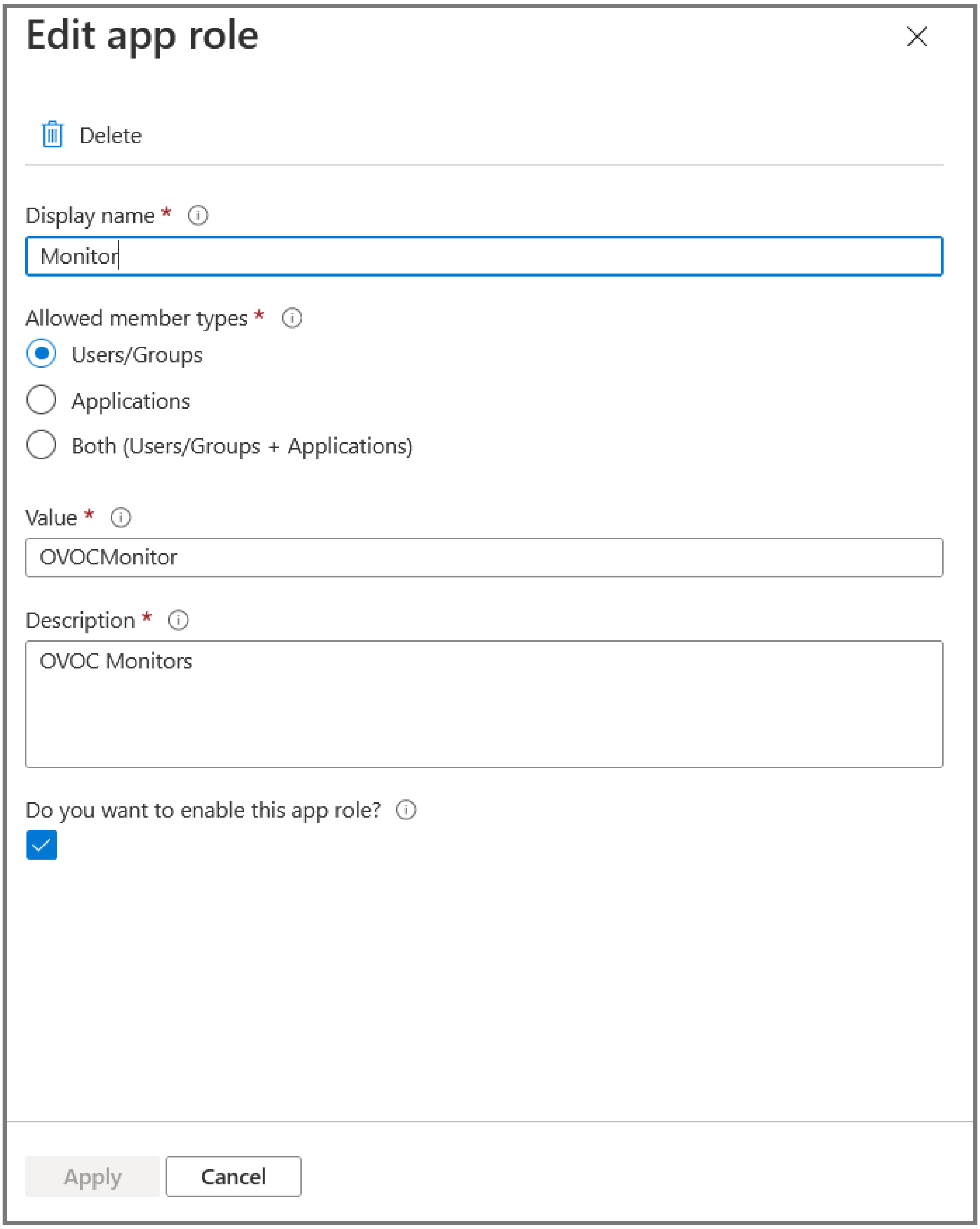
Value * OVOCOperator

Description * OVOC Operators

Do you want to enable this app role?
☑

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

Figure 10-45: Operator Role



Edit app role

Delete

Display name * Monitor

Allowed member types *

● Users/Groups

○ Applications

○ Both (Users/Groups + Applications)

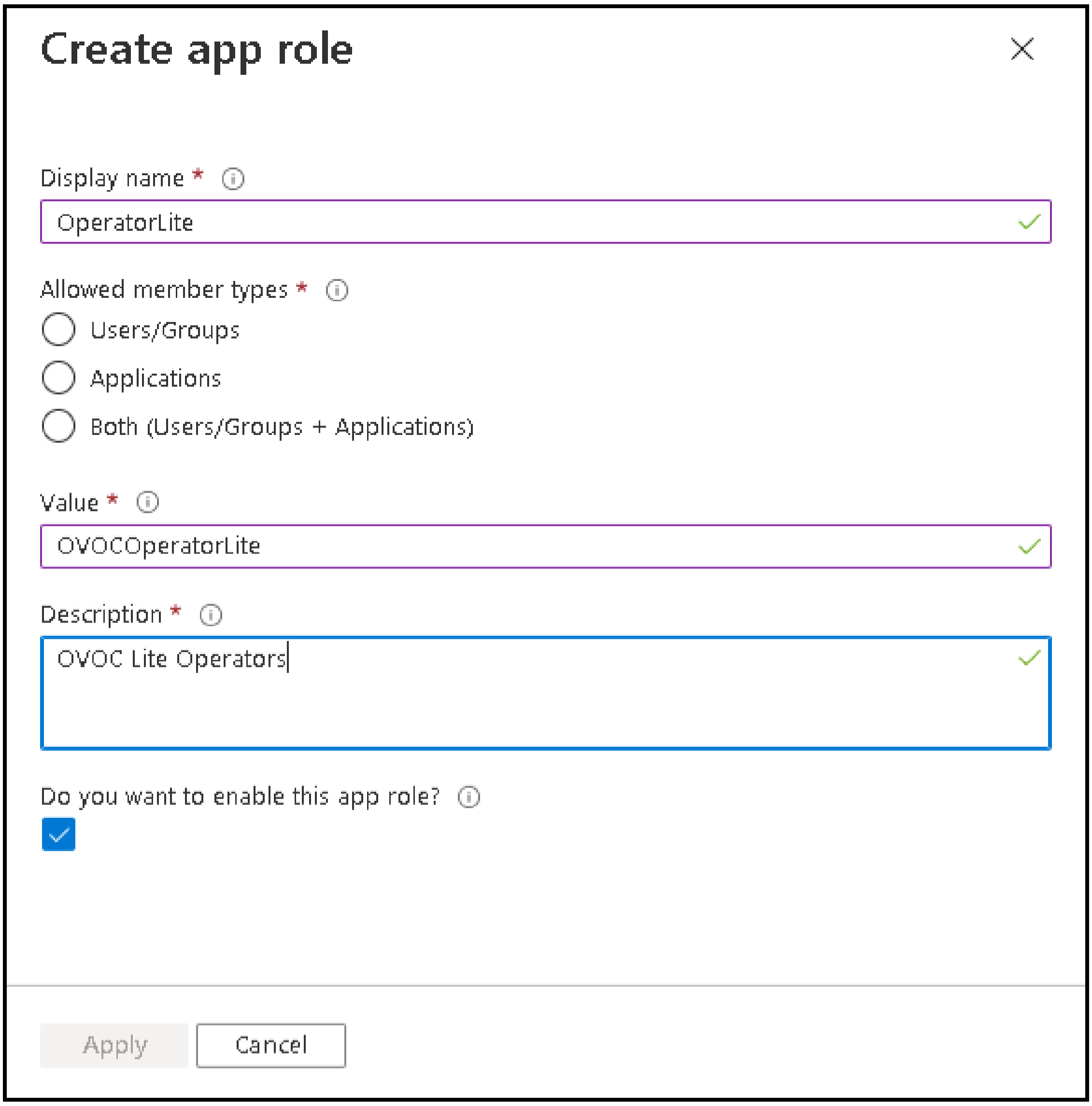
Value * OVOCMonitor

Description * OVOC Monitors

Do you want to enable this app role? ☑

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

Figure 10-46: OVOC Operator Lite



Create app role

Display name * ⓘ

OperatorLite ✓

Allowed member types * ⓘ

○ Users/Groups

○ Applications

○ Both (Users/Groups + Applications)

Value * ⓘ

OVOCOperatorLite ✓

Description * ⓘ

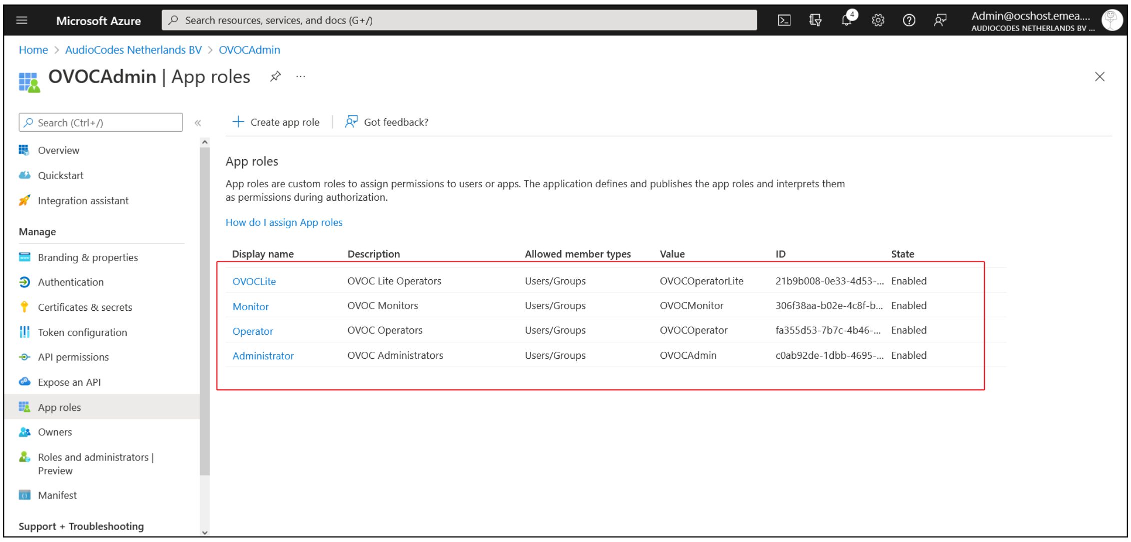
OVOC Lite Operators ✓

Do you want to enable this app role? ⓘ

☑

The new roles are displayed:

Figure 10-47: App roles



Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Home > AudioCodes Netherlands BV > OVOCAdmin

OVOCAdmin | App roles

App roles

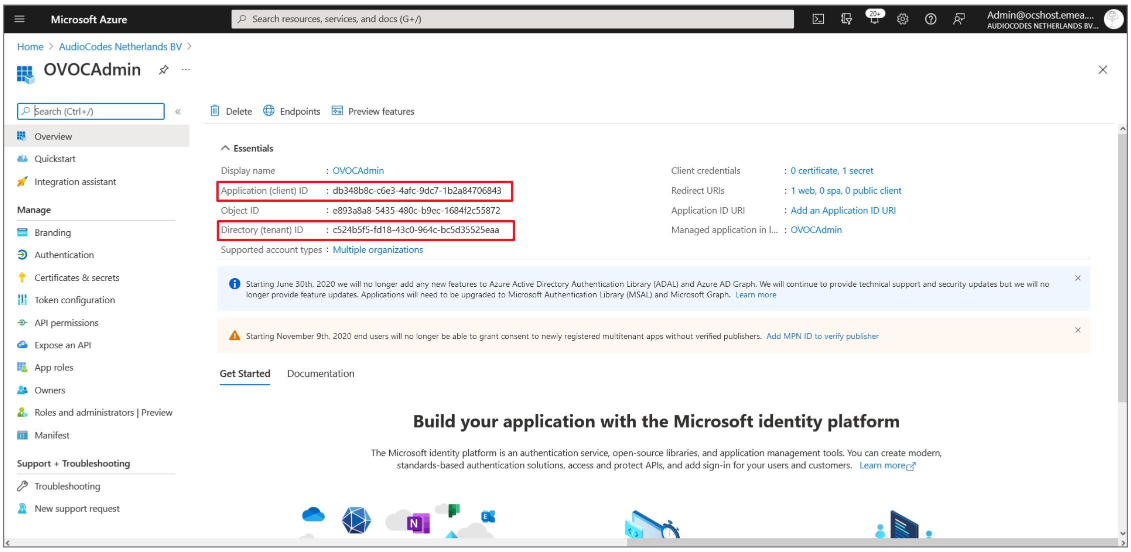
App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
OVOCLite	OVOC Lite Operators	Users/Groups	OVOCOperatorLite	21b9b008-0e33-4d53-...	Enabled
Monitor	OVOC Monitors	Users/Groups	OVOCMonitor	306f38aa-b02e-4c8f-b...	Enabled
Operator	OVOC Operators	Users/Groups	OVOCOperator	fa355d53-7b7c-4b46-...	Enabled
Administrator	OVOC Administrators	Users/Groups	OVOCAdmin	c0ab92de-1dbb-4695-...	Enabled

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

Figure 10-48: Overview Page



Display name : OVOCAdmin
Application (client) ID : db348b8c-c6e3-4afc-9dc7-1b2a84706843
Object ID : e893a8a8-5435-480c-b9ec-1684f2c55872
Directory (tenant) ID : c524b5f5-fd18-43c0-964c-bc5d35525eaa
Supported account types : Multiple organizations

Client credentials : 0 certificate, 1 secret
Redirect URIs : 1 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : OVOCAdmin

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

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 123

31. Add operators of external tenants and assign them roles as described in Add External Tenant Operators and Assign Roles on page 128

32. Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings - Multitenant Setup below

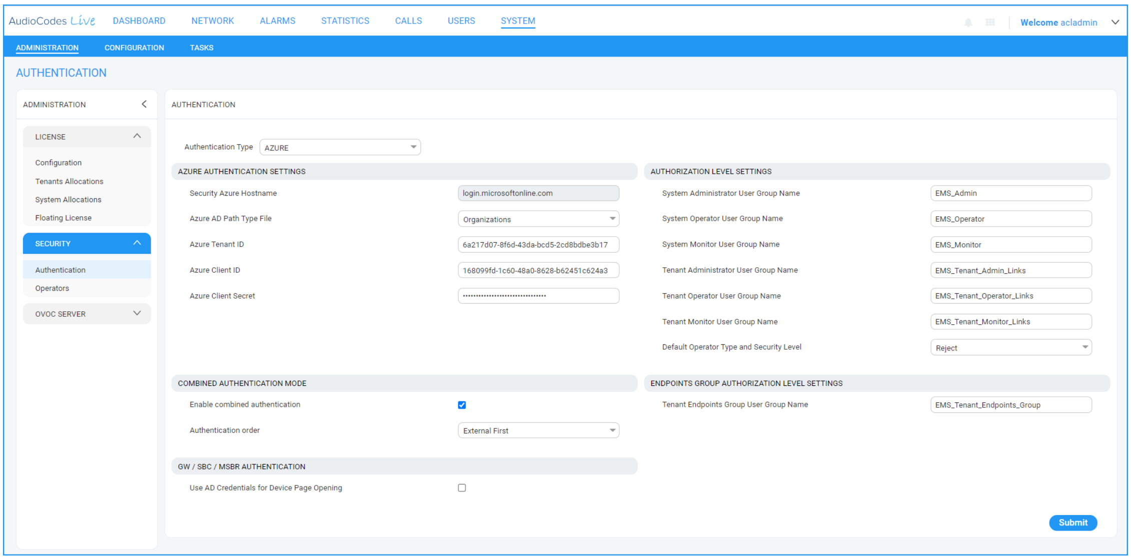
Configuring OVOC Web Azure Settings - Multitenant Setup

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 10-49: Azure Authentication



AUTHENTICATION

Authentication Type: AZURE

AZURE AUTHENTICATION SETTINGS

Security Azure Hostname: login.microsoftonline.com
Azure AD Path Type File: Organizations
Azure Tenant ID: 6a217d07-8f6d-43da-bcd5-2cd8bdbe3b17
Azure Client ID: 168099fd-1c60-48a0-8628-b62451c624a3
Azure Client Secret: ••••••••••••••••••••••••••••••••

AUTHORIZATION LEVEL SETTINGS

System Administrator User Group Name: EMS_Admin
System Operator User Group Name: EMS_Operator
System Monitor User Group Name: EMS_Monitor
Tenant Administrator User Group Name: EMS_Tenant_Admin_Links
Tenant Operator User Group Name: EMS_Tenant_Operator_Links
Tenant Monitor User Group Name: EMS_Tenant_Monitor_Links
Default Operator Type and Security Level: Reject

COMBINED AUTHENTICATION MODE

Enable combined authentication ☑
Authentication order: External First

ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS

Tenant Endpoints Group User Group Name: EMS_Tenant_Endpoints_Group

GW / SBC / MSBR AUTHENTICATION

Use AD Credentials for Device Page Opening ☐

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**.

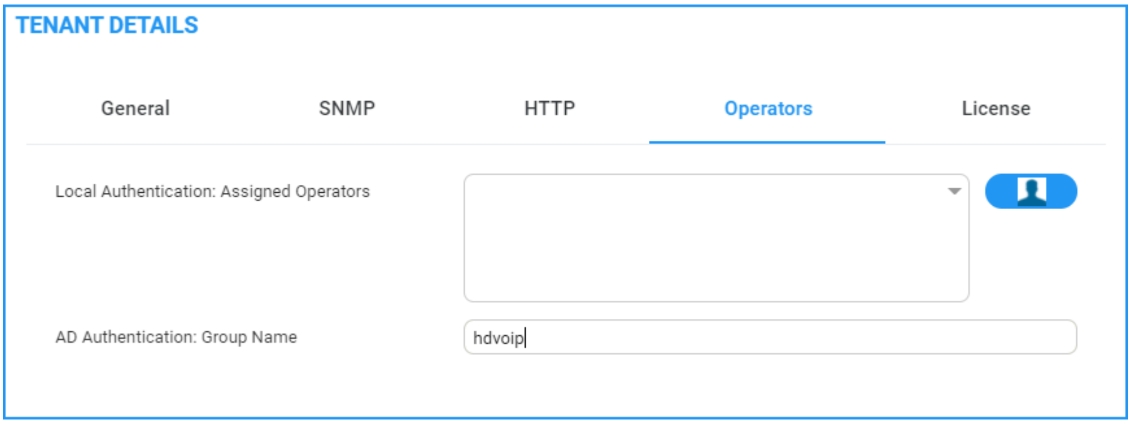
6. In the screen section 'GW / SBC / MSBR Authentication', select the option 'Use AD Credentials for Device Page Opening' for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to OVOC. The AudioCodes device will then perform authentication with the Azure 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 10-50: AD Authentication Group Name

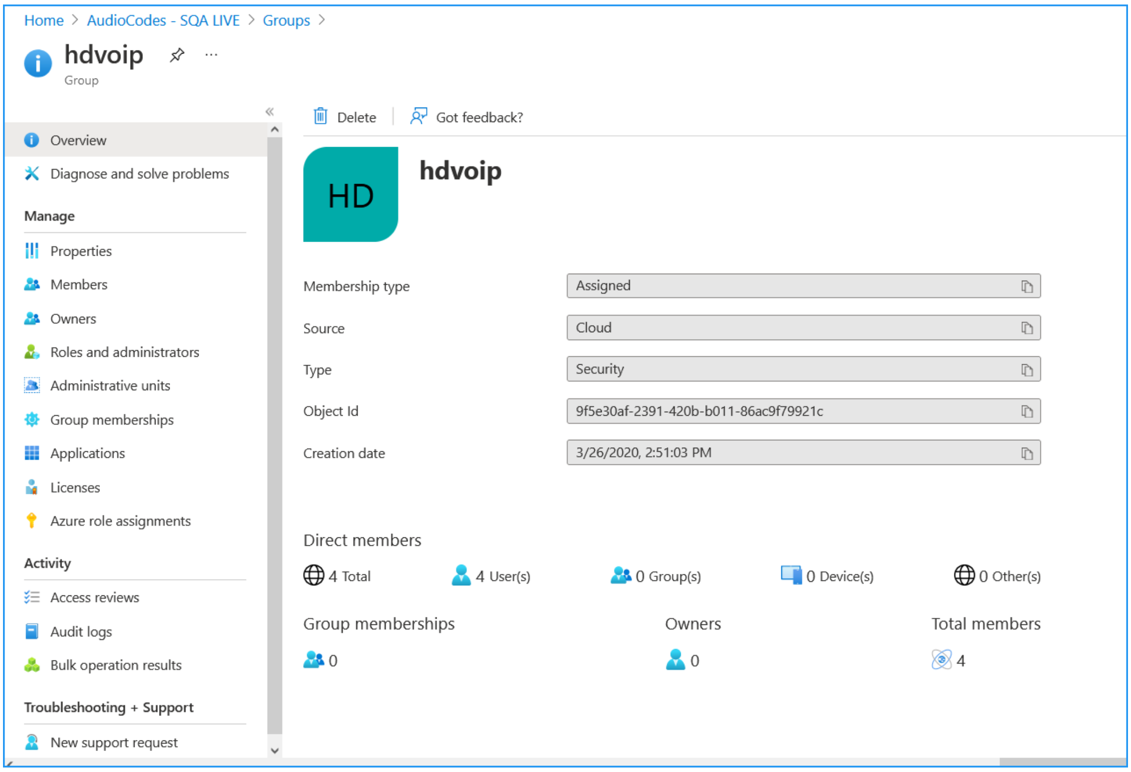


TENANT DETAILS

Local Authentication: Assigned Operators

AD Authentication: Group Name: hdvoip

Figure 10-51: Matching Group on Azure



Home > AudioCodes - SQA LIVE > Groups >

hdvoip

Group

hdvoip

Membership type	Assigned
Source	Cloud
Type	Security
Object Id	9f5e30af-2391-420b-b011-86ac9f79921c
Creation date	3/26/2020, 2:51:03 PM

Direct members

4 Total 4 User(s) 0 Group(s) 0 Device(s) 0 Other(s)

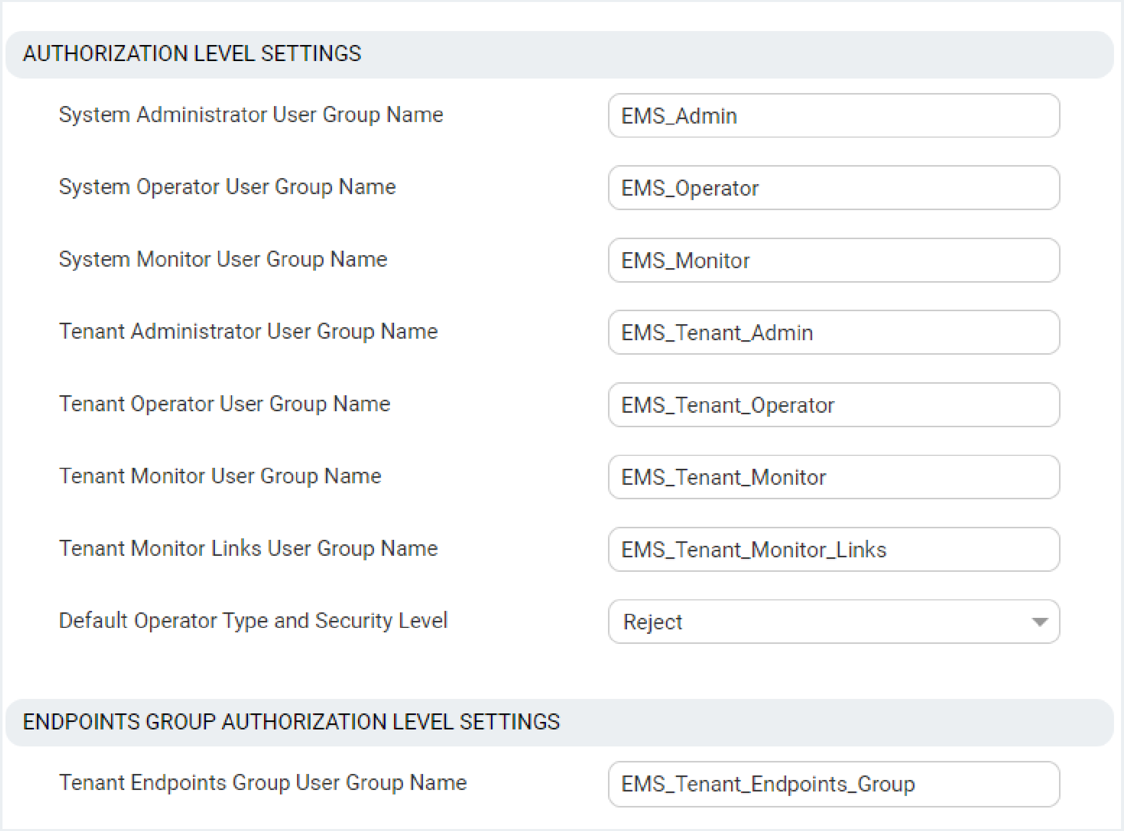
Group memberships 0

Owners 0

Total members 4

7. In the screen section Authorization Level Settings, configure the user group names exactly as defined on Azure in Create Azure Groups and Assign Members on page 123. When an operator is not assigned to a group on Azure, the parameter 'Default Operator Type and Security Level' is applied.

Figure 10-52: Authorization Level Settings



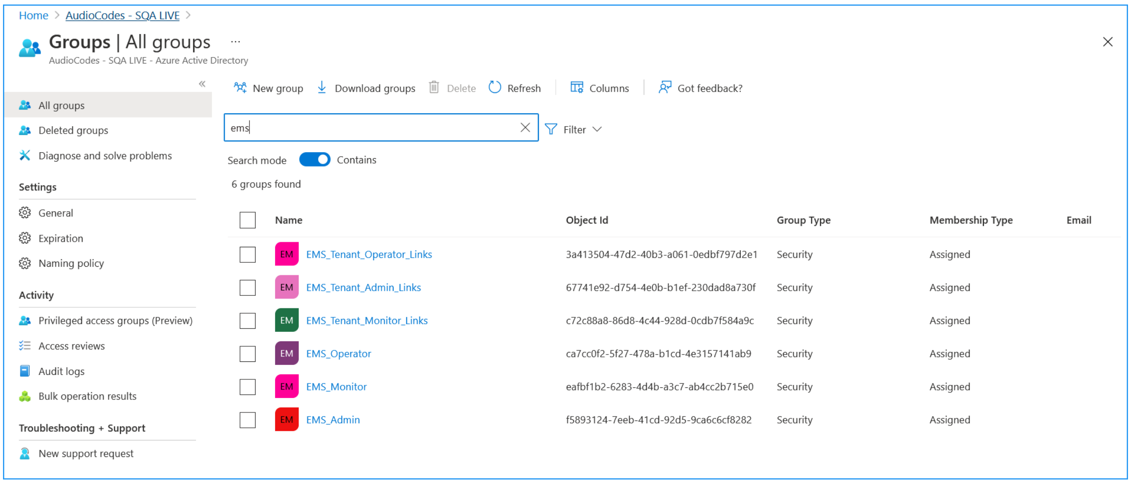
AUTHORIZATION LEVEL SETTINGS

System Administrator User Group Name	EMS_Admin
System Operator User Group Name	EMS_Operator
System Monitor User Group Name	EMS_Monitor
Tenant Administrator User Group Name	EMS_Tenant_Admin
Tenant Operator User Group Name	EMS_Tenant_Operator
Tenant Monitor User Group Name	EMS_Tenant_Monitor
Tenant Monitor Links User Group Name	EMS_Tenant_Monitor_Links
Default Operator Type and Security Level	Reject

ENDPOINTS GROUP AUTHORIZATION LEVEL SETTINGS

Tenant Endpoints Group User Group Name	EMS_Tenant_Endpoints_Group

Figure 10-53: Matching Groups on Azure



ems

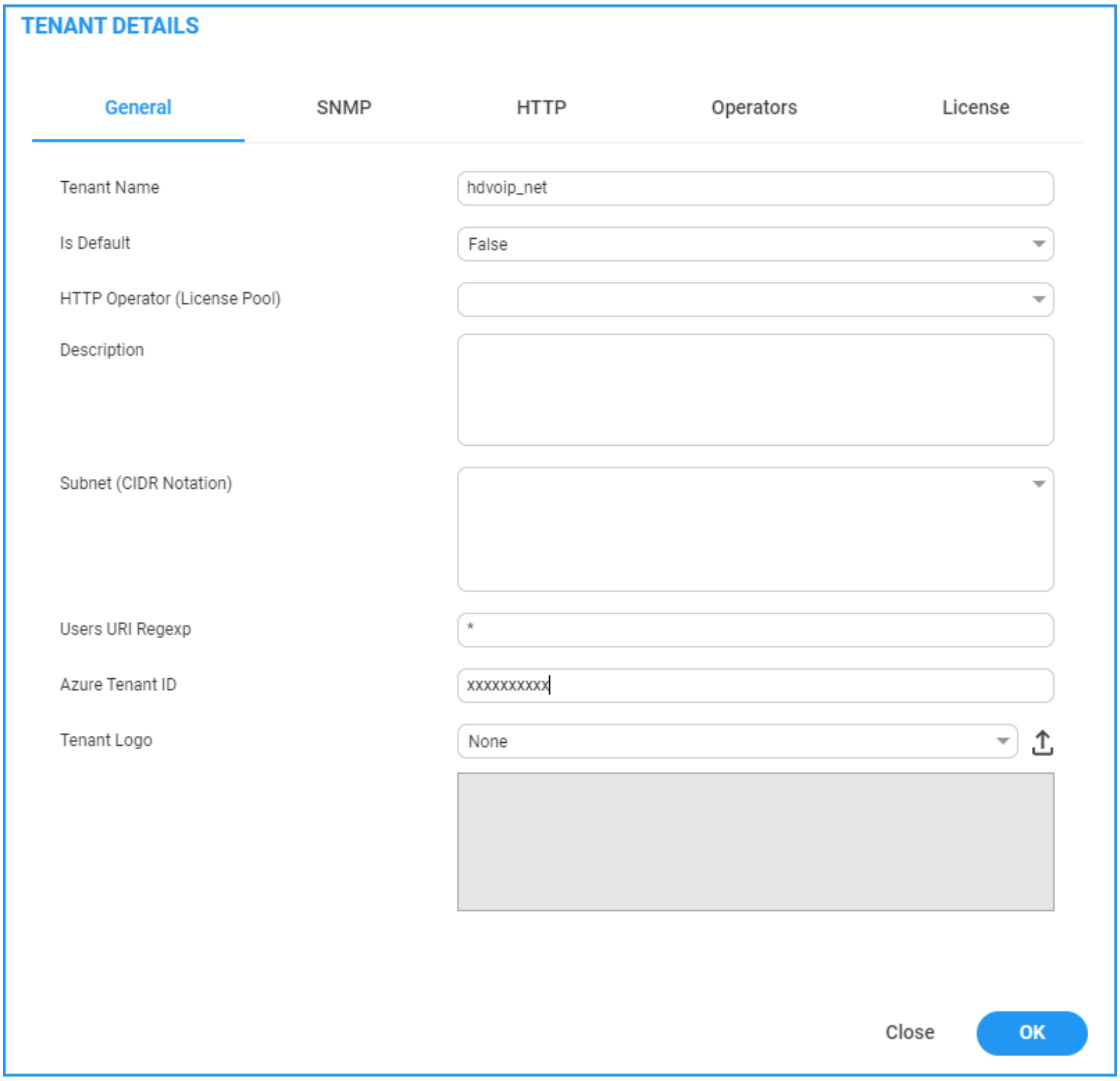
Search mode Contains

6 groups found

☐	Name	Object Id	Group Type	Membership Type	Email
☐	EM EMS_Tenant_Operator_Links	3a413504-47d2-40b3-a061-0edbf797d2e1	Security	Assigned	
☐	EM EMS_Tenant_Admin_Links	67741e92-d754-4e0b-b1ef-230dad8a730f	Security	Assigned	
☐	EM EMS_Tenant_Monitor_Links	c72c88a8-86d8-4c44-928d-0cdb7f584a9c	Security	Assigned	
☐	EM EMS_Operator	ca7cc0f2-5f27-478a-b1cd-4e3157141ab9	Security	Assigned	
☐	EM EMS_Monitor	eafbf1b2-6283-4d4b-a3c7-ab4cc2b715e0	Security	Assigned	
☐	EM EMS_Admin	f5893124-7eeb-41cd-92d5-9ca6c6cf8282	Security	Assigned	

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

Figure 10-54: Tenant Details



TENANT DETAILS

Tenant Name: hdvoip_net

Is Default: False

HTTP Operator (License Pool):

Description:

Subnet (CIDR Notation):

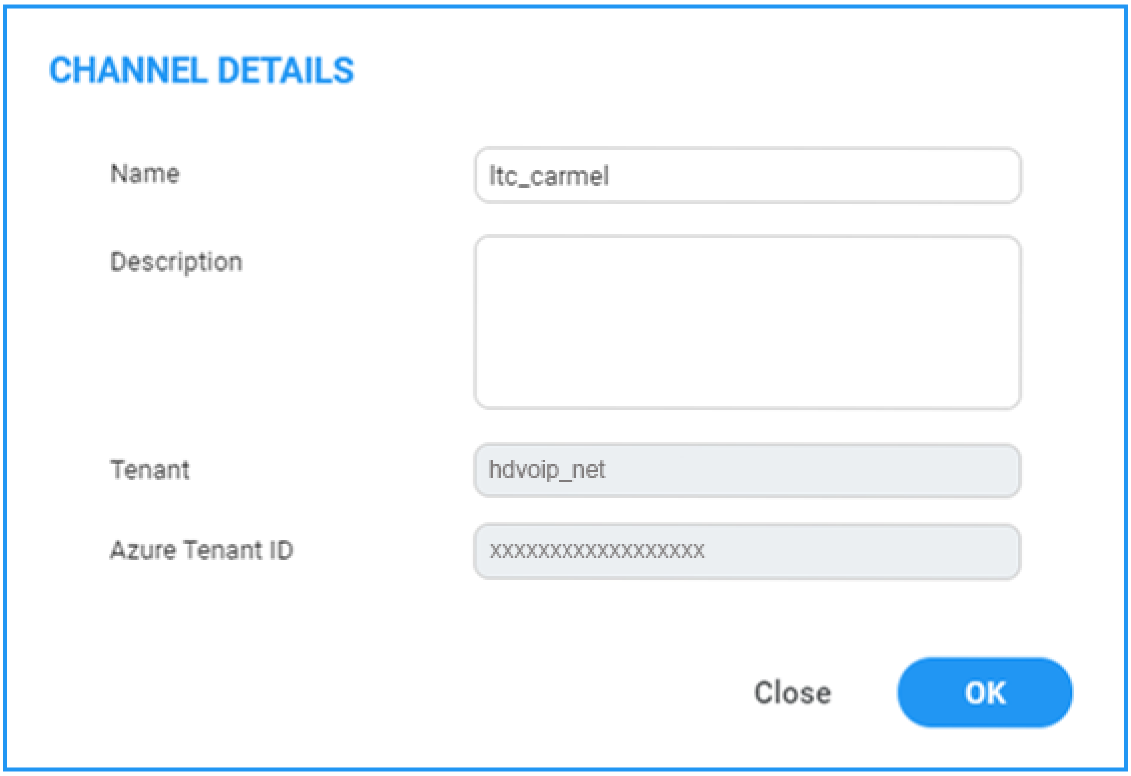
Users URI Regexp: *

Azure Tenant ID: xxxxxxxxxx

Tenant Logo: None

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 10-55: Channel Details



CHANNEL DETAILS

Name: ltc_carmel

Description:

Tenant: hdvoip_net

Azure Tenant ID: xxxxxxxxxxxxxxxxxxx

Upgrading from Single Tenant to Multitenant

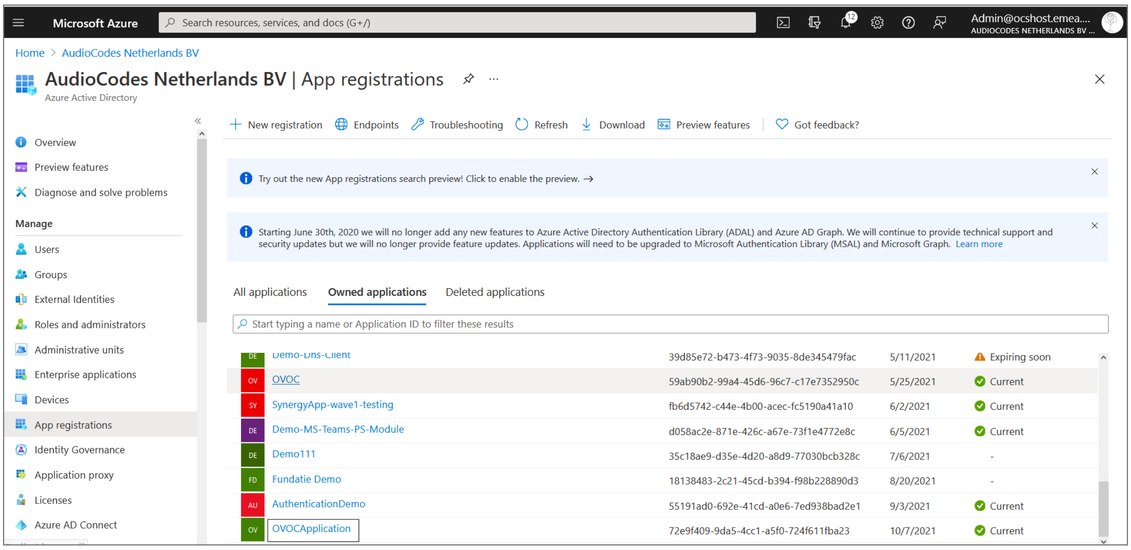
This procedure describes how to upgrade from Single tenant to Multitenant setup.

⚠ 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 10-56: App registrations



AudioCodes Netherlands BV | App registrations

Azure Active Directory

Try out the new App registrations search preview! Click to enable the preview. →

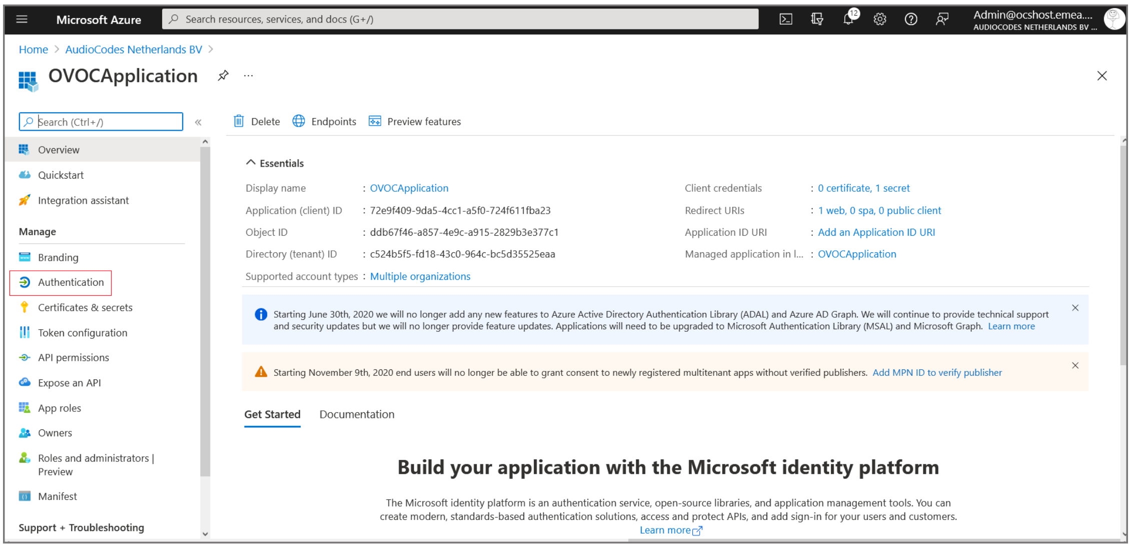
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Start typing a name or Application ID to filter these results

DE	Demo-Dns-Client	39d85e72-b473-4f73-9035-8de345479fac	5/11/2021	⚠ Expiring soon
OV	OVOC	59ab90b2-99a4-45d6-96c7-c17e7352950c	5/25/2021	✓ Current
SY	SynergyApp-wave1-testing	fb6d5742-c44e-4b00-acec-fc5190a41a10	6/2/2021	✓ Current
DE	Demo-MS-Teams-PS-Module	d058ac2e-871e-426c-a67e-73f1e4772e8c	6/5/2021	✓ Current
DE	Demo111	35c18ae9-d35e-4d20-a8d9-77030bcb328c	7/6/2021	-
FD	Fundatie Demo	18138483-2c21-45cd-b394-f98b228890d3	8/20/2021	-
AU	AuthenticationDemo	55191ad0-692e-41cd-a0e6-7ed938bad2e1	9/3/2021	✓ Current
OV	OVOCApplication	72e9f409-9da5-4cc1-a5f0-724f611fba23	10/7/2021	✓ Current

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

Figure 10-57: OVOC Application



OVOCApplication

Essentials

Display name	: OVOCApplication	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: 72e9f409-9da5-4cc1-a5f0-724f611fba23	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: ddb67f46-a857-4e9c-a915-2829b3e377c1	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: c524b5f5-fd18-43c0-964c-bc5d35525eaa	Managed application in l...	: OVOCApplication
Supported account types	: Multiple organizations		

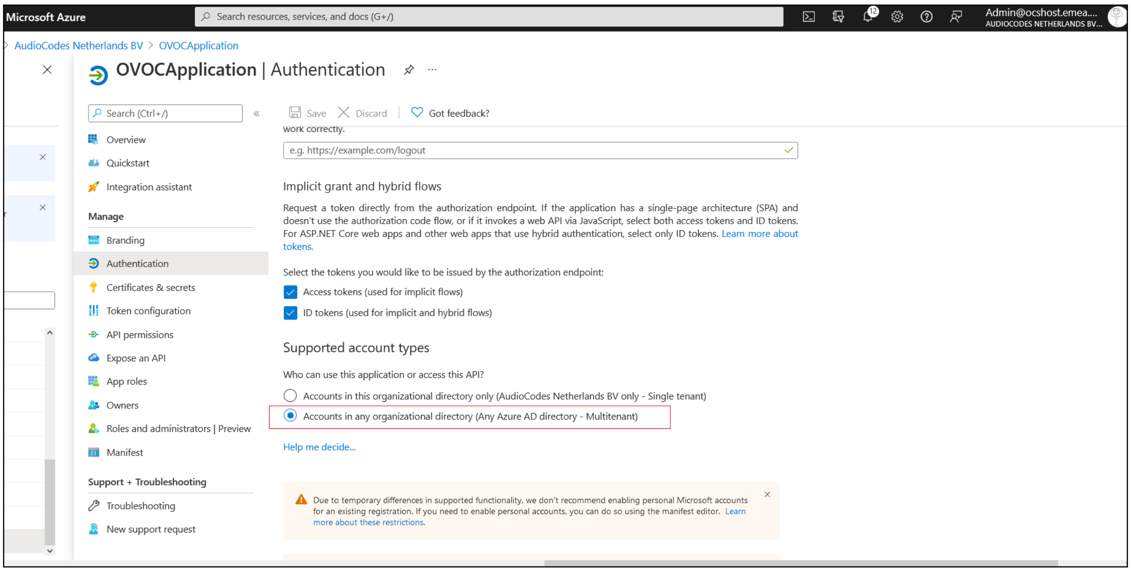
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Figure 10-58: Authentication Screen



work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant)

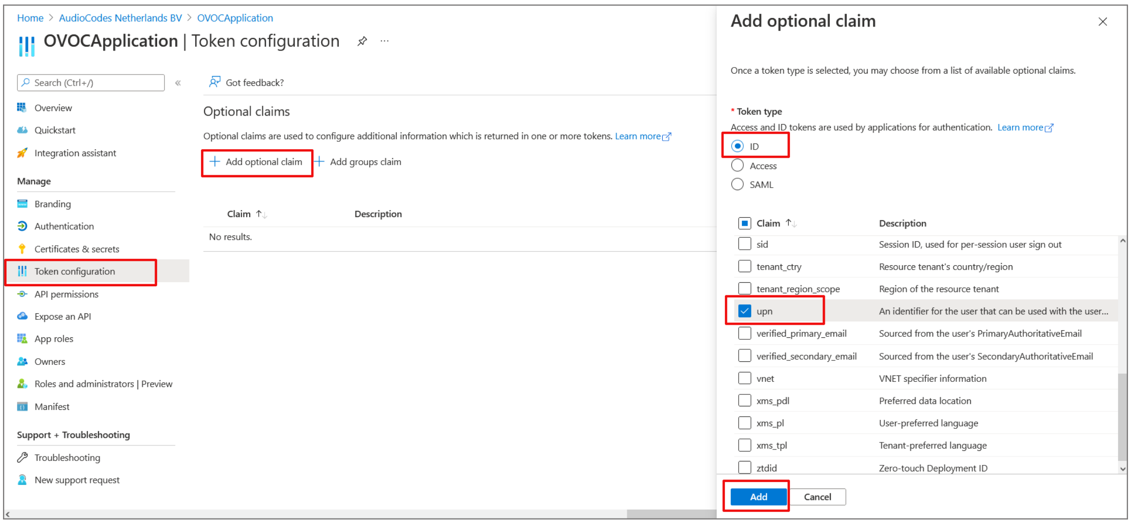
Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

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 10-59: Token Configuration-Add



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

● ID

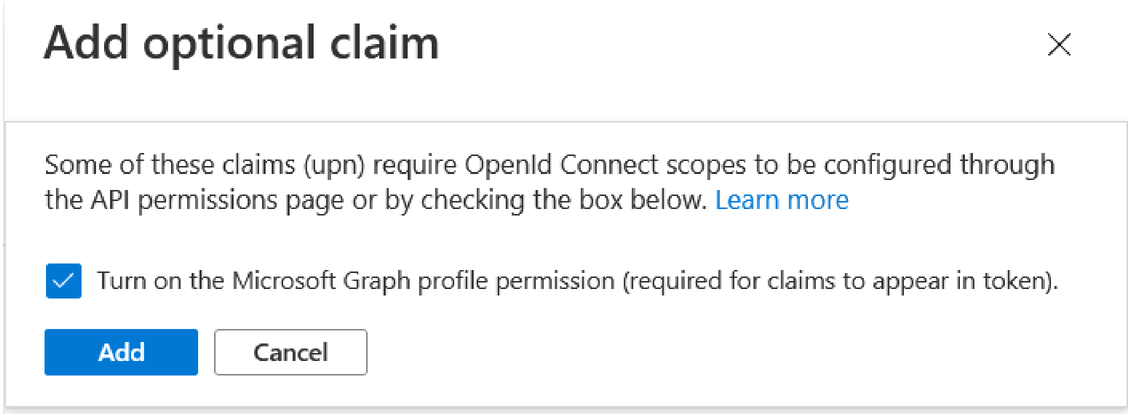
○ Access

○ SAML

Claim ↑	Description
□ sid	Session ID, used for per-session user sign out
□ tenant_ctry	Resource tenant's country/region
□ tenant_region_scope	Region of the resource tenant
☑ upn	An identifier for the user that can be used with the user...
□ verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
□ verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail
□ vnet	VNET specifier information
□ xms_pdl	Preferred data location
□ xms_pl	User-preferred language
□ xms_tpl	Tenant-preferred language
□ ztdid	Zero-touch Deployment ID

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

Figure 10-60: Turn on Profile Permission



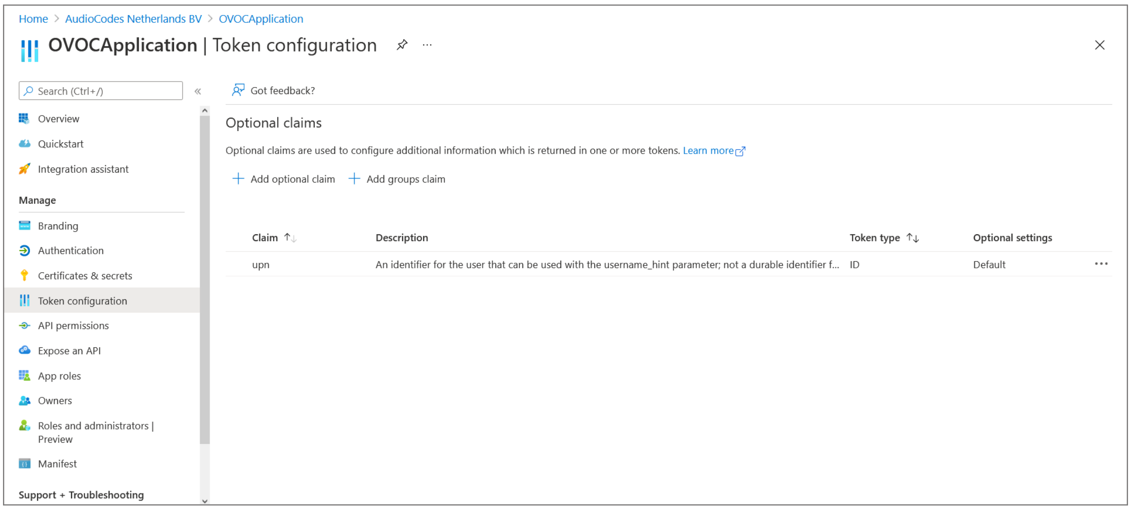
Add optional claim

Some of these claims (upn) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph profile permission (required for claims to appear in token).

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 10-61: Optional claims Added



Home > AudioCodes Netherlands BV > OVOCApplication

OVOCApplication | Token configuration

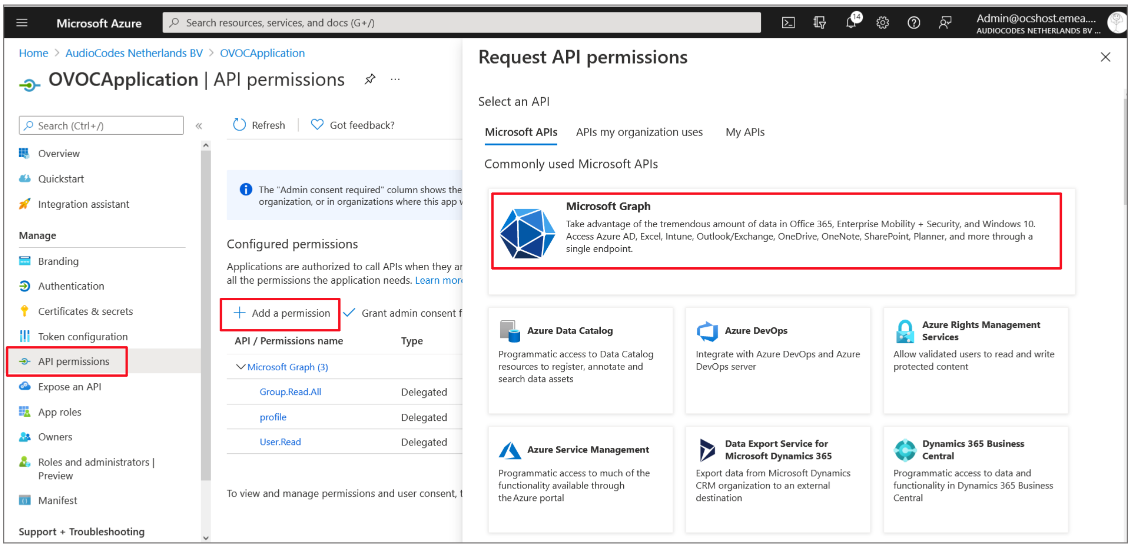
Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description	Token type ↑↓	Optional settings
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier f...	ID	Default

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

Figure 10-62: API Permissions



Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...

Home > AudioCodes Netherlands BV > OVOCApplication

OVOCApplication | API permissions

The "Admin consent required" column shows the organization, or in organizations where this app w

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (3)	
Group.Read.All	Delegated
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

Request API permissions

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

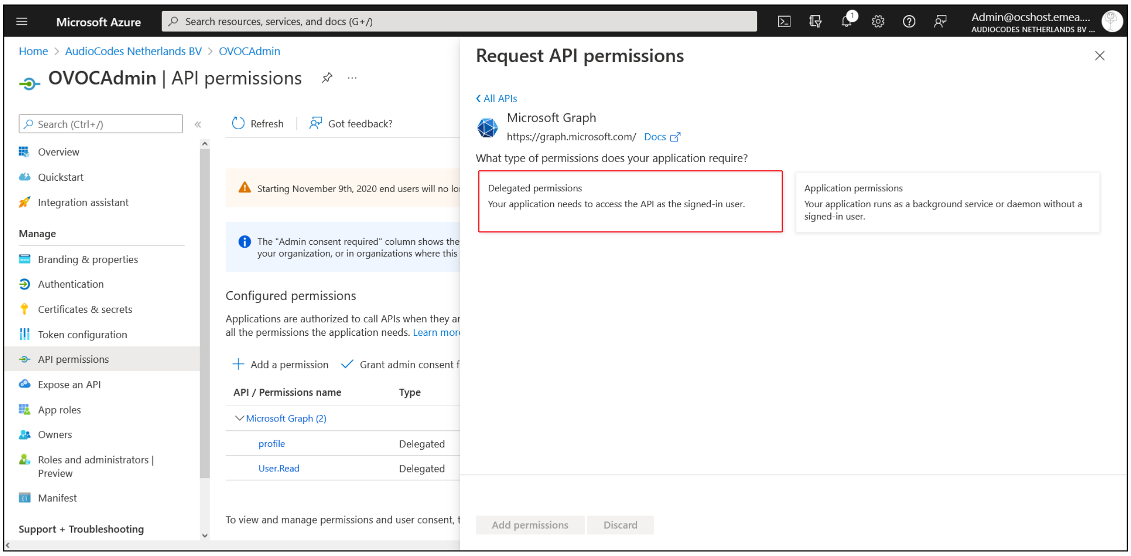
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

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

Figure 10-63: Delegated permissions



Starting November 9th, 2020 end users will no lo

The "Admin consent required" column shows the your organization, or in organizations where this

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn more

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

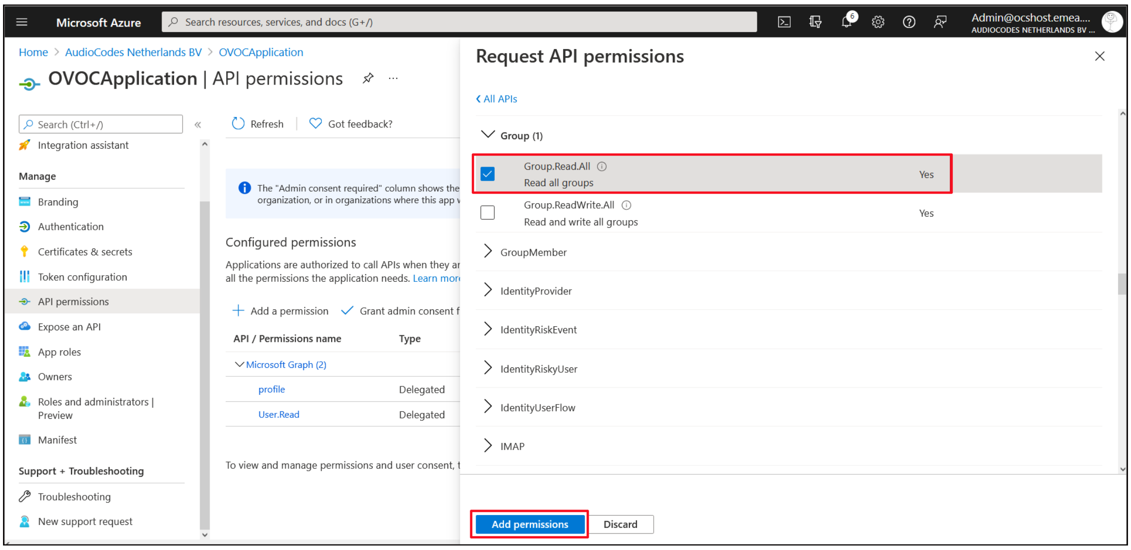
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

10. Click **Delegated permissions.**

Figure 10-64: Microsoft Graph Permissions



The "Admin consent required" column shows the organization, or in organizations where this app v

Configured permissions

Applications are authorized to call APIs when they ar all the permissions the application needs. Learn more

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

To view and manage permissions and user consent, t

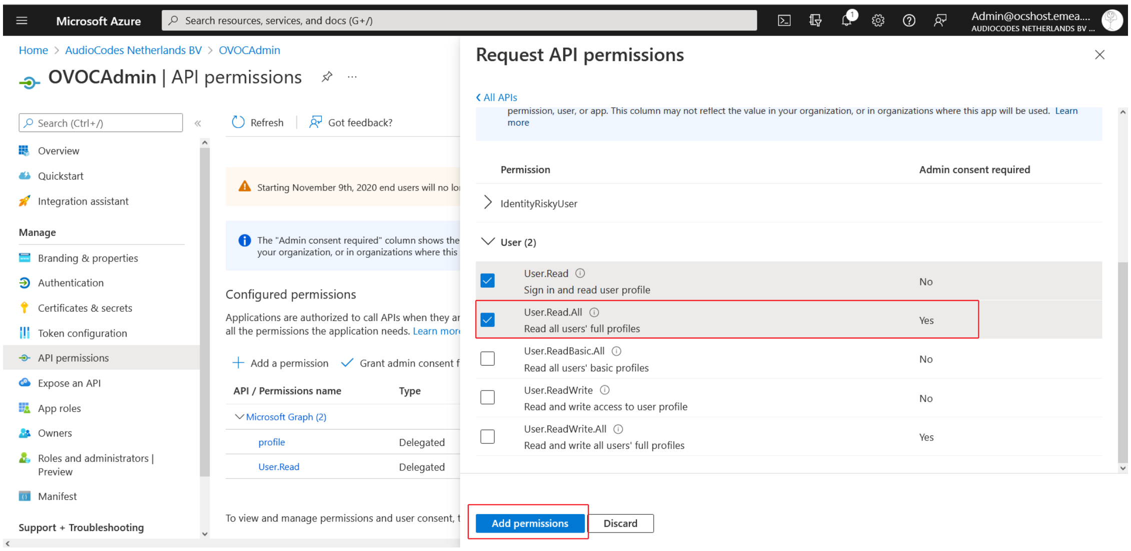
☑ Group.Read.All
Read all groups — Yes

☐ Group.ReadWrite.All
Read and write all groups — Yes

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 10-65: Delegated permissions


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Home > AudioCodes Netherlands BV > OVOCAdmin
OVOCAdmin | API permissions
Search (Ctrl+/)
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Refresh
Got feedback?
Starting November 9th, 2020 end users will no lo
The "Admin consent required" column shows the
your organization, or in organizations where this
Configured permissions
Applications are authorized to call APIs when they ar
all the permissions the application needs. Learn more
Add a permission
Grant admin consent f
To view and manage permissions and user consent, t

API / Permissions name	Type
Microsoft Graph (2)	
profile	Delegated
User.Read	Delegated

Request API permissions

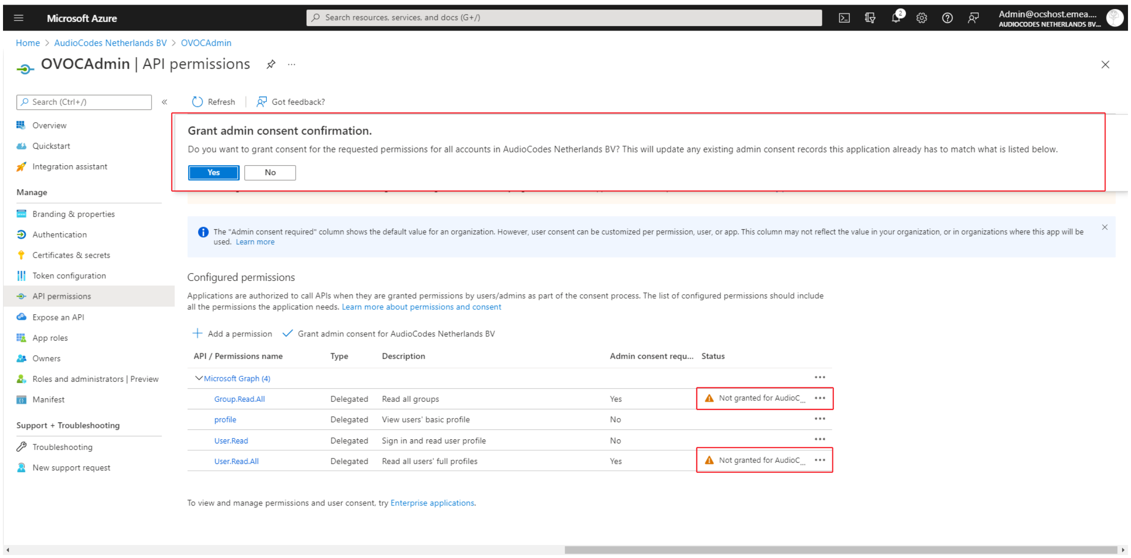
< All APIs

permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

	Permission	Admin consent required
	> IdentityRiskyUser	
	User (2)	
☑	User.Read Sign in and read user profile	No
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadBasic.All Read all users' basic profiles	No
□	User.ReadWrite Read and write access to user profile	No
□	User.ReadWrite.All Read and write all users' full profiles	Yes

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 10-66: Grant Admin Consent for all Accounts



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in AudioCodes Netherlands BV? This will update any existing admin consent records this application already has to match what is listed below.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

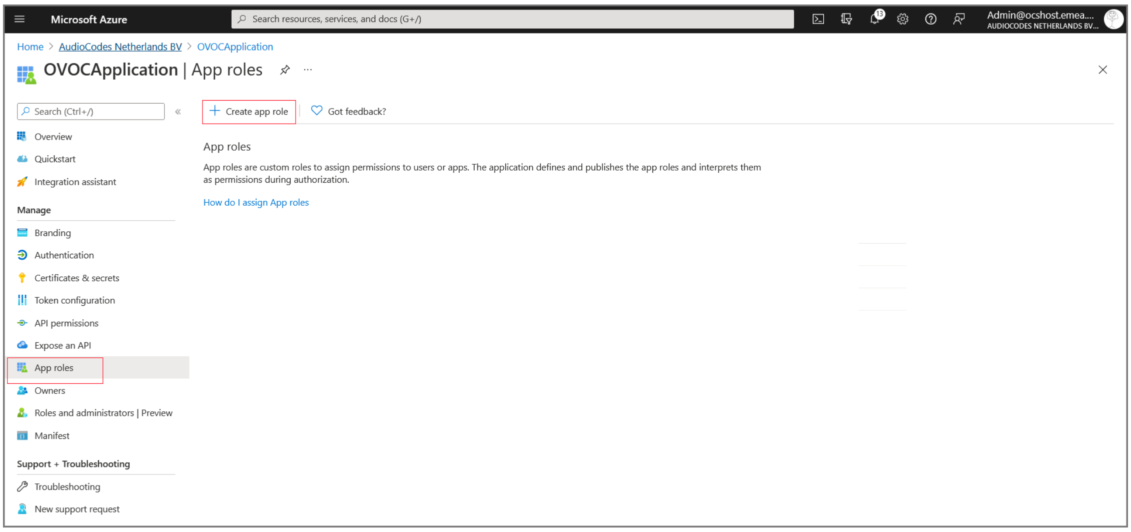
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Group.Read.All	Delegated	Read all groups	Yes	Not granted for AudioC...
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for AudioC...

To view and manage permissions and user consent, try Enterprise applications.

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

Figure 10-67: Create App Roles



App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

15. Create an app role with Admin permissions:

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

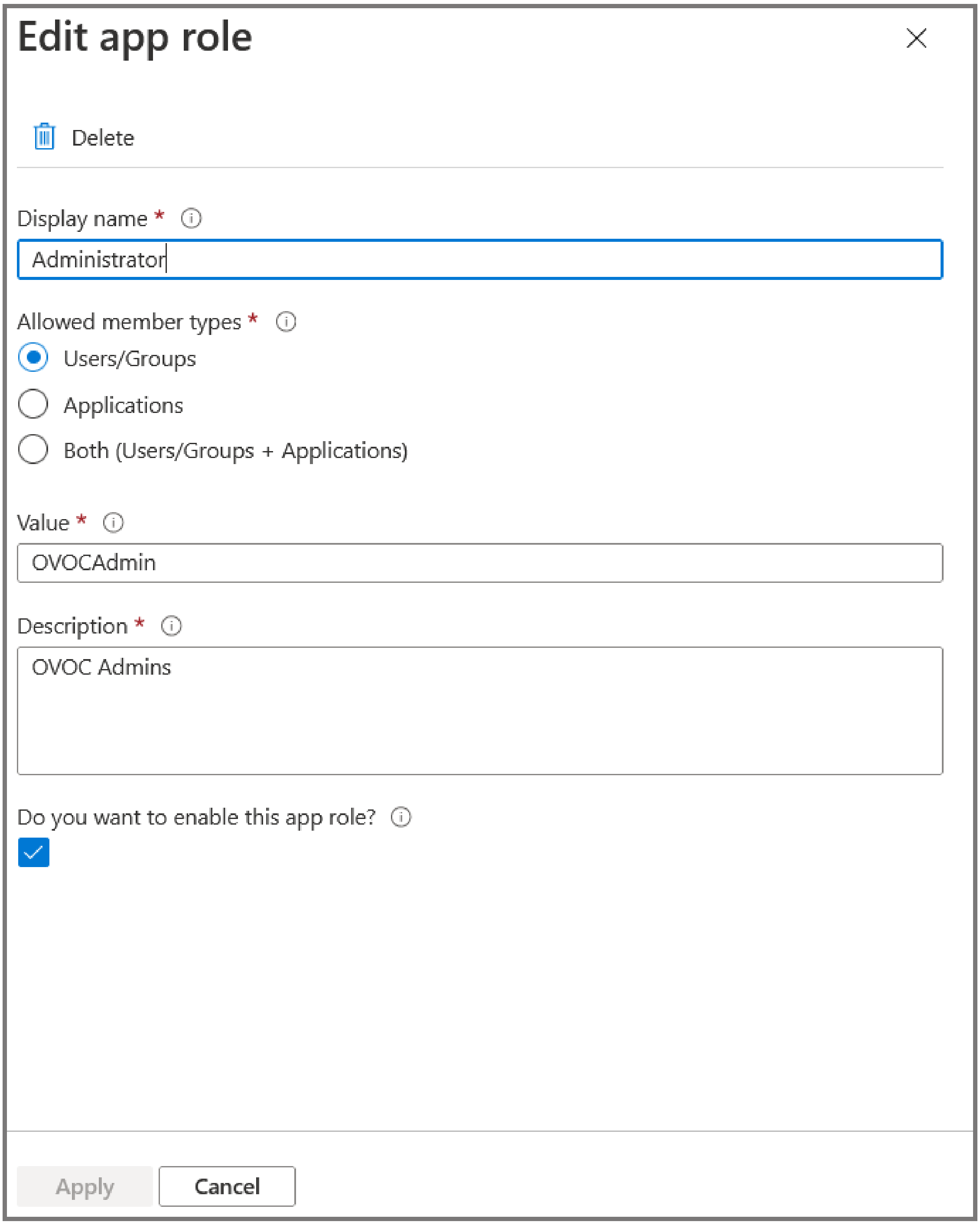
    b. Select Users/Groups check box

    c. Enter value "OVOCAdmin"

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

    e. Click **Apply**

Figure 10-68: Admin Role



Edit app role

Display name * ⓘ

Administrator

Allowed member types * ⓘ

● Users/Groups

○ Applications

○ Both (Users/Groups + Applications)

Value * ⓘ

OVOCAdmin

Description * ⓘ

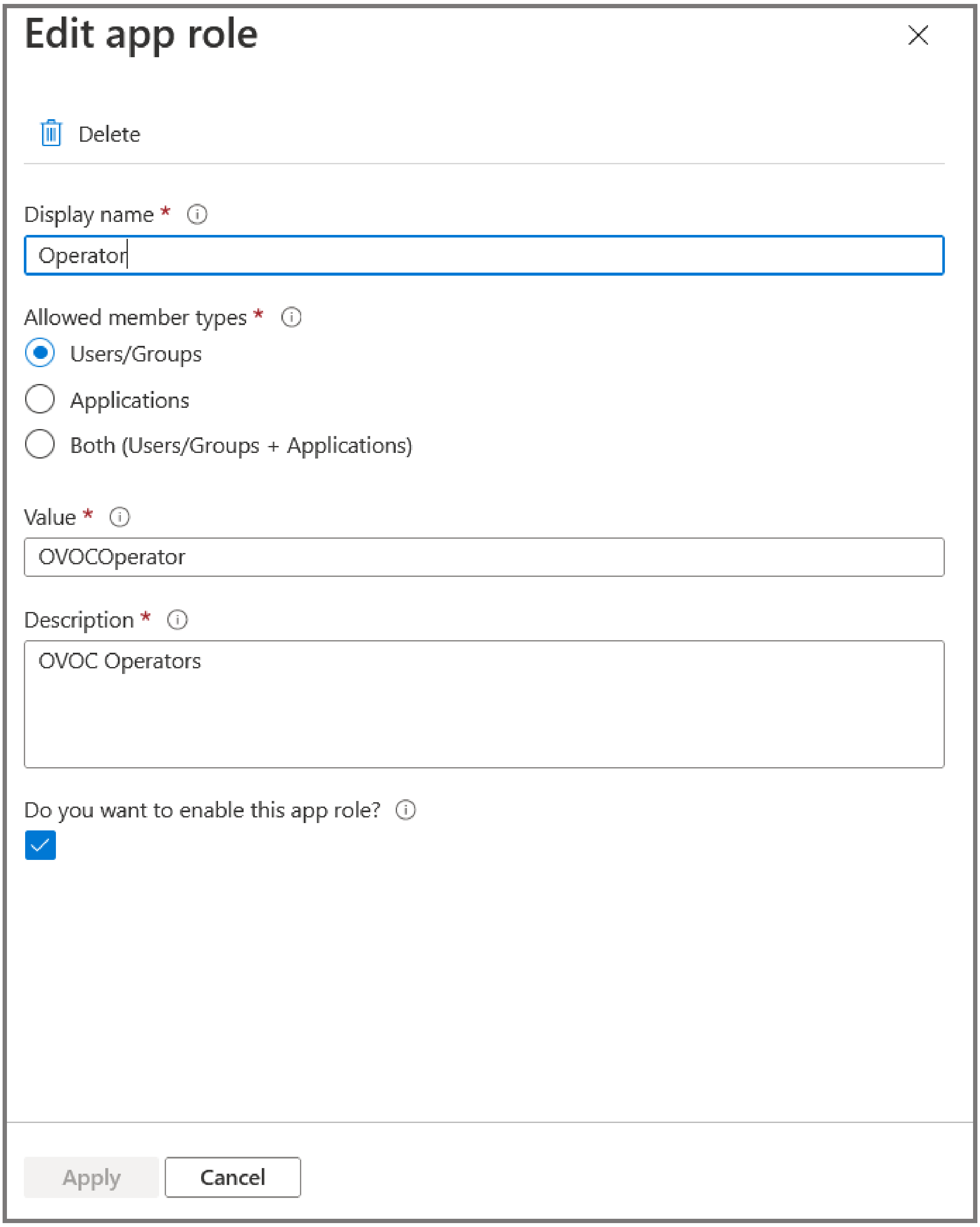
OVOC Admins

Do you want to enable this app role? ⓘ

☑

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

Figure 10-69: Operator Role



Edit app role

Delete

Display name * : Operator

Allowed member types *
● Users/Groups
○ Applications
○ Both (Users/Groups + Applications)

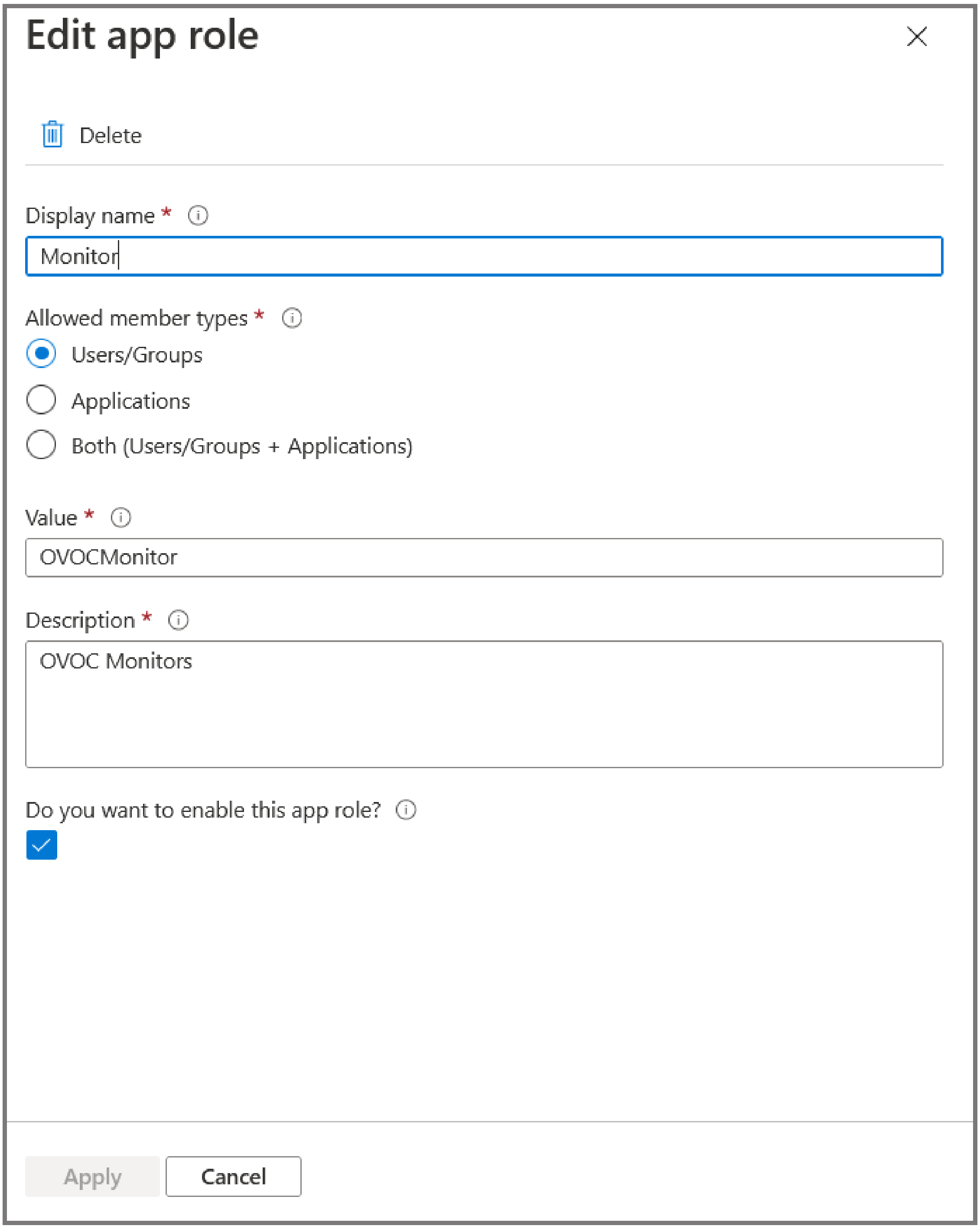
Value * : OVOCOperator

Description * : OVOC Operators

Do you want to enable this app role? ☑

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

Figure 10-70: Operator Role



Edit app role

Delete

Display name *

Monitor

Allowed member types *

● Users/Groups

○ Applications

○ Both (Users/Groups + Applications)

Value *

OVOCMonitor

Description *

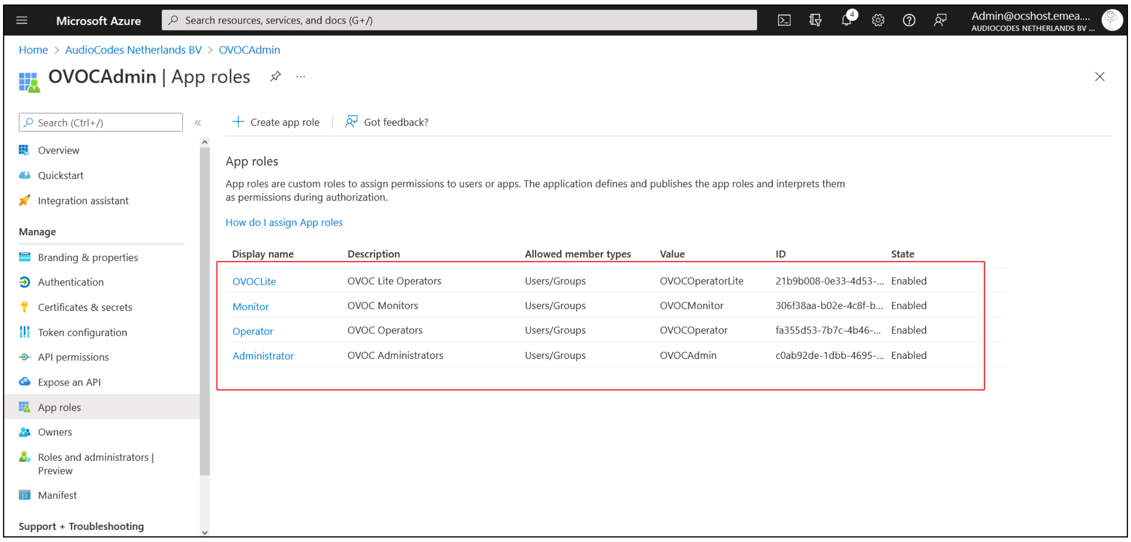
OVOC Monitors

Do you want to enable this app role?

☑

The new roles are displayed:

Figure 10-71: App roles Configured



OVOCAdmin | App roles

App roles

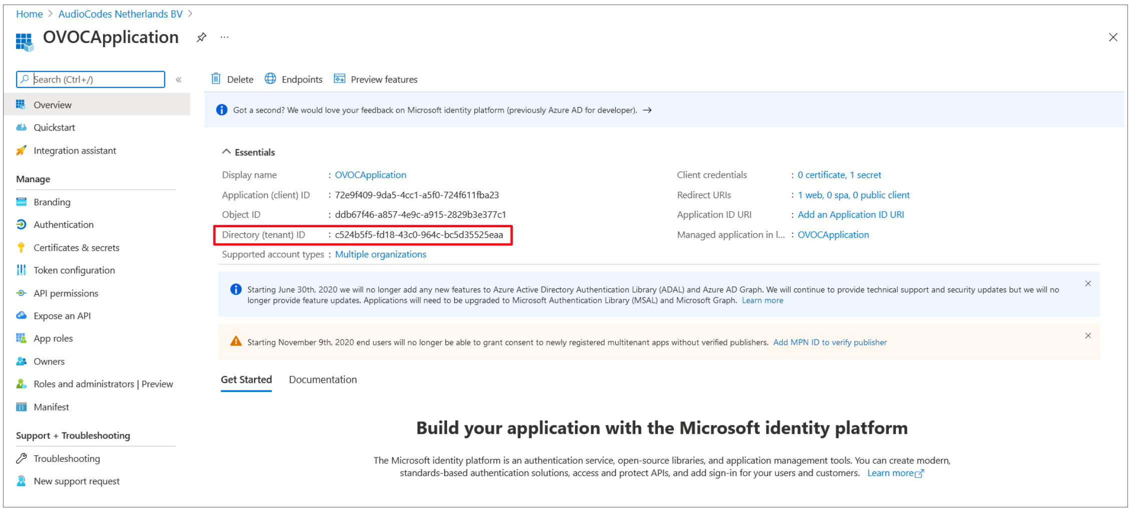
App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
OVOCLite	OVOC Lite Operators	Users/Groups	OVOCOperatorLite	21b9b008-0e33-4d53-...	Enabled
Monitor	OVOC Monitors	Users/Groups	OVOCMonitor	306f38aa-b02e-4c8f-b...	Enabled
Operator	OVOC Operators	Users/Groups	OVOCOperator	fa355d53-7b7c-4b46-...	Enabled
Administrator	OVOC Administrators	Users/Groups	OVOCAdmin	c0ab92de-1dbb-4695-...	Enabled

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

Figure 10-72: Overview Page



OVOCApplication

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	:	OVOCApplication	Client credentials	:	0 certificate, 1 secret
Application (client) ID	:	72e9f409-9da5-4cc1-a5f0-724f611fba23	Redirect URIs	:	1 web, 0 spa, 0 public client
Object ID	:	ddb67f46-a857-4e9c-a915-2829b3e377c1	Application ID URI	:	Add an Application ID URI
Directory (tenant) ID	:	c524b5f5-fd18-43c0-964c-bc5d35525eaa	Managed application in l...	:	OVOCApplication
Supported account types	:	Multiple organizations			

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

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 128

21. Configure Azure settings in OVOC Web as described in Configuring OVOC Web Azure Settings - Multitenant Upgrade below

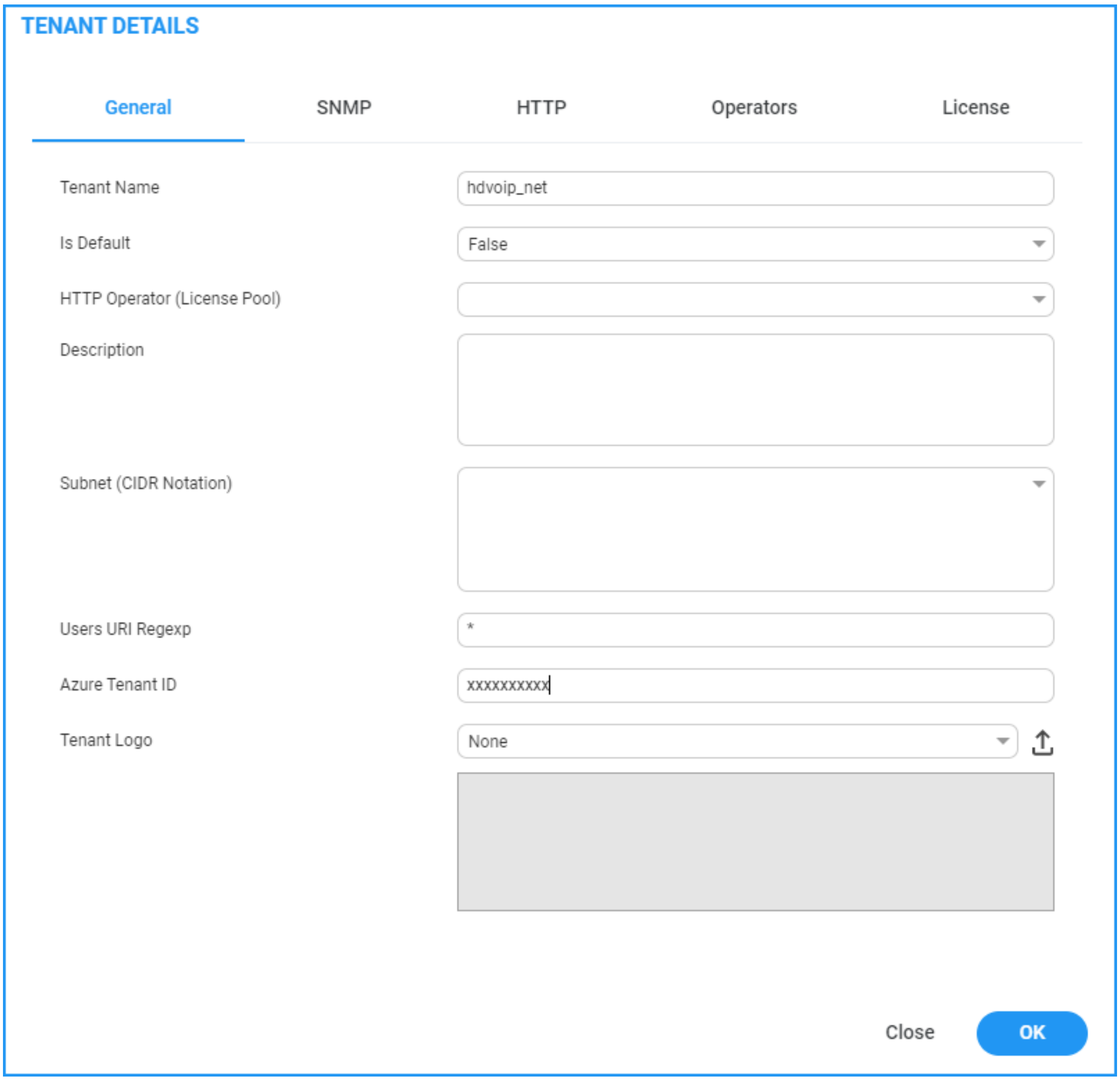
Configuring OVOC Web Azure Settings - Multitenant Upgrade

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 10-73: Tenant Details

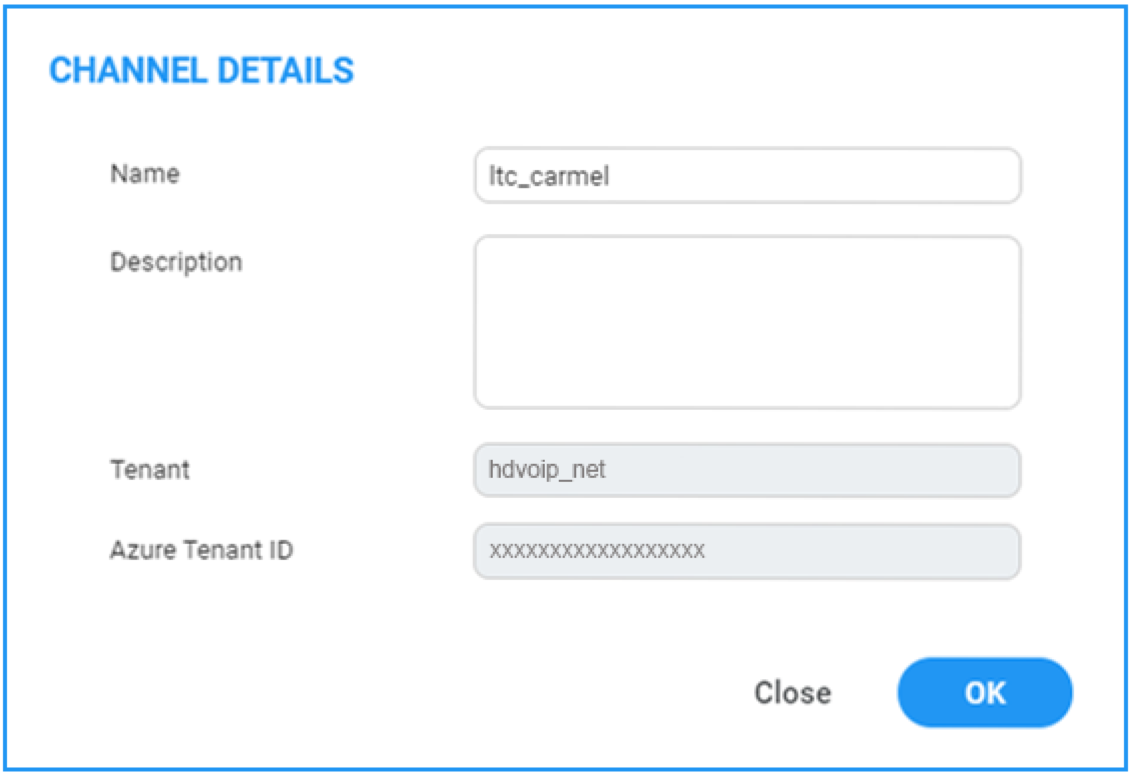


TENANT DETAILS

Tenant Name	hdvoip_net
Is Default	False
HTTP Operator (License Pool)	
Description	
Subnet (CIDR Notation)	
Users URI Regexp	*
Azure Tenant ID	xxxxxxxxxx
Tenant Logo	None

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 10-74: Channel Details



CHANNEL DETAILS

Name: ltc_carmel

Description:

Tenant: hdvoip_net

Azure Tenant ID: xxxxxxxxxxxxxxxxxx

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 10-1: 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'.

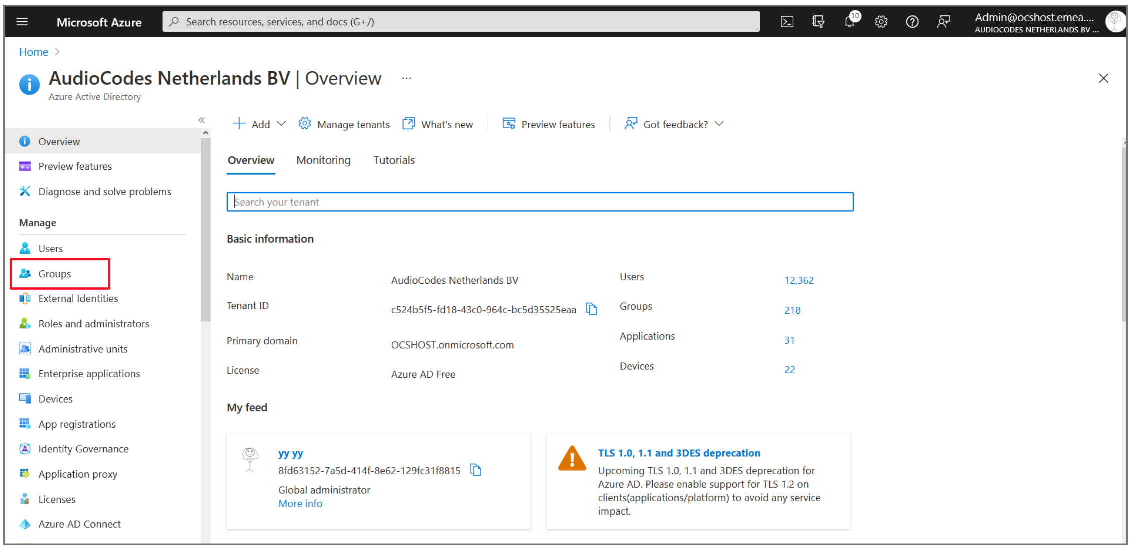
Security Group OVOC (Parameter Name)	Description
Tenant Operator User Group Name	The name of the User Group of the 'Tenant' type operator whose security level is 'Operator'.
Tenant Monitor User Group Name	The name of the name of the User Group of the 'Tenant' type operator whose security level is 'Monitor'.
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 10-75: Tenant Overview Page



AudioCodes Netherlands BV | Overview

Azure Active Directory

Basic information

Name	AudioCodes Netherlands BV	Users	12,362
Tenant ID	c524b5f5-fd18-43c0-964c-bc5d35525eaa	Groups	218
Primary domain	OCSHOST.onmicrosoft.com	Applications	31
License	Azure AD Free	Devices	22

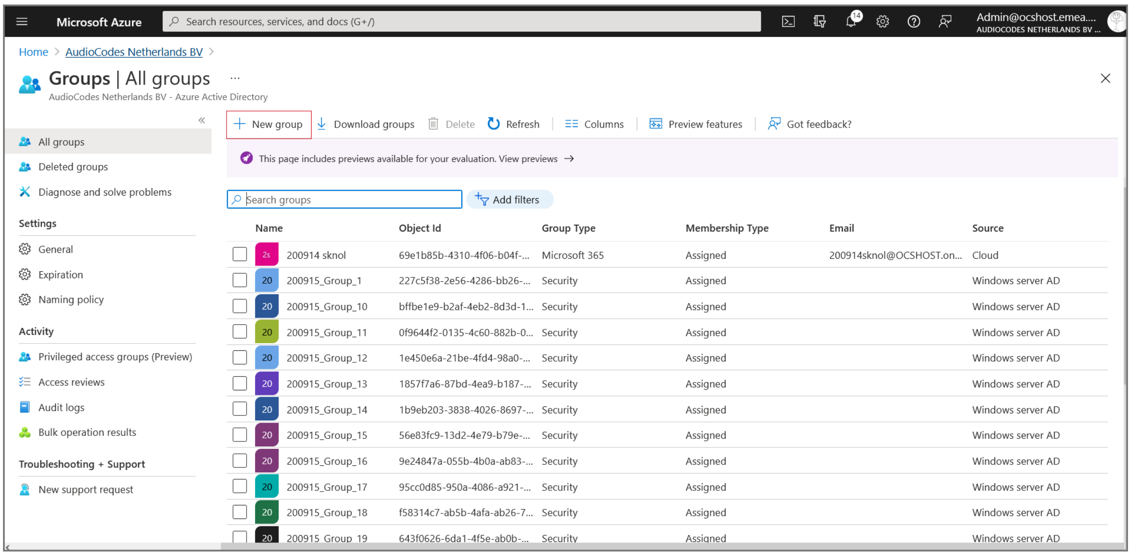
My feed

yy yy
8fd63152-7a5d-414f-8e62-129fc31f8815
Global administrator
More info

TLS 1.0, 1.1 and 3DES deprecation
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

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

Figure 10-76: Create New Group

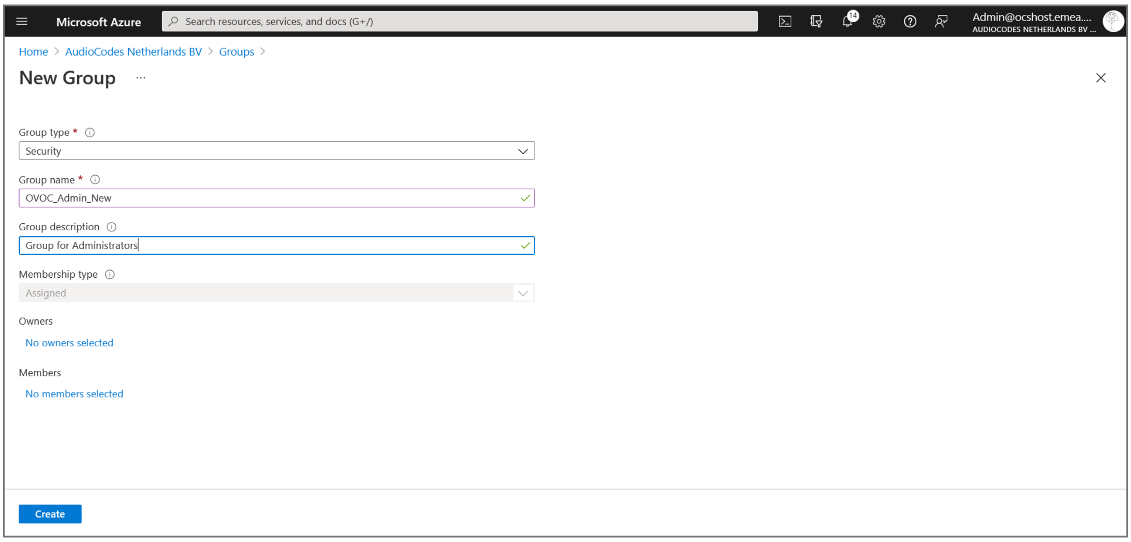


This page includes previews available for your evaluation. View previews →

	Name	Object Id	Group Type	Membership Type	Email	Source
□	2s 200914 sknol	69e1b85b-4310-4f06-b04f-...	Microsoft 365	Assigned	200914sknol@OCSHOST.on...	Cloud
□	20 200915_Group_1	227c5f38-2e56-4286-bb26-...	Security	Assigned		Windows server AD
□	20 200915_Group_10	bffbe1e9-b2af-4eb2-8d3d-1...	Security	Assigned		Windows server AD
□	20 200915_Group_11	0f9644f2-0135-4c60-882b-0...	Security	Assigned		Windows server AD
□	20 200915_Group_12	1e450e6a-21be-4fd4-98a0-...	Security	Assigned		Windows server AD
□	20 200915_Group_13	1857f7a6-87bd-4ea9-b187-...	Security	Assigned		Windows server AD
□	20 200915_Group_14	1b9eb203-3838-4026-8697-...	Security	Assigned		Windows server AD
□	20 200915_Group_15	56e83fc9-13d2-4e79-b79e-...	Security	Assigned		Windows server AD
□	20 200915_Group_16	9e24847a-055b-4b0a-ab83-...	Security	Assigned		Windows server AD
□	20 200915_Group_17	95cc0d85-950a-4086-a921-...	Security	Assigned		Windows server AD
□	20 200915_Group_18	f58314c7-ab5b-4afa-ab26-7...	Security	Assigned		Windows server AD
□	20 200915_Group_19	643f0626-6da1-4f5e-ab0b-...	Security	Assigned		Windows server AD

4. Click **New group**.

Figure 10-77: New Group


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV ...
Home > AudioCodes Netherlands BV > Groups >
New Group ...
Create

Group type * Security

Group name * OVOC_Admin_New

Group description Group for Administrators

Membership type Assigned

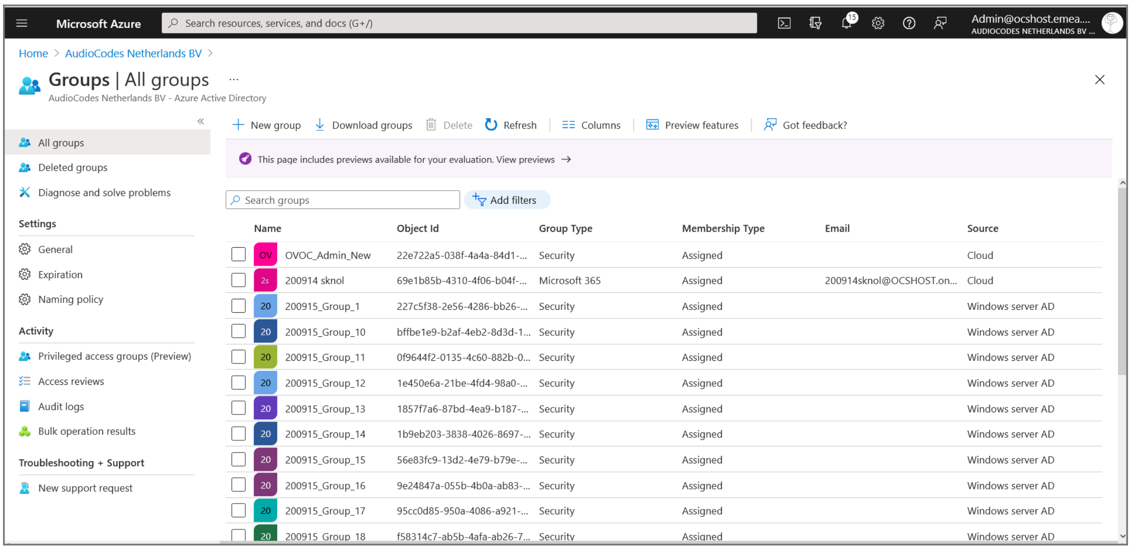
Owners
No owners selected

Members
No members selected

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 90)

Figure 10-78: Created Group



Groups | All groups

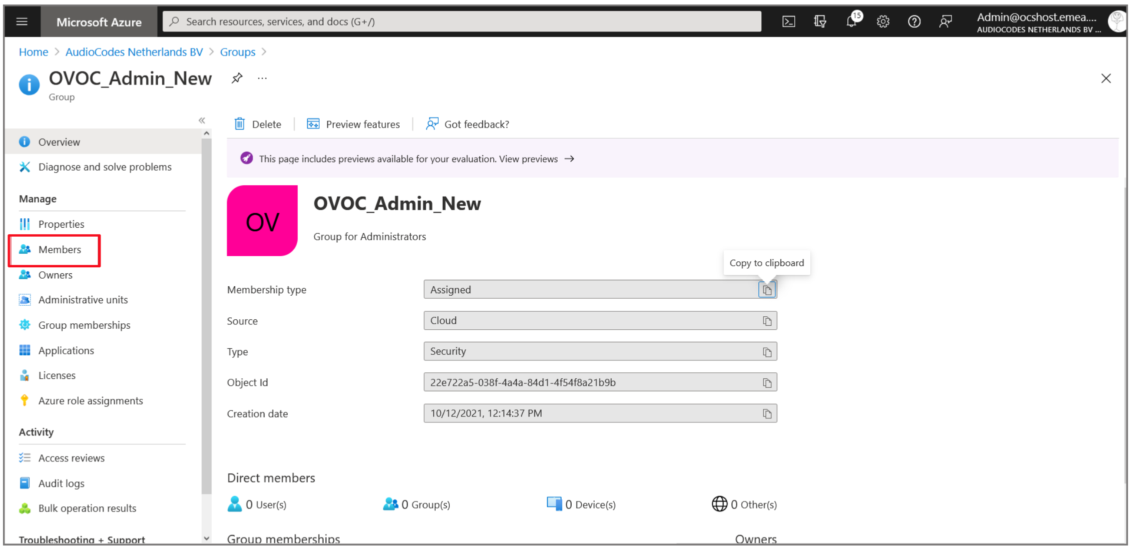
AudioCodes Netherlands BV - Azure Active Directory

	Name	Object Id	Group Type	Membership Type	Email	Source
□	OV OVOC_Admin_New	22e722a5-038f-4a4a-84d1-...	Security	Assigned		Cloud
□	2s 200914 sknol	69e1b85b-4310-4f06-b04f-...	Microsoft 365	Assigned	200914sknol@OCSHOST.on...	Cloud
□	20 200915_Group_1	227c5f38-2e56-4286-bb26-...	Security	Assigned		Windows server AD
□	20 200915_Group_10	bffbe1e9-b2af-4eb2-8d3d-1...	Security	Assigned		Windows server AD
□	20 200915_Group_11	0f9644f2-0135-4c60-882b-0...	Security	Assigned		Windows server AD
□	20 200915_Group_12	1e450e6a-21be-4fd4-98a0-...	Security	Assigned		Windows server AD
□	20 200915_Group_13	1857f7a6-87bd-4ea9-b187-...	Security	Assigned		Windows server AD
□	20 200915_Group_14	1b9eb203-3838-4026-8697-...	Security	Assigned		Windows server AD
□	20 200915_Group_15	56e83fc9-13d2-4e79-b79e-...	Security	Assigned		Windows server AD
□	20 200915_Group_16	9e24847a-055b-4b0a-ab83-...	Security	Assigned		Windows server AD
□	20 200915_Group_17	95cc0d85-950a-4086-a921-...	Security	Assigned		Windows server AD
□	20 200915_Group_18	f58314c7-ab5b-4afa-ab26-7...	Security	Assigned		Windows server AD

6. Select the new group.

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

Figure 10-79: Add Members to Group



OVOC_Admin_New

Group for Administrators

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: 22e722a5-038f-4a4a-84d1-4f54f8a21b9b

Creation date: 10/12/2021, 12:14:37 PM

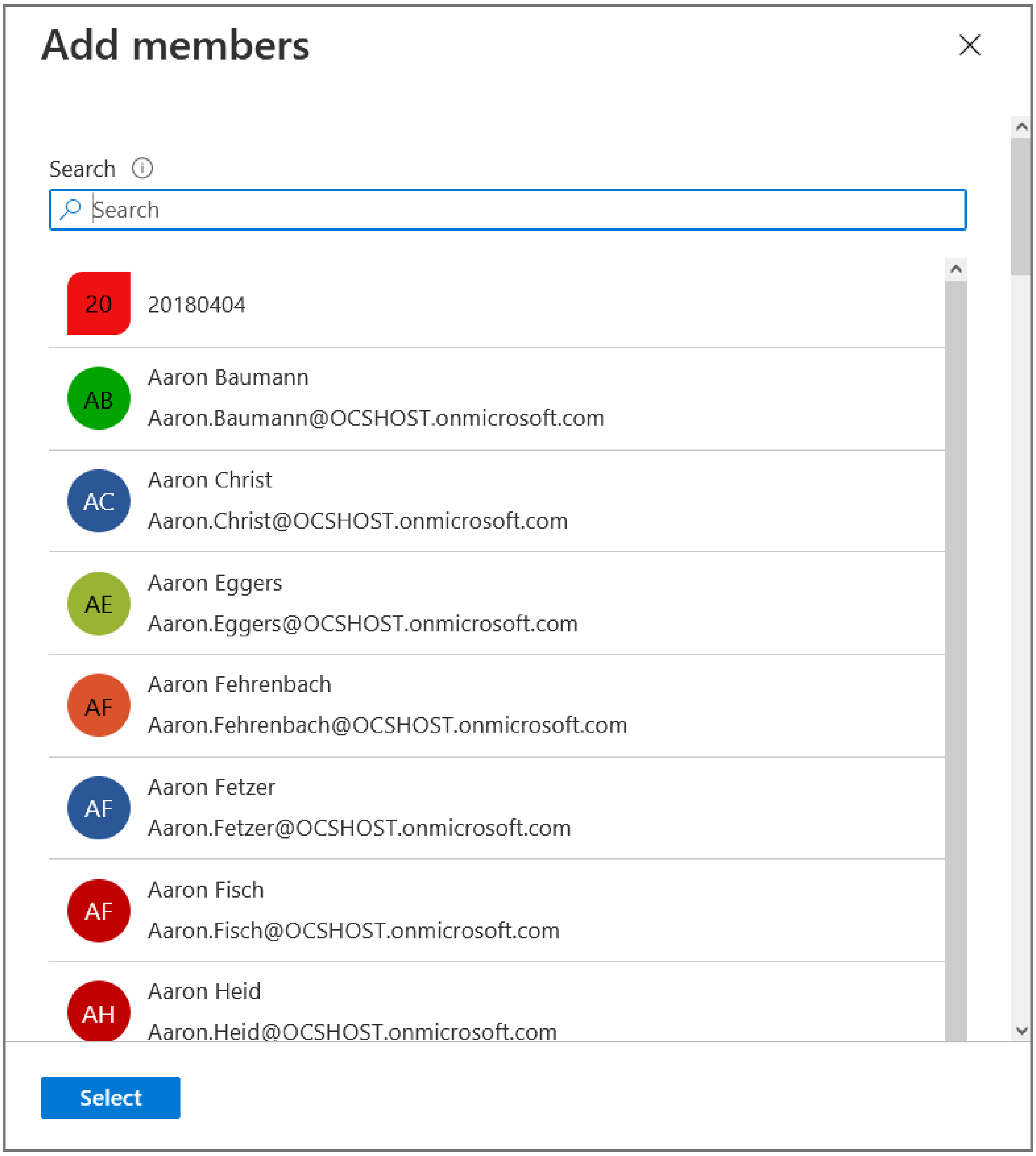
Direct members

0 User(s) 0 Group(s) 0 Device(s) 0 Other(s)

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

9. Select the members to add to the Group.

Figure 10-80: Select Group Members



Add members

Search

Search

20 20180404

AB Aaron Baumann
Aaron.Baumann@OCSHOST.onmicrosoft.com

AC Aaron Christ
Aaron.Christ@OCSHOST.onmicrosoft.com

AE Aaron Eggers
Aaron.Eggers@OCSHOST.onmicrosoft.com

AF Aaron Fehrenbach
Aaron.Fehrenbach@OCSHOST.onmicrosoft.com

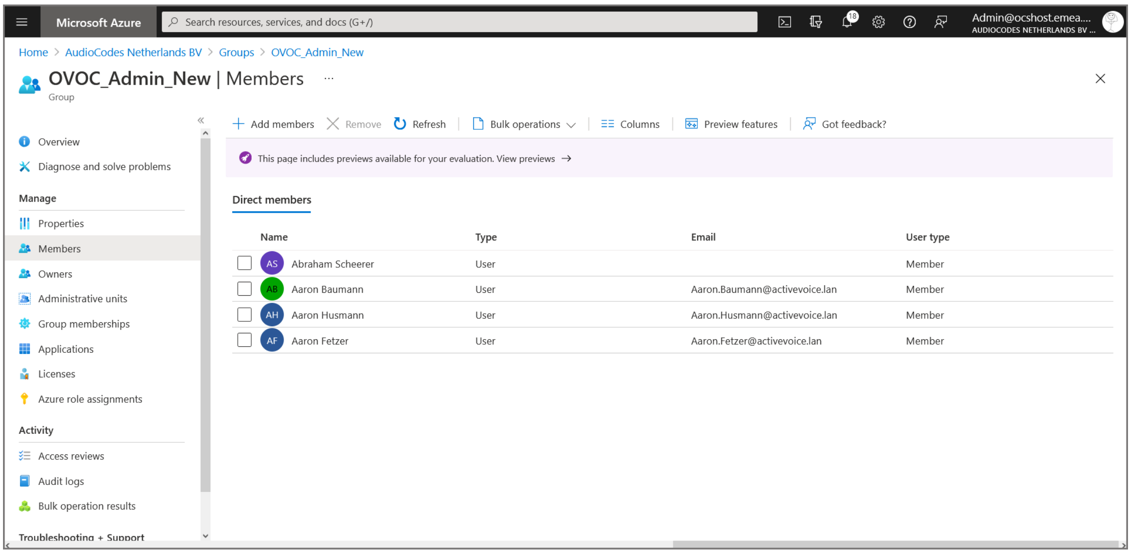
AF Aaron Fetzer
Aaron.Fetzer@OCSHOST.onmicrosoft.com

AF Aaron Fisch
Aaron.Fisch@OCSHOST.onmicrosoft.com

AH Aaron Heid
Aaron.Heid@OCSHOST.onmicrosoft.com

The new members are added to the group.

Figure 10-81: New Group Members



	Name	Type	Email	User type
□	AS Abraham Scheerer	User		Member
□	AB Aaron Baumann	User	Aaron.Baumann@activevoice.lan	Member
□	AH Aaron Husmann	User	Aaron.Husmann@activevoice.lan	Member
□	AF Aaron Fetzer	User	Aaron.Fetzer@activevoice.lan	Member

10. Proceed to Configuring OVOC Web Azure Settings - Single Tenant Setup on page 90.

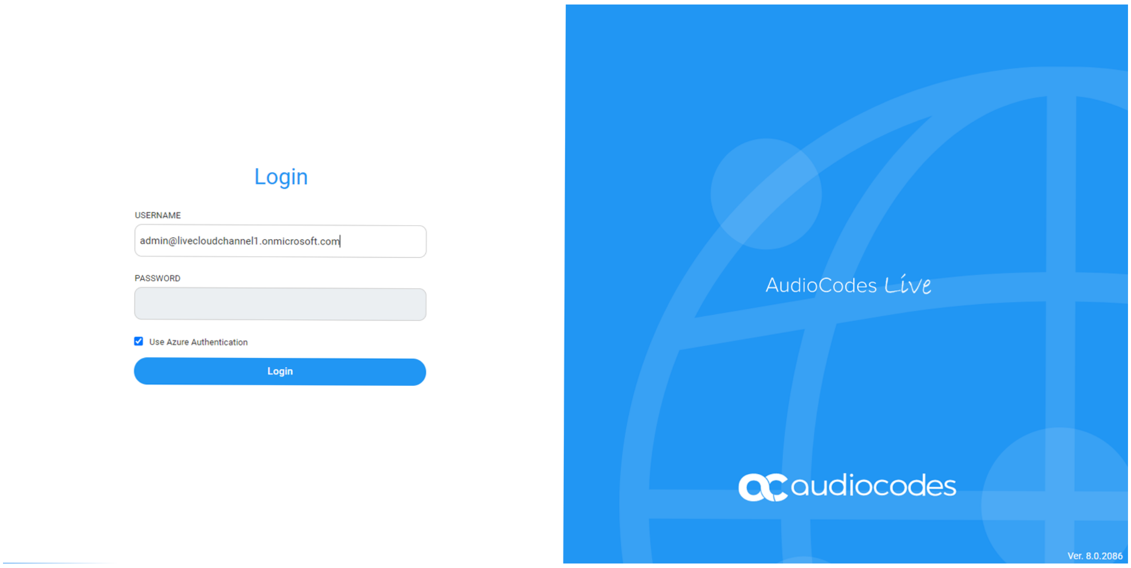
Add External Tenant Operators and Assign Roles

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 123.

Figure 10-82: Initial Operator Login



USERNAME
admin@livecloudchannel1.onmicrosoft.com

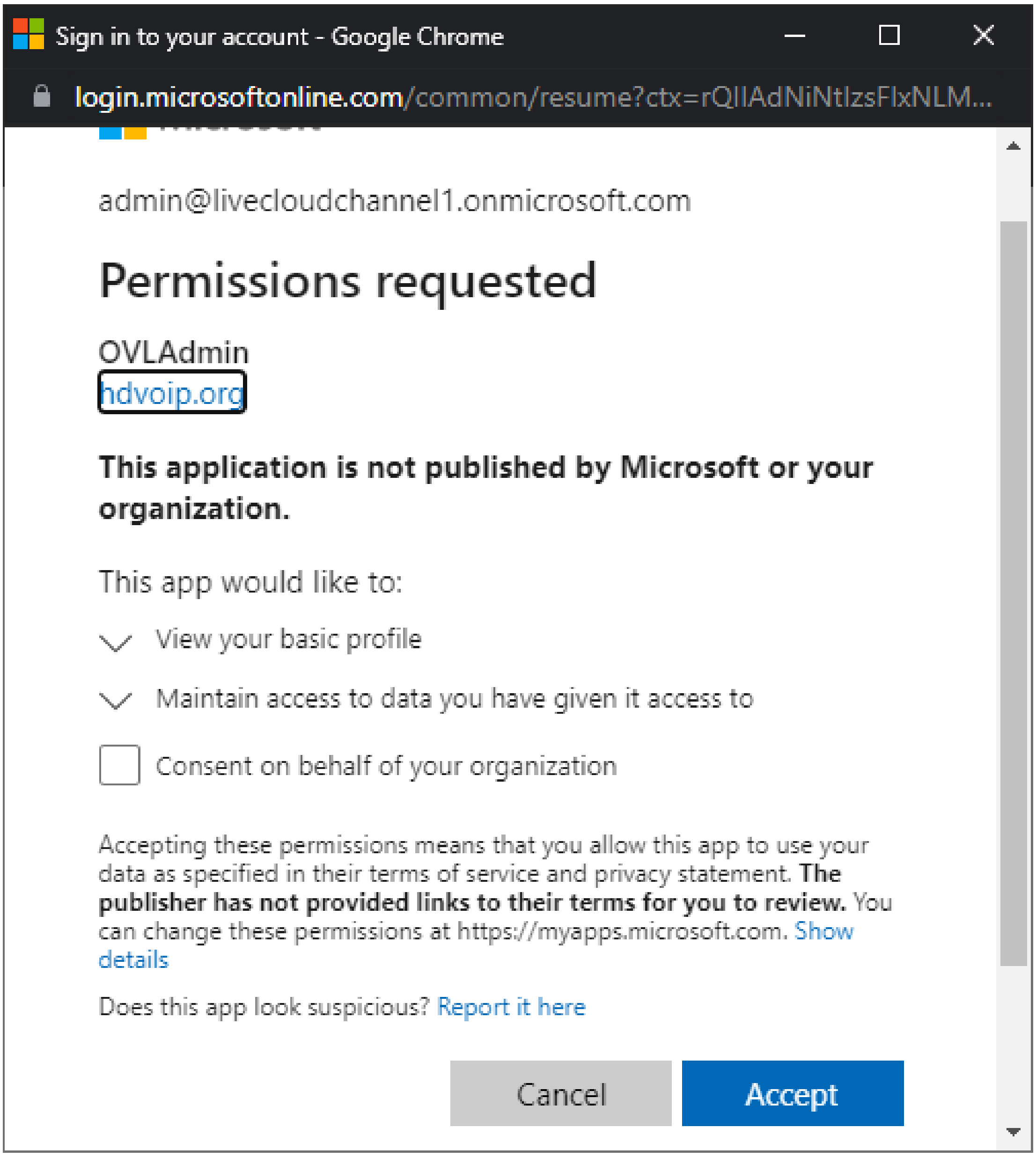
PASSWORD

☑ Use Azure Authentication

Login

The Azure authentication and Permissions request dialog is displayed:

Figure 10-83: Permissions requested


Sign in to your account - Google Chrome
login.microsoftonline.com/common/resume?ctx=rQIIAdNiNtIzsFlxNLM...

admin@livecloudchannel1.onmicrosoft.com

Permissions requested

OVLAdmin
hdvoip.org

This application is not published by Microsoft or your organization.

This app would like to:

- View your basic profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

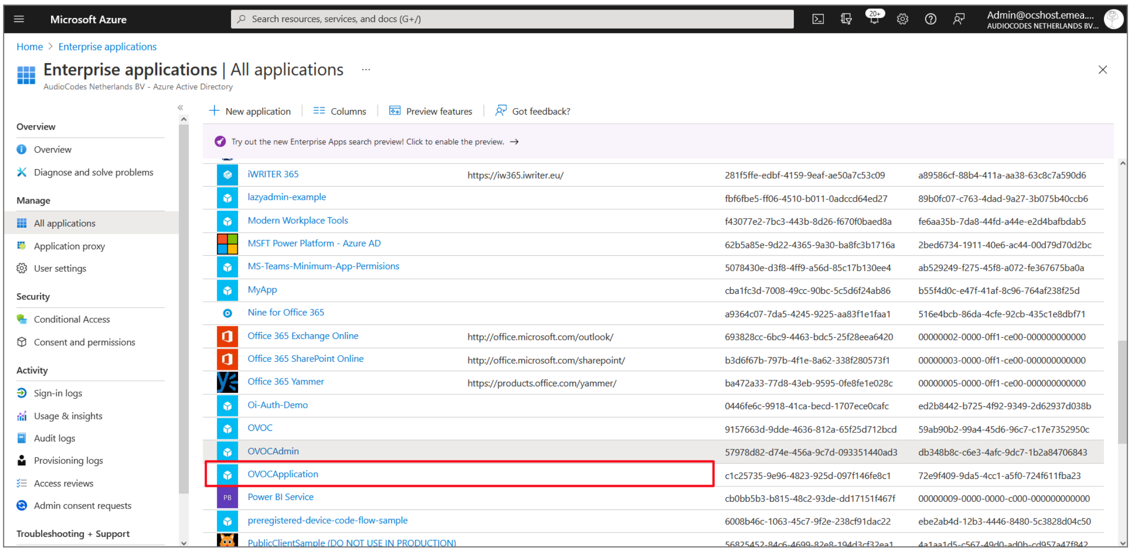
Does this app look suspicious? Report it here

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 135.

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

Figure 10-84: OVOC Application

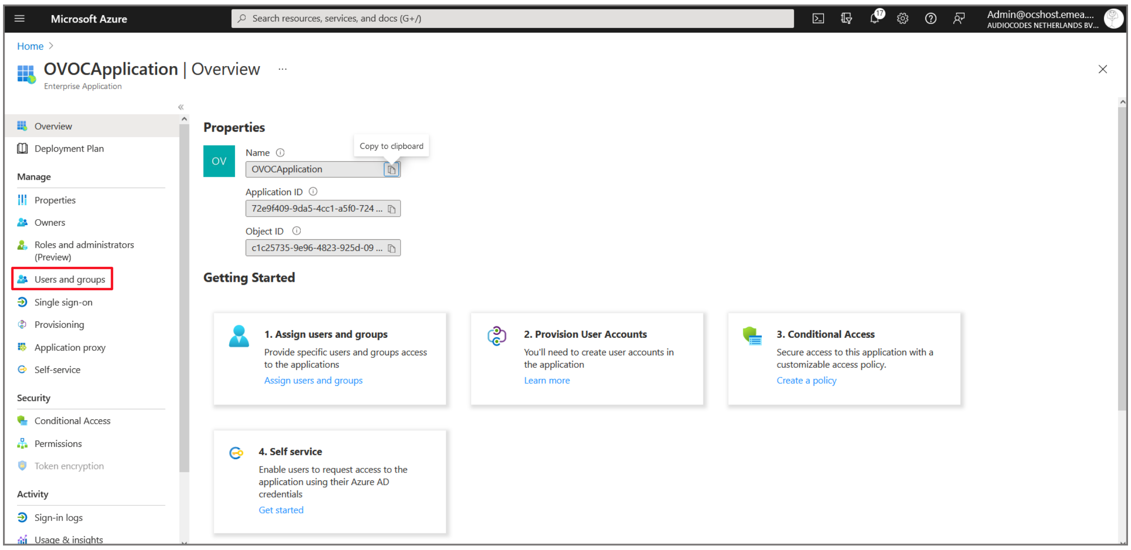


Try out the new Enterprise Apps search preview! Click to enable the preview. →

iWRITER 365	https://iw365.iwriter.eu/	281f5ffe-edbf-4159-9eaf-ae50a7c53c09	a89586cf-88b4-411a-aa38-63c8c7a590d6
lazyadmin-example		fbf6fbe5-ff06-4510-b011-0adccd64ed27	89b0fc07-c763-4dad-9a27-3b075b40ccb6
Modern Workplace Tools		f43077e2-7bc3-443b-8d26-f670f0baed8a	fe6aa35b-7da8-44fd-a44e-e2d4bafbdab5
MSFT Power Platform - Azure AD		62b5a85e-9d22-4365-9a30-ba8fc3b1716a	2bed6734-1911-40e6-ac44-00d79d70d2bc
MS-Teams-Minimum-App-Permisions		5078430e-d3f8-4ff9-a56d-85c17b130ee4	ab529249-f275-45f8-a072-fe367675ba0a
MyApp		cba1fc3d-7008-49cc-90bc-5c5d6f24ab86	b55f4d0c-e47f-41af-8c96-764af238f25d
Nine for Office 365		a9364c07-7da5-4245-9225-aa83f1e1faa1	516e4bcb-86da-4cfe-92cb-435c1e8dbf71
Office 365 Exchange Online	http://office.microsoft.com/outlook/	693828cc-6bc9-4463-bdc5-25f28eea6420	00000002-0000-0ff1-ce00-000000000000
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	b3d6f67b-797b-4f1e-8a62-338f280573f1	00000003-0000-0ff1-ce00-000000000000
Office 365 Yammer	https://products.office.com/yammer/	ba472a33-77d8-43eb-9595-0fe8fe1e028c	00000005-0000-0ff1-ce00-000000000000
Oi-Auth-Demo		0446fe6c-9918-41ca-becd-1707ece0cafc	ed2b8442-b725-4f92-9349-2d62937d038b
OVOC		9157663d-9dde-4636-812a-65f25d712bcd	59ab90b2-99a4-45d6-96c7-c17e7352950c
OVOCAdmin		57978d82-d74e-456a-9c7d-093351440ad3	db348b8c-c6e3-4afc-9dc7-1b2a84706843
OVOCApplication		c1c25735-9e96-4823-925d-097f146fe8c1	72e9f409-9da5-4cc1-a5f0-724f611fba23
PB Power BI Service		cb0bb5b3-b815-48c2-93de-dd17151f467f	00000009-0000-0000-c000-000000000000
preregistered-device-code-flow-sample		6008b46c-1063-45c7-9f2e-238cf91dac22	ebe2ab4d-12b3-4446-8480-5c3828d04c50
PublicClientSample (DO NOT USE IN PRODUCTION)		56825452-84c6-4699-82e8-194d3cf32ea1	4a1aa1d5-c567-49d0-ad0b-cd957a47f842

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

Figure 10-85: Users and Groups



Properties

Name: OVOCApplication

Application ID: 72e9f409-9da5-4cc1-a5f0-724 ...

Object ID: c1c25735-9e96-4823-925d-09 ...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Provision User Accounts
You'll need to create user accounts in the application
Learn more

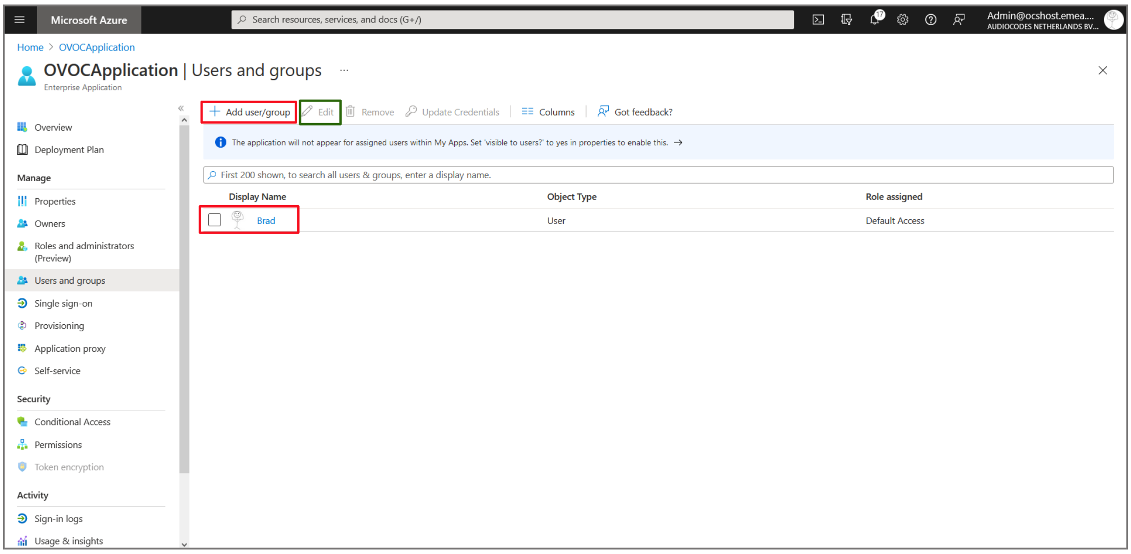
3. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

4. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

5. Do one of the following:

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

Figure 10-86: Assign Role to New User /Existing User



Microsoft Azure | Search resources, services, and docs (G+/) | Admin@ocshost.emea.... AUDIOCODES NETHERLANDS BV...

Home > OVOCApplication

OVOCApplication | Users and groups

Enterprise Application

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

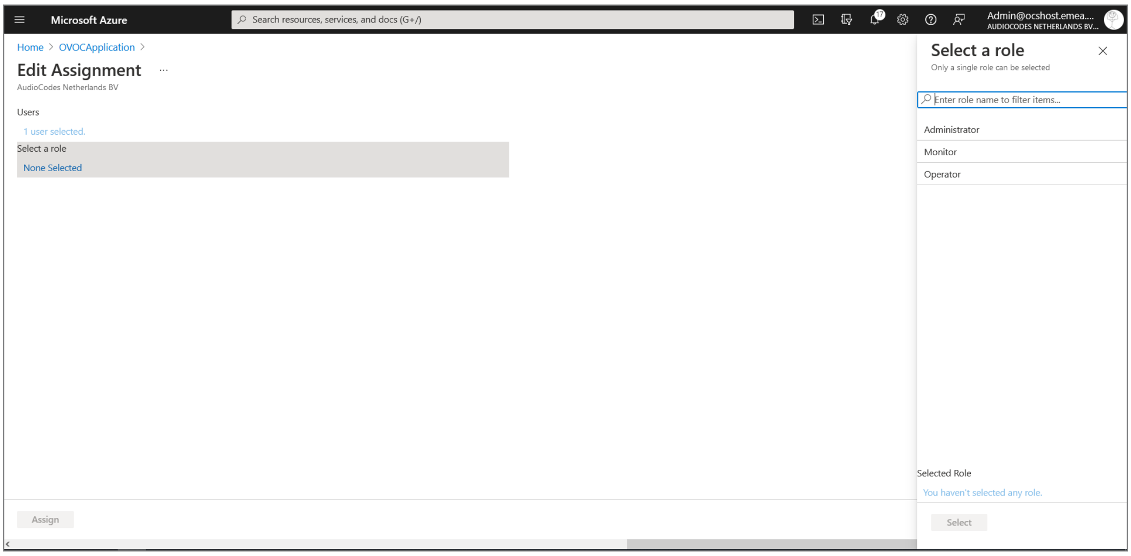
First 200 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	Brad	User	Default Access

➢ To assign a role to an existing user:

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

Figure 10-87: Edit Assignment



Microsoft Azure | Search resources, services, and docs (G+/) | Admin@ocshost.emea.... AUDIOCODES NETHERLANDS BV...

Home > OVOCApplication >

Edit Assignment

AudioCodes Netherlands BV

Users

1 user selected.

Select a role

None Selected

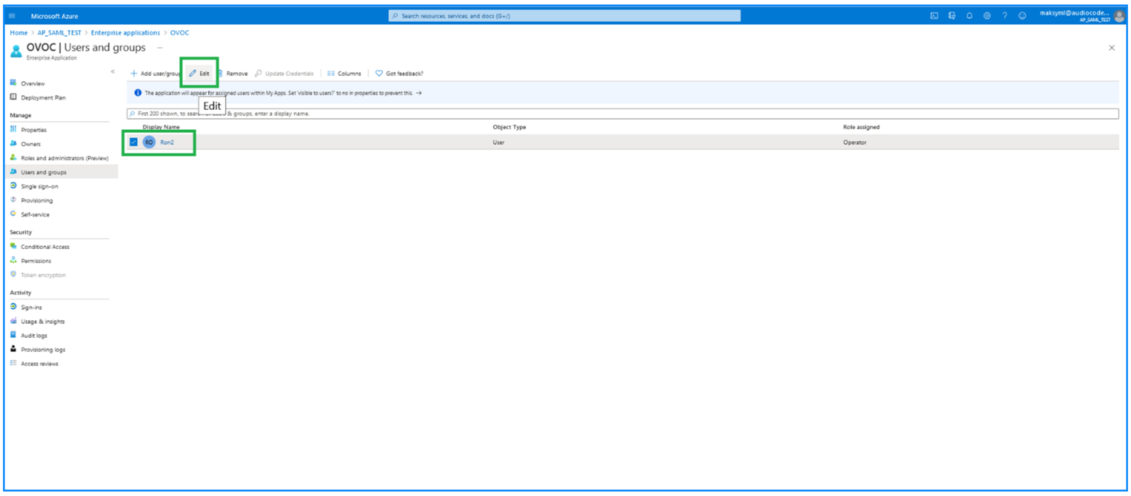
Select a role

Only a single role can be selected

Enter role name to filter items...

Selected Role

You haven't selected any role.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

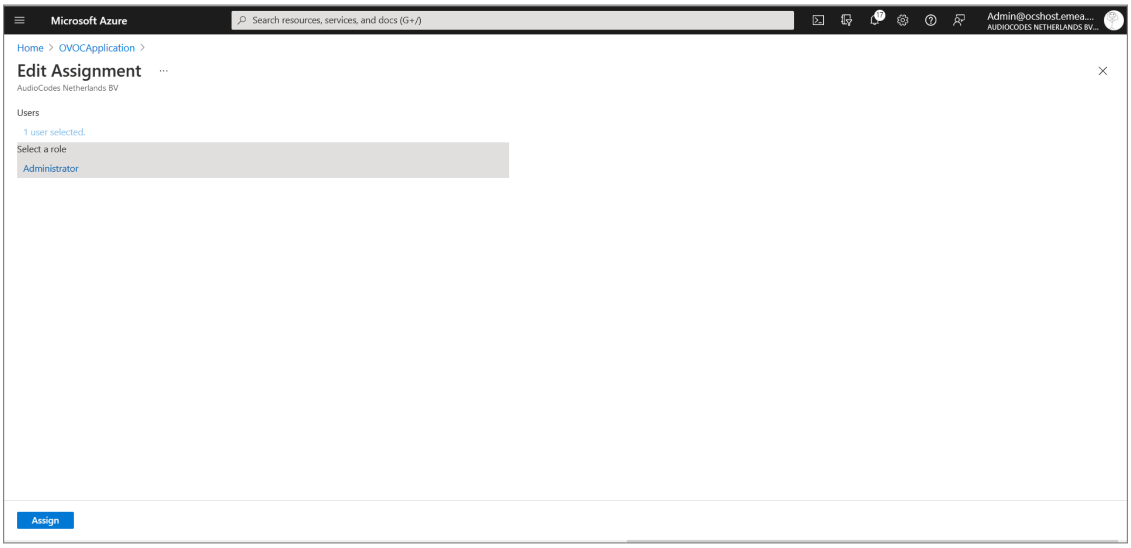
First 200 shown, to search users & groups, enter a display name.

Display Name	Object Type	Role assigned
Ron2	User	Operator

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 10-88: Add Assignment


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV...
Home > OVOCApplication >

Edit Assignment

AudioCodes Netherlands BV

Users

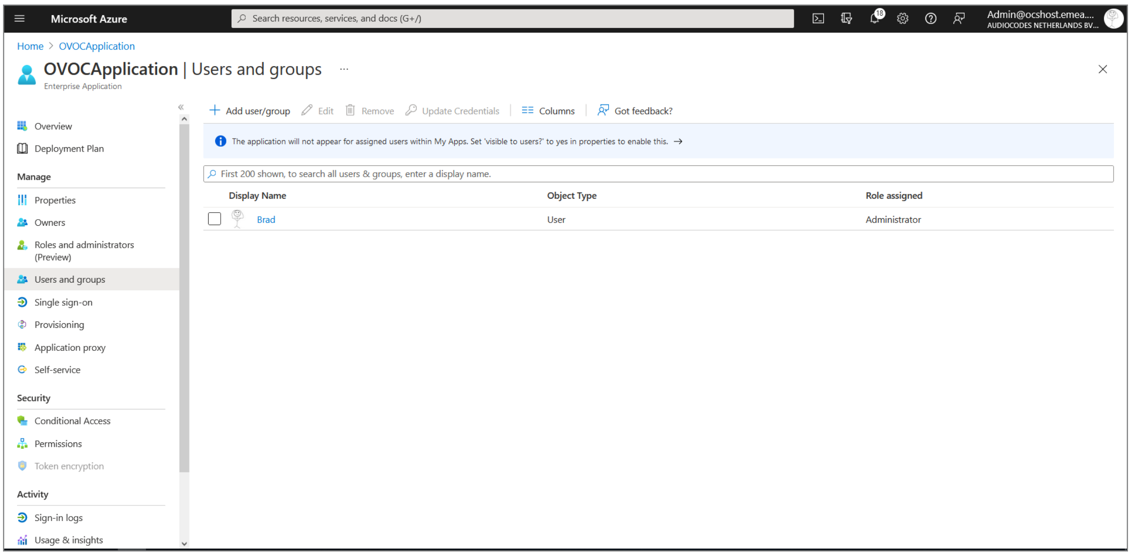
1 user selected.

Select a role

Administrator

4. Confirm by clicking **Assign.**

Figure 10-89: Existing User Defined with "Admin" Role



The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

First 200 shown, to search all users & groups, enter a display name.

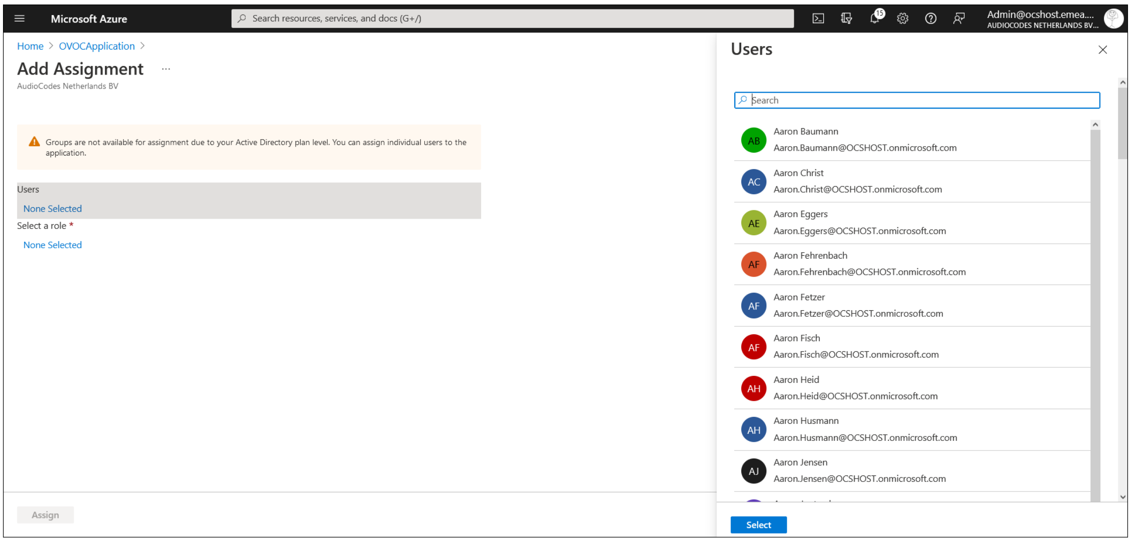
Display Name	Object Type	Role assigned
Brad	User	Administrator

➢ 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**.

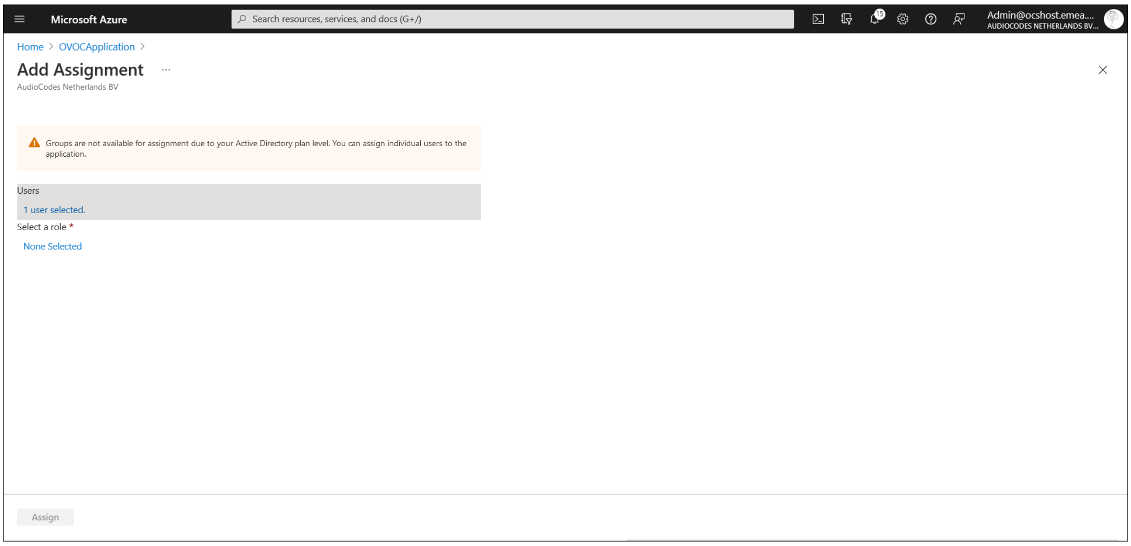
Figure 10-90: Choose User



Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

AB	Aaron Baumann Aaron.Baumann@OCSHOST.onmicrosoft.com
AC	Aaron Christ Aaron.Christ@OCSHOST.onmicrosoft.com
AE	Aaron Eggers Aaron.Eggers@OCSHOST.onmicrosoft.com
AF	Aaron Fehrenbach Aaron.Fehrenbach@OCSHOST.onmicrosoft.com
AF	Aaron Fetzer Aaron.Fetzer@OCSHOST.onmicrosoft.com
AF	Aaron Fisch Aaron.Fisch@OCSHOST.onmicrosoft.com
AH	Aaron Heid Aaron.Heid@OCSHOST.onmicrosoft.com
AH	Aaron Husmann Aaron.Husmann@OCSHOST.onmicrosoft.com
AJ	Aaron Jensen Aaron.Jensen@OCSHOST.onmicrosoft.com

Figure 10-91: User Selected



Microsoft Azure

Search resources, services, and docs (G+/)

Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV...

Home > OVOCApplication >

Add Assignment

AudioCodes Netherlands BV

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

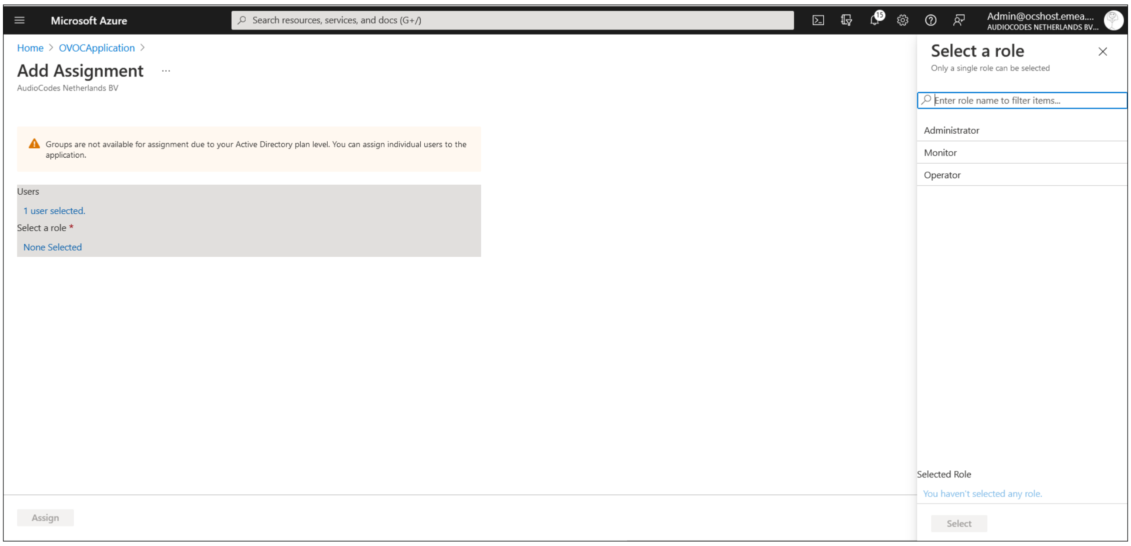
1 user selected.

Select a role *

None Selected

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

Figure 10-92: Select a Role



Microsoft Azure

Search resources, services, and docs (G+/)

Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV...

Home > OVOCApplication >

Add Assignment

AudioCodes Netherlands BV

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

1 user selected.

Select a role *

None Selected

Select a role

Only a single role can be selected

Enter role name to filter items...

Administrator

Monitor

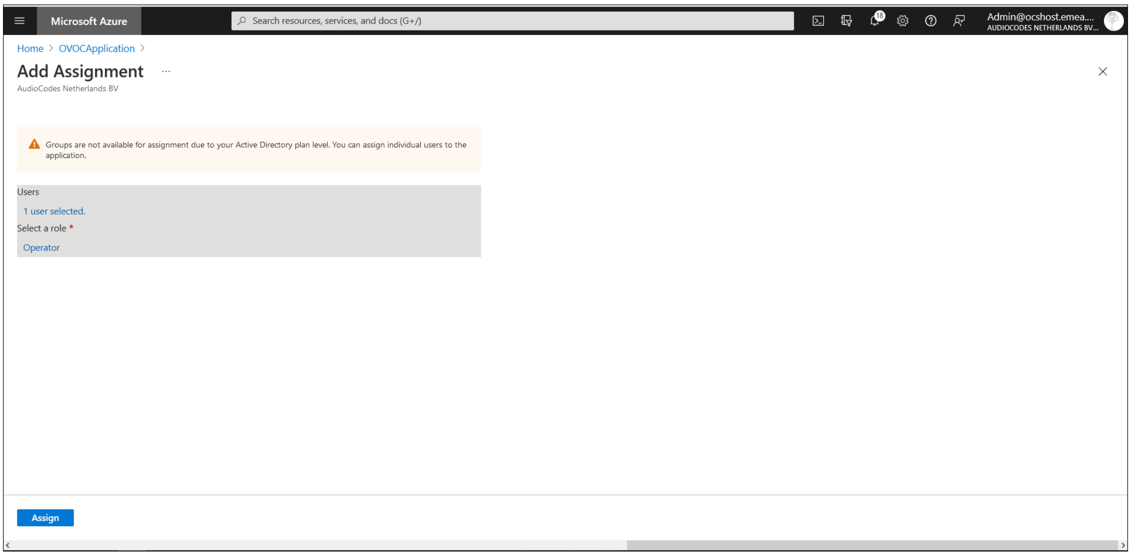
Operator

Selected Role

You haven't selected any role.

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

Figure 10-93: Assign Role to New User


Microsoft Azure
Search resources, services, and docs (G+/)
Admin@ocshost.emea....
AUDIOCODES NETHERLANDS BV...
Home > OVOCApplication >
Assign

Add Assignment

AudioCodes Netherlands BV

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

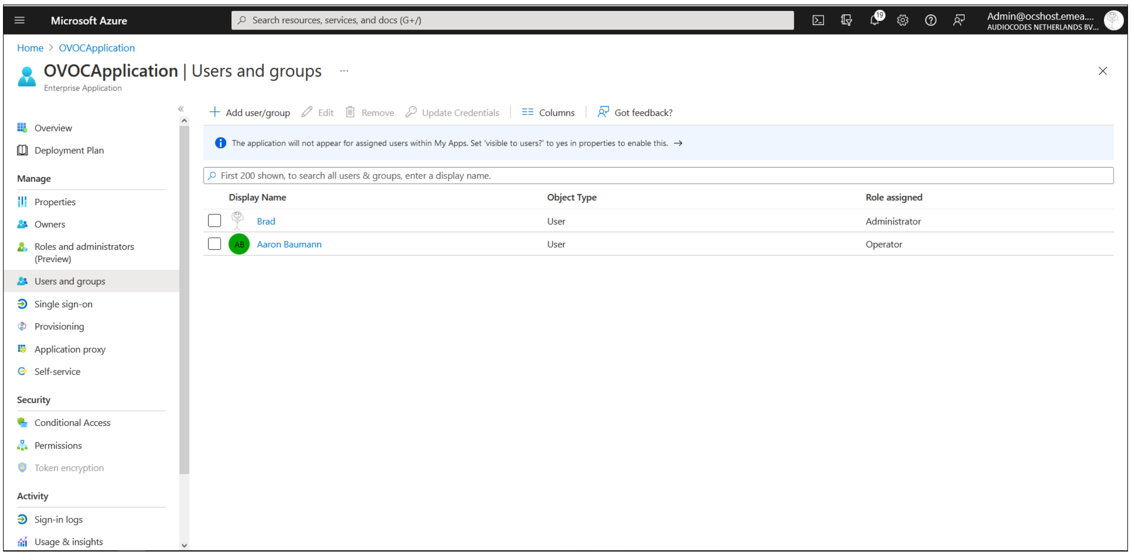
1 user selected.

Select a role *

Operator

5. Confirm by clicking **Assign**.

Figure 10-94: New User Assigned "Operator" Role



OVOCApplication | Users and groups

Enterprise Application

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
Brad	User	Administrator
AB Aaron Baumann	User	Operator

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 106.
- If upgrading from a Single Tenant setup proceed to Configuring OVOC Web Azure Settings - Multitenant Upgrade on page 121

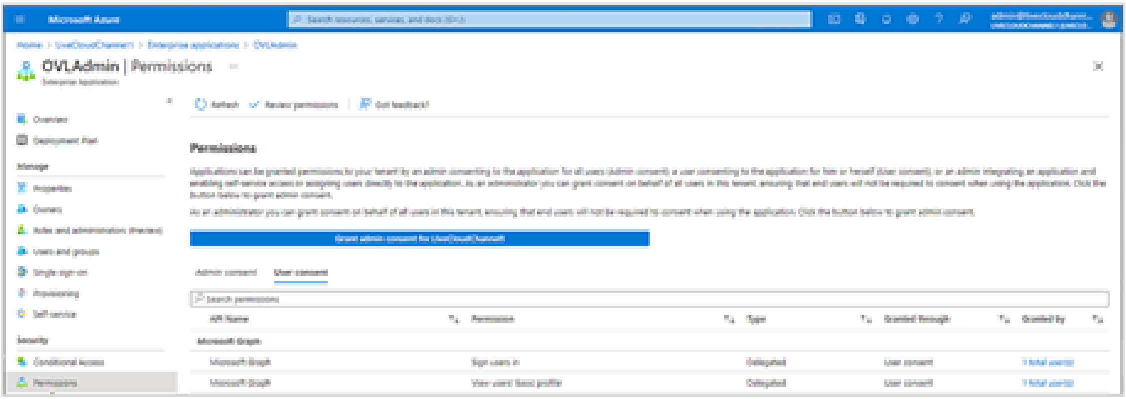
Troubleshooting - Granting Admin Consent

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 10-95: Permissions



OVLAdmin | Permissions

Enterprise Application

Permissions

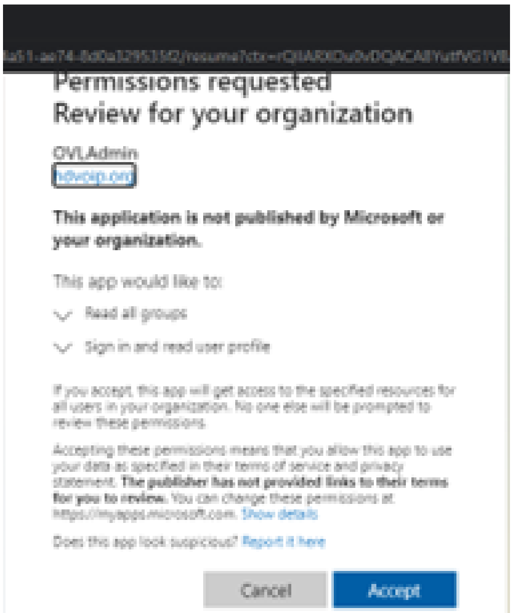
Applications can be granted permissions to your tenant by an admin consenting to the application for all users (Admin consent), a user consenting to the application for him or herself (User consent), or an admin integrating an application and enabling self-service access or assigning users directly to the application. As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

API Name	Permission	Type	Granted through	Granted by
Microsoft Graph				
Microsoft Graph	Sign users in	Delegated	User consent	1 total user(s)
Microsoft Graph	View users' basic profile	Delegated	User consent	1 total user(s)

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

Figure 10-96: Permissions Requested



la51-ae74-8d0a3295350/resume?ctx=rQIIARXOu0vDQACAllYutfVG1VB

Permissions requested

Review for your organization

OVLAdmin
hdvoip.org

This application is not published by Microsoft or your organization.

This app would like to:

- Read all groups
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

5. Click **Accept**.

11 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 141
- Define OVOC FQDN and Load Certificate on page 144

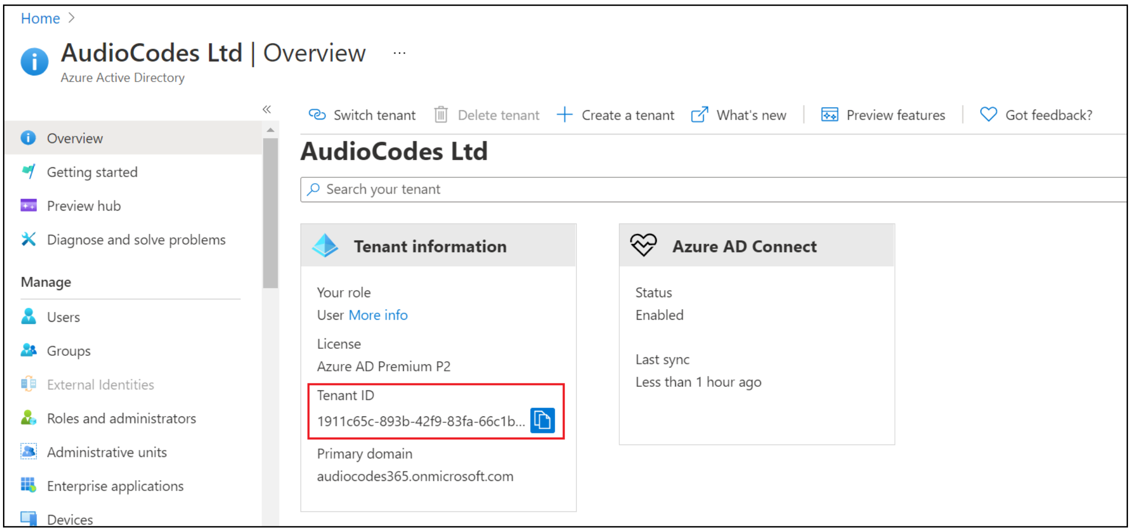
Register Microsoft Teams Application

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 11-1: Tenant ID



AudioCodes Ltd

Your role
User More info

License
Azure AD Premium P2

Tenant ID
1911c65c-893b-42f9-83fa-66c1b...

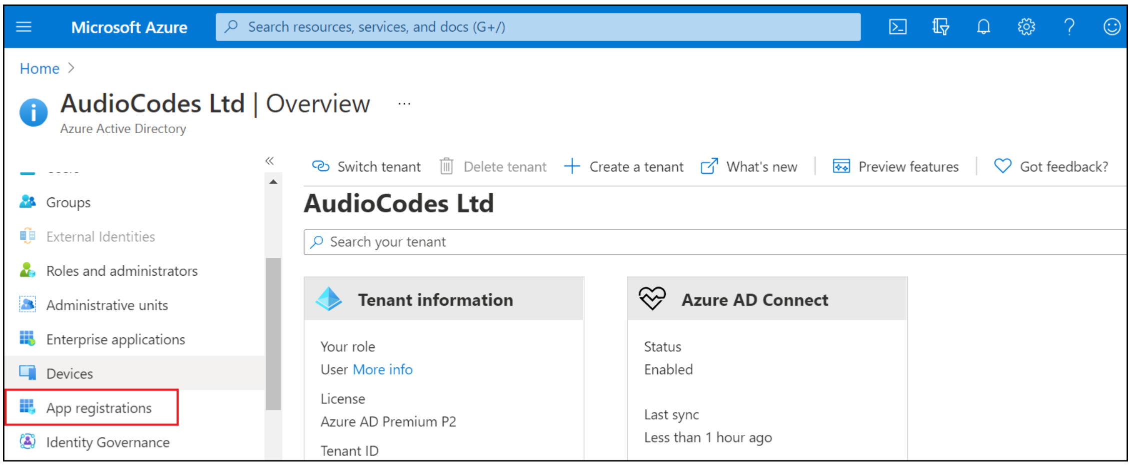
Primary domain
audiocodes365.onmicrosoft.com

Status
Enabled

Last sync
Less than 1 hour ago

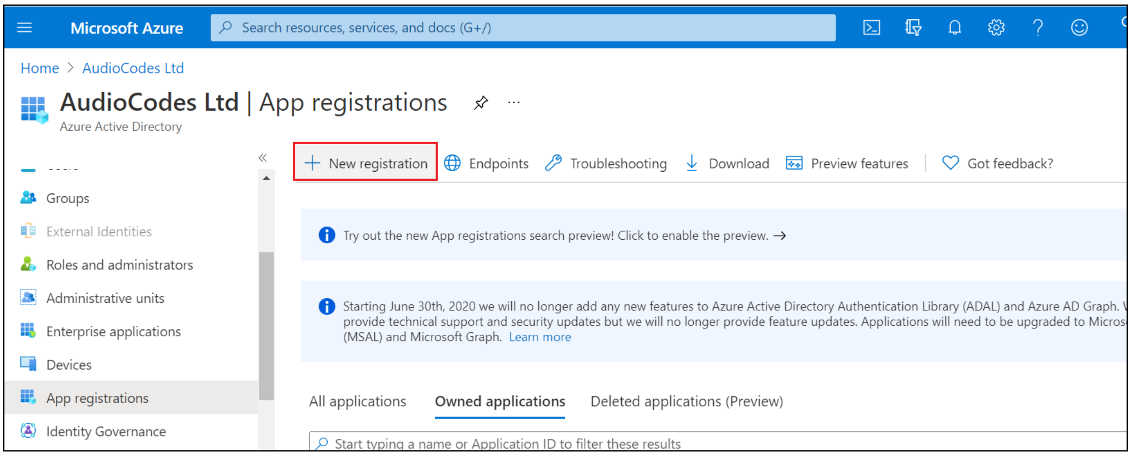
2. In the Navigation pane, select **App registrations.**

Figure 11-2: App Registrations



3. Click **New registration.**

Figure 11-3: New registration

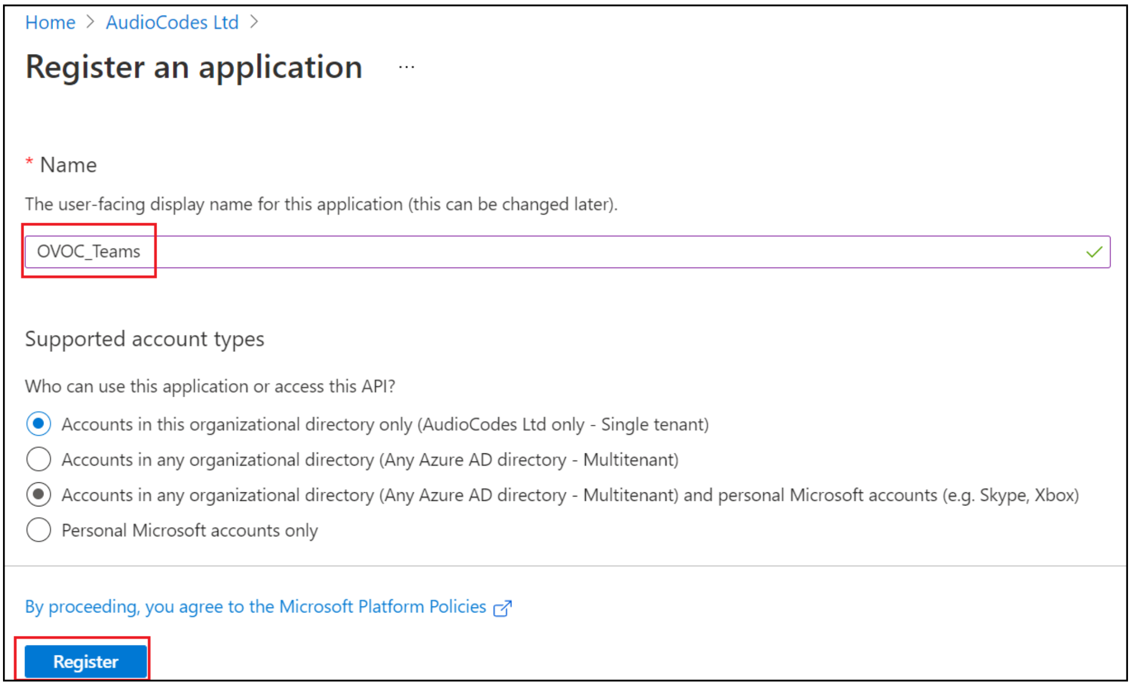


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. W provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Micros (MSAL) and Microsoft Graph. Learn more

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

Figure 11-4: Name the application



Home > AudioCodes Ltd >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

OVOC_Teams ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Ltd only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

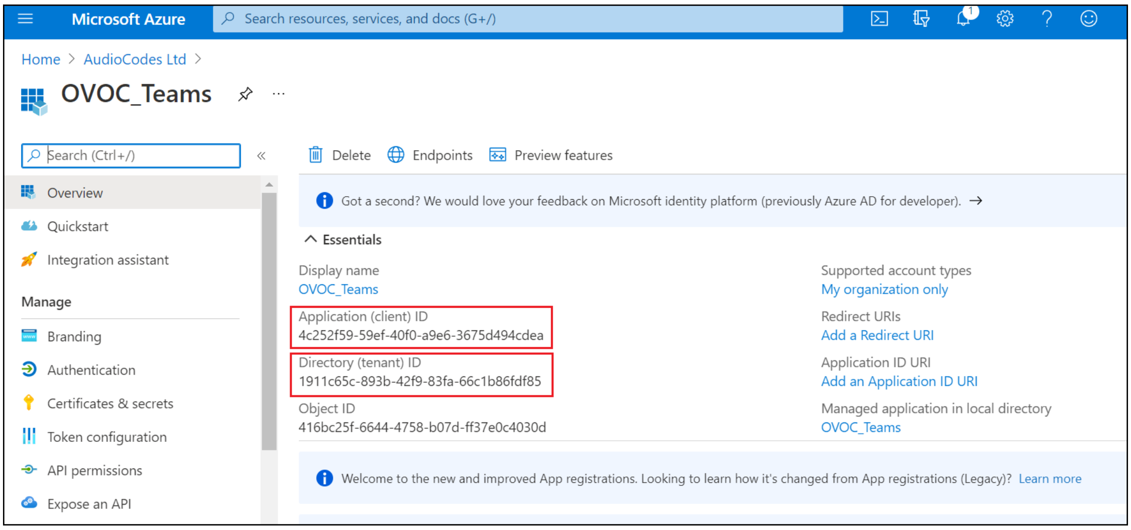
● Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

By proceeding, you agree to the Microsoft Platform Policies

Register

Figure 11-5: Successful Registration



OVOC_Teams

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

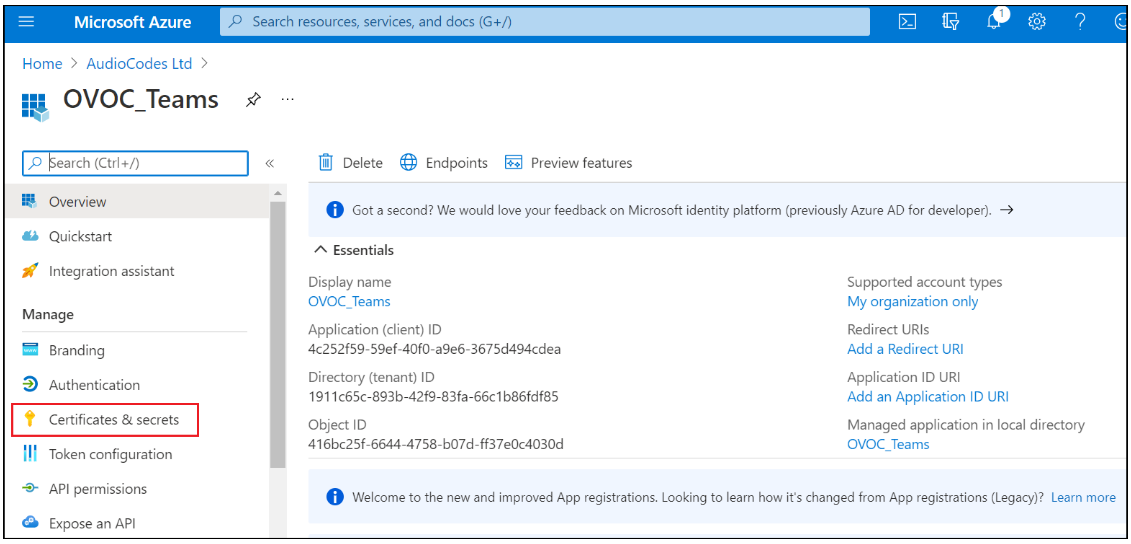
Essentials

Display name OVOC_Teams	Supported account types My organization only
Application (client) ID 4c252f59-59ef-40f0-a9e6-3675d494cdea	Redirect URIs Add a Redirect URI
Directory (tenant) ID 1911c65c-893b-42f9-83fa-66c1b86fdf85	Application ID URI Add an Application ID URI
Object ID 416bc25f-6644-4758-b07d-ff37e0c4030d	Managed application in local directory OVOC_Teams

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

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

Figure 11-6: Certificate & Secrets



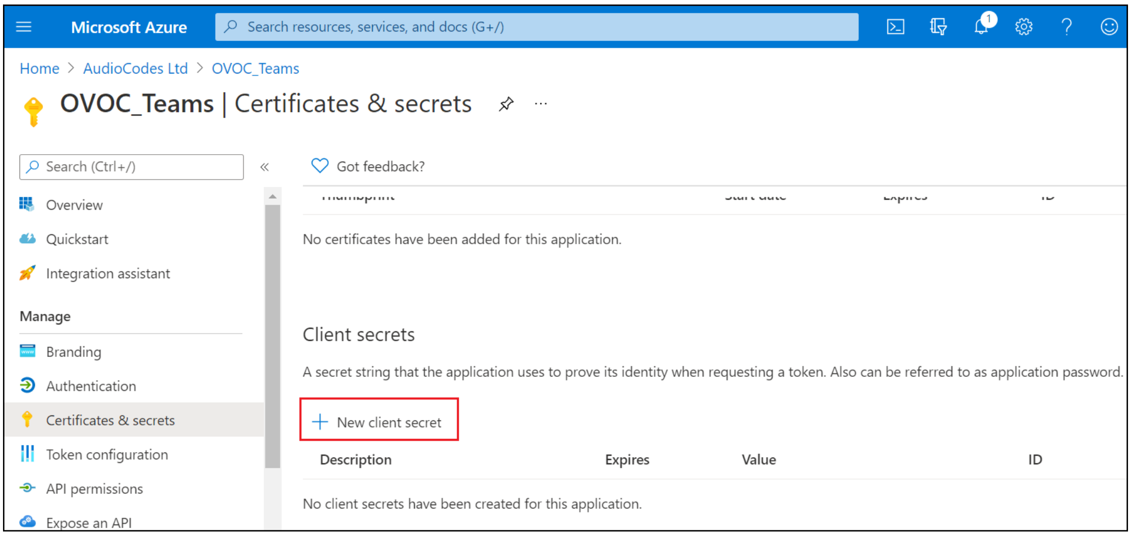
Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name OVOC_Teams	Supported account types My organization only
Application (client) ID 4c252f59-59ef-40f0-a9e6-3675d494cdea	Redirect URIs Add a Redirect URI
Directory (tenant) ID 1911c65c-893b-42f9-83fa-66c1b86fdf85	Application ID URI Add an Application ID URI
Object ID 416bc25f-6644-4758-b07d-ff37e0c4030d	Managed application in local directory OVOC_Teams

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

6. Click **New client secret**.

Figure 11-7: New Client Secret



No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

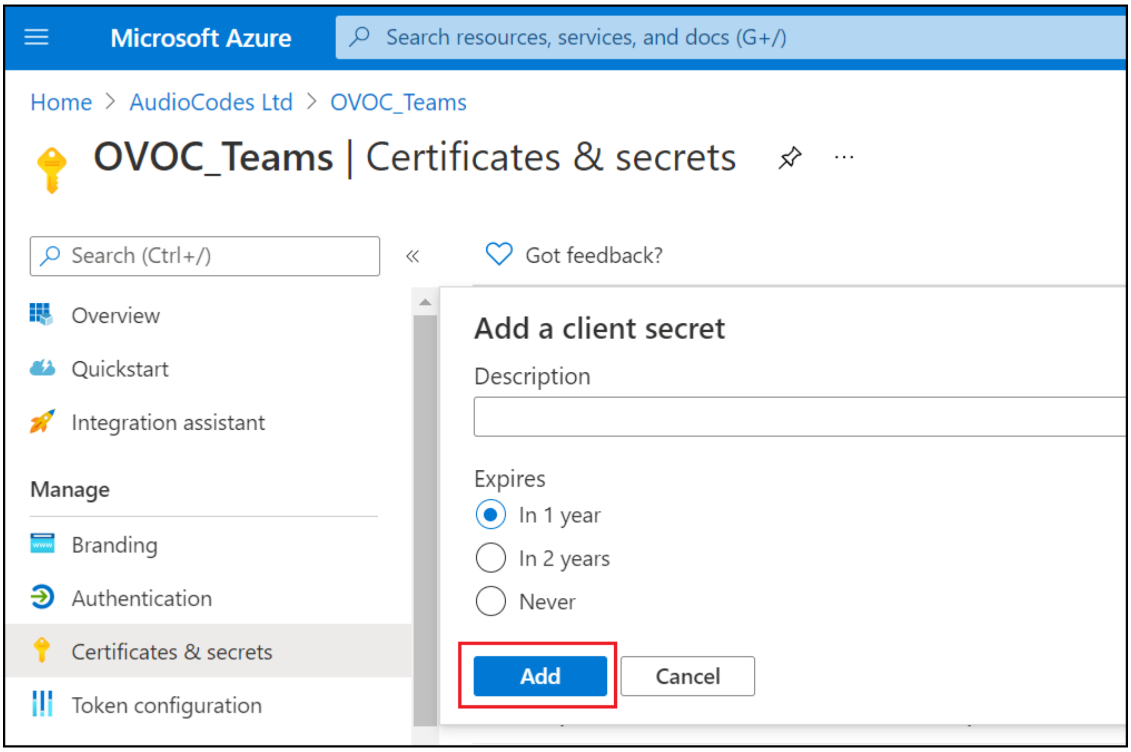
Description	Expires	Value	ID

No client secrets have been created for this application.

7. Click **Add**.

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

Figure 11-8: Add a client secret



Add a client secret

Description

Expires

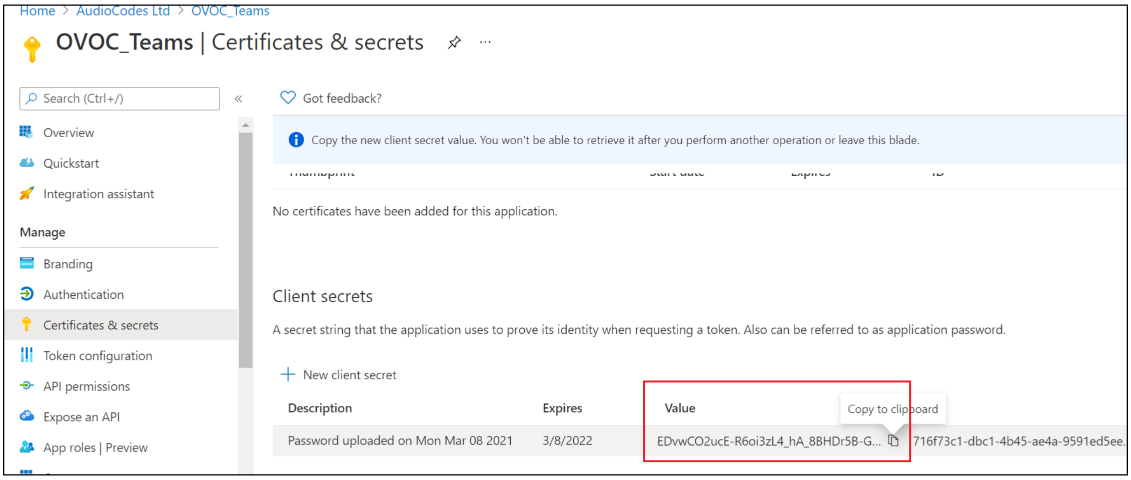
● In 1 year

○ In 2 years

○ Never

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 11-9: Added Certificates & Secrets



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	
Password uploaded on Mon Mar 08 2021	3/8/2022	EDvwCO2ucE-R6oi3zL4_hA_8BHDr5B-G...	716f73c1-dbc1-4b45-ae4a-9591ed5ee.

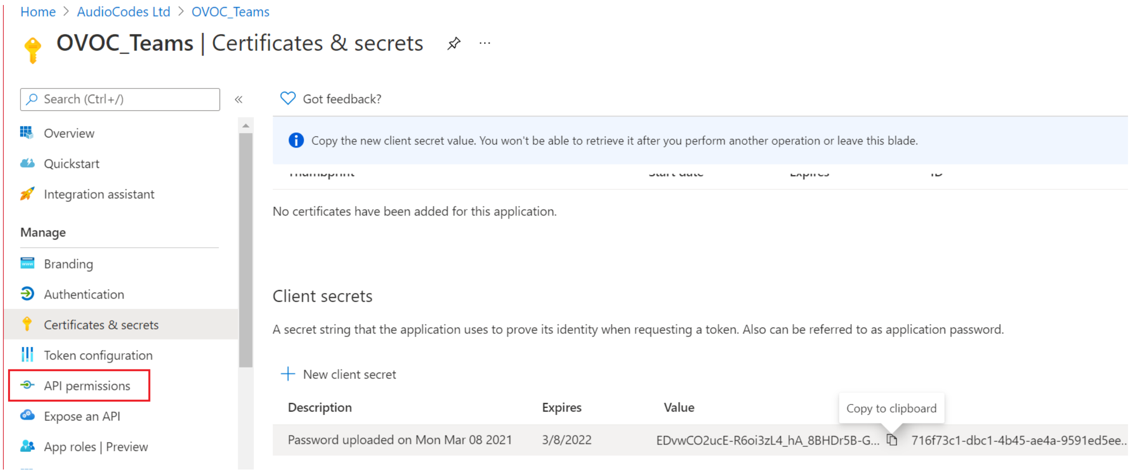
Configure Microsoft Graph API Permissions

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 11-10: API Permissions



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

No certificates have been added for this application.

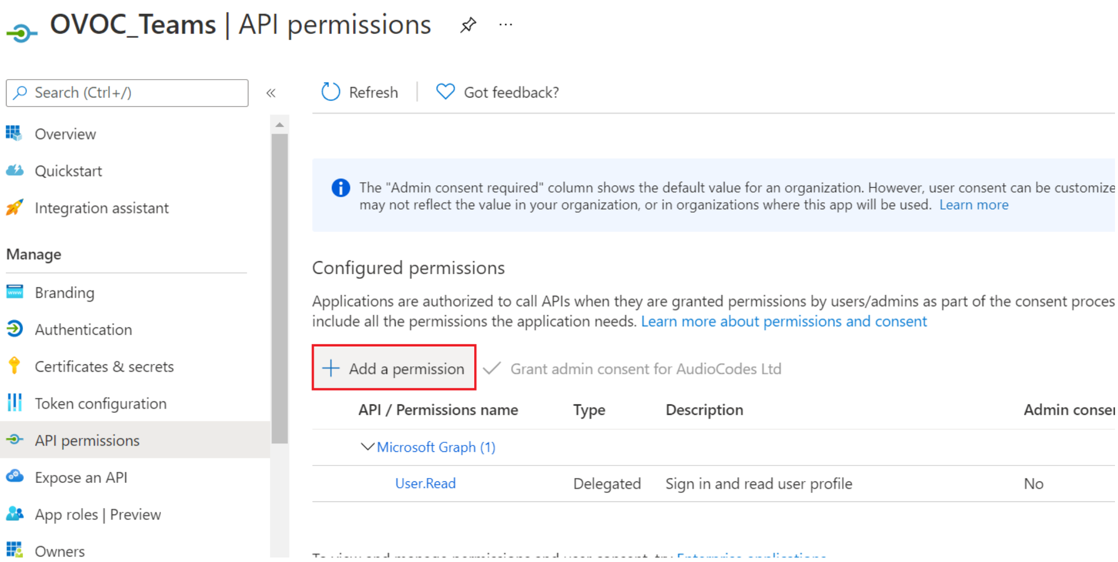
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	
Password uploaded on Mon Mar 08 2021	3/8/2022	EDvwCO2ucE-R6oi3zL4_hA_8BHDr5B-G...	716f73c1-dbc1-4b45-ae4a-9591ed5ee..

2. Click **Add a permission.**

Figure 11-11: Add a permission



The "Admin consent required" column shows the default value for an organization. However, user consent can be customize may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent proces include all the permissions the application needs. Learn more about permissions and consent

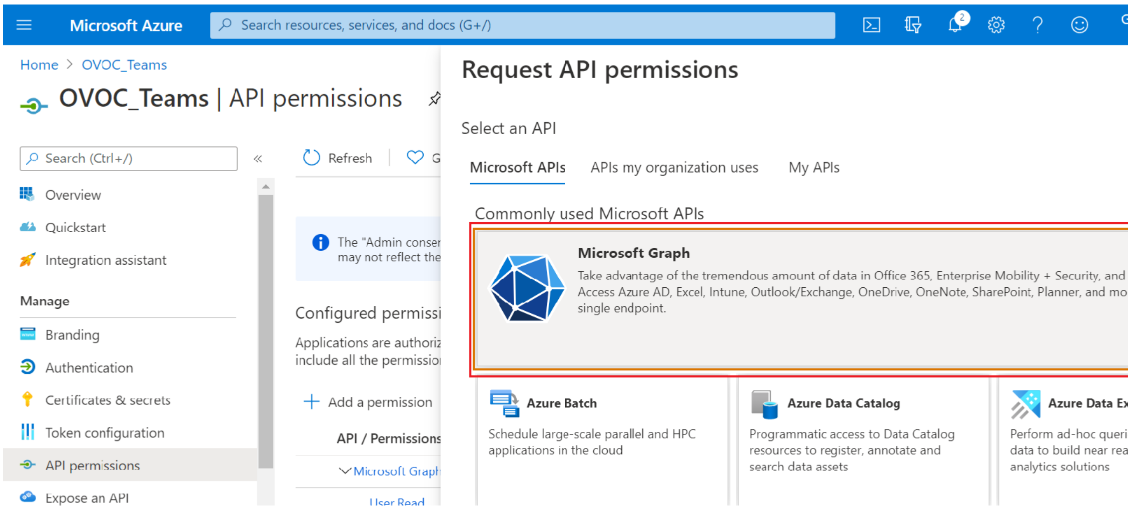
API / Permissions name	Type	Description	Admin consei
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

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 11-12: Request API Permissions



The "Admin conser may not reflect the

Applications are authoriz include all the permissio

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and mo single endpoint.

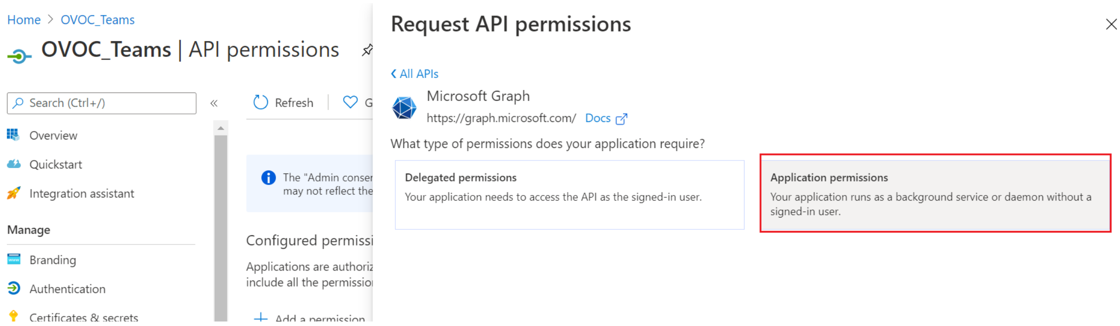
Schedule large-scale parallel and HPC applications in the cloud

Programmatic access to Data Catalog resources to register, annotate and search data assets

Perform ad-hoc queri data to build near rea analytics solutions

5. Select **Application permissions**.

Figure 11-13: Application permissions



The "Admin conser may not reflect the

Applications are authoriz include all the permissio

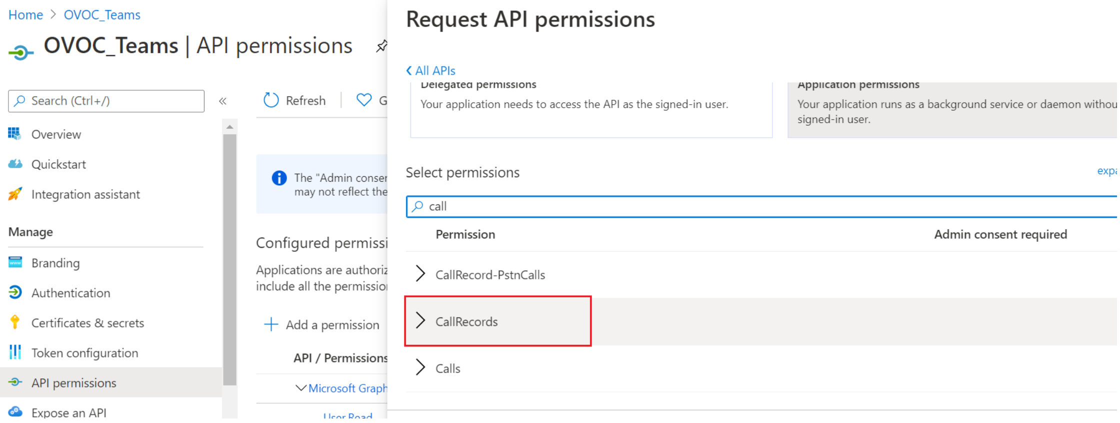
What type of permissions does your application require?

Your application needs to access the API as the signed-in user.

Your application runs as a background service or daemon without a signed-in user.

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

Figure 11-14: Call Records



The "Admin conser may not reflect the

Applications are authoriz include all the permissio

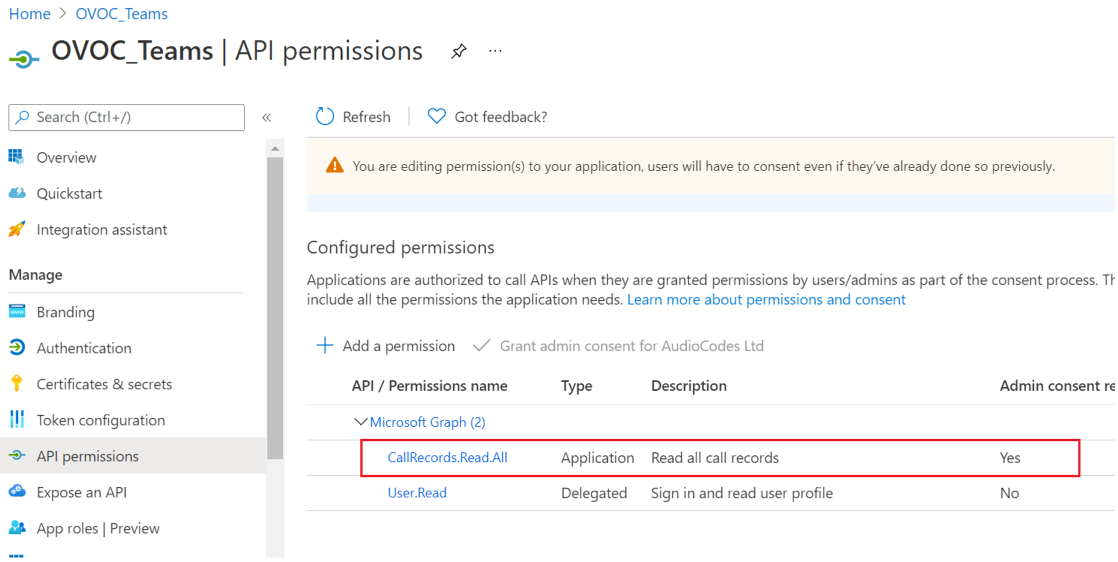
Your application needs to access the API as the signed-in user.

Your application runs as a background service or daemon withou signed-in user.

call

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

Figure 11-15: API Permissions



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

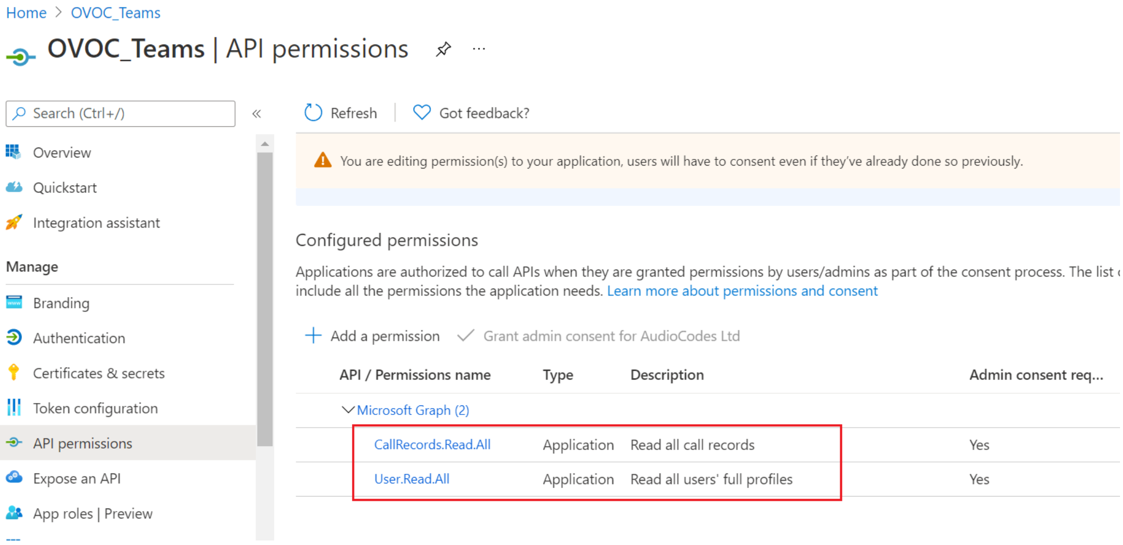
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. Th include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent re
Microsoft Graph (2)			
CallRecords.Read.All	Application	Read all call records	Yes
User.Read	Delegated	Sign in and read user profile	No

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

Figure 11-16: User Read Permissions



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (2)			
CallRecords.Read.All	Application	Read all call records	Yes
User.Read.All	Application	Read all users' full profiles	Yes

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.

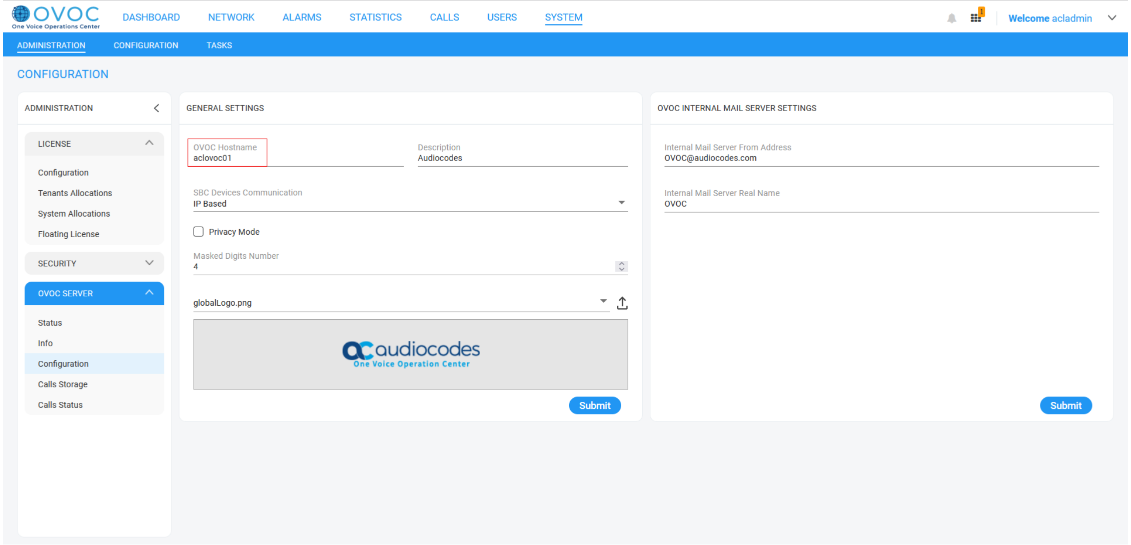
➢ **Do the following:**

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 11-17: OVOC Server Configuration



OVOC Hostname: aclovoc01

Description: Audiocodes

SBC Devices Communication: IP Based

□ Privacy Mode

Masked Digits Number: 4

globalLogo.png

Internal Mail Server From Address: OVOC@audiocodes.com

Internal Mail Server Real Name: OVOC

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 265

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

12 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 151

The table below describes the different connection scenarios.

Table 12-1: 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 149

Configure OVOC Server with NAT IP Address per Interface

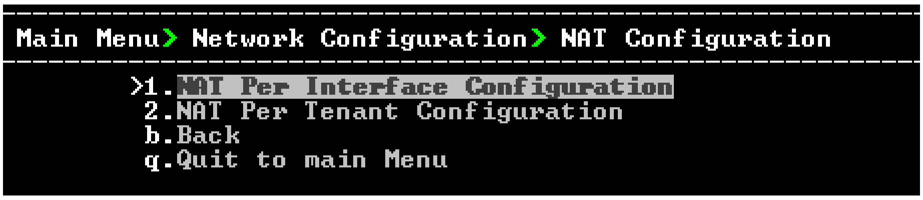
This option configures the OVOC server with a physical NAT interface for connecting to devices that are deployed behind a NAT in a remote Enterprise or Cloud network.

- 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 156 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.

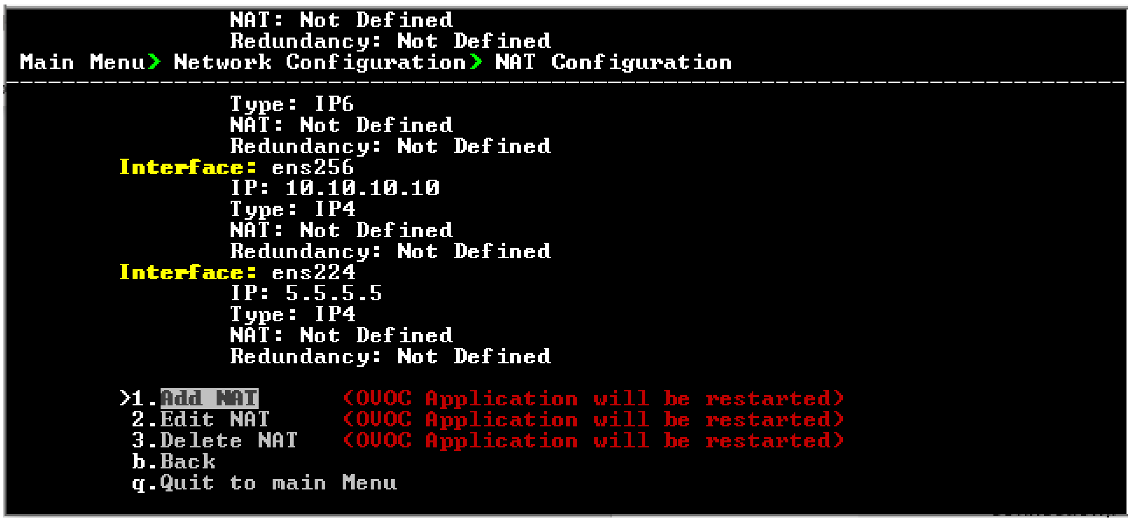
Figure 12-1: Configure NAT IP



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

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

Figure 12-2: NAT Per Interface Configuration

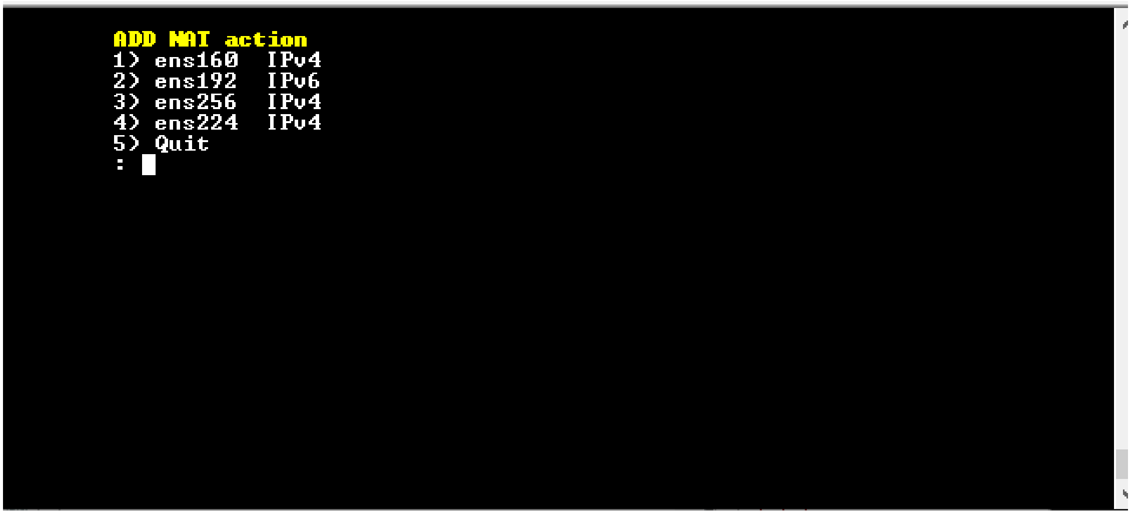


```
                NAT: Not Defined
                Redundancy: Not Defined
 Main Menu> Network Configuration> NAT Configuration
------------------------------------------------------------------------
                Type: IP6
                NAT: Not Defined
                Redundancy: Not Defined
        Interface: ens256
                IP: 10.10.10.10
                Type: IP4
                NAT: Not Defined
                Redundancy: Not Defined
        Interface: ens224
                IP: 5.5.5.5
                Type: IP4
                NAT: Not Defined
                Redundancy: Not Defined

        >1.Add NAT      <OVOC Application will be restarted>
         2.Edit NAT     <OVOC Application will be restarted>
         3.Delete NAT   <OVOC Application will be restarted>
         b.Back
         q.Quit to main Menu
```

➢ To add a NAT interface:

1. Choose option **1**.

Figure 12-3: Add NAT



```
ADD NAT action
1) ens160  IPv4
2) ens192  IPv6
3) ens256  IPv4
4) ens224  IPv4
5) Quit
:
```

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.

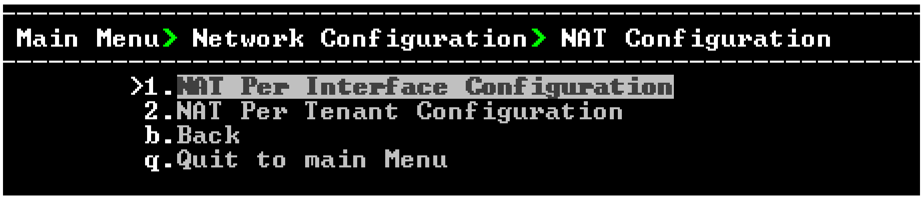
Configure OVOC Server with NAT IP per Tenant

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:

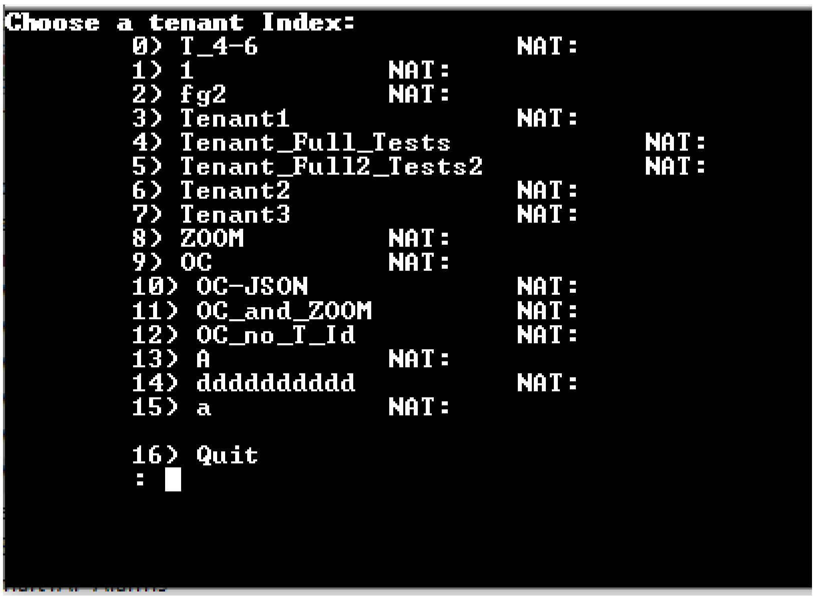
1. From the Network Configuration menu, choose **NAT**, and then press Enter.

Figure 12-4: NAT Configuration per Tenant



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

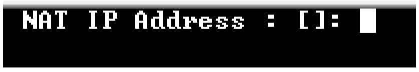
2. Choose option **NAT Per Tenant Configuration**.



```
Choose a tenant Index:
        0) T_4-6                        NAT:
        1) 1                    NAT:
        2) fg2                  NAT:
        3) Tenant1                      NAT:
        4) Tenant_Full_Tests                    NAT:
        5) Tenant_Full2_Tests2                  NAT:
        6) Tenant2                      NAT:
        7) Tenant3                      NAT:
        8) ZOOM                 NAT:
        9) OC                   NAT:
        10) OC-JSON                     NAT:
        11) OC_and_ZOOM                 NAT:
        12) OC_no_T_Id                  NAT:
        13) A                   NAT:
        14) dddddddddd                  NAT:
        15) a                   NAT:

        16) Quit
        :
```

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

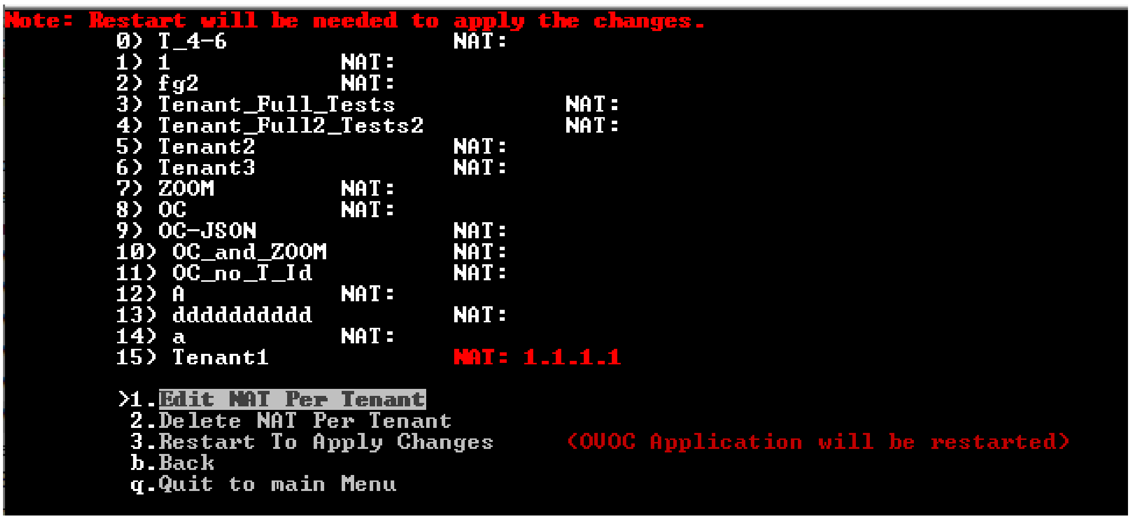
Figure 12-5: NAT IP Address



```
NAT IP Address : []:
```

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

Figure 12-6: Configure WAN



```
Note: Restart will be needed to apply the changes.
        0) T_4-6                        NAT:
        1) 1                NAT:
        2) fg2              NAT:
        3) Tenant_Full_Tests                    NAT:
        4) Tenant_Full2_Tests2                  NAT:
        5) Tenant2                      NAT:
        6) Tenant3                      NAT:
        7) ZOOM             NAT:
        8) OC               NAT:
        9) OC-JSON                      NAT:
        10) OC_and_ZOOM                 NAT:
        11) OC_no_T_Id                  NAT:
        12) A               NAT:
        13) dddddddddd                  NAT:
        14) a               NAT:
        15) Tenant1                     NAT: 1.1.1.1

        >1.Edit NAT Per Tenant
         2.Delete NAT Per Tenant
         3.Restart To Apply Changes        (OVOC Application will be restarted)
         b.Back
         q.Quit to main Menu
```

➢ **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

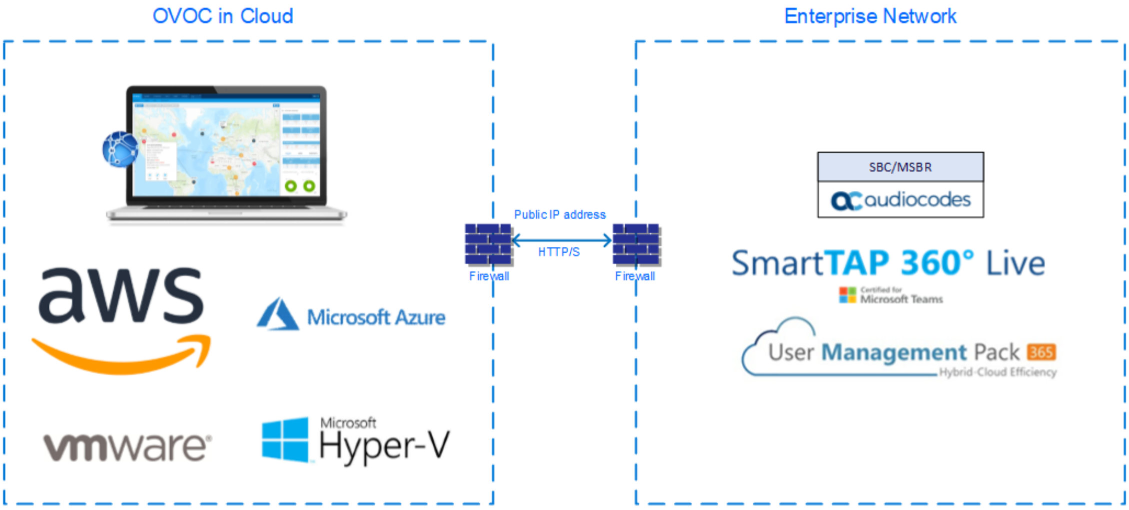
The Automatic Detection feature enables devices to be automatically connected to OVOC over SNMP. When devices are connected to the power supply in the enterprise network and/or are rebooted and initialized, they're automatically detected by the OVOC and added by default to the AutoDetection region. For 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 12-7: 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 156

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 155

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 290.

- 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)

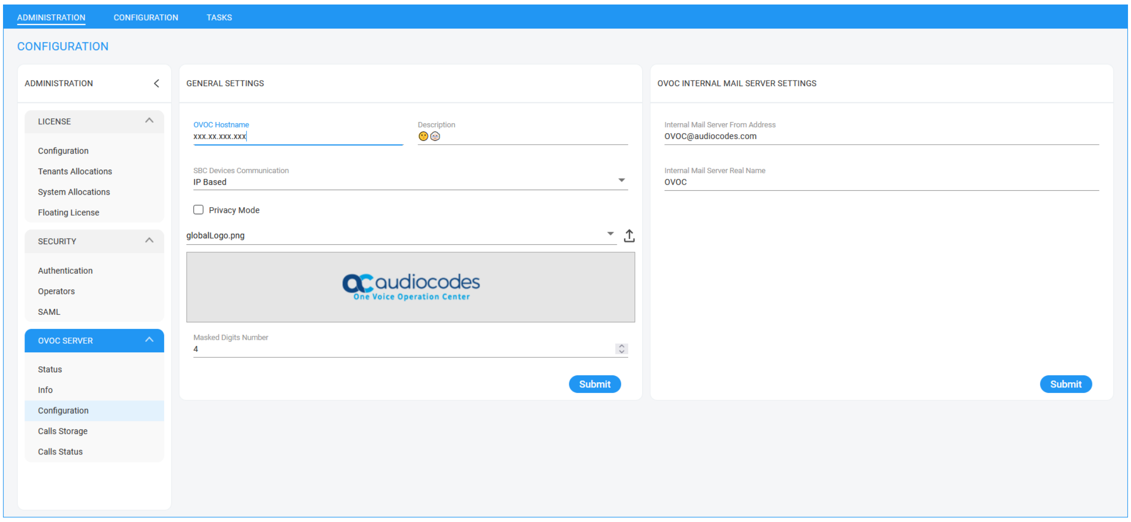
Configuring OVOC Web Interface for Tunnel Mode

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 12-8: SBC Devices Communication



OVOC Hostname: xxx.xx.xxx.xxx

Description:

SBC Devices Communication: IP Based

□ Privacy Mode

globalLogo.png

Masked Digits Number: 4

Internal Mail Server From Address: OVOC@audiocodes.com

Internal Mail Server Real Name: OVOC

2. Set parameter SBC Devices Communication to **IP Based**.

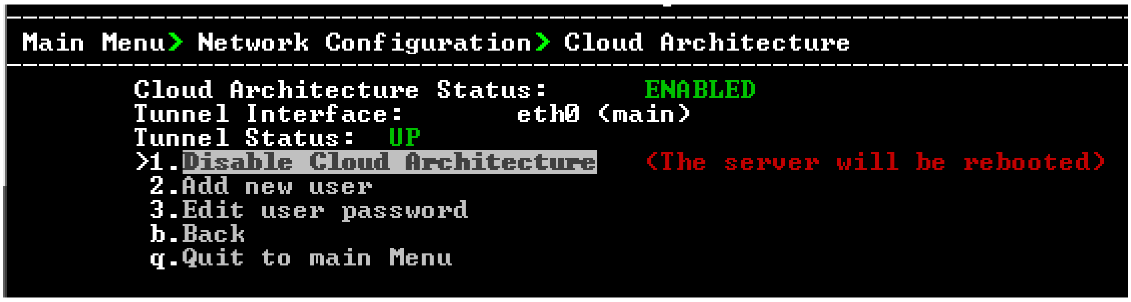
Configuring Cloud Architecture Mode (WebSocket Tunnel)

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 12-9: Cloud Architecture

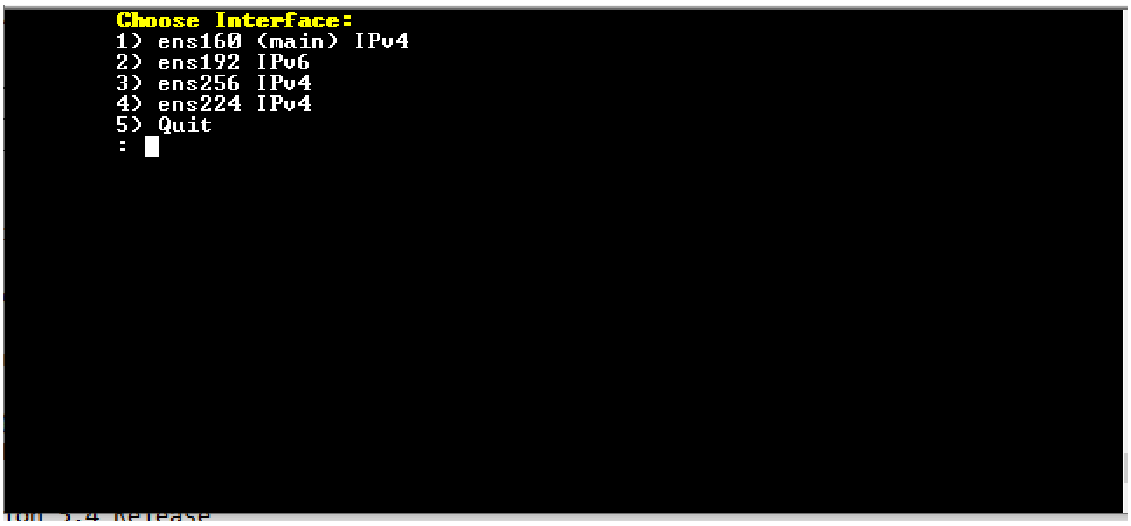


```
Main Menu> Network Configuration> Cloud Architecture
        Cloud Architecture Status:      ENABLED
        Tunnel Interface:        eth0 (main)
        Tunnel Status:  UP
        >1.Disable Cloud Architecture   (The server will be rebooted)
         2.Add new user
         3.Edit user password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

2. Select option **Enable Cloud Architecture**.

3. Select the IPv4 interface for which to enable this mode and then press Enter.

Figure 12-10: Choose IP Interface



```
Choose Interface:
1) ens160 (main) IPv4
2) ens192 IPv6
3) ens256 IPv4
4) ens224 IPv4
5) Quit
:
```

The OVOC server is restarted.

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

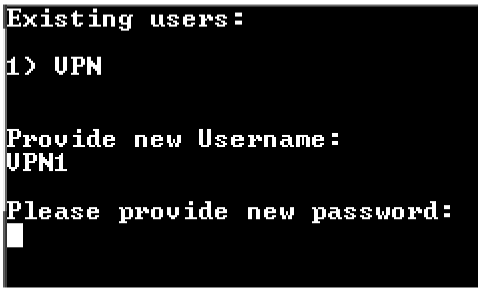
Add New Cloud Architecture Mode User

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 12-11: Create New Cloud Architecture User



```
Existing users:
1) VPN

Provide new Username:
VPN1

Please provide new password:
```

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

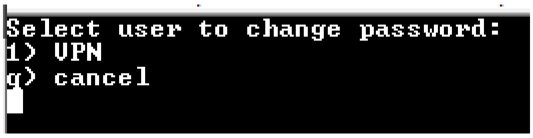
Change the Cloud Architecture Mode Service Password

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

➢ **To change the password:**

1. Select Option **3 Edit User Password**.

Figure 12-12: Edit User Password



```
Select user to change password:
1) VPN
q) cancel
```

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 232.

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

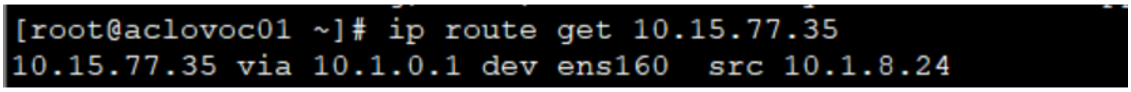
- NAT IP Interface (Configure OVOC Server with NAT IP Address per Interface on page 148
- WebSocket Tunnel (Cloud Architecture Mode) (Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 152)
- Public IP address
- Private IP address

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 152) 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 148), 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
```

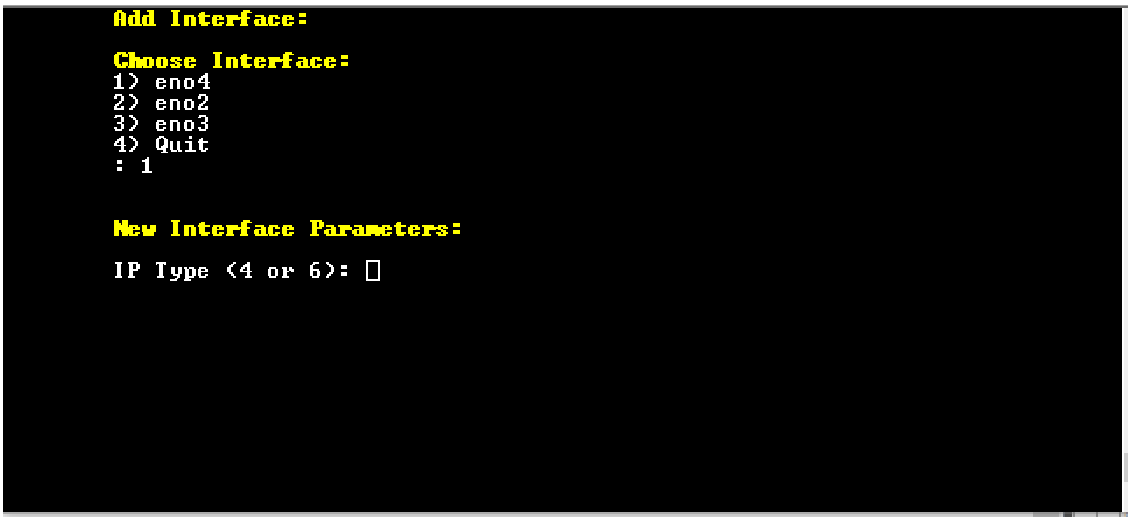
In the output it can be seen that ens160 is used for this IP address. Only one interface can be selected from all interfaces on the server to be use for routing this IP address.

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 148) 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.

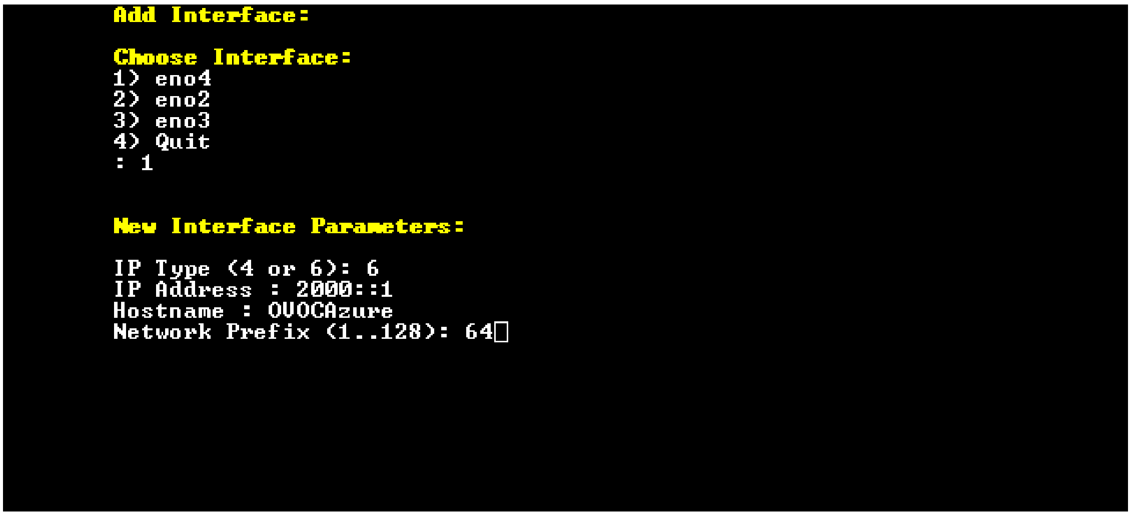
Figure 12-13: Add Interface



```
Add Interface:

Choose Interface:
1) eno4
2) eno2
3) eno3
4) Quit
: 1

New Interface Parameters:

IP Type (4 or 6): 
```

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

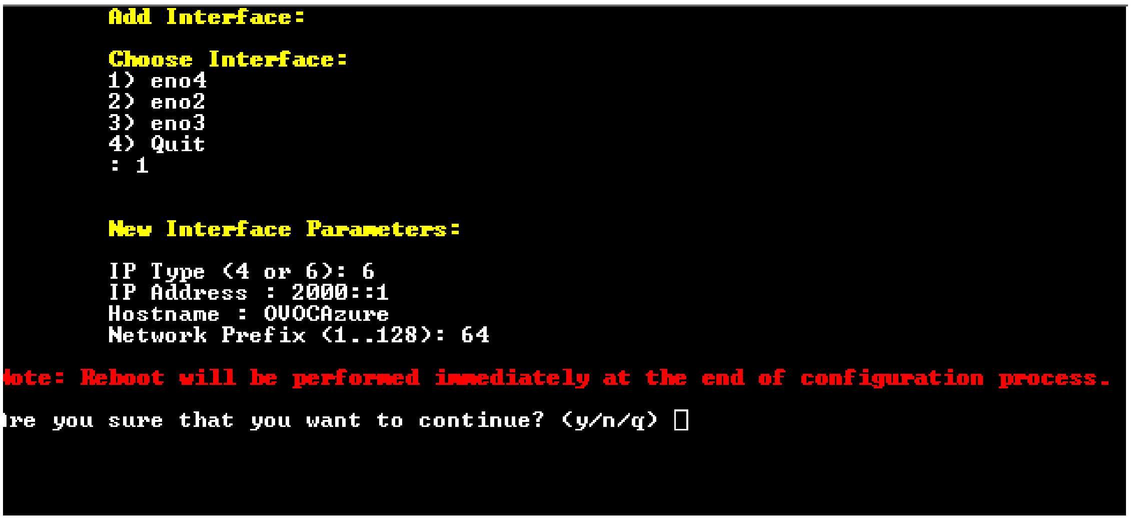
Figure 12-14: Add Interface



```
Add Interface:

Choose Interface:
1) eno4
2) eno2
3) eno3
4) Quit
: 1


New Interface Parameters:

IP Type (4 or 6): 6
IP Address : 2000::1
Hostname : OVOCAzure
Network Prefix (1..128): 64
```

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

Figure 12-15: Confirm Update



```
        Add Interface:

        Choose Interface:
        1) eno4
        2) eno2
        3) eno3
        4) Quit
        : 1


        New Interface Parameters:

        IP Type (4 or 6): 6
        IP Address : 2000::1
        Hostname : OVOCAzure
        Network Prefix (1..128): 64
lote: Reboot will be performed immediately at the end of configuration process.

lre you sure that you want to continue? (y/n/q)
```

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:

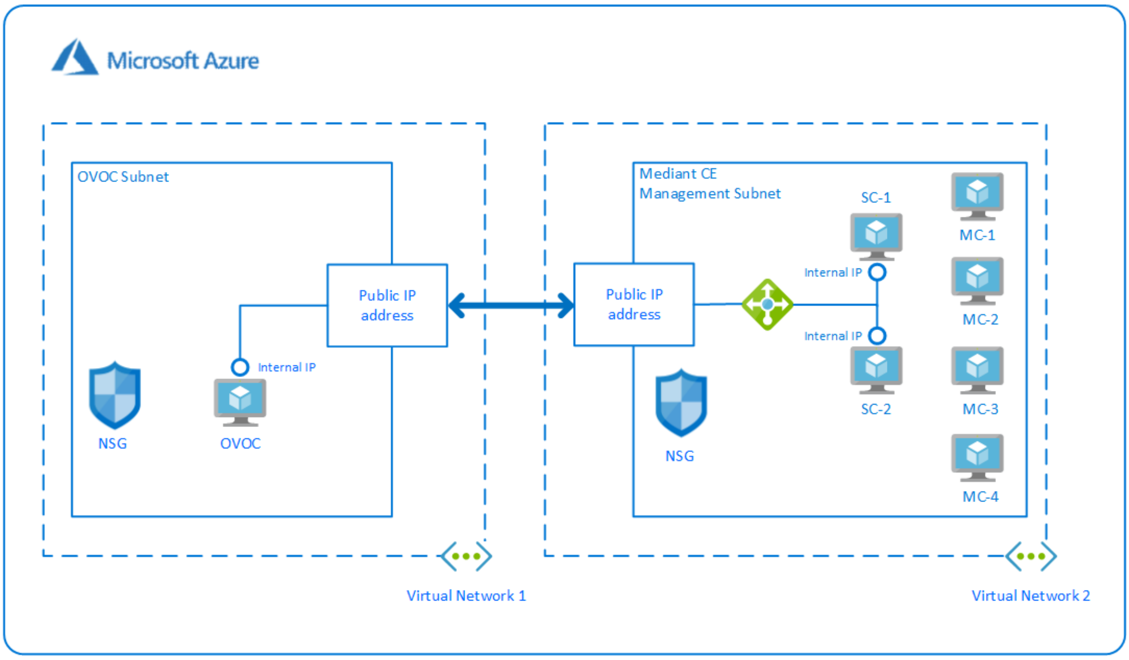
- Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on the next page
- Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address on page 162

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 148). 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 12-16: 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 196).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 257)
   - root OS user (see OS Users Passwords on page 257)

⚠ 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 213).
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 148). 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 240).

⚠ 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

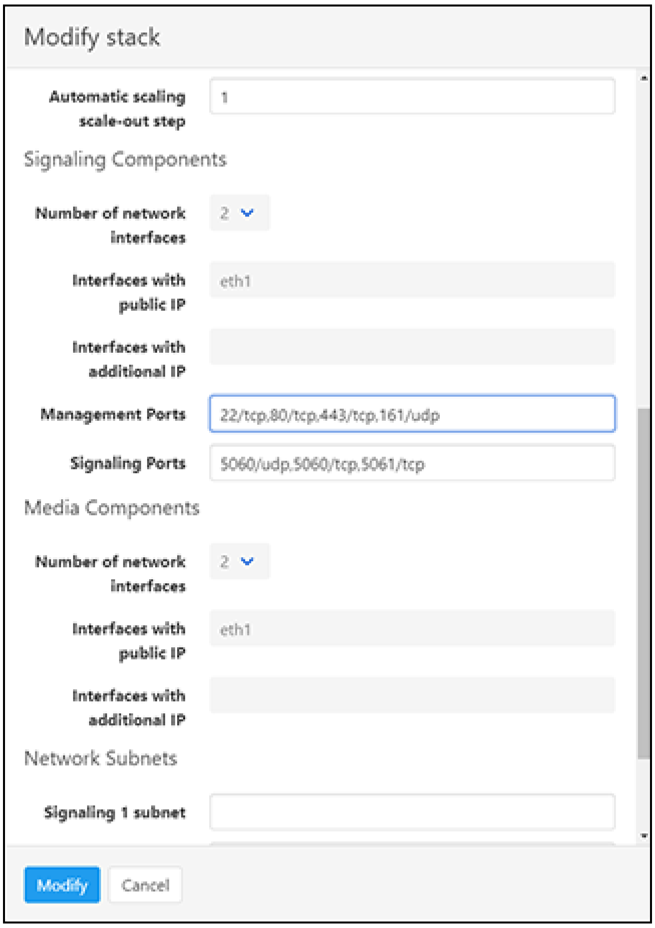
Configuring Mediant CE SNMP Public IP Connection using Stack Manager

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 12-17: Modify Stack



Modify stack

Automatic scaling scale-out step: 1

Signaling Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Management Ports: 22/tcp,80/tcp,443/tcp,161/udp

Signaling Ports: 5060/udp,5060/tcp,5061/tcp

Media Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Network Subnets

Signaling 1 subnet:

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>
```

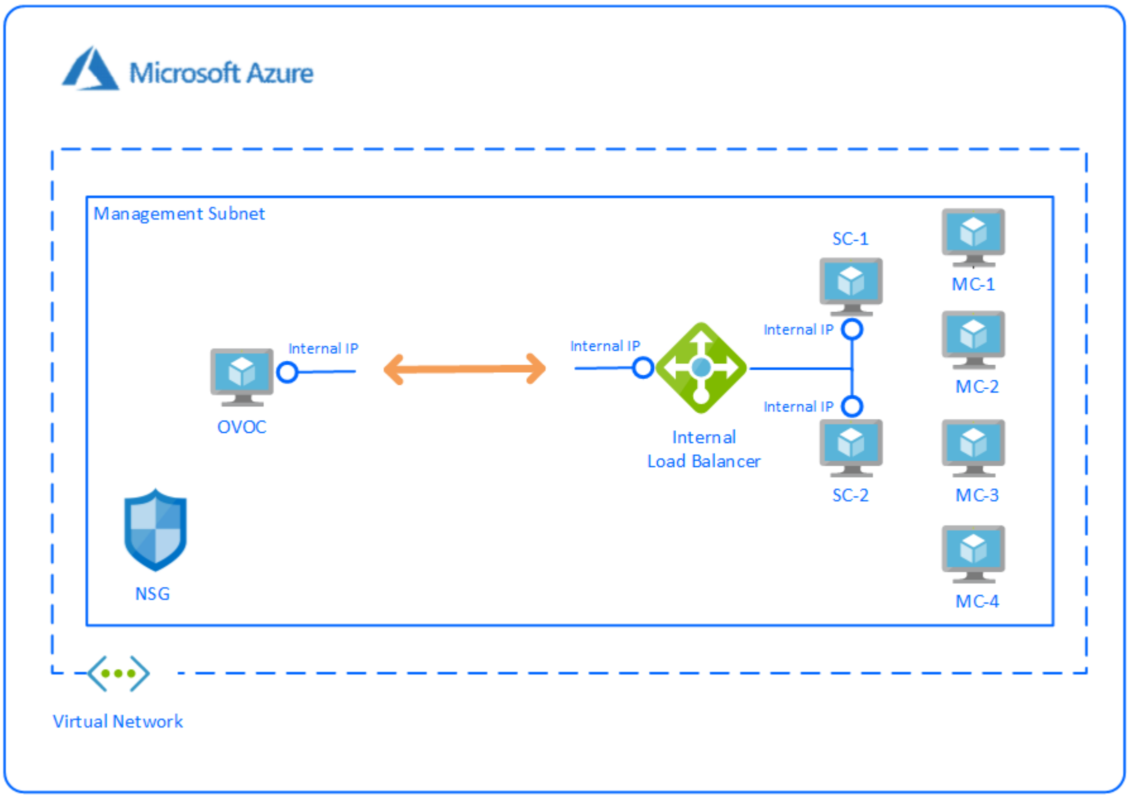
11. Reset the device for your settings to take effect (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

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 12-18: 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 196).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 257)

- root OS user (see OS Users Passwords on page 257)

> ⚠ 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 213).

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 225). 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 240).

> ⚠ 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:**

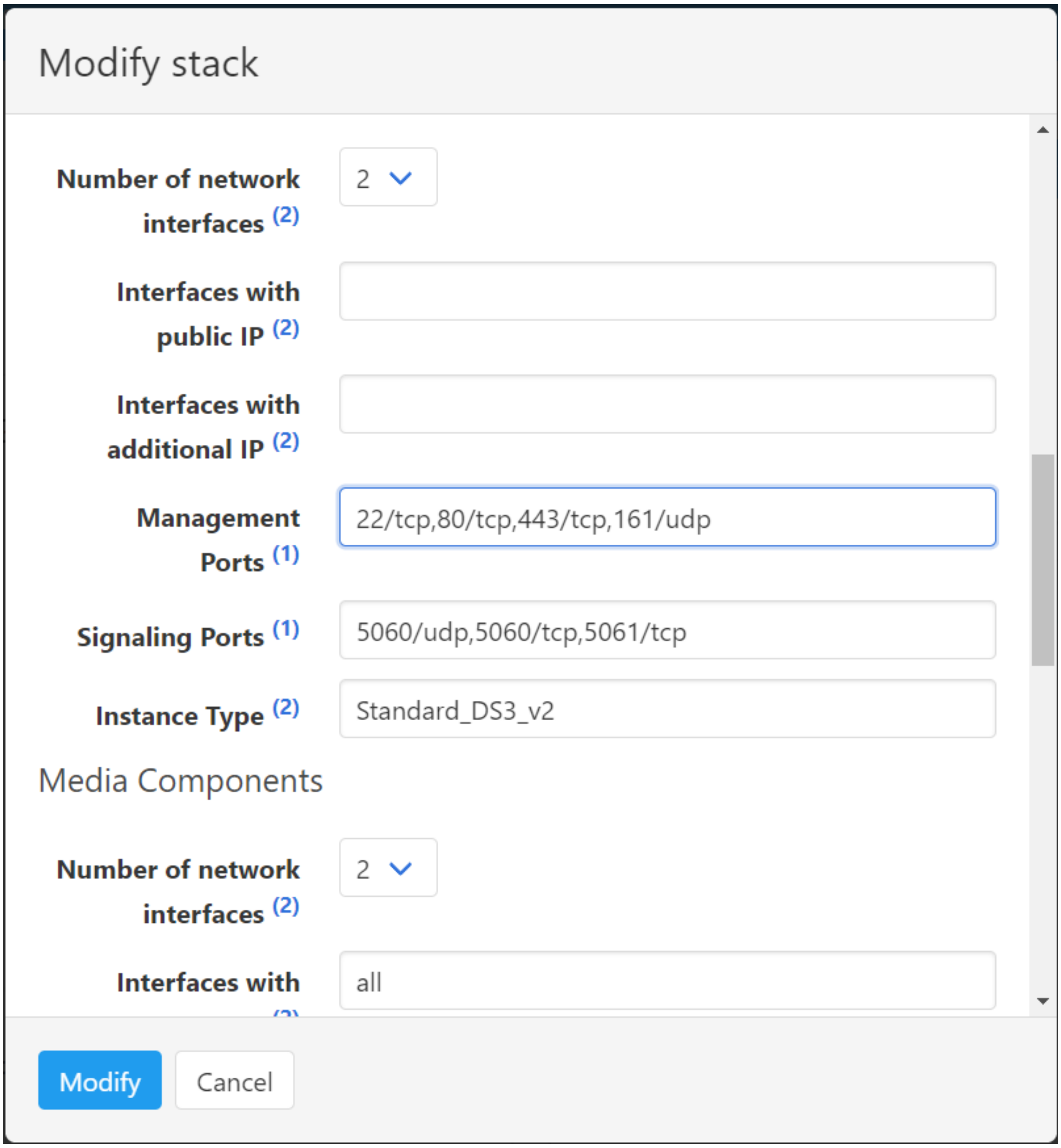
1. Log in to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual.*

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 12-19: Modify Stack



Modify stack

Number of network interfaces (2): 2

Interfaces with public IP (2):

Interfaces with additional IP (2):

Management Ports (1): 22/tcp,80/tcp,443/tcp,161/udp

Signaling Ports (1): 5060/udp,5060/tcp,5061/tcp

Instance Type (2): Standard_DS3_v2

Media Components

Number of network interfaces (2): 2

Interfaces with: all

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 148) or by configuring OVOC Cloud Architecture mode (seeConfigure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 152

⚠ 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 196).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 257)
   - root OS user (see OS Users Passwords on page 257)

> ⚠ 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 213).
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 148). 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 240).

> ⚠ 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

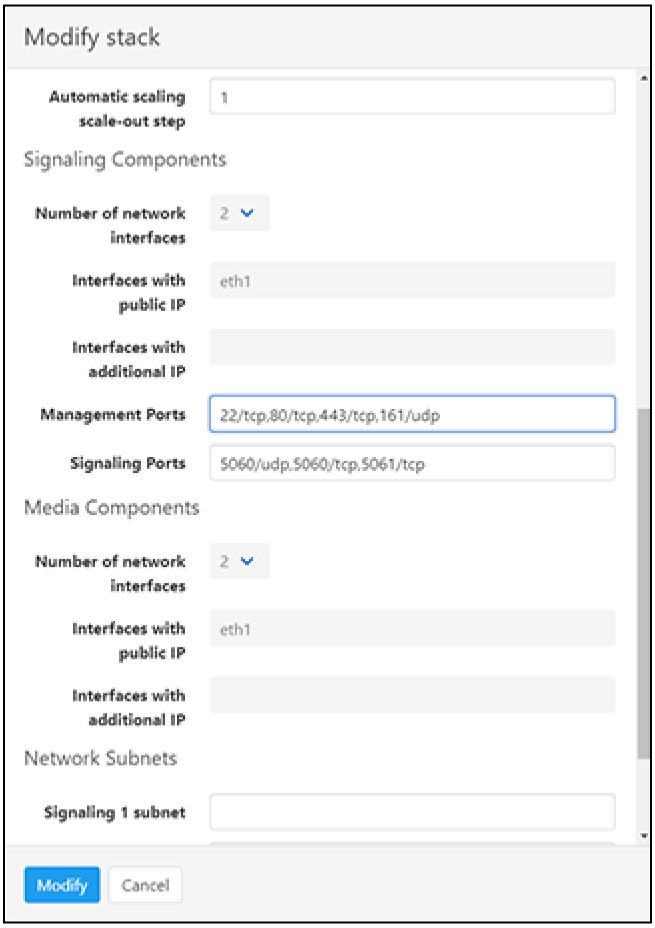
Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager

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 12-20: Modify Stack



Modify stack

Automatic scaling scale-out step: 1

Signaling Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Management Ports: 22/tcp,80/tcp,443/tcp,161/udp

Signaling Ports: 5060/udp,5060/tcp,5061/tcp

Media Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Network Subnets

Signaling 1 subnet:

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 194).
- 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

13 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 189).
- 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 174

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 212
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:**

➢ **HiTo install DVD3:**

1. Download the **DVD3**.ISO file Version 8.2.3000 to your PC.
2. Using the WinSCP utility (see Transferring Files on page 326) 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:

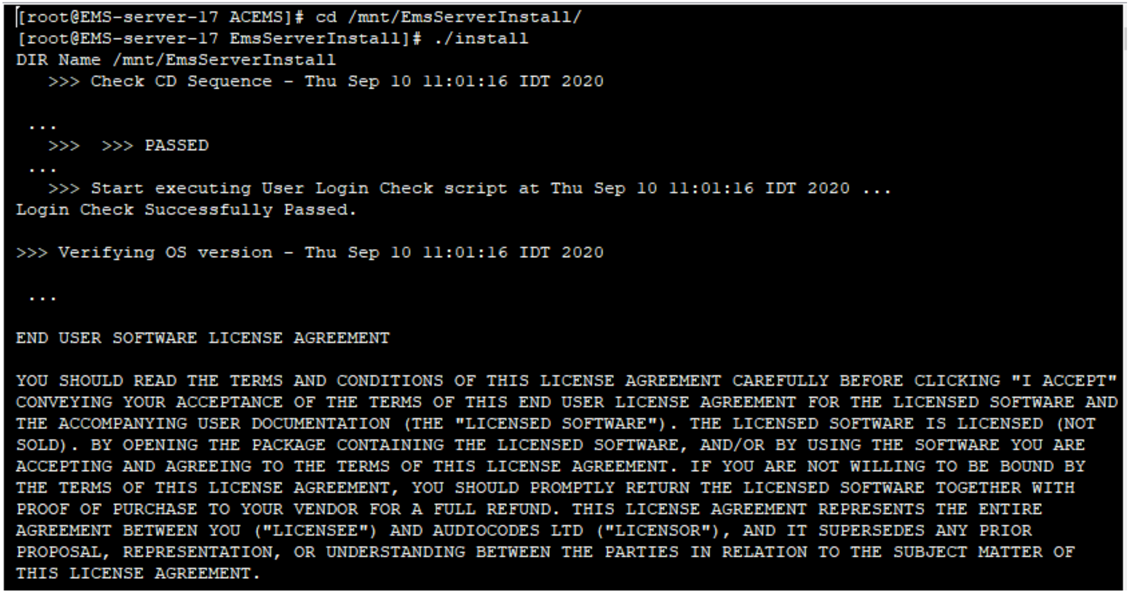
```
mount /home/acems/DVD3_OVOC_ 8.2.3000.iso /mnt
```

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

7. Run the installation script from its location:

```
./install
```

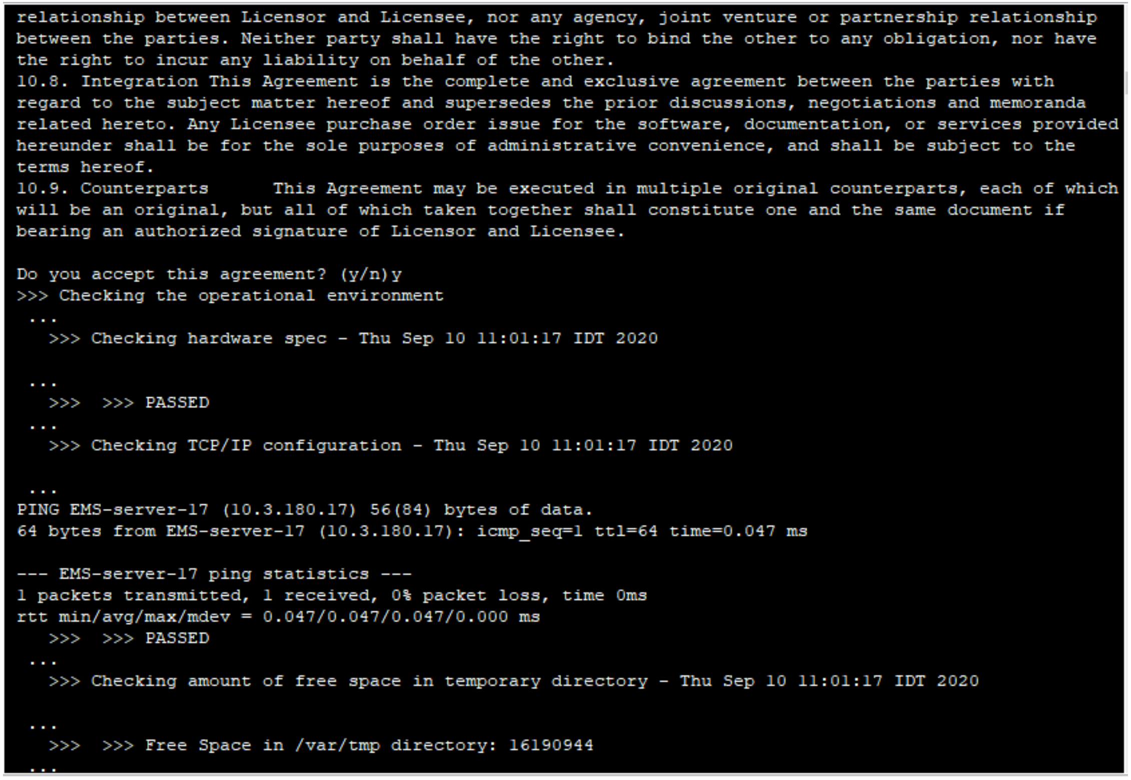
Figure 13-1: OVOC server Installation Script



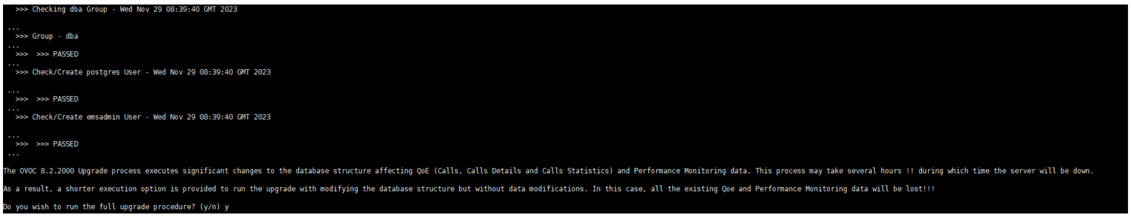
```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> 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 13-2: OVOC server Upgrade – License Agreement



```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```



```
  >>> Checking dba Group - Wed Nov 29 08:39:40 GMT 2023

...
  >>> Group - dba
...
  >>>  >>> PASSED
...
  >>> Check/Create postgres User - Wed Nov 29 08:39:40 GMT 2023

...
  >>>  >>> PASSED
...
  >>> Check/Create emsadmin User - Wed Nov 29 08:39:40 GMT 2023

...
  >>>  >>> PASSED
...
The OVOC 8.2.2000 Upgrade process executes significant changes to the database structure affecting QoE (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. This process may take several hours !! during which time the server will be down.
As a result, a shorter execution option is provided to run the upgrade with modifying the database structure but without data modifications. In this case, all the existing Qoe and Performance Monitoring data will be lost!!!
Do you wish to run the full upgrade procedure? (y/n) y
```

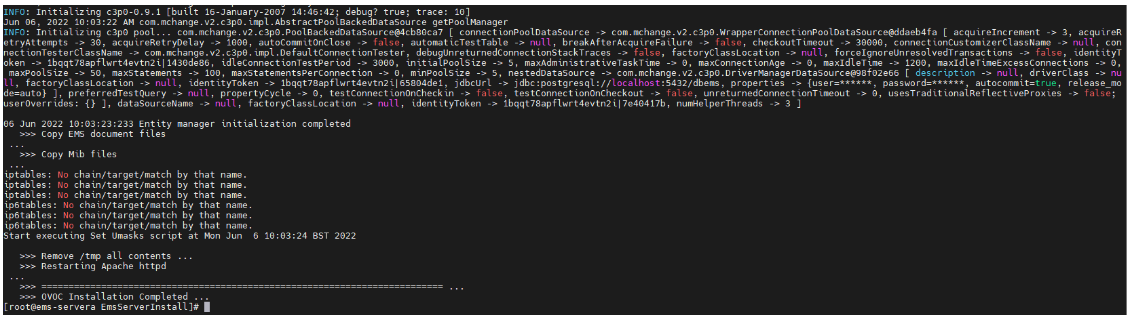
9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter **y** to 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 13-3: OVOC Server Installation Complete



```
INFO: Initializing c3p0-0.9.1 [built 16-January-2007 14:46:42; debug? true; trace: 10]
Jun 06, 2022 10:03:22 AM com.mchange.v2.c3p0.impl.AbstractPoolBackedDataSource getPoolManager
INFO: Initializing c3p0 pool... com.mchange.v2.c3p0.PoolBackedDataSource@4cb80ca7 [ connectionPoolDataSource -> com.mchange.v2.c3p0.WrapperConnectionPoolDataSource@ddaeb4fa [ acquireIncrement -> 3, acquireR
etryAttempts -> 30, acquireRetryDelay -> 1000, autoCommitOnClose -> false, automaticTestTable -> null, breakAfterAcquireFailure -> false, checkoutTimeout -> 30000, connectionCustomizerClassName -> null, con
nectionTesterClassName -> com.mchange.v2.c3p0.impl.DefaultConnectionTester, debugUnreturnedConnectionStackTraces -> false, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, identityT
oken -> 1bqqt78apflwrt4evtn2i|1430de86, idleConnectionTestPeriod -> 3000, initialPoolSize -> 5, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 1200, maxIdleTimeExcessConnections -> 0,
 maxPoolSize -> 50, maxStatements -> 100, maxStatementsPerConnection -> 0, minPoolSize -> 5, nestedDataSource -> com.mchange.v2.c3p0.DriverManagerDataSource@98f02e66 [ description -> null, driverClass -> nu
ll, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|65804de1, jdbcUrl -> jdbc:postgresql://localhost:5432/dbems, properties -> {user=******, password=******, autocommit=true, release_mo
de=auto} ], preferredTestQuery -> null, propertyCycle -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, usesTraditionalReflectiveProxies -> false;
userOverrides: {} ], dataSourceName -> null, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|7e40417b, numHelperThreads -> 3 ]

06 Jun 2022 10:03:23:233 Entity manager initialization completed
   >>> Copy EMS document files
 ...
   >>> Copy Mib files
 ...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
Start executing Set Umasks script at Mon Jun  6 10:03:24 BST 2022

   >>> Remove /tmp all contents ...
   >>> Restarting Apache httpd
 ...
   >>> ========================================================================== ...
   >>> OVOC Installation Completed ...
[root@ems-servera EmsServerInstall]# 
```

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:

```
# EmsServerManager
```

15. Verify that all processes are up and running (Viewing Process Statuses on page 201) 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 189)
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 191).

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

14 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 189).
- 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.

➢ **HiTo install DVD3:**

1. Download the **DVD3**.ISO file Version 8.2.3000 to your PC.
2. Using the WinSCP utility (see Transferring Files on page 326) 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:

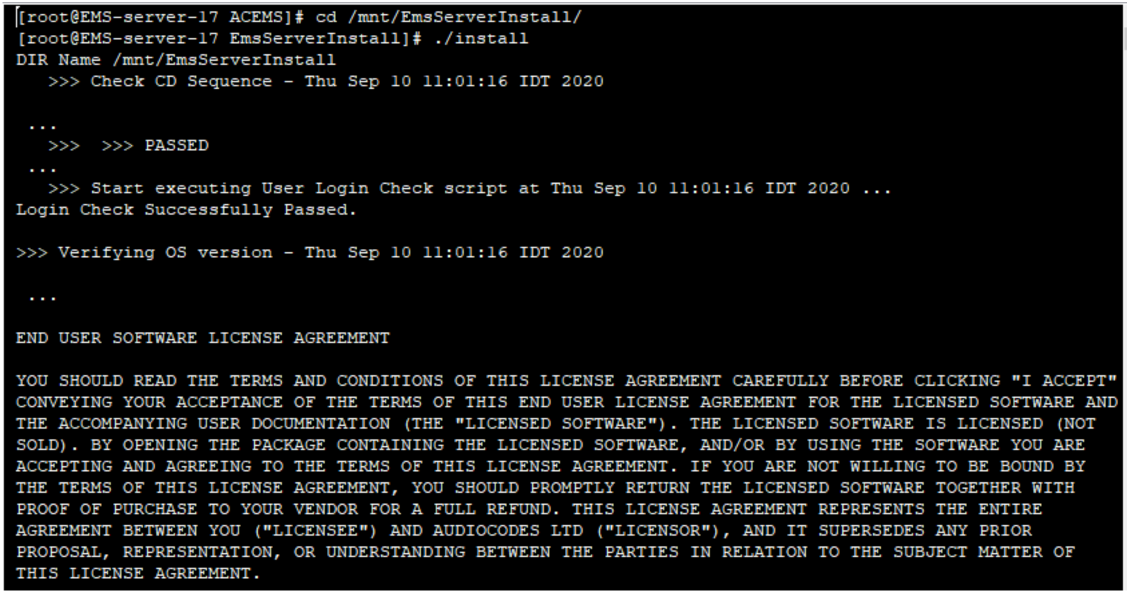
```
mount /home/acems/DVD3_OVOC_ 8.2.3000.iso /mnt
```

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

7. Run the installation script from its location:

```
./install
```

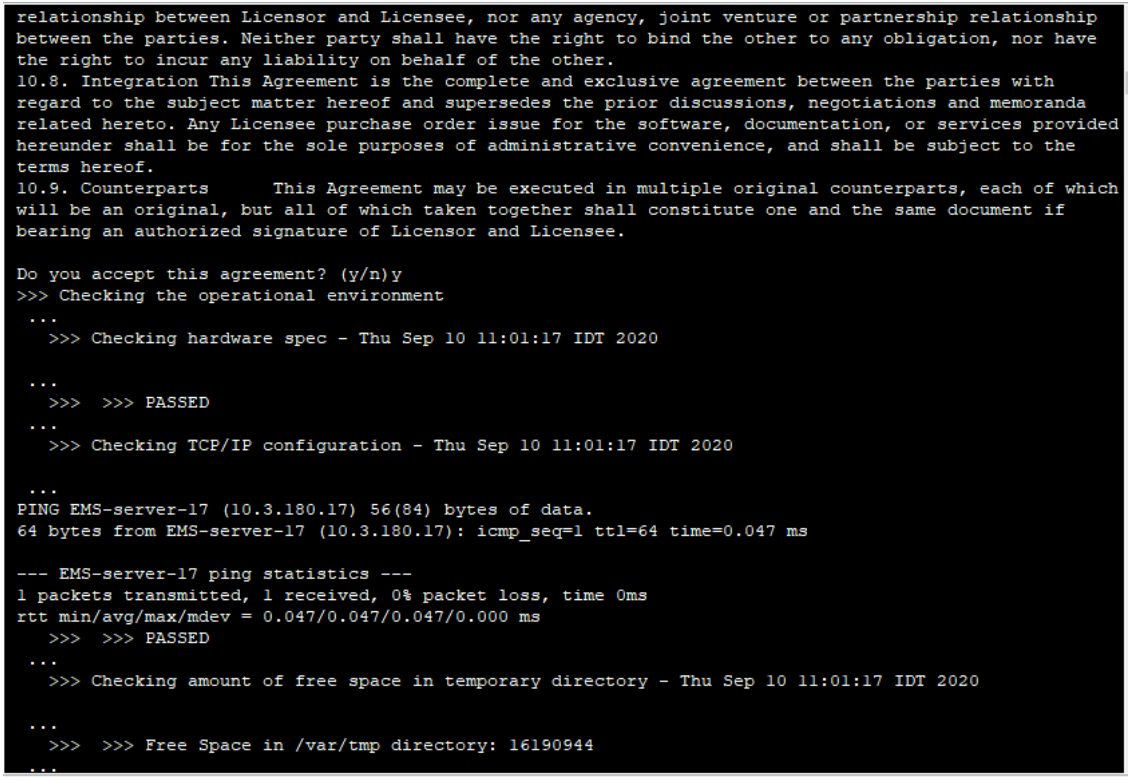
Figure 14-1: OVOC server Installation Script



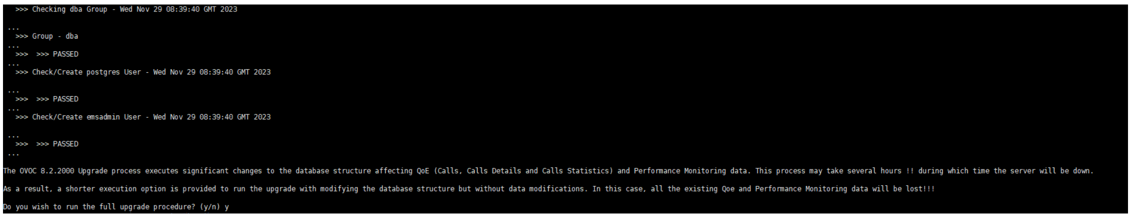
```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> 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



```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```



```
  >>> Checking dba Group - Wed Nov 29 08:39:40 GMT 2023

 ...
  >>> Group - dba
 ...
  >>>  >>> PASSED
 ...
  >>> Check/Create postgres User - Wed Nov 29 08:39:40 GMT 2023

 ...
  >>>  >>> PASSED
 ...
  >>> Check/Create emsadmin User - Wed Nov 29 08:39:40 GMT 2023

 ...
  >>>  >>> PASSED
 ...
The OVOC 8.2.2000 Upgrade process executes significant changes to the database structure affecting QoE (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. This process may take several hours !! during which time the server will be down.
As a result, a shorter execution option is provided to run the upgrade with modifying the database structure but without data modifications. In this case, all the existing Qoe and Performance Monitoring data will be lost!!!
Do you wish to run the full upgrade procedure? (y/n) y
```

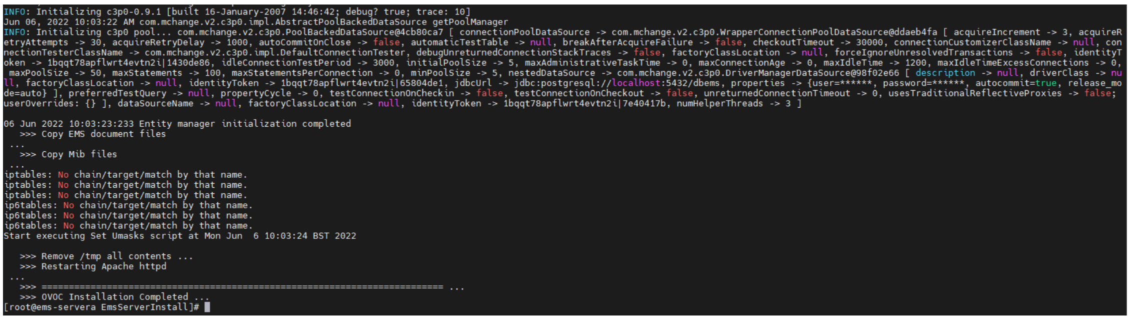
9. You are prompted to either run a Full Upgrade procedure affecting QoE data (Calls, Calls Details and Calls Statistics) and Performance Monitoring data. As an alternative, you can run a shorter execution, however in this case, existing QoE and Performance Monitoring data is not saved. Enter **y** to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



```
INFO: Initializing c3p0-0.9.1 [built 16-January-2007 14:46:42; debug? true; trace: 10]
Jun 06, 2022 10:03:22 AM com.mchange.v2.c3p0.impl.AbstractPoolBackedDataSource getPoolManager
INFO: Initializing c3p0 pool... com.mchange.v2.c3p0.PoolBackedDataSource@4cb80ca7 [ connectionPoolDataSource -> com.mchange.v2.c3p0.WrapperConnectionPoolDataSource@ddaeb4fa [ acquireIncrement -> 3, acquireR
etryAttempts -> 30, acquireRetryDelay -> 1000, autoCommitOnClose -> false, automaticTestTable -> null, breakAfterAcquireFailure -> false, checkoutTimeout -> 30000, connectionCustomizerClassName -> null, con
nectionTesterClassName -> com.mchange.v2.c3p0.impl.DefaultConnectionTester, debugUnreturnedConnectionStackTraces -> false, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, identityT
oken -> 1bqqt78apflwrt4evtn2i|1430de86, idleConnectionTestPeriod -> 3000, initialPoolSize -> 5, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 1200, maxIdleTimeExcessConnections -> 0,
 maxPoolSize -> 50, maxStatements -> 100, maxStatementsPerConnection -> 0, minPoolSize -> 5, nestedDataSource -> com.mchange.v2.c3p0.DriverManagerDataSource@98f02e66 [ description -> null, driverClass -> nu
ll, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|65804de1, jdbcUrl -> jdbc:postgresql://localhost:5432/dbems, properties -> {user=******, password=******, autocommit=true, release_mo
de=auto} ], preferredTestQuery -> null, propertyCycle -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, usesTraditionalReflectiveProxies -> false;
userOverrides: {} ], dataSourceName -> null, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|7e40417b, numHelperThreads -> 3 ]

06 Jun 2022 10:03:23:233 Entity manager initialization completed
   >>> Copy EMS document files
 ...
   >>> Copy Mib files
 ...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
Start executing Set Umasks script at Mon Jun  6 10:03:24 BST 2022

   >>> Remove /tmp all contents ...
   >>> Restarting Apache httpd
 ...
   >>> ========================================================================== ...
   >>> OVOC Installation Completed ...
[root@ems-servera EmsServerInstall]#
```

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:

```
# EmsServerManager
```

15. Verify that all processes are up and running (Viewing Process Statuses on page 201) and verify that login to OVOC Web client is successful.

15 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):

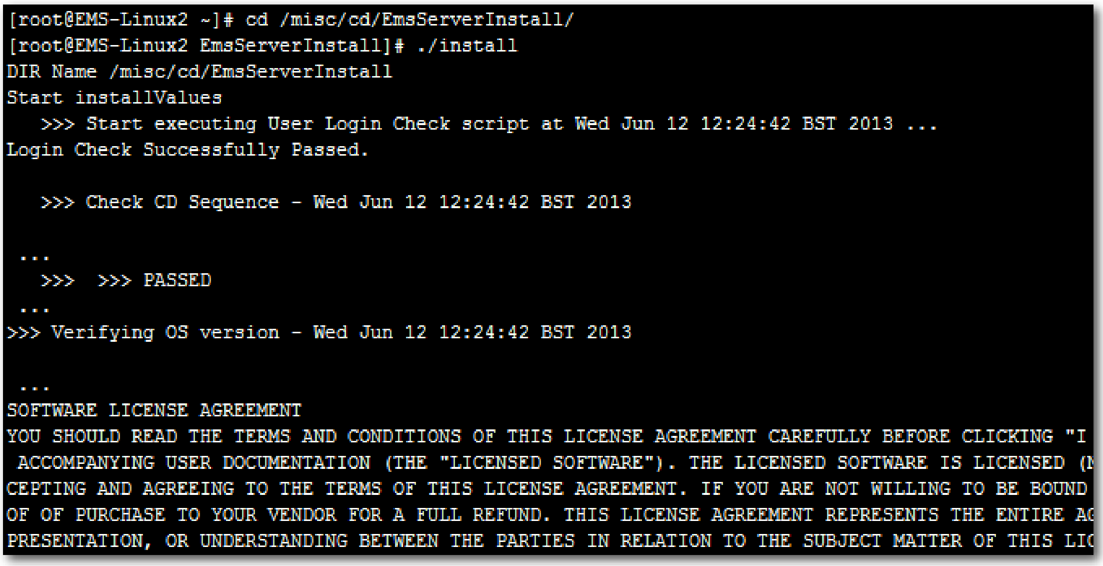
   ```
   mount /home/acems/DVD3_OVOC_/mnt
   ```

5. Run the installation script from its location:

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

   ```
   ./install
   ```

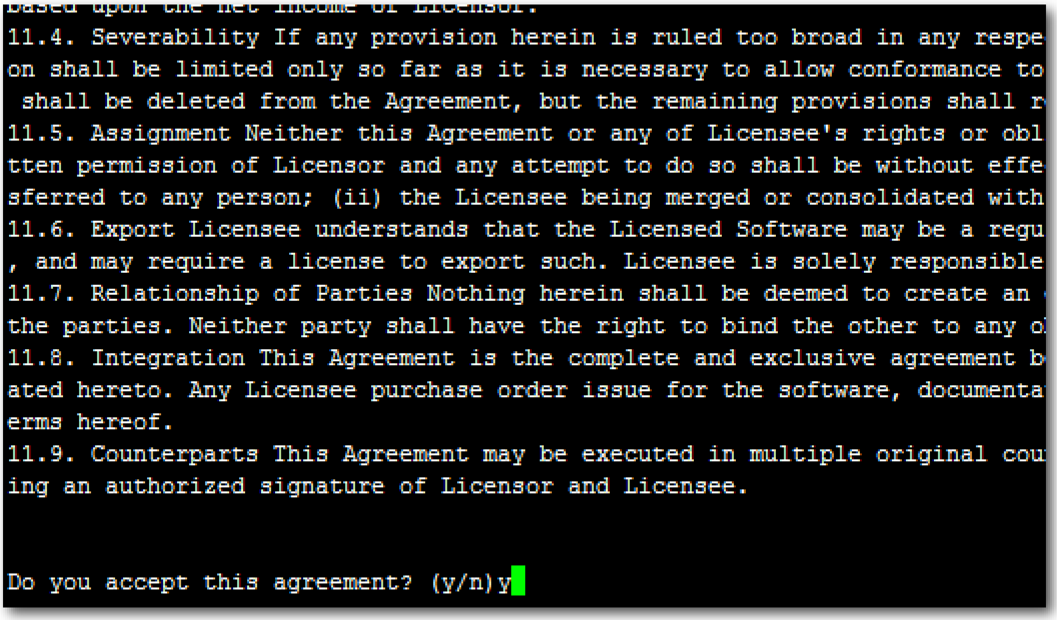
Figure 15-1: OVOC server Upgrade



```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/
[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
   >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

   >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

 ...
   >>>  >>> PASSED
 ...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

 ...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
 ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

Figure 15-2: OVOC server Upgrade – License Agreement

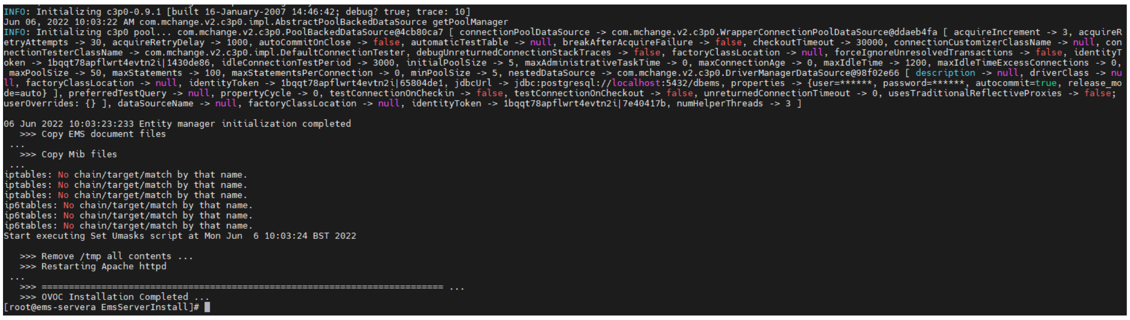


```
based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
 shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement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


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

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

   - If you are prompted to reboot, press Enter to reboot the OVOC server, 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 15-3: OVOC server Installation Complete



```
INFO: Initializing c3p0-0.9.1 [built 16-January-2007 14:46:42; debug? true; trace: 10]
Jun 06, 2022 10:03:22 AM com.mchange.v2.c3p0.impl.AbstractPoolBackedDataSource getPoolManager
INFO: Initializing c3p0 pool... com.mchange.v2.c3p0.PoolBackedDataSource@4cb80ca7 [ connectionPoolDataSource -> com.mchange.v2.c3p0.WrapperConnectionPoolDataSource@ddaeb4fa [ acquireIncrement -> 3, acquireR
etryAttempts -> 30, acquireRetryDelay -> 1000, autoCommitOnClose -> false, automaticTestTable -> null, breakAfterAcquireFailure -> false, checkoutTimeout -> 30000, connectionCustomizerClassName -> null, con
nectionTesterClassName -> com.mchange.v2.c3p0.impl.DefaultConnectionTester, debugUnreturnedConnectionStackTraces -> false, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, identityT
oken -> 1bqqt78apflwrt4evtn2i|1430de86, idleConnectionTestPeriod -> 3000, initialPoolSize -> 5, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 1200, maxIdleTimeExcessConnections -> 0,
 maxPoolSize -> 50, maxStatements -> 100, maxStatementsPerConnection -> 0, minPoolSize -> 5, nestedDataSource -> com.mchange.v2.c3p0.DriverManagerDataSource@98f02e66 [ description -> null, driverClass -> nu
ll, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|65804de1, jdbcUrl -> jdbc:postgresql://localhost:5432/dbems, properties -> {user=******, password=******, autocommit=true, release_mo
de=auto} ], preferredTestQuery -> null, propertyCycle -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, usesTraditionalReflectiveProxies -> false;
userOverrides: {} ], dataSourceName -> null, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|7e40417b, numHelperThreads -> 3 ]

06 Jun 2022 10:03:23:233 Entity manager initialization completed
   >>> Copy EMS document files
 ...
   >>> Copy Mib files
 ...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
Start executing Set Umasks script at Mon Jun  6 10:03:24 BST 2022

   >>> Remove /tmp all contents ...
   >>> Restarting Apache httpd
 ...
   >>> ========================================================================= ...
   >>> OVOC Installation Completed ...
[root@ems-servera EmsServerInstall]#
```

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:

```
# EmsServerManager
```

12. Verify that all processes are up and running (Viewing Process Statuses on page 201) 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 326), 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:

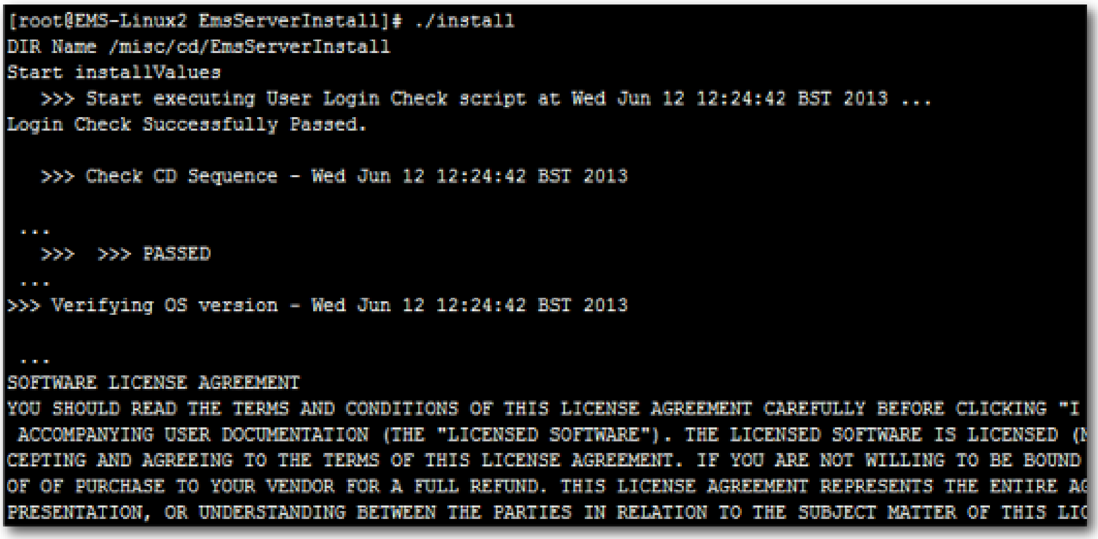
```
mount /home/acems/DVD3_OVOC_ 8.2.3000.iso /mnt
```

```
cd /mnt/EmsServerInstall
```

5. Run the installation script from its location:

```
./install
```

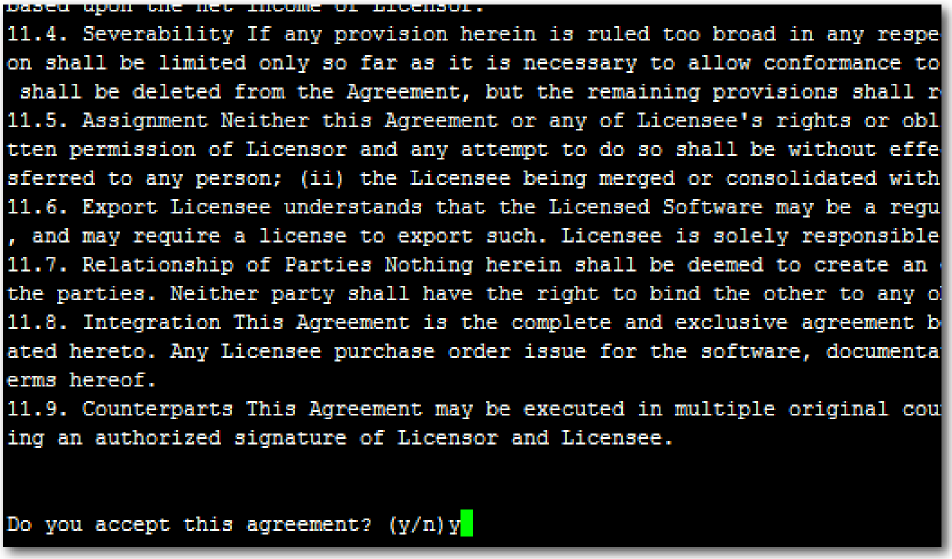
Figure 15-4: OVOC server Upgrade



```
[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
   >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

   >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

 ...
   >>>  >>> PASSED
 ...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

 ...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
 ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

Figure 15-5: OVOC server Upgrade– License Agreement

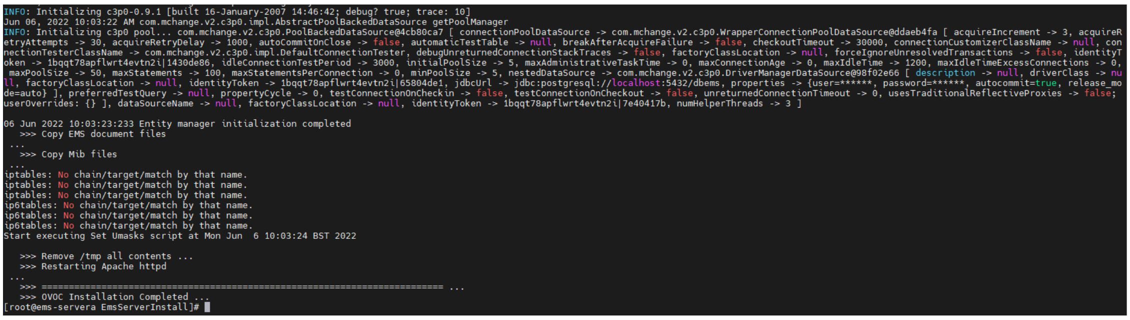


```
based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
 shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement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


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

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

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

Figure 15-6: OVOC server Installation Complete



```
INFO: Initializing c3p0-0.9.1 [built 16-January-2007 14:46:42; debug? true; trace: 10]
Jun 06, 2022 10:03:22 AM com.mchange.v2.c3p0.impl.AbstractPoolBackedDataSource getPoolManager
INFO: Initializing c3p0 pool... com.mchange.v2.c3p0.PoolBackedDataSource@4cb80ca7 [ connectionPoolDataSource -> com.mchange.v2.c3p0.WrapperConnectionPoolDataSource@ddaeb4fa [ acquireIncrement -> 3, acquireR
etryAttempts -> 30, acquireRetryDelay -> 1000, autoCommitOnClose -> false, automaticTestTable -> null, breakAfterAcquireFailure -> false, checkoutTimeout -> 30000, connectionCustomizerClassName -> null, con
nectionTesterClassName -> com.mchange.v2.c3p0.impl.DefaultConnectionTester, debugUnreturnedConnectionStackTraces -> false, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, identityT
oken -> 1bqqt78apflwrt4evtn2i|1430de86, idleConnectionTestPeriod -> 3000, initialPoolSize -> 5, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 1200, maxIdleTimeExcessConnections -> 0,
 maxPoolSize -> 50, maxStatements -> 100, maxStatementsPerConnection -> 0, minPoolSize -> 5, nestedDataSource -> com.mchange.v2.c3p0.DriverManagerDataSource@98f02e66 [ description -> null, driverClass -> nu
ll, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|65804de1, jdbcUrl -> jdbc:postgresql://localhost:5432/dbems, properties -> {user=******, password=******, autocommit=true, release_mo
de=auto} ], preferredTestQuery -> null, propertyCycle -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, usesTraditionalReflectiveProxies -> false;
userOverrides: {} ], dataSourceName -> null, factoryClassLocation -> null, identityToken -> 1bqqt78apflwrt4evtn2i|7e40417b, numHelperThreads -> 3 ]

06 Jun 2022 10:03:23:233 Entity manager initialization completed
   >>> Copy EMS document files
 ...
   >>> Copy Mib files
 ...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
ip6tables: No chain/target/match by that name.
Start executing Set Umasks script at Mon Jun  6 10:03:24 BST 2022

   >>> Remove /tmp all contents ...
   >>> Restarting Apache httpd
 ...
   >>> ========================================================================== ...
   >>> OVOC Installation Completed ...
[root@ems-servera EmsServerInstall]# 
```

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:

```
# EmsServerManager
```

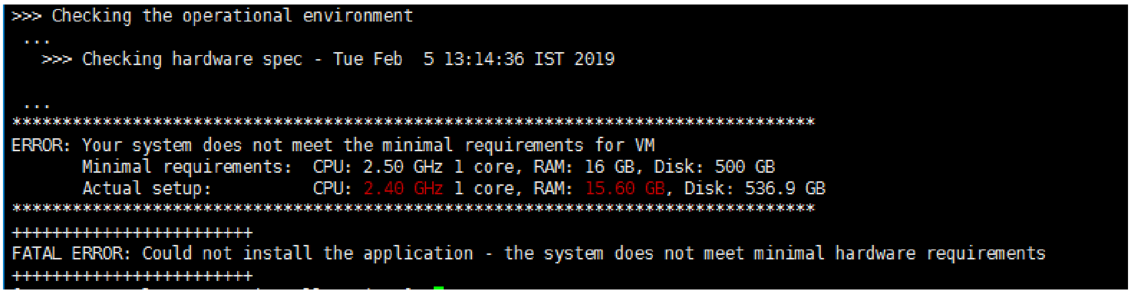
12. Verify that all processes are up and running (Viewing Process Statuses on page 201) and verify that login to OVOC Web client is successful.

16 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:

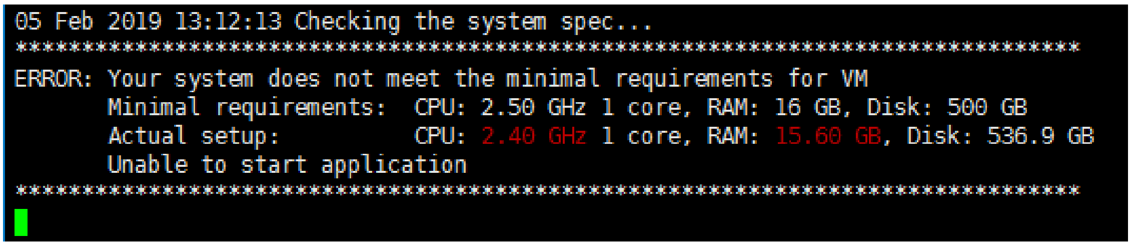
Figure 16-1: Minimum Hardware Requirements Upgrade



```
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Tue Feb  5 13:14:36 IST 2019

 ...
********************************************************************************
ERROR: Your system does not meet the minimal requirements for VM
       Minimal requirements:  CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
       Actual setup:          CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
********************************************************************************
++++++++++++++++++++++++
FATAL ERROR: Could not install the application - the system does not meet minimal hardware requirements
++++++++++++++++++++++++
```

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

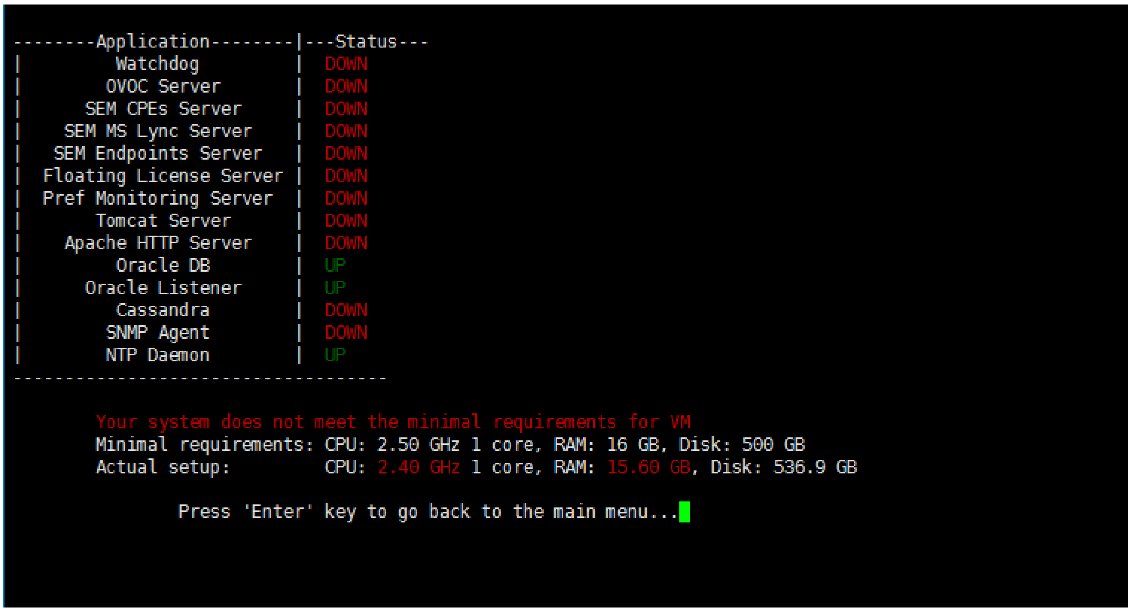
Figure 16-2: Minimum Hardware Requirements System Error



```
05 Feb 2019 13:12:13 Checking the system spec...
********************************************************************************
ERROR: Your system does not meet the minimal requirements for VM
       Minimal requirements:  CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
       Actual setup:          CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
       Unable to start application
********************************************************************************
```

- 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 :

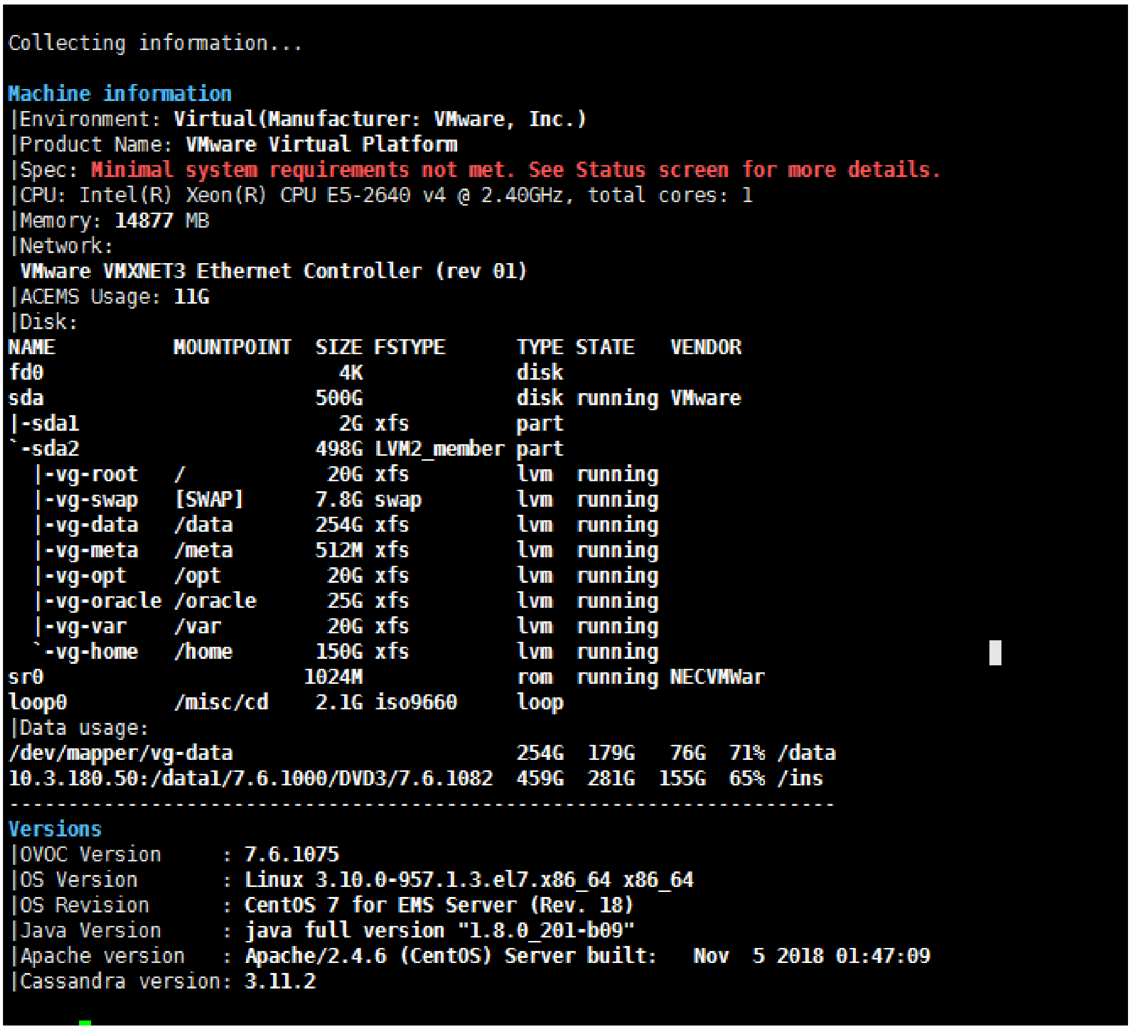
Figure 16-3: Status Screen Error



```
--------Application--------|---Status---
|         Watchdog          |  DOWN
|        OVOC Server        |  DOWN
|      SEM CPEs Server      |  DOWN
|    SEM MS Lync Server     |  DOWN
|   SEM Endpoints Server    |  DOWN
|  Floating License Server  |  DOWN
|  Pref Monitoring Server   |  DOWN
|       Tomcat Server       |  DOWN
|    Apache HTTP Server     |  DOWN
|         Oracle DB         |  UP
|      Oracle Listener      |  UP
|         Cassandra         |  DOWN
|        SNMP Agent         |  DOWN
|        NTP Daemon         |  UP
------------------------------------

        Your system does not meet the minimal requirements for VM
        Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
        Actual setup:         CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB

                Press 'Enter' key to go back to the main menu...
```

- 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 16-4: General Info Minimum Requirements



```
Collecting information...

Machine information
|Environment: Virtual(Manufacturer: VMware, Inc.)
|Product Name: VMware Virtual Platform
|Spec: Minimal system requirements not met. See Status screen for more details.
|CPU: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz, total cores: 1
|Memory: 14877 MB
|Network:
 VMware VMXNET3 Ethernet Controller (rev 01)
|ACEMS Usage: 11G
|Disk:
NAME          MOUNTPOINT  SIZE FSTYPE      TYPE STATE   VENDOR
fd0                         4K             disk
sda                       500G             disk running VMware
|-sda1                      2G xfs         part
`-sda2                    498G LVM2_member part
  |-vg-root   /            20G xfs         lvm  running
  |-vg-swap   [SWAP]      7.8G swap        lvm  running
  |-vg-data   /data       254G xfs         lvm  running
  |-vg-meta   /meta       512M xfs         lvm  running
  |-vg-opt    /opt         20G xfs         lvm  running
  |-vg-oracle /oracle      25G xfs         lvm  running
  |-vg-var    /var         20G xfs         lvm  running
  `-vg-home   /home       150G xfs         lvm  running
sr0                      1024M             rom  running NECVMWar
loop0         /misc/cd    2.1G iso9660     loop
|Data usage:
/dev/mapper/vg-data                        254G  179G   76G  71% /data
10.3.180.50:/data1/7.6.1000/DVD3/7.6.1082  459G  281G  155G  65% /ins
----------------------------------------------------------------------
Versions
|OVOC Version     : 7.6.1075
|OS Version       : Linux 3.10.0-957.1.3.el7.x86_64 x86_64
|OS Revision      : CentOS 7 for EMS Server (Rev. 18)
|Java Version     : java full version "1.8.0_201-b09"
|Apache version   : Apache/2.4.6 (CentOS) Server built:   Nov  5 2018 01:47:09
|Cassandra version: 3.11.2
```

Part V

OVOC Server Machine Backup and Restore

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

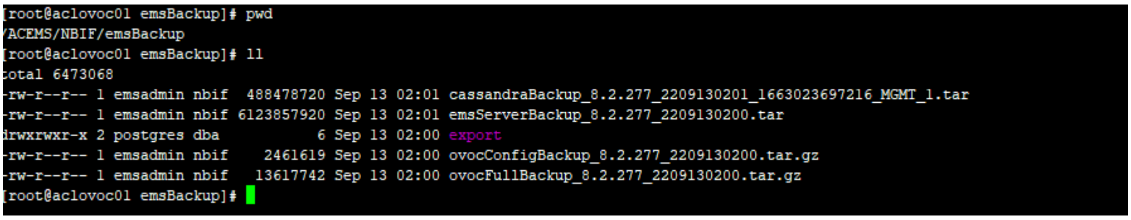
17 OVOC Server Backup Processes

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 17-1: Backup Log



```
[root@aclovoc01 emsBackup]# pwd
/ACEMS/NBIF/emsBackup
[root@aclovoc01 emsBackup]# ll
total 6473068
-rw-r--r-- 1 emsadmin nbif  488478720 Sep 13 02:01 cassandraBackup_8.2.277_2209130201_1663023697216_MGMT_1.tar
-rw-r--r-- 1 emsadmin nbif 6123857920 Sep 13 02:01 emsServerBackup_8.2.277_2209130200.tar
drwxrwxr-x 2 postgres dba           6 Sep 13 02:00 export
-rw-r--r-- 1 emsadmin nbif    2461619 Sep 13 02:00 ovocConfigBackup_8.2.277_2209130200.tar.gz
-rw-r--r-- 1 emsadmin nbif   13617742 Sep 13 02:00 ovocFullBackup_8.2.277_2209130200.tar.gz
[root@aclovoc01 emsBackup]# 
```

➢ **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

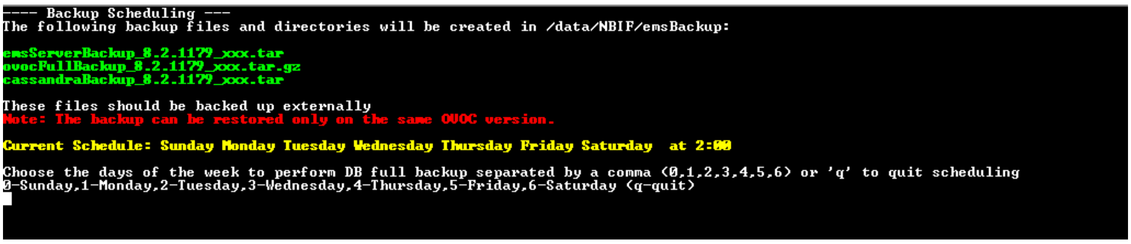
This step describes how to reschedule the time to run the automatic backup of the files described in OVOC Server Backup Processes above. By default, the backup is run daily at 2:00

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 17-2: Backup Scheduling



```
---- Backup Scheduling ---
The following backup files and directories will be created in /data/NBIF/emsBackup:

emsServerBackup_8.2.1179_xxx.tar
ovocFullBackup_8.2.1179_xxx.tar.gz
cassandraBackup_8.2.1179_xxx.tar

These files should be backed up externally
Note: The backup can be restored only on the same OVOC version.

Current Schedule: Sunday Monday Tuesday Wednesday Thursday Friday Saturday  at 2:00

Choose the days of the week to perform DB full backup separated by a comma (0,1,2,3,4,5,6) or 'q' to quit scheduling
0-Sunday,1-Monday,2-Tuesday,3-Wednesday,4-Thursday,5-Friday,6-Saturday (q-quit)
```

18 OVOC Server Restore

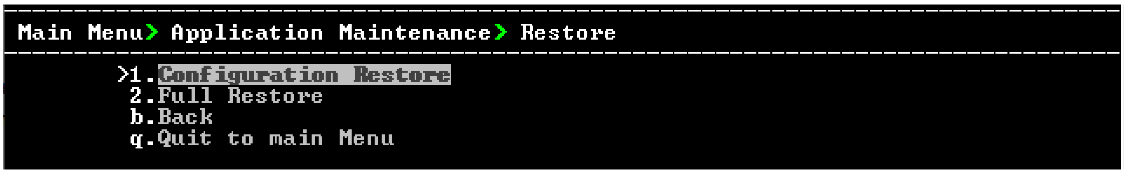
The OVOC server can be restored from the original machine where the backup files were created or from any other machine.

- 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 196.
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 189 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 18-1: Restore Menu



```
Main Menu> Application Maintenance> Restore
        >1.Configuration Restore
         2.Full Restore
         b.Back
         q.Quit to main Menu
```

7. Choose one of the following options:
   - Configuration Restore below
   - Full Restore on page 193

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:

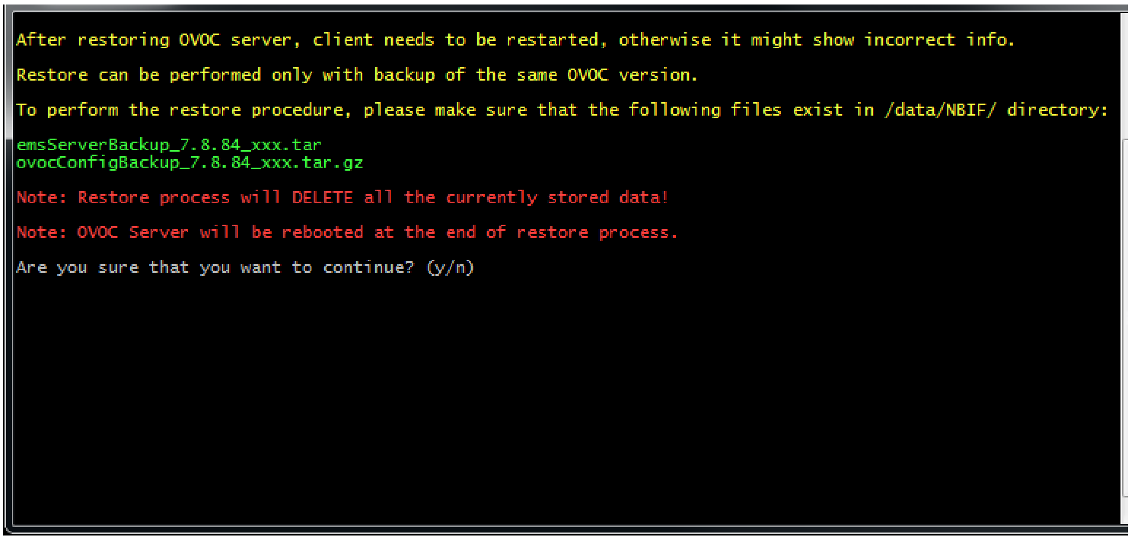
- emsServerBackup_<version>_<time&date>.tar
- ovocConfigBackup_<version>_<time&date>.tar.gz

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

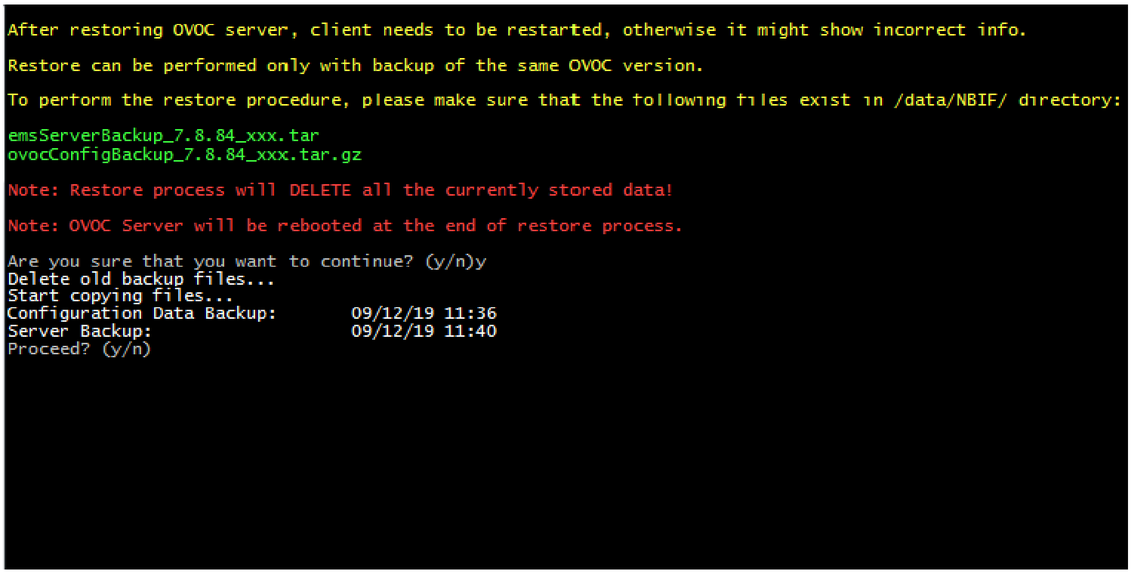
Figure 18-2: Configuration Restore Prompt



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.
Restore can be performed only with backup of the same OVOC version.
To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:
emsServerBackup_7.8.84_xxx.tar
ovocConfigBackup_7.8.84_xxx.tar.gz
Note: Restore process will DELETE all the currently stored data!
Note: OVOC Server will be rebooted at the end of restore process.
Are you sure that you want to continue? (y/n)
```

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

Figure 18-3: Configuration Restore-Confirm



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.

Restore can be performed only with backup of the same OVOC version.

To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:

emsServerBackup_7.8.84_xxx.tar
ovocConfigBackup_7.8.84_xxx.tar.gz

Note: Restore process will DELETE all the currently stored data!

Note: OVOC Server will be rebooted at the end of restore process.

Are you sure that you want to continue? (y/n)y
Delete old backup files...
Start copying files...
Configuration Data Backup:        09/12/19 11:36
Server Backup:                    09/12/19 11:40
Proceed? (y/n)
```

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 313).

Full Restore

This option restores OVOC topology, OVOC Web configuration (as detailed inConfiguration Restore on page 191) and data that is retrieved from managed devices including PMs, calls, alarms and journals. Data from the following backup files is restored:

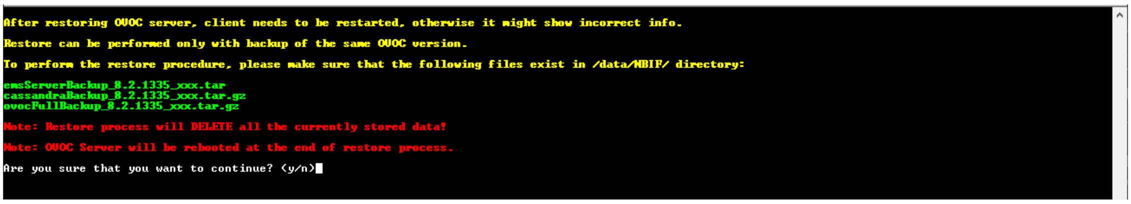
- emsServerBackup_<version>_<time&date>.tar
- cassandraBackup_<version>_<date>_<snapshotId>_<MGMT>_numberOfNodes.tar
- ovocFullBackup_<version>_<time&date>.tar.gz

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

➢ To run the full restore operation:

1. Select **Option 2: Full Restore**. A screen similar to the following is displayed:

Figure 18-4: Full Restore Prompt



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.

Restore can be performed only with backup of the same OVOC version.

To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:

emsServerBackup_8.2.1335_xxx.tar
cassandraBackup_8.2.1335_xxx.tar.gz
ovocFullBackup_8.2.1335_xxx.tar.gz

Note: Restore process will DELETE all the currently stored data!

Note: OVOC Server will be rebooted at the end of restore process.

Are you sure that you want to continue? (y/n)
```

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 313).

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 240).
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.

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.

19 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):

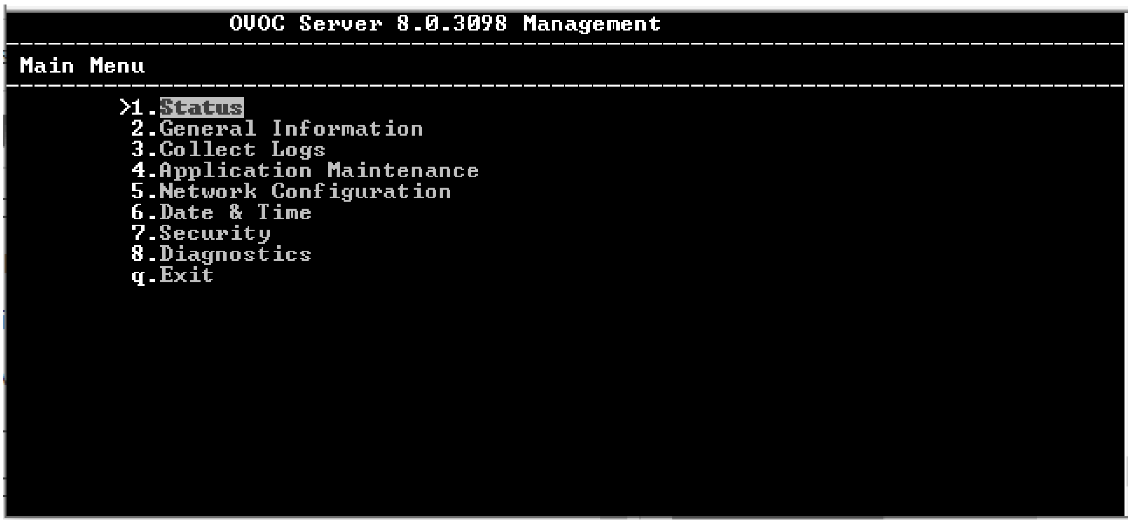
```
su - root
```

3. Type the following command:

```
# EmsServerManager
```

The OVOC Server Manager menu is displayed:

Figure 19-1: OVOC Server Manager Menu



```
                OVOC Server 8.0.3098 Management
---------------------------------------------------------------------------
Main Menu
---------------------------------------------------------------------------
        >1.Status
         2.General Information
         3.Collect Logs
         4.Application Maintenance
         5.Network Configuration
         6.Date & Time
         7.Security
         8.Diagnostics
         q.Exit
```

- 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 201)
- **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 204).
- **Collect Logs** – Collates all important logs into a single compressed file (Collecting Full Logs on page 206):
- **Application Maintenance** – Manages system maintenance actions (Application Maintenance on page 211):
  - 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 224):
  - 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 245):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (Security on page 246):
  - 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 280):
    - Server Syslog
    - Devices Syslog

- Devices Debug
- Server Logger Levels
- Network Traffic Capture

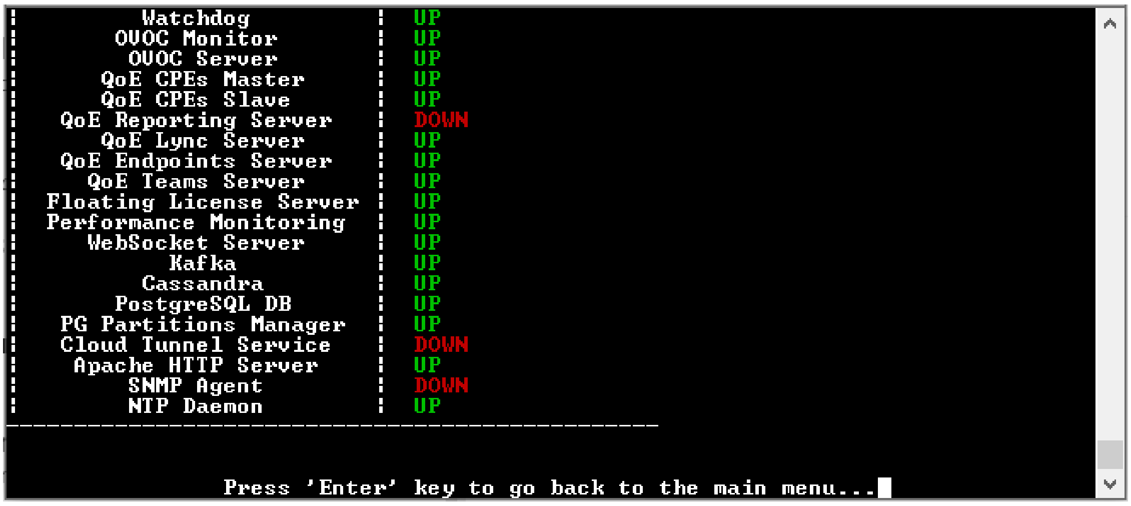
20 Viewing Process Statuses

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 20-1: Application Status in Standalone Mode



```
|          Watchdog           |  UP
|        OVOC Monitor         |  UP
|         OVOC Server         |  UP
|       QoE CPEs Master       |  UP
|       QoE CPEs Slave        |  UP
|    QoE Reporting Server     |  DOWN
|       QoE Lync Server       |  UP
|    QoE Endpoints Server     |  UP
|      QoE Teams Server       |  UP
|   Floating License Server   |  UP
|   Performance Monitoring    |  UP
|      WebSocket Server       |  UP
|            Kafka            |  UP
|          Cassandra          |  UP
|        PostgreSQL DB        |  UP
|    PG Partitions Manager    |  UP
|    Cloud Tunnel Service     |  DOWN
|     Apache HTTP Server      |  UP
|         SNMP Agent          |  DOWN
|         NTP Daemon          |  UP
------------------------------------------------


                Press 'Enter' key to go back to the main menu...
```

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

Table 20-1: 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 Microsoft Lync server.

Application	Status
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.
Cloud Tunnel Service	Indicates the status of the Cloud Tunnel Service (see Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 152.
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. ■ 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

Application	Status
	AudioCodes devices.
NTP Daemon	Indicates the status of the NTP Daemon process.

21 Viewing General Information

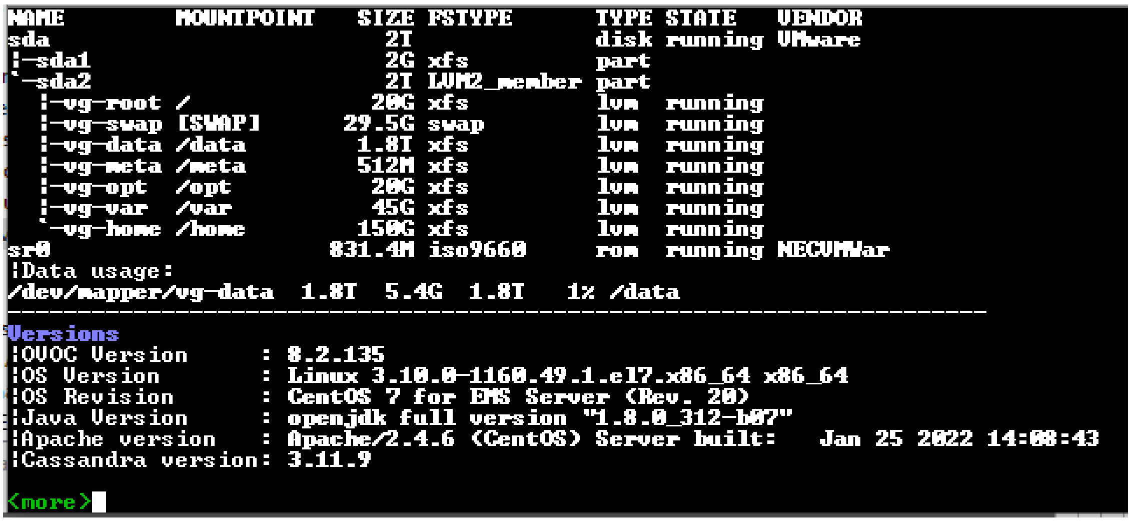
This section describes the General Information and Logs collection options. The General Information option provides detailed information about the OVOC server configuration and current status variables. The following information is provided:

- 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.

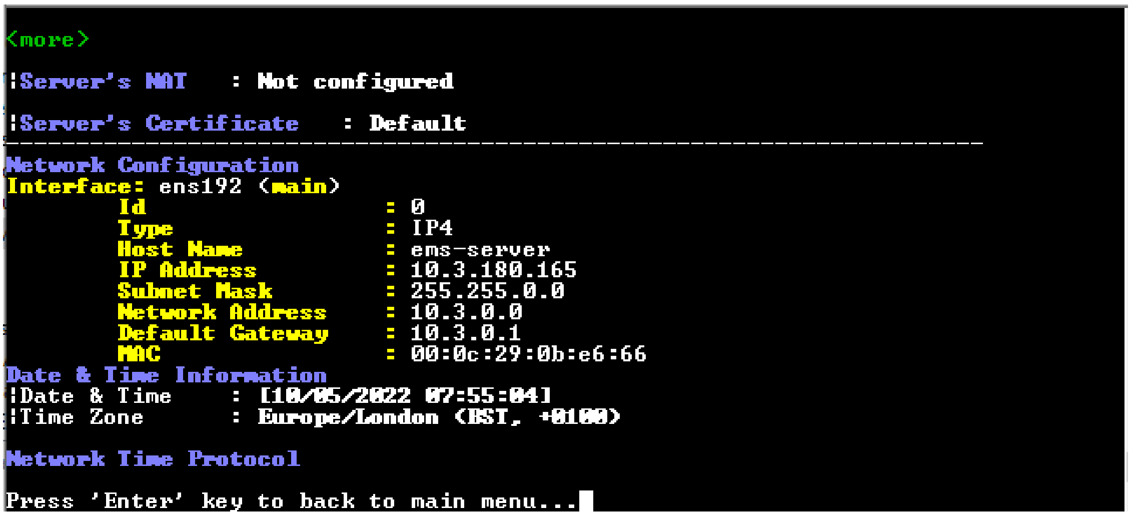
Figure 21-1: General Information



```
NAME          MOUNTPOINT    SIZE FSTYPE       TYPE STATE   VENDOR
sda                           2T              disk running VMware
|-sda1                        2G xfs          part
`-sda2                        2T LVM2_member  part
  |-vg-root /               20G xfs          lvm  running
  |-vg-swap [SWAP]        29.5G swap         lvm  running
  |-vg-data /data          1.8T xfs          lvm  running
  |-vg-meta /meta          512M xfs          lvm  running
  |-vg-opt  /opt            20G xfs          lvm  running
  |-vg-var  /var            45G xfs          lvm  running
  `-vg-home /home          150G xfs          lvm  running
sr0                     831.4M iso9660      rom  running NECVMWar
|Data usage:
/dev/mapper/vg-data  1.8T  5.4G  1.8T   1% /data
----------------------------------------------------------------------
Versions
|OVOC Version      : 8.2.135
|OS Version        : Linux 3.10.0-1160.49.1.el7.x86_64 x86_64
|OS Revision       : CentOS 7 for EMS Server (Rev. 20)
|Java Version      : openjdk full version "1.8.0_312-b07"
|Apache version    : Apache/2.4.6 (CentOS) Server built:   Jan 25 2022 14:08:43
|Cassandra version: 3.11.9

<more>
```

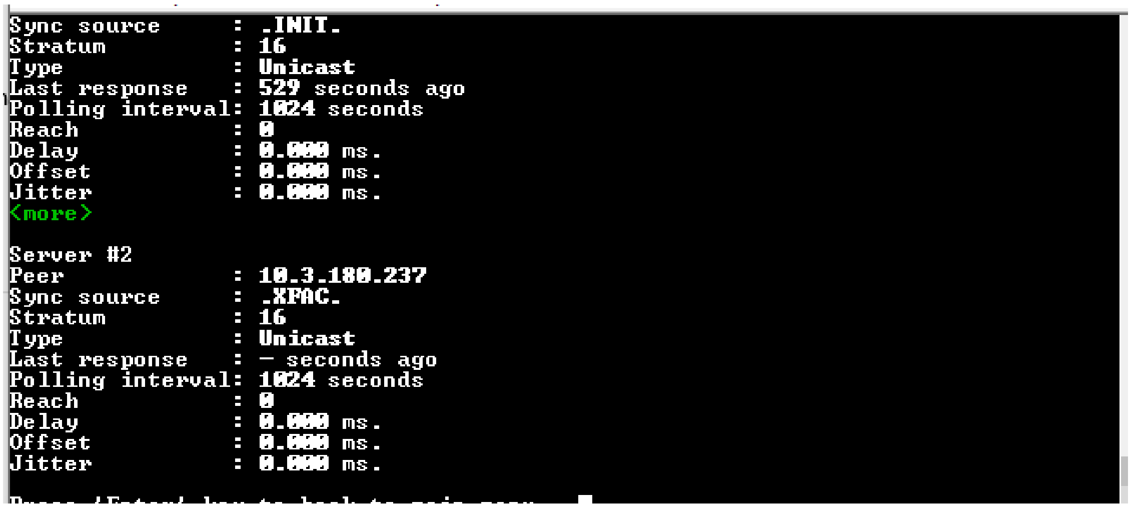
2. Press **<more>** to view more information; the following is displayed:

Figure 21-2: General Information 1



```
<more>

¦Server's NAT    : Not configured

¦Server's Certificate    : Default
---------------------------------------------------------------------------------------------
Network Configuration
Interface: ens192 (main)
        Id                  : 0
        Type                : IP4
        Host Name           : ems-server
        IP Address          : 10.3.180.165
        Subnet Mask         : 255.255.0.0
        Network Address     : 10.3.0.0
        Default Gateway     : 10.3.0.1
        MAC                 : 00:0c:29:0b:e6:66
Date & Time Information
¦Date & Time       : [10/05/2022 07:55:04]
¦Time Zone         : Europe/London (BST, +0100)

Network Time Protocol

Press 'Enter' key to back to main menu...
```

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



```
Sync source      : .INIT.
Stratum          : 16
Type             : Unicast
Last response    : 529 seconds ago
Polling interval: 1024 seconds
Reach            : 0
Delay            : 0.000 ms.
Offset           : 0.000 ms.
Jitter           : 0.000 ms.
<more>

Server #2
Peer             : 10.3.180.237
Sync source      : .XFAC.
Stratum          : 16
Type             : Unicast
Last response    : - seconds ago
Polling interval: 1024 seconds
Reach            : 0
Delay            : 0.000 ms.
Offset           : 0.000 ms.
Jitter           : 0.000 ms.

Press 'Enter' key to back to main menu...
```

22 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.

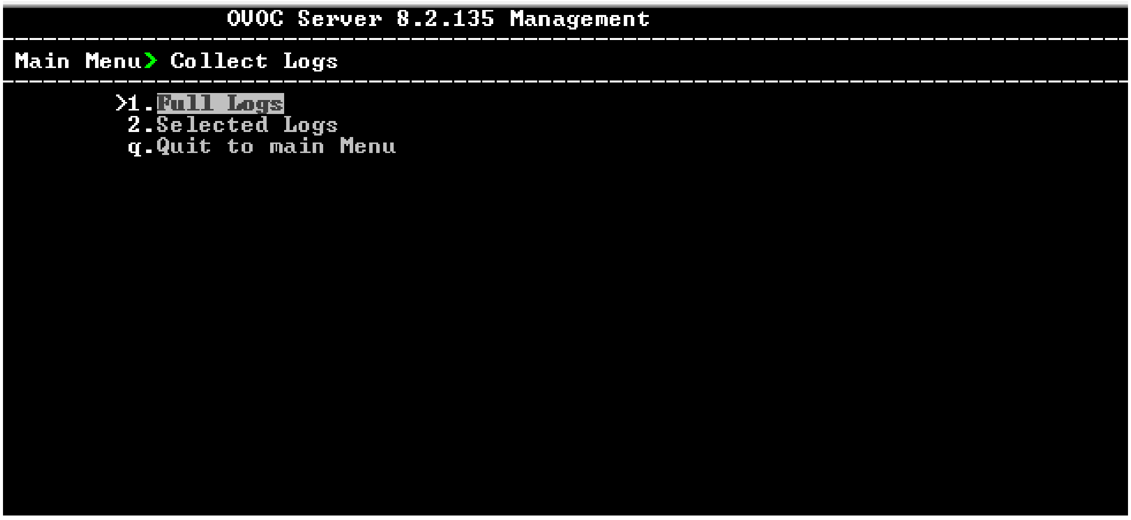
The following log files are collected:

- 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.

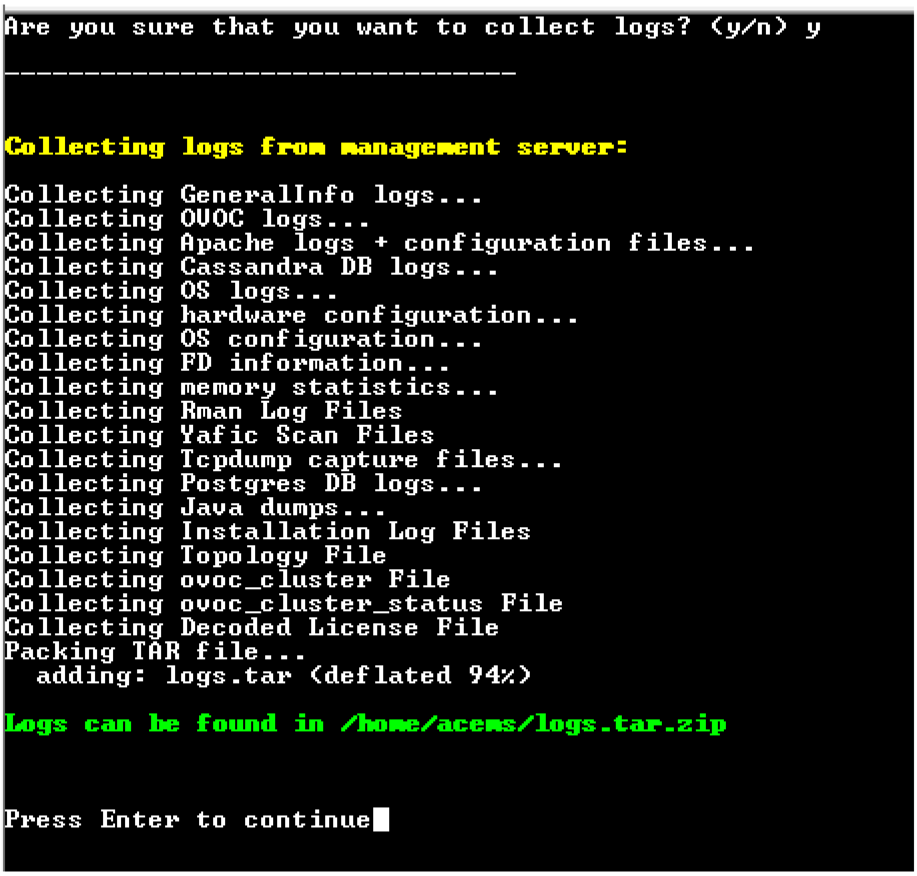
Figure 22-1: Collect Logs



```
                    OVOC Server 8.2.135 Management
------------------------------------------------------------------------------------------------
Main Menu> Collect Logs
------------------------------------------------------------------------------------------------
         >1.Full Logs
          2.Selected Logs
          q.Quit to main Menu
```

2. Select option **Full Logs**, and then press Enter.
3. You are prompted if you wish to collect logs, enter **y** to proceed. The logs are collected. This process can take a few minutes. Once all of the logs have been collected, a message is displayed informing you that a Diagnostic tar file has been created and the location of the tar file.

Figure 22-2: Collecting Logs



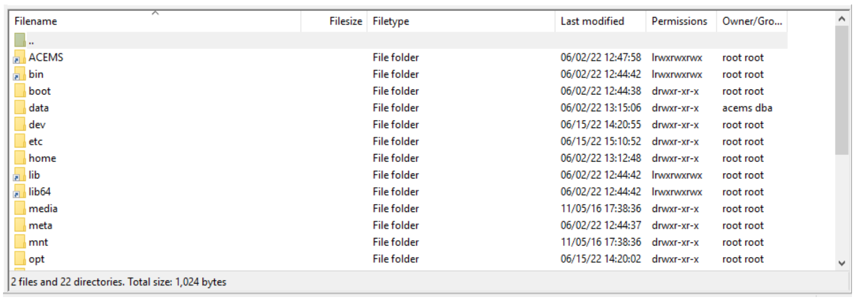
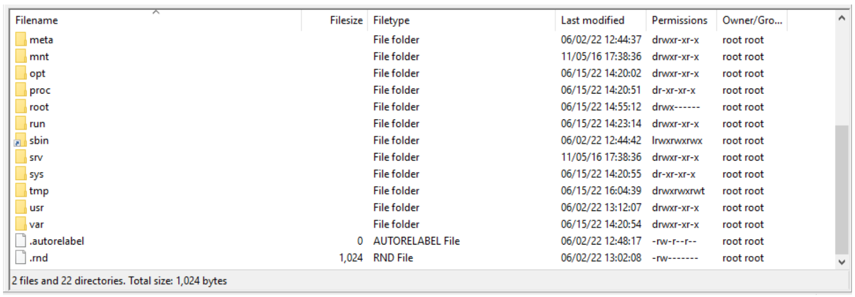
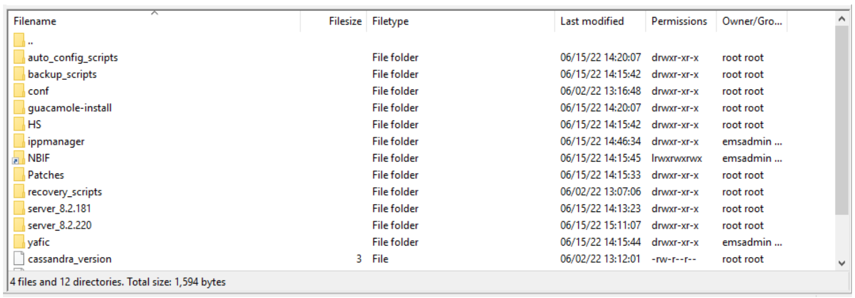
```
Are you sure that you want to collect logs? (y/n) y

--------------------------------

Collecting logs from management server:

Collecting GeneralInfo logs...
Collecting OVOC logs...
Collecting Apache logs + configuration files...
Collecting Cassandra DB logs...
Collecting OS logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting FD information...
Collecting memory statistics...
Collecting Rman Log Files
Collecting Yafic Scan Files
Collecting Tcpdump capture files...
Collecting Postgres DB logs...
Collecting Java dumps...
Collecting Installation Log Files
Collecting Topology File
Collecting ovoc_cluster File
Collecting ovoc_cluster_status File
Collecting Decoded License File
Packing TAR file...
  adding: logs.tar (deflated 94%)

Logs can be found in /home/acems/logs.tar.zip


Press Enter to continue
```

Selected Logs

This options lets you filter the collection of specific types of logs, in addition to the set of Basic logs that are collected by default.

Table 22-1: Log Types

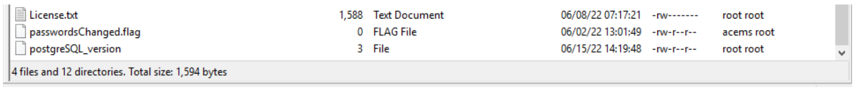
Log Type	Description
OVOC Full Logs	Full set of OVOC logs including all logs described in this table.
Apache Logs	Apache HTTP/S server logs for OVOC server > client connections; OVOC > device connections and for endpoints downloading of firmware and configuration files.
Cassandra Logs	Cassandra database 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 280).
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: 

```
Filename                 Filesize  Filetype     Last modified      Permissions  Owner/Gro...
..
ACEMS                              File folder  06/02/22 12:47:58  lrwxrwxrwx   root root
bin                                File folder  06/02/22 12:44:42  lrwxrwxrwx   root root
boot                               File folder  06/02/22 12:44:38  drwxr-xr-x   root root
data                               File folder  06/02/22 13:15:06  drwxr-xr-x   acems dba
dev                                File folder  06/15/22 14:20:55  drwxr-xr-x   root root
etc                                File folder  06/15/22 15:10:52  drwxr-xr-x   root root
home                               File folder  06/02/22 13:12:48  drwxr-xr-x   root root
lib                                File folder  06/02/22 12:44:42  lrwxrwxrwx   root root
lib64                              File folder  06/02/22 12:44:42  lrwxrwxrwx   root root
media                              File folder  11/05/16 17:38:36  drwxr-xr-x   root root
meta                               File folder  06/02/22 12:44:37  drwxr-xr-x   root root
mnt                                File folder  11/05/16 17:38:36  drwxr-xr-x   root root
opt                                File folder  06/15/22 14:20:02  drwxr-xr-x   root root
2 files and 22 directories. Total size: 1,024 bytes
```

```
Filename                 Filesize  Filetype          Last modified      Permissions  Owner/Gro...
meta                               File folder       06/02/22 12:44:37  drwxr-xr-x   root root
mnt                                File folder       11/05/16 17:38:36  drwxr-xr-x   root root
opt                                File folder       06/15/22 14:20:02  drwxr-xr-x   root root
proc                               File folder       06/15/22 14:20:51  dr-xr-xr-x   root root
root                               File folder       06/15/22 14:55:12  drwx------   root root
run                                File folder       06/15/22 14:23:14  drwxr-xr-x   root root
sbin                               File folder       06/02/22 12:44:42  lrwxrwxrwx   root root
srv                                File folder       11/05/16 17:38:36  drwxr-xr-x   root root
sys                                File folder       06/15/22 14:20:55  dr-xr-xr-x   root root
tmp                                File folder       06/15/22 16:04:39  drwxrwxrwt   root root
usr                                File folder       06/02/22 13:12:07  drwxr-xr-x   root root
var                                File folder       06/15/22 14:20:54  drwxr-xr-x   root root
.autorelabel                    0  AUTORELABEL File  06/02/22 12:48:17  -rw-r--r--   root root
.rnd                        1,024  RND File          06/02/22 13:02:08  -rw-------   root root
2 files and 22 directories. Total size: 1,024 bytes
```

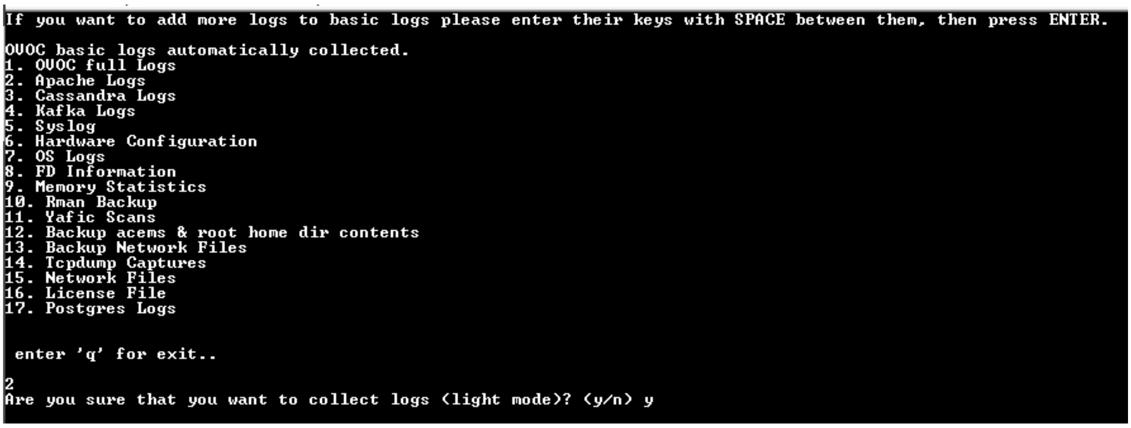
```
Filename                 Filesize  Filetype     Last modified      Permissions  Owner/Gro...
..
auto_config_scripts                File folder  06/15/22 14:20:07  drwxr-xr-x   root root
backup_scripts                     File folder  06/15/22 14:15:42  drwxr-xr-x   root root
conf                               File folder  06/02/22 13:16:48  drwxr-xr-x   root root
guacamole-install                  File folder  06/15/22 14:20:07  drwxr-xr-x   root root
HS                                 File folder  06/15/22 14:15:42  drwxr-xr-x   root root
ippmanager                         File folder  06/15/22 14:46:34  drwxr-xr-x   emsadmin ...
NBIF                               File folder  06/15/22 14:15:45  lrwxrwxrwx   emsadmin ...
Patches                            File folder  06/15/22 14:15:33  drwxr-xr-x   root root
recovery_scripts                   File folder  06/02/22 13:07:06  drwxr-xr-x   root root
server_8.2.181                     File folder  06/15/22 14:13:23  drwxr-xr-x   root root
server_8.2.220                     File folder  06/15/22 15:11:07  drwxr-xr-x   root root
yafic                              File folder  06/15/22 14:15:44  drwxr-xr-x   emsadmin ...
cassandra_version               3  File         06/02/22 13:12:01  -rw-r--r--   root root
4 files and 12 directories. Total size: 1,594 bytes
```

Log Type	Description
	 License.txt 1,588 Text Document 06/08/22 07:17:21 -rw------- root root passwordsChanged.flag 0 FLAG File 06/02/22 13:01:49 -rw-r--r-- acems root postgreSQL_version 3 File 06/15/22 14:19:48 -rw-r--r-- root root 4 files and 12 directories. Total size: 1,594 bytes
Backup Network Files	Network Backup Files
Tcpdump Captures	TCPdump captures
License File	OVOC license file (see OVOC License on page 214).
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 22-3: Select Logs

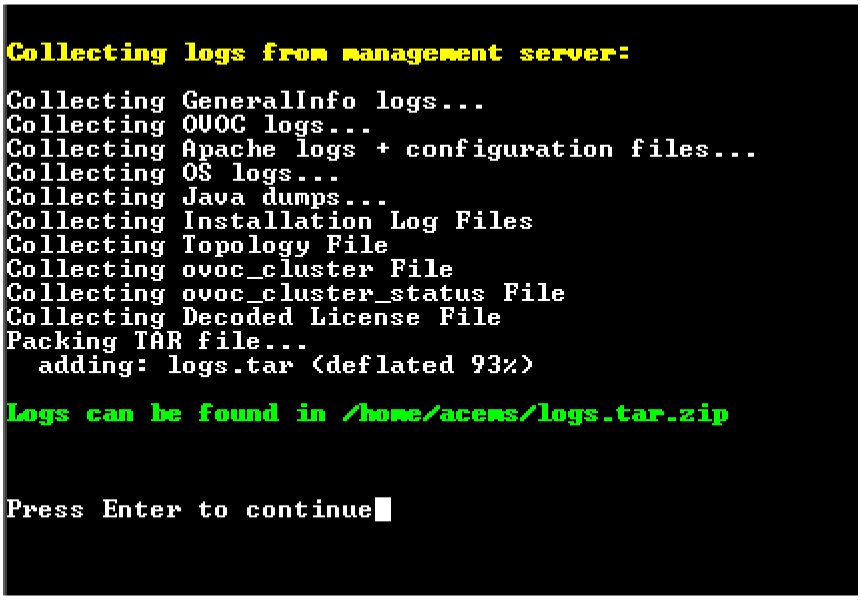


```
If you want to add more logs to basic logs please enter their keys with SPACE between them, then press ENTER.

OVOC basic logs automatically collected.
1. OVOC full Logs
2. Apache Logs
3. Cassandra Logs
4. Kafka Logs
5. Syslog
6. Hardware Configuration
7. OS Logs
8. FD Information
9. Memory Statistics
10. Rman Backup
11. Yafic Scans
12. Backup acems & root home dir contents
13. Backup Network Files
14. Tcpdump Captures
15. Network Files
16. License File
17. Postgres Logs

 enter 'q' for exit..

2
Are you sure that you want to collect logs (light mode)? (y/n) y
```

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 22-4: Log Directory

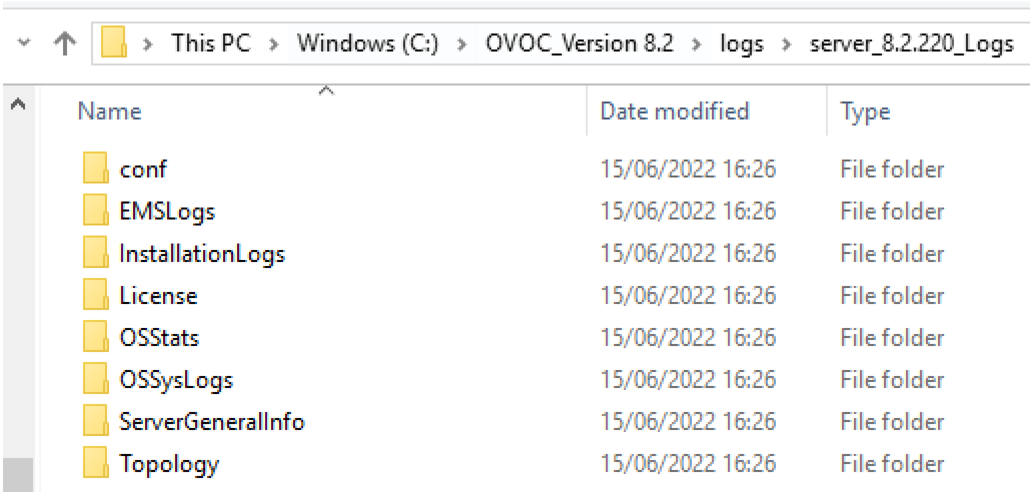


```
Collecting logs from management server:

Collecting GeneralInfo logs...
Collecting OVOC logs...
Collecting Apache logs + configuration files...
Collecting OS logs...
Collecting Java dumps...
Collecting Installation Log Files
Collecting Topology File
Collecting ovoc_cluster File
Collecting ovoc_cluster_status File
Collecting Decoded License File
Packing TAR file...
  adding: logs.tar (deflated 93%)

Logs can be found in /home/acems/logs.tar.zip


Press Enter to continue
```

3. Transfer the log file to your desired location (see Transferring Files on page 326).

   The following screen shows the contents of the extracted tar file for the "OVOC Full Logs" directory:

Figure 22-5: OVOC "Full Logs"



This PC › Windows (C:) › OVOC_Version 8.2 › logs › server_8.2.220_Logs

Name	Date modified	Type
conf	15/06/2022 16:26	File folder
EMSLogs	15/06/2022 16:26	File folder
InstallationLogs	15/06/2022 16:26	File folder
License	15/06/2022 16:26	File folder
OSStats	15/06/2022 16:26	File folder
OSSysLogs	15/06/2022 16:26	File folder
ServerGeneralInfo	15/06/2022 16:26	File folder
Topology	15/06/2022 16:26	File folder

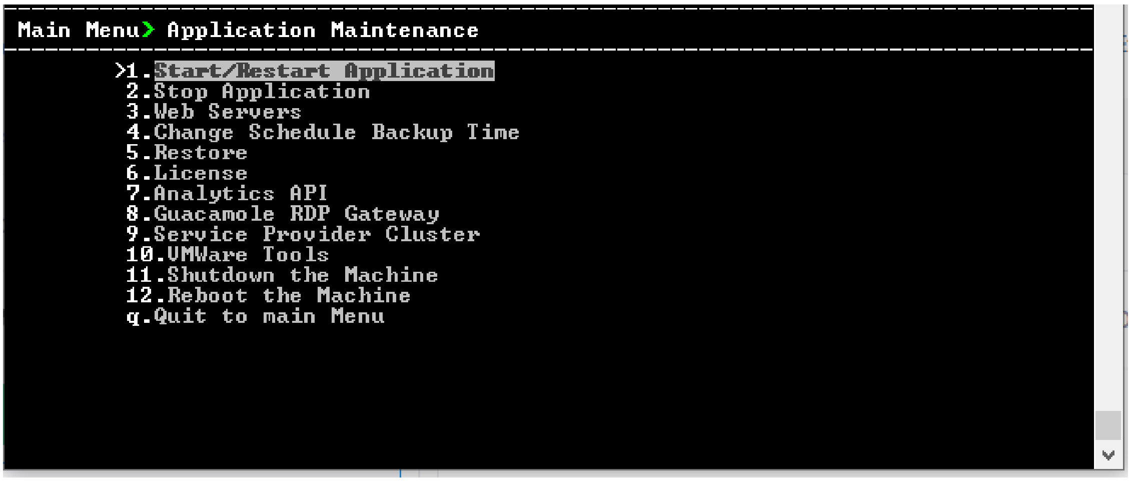
23 Application Maintenance

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 23-1: Application Maintenance



```
Main Menu> Application Maintenance
        >1.Start/Restart Application
         2.Stop Application
         3.Web Servers
         4.Change Schedule Backup Time
         5.Restore
         6.License
         7.Analytics API
         8.Guacamole RDP Gateway
         9.Service Provider Cluster
         10.VMWare Tools
         11.Shutdown the Machine
         12.Reboot the Machine
         q.Quit to main Menu
```

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 213)
- Change Schedule Backup Time (Change Schedule Backup Time on page 189)
- Restore (OVOC Server Restore on page 191)
- License (License on page 213)
- analytics API (analytics API on page 218)
- Guacamole RDP Gateway (Guacamole RDP Gateway on page 219)
- VMware Tools (see VMware Tools on page 221
- Shutdown the Machine (Shutdown the OVOC Server Machine on page 222)
- Reboot the Machine (Reboot the OVOC Server Machine on page 222)

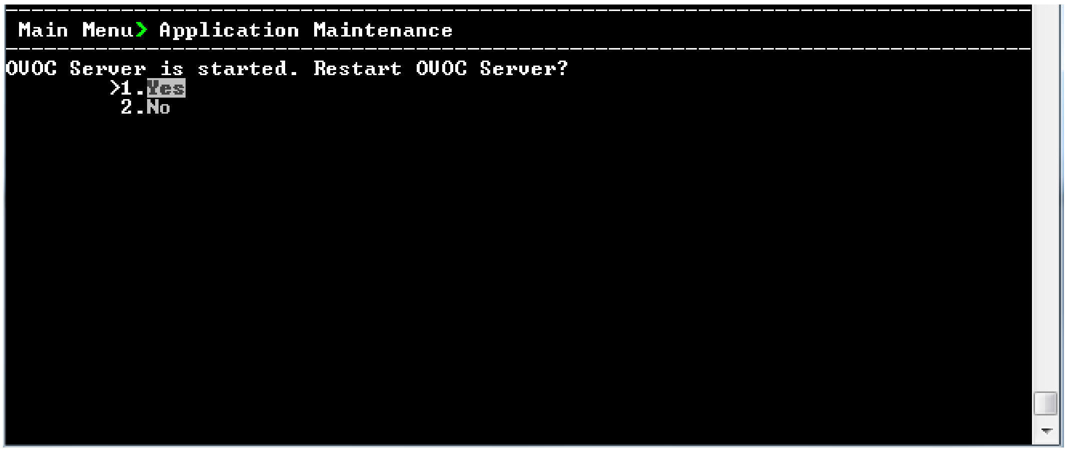
Start or Restart the Application

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 23-2: Start or Restart the OVOC server



```
 Main Menu> Application Maintenance
OVOC Server is started. Restart OVOC Server?
        >1.Yes
         2.No
```

2. Do one of the following:
   - Select **Yes** to start/restart the OVOC server.
   - Select **No** to return to menu.

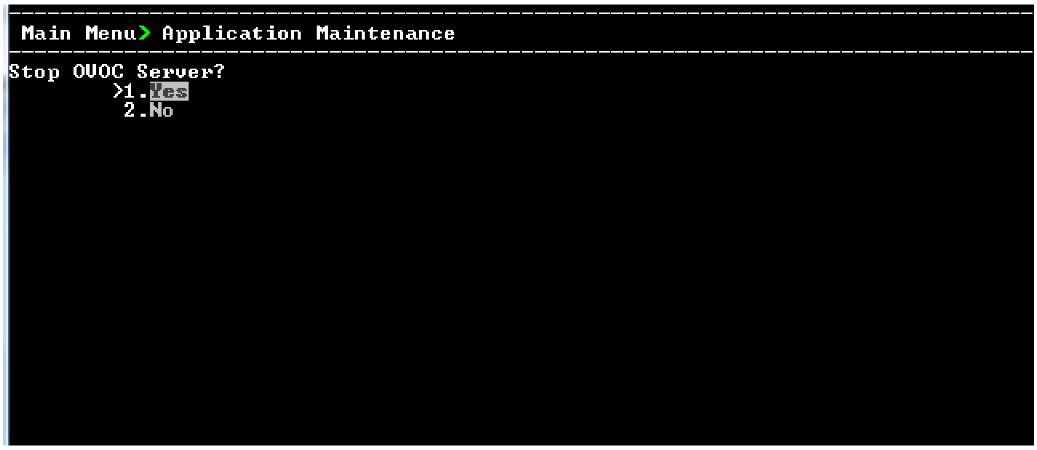
Stop the Application

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 23-3: Stop OVOC server



```
 Main Menu> Application Maintenance
Stop OVOC Server?
        >1.Yes
         2.No
```

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

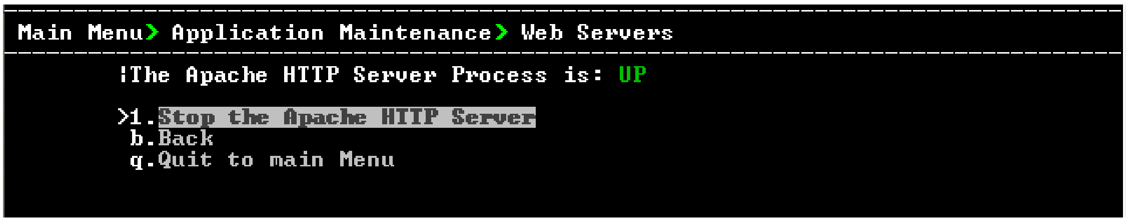
Web Servers

This option enables you to stop and start the Apache HTTP Web server.

➢ **To stop/start the Apache HTTP Web server:**

1. From the Application maintenance menu, choose **Web Servers**, and then press Enter.

Figure 23-4: Web Servers



```
Main Menu> Application Maintenance> Web Servers
        |The Apache HTTP Server Process is: UP

        >1.Stop the Apache HTTP Server
         b.Back
         q.Quit to main Menu
```

2. Select option **Stop/Start the Apache HTTP Server**, and then press Enter.

License

The License menu enables you to view the details of the existing license or upload a new license.

The OVOC server License (SBC License pool, IP Phones and Voice Quality) should have a valid license loaded to the server in order for it to be fully operational.

To obtain a valid license for your OVOC server License you should activate your product through License Activation tool at 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 244).

> ⚠
> - 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)*.

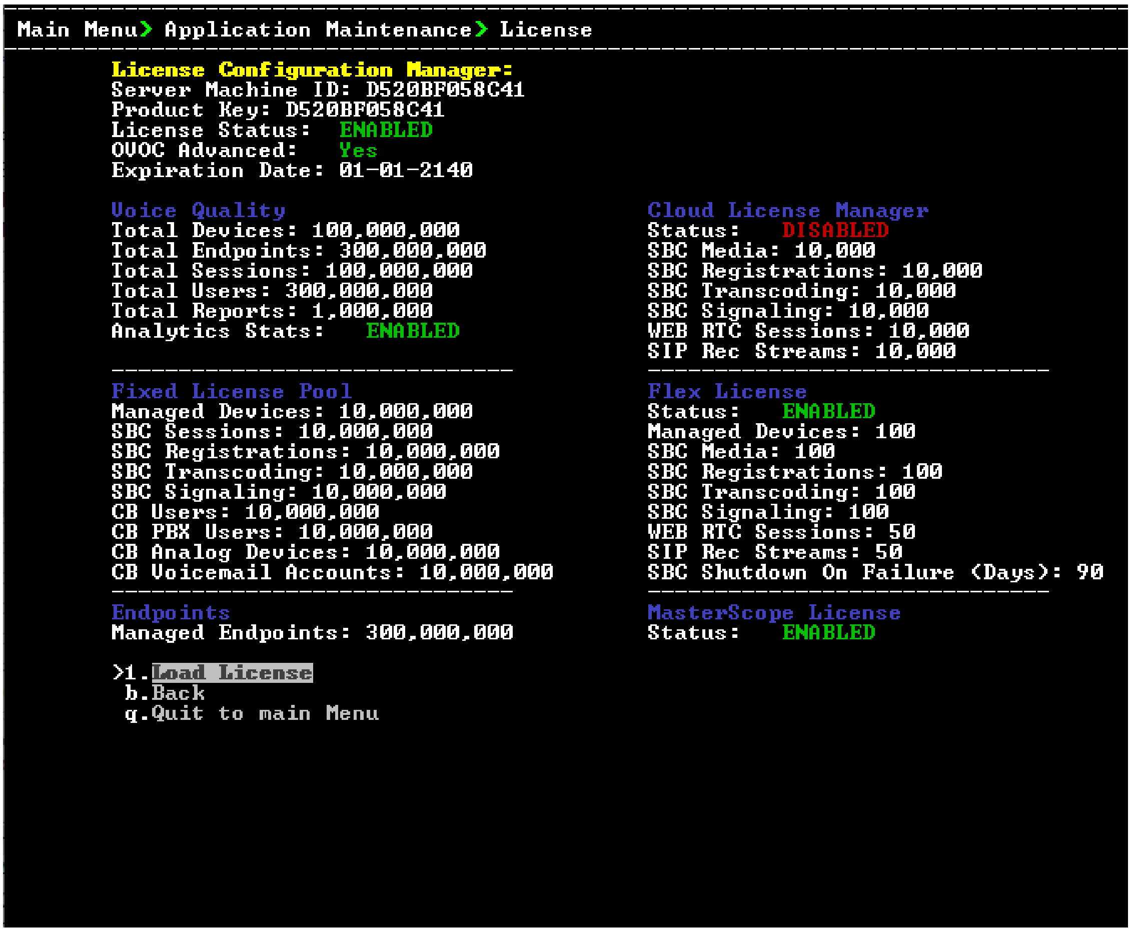
➢ To view the license details or upload a new license:

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 23-5: License Manager



```
Main Menu> Application Maintenance> License

       License Configuration Manager:
       Server Machine ID: D520BF058C41
       Product Key: D520BF058C41
       License Status:  ENABLED
       OVOC Advanced:   Yes
       Expiration Date: 01-01-2140

       Voice Quality                           Cloud License Manager
       Total Devices: 100,000,000              Status:   DISABLED
       Total Endpoints: 300,000,000            SBC Media: 10,000
       Total Sessions: 100,000,000             SBC Registrations: 10,000
       Total Users: 300,000,000                SBC Transcoding: 10,000
       Total Reports: 1,000,000                SBC Signaling: 10,000
       Analytics Stats:   ENABLED              WEB RTC Sessions: 10,000
                                               SIP Rec Streams: 10,000
       ------------------------------          ------------------------------
       Fixed License Pool                      Flex License
       Managed Devices: 10,000,000             Status:   ENABLED
       SBC Sessions: 10,000,000                Managed Devices: 100
       SBC Registrations: 10,000,000           SBC Media: 100
       SBC Transcoding: 10,000,000             SBC Registrations: 100
       SBC Signaling: 10,000,000               SBC Transcoding: 100
       CB Users: 10,000,000                    SBC Signaling: 100
       CB PBX Users: 10,000,000                WEB RTC Sessions: 50
       CB Analog Devices: 10,000,000           SIP Rec Streams: 50
       CB Voicemail Accounts: 10,000,000       SBC Shutdown On Failure (Days): 90
       ------------------------------          ------------------------------
       Endpoints                               MasterScope License
       Managed Endpoints: 300,000,000          Status:   ENABLED

       >1.Load License
        b.Back
        q.Quit to main Menu
```

Table 23-1: 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.

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 214) and in the procedure described below.

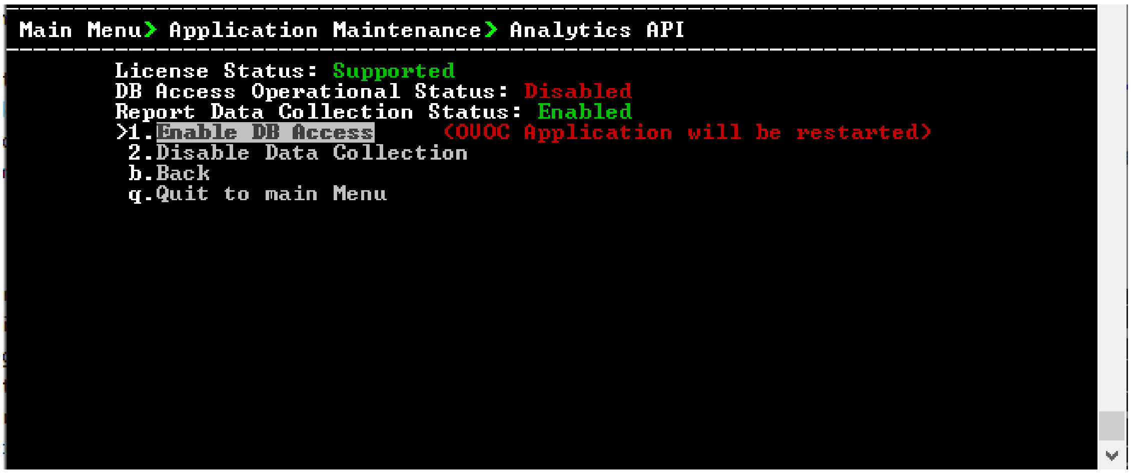
For more information, refer to OVOC Northbound Integration Guide.

➢ 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 23-6: analytics API



```
Main Menu> Application Maintenance> Analytics API

        License Status: Supported
        DB Access Operational Status: Disabled
        Report Data Collection Status: Enabled
        >1.Enable DB Access      (OVOC Application will be restarted)
         2.Disable Data Collection
         b.Back
         q.Quit to main Menu
```

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.

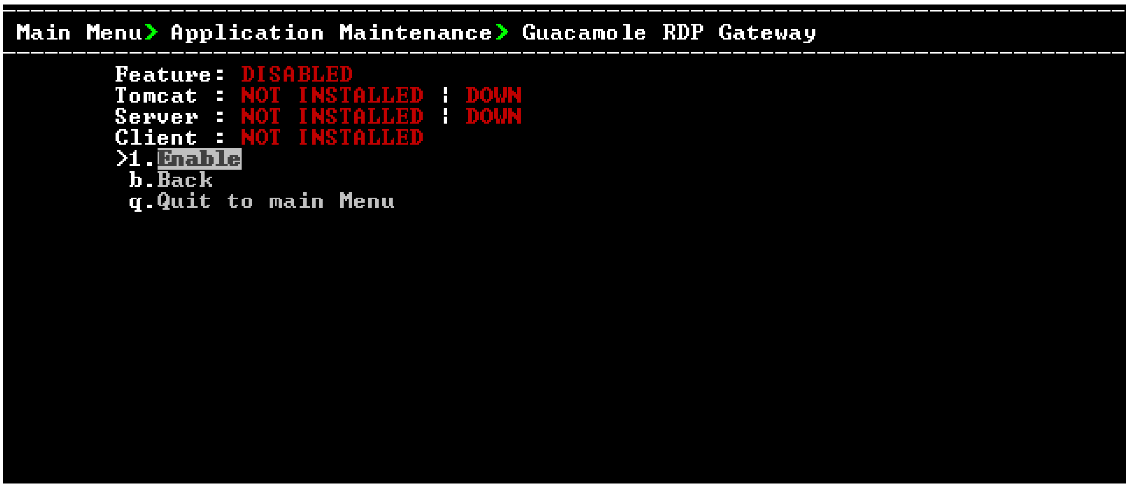
Guacamole RDP Gateway

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 23-7: Guacamole RDP Gateway

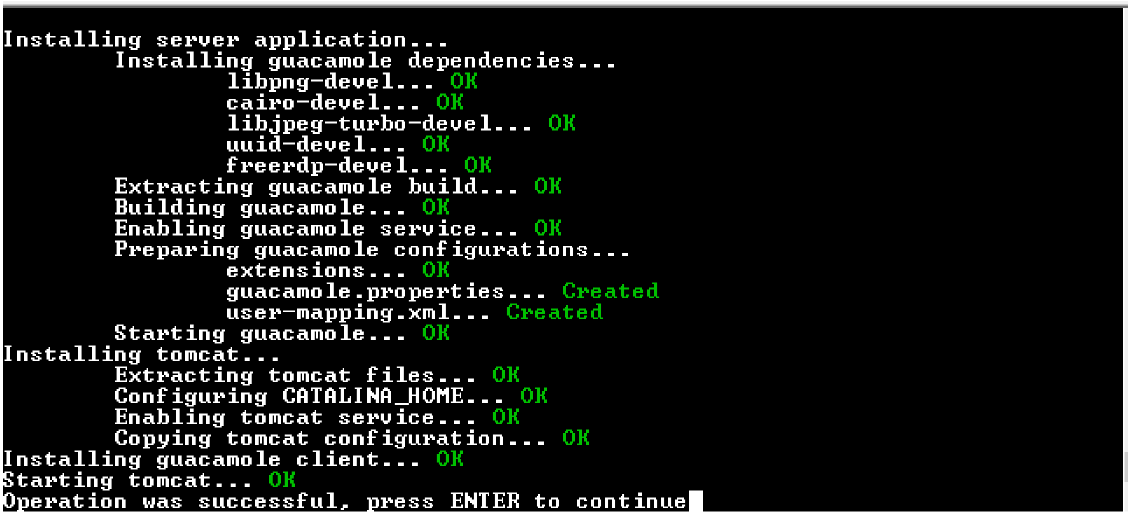


```
Main Menu> Application Maintenance> Guacamole RDP Gateway
--------------------------------------------------------------------------------
        Feature: DISABLED
        Tomcat : NOT INSTALLED | DOWN
        Server : NOT INSTALLED | DOWN
        Client : NOT INSTALLED
        >1.Enable
         b.Back
         q.Quit to main Menu
```

2. Select Option **1** to enable the RDP Gateway.

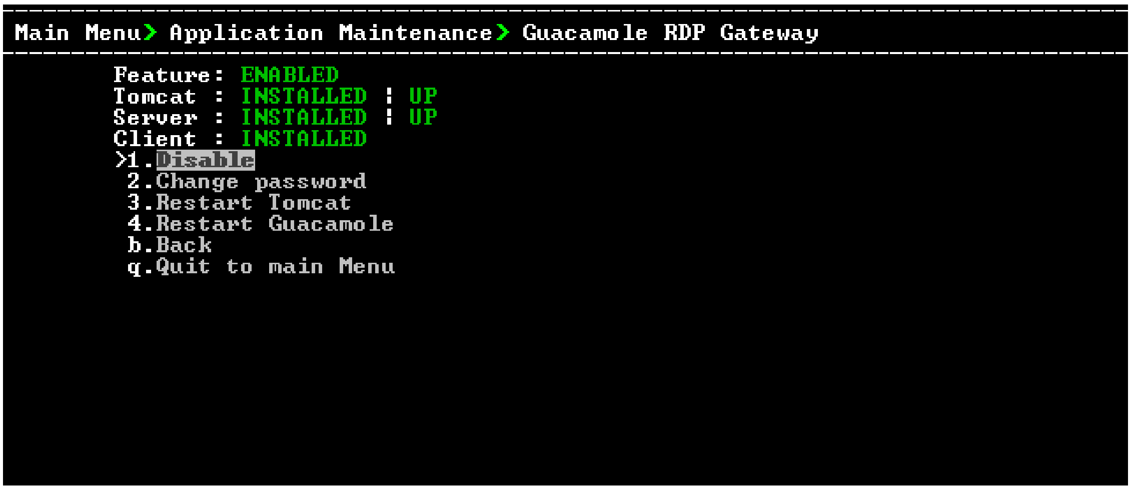
   The gateway is built and installed.

Figure 23-8: Building and Installing RDP Gateway



```
Installing server application...
        Installing guacamole dependencies...
                libpng-devel... OK
                cairo-devel... OK
                libjpeg-turbo-devel... OK
                uuid-devel... OK
                freerdp-devel... OK
        Extracting guacamole build... OK
        Building guacamole... OK
        Enabling guacamole service... OK
        Preparing guacamole configurations...
                extensions... OK
                guacamole.properties... Created
                user-mapping.xml... Created
        Starting guacamole... OK
Installing tomcat...
        Extracting tomcat files... OK
        Configuring CATALINA_HOME... OK
        Enabling tomcat service... OK
        Copying tomcat configuration... OK
Installing guacamole client... OK
Starting tomcat... OK
Operation was successful, press ENTER to continue
```

Figure 23-9: Enabled Guacamole RDP Gateway



```
Main Menu> Application Maintenance> Guacamole RDP Gateway
--------------------------------------------------------------------------------
        Feature: ENABLED
        Tomcat : INSTALLED | UP
        Server : INSTALLED | UP
        Client : INSTALLED
        >1.Disable
         2.Change password
         3.Restart Tomcat
         4.Restart Guacamole
         b.Back
         q.Quit to main Menu
```

3. Do one of the following:

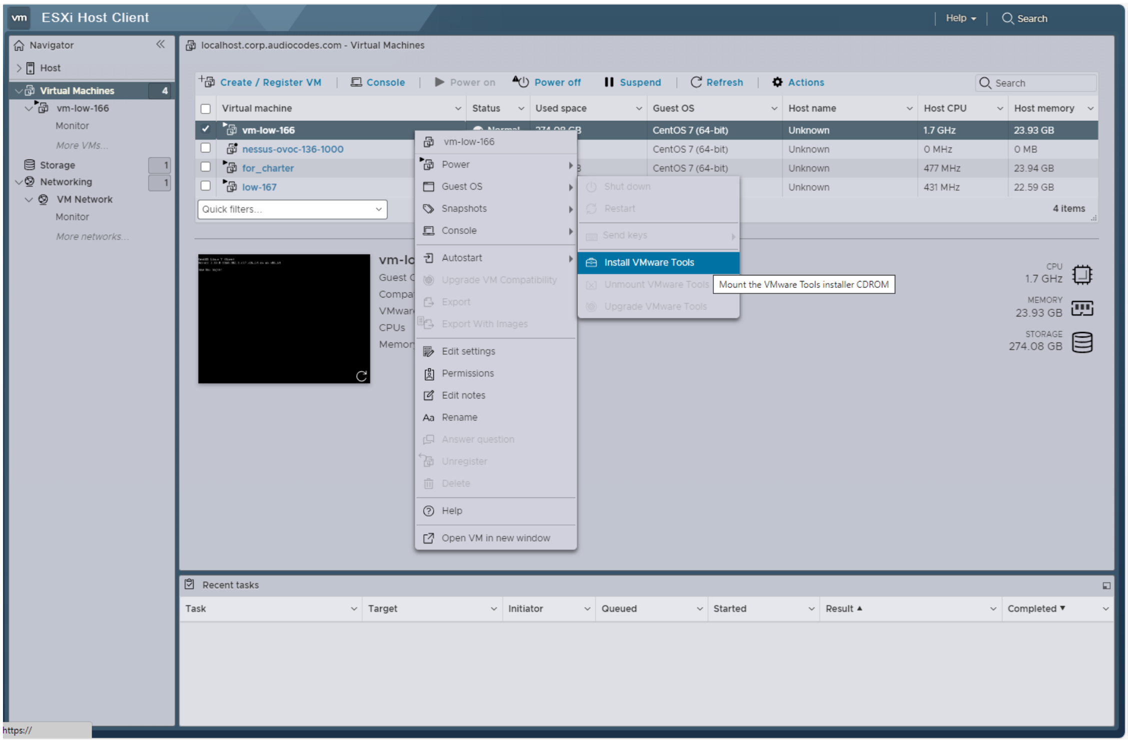
- **Change password:** Select Option **2**, enter the current password, enter new password and confirm (default username *umpman*, default password: *umppass*)
- **Restart Tomcat:** Select Option **3** and confirm.
- **Restart Guacomole:** Select Option **4** and confirm.

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.

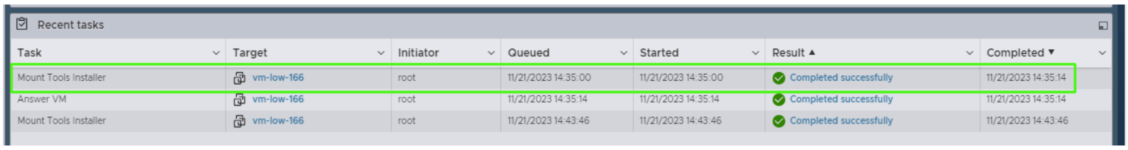
➢ To install VMware tools:

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



Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
vm-low-166			CentOS 7 (64-bit)	Unknown	1.7 GHz	23.93 GB
nessus-ovoc-136-1000			CentOS 7 (64-bit)	Unknown	0 MHz	0 MB
for_charter			CentOS 7 (64-bit)	Unknown	477 MHz	23.94 GB
low-167				Unknown	431 MHz	22.59 GB

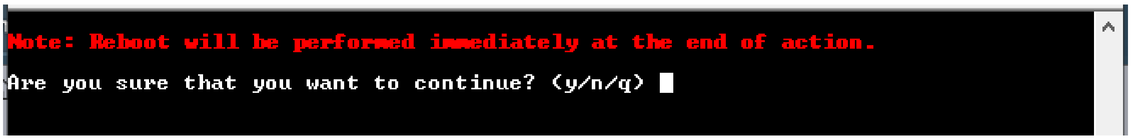
The Completed Successfully indication is displayed in the Task pane:



Recent tasks

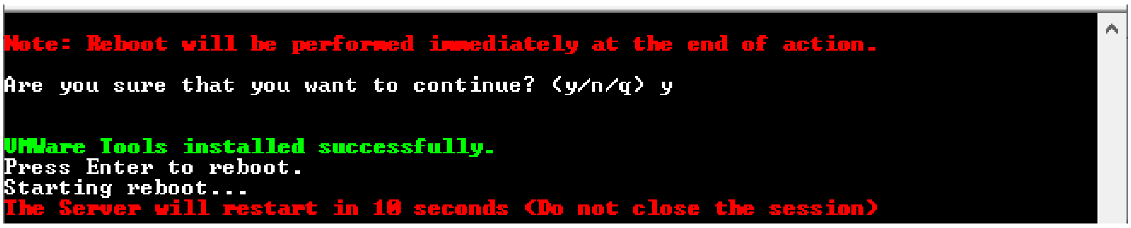
Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Mount Tools Installer	vm-low-166	root	11/21/2023 14:35:00	11/21/2023 14:35:00	✓ Completed successfully	11/21/2023 14:35:14
Answer VM	vm-low-166	root	11/21/2023 14:35:14	11/21/2023 14:35:14	✓ Completed successfully	11/21/2023 14:35:14
Mount Tools Installer	vm-low-166	root	11/21/2023 14:43:46	11/21/2023 14:43:46	✓ Completed successfully	11/21/2023 14:43:46

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



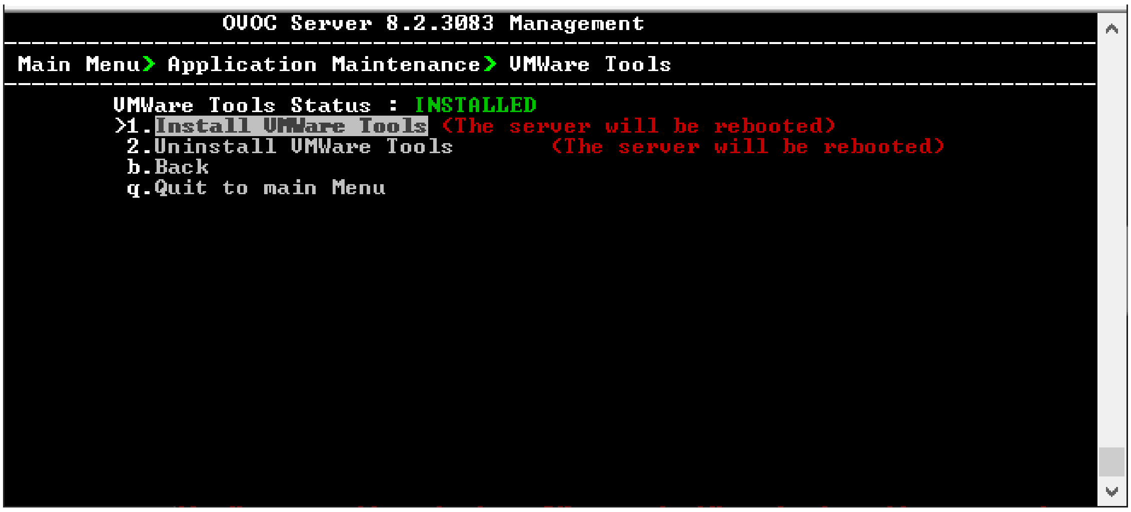
```
Note: Reboot will be performed immediately at the end of action.

Are you sure that you want to continue? (y/n/q)
```

4. Type **y** to confirm. The server is restarted.



```
Note: Reboot will be performed immediately at the end of action.

Are you sure that you want to continue? (y/n/q) y

VMWare Tools installed successfully.
Press Enter to reboot.
Starting reboot...
The Server will restart in 10 seconds (Do not close the session)
```

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**.



```
                OVOC Server 8.2.3083 Management
--------------------------------------------------------------------------------
 Main Menu> Application Maintenance> VMWare Tools
--------------------------------------------------------------------------------
        VMWare Tools Status : INSTALLED
        >1.Install VMWare Tools (The server will be rebooted)
         2.Uninstall VMWare Tools        (The server will be rebooted)
         b.Back
         q.Quit to main Menu
```

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.

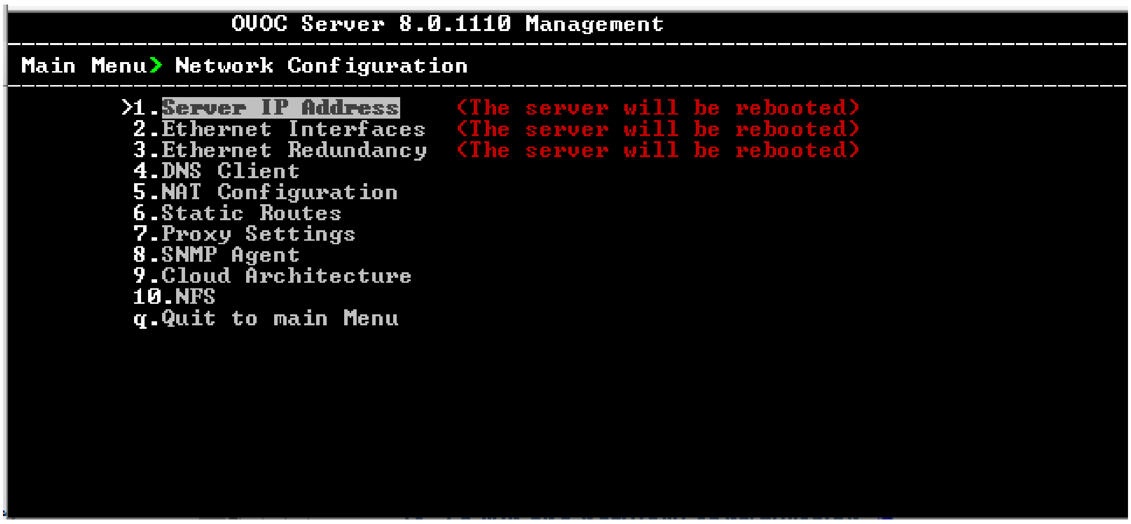
24 Network Configuration

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 24-1: Network Configuration



```
                OVOC Server 8.0.1110 Management
--------------------------------------------------------------------------
 Main Menu> Network Configuration
--------------------------------------------------------------------------
        >1.Server IP Address    (The server will be rebooted)
         2.Ethernet Interfaces  (The server will be rebooted)
         3.Ethernet Redundancy  (The server will be rebooted)
         4.DNS Client
         5.NAT Configuration
         6.Static Routes
         7.Proxy Settings
         8.SNMP Agent
         9.Cloud Architecture
         10.NFS
         q.Quit to main Menu
```

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 226)
- Ethernet Redundancy (the server will be rebooted) (Ethernet Redundancy on page 228)
- DNS Client (DNS Client on page 231)
- NAT (Configure OVOC Server with NAT IP Address per Interface on page 148)
- Static Routes (Static Routes on page 232)
- OVOC Proxy Settings (Proxy Settings on page 235)
- SNMP Agent (SNMP Agent on page 236)
- Cloud Architecture (Configure OVOC Cloud Architecture Mode (WebSocket Tunnel) on page 152)
- NFS (NFS on page 239)

- 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

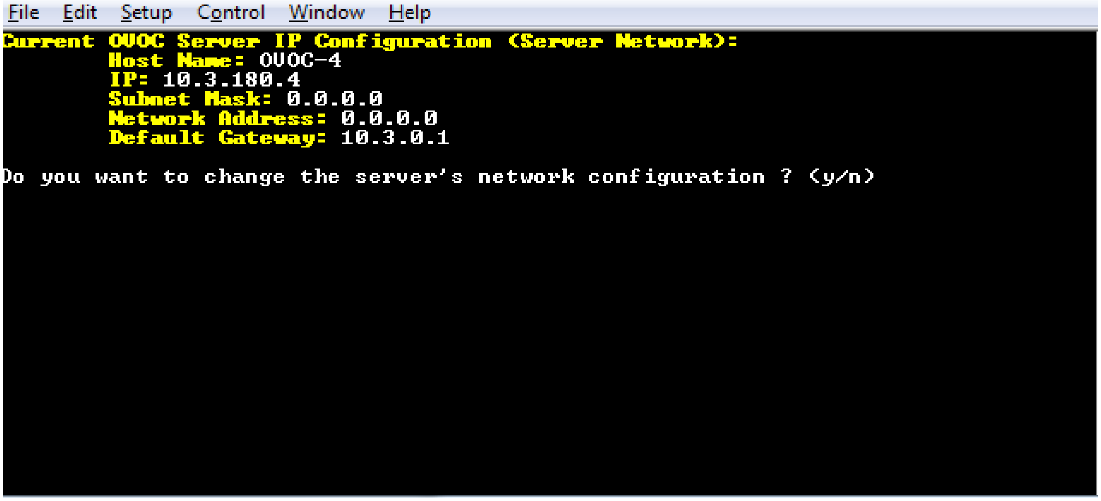
This option enables you to update the OVOC server's IP address. This option also enables you to modify the OVOC server host name.

- 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 24-2: OVOC Server Manager – Change Server's IP Address



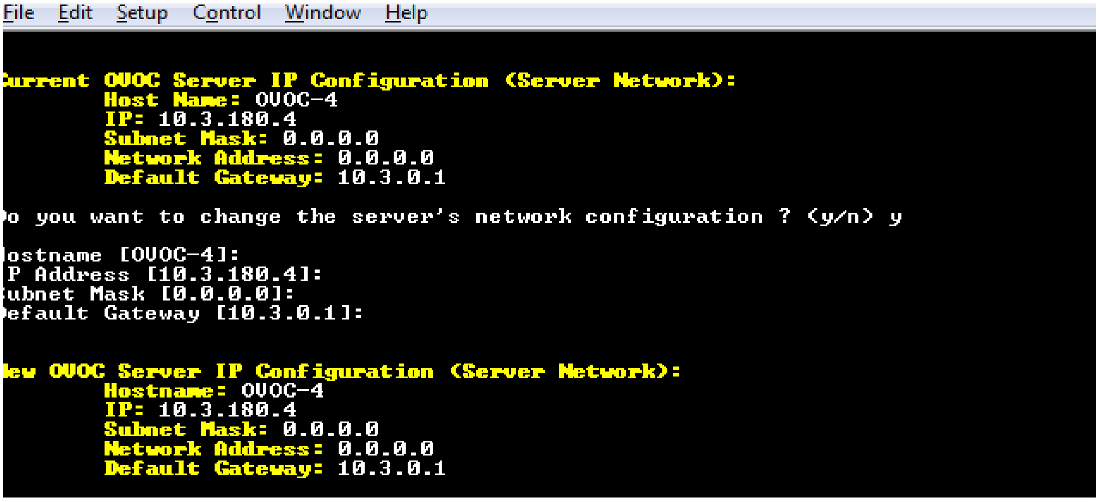
```
Current OVOC Server IP Configuration (Server Network):
        Host Name: OVOC-4
        IP: 10.3.180.4
        Subnet Mask: 0.0.0.0
        Network Address: 0.0.0.0
        Default Gateway: 10.3.0.1

Do you want to change the server's network configuration ? (y/n)
```

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 24-3: IP Configuration Complete



```
urrent OVOC Server IP Configuration (Server Network):
         Host Name: OVOC-4
         IP: 10.3.180.4
         Subnet Mask: 0.0.0.0
         Network Address: 0.0.0.0
         Default Gateway: 10.3.0.1

o you want to change the server's network configuration ? (y/n) y

ostname [OVOC-4]:
P Address [10.3.180.4]:
ubnet Mask [0.0.0.0]:
efault Gateway [10.3.0.1]:

ew OVOC Server IP Configuration (Server Network):
         Hostname: OVOC-4
         IP: 10.3.180.4
         Subnet Mask: 0.0.0.0
         Network Address: 0.0.0.0
         Default Gateway: 10.3.0.1
```

Upon confirmation, the OVOC automatically reboots for the changes to take effect.

Ethernet Interfaces

This section describes the maintenance actions for managing multiple ethernet interfaces.

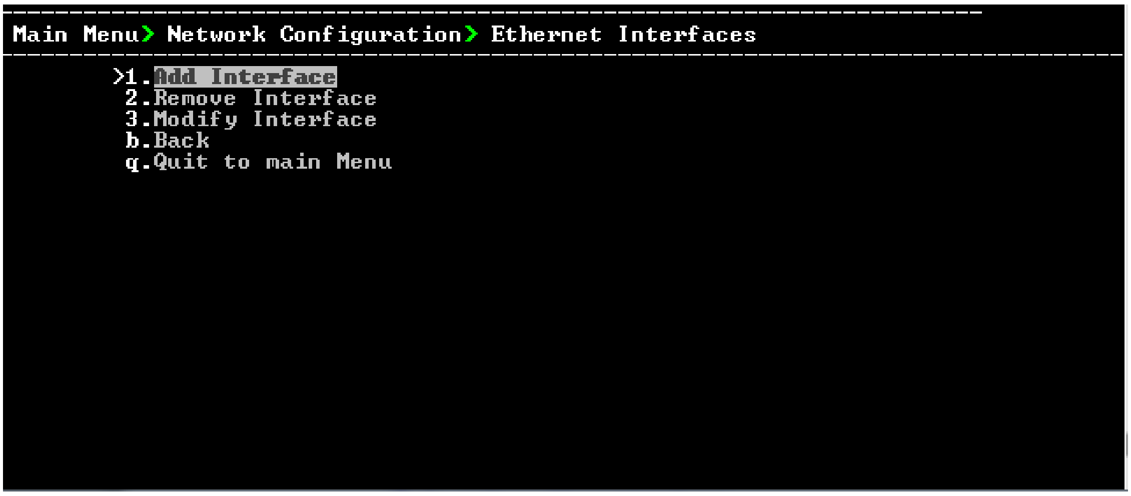
- The OVOC Main Management interface only supports IPv4.
- Each IPv4 interface can be configured for NAT and one of the IPv4 interfaces can be configured to work in the Cloud Architecture mode.

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 232.

➢ To configure Ethernet Interfaces:

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

Figure 24-4: OVOC Server Manager – Configure Ethernet Interfaces



```
Main Menu> Network Configuration> Ethernet Interfaces

        >1.Add Interface
         2.Remove Interface
         3.Modify Interface
         b.Back
         q.Quit to main Menu
```

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 156).
- **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).

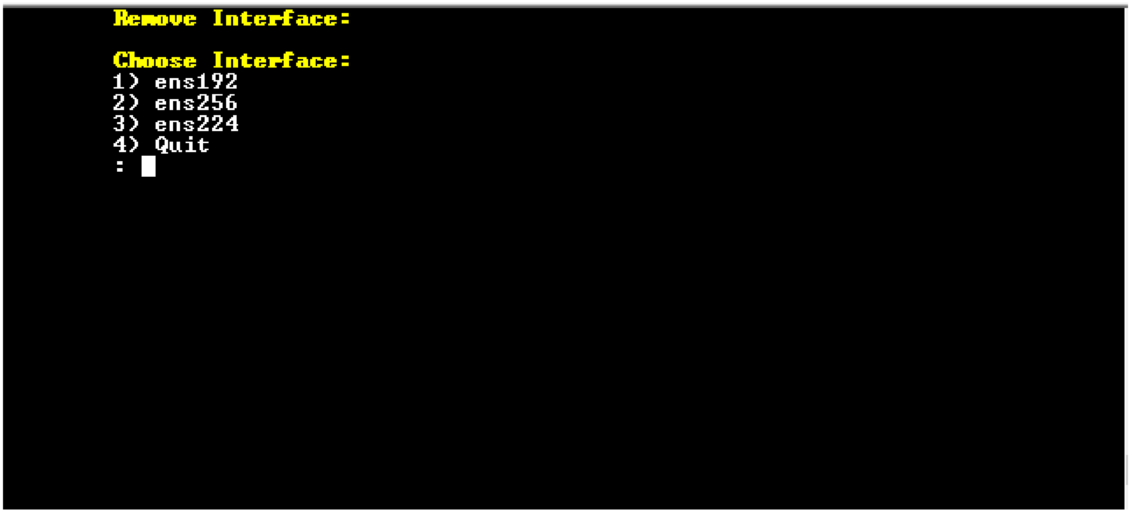
Remove Interface

This section describes how to remove an Ethernet Interface.

➢ To remove an existing interface:

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

Figure 24-5: Remove Ethernet Interface



```
Remove Interface:

Choose Interface:
1) ens192
2) ens256
3) ens224
4) Quit
:
```

2. Enter the number corresponding to the interface that you wish to remove.
3. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

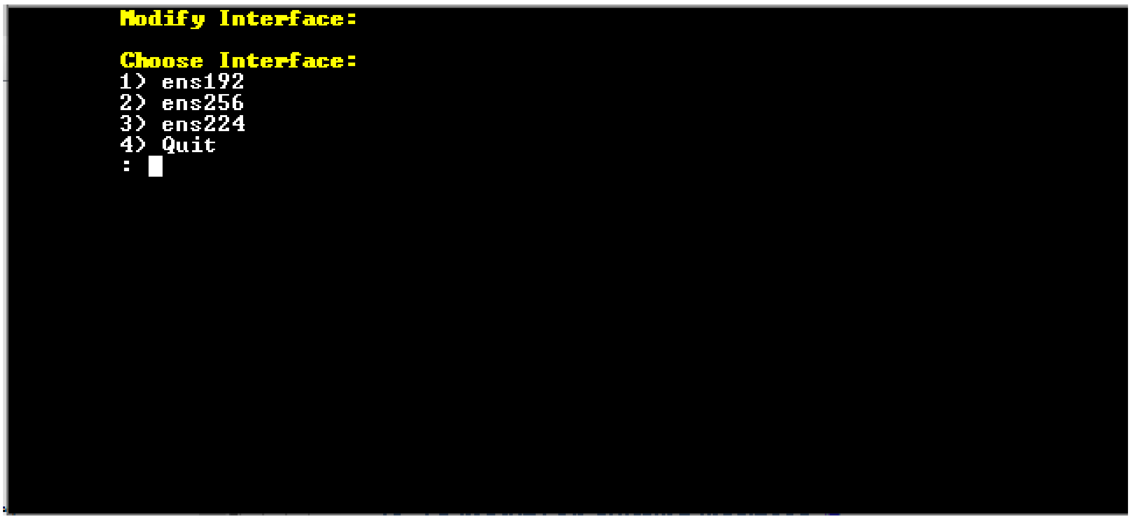
Modify Interface

This section describes how to modify an existing Ethernet Interface.

➢ To modify an existing interface:

1. From the Ethernet Interfaces menu, choose option **3**.

Figure 24-6: Modify Interface



```
Modify Interface:

Choose Interface:
1) ens192
2) ens256
3) ens224
4) Quit
:
```

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

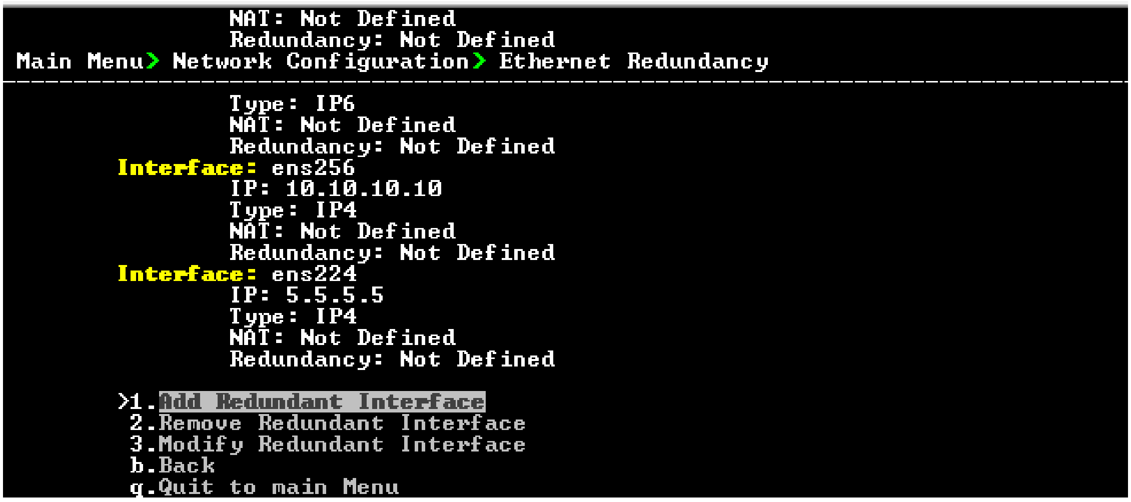
This section describes how to configure Ethernet Redundancy. Physical Ethernet Interfaces Redundancy balances traffic between multiple network interfaces that are connected to the same IP link and provides a failover mechanism.

> ⚠ 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 24-7: Ethernet Redundancy Configuration



```
                NAT: Not Defined
                Redundancy: Not Defined
Main Menu> Network Configuration> Ethernet Redundancy
--------------------------------------------------------------------------------
                Type: IP6
                NAT: Not Defined
                Redundancy: Not Defined
        Interface: ens256
                IP: 10.10.10.10
                Type: IP4
                NAT: Not Defined
                Redundancy: Not Defined
        Interface: ens224
                IP: 5.5.5.5
                Type: IP4
                NAT: Not Defined
                Redundancy: Not Defined

        >1.Add Redundant Interface
         2.Remove Redundant Interface
         3.Modify Redundant Interface
         b.Back
         q.Quit to main Menu
```

2. This menu includes the following options:

- Add Redundant Interface (Add Redundant Interface below).
- Remove Redundant Interface (Remove Ethernet Redundancy on the next page).
- Modify Redundant Interface (Modify Redundant Interface on page 231).

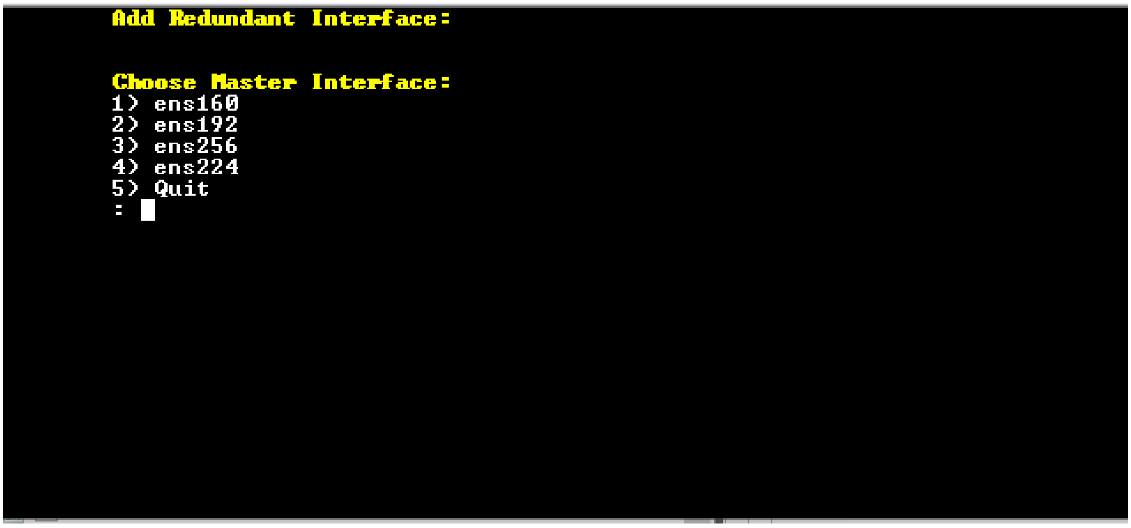
Add Redundant Interface

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.

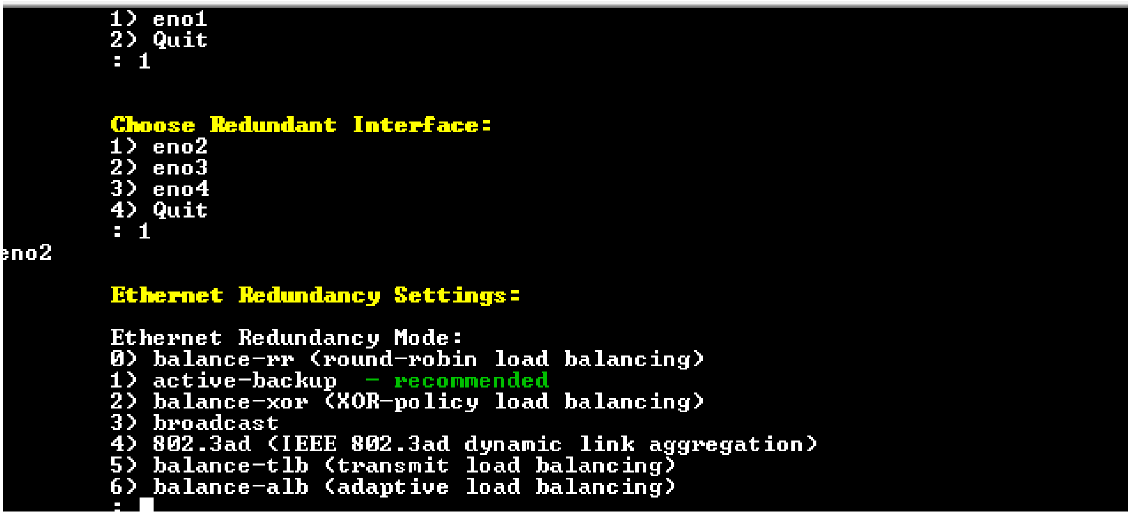
Figure 24-8: Add Redundant Interface



```
        Add Redundant Interface:

        Choose Master Interface:
        1) ens160
        2) ens192
        3) ens256
        4) ens224
        5) Quit
        :
```

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

Figure 24-9: Ethernet Redundancy Mode

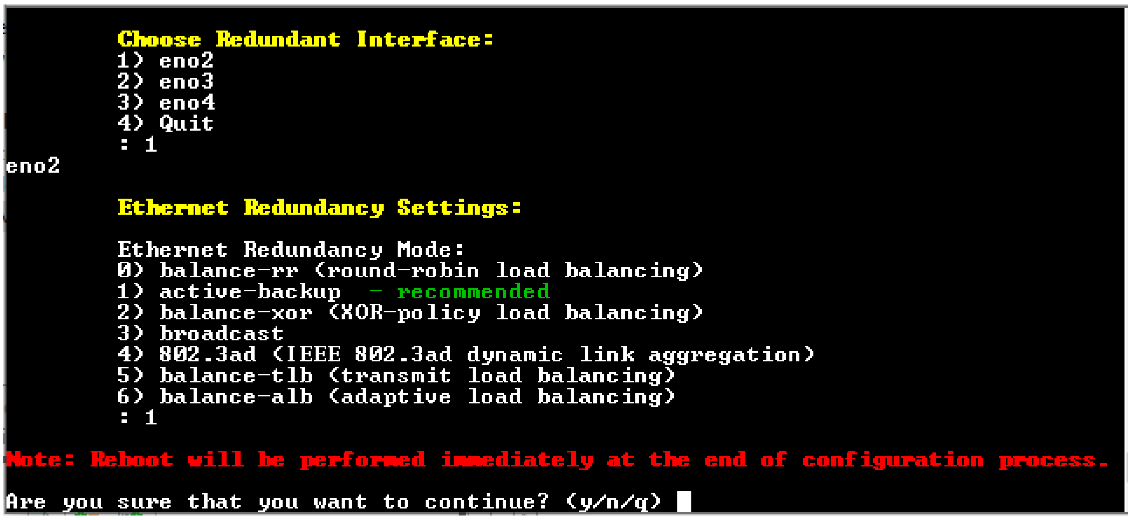


```
        1) eno1
        2) Quit
        : 1


        Choose Redundant Interface:
        1) eno2
        2) eno3
        3) eno4
        4) Quit
        : 1
eno2

        Ethernet Redundancy Settings:

        Ethernet Redundancy Mode:
        0) balance-rr (round-robin load balancing)
        1) active-backup   - recommended
        2) balance-xor (XOR-policy load balancing)
        3) broadcast
        4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
        5) balance-tlb (transmit load balancing)
        6) balance-alb (adaptive load balancing)
        :
```

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 24-10: Confirm Ethernet Redundancy Update



```
        Choose Redundant Interface:
        1) eno2
        2) eno3
        3) eno4
        4) Quit
        : 1
eno2

        Ethernet Redundancy Settings:

        Ethernet Redundancy Mode:
        0) balance-rr (round-robin load balancing)
        1) active-backup   - recommended
        2) balance-xor (XOR-policy load balancing)
        3) broadcast
        4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
        5) balance-tlb (transmit load balancing)
        6) balance-alb (adaptive load balancing)
        : 1
Note: Reboot will be performed immediately at the end of configuration process.

Are you sure that you want to continue? (y/n/q)
```

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

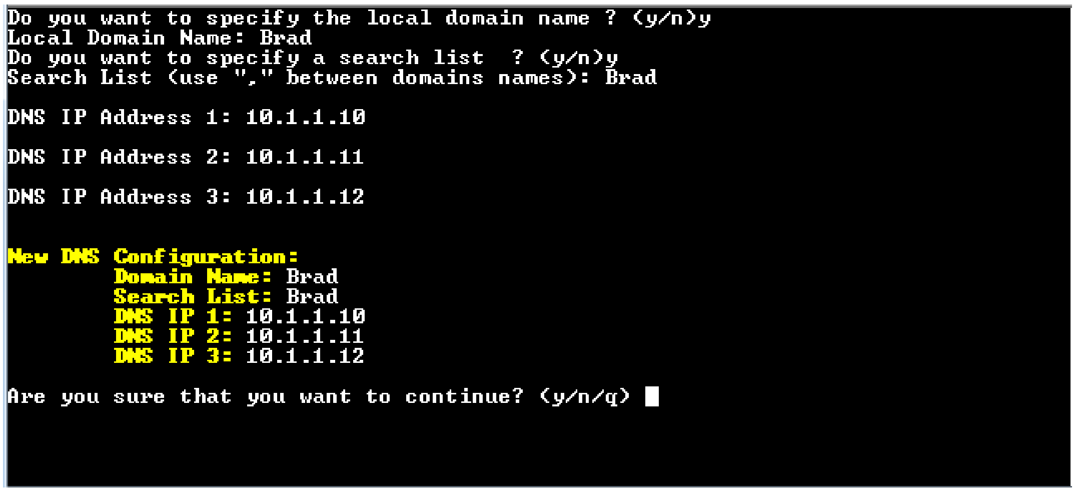
Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

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 24-11: DNS Setup



```
Do you want to specify the local domain name ? (y/n)y
Local Domain Name: Brad
Do you want to specify a search list  ? (y/n)y
Search List (use "," between domains names): Brad

DNS IP Address 1: 10.1.1.10

DNS IP Address 2: 10.1.1.11

DNS IP Address 3: 10.1.1.12


New DNS Configuration:
        Domain Name: Brad
        Search List: Brad
        DNS IP 1: 10.1.1.10
        DNS IP 2: 10.1.1.11
        DNS IP 3: 10.1.1.12

Are you sure that you want to continue? (y/n/q)
```

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.

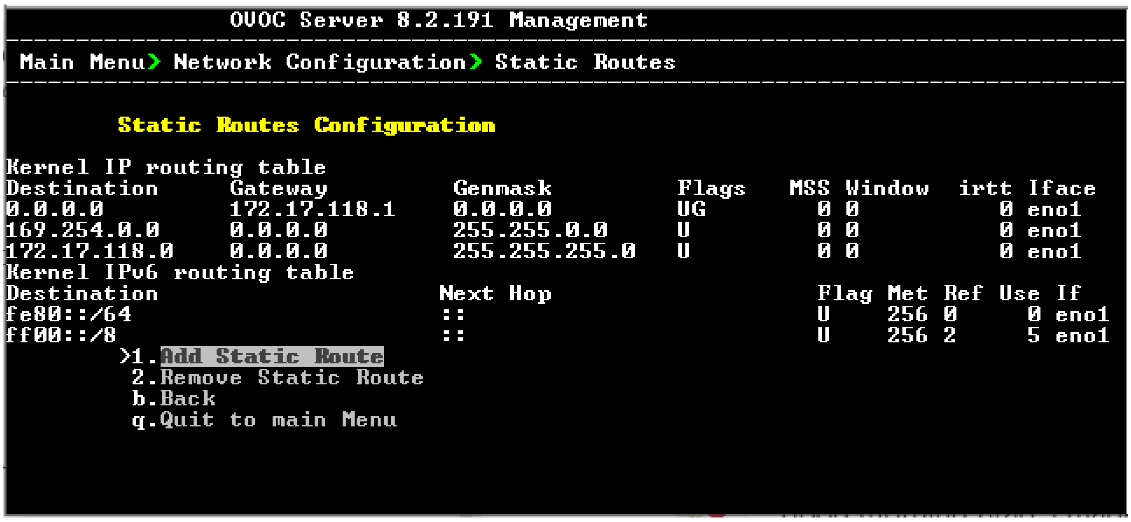
Static Routes

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 24-12: Routing Table and Menu



```
                OVOC Server 8.2.191 Management
--------------------------------------------------------------------------------
 Main Menu> Network Configuration> Static Routes
--------------------------------------------------------------------------------

        Static Routes Configuration

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.17.118.1    0.0.0.0         UG        0 0          0 eno1
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eno1
172.17.118.0    0.0.0.0         255.255.255.0   U         0 0          0 eno1
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
fe80::/64                      ::                         U    256 0     0 eno1
ff00::/8                       ::                         U    256 2     5 eno1
        >1.Add Static Route
         2.Remove Static Route
         b.Back
         q.Quit to main Menu
```

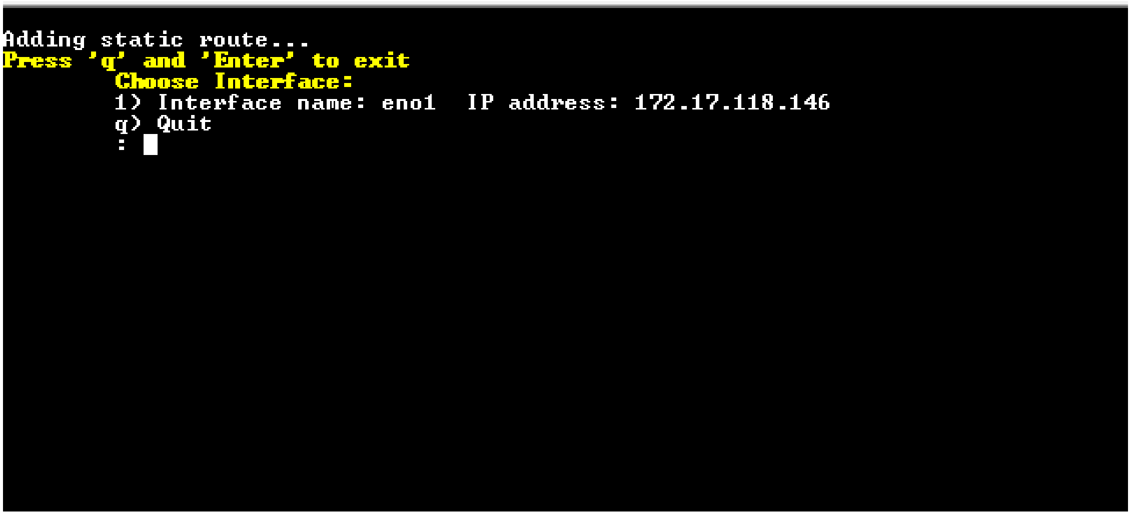
2. From the Static Routes configuration screen, choose one of the following options:

- 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.

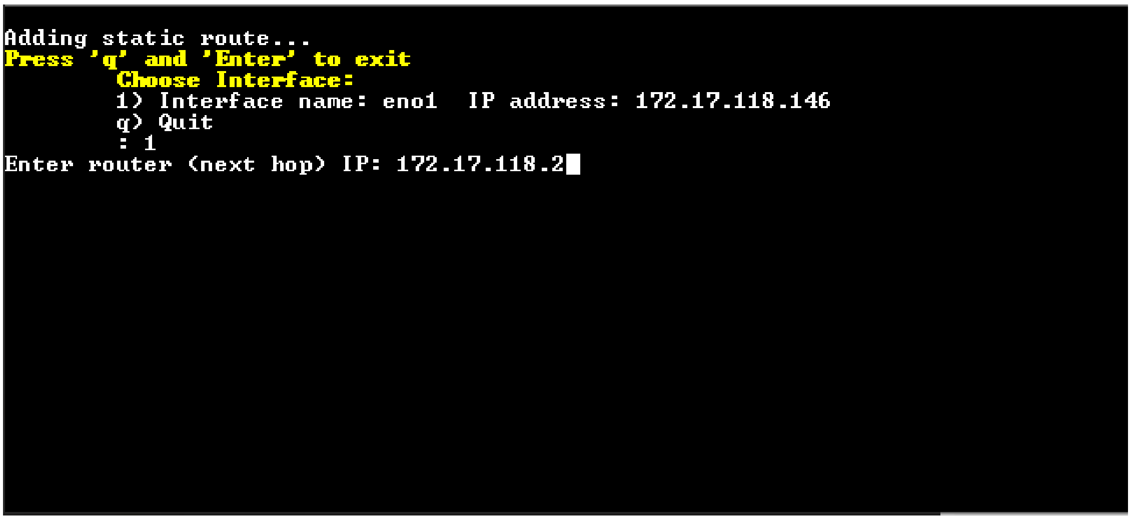
Figure 24-13: Select Interface



```
Adding static route...
Press 'q' and 'Enter' to exit
        Choose Interface:
        1) Interface name: eno1   IP address: 172.17.118.146
        q) Quit
        :
```

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

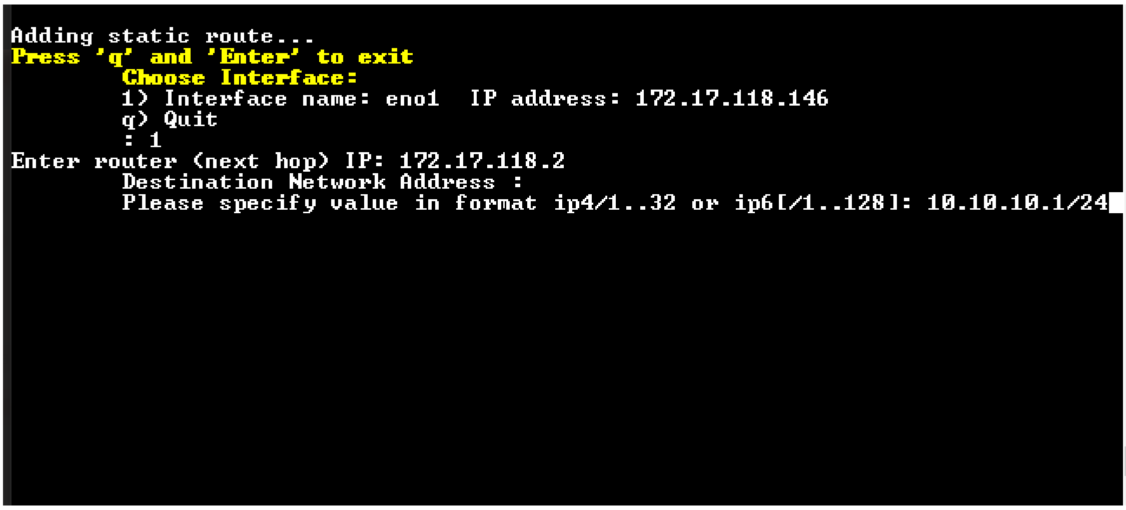
Figure 24-14: Enter Router (next hop)



```
Adding static route...
Press 'q' and 'Enter' to exit
        Choose Interface:
        1) Interface name: eno1   IP address: 172.17.118.146
        q) Quit
        : 1
Enter router (next hop) IP: 172.17.118.2
```

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

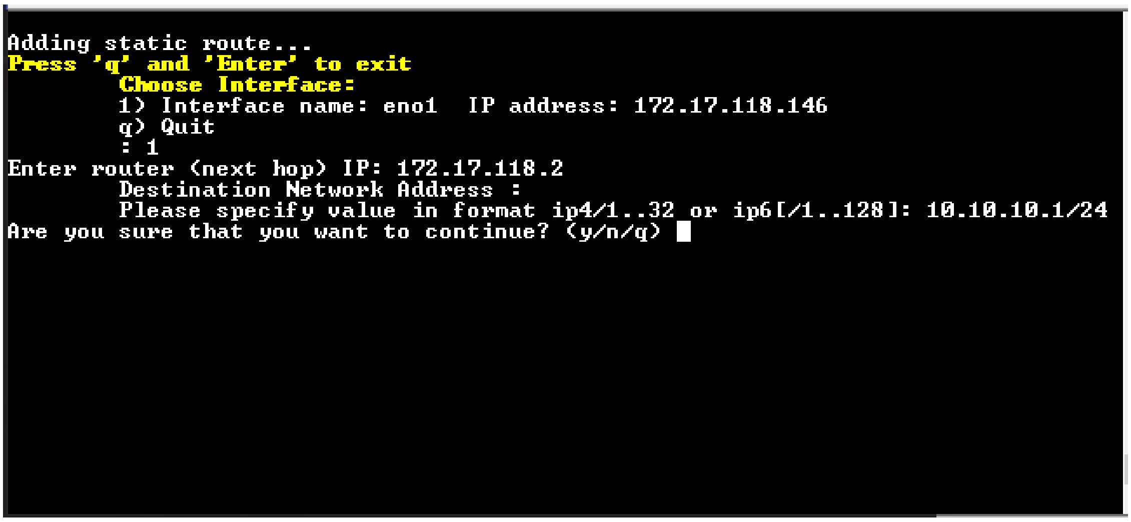
Figure 24-15: Destination Network Address



```
Adding static route...
Press 'q' and 'Enter' to exit
        Choose Interface:
        1) Interface name: eno1   IP address: 172.17.118.146
        q) Quit
        : 1
Enter router (next hop) IP: 172.17.118.2
        Destination Network Address :
        Please specify value in format ip4/1..32 or ip6[/1..128]: 10.10.10.1/24
```

4. Enter the Destination Network Address in specified format, and then press Enter.

Figure 24-16: Confirm New IP Address



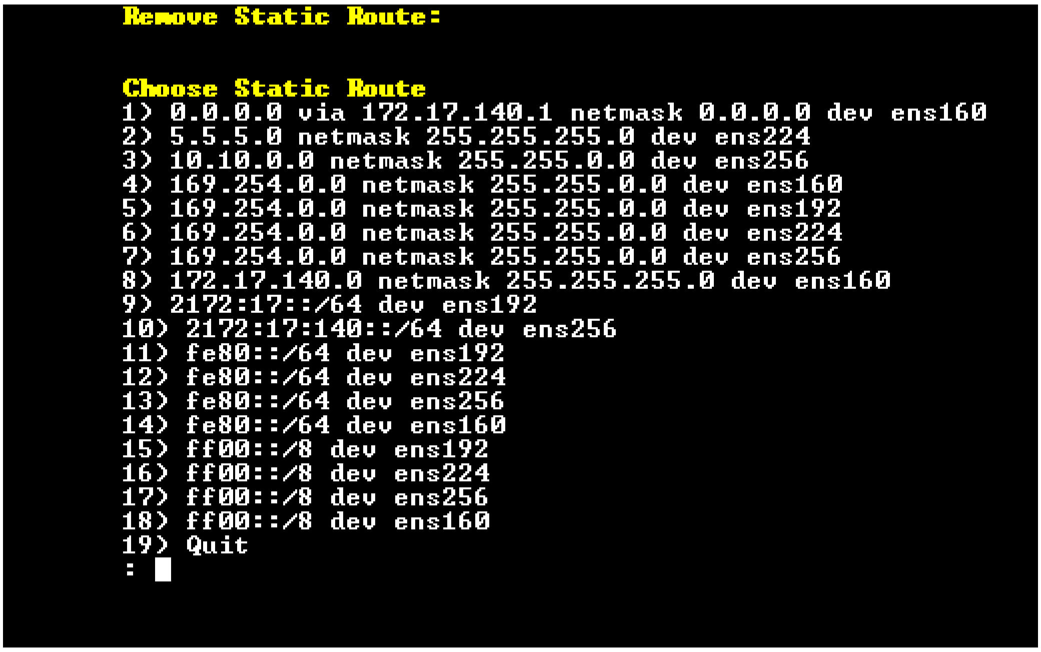
```
Adding static route...
Press 'q' and 'Enter' to exit
        Choose Interface:
        1) Interface name: eno1   IP address: 172.17.118.146
        q) Quit
        : 1
Enter router (next hop) IP: 172.17.118.2
        Destination Network Address :
        Please specify value in format ip4/1..32 or ip6[/1..128]: 10.10.10.1/24
Are you sure that you want to continue? (y/n/q)
```

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

➢ To remove a static route:

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

Figure 24-17: Remove Static Route



```
Remove Static Route:


Choose Static Route
1) 0.0.0.0 via 172.17.140.1 netmask 0.0.0.0 dev ens160
2) 5.5.5.0 netmask 255.255.255.0 dev ens224
3) 10.10.0.0 netmask 255.255.0.0 dev ens256
4) 169.254.0.0 netmask 255.255.0.0 dev ens160
5) 169.254.0.0 netmask 255.255.0.0 dev ens192
6) 169.254.0.0 netmask 255.255.0.0 dev ens224
7) 169.254.0.0 netmask 255.255.0.0 dev ens256
8) 172.17.140.0 netmask 255.255.255.0 dev ens160
9) 2172:17::/64 dev ens192
10) 2172:17:140::/64 dev ens256
11) fe80::/64 dev ens192
12) fe80::/64 dev ens224
13) fe80::/64 dev ens256
14) fe80::/64 dev ens160
15) ff00::/8 dev ens192
16) ff00::/8 dev ens224
17) ff00::/8 dev ens256
18) ff00::/8 dev ens160
19) Quit
:
```

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.

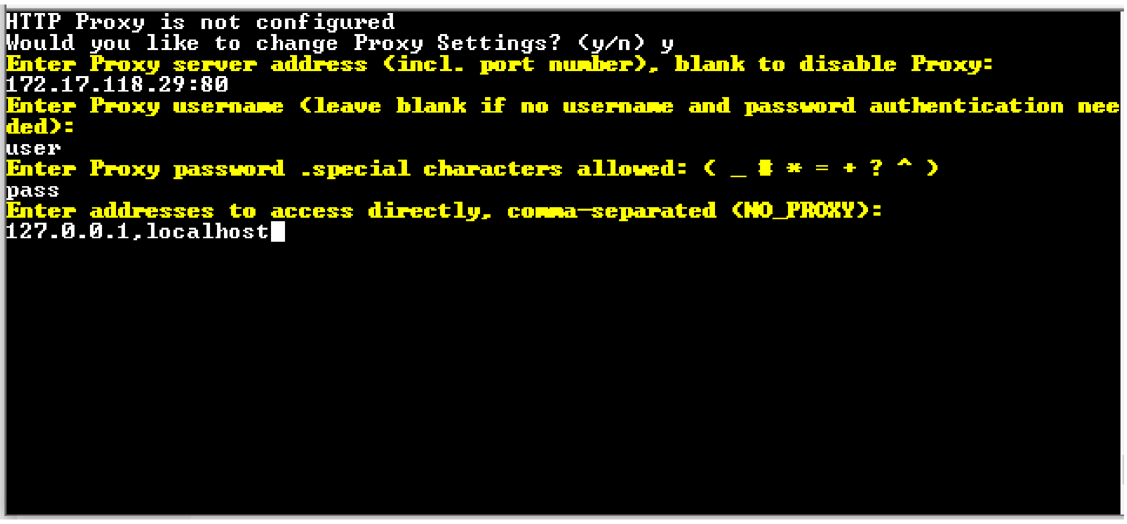
➢ To configure proxy settings:

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 24-18: Proxy Settings



```
HTTP Proxy is not configured
Would you like to change Proxy Settings? (y/n) y
Enter Proxy server address (incl. port number), blank to disable Proxy:
172.17.118.29:80
Enter Proxy username (leave blank if no username and password authentication nee
ded):
user
Enter Proxy password .special characters allowed: ( _ # * = + ? ^ )
pass
Enter addresses to access directly, comma-separated (NO_PROXY):
127.0.0.1,localhost
```

SNMP Agent

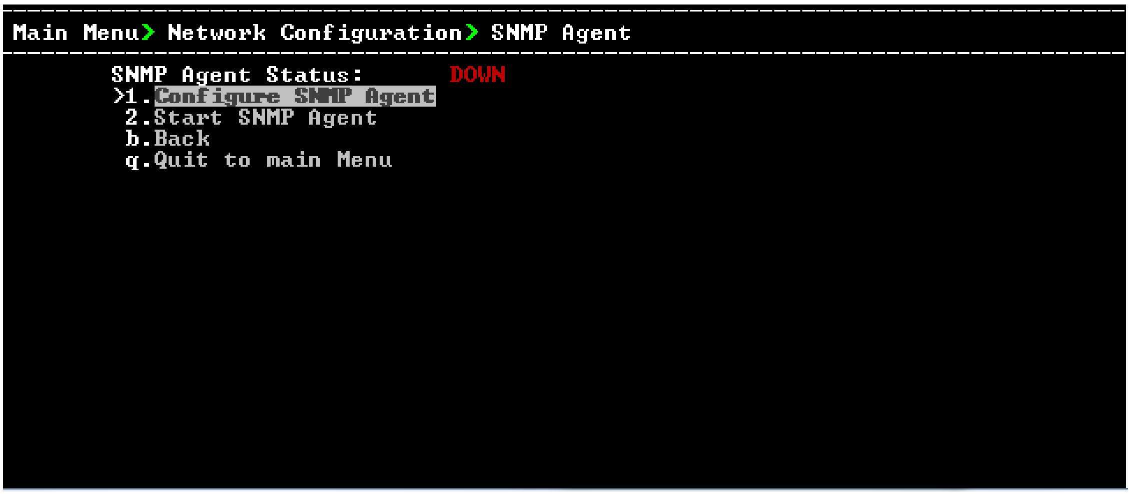
The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP). This agent serves OVOC, NMS, or higher-level management system synchronization. This menu includes the 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 238).
  - Configure the SNMPv3 Engine ID (Server SNMPv3 Engine ID on page 238)

➢ **To configure SNMP Agent:**

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

Figure 24-19: SNMP Agent



```
Main Menu> Network Configuration> SNMP Agent
       SNMP Agent Status:        DOWN
       >1.Configure SNMP Agent
        2.Start SNMP Agent
        b.Back
        q.Quit to main Menu
```

The SNMP Agent status is displayed.

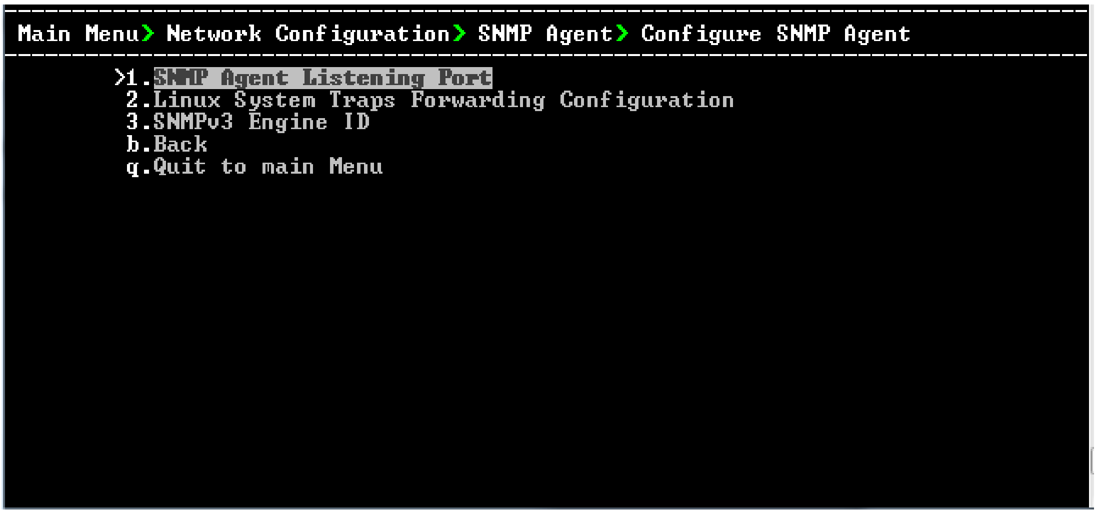
➢ **To start the SNMP Agent:**

- Choose option **2**

➢ **To configure SNMP Agent:**

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

Figure 24-20: Configure SNMP Agent



```
Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent
       >1.SNMP Agent Listening Port
        2.Linux System Traps Forwarding Configuration
        3.SNMPv3 Engine ID
        b.Back
        q.Quit to main Menu
```

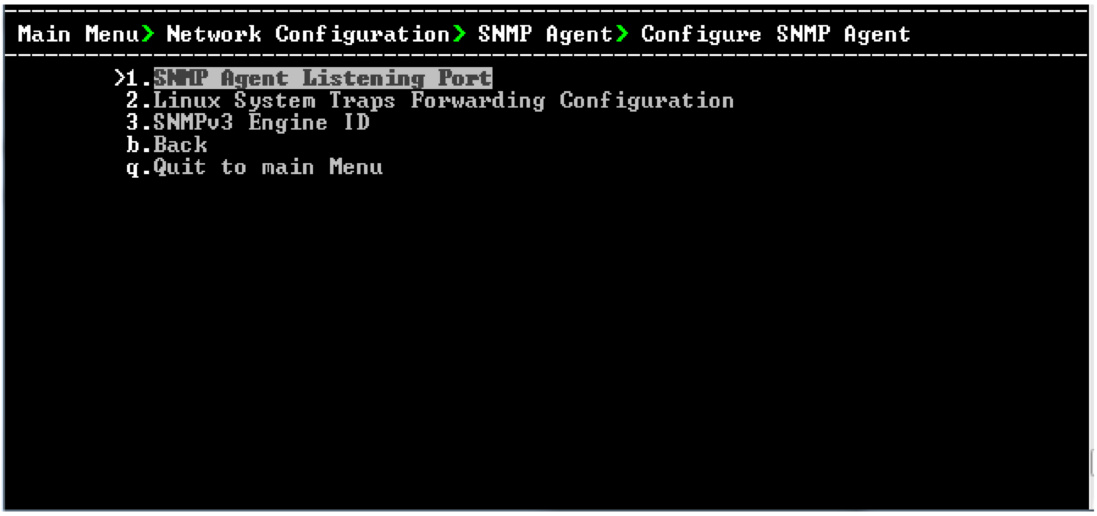
SNMP Agent Listening Port

The SNMP Agent Listening port is a bi-directional UDP port used by the SNMP agent for listening for traps from managed devices. You can change this listening port according to your network traffic management setup.

➢ **To configure SNMP Agent Listening port**

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

Figure 24-21: SNMP Agent Listening Port



```
Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent

        >1.SNMP Agent Listening Port
         2.Linux System Traps Forwarding Configuration
         3.SNMPv3 Engine ID
         b.Back
         q.Quit to main Menu
```

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.

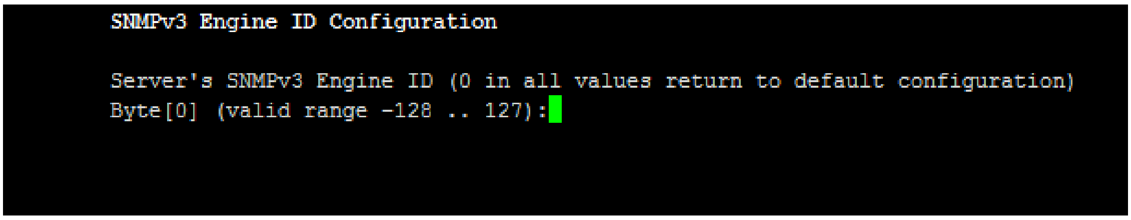
Server SNMPv3 Engine ID

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 24-22: OVOC Server Manager – Configure SNMPv3 Engine ID

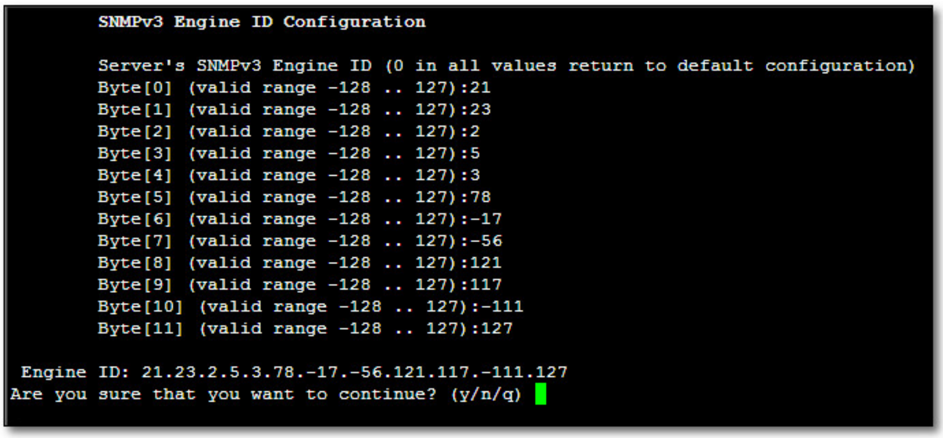


```
SNMPv3 Engine ID Configuration

Server's SNMPv3 Engine ID (0 in all values return to default configuration)
Byte[0] (valid range -128 .. 127):
```

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 24-23: SNMPv3 Engine ID Configuration – Complete Configuration



```
        SNMPv3 Engine ID Configuration

        Server's SNMPv3 Engine ID (0 in all values return to default configuration)
        Byte[0] (valid range -128 .. 127):21
        Byte[1] (valid range -128 .. 127):23
        Byte[2] (valid range -128 .. 127):2
        Byte[3] (valid range -128 .. 127):5
        Byte[4] (valid range -128 .. 127):3
        Byte[5] (valid range -128 .. 127):78
        Byte[6] (valid range -128 .. 127):-17
        Byte[7] (valid range -128 .. 127):-56
        Byte[8] (valid range -128 .. 127):121
        Byte[9] (valid range -128 .. 127):117
        Byte[10] (valid range -128 .. 127):-111
        Byte[11] (valid range -128 .. 127):127

 Engine ID: 21.23.2.5.3.78.-17.-56.121.117.-111.127
Are you sure that you want to continue? (y/n/q)
```

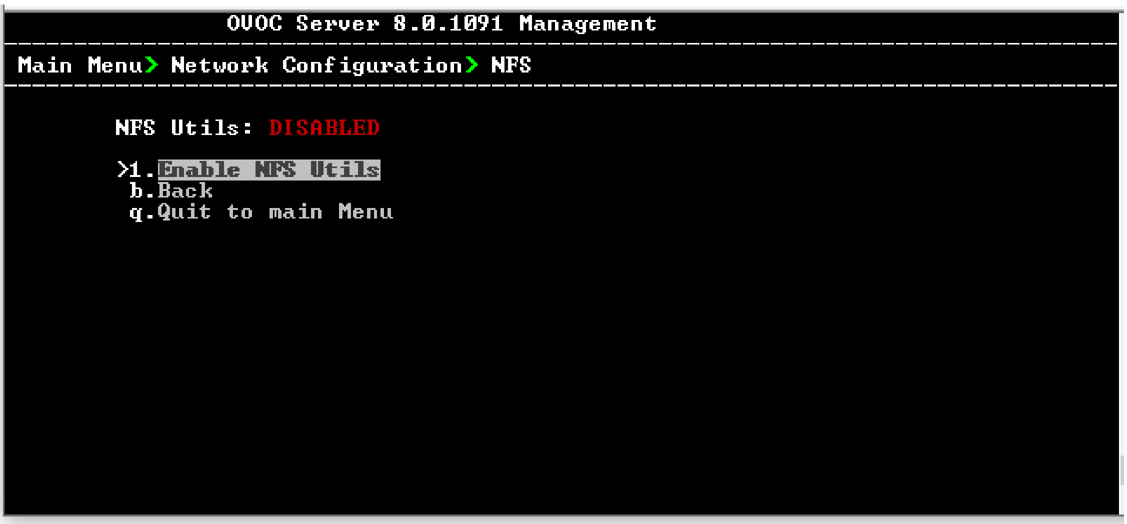
NFS

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 24-24: Network File System (NFS)



```
                OVOC Server 8.0.1091 Management
-----------------------------------------------------------------
 Main Menu> Network Configuration> NFS
-----------------------------------------------------------------

        NFS Utils: DISABLED

        >1.Enable NFS Utils
         b.Back
         q.Quit to main Menu
```

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

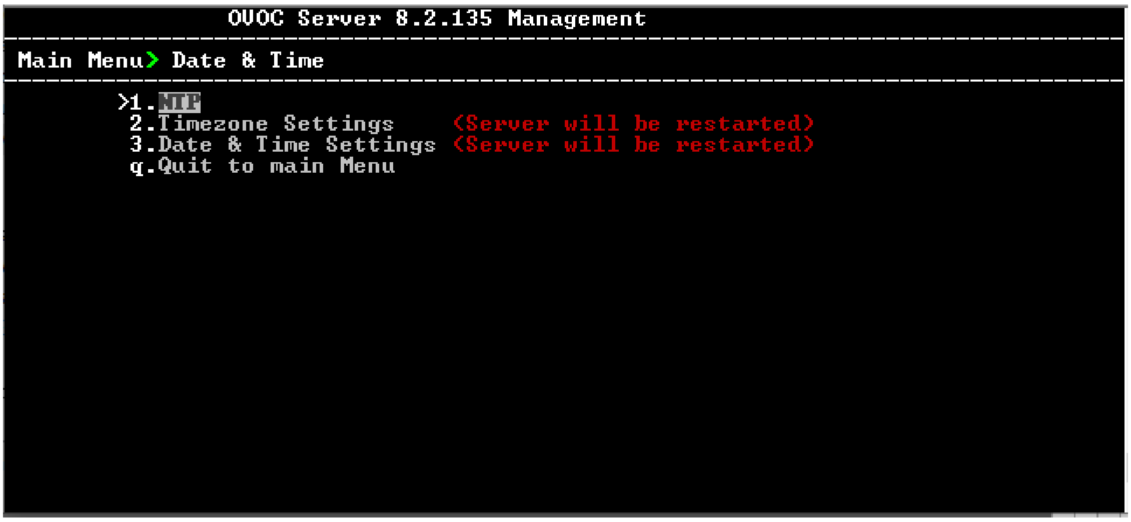
25 NTP & Clock Settings

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 25-1: Date & Time Settings



```
                OVOC Server 8.2.135 Management
--------------------------------------------------------------------------------
 Main Menu> Date & Time
--------------------------------------------------------------------------------
        >1.NTP
         2.Timezone Settings    (Server will be restarted)
         3.Date & Time Settings (Server will be restarted)
         q.Quit to main Menu
```

This menu includes the following options:

- NTP (NTP below)
- Timezone Settings (Timezone Settings on page 244)
- Date & Time Settings (Date and Time Settings on page 245)

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:

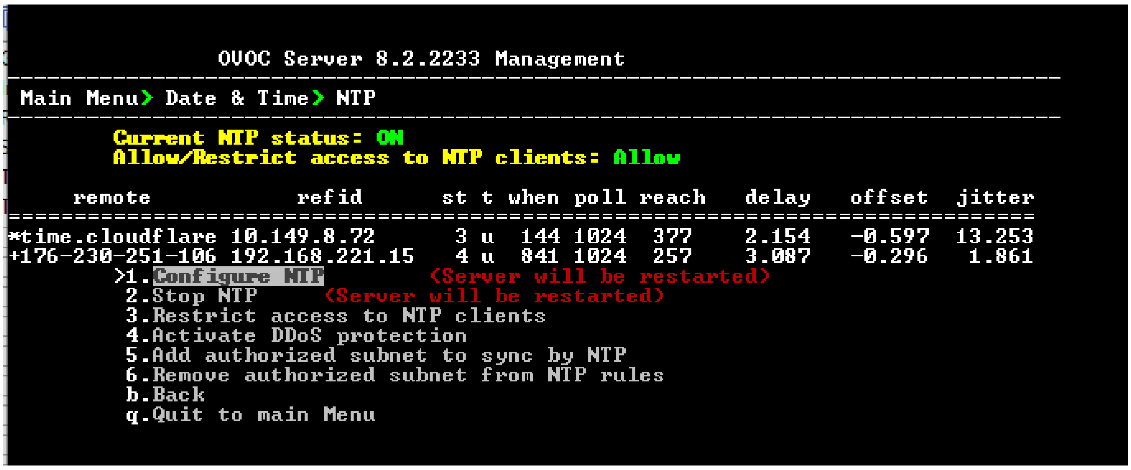
- Configure the OVOC server to obtain its clock from an external NTP clock source. Other devices that are connected to the OVOC server in the IP network can synchronize with this clock source. These devices may be any device containing an NTP server or client.
- Configure the OVOC server as the NTP server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

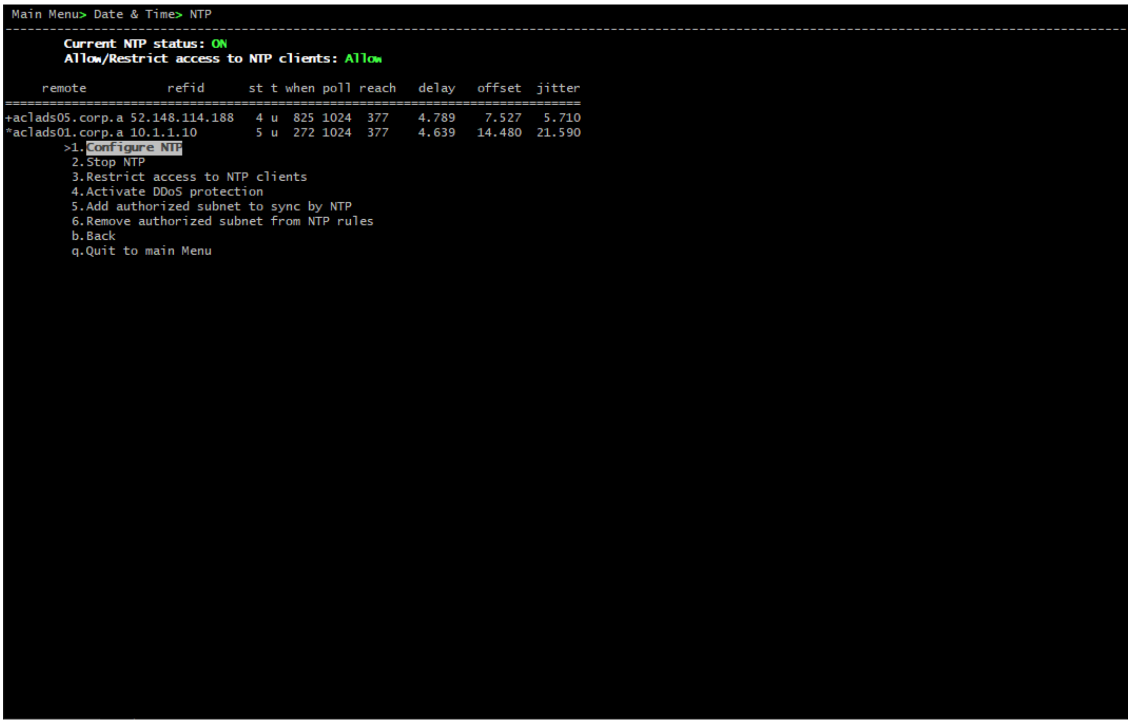
Figure 25-2: OVOC Server Manager - Configure NTP



```
                OVOC Server 8.2.2233 Management
--------------------------------------------------------------------------------
 Main Menu> Date & Time> NTP
--------------------------------------------------------------------------------
        Current NTP status: ON
        Allow/Restrict access to NTP clients: Allow

     remote           refid        st t when poll reach   delay   offset  jitter
==============================================================================
*time.cloudflare 10.149.8.72      3 u  144 1024  377    2.154   -0.597  13.253
+176-230-251-106 192.168.221.15   4 u  841 1024  257    3.087   -0.296   1.861
        >1.Configure NTP        (Server will be restarted)
         2.Stop NTP      (Server will be restarted)
         3.Restrict access to NTP clients
         4.Activate DDoS protection
         5.Add authorized subnet to sync by NTP
         6.Remove authorized subnet from NTP rules
         b.Back
         q.Quit to main Menu
```

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.

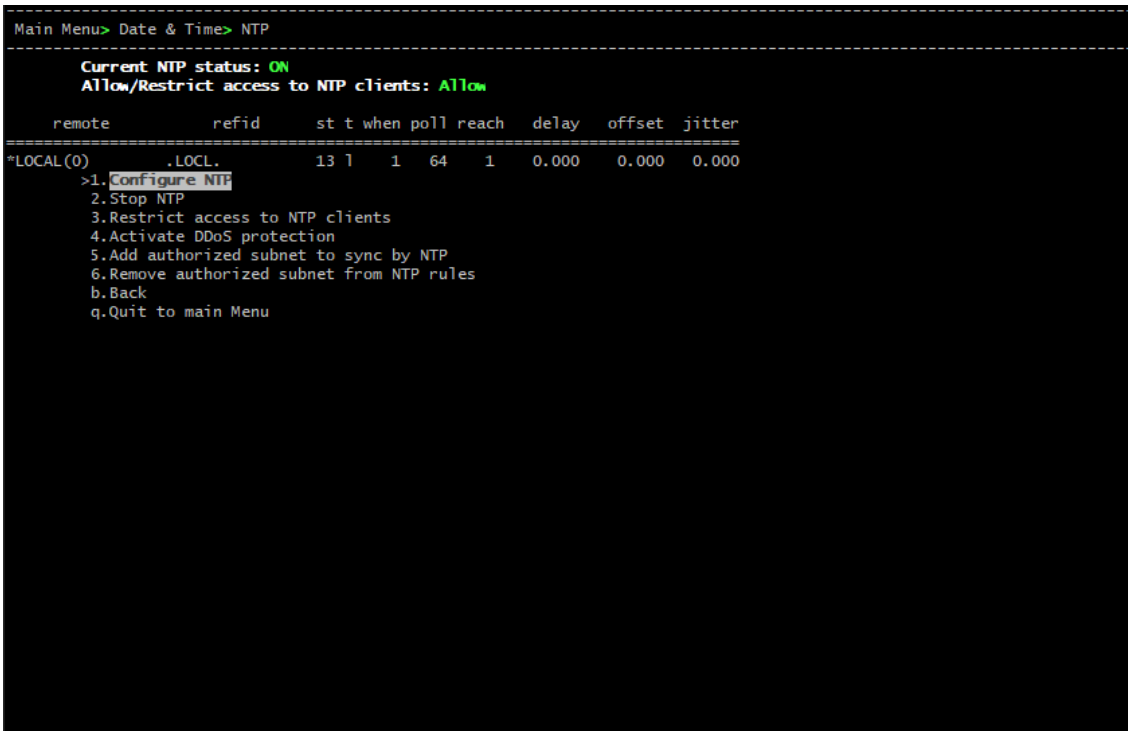
Figure 25-3: External Clock Source



```
 Main Menu> Date & Time> NTP
------------------------------------------------------------------------------------------------------------------
       Current NTP status: ON
       Allow/Restrict access to NTP clients: Allow

    remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+aclads05.corp.a 52.148.114.188   4 u  825 1024  377    4.789    7.527   5.710
*aclads01.corp.a 10.1.1.10        5 u  272 1024  377    4.639   14.480  21.590
       >1.Configure NTP
        2.Stop NTP
        3.Restrict access to NTP clients
        4.Activate DDoS protection
        5.Add authorized subnet to sync by NTP
        6.Remove authorized subnet from NTP rules
        b.Back
        q.Quit to main Menu
```

- 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 25-4: Local Clock Source



```
------------------------------------------------------------------------------------------------------------------
 Main Menu> Date & Time> NTP
------------------------------------------------------------------------------------------------------------------
       Current NTP status: ON
       Allow/Restrict access to NTP clients: Allow

    remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.          13 l    1   64    1    0.000    0.000   0.000
       >1.Configure NTP
        2.Stop NTP
        3.Restrict access to NTP clients
        4.Activate DDoS protection
        5.Add authorized subnet to sync by NTP
        6.Remove authorized subnet from NTP rules
        b.Back
        q.Quit to main Menu
```

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.

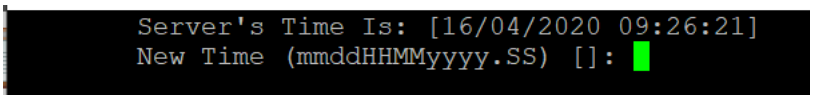
Date and Time Settings

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 & Tim**e **Settings**, and then press Enter.

Figure 26-1: New Server Time



```
Server's Time Is: [16/04/2020 09:26:21]
New Time (mmddHHMMyyyy.SS) []:
```

2. Enter the new time as shown in the following example:

mmddHHMMyyyy.SS : month(08),day(16),Hour(16),Minute(08),year(2007),”.” Second.

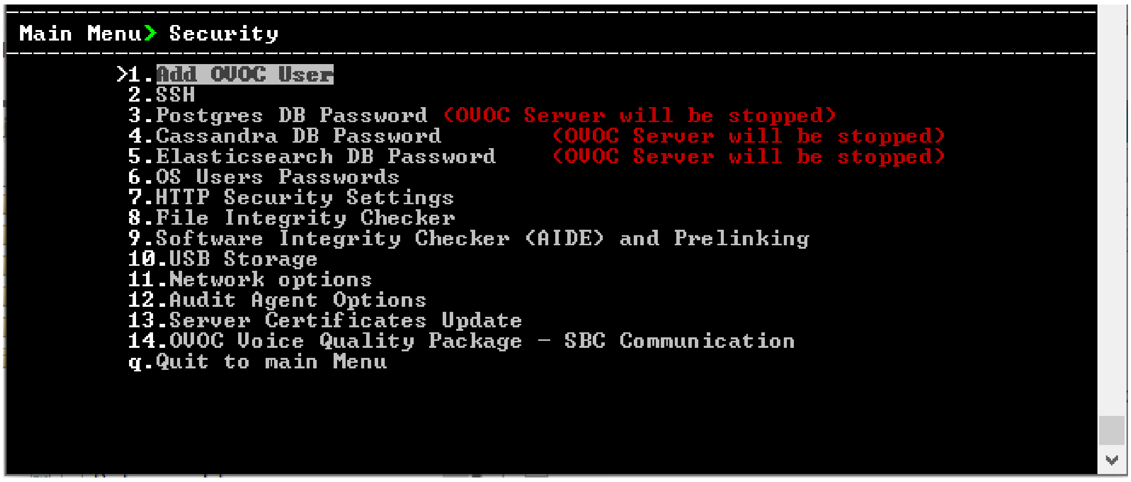
27 Security

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 27-1: Security Settings



```
 Main Menu> Security
        >1.Add OVOC User
         2.SSH
         3.Postgres DB Password (OVOC Server will be stopped)
         4.Cassandra DB Password        (OVOC Server will be stopped)
         5.Elasticsearch DB Password    (OVOC Server will be stopped)
         6.OS Users Passwords
         7.HTTP Security Settings
         8.File Integrity Checker
         9.Software Integrity Checker (AIDE) and Prelinking
         10.USB Storage
         11.Network options
         12.Audit Agent Options
         13.Server Certificates Update
         14.OVOC Voice Quality Package - SBC Communication
         q.Quit to main Menu
```

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 254)
- Cassandra Password (Cassandra Password on page 256)
- Elasticsearch DB Password (Elastic Search DB Password on page 257)
- OS Users Password (OS Users Passwords on page 257)
- HTTP Security Settings (HTTPS SSL TLS Security on page 264)
    - Server Certificate Update (Server Certificates Update on page 265)
- File Integrity Checker (File Integrity Checker on page 261)
- Software Integrity Checker (AIDE) and Pre-linking (Software Integrity Checker (AIDE) and Pre-linking on page 261)
- USB Storage (USB Storage on page 262)
- Network options (Network Options on page 262)
- Audit Agent Options (Auditd Agent Options on page 263)
- OVOC Voice Quality Package (OVOC Voice Quality Package - SBC Communication on page 263)

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.

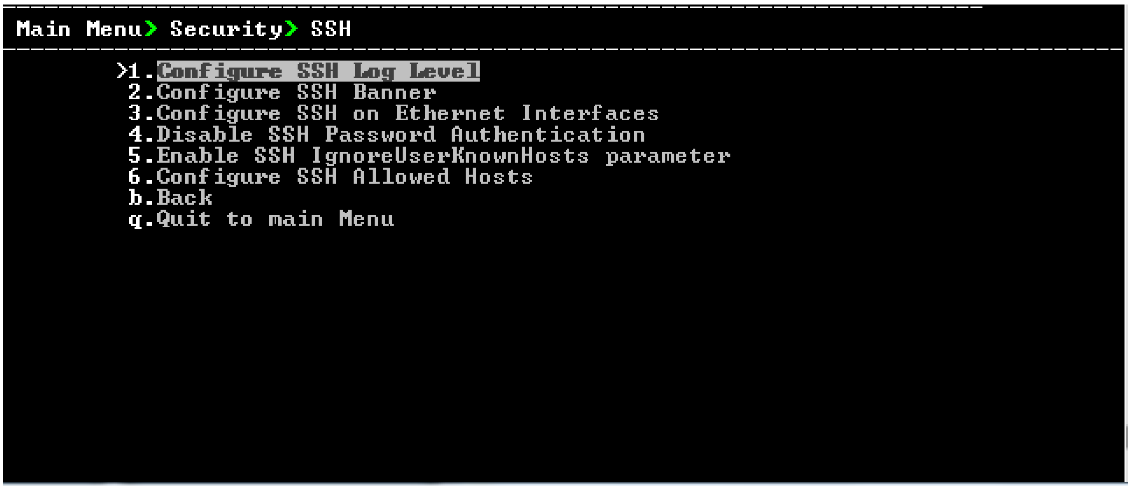
SSH

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 27-2: SSH Configuration



```
Main Menu> Security> SSH

        >1.Configure SSH Log Level
         2.Configure SSH Banner
         3.Configure SSH on Ethernet Interfaces
         4.Disable SSH Password Authentication
         5.Enable SSH IgnoreUserKnownHosts parameter
         6.Configure SSH Allowed Hosts
         b.Back
         q.Quit to main Menu
```

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 249).

- Disable SSH Password Authentication (Enable/Disable SSH Password Authentication on page 251).
- Enable SSH Ignore User Known Hosts Parameter (Enable SSH IgnoreUserKnownHosts Parameter on page 251).
- Configure SSH Allowed Hosts (SSH Allowed Hosts on page 252).

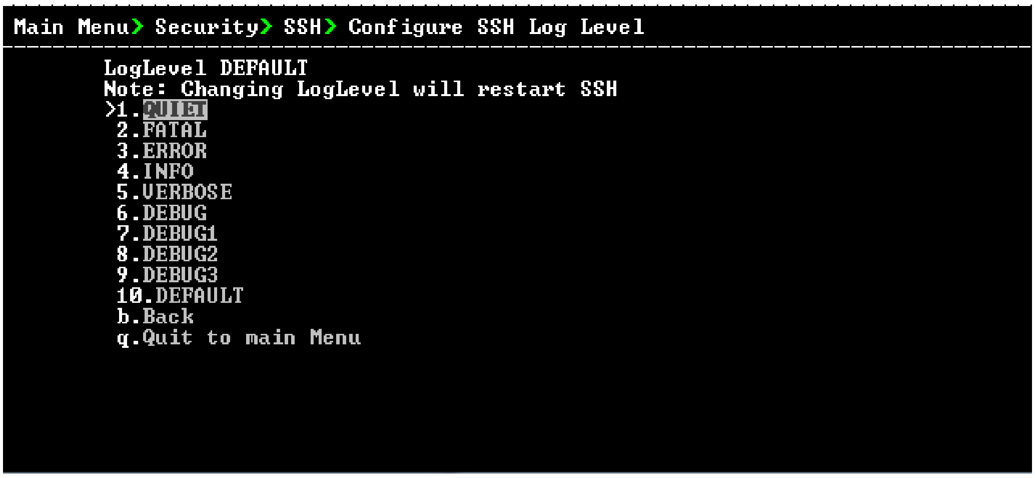
SSH Log Level

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 27-3: SSH Log Level Manager



```
Main Menu> Security> SSH> Configure SSH Log Level
------------------------------------------------------------------------------
        LogLevel DEFAULT
        Note: Changing LogLevel will restart SSH
        >1.QUIET
         2.FATAL
         3.ERROR
         4.INFO
         5.VERBOSE
         6.DEBUG
         7.DEBUG1
         8.DEBUG2
         9.DEBUG3
         10.DEFAULT
         b.Back
         q.Quit to main Menu
```

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press Enter.

   The SSH daemon restarts automatically. The Log Level status is updated on the screen to the configured value.

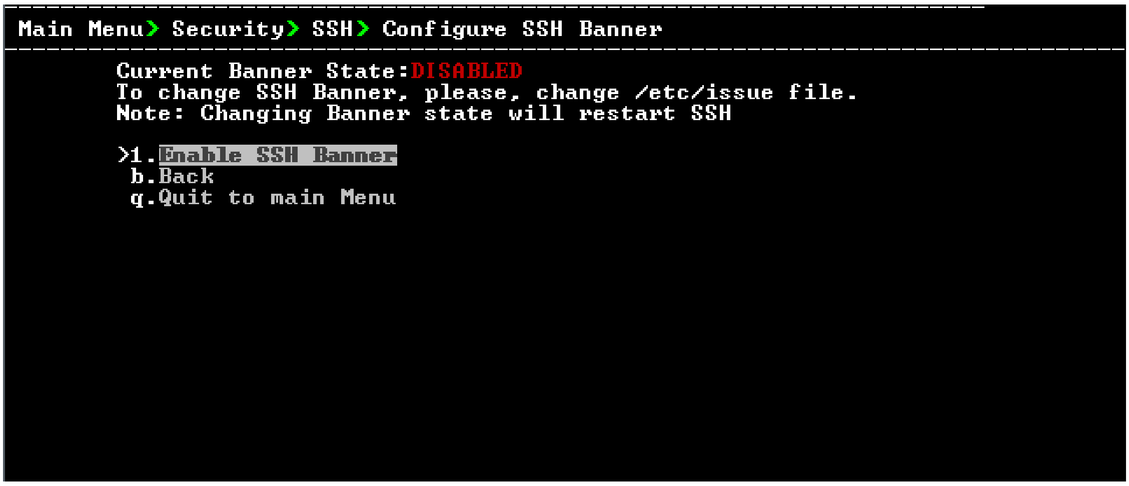
SSH Banner

The SSH Banner displays a pre-defined text message each time the user connects to the OVOC server using an SSH connection. You can customize this message. By default this option is disabled.

➢ To configure the SSH banner:

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

Figure 27-4: SSH Banner Manager



```
 Main Menu> Security> SSH> Configure SSH Banner
----------------------------------------------------------------------------
        Current Banner State:DISABLED
        To change SSH Banner, please, change /etc/issue file.
        Note: Changing Banner state will restart SSH

        >1.Enable SSH Banner
         b.Back
         q.Quit to main Menu
```

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.

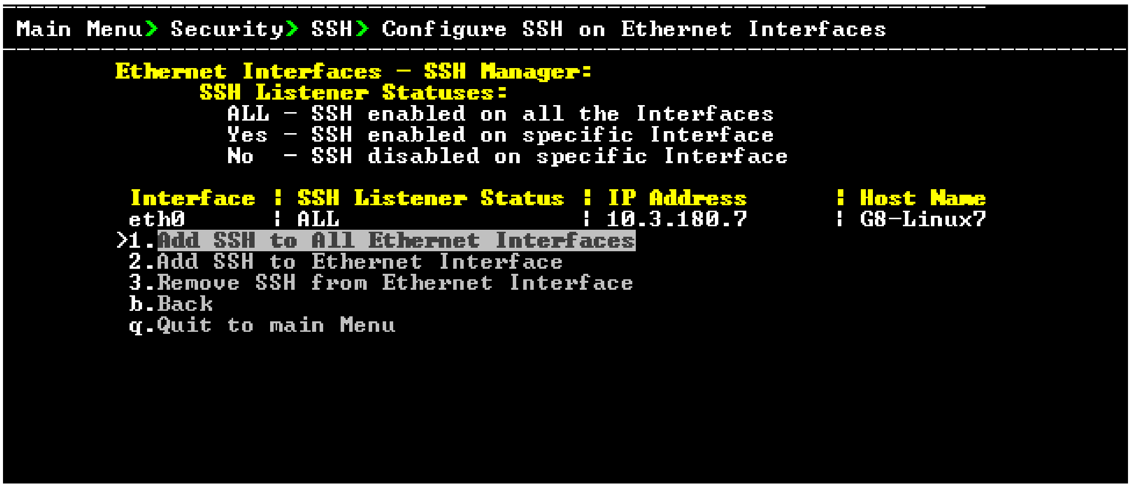
SSH on Ethernet Interfaces

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 27-5: Configure SSH on Ethernet Interfaces



```
 Main Menu> Security> SSH> Configure SSH on Ethernet Interfaces
----------------------------------------------------------------------------
        Ethernet Interfaces - SSH Manager:
              SSH Listener Statuses:
                ALL - SSH enabled on all the Interfaces
                Yes - SSH enabled on specific Interface
                No  - SSH disabled on specific Interface

         Interface ¦ SSH Listener Status ¦ IP Address       ¦ Host Name
         eth0      ¦ ALL                 ¦ 10.3.180.7       ¦ G8-Linux7
        >1.Add SSH to All Ethernet Interfaces
         2.Add SSH to Ethernet Interface
         3.Remove SSH from Ethernet Interface
         b.Back
         q.Quit to main Menu
```

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.

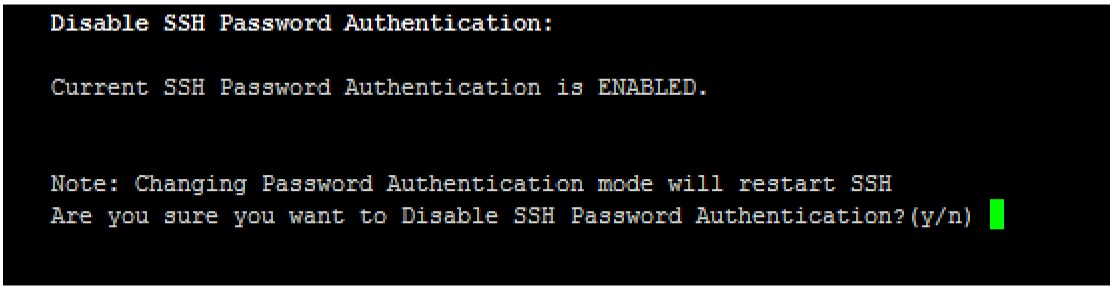
Enable/Disable SSH Password Authentication

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 27-6: Disable Password Authentication



```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.


Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Disable SSH Password Authentication?(y/n)
```

2. Type **y** to disable SSH password authentication or **n** to enable, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

Once you perform this action, you cannot reconnect to the OVOC server using User/Password authentication. Therefore, before you disable this authentication method, ensure that you provision an alternative SSH connection method. For example, using an RSA keys pair. For detailed instructions on how to perform such an action, see www.junauza.com or search the internet for an alternative method.

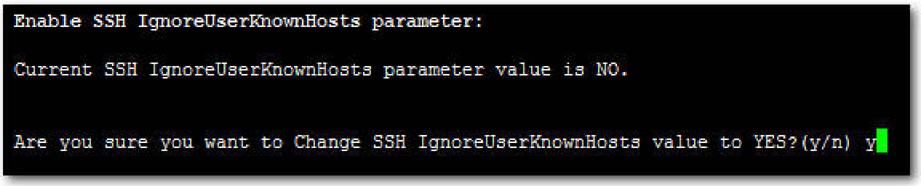
Enable SSH IgnoreUserKnownHosts Parameter

This option enables you to disable the use of the '$HOME/.ssh/known_host' file with stored remote servers fingerprints.

➢ To enable SSH IgnoreUserKnowHosts parameter:

1. From the SSH menu, choose option **5**, and then press Enter.

Figure 27-7: SSH IgnoreUserKnowHosts Parameter - Confirm



```
Enable SSH IgnoreUserKnownHosts parameter:

Current SSH IgnoreUserKnownHosts parameter value is NO.


Are you sure you want to Change SSH IgnoreUserKnownHosts value to YES?(y/n) y
```

2. Type **y** to change this parameter value to either 'YES' or '**NO**' or type **n** to leave as is, and then press Enter.

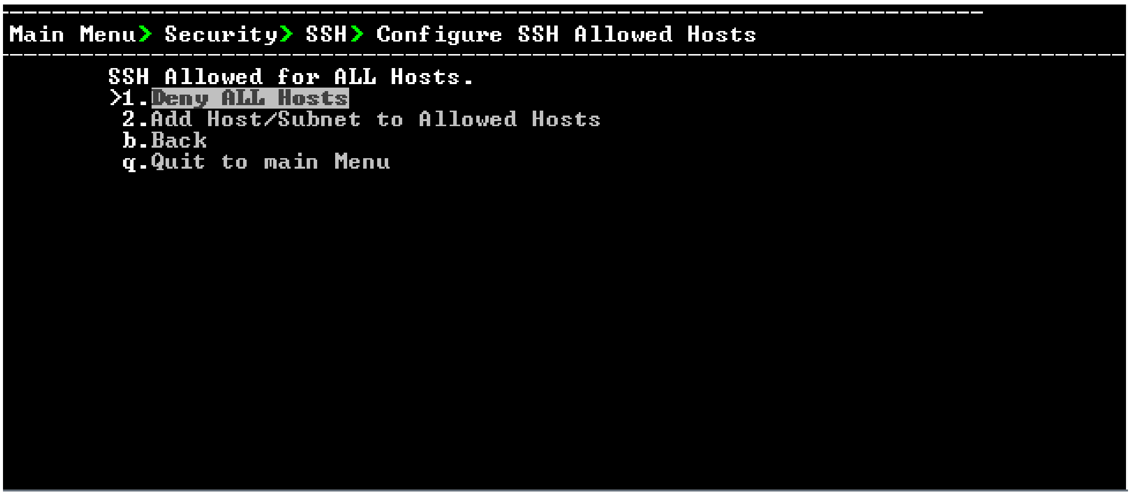
SSH Allowed Hosts

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 27-8: Configure SSH Allowed Hosts



```
Main Menu> Security> SSH> Configure SSH Allowed Hosts
---------------------------------------------------------------------------
       SSH Allowed for ALL Hosts.
       >1.Deny ALL Hosts
        2.Add Host/Subnet to Allowed Hosts
        b.Back
        q.Quit to main Menu
```

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 254).

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.

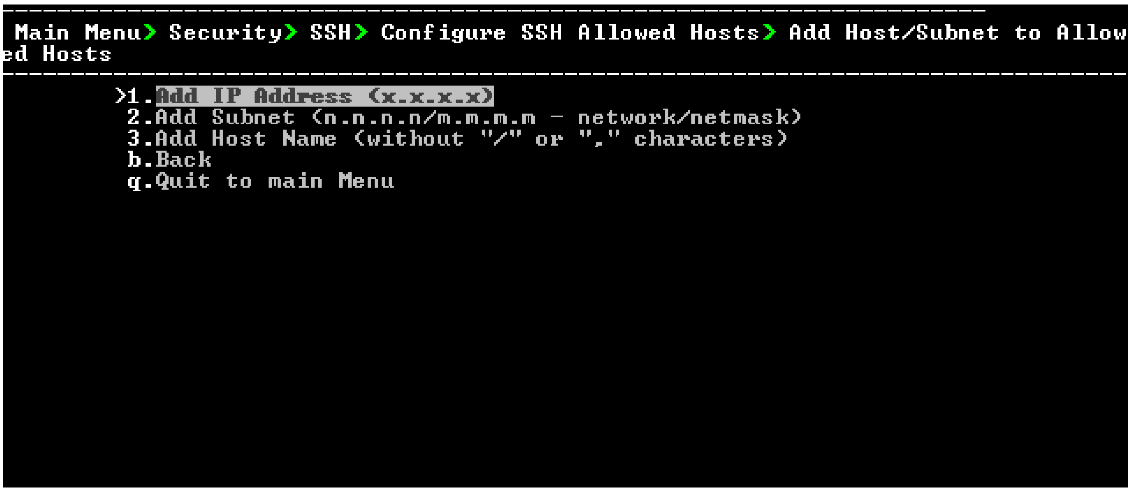
Add Hosts to Allowed Hosts

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 27-9: Add Host/Subnet to Allowed Hosts



```
----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allow
ed Hosts
--------------------------------------------------------------------------------
        >1.Add IP Address (x.x.x.x)
         2.Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
         3.Add Host Name (without "/" or "," characters)
         b.Back
         q.Quit to main Menu
```

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:

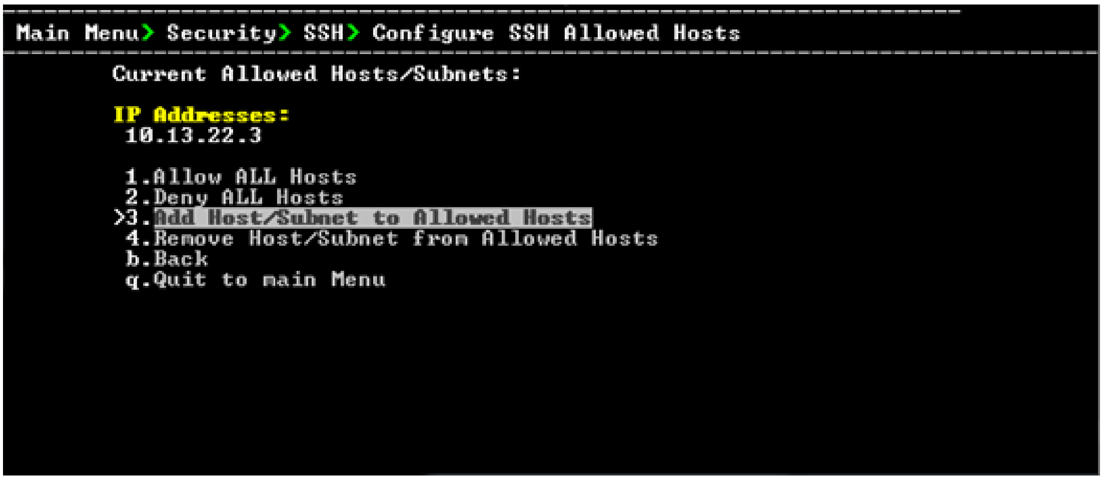
- Verify your remote host name appears in the DNS server database and your OVOC server has an access to the DNS server.
- Provide the host name of the desired network interface defined in "/etc/hosts" file.

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 27-10: Add Host/Subnet to Allowed Hosts-Configured Host



```
Main Menu> Security> SSH> Configure SSH Allowed Hosts

        Current Allowed Hosts/Subnets:

        IP Addresses:
         10.13.22.3

         1.Allow ALL Hosts
         2.Deny ALL Hosts
        >3.Add Host/Subnet to Allowed Hosts
         4.Remove Host/Subnet from Allowed Hosts
         b.Back
         q.Quit to main Menu
```

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

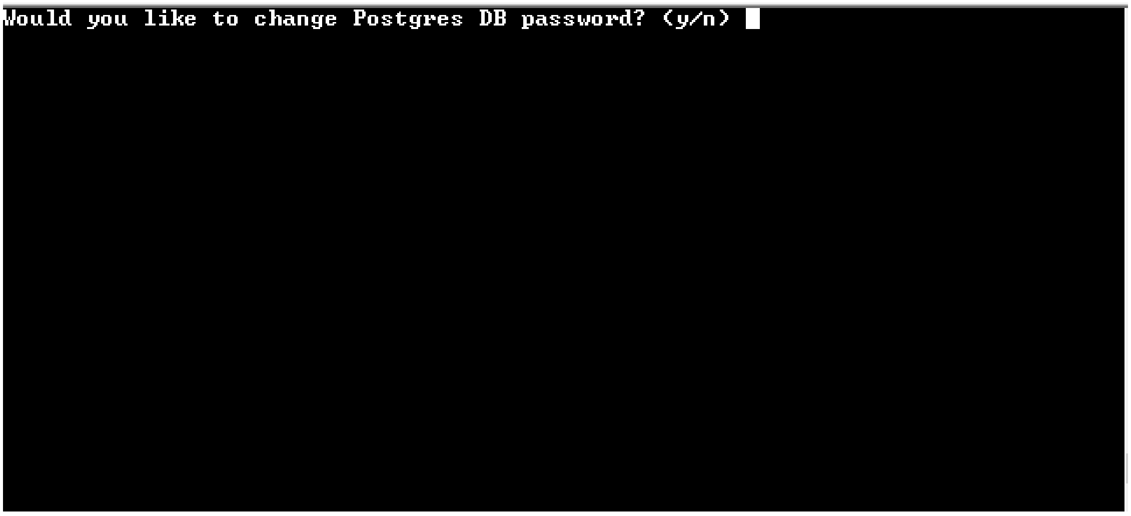
This option enables you to change the default PostgreSQL Database password "pass_1234". The OVOC server shuts down automatically before changing the PostgreSQL Database password.

- 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.

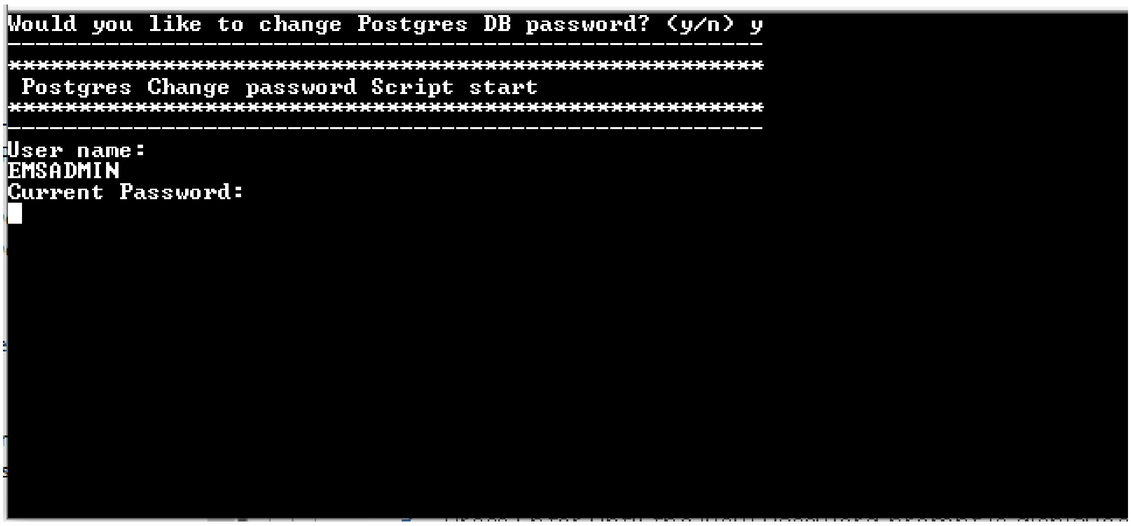
Figure 27-11: Postgre DB Password



```
Would you like to change Postgres DB password? (y/n) █
```

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

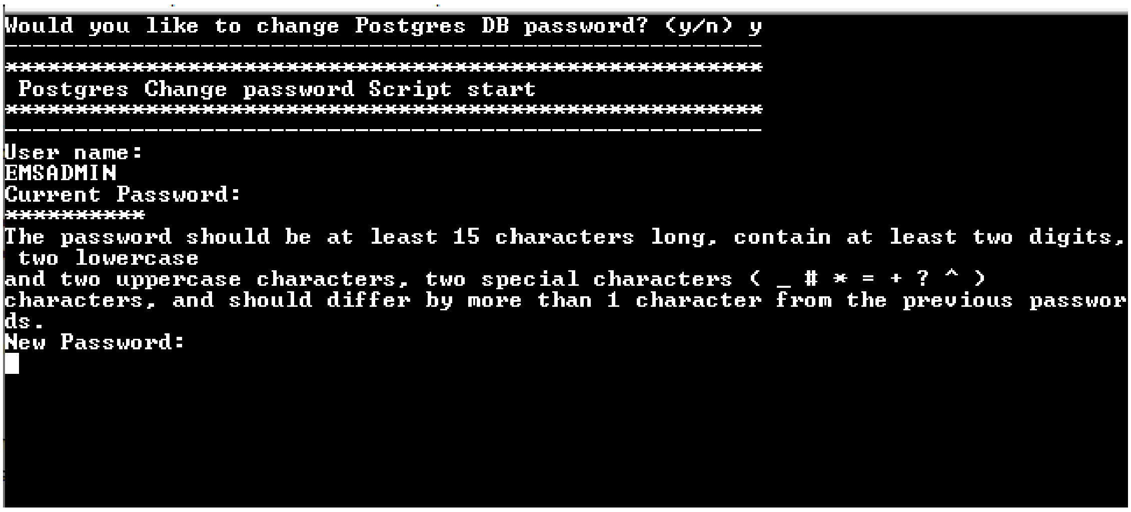
Figure 27-12: Current Password



```
Would you like to change Postgres DB password? (y/n) y
----------------------------------------------------
****************************************************
 Postgres Change password Script start
****************************************************
----------------------------------------------------
User name:
EMSADMIN
Current Password:
█
```

3. Enter the current password.

Figure 27-13: New Password



```
Would you like to change Postgres DB password? (y/n) y
------------------------------------------------------
******************************************************
 Postgres Change password Script start
******************************************************
------------------------------------------------------
User name:
EMSADMIN
Current Password:
**********
The password should be at least 15 characters long, contain at least two digits,
 two lowercase
and two uppercase characters, two special characters ( _ # * = + ? ^ )
characters, and should differ by more than 1 character from the previous passwor
ds.
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

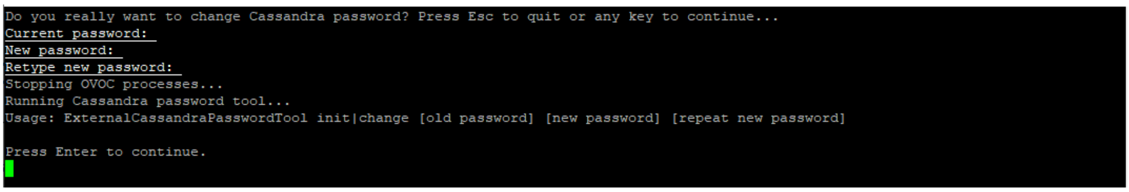
This section describes how to change the Cassandra password.

➢ 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 27-14: Change Cassandra Password



```
Do you really want to change Cassandra password? Press Esc to quit or any key to continue...
Current password:
New password:
Retype new password:
Stopping OVOC processes...
Running Cassandra password tool...
Usage: ExternalCassandraPasswordTool init|change [old password] [new password] [repeat new password]

Press Enter to continue.
```

3. Enter the new password and confirm.

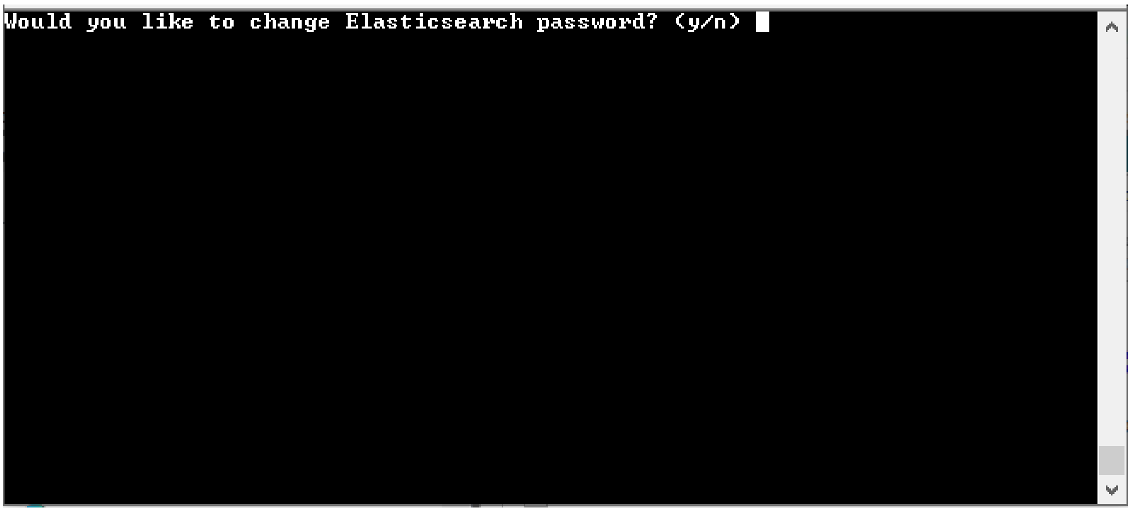
Elastic Search DB Password

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 27-15: Elastic Search DB Password



```
Would you like to change Elasticsearch password? (y/n)
```

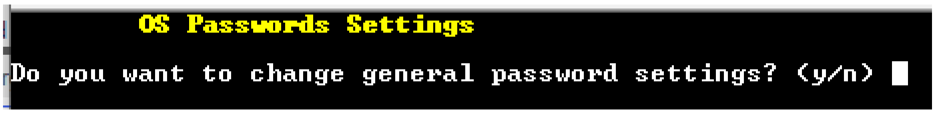
3. Enter the new password and confirm.

OS Users Passwords

This section describes how to change the OS password settings.

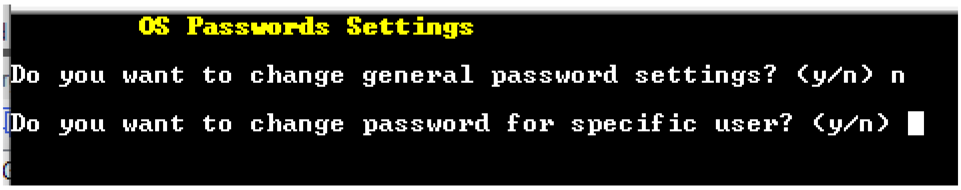
➢ **To change OS passwords:**

1. From the Security menu, choose **OS Users Passwords**, and then press Enter.



```
          OS Passwords Settings
Do you want to change general password settings? (y/n)
```

- Type **y** to change General Password settings (see General Password Settings on the next page).
- Type **n** to change User Security Extensions.



```
          OS Passwords Settings
Do you want to change general password settings? (y/n) n
Do you want to change password for specific user? (y/n)
```

- 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]:
```

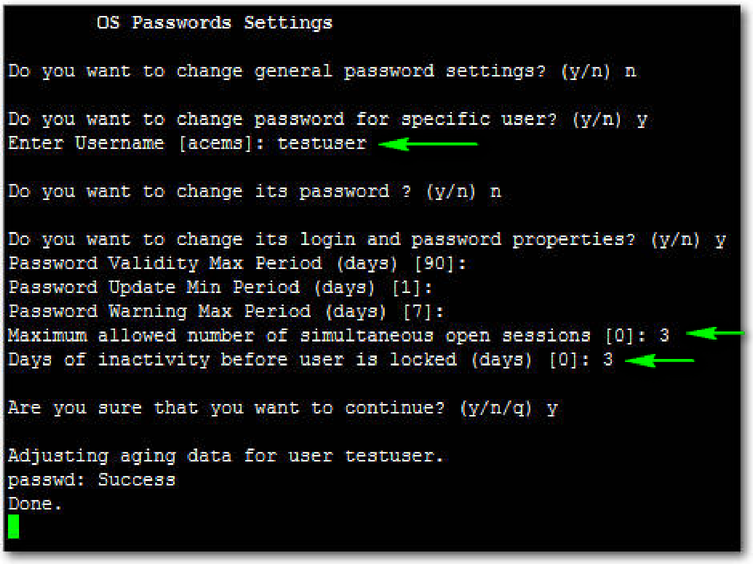
9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user, and then press Enter.

```
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]:
```

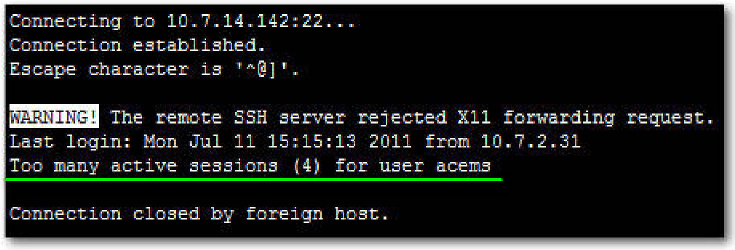
Figure 27-16: OS Passwords Settings with Security Extensions



```
        OS Passwords Settings

Do you want to change general password settings? (y/n) n

Do you want to change password for specific user? (y/n) y
Enter Username [acems]: testuser

Do you want to change its password ? (y/n) n

Do you want to change its login and password properties? (y/n) y
Password Validity Max Period (days) [90]:
Password Update Min Period (days) [1]:
Password Warning Max Period (days) [7]:
Maximum allowed number of simultaneous open sessions [0]: 3
Days of inactivity before user is locked (days) [0]: 3

Are you sure that you want to continue? (y/n/q) y

Adjusting aging data for user testuser.
passwd: Success
Done.
```

If the user attempts to open more than three SSH sessions simultaneously, they are prompted and immediately disconnected from the fourth session as displayed in the figure below.

Figure 27-17: Maximum Active SSH Sessions



```
Connecting to 10.7.14.142:22...
Connection established.
Escape character is '^@]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Jul 11 15:15:13 2011 from 10.7.2.31
Too many active sessions (4) for user acems

Connection closed by foreign host.
```

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

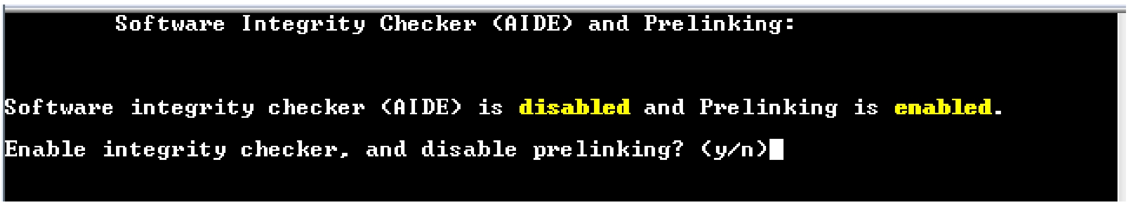
AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

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 27-18: Software Integrity Checker (AIDE) and Pre-linking



```
        Software Integrity Checker (AIDE) and Prelinking:


Software integrity checker (AIDE) is disabled and Prelinking is enabled.

Enable integrity checker, and disable prelinking? (y/n)
```

2. Do one of the following:
   - Type **y** to enable AIDE and disable pre-linking, and then press Enter.
   - Type **n** to disable AIDE and enable pre-linking, and then press Enter.

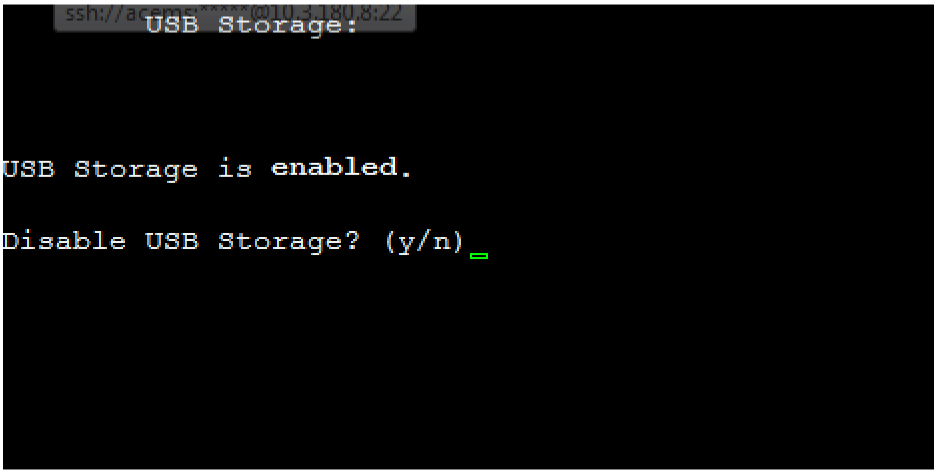
USB Storage

This menu option allows enabling or disabling the OVOC server’s USB storage access as required.

➢ To enable USB storage:

1. From the Security menu, choose **USB Storage**, and then press Enter.

Figure 27-19: USB Storage



```
ssh://acems:*****@10.3.180.8:22
            USB Storage:


USB Storage is enabled.

Disable USB Storage? (y/n)
```

2. Enable or disable USB storage as required.

Network Options

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

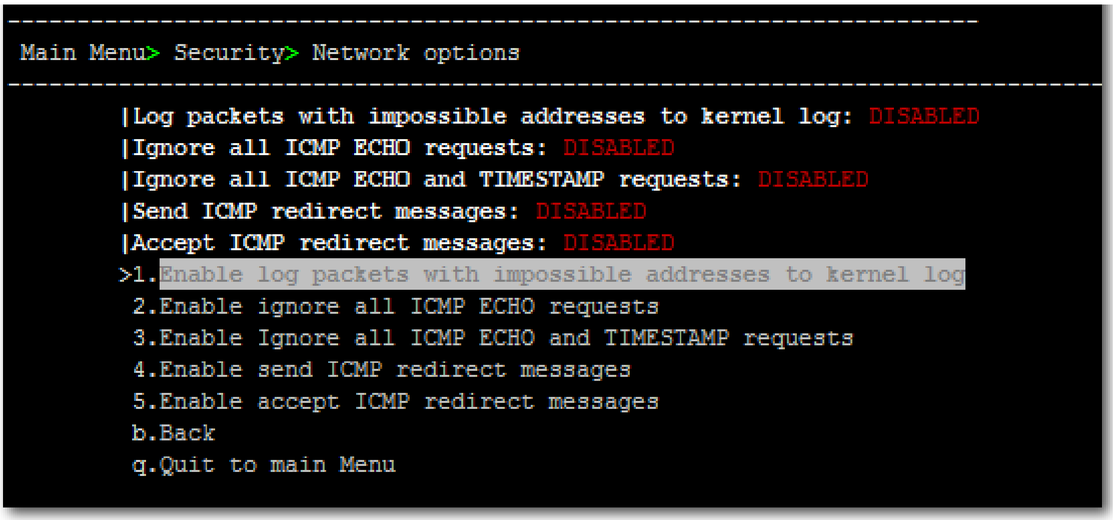
- **Ignore Internet Control Message Protocol (ICMP) Echo requests**: This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.
- **Ignore ICMP Echo and Timestamp requests:** 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 27-20: Network Options



```
-----------------------------------------------------------------------
 Main Menu> Security> Network options
-------------------------------------------------------------------------------
        |Log packets with impossible addresses to kernel log: DISABLED
        |Ignore all ICMP ECHO requests: DISABLED
        |Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
        |Send ICMP redirect messages: DISABLED
        |Accept ICMP redirect messages: DISABLED
        >1.Enable log packets with impossible addresses to kernel log
         2.Enable ignore all ICMP ECHO requests
         3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
         4.Enable send ICMP redirect messages
         5.Enable accept ICMP redirect messages
         b.Back
         q.Quit to main Menu
```

2. Set the required network options.

Auditd Agent Options

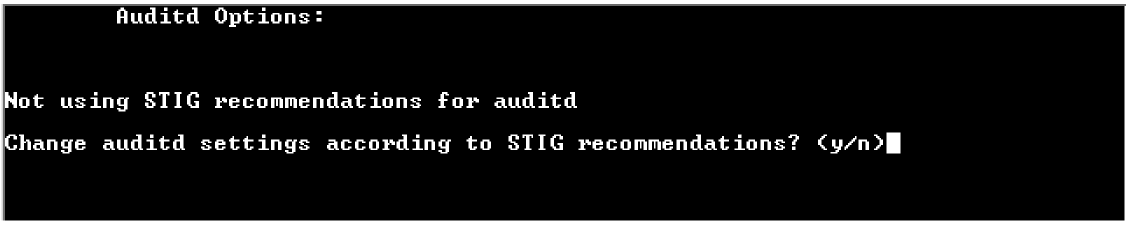
Auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk. Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

➢ To set Auditd options according to STIG:

1. From the Security menu, choose **Auditd Options**, and then press Enter.

Figure 27-21: Auditd Options

Figure 27-22:



```
        Auditd Options:


Not using STIG recommendations for auditd

Change auditd settings according to STIG recommendations? (y/n)
```

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

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

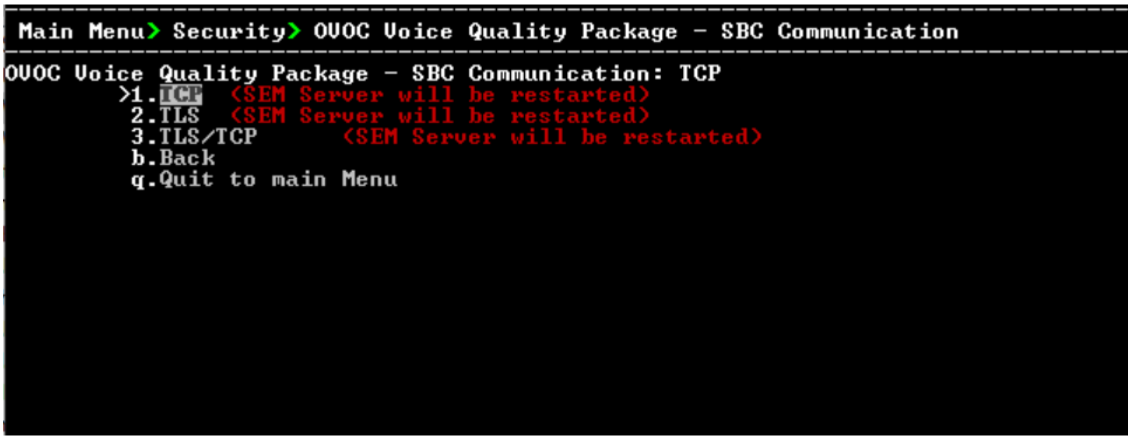
OVOC Voice Quality Package - SBC Communication

This option allows you to configure the transport type for the XML based OVOC Voice Quality Package communication from the OVOC managed devices to the OVOC server. You can enable the TCP port (port 5000), the TLS port (port 5001) connections or both port connections.

➢ To configure the OVOC Voice Quality Package - SBC Communication:

1. From the Security menu, select **OVOC Voice Quality Package – SBC Communication**, and then press Enter.

Figure 27-23: OVOC Voice Quality Package – SBC Communication



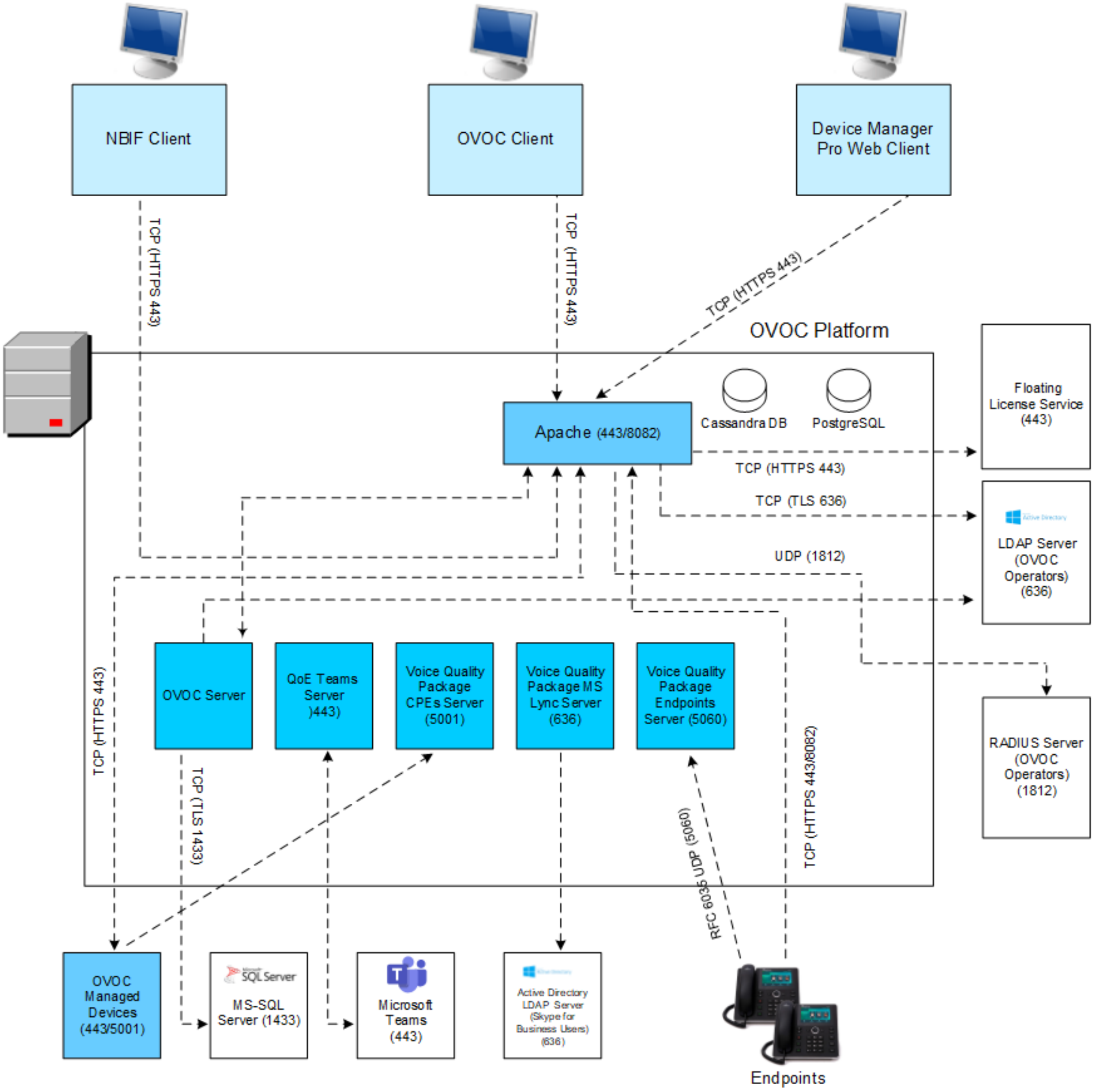
```
 Main Menu> Security> OVOC Voice Quality Package - SBC Communication
OVOC Voice Quality Package - SBC Communication: TCP
        >1.TCP  (SEM Server will be restarted)
         2.TLS  (SEM Server will be restarted)
         3.TLS/TCP      (SEM Server will be restarted)
         b.Back
         q.Quit to main Menu
```

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 27-24: OVOC Maximum Security Implementation


NBIF Client
OVOC Client
Device Manager Pro Web Client
TCP (HTTPS 443)
TCP (HTTPS 443)
TCP (HTTPS 443)
OVOC Platform
Apache (443/8082)
Cassandra DB
PostgreSQL
Floating License Service (443)
TCP (HTTPS 443)
TCP (TLS 636)
LDAP Server (OVOC Operators) (636)
UDP (1812)
RADIUS Server (OVOC Operators) (1812)
TCP (HTTPS 443)
OVOC Server
QoE Teams Server)443)
Voice Quality Package CPEs Server (5001)
Voice Quality Package MS Lync Server (636)
Voice Quality Package Endpoints Server (5060)
TCP (TLS 1433)
RFC 6035 UDP (5060)
TCP (HTTPS 443/8082)
OVOC Managed Devices (443/5001)
SQL Server
MS-SQL Server (1433)
Microsoft Teams (443)
Active Directory LDAP Server (Skype for Business Users) (636)
Endpoints

- 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 TLSv1.0, TLSv1.1, and TLSv1.2. **Default: TLSv1.2**

- See Server Certificates Update below
- See HTTP Security Settings Menu Options on page 270

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.

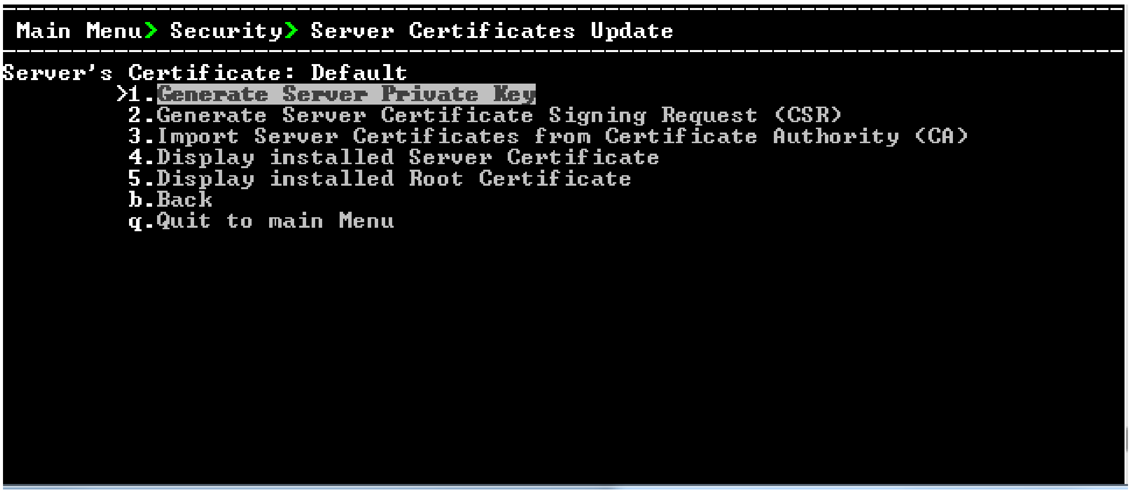
➢ The procedure for server certificates update consists of the following steps:

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 313).

➢ To generate server certificates:

1. From the Security menu, choose **Server Certificates Update**, and then press Enter.

Figure 27-25: Server Certificate Updates



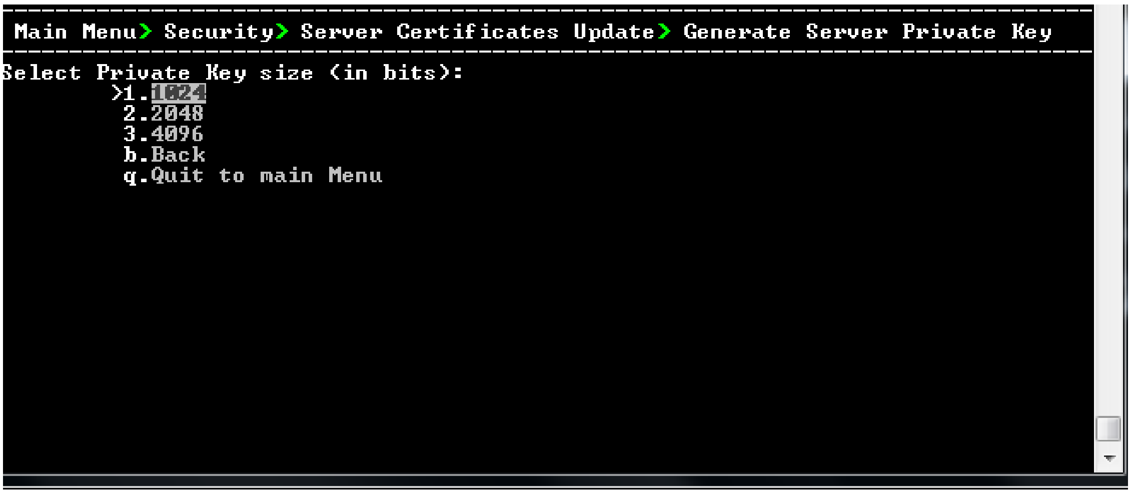
```
 Main Menu> Security> Server Certificates Update
Server's Certificate: Default
             >1.Generate Server Private Key
              2.Generate Server Certificate Signing Request (CSR)
              3.Import Server Certificates from Certificate Authority (CA)
              4.Display installed Server Certificate
              5.Display installed Root Certificate
              b.Back
              q.Quit to main Menu
```

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 27-26: Generate Server Private Key



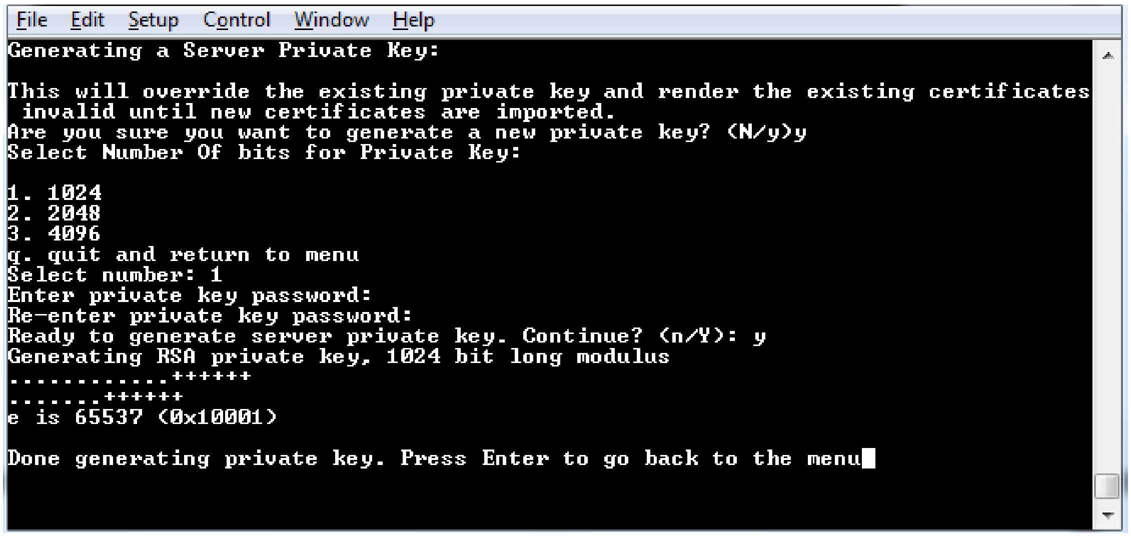
```
 Main Menu> Security> Server Certificates Update> Generate Server Private Key
Select Private Key size (in bits):
        >1.1024
         2.2048
         3.4096
         b.Back
         q.Quit to main Menu
```

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 27-27: Server Private Key Generated



```
Generating a Server Private Key:

This will override the existing private key and render the existing certificates
 invalid until new certificates are imported.
Are you sure you want to generate a new private key? (N/y)y
Select Number Of bits for Private Key:

1. 1024
2. 2048
3. 4096
q. quit and return to menu
Select number: 1
Enter private key password:
Re-enter private key password:
Ready to generate server private key. Continue? (n/Y): y
Generating RSA private key, 1024 bit long modulus
............++++++
.......++++++
e is 65537 (0x10001)

Done generating private key. Press Enter to go back to the menu
```

➢ **Step 2: Generate a CSR for the server:**

1. Select option **2**, and then press Enter.

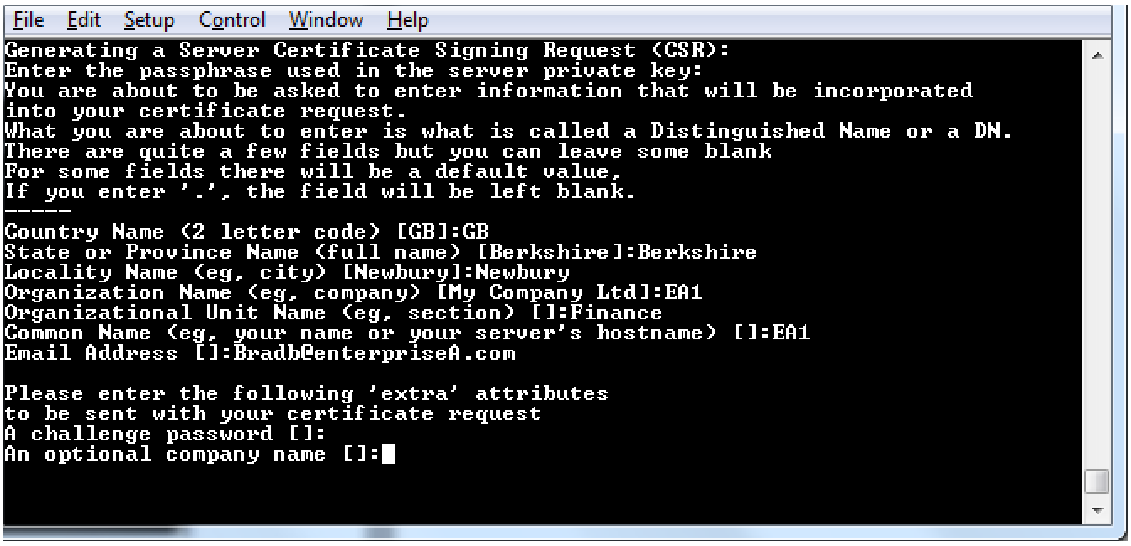
2. Enter the private key password (the password that you entered in the procedure above).

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 27-28: Generating a Server Certificate Signing Request (CSR)

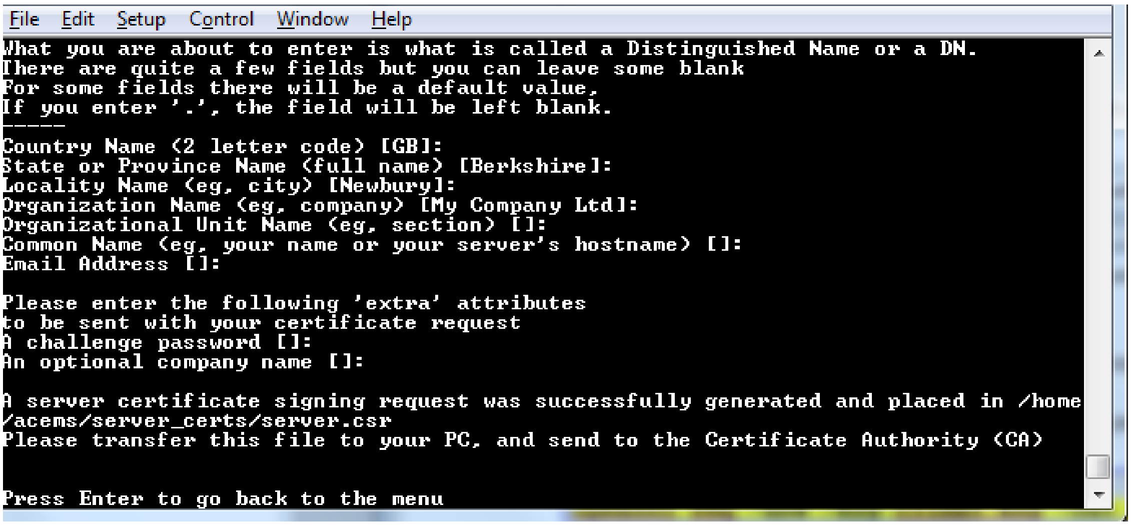


```
Generating a Server Certificate Signing Request (CSR):
Enter the passphrase used in the server private key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name (full name) [Berkshire]:Berkshire
Locality Name (eg, city) [Newbury]:Newbury
Organization Name (eg, company) [My Company Ltd]:EA1
Organizational Unit Name (eg, section) []:Finance
Common Name (eg, your name or your server's hostname) []:EA1
Email Address []:Bradb@enterpriseA.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

➢ 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 326.

Figure 27-29: Transfer CSR File to PC



```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

A server certificate signing request was successfully generated and placed in /home
/acems/server_certs/server.csr
Please transfer this file to your PC, and send to the Certificate Authority (CA)


Press Enter to go back to the menu
```

➢ 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 326.

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.

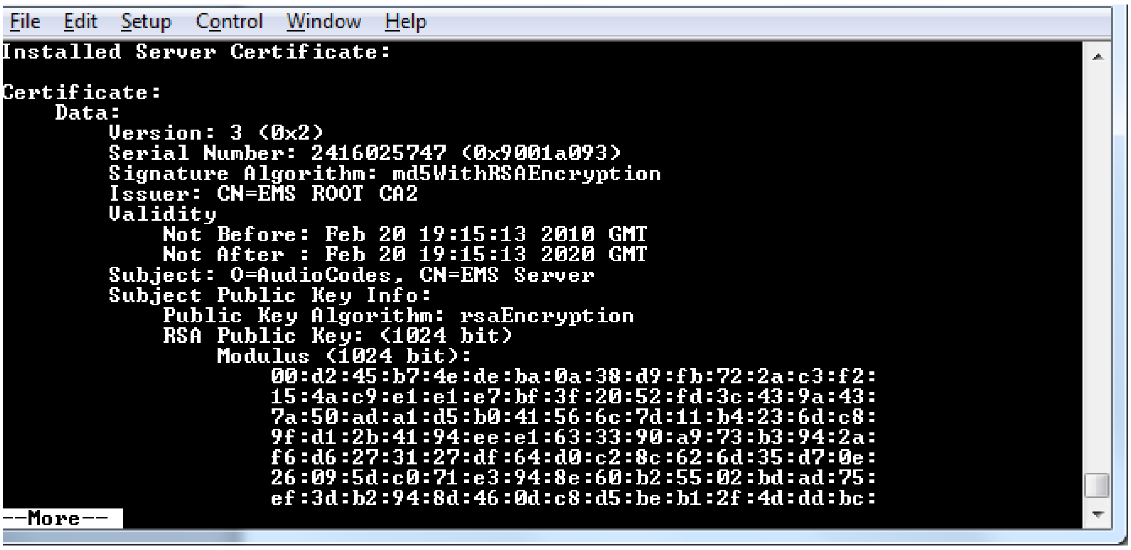
- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format and appear as follows (see Verifying and Converting Certificates on page 327 for information on converting files):

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1
UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0
MFowKjET
Tl6vqn5I27Oq/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 27-30: Installed Server Certificate

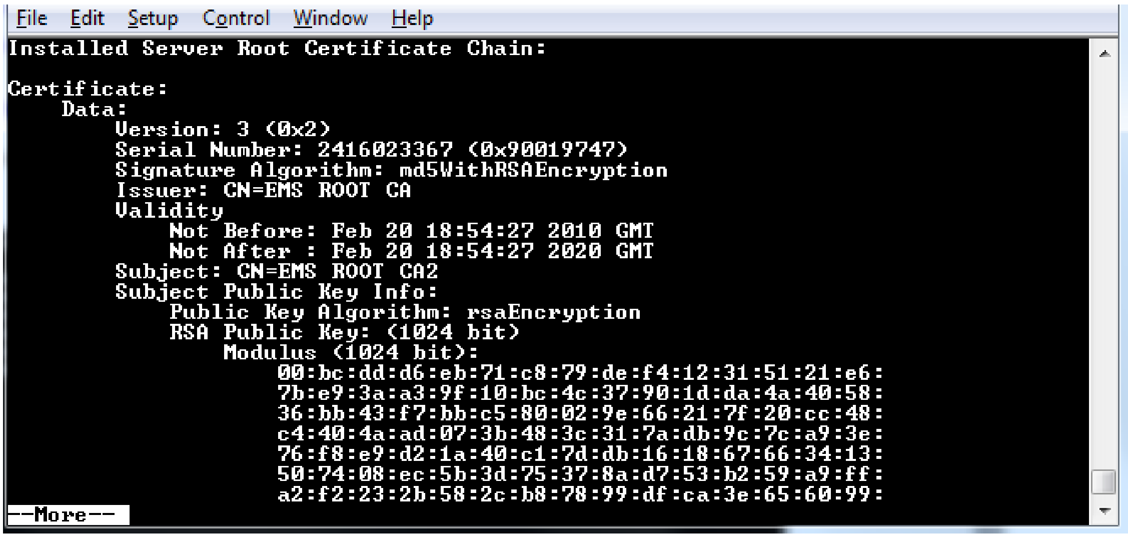


```
Installed Server Certificate:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2416025747 (0x9001a093)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=EMS ROOT CA2
        Validity
            Not Before: Feb 20 19:15:13 2010 GMT
            Not After : Feb 20 19:15:13 2020 GMT
        Subject: O=AudioCodes, CN=EMS Server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d2:45:b7:4e:de:ba:0a:38:d9:fb:72:2a:c3:f2:
                    15:4a:c9:e1:e1:e7:bf:3f:20:52:fd:3c:43:9a:43:
                    7a:50:ad:a1:d5:b0:41:56:6c:7d:11:b4:23:6d:c8:
                    9f:d1:2b:41:94:ee:e1:63:33:90:a9:73:b3:94:2a:
                    f6:d6:27:31:27:df:64:d0:c2:8c:62:6d:35:d7:0e:
                    26:09:5d:c0:71:e3:94:8e:60:b2:55:02:bd:ad:75:
                    ef:3d:b2:94:8d:46:0d:c8:d5:be:b1:2f:4d:dd:bc:
--More--
```

➢ Step 7: Verify the installed root certificate:

- Select Option **5**, and then press Enter. The installed root certificate is displayed:

Figure 27-31: Installed Root Certificate



```
Installed Server Root Certificate Chain:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2416023367 (0x90019747)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=EMS ROOT CA
        Validity
            Not Before: Feb 20 18:54:27 2010 GMT
            Not After : Feb 20 18:54:27 2020 GMT
        Subject: CN=EMS ROOT CA2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bc:dd:d6:eb:71:c8:79:de:f4:12:31:51:21:e6:
                    7b:e9:3a:a3:9f:10:bc:4c:37:90:1d:da:4a:40:58:
                    36:bb:43:f7:bb:c5:80:02:9e:66:21:7f:20:cc:48:
                    c4:40:4a:ad:07:3b:48:3c:31:7a:db:9c:7c:a9:3e:
                    76:f8:e9:d2:1a:40:c1:7d:db:16:18:67:66:34:13:
                    50:74:08:ec:5b:3d:75:37:8a:d7:53:b2:59:a9:ff:
                    a2:f2:23:2b:58:2c:b8:78:99:df:ca:3e:65:60:99:
--More--
```

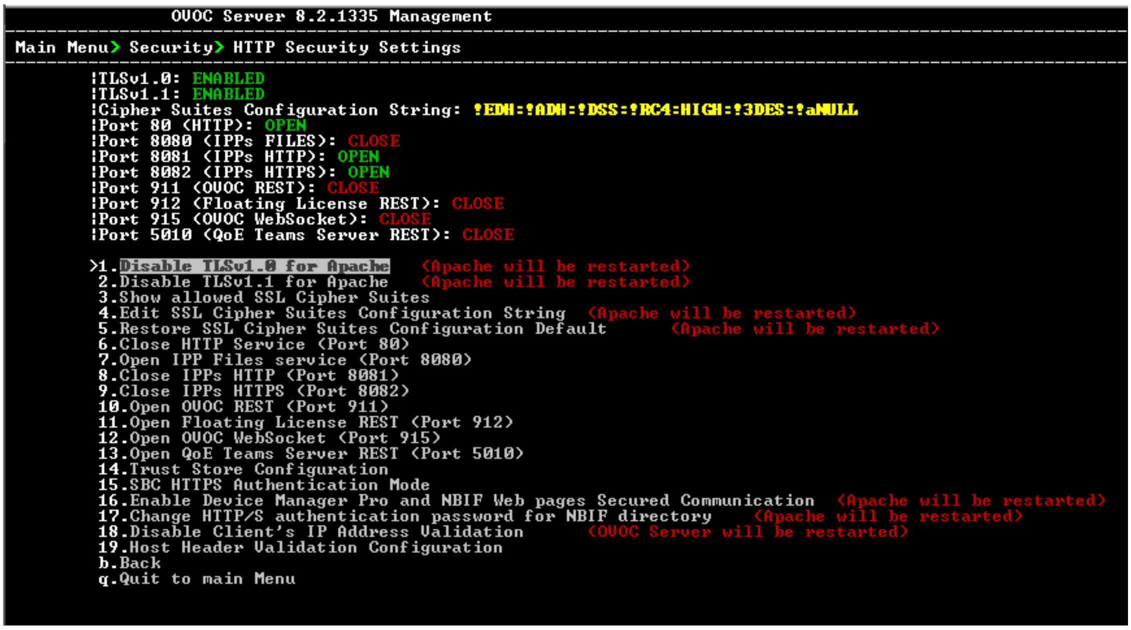
➢ Step 8: Install device certificates and perform supplementary procedures

- See Supplementary Security Procedures on page 313.

HTTP Security Settings Menu Options

From the OVOC Server Manager root menu, choose **HTTP Security Settings**.

Figure 27-32: HTTP Security Settings



```
                OVOC Server 8.2.1335 Management
---------------------------------------------------------------------------------------------------------
 Main Menu> Security> HTTP Security Settings
---------------------------------------------------------------------------------------------------------
        |TLSv1.0: ENABLED
        |TLSv1.1: ENABLED
        |Cipher Suites Configuration String: !EDH:!ADH:!DSS:!RC4:HIGH:!3DES:!aNULL
        |Port 80 (HTTP): OPEN
        |Port 8080 (IPPs FILES): CLOSE
        |Port 8081 (IPPs HTTP): OPEN
        |Port 8082 (IPPs HTTPS): OPEN
        |Port 911 (OVOC REST): CLOSE
        |Port 912 (Floating License REST): CLOSE
        |Port 915 (OVOC WebSocket): CLOSE
        |Port 5010 (QoE Teams Server REST): CLOSE

       >1.Disable TLSv1.0 for Apache   (Apache will be restarted)
        2.Disable TLSv1.1 for Apache   (Apache will be restarted)
        3.Show allowed SSL Cipher Suites
        4.Edit SSL Cipher Suites Configuration String  (Apache will be restarted)
        5.Restore SSL Cipher Suites Configuration Default       (Apache will be restarted)
        6.Close HTTP Service (Port 80)
        7.Open IPP Files service (Port 8080)
        8.Close IPPs HTTP (Port 8081)
        9.Close IPPs HTTPS (Port 8082)
        10.Open OVOC REST (Port 911)
        11.Open Floating License REST (Port 912)
        12.Open OVOC WebSocket (Port 915)
        13.Open QoE Teams Server REST (Port 5010)
        14.Trust Store Configuration
        15.SBC HTTPS Authentication Mode
        16.Enable Device Manager Pro and NBIF Web pages Secured Communication  (Apache will be restarted)
        17.Change HTTP/S authentication password for NBIF directory    (Apache will be restarted)
        18.Disable Client's IP Address Validation      (OVOC Server will be restarted)
        19.Host Header Validation Configuration
        b.Back
        q.Quit to main Menu
```

This menu allows you to configure the following Apache server security settings:

- Disable TLSv1.0 (TLSv1.0 for Apache on the next page

- Disable TLSv1.1 (TLSv1.1 for Apache below)

> ⚠ **Default: TLSv1.2**

- Show Allowed SSL Cipher Suites on the next page
- Edit SSL Cipher Suites Configuration String on the next page
- Restore SSL Cipher Suites Configuration Default on page 273
- Manage HTTP Service Port (80) on page 273
- Manage IPP Files Service Port (8080) on page 273
- Manage IPPs HTTP Port (8081) on page 274
- Manage IPPs HTTPS Port (8082) on page 274
- OVOC Rest (Port 911) on page 274
- (Floating License (Port 912) on page 275
- OVOC WebSocket (Port 915) on page 275
- QoE Teams Server REST (Port 5010) on page 275
- (Trust Store Configuration on page 275)
- (SBC HTTPS Authentication Mode on page 276)
- (Enable Device Manager Pro and NBIF Web Pages Secured Communication on page 277)
- (Change HTTP/S Authentication Password for NBIF Directory on page 277)
- (Disable Client's IP Address Validation on page 278)
- (Host Header Validation Configuration on page 278)

TLSv1.0 for Apache

This option enables and disables TLSv1.0 on port 443 (Apache server is restarted).

➢ **To enable or disable TLSv1.0:**

- From the HTTP Security Settings menu, select option **Enable TLSv1.0 for Apache**, and then press Enter.

> ⚠ When TLSv1.1 is disabled, TLSv1.0 is also disabled. Likewise, if TLSv1.0 is enabled, TLSv1.1 is also enabled.

Apache server is restarted. Default (enabled).

TLSv1.1 for Apache

This option enables and disables TLS Version 1.1 on port 443 (Apache server is restarted).

➢ To enable or disable TLSv1.1:

- From the HTTP Security Settings menu, select option **Enable TLSv1.1 for Apache**, and then press Enter.

  Default (enabled). Apache server is restarted.

> When TLSv1.1 is disabled, TLSv1.0 is also disabled. Likewise, if TLSv1.0 is enabled, TLSv1.1 is also enabled.

Show Allowed SSL Cipher Suites

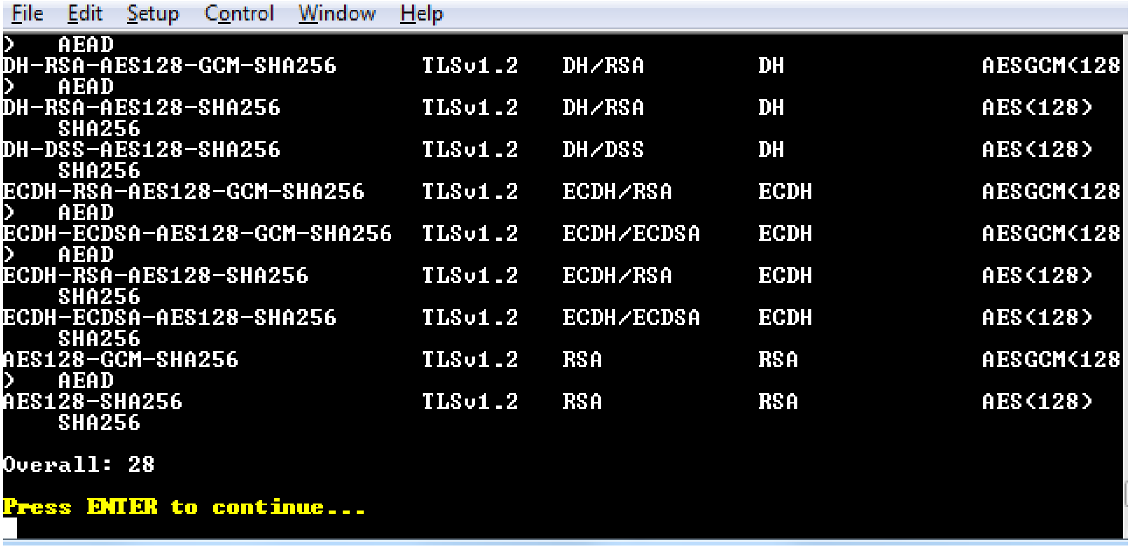
This option allows you to view the currently configured SSL cipher suites.

➢ 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 27-33: Show Allowed SSL Cipher Suites



```
>    AEAD
DH-RSA-AES128-GCM-SHA256      TLSv1.2   DH/RSA      DH          AESGCM(128
>    AEAD
DH-RSA-AES128-SHA256          TLSv1.2   DH/RSA      DH          AES(128)
     SHA256
DH-DSS-AES128-SHA256          TLSv1.2   DH/DSS      DH          AES(128)
     SHA256
ECDH-RSA-AES128-GCM-SHA256    TLSv1.2   ECDH/RSA    ECDH        AESGCM(128
>    AEAD
ECDH-ECDSA-AES128-GCM-SHA256  TLSv1.2   ECDH/ECDSA  ECDH        AESGCM(128
>    AEAD
ECDH-RSA-AES128-SHA256        TLSv1.2   ECDH/RSA    ECDH        AES(128)
     SHA256
ECDH-ECDSA-AES128-SHA256      TLSv1.2   ECDH/ECDSA  ECDH        AES(128)
     SHA256
AES128-GCM-SHA256             TLSv1.2   RSA         RSA         AESGCM(128
>    AEAD
AES128-SHA256                 TLSv1.2   RSA         RSA         AES(128)
     SHA256

Overall: 28

Press ENTER to continue...
```

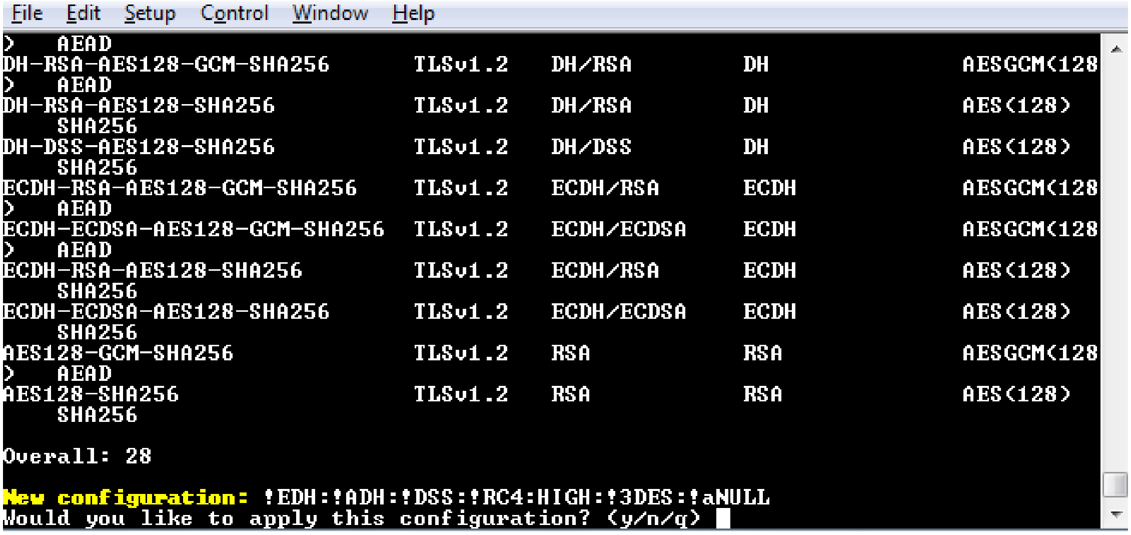
Edit SSL Cipher Suites Configuration String

This option allows you to edit the SSL Cipher Suites configuration string.

➢ To edit the SSL cipher suites configuration string:

1. From the HTTP Security Settings menu, select option **Edit SSL Cipher Suites Configuration String**, and then press Enter.

Figure 27-34: Show SSL Cipher Suites Configuration



```
>    AEAD
DH-RSA-AES128-GCM-SHA256        TLSv1.2    DH/RSA        DH              AESGCM(128
>    AEAD
DH-RSA-AES128-SHA256            TLSv1.2    DH/RSA        DH              AES(128)
     SHA256
DH-DSS-AES128-SHA256            TLSv1.2    DH/DSS        DH              AES(128)
     SHA256
ECDH-RSA-AES128-GCM-SHA256      TLSv1.2    ECDH/RSA      ECDH            AESGCM(128
>    AEAD
ECDH-ECDSA-AES128-GCM-SHA256    TLSv1.2    ECDH/ECDSA    ECDH            AESGCM(128
>    AEAD
ECDH-RSA-AES128-SHA256          TLSv1.2    ECDH/RSA      ECDH            AES(128)
     SHA256
ECDH-ECDSA-AES128-SHA256        TLSv1.2    ECDH/ECDSA    ECDH            AES(128)
     SHA256
AES128-GCM-SHA256               TLSv1.2    RSA           RSA             AESGCM(128
>    AEAD
AES128-SHA256                   TLSv1.2    RSA           RSA             AES(128)
     SHA256

Overall: 28

New configuration: !EDH:!ADH:!DSS:!RC4:HIGH:!3DES:!aNULL
Would you like to apply this configuration? (y/n/q)
```

2. Edit the new configuration and select **y** to apply the changes.

3. Run the **Show Allowed SSL Cipher Suites** command to display the new configuration.

Restore SSL Cipher Suites Configuration Default

This option allows you to restore the SSL Cipher Suites to the OVOC default values.

➢ To restore the SSL Cipher Suites Configuration default:

- From the HTTP Security Settings menu, select **Restore SSL Cipher Suites Configuration Default**, and then press Enter.

Manage HTTP Service Port (80)

This option allows you to open and close HTTP Service Port 80.

➢ To open/close HTTP Service (Port 80):

- In the HTTP Security Settings menu, choose option **Open/Close HTTP Service (Port 80)**, and then press Enter.

  This HTTP port is used for the connection between the OVOC server and all AudioCodes devices with the Device Manager Pro Web browser.

Manage IPP Files Service Port (8080)

This option allows you to open and close Service Port 8080.

➢ To open/close IPPs files service (port 8080):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs files(Port 8080)**, and then press Enter.

This HTTP port is used for downloading firmware and configuration files from the OVOC server to the endpoints.

⚠ This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTP Port (8081)

This option allows you to open and close HTTP port 8081.

➢ **To open/close IPPs HTTP (Port 8081):**

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTP (Port 8081)**, and then press Enter.

  This HTTP port is used for sending REST updates from the endpoints to the OVOC server, such as alarms and statuses.

⚠ This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTPS Port (8082)

This option allows to open and close HTTPS port 8082.

➢ **To open/close IPPs HTTPS (Port 8082):**

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTPS (Port 8082)**, and then press Enter.

  This HTTPS port is used for sending secure REST updates from the endpoints to the OVOC server, such as alarms and statuses (HTTPS without certificate authentication).

⚠ This option is reserved for backward compatibility with older device versions.

OVOC Rest (Port 911)

This option allows you to open and close the REST port connection for (internal) port and server debugging.

➢ **To configure OVOC REST:**

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC REST (Port 911)**, and then press Enter.

Floating License (Port 912)

This option allows you to open and close the Floating license REST service (internal) and Floating license service debugging.

➢ **To open/close the Floating License port:**

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.

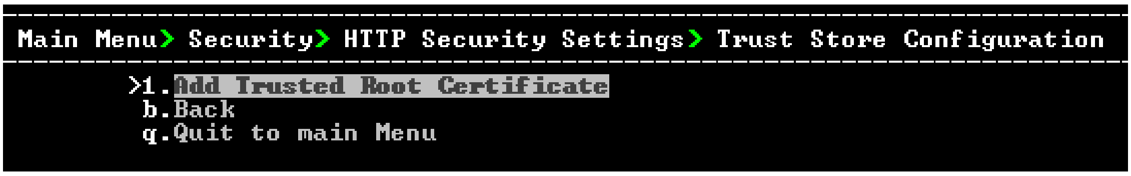
Trust Store Configuration

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 27-35: Trust Store Configuration



```
------------------------------------------------------------------------------
 Main Menu> Security> HTTP Security Settings> Trust Store Configuration
------------------------------------------------------------------------------
        >1.Add Trusted Root Certificate
         b.Back
         q.Quit to main Menu
```

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:

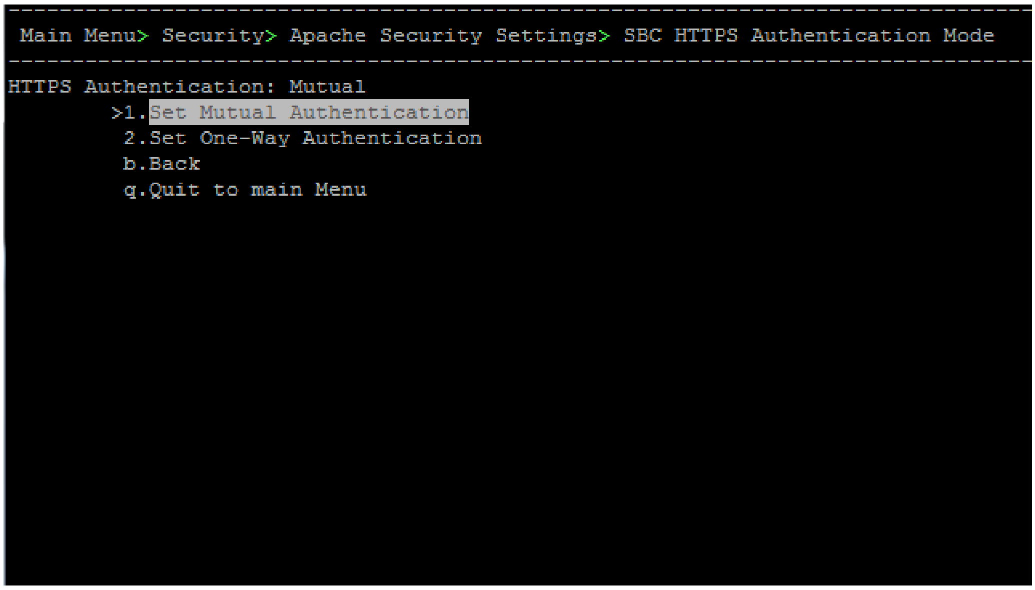
- **Mutual Authentication:** the OVOC authenticates the device connection request using certificates and the device authenticates the OVOC connection request using certificates. When this option is configured:
  - The same root CA must sign the certificate that is loaded to the device and certificate 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 317).
- **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 265 to load the certificate file to the OVOC server.
> - See Step 5: Configure HTTPS Parameters on the Device on page 317 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 27-36: SBC HTTPS Authentication



```
---------------------------------------------------------------------------------
 Main Menu> Security> Apache Security Settings> SBC HTTPS Authentication Mode
---------------------------------------------------------------------------------
HTTPS Authentication: Mutual
        >1.Set Mutual Authentication
         2.Set One-Way Authentication
         b.Back
         q.Quit to main Menu
```

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

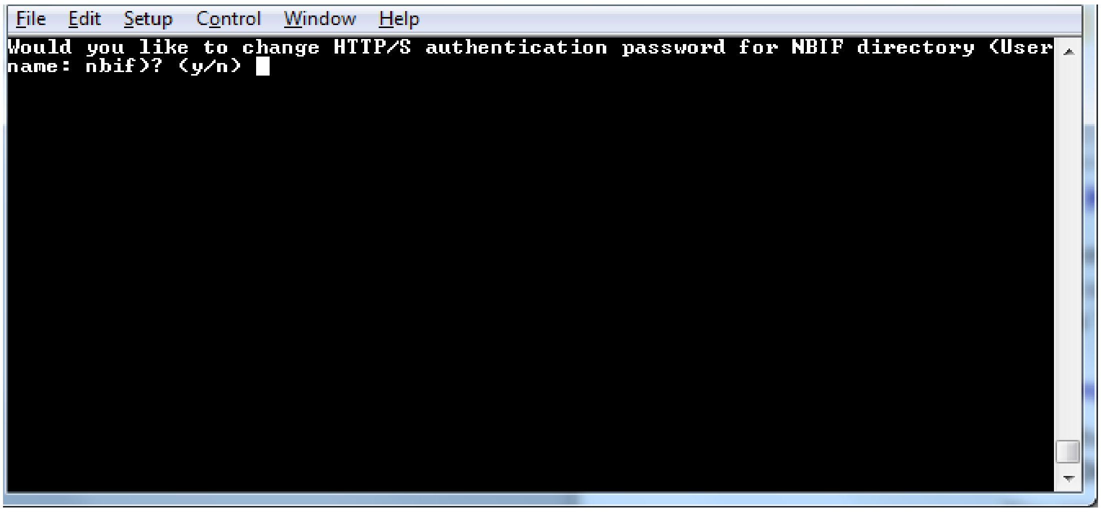
This option enables you to change the password for logging to the OVOC client from a NBIF client over an HTTP/S connection. The default user name is “nbif” and default password is “pass_1234”.

➢ 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 27-37: Change HTTP/S Authentication Password for NBIF Directory



```
Would you like to change HTTP/S authentication password for NBIF directory (User
name: nbif)? (y/n)
```

2. Enter the new password.
3. Reenter the new password.

A confirmation message is displayed and the Apache server is restarted.

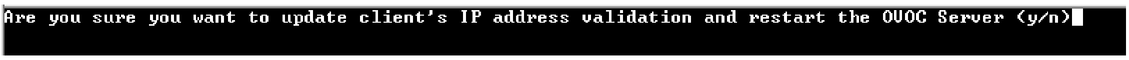
Disable Client's IP Address Validation

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 27-38: Confirm Disabling of Client IP Address Validation



```
Are you sure you want to update client's IP address validation and restart the OVOC Server (y/n)
```

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

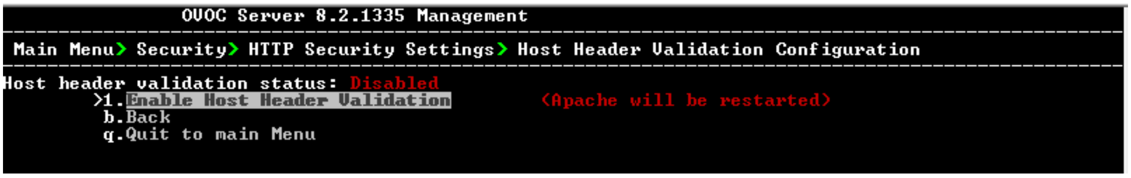
Host Header Validation Configuration

This option prevents host header injection attacks through the configuration of a list of valid OVOC server IP addresses and FQDNs.

➢ **To enable Host Header validation:**

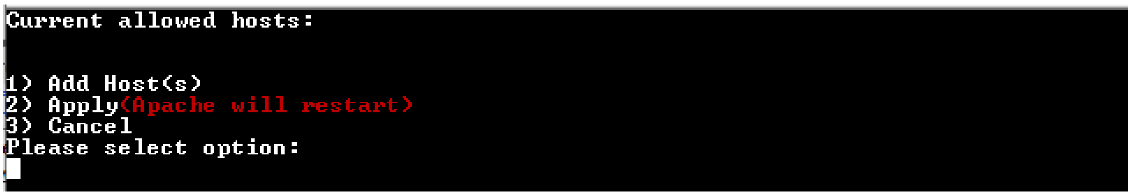
1. From the HTTP Security Settings menu, choose **Enable Host Header Validation**, and then press Enter.

Figure 27-39: Host Header Validation



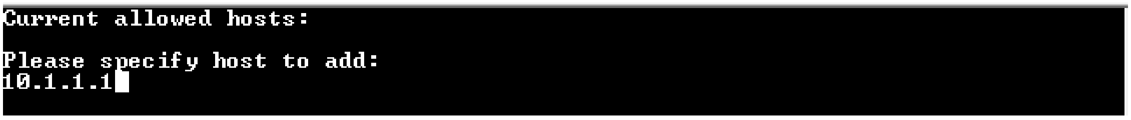
```
                    OVOC Server 8.2.1335 Management
----------------------------------------------------------------------------------------------------
 Main Menu> Security> HTTP Security Settings> Host Header Validation Configuration
----------------------------------------------------------------------------------------------------
Host header validation status: Disabled
        >1.Enable Host Header Validation          (Apache will be restarted)
         b.Back
         q.Quit to main Menu
```

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



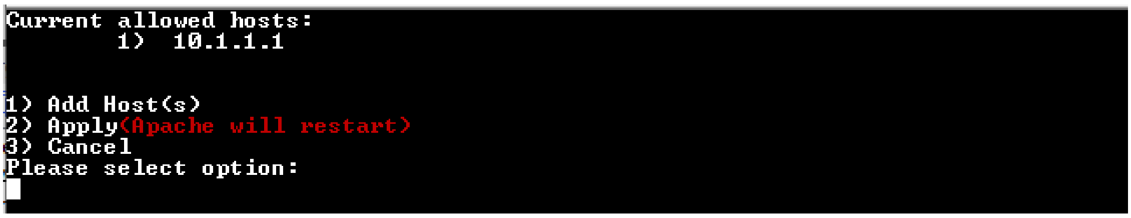
```
Current allowed hosts:

1) Add Host(s)
2) Apply(Apache will restart)
3) Cancel
Please select option:
```

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



```
Current allowed hosts:

Please specify host to add:
10.1.1.1
```

You are prompted to restart the Apache server.



```
Current allowed hosts:
        1)  10.1.1.1


1) Add Host(s)
2) Apply(Apache will restart)
3) Cancel
Please select option:
```

28 Diagnostics

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

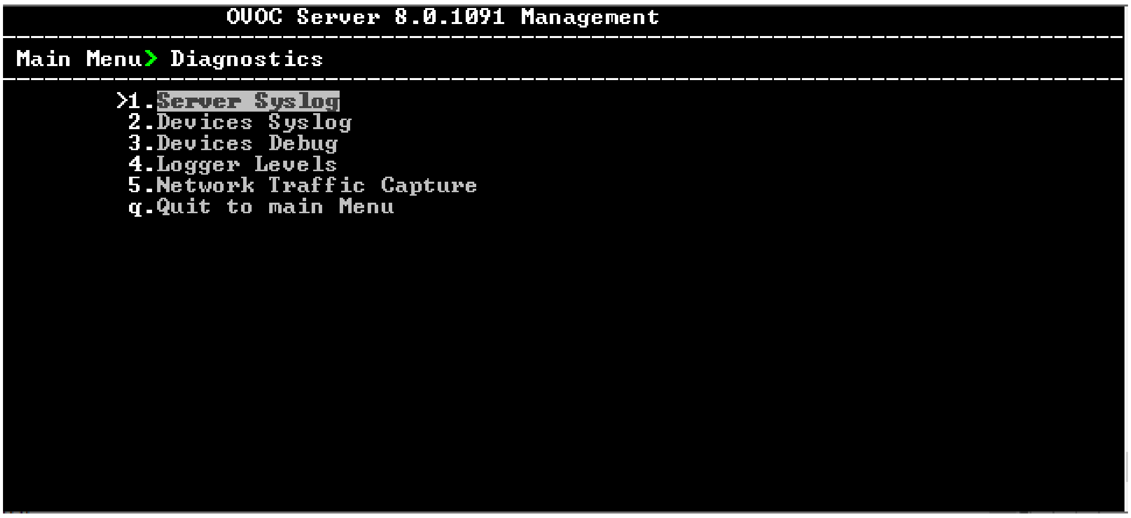
An IPv6 address can be configured for the following:

- 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 28-1: Diagnostics



```
                    OVOC Server 8.0.1091 Management
--------------------------------------------------------------------------------
Main Menu> Diagnostics
--------------------------------------------------------------------------------
        >1.Server Syslog
         2.Devices Syslog
         3.Devices Debug
         4.Logger Levels
         5.Network Traffic Capture
         q.Quit to main Menu
```

This menu includes the following options:

- Server Syslog Configuration (Server Syslog Configuration below).
- Devices Syslog Configuration (Devices Syslog Configuration on page 283).
- Devices Debug Configuration (Devices Debug Configuration on page 284).
- Server Logger Levels (Server Logger Levels on page 285)
- Network Traffic Capture (Network Traffic Capture on page 286)

Server Syslog Configuration

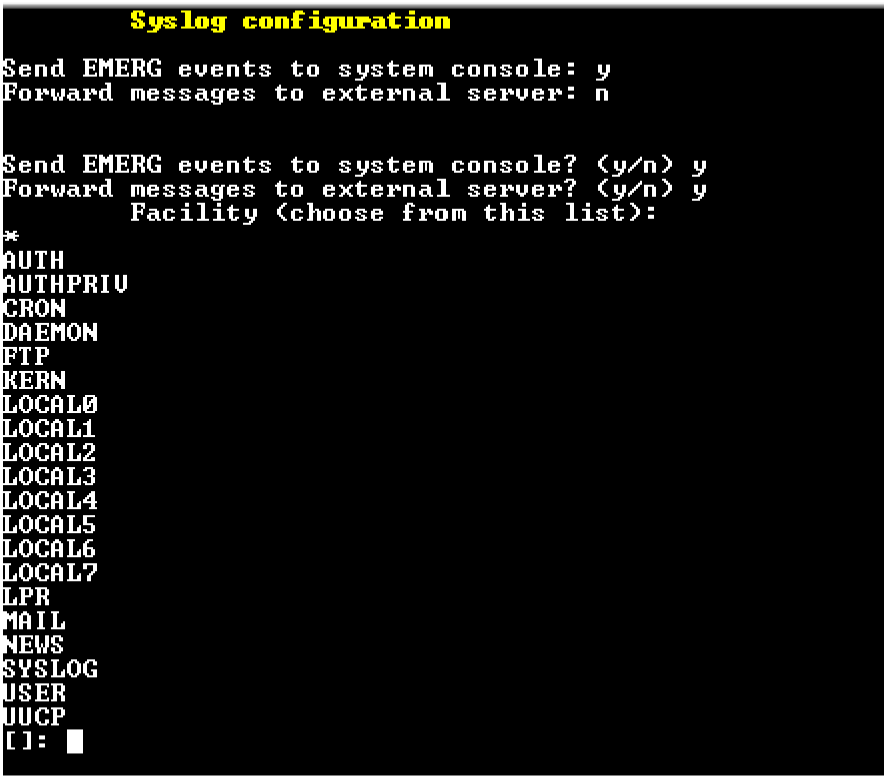
This section describes how to send OVOC server Operating System (OS)-related syslog EMERG events to the system console and other OVOC server OS related messages to a designated external server.

➢ 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 28-2: Syslog Configuration



```
        Syslog configuration

Send EMERG events to system console: y
Forward messages to external server: n


Send EMERG events to system console? (y/n) y
Forward messages to external server? (y/n) y
        Facility (choose from this list):
*
AUTH
AUTHPRIV
CRON
DAEMON
FTP
KERN
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: █
```

3. You are prompted to forward messages to an external server, type **y**, and then press Enter. The OVOC server is rebooted.

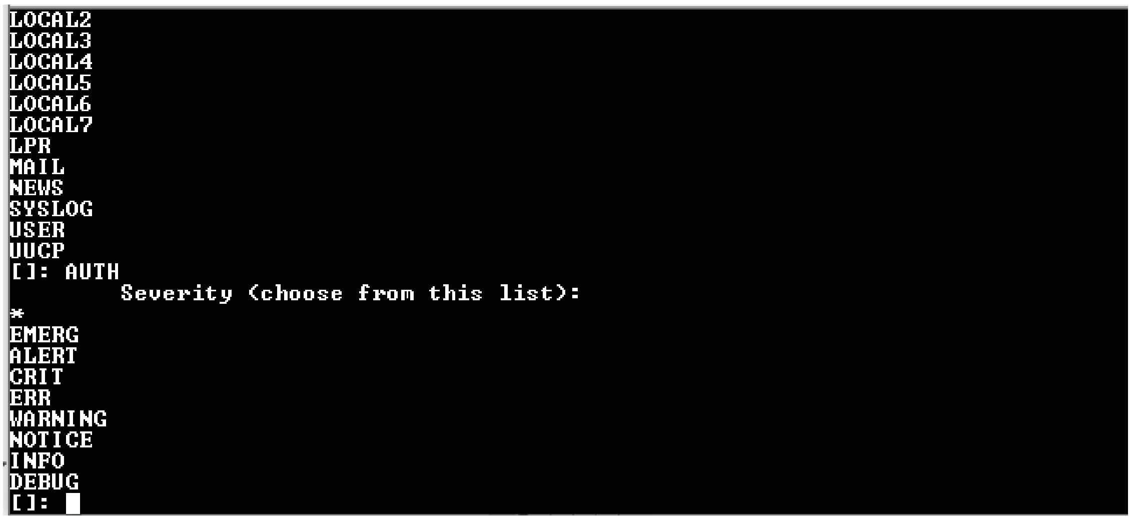
4. Type one of the following **Facilities** from the list (case-sensitive) or select the wildcard * to select all facilities in the list, and then press Enter:

   - **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 28-3: Syslog Severities



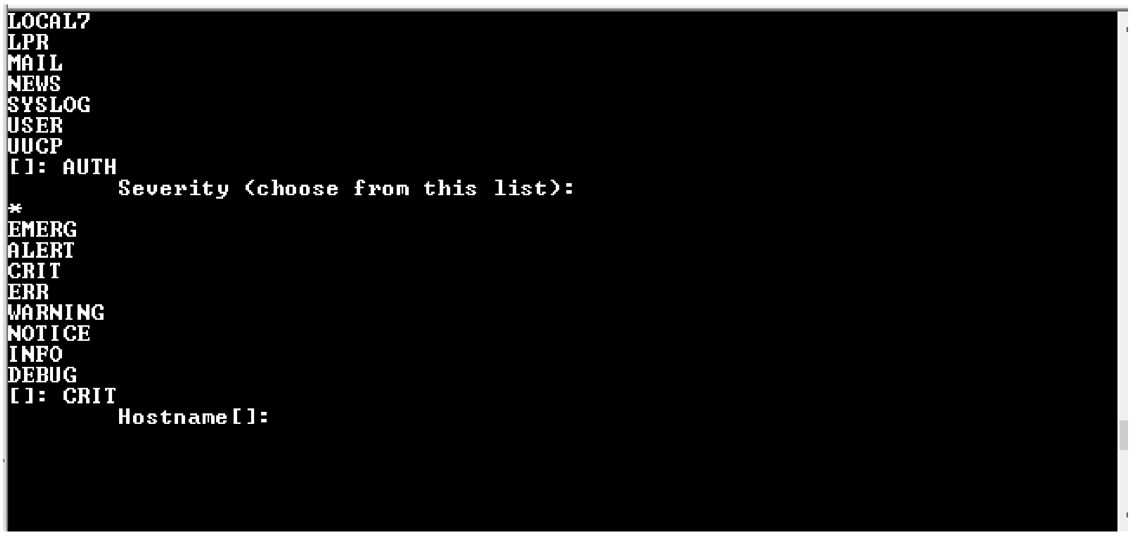
```
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: AUTH
        Severity (choose from this list):
*
EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG
[]:
```

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.

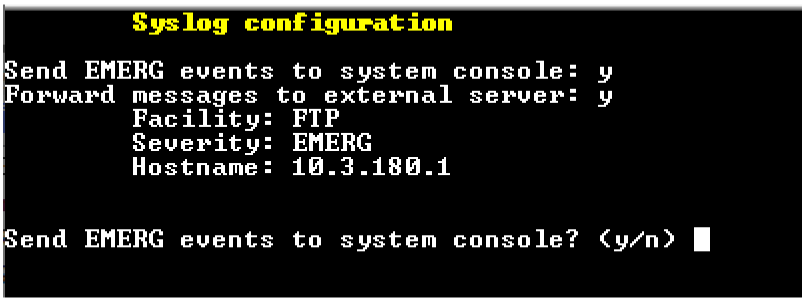
6. Type the external server Hostname or IP address of the Syslog server.

Figure 28-4: Syslog Hostname



```
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: AUTH
        Severity (choose from this list):
*
EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG
[]: CRIT
        Hostname[]:
```

The example Message forwarding configuration is shown below.



```
         Syslog configuration

Send EMERG events to system console: y
Forward messages to external server: y
        Facility: FTP
        Severity: EMERG
        Hostname: 10.3.180.1

Send EMERG events to system console? (y/n)
```

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.

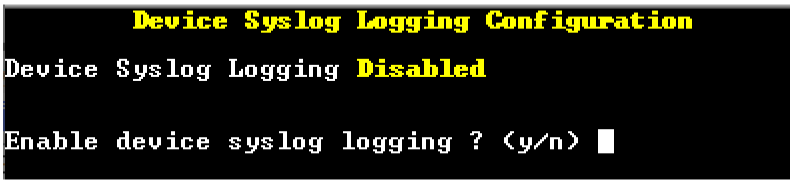
The syslog log file 'syslog' is located in the following OVOC server directory:

/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.



```
        Device Syslog Logging Configuration
Device Syslog Logging Disabled

Enable device syslog logging ? (y/n)
```

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

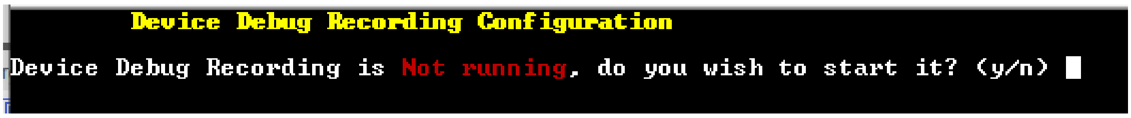
The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close; if the file reaches 10MB in less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

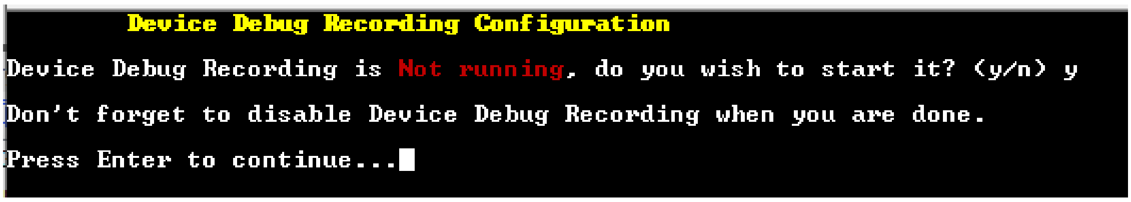
1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.

   A message is displayed indicating that debug recording is either enabled or disabled.



```
            Device Debug Recording Configuration

Device Debug Recording is Not running, do you wish to start it? (y/n)
```

2. Type **y** and then press Enter to enable Device Debug Recording.



```
        Device Debug Recording Configuration
Device Debug Recording is Not running, do you wish to start it? (y/n) y
Don't forget to disable Device Debug Recording when you are done.
Press Enter to continue...
```

3. Press Enter to continue.

   Recording files are saved in /data/NBIF/mgDebug directory on the server.

It is highly recommended to disable this option when you have completed recording because this feature heavily utilizes system resources.

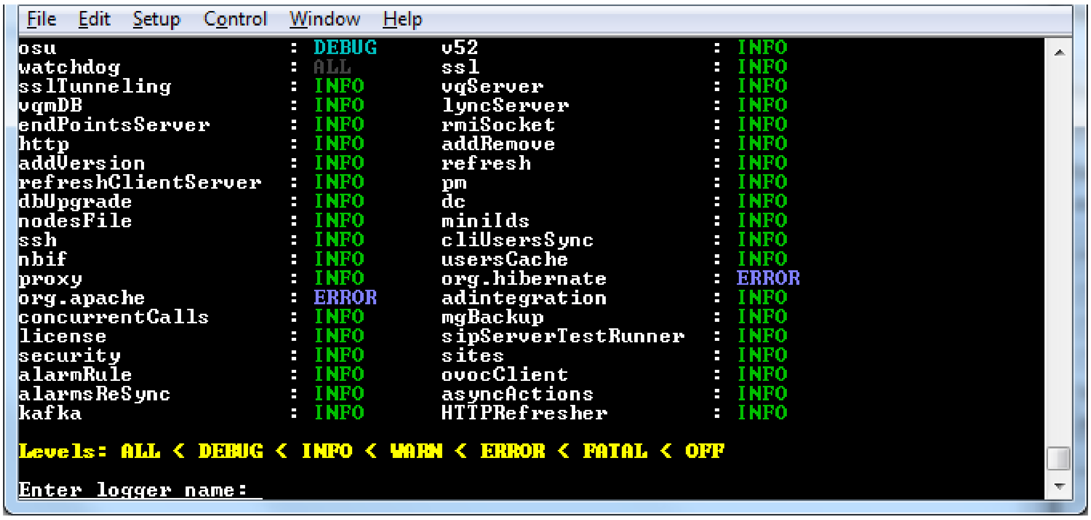
Server Logger Levels

This option allows you to change the log level for the different OVOC server log directories.

After completing the debugging, revert to the previous configuration to prevent over utilization of CPU resources.

➢ To change the <tc> server logger level:

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



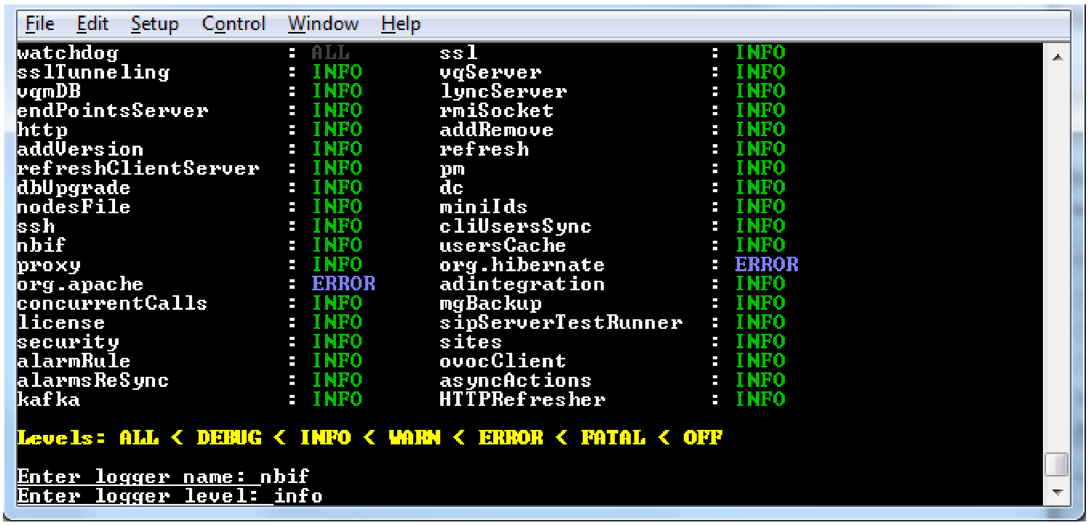
```
osu                     : DEBUG     v52                       : INFO
watchdog                : ALL       ssl                       : INFO
sslTunneling            : INFO      vqServer                  : INFO
vqmDB                   : INFO      lyncServer                : INFO
endPointsServer         : INFO      rmiSocket                 : INFO
http                    : INFO      addRemove                 : INFO
addVersion              : INFO      refresh                   : INFO
refreshClientServer     : INFO      pm                        : INFO
dbUpgrade               : INFO      dc                        : INFO
nodesFile               : INFO      miniIds                   : INFO
ssh                     : INFO      cliUsersSync              : INFO
nbif                    : INFO      usersCache                : INFO
proxy                   : INFO      org.hibernate             : ERROR
org.apache              : ERROR     adintegration             : INFO
concurrentCalls         : INFO      mgBackup                  : INFO
license                 : INFO      sipServerTestRunner       : INFO
security                : INFO      sites                     : INFO
alarmRule               : INFO      ovocClient                : INFO
alarmsReSync            : INFO      asyncActions              : INFO
kafka                   : INFO      HTTPRefresher             : INFO

Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

Enter logger name: _
```

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 28-5: Server Logger Name and Level



```
watchdog                : ALL       ssl                    : INFO
sslTunneling            : INFO      vqServer               : INFO
vqmDB                   : INFO      lyncServer             : INFO
endPointsServer         : INFO      rmiSocket              : INFO
http                    : INFO      addRemove              : INFO
addVersion              : INFO      refresh                : INFO
refreshClientServer     : INFO      pm                     : INFO
dbUpgrade               : INFO      dc                     : INFO
nodesFile               : INFO      miniIds                : INFO
ssh                     : INFO      cliUsersSync           : INFO
nbif                    : INFO      usersCache             : INFO
proxy                   : INFO      org.hibernate          : ERROR
org.apache              : ERROR     adintegration          : INFO
concurrentCalls         : INFO      mgBackup               : INFO
license                 : INFO      sipServerTestRunner    : INFO
security                : INFO      sites                  : INFO
alarmRule               : INFO      ovocClient             : INFO
alarmsReSync            : INFO      asyncActions           : INFO
kafka                   : INFO      HTTPRefresher          : INFO

Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

Enter logger name: nbif
Enter logger level: info
```

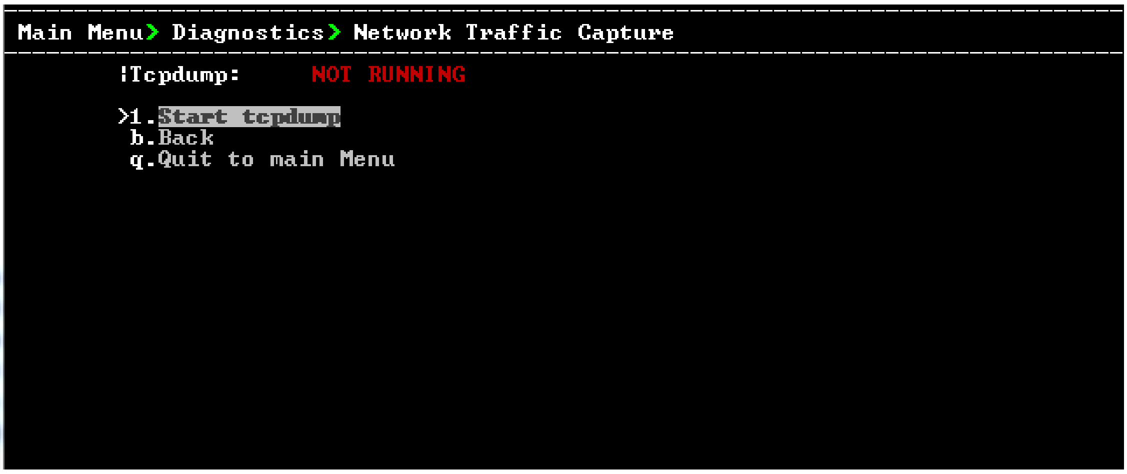
Network Traffic Capture

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 28-6: Network Traffic Capture

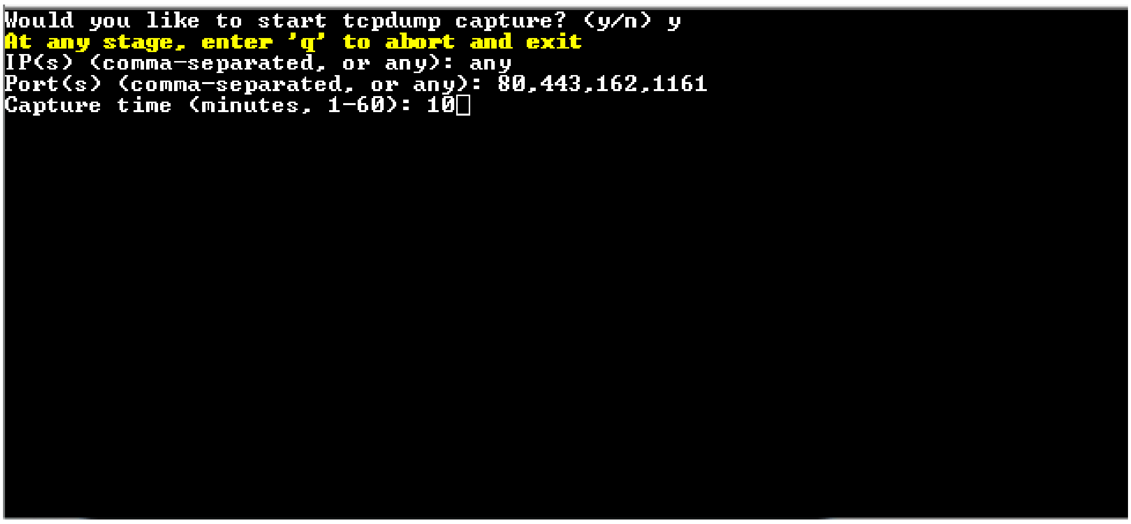


```
 Main Menu> Diagnostics> Network Traffic Capture
----------------------------------------------------------------------
        !Tcpdump:      NOT RUNNING

        >1.Start tcpdump
         b.Back
         q.Quit to main Menu
```

2. Select option **1 Start tcpdump.**

3. Select **y** to start the tcpdump.

Figure 28-7: TCP Dump



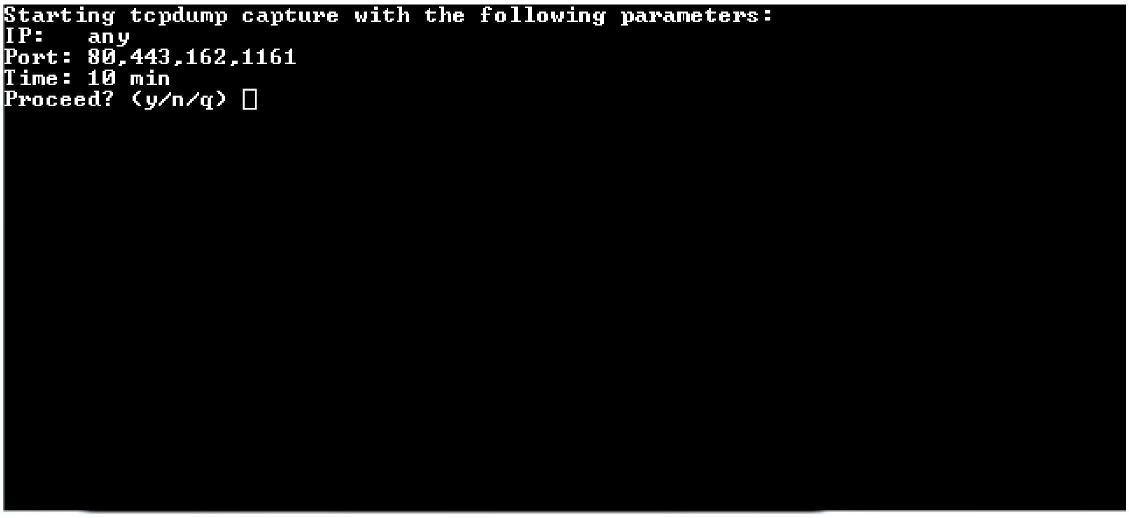
```
Would you like to start tcpdump capture? (y/n) y
At any stage, enter 'q' to abort and exit
IP(s) (comma-separated, or any): any
Port(s) (comma-separated, or any): 80,443,162,1161
Capture time (minutes, 1-60): 10
```

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.

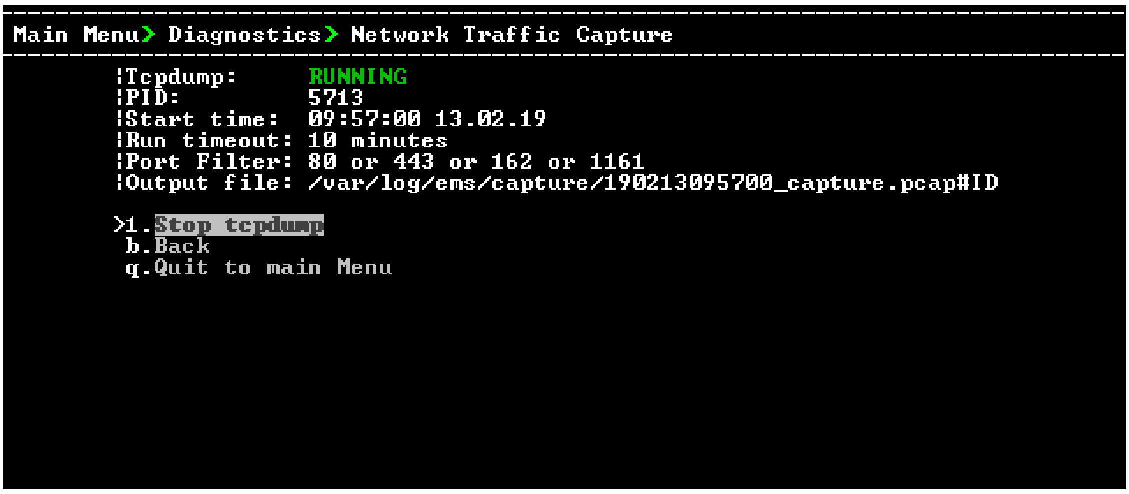
Figure 28-8: Starting TCP Dump



```
Starting tcpdump capture with the following parameters:
IP:    any
Port: 80,443,162,1161
Time: 10 min
Proceed? (y/n/q)
```

7. Select **y** to proceed.

Figure 28-9: TCP Dump Running



```
Main Menu> Diagnostics> Network Traffic Capture

       |Tcpdump:      RUNNING
       |PID:          5713
       |Start time:   09:57:00 13.02.19
       |Run timeout:  10 minutes
       |Port Filter:  80 or 443 or 162 or 1161
       |Output file:  /var/log/ems/capture/190213095700_capture.pcap#ID

       >1.Stop tcpdump
        b.Back
        q.Quit to main Menu
```

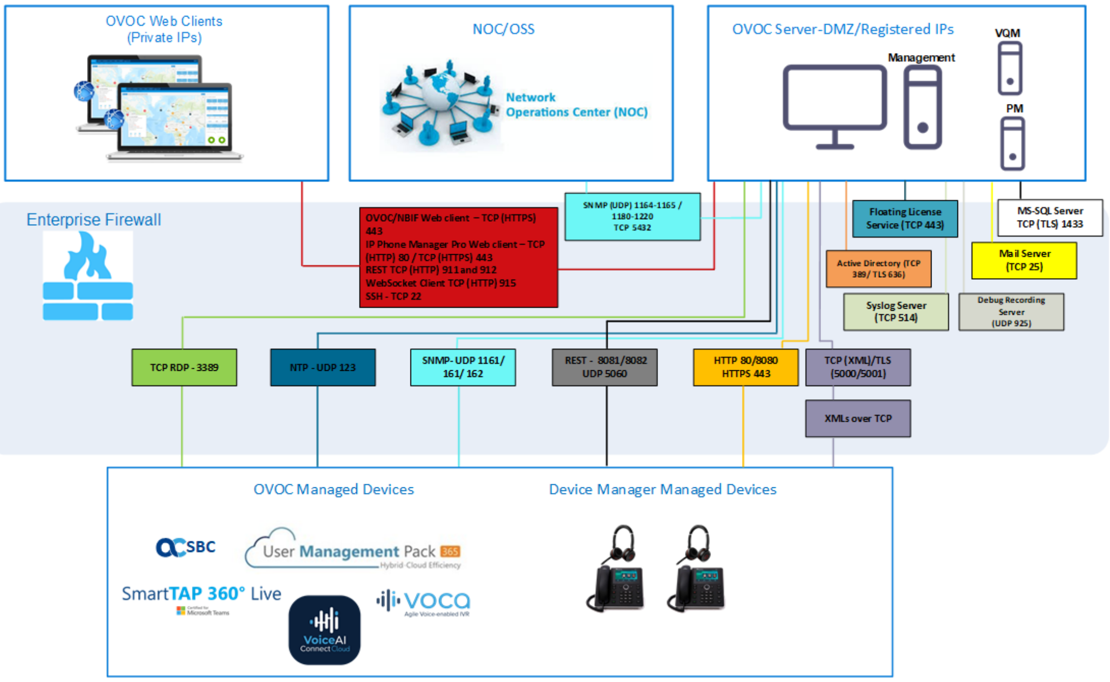
Part VII

Configuring the Firewall

This part describes how to configure the OVOC firewall.

29 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.


OVOC Web Clients
(Private IPs)
NOC/OSS
Network
Operations Center (NOC)
OVOC Server-DMZ/Registered IPs
Management
VQM
PM
Enterprise Firewall
OVOC/NBIF Web client – TCP (HTTPS) 443
IP Phone Manager Pro Web client – TCP (HTTP) 80 / TCP (HTTPS) 443
REST TCP (HTTP) 911 and 912
WebSocket Client TCP (HTTP) 915
SSH - TCP 22
SNMP (UDP) 1164-1165 / 1180-1220
TCP 5432
Floating License Service (TCP 443)
MS-SQL Server TCP (TLS) 1433
Active Directory (TCP 389/ TLS 636)
Mail Server (TCP 25)
Syslog Server (TCP 514)
Debug Recording Server (UDP 925)
TCP RDP - 3389
NTP - UDP 123
SNMP- UDP 1161/ 161/ 162
REST - 8081/8082 UDP 5060
HTTP 80/8080 HTTPS 443
TCP (XML)/TLS (5000/5001)
XMLs over TCP
OVOC Managed Devices
Device Manager Managed Devices
SBC
User Management Pack 365
Hybrid-Cloud Efficiency
SmartTAP 360° Live
VOCA
Agile Voice-enabled IVR
VoiceAI Connect Cloud

See also:

- Cloud Architecture Mode (WebSocket Tunnel) Firewall Settings on page 295
- Firewall Settings for NAT Deployment on page 295
- Firewall Settings for OVOC Server Provider (Single Node)

Table 29-1: 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 debugging. ■ 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 Communication (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 29-2: 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 218).	×	N/A	5432

Table 29-3: 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 29-1: 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 152), 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 147.

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 147.	.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 29-4: 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	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. ■ 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.

30 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 302

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:

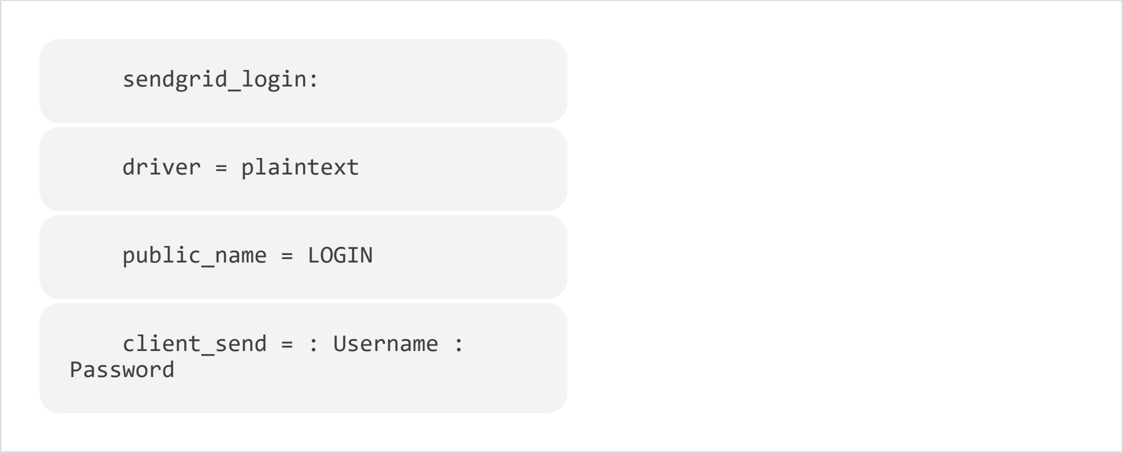
```
 begin transports

    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.

31 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

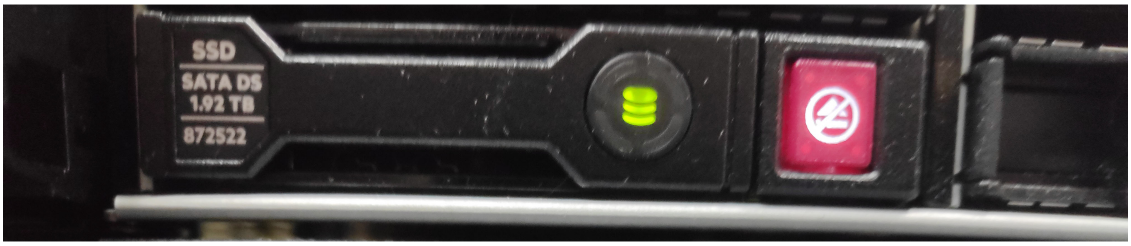
This procedure requires the following:

- 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 31-1: 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).

32 Managing Clusters

This appendix describes how to manually migrate or move OVOC VMs to another cluster node.

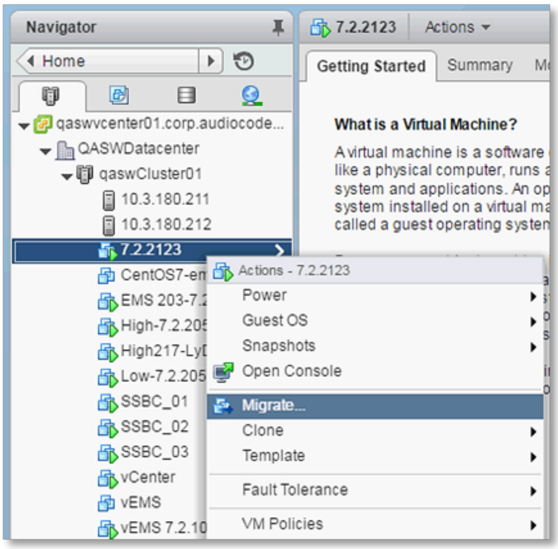
Migrating OVOC Virtual Machines in a VMware Cluster

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

➢ To migrate your OVOC virtual machine:

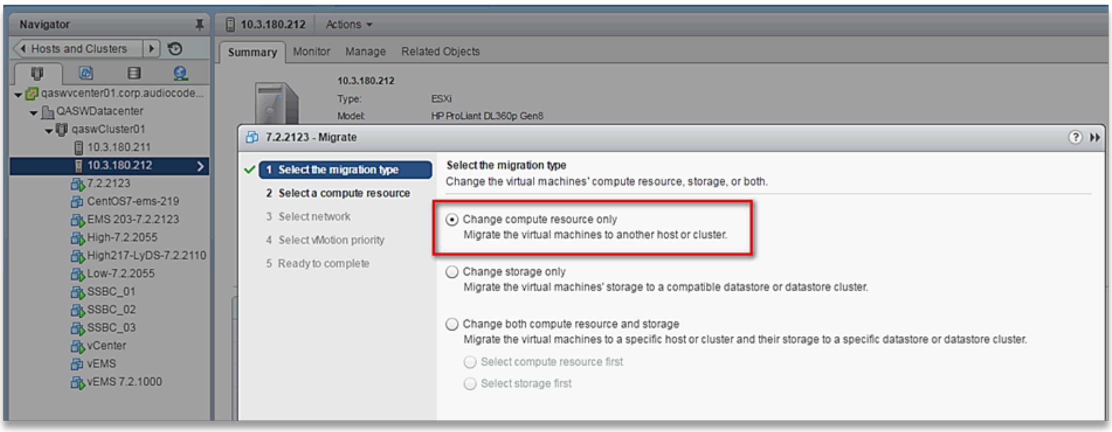
1. Select the OVOC virtual machine that you wish to migrate and then choose the **Migrate** option.

Figure 32-1: Migration



2. Change a cluster host for migration.

Figure 32-2: Change Host



10.3.180.212
Type: ESXi
Model: HP ProLiant DL360p Gen8

7.2.2123 - Migrate

1 Select the migration type
2 Select a compute resource
3 Select network
4 Select vMotion priority
5 Ready to complete

Select the migration type
Change the virtual machines' compute resource, storage, or both.

● Change compute resource only
Migrate the virtual machines to another host or cluster.

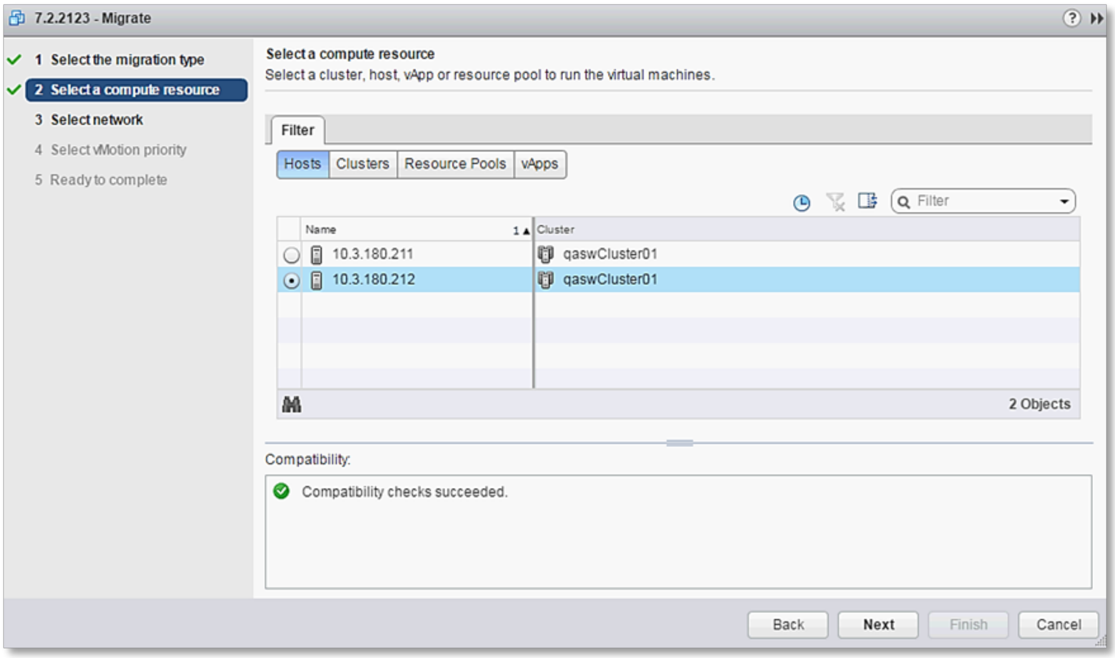
○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Select compute resource first
○ Select storage first

3. Choose the target host for migration.

Figure 32-3: Target Host for Migration



7.2.2123 - Migrate

1. Select the migration type
2. Select a compute resource
3. Select network
4. Select vMotion priority
5. Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

Filter

Hosts | Clusters | Resource Pools | vApps

Filter

	Name	Cluster
○	10.3.180.211	qaswCluster01
●	10.3.180.212	qaswCluster01

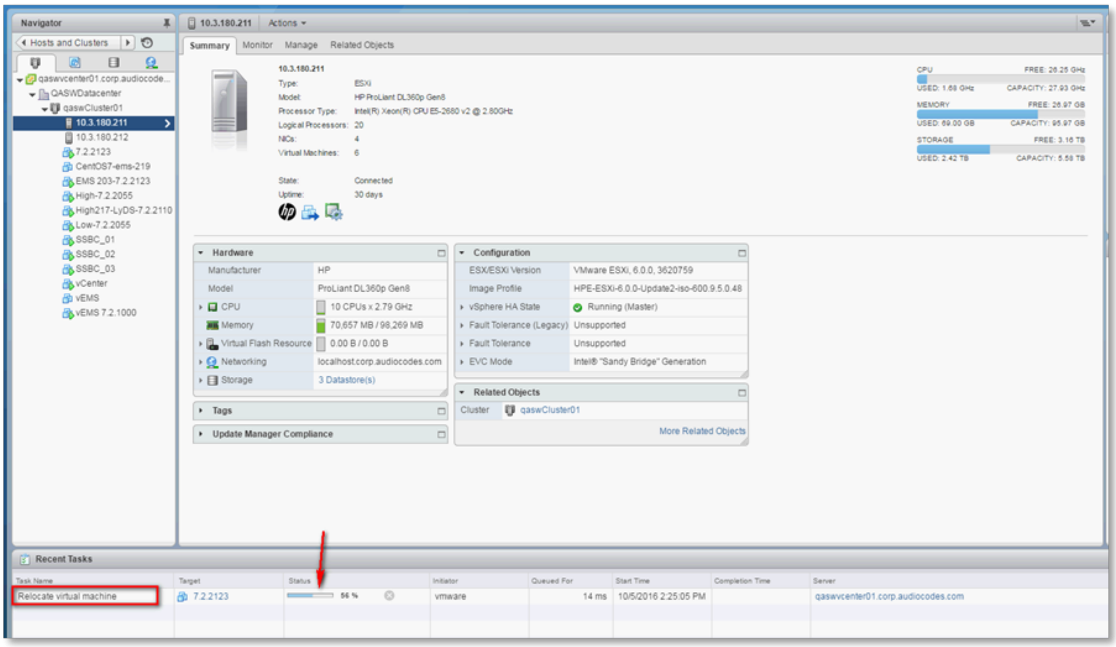
2 Objects

Compatibility:

✓ Compatibility checks succeeded.

The migration process commences.

Figure 32-4: Migration Process Started



10.3.180.211

Type: ESXi
Model: HP ProLiant DL360p Gen8
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 20
NICs: 4
Virtual Machines: 6

State: Connected
Uptime: 30 days

CPU FREE: 26.25 GHz
USED: 1.68 GHz CAPACITY: 27.93 GHz
MEMORY FREE: 26.97 GB
USED: 69.00 GB CAPACITY: 95.97 GB
STORAGE FREE: 3.16 TB
USED: 2.42 TB CAPACITY: 5.58 TB

Hardware	
Manufacturer	HP
Model	ProLiant DL360p Gen8
CPU	10 CPUs x 2.79 GHz
Memory	70,657 MB / 98,269 MB
Virtual Flash Resource	0.00 B / 0.00 B
Networking	localhost.corp.audiocodes.com
Storage	3 Datastore(s)

Configuration	
ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759
Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.0.48
vSphere HA State	✓ Running (Master)
Fault Tolerance (Legacy)	Unsupported
Fault Tolerance	Unsupported
EVC Mode	Intel® "Sandy Bridge" Generation

Related Objects

Cluster: qaswCluster01

More Related Objects

Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Relocate virtual machine	7.2.2123	56 %	vmware	14 ms	10/5/2016 2:25:05 PM		qaswvcenter01.corp.audiocodes.com

After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's host.

Moving OVOC VMs in a Hyper-V Cluster

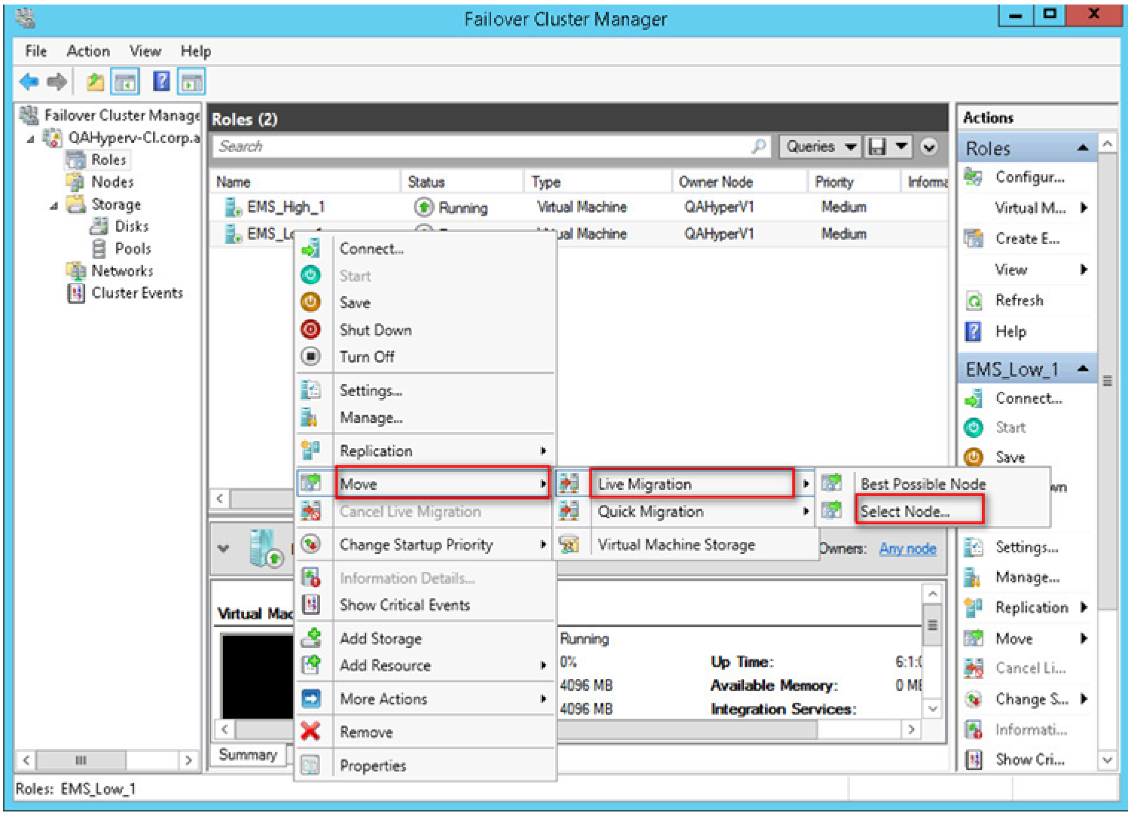
Moving OVOC VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

➢ To move a Virtual Machine to another node of the cluster:

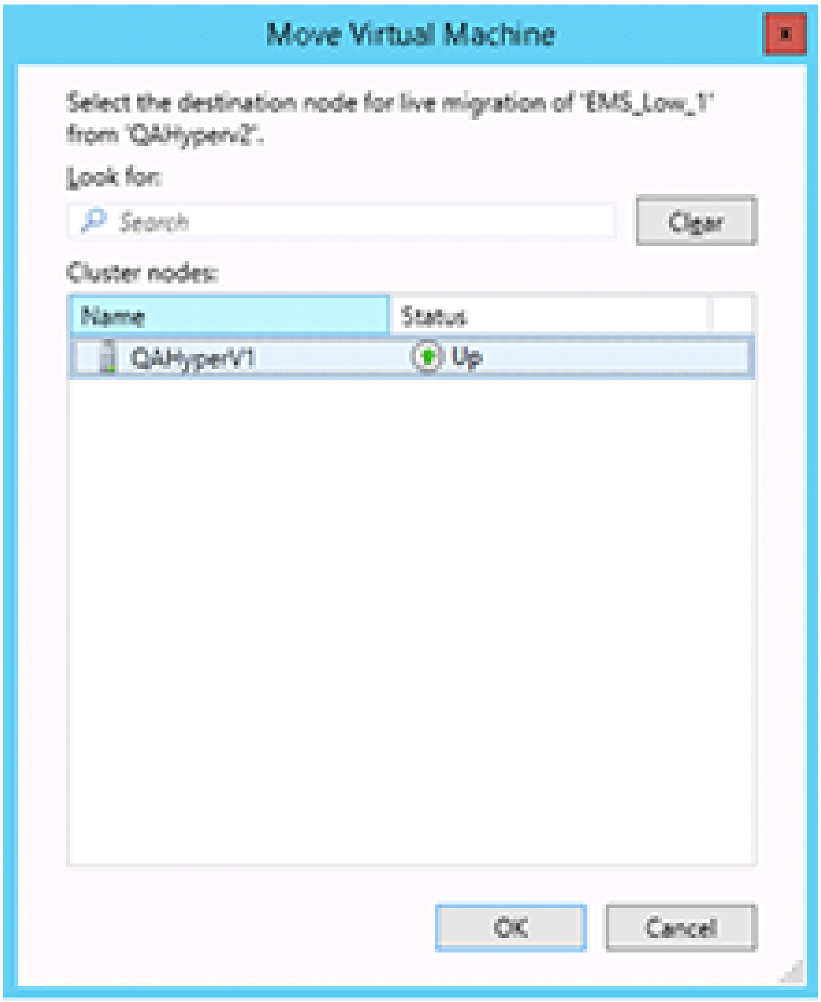
1. Select the Virtual Machine, right-click and from the menu, choose **Move** > **Live Migration > Select Node**.

Figure 32-5: Hyper-V Live Migration



The following screen is displayed:

Figure 32-6: Move Virtual Machine



Move Virtual Machine

Select the destination node for live migration of 'EMS_Low_1' from 'QAHyperv2'.

Look for:

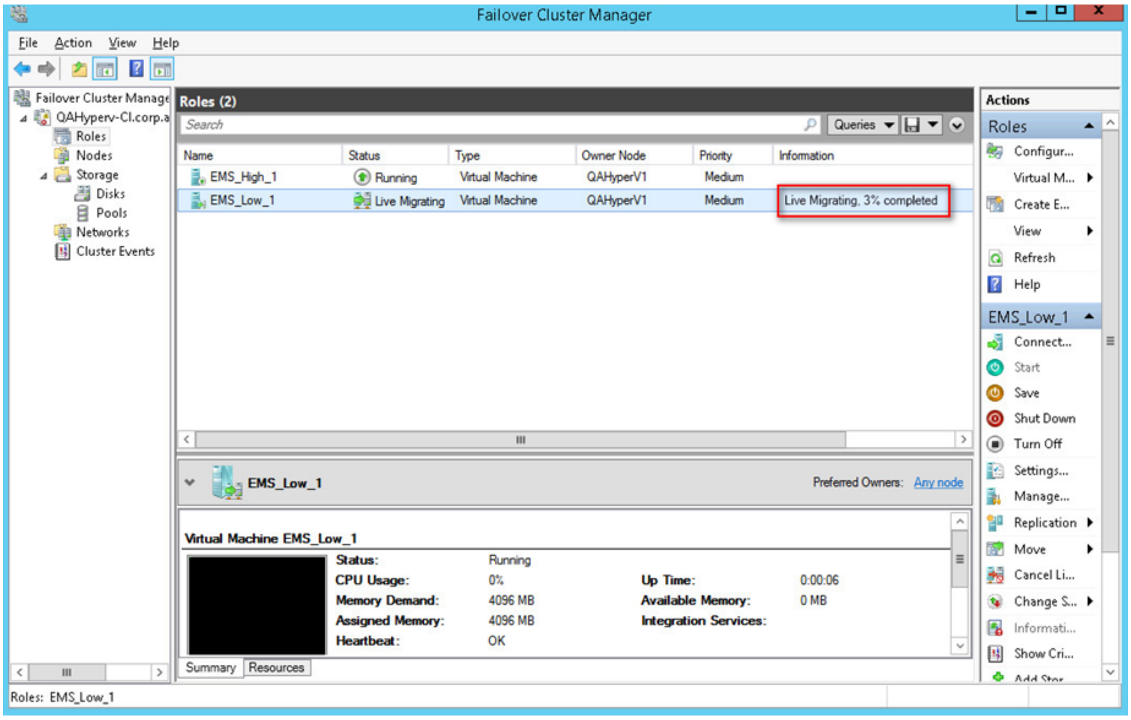
Cluster nodes:

Name	Status
QAHyperV1	Up

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

   The migration process starts.

Figure 32-7: Hyper-V Migration Process Started



Roles (2)

Name	Status	Type	Owner Node	Priority	Information
EMS_High_1	Running	Virtual Machine	QAHyperV1	Medium	
EMS_Low_1	Live Migrating	Virtual Machine	QAHyperV1	Medium	Live Migrating, 3% completed

EMS_Low_1

Virtual Machine EMS_Low_1

Status:	Running		
CPU Usage:	0%	Up Time:	0:00:06
Memory Demand:	4096 MB	Available Memory:	0 MB
Assigned Memory:	4096 MB	Integration Services:	
Heartbeat:	OK		

After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's node.

33 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 325)

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 320).

> ⚠
> - 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.**

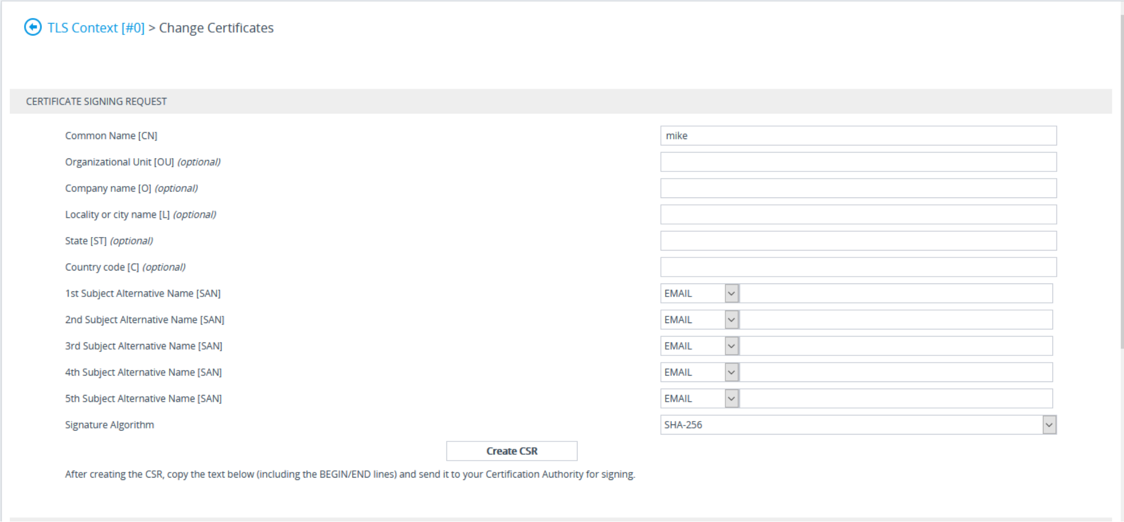
Step 1: Generate a Certificate Signing Request (CSR)

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 33-1: Context Certificates



TLS Context [#0] > Change Certificates

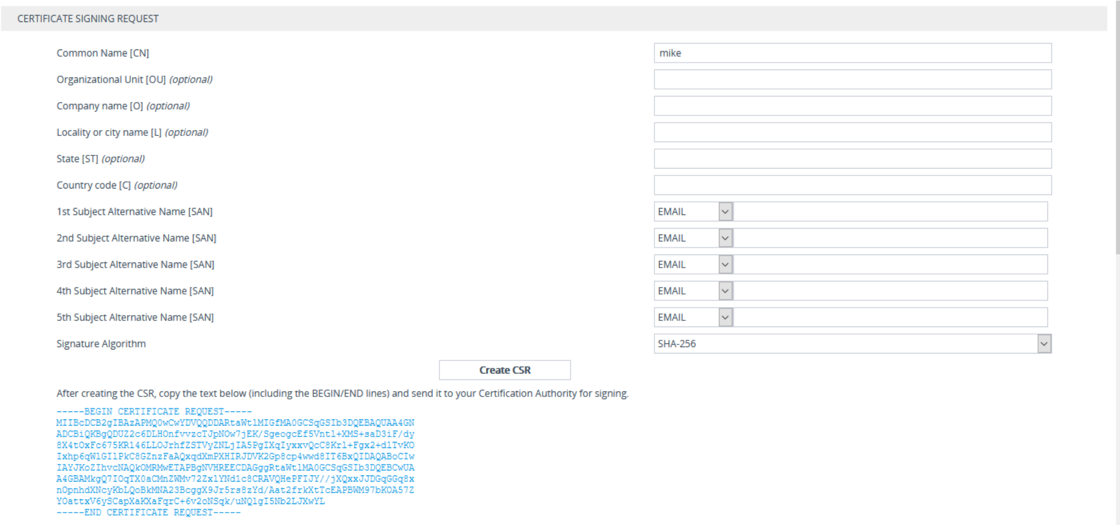
CERTIFICATE SIGNING REQUEST

Common Name [CN]	mike
Organizational Unit [OU] *(optional)*	
Company name [O] *(optional)*	
Locality or city name [L] *(optional)*	
State [ST] *(optional)*	
Country code [C] *(optional)*	
1st Subject Alternative Name [SAN]	EMAIL
2nd Subject Alternative Name [SAN]	EMAIL
3rd Subject Alternative Name [SAN]	EMAIL
4th Subject Alternative Name [SAN]	EMAIL
5th Subject Alternative Name [SAN]	EMAIL
Signature Algorithm	SHA-256

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

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 33-2: Certificate Signing Request Group



CERTIFICATE SIGNING REQUEST

Common Name [CN]	mike
Organizational Unit [OU] *(optional)*	
Company name [O] *(optional)*	
Locality or city name [L] *(optional)*	
State [ST] *(optional)*	
Country code [C] *(optional)*	
1st Subject Alternative Name [SAN]	EMAIL
2nd Subject Alternative Name [SAN]	EMAIL
3rd Subject Alternative Name [SAN]	EMAIL
4th Subject Alternative Name [SAN]	EMAIL
5th Subject Alternative Name [SAN]	EMAIL
Signature Algorithm	SHA-256

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBcDCB2gIBAzAPMQ0wCwYDVQQDDARtaWtlMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDUZ2c6DLHOnfvvzcTJpNOw7jEK/SgeogcEf5Vntl+XMS+saD3iF/dy
8X4tOxFc675KR146LLOJrhfZSTVyZNLjIA5PgIXqIyxxvQcC8Krl+Fgx2+dlTvKO
Ixhp6qWlGIlPkC8GZnzFaAQxqdXmPXHIRJDVK2Gp8cp4wwd8IT6BxQIDAQABoCIw
IAYJKoZIhvcNAQkOMRMwETAPBgNVHREECDAGggRtaWtlMA0GCSqGSIb3DQEBCwUA
A4GBAMkgQ7IOqTX0aCMnZWMv72ZxlYNd1c8CRAVQHePFIJY//jXQxxJJDGqGGq8x
nOpnhdXNcyKbLQoBkMNA23BcggX9Jr5rs8zYd/Aat2frkXtTcEAPBWM97bKOA57Z
YOattxV6ySCapXaKXaFqrC+6v2oNSqk/uNQlgI5Nb2LJXwYL
-----END CERTIFICATE REQUEST-----
```

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.

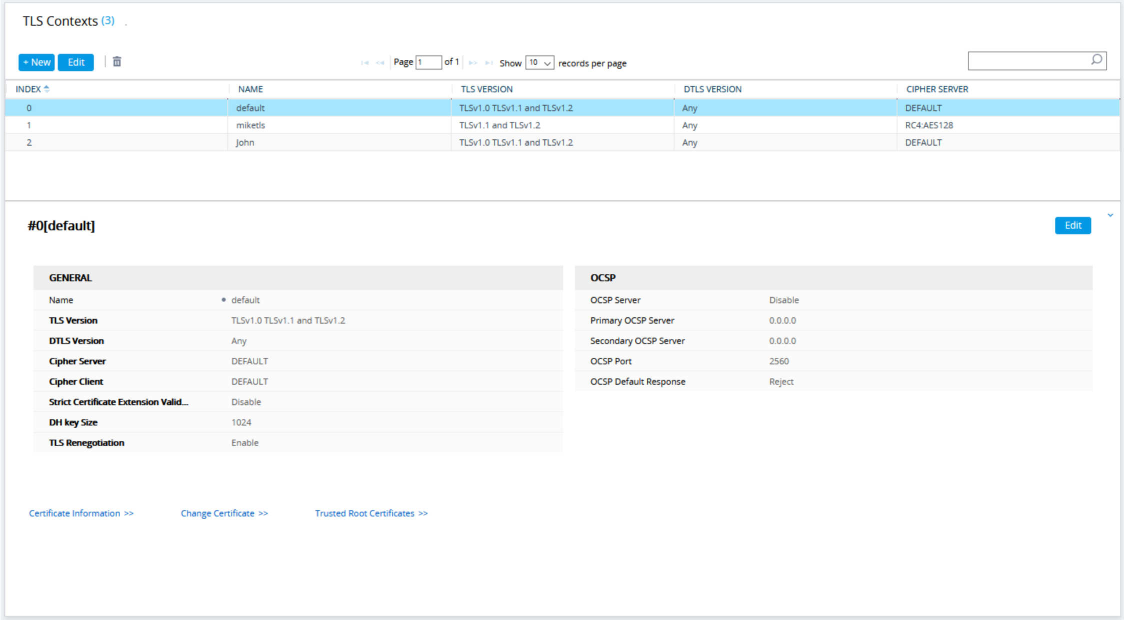
Step 3: Update Device with New Certificate

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 33-3: TLS Contexts Table



TLS Contexts (3)

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT
1	miketls	TLSv1.1 and TLSv1.2	Any	RC4:AES128
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT

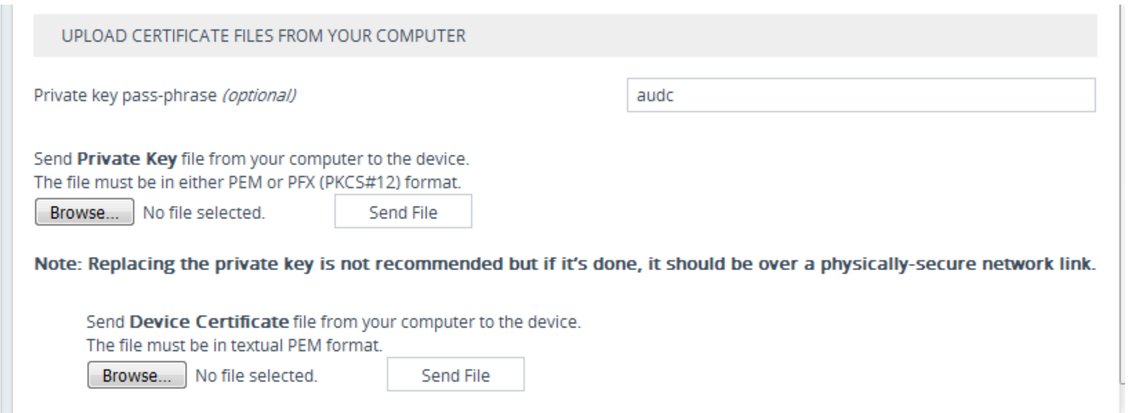
#0[default]

GENERAL	
Name	• default
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version	Any
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Strict Certificate Extension Valid...	Disable
DH key Size	1024
TLS Renegotiation	Enable

OCSP	
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

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 33-4: Upload Certificate Files from your Computer Group



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

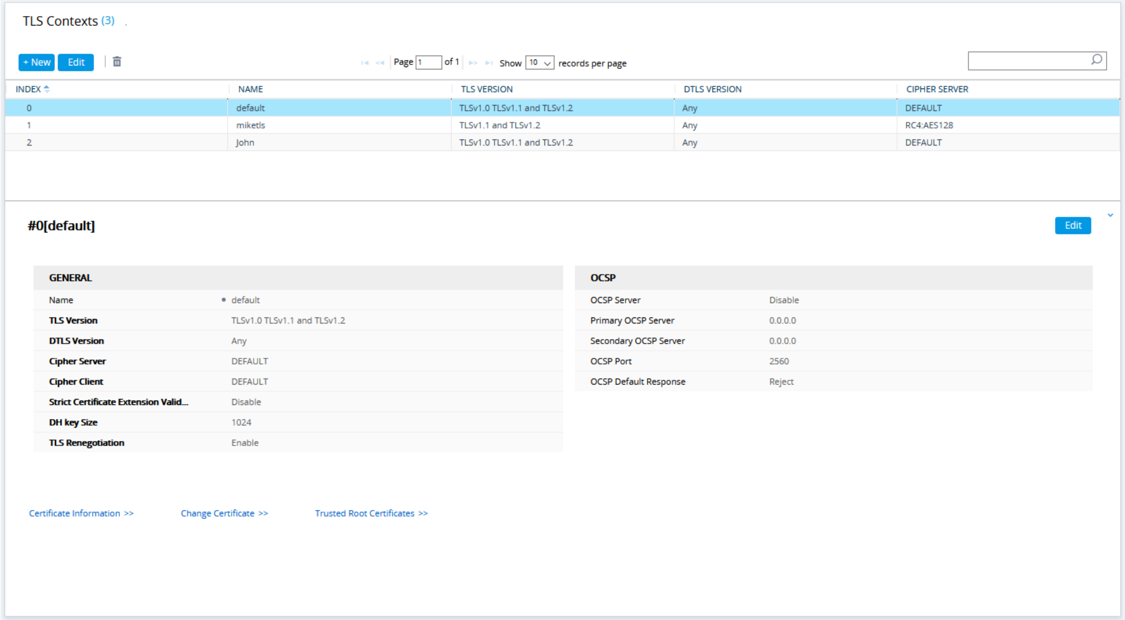
Step 4: Update Device's Trusted Certificate Store

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 33-5: Trusted Root Certificates



TLS Contexts (3)

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT
1	miketls	TLSv1.1 and TLSv1.2	Any	RC4:AES128
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT

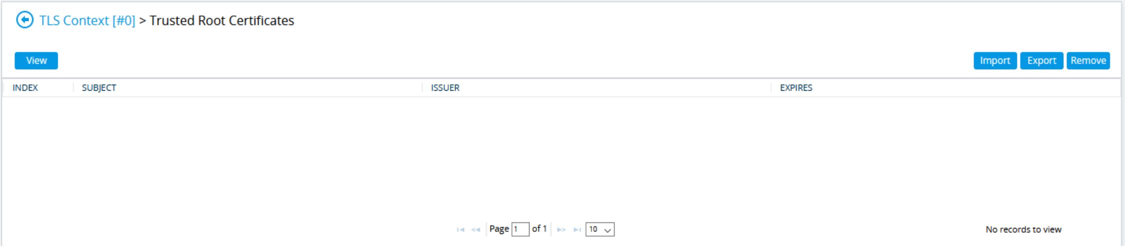
#0[default]

GENERAL	
Name	• default
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version	Any
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Strict Certificate Extension Valid...	Disable
DH key Size	1024
TLS Renegotiation	Enable

OCSP	
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

Figure 33-6: Importing Certificate into Trusted Certificates Store



TLS Context [#0] > Trusted Root Certificates

INDEX	SUBJECT	ISSUER	EXPIRES

No records to view

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

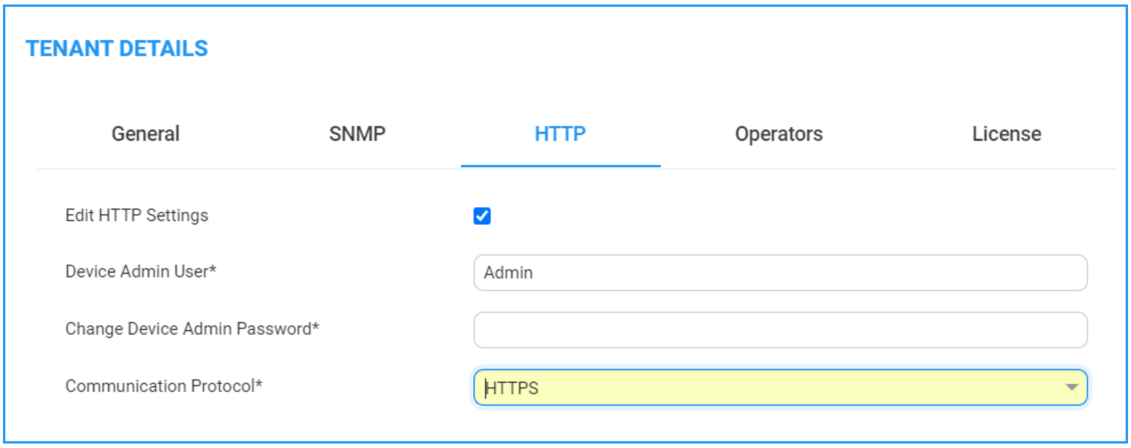
This section describes how to configure HTTPS related parameters on the device.

- 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 33-7: Tenant Details



TENANT DETAILS

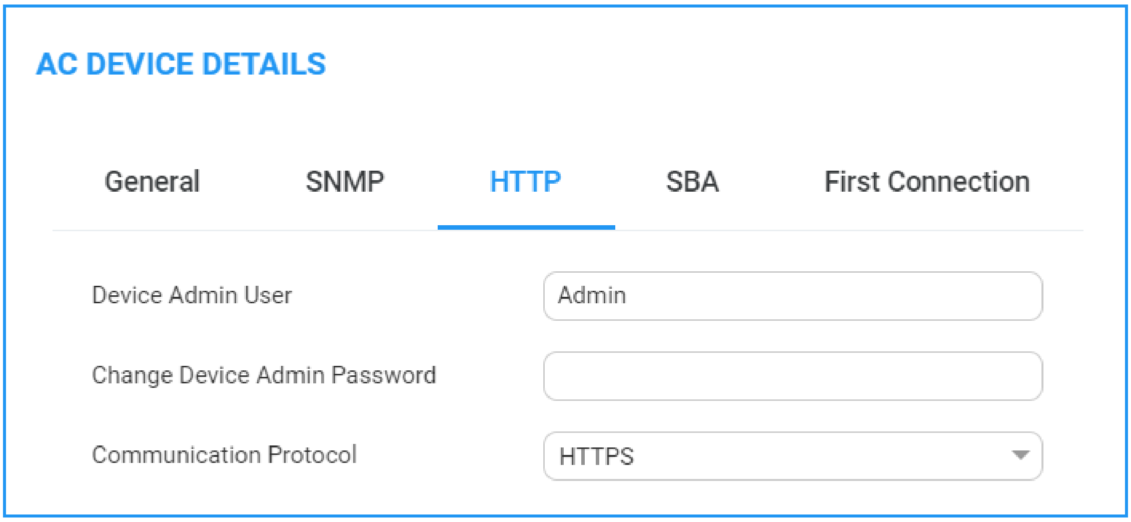
Edit HTTP Settings ☑

Device Admin User* Admin

Change Device Admin Password*

Communication Protocol* HTTPS

Figure 33-8: Device Details (Default HTTPS)



AC DEVICE DETAILS

Device Admin User Admin

Change Device Admin Password

Communication Protocol 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:

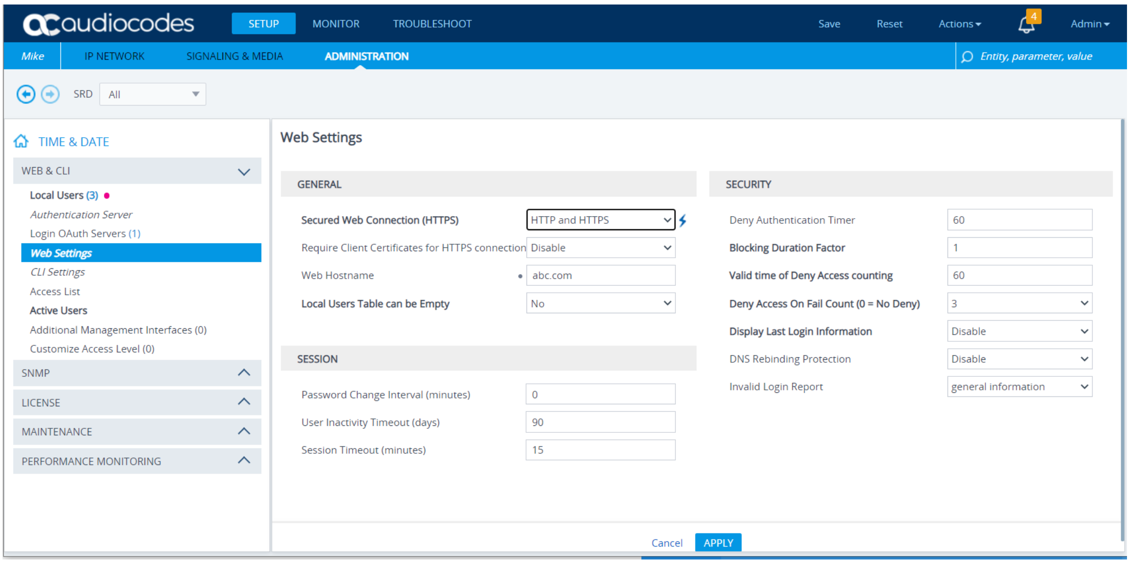
     AUPDVerifyCertificates=1
   - For MP-1xx devices, the ini file should include the following two lines::

     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 33-9: SBC Web Settings Page



Web Settings

GENERAL

Secured Web Connection (HTTPS)	HTTP and HTTPS
Require Client Certificates for HTTPS connection	Disable
Web Hostname	abc.com
Local Users Table can be Empty	No

SESSION

Password Change Interval (minutes)	0
User Inactivity Timeout (days)	90
Session Timeout (minutes)	15

SECURITY

Deny Authentication Timer	60
Blocking Duration Factor	1
Valid time of Deny Access counting	60
Deny Access On Fail Count (0 = No Deny)	3
Display Last Login Information	Disable
DNS Rebinding Protection	Disable
Invalid Login Report	general information

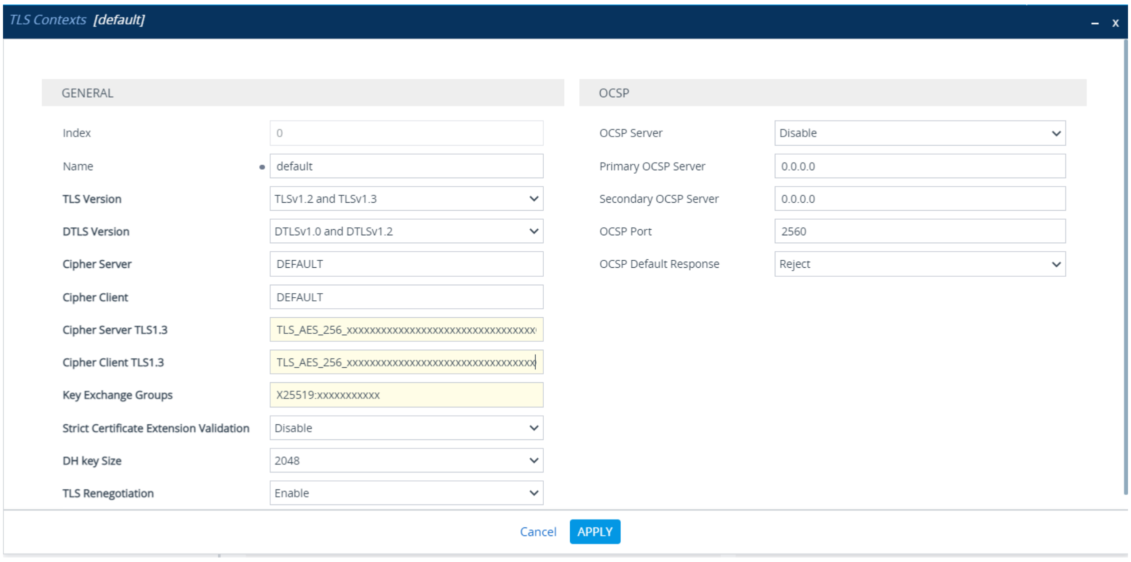
7. If you configured the SBC Devices Communication parameter to **Hostname-Based** in the OVOC Web, you must configure the parameter "Verify Certificate SubjectName" on the managed device (**Setup** Menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience Settings**).

Figure 33-10: 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 33-11: TLS Contexts



GENERAL

Index	0
Name	default
TLS Version	TLSv1.2 and TLSv1.3
DTLS Version	DTLSv1.0 and DTLSv1.2
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Cipher Server TLS1.3	TLS_AES_256_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Cipher Client TLS1.3	TLS_AES_256_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Key Exchange Groups	X25519:xxxxxxxxxxx
Strict Certificate Extension Validation	Disable
DH key Size	2048
TLS Renegotiation	Enable

OCSP

OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

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*.

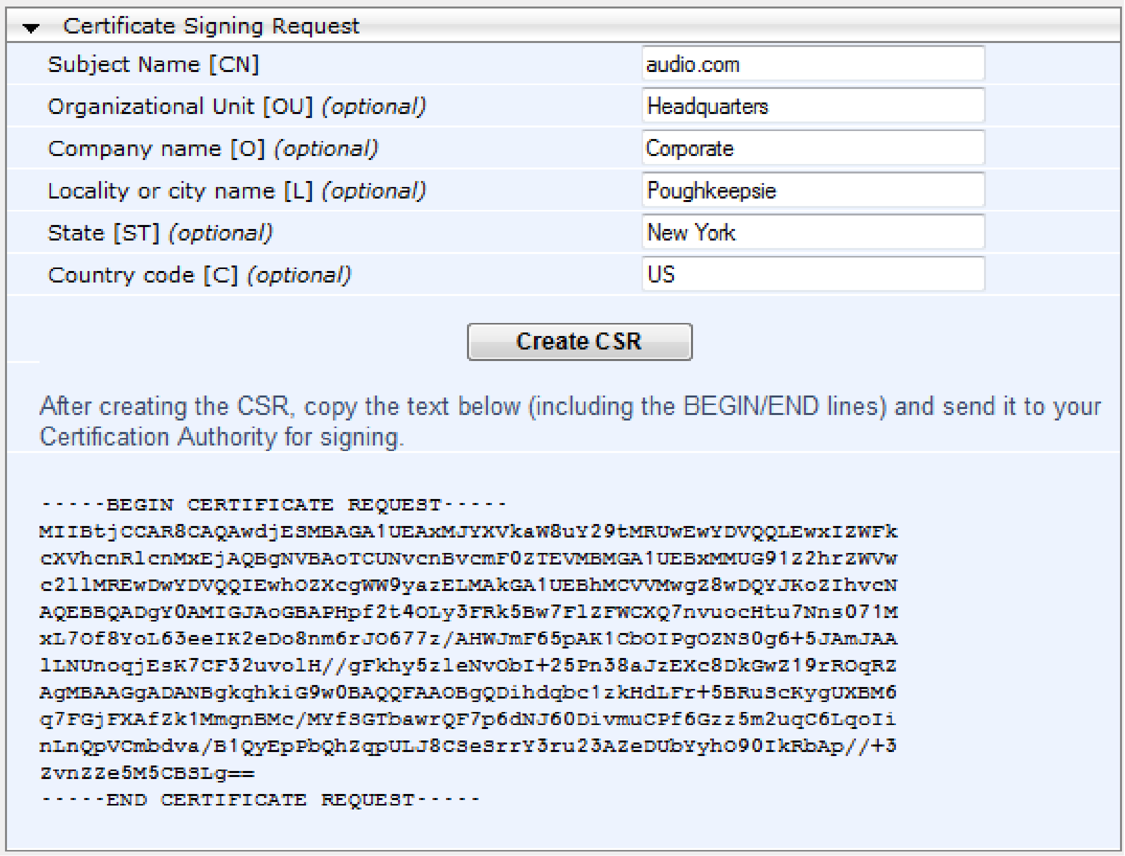
Step 1: Generate a Certificate Signing Request (CSR)

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 33-12: Certificate Signing Request Group



▼ Certificate Signing Request

Subject Name [CN]	audio.com
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwdjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLEwxIZWFk
cXVhcnRlcnMxEjAQBgNVBAoTCUNvcnBvcmF0ZTEVMBMGA1UEBxMMUG91z2hrZWVw
c2llMREwDwYDVQQIEwhOZXcgWW9yazELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPHpf2t4OLy3FRk5Bw7FlZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CbOIPgOZN30g6+5JAmJAA
lLNUnoqjEsK7CF32uvolH//gFkhy5zleNvObI+25Pn38aJzEXc8DkGwZ19rROqRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbc1zkHdLFr+5BRu3cKygUXBM6
q7FGjFXAfZk1MmgnBMc/MYf3GTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LqoIi
nLnQpVCmbdva/B1QyEpPbQhZqpULJ8C3e3rrY3ru23AZeDUbYyhO90IkRbAp//+3
ZvnZZe5M5CB3Lg==
-----END CERTIFICATE REQUEST-----
```

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
```

```
7uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3IRefiXDmuOe+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 325 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 317 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
```

34 Transferring Files

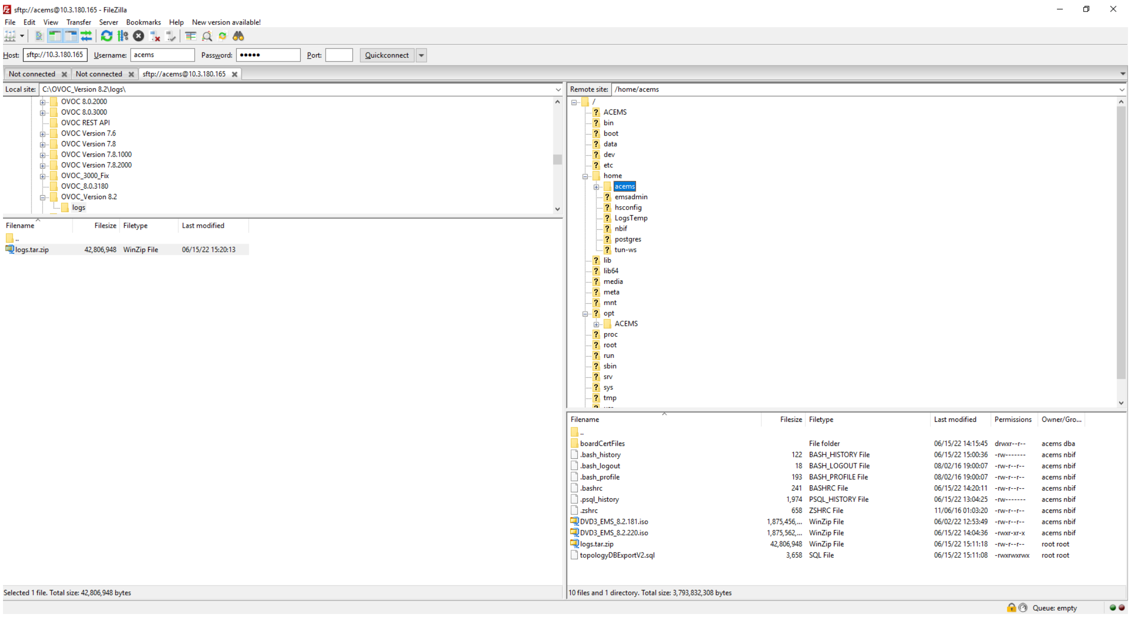
This appendix describes how to transfer files to and from the OVOC server using any SFTP/SCP file transfer application.

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 34-1: FileZilla



sftp://acems@10.3.180.165 - FileZilla

Host: sftp://10.3.180.165 Username: acems Password: ●●●●● Port:

Local site: C:\OVOC_Version 8.2\logs\

- OVOC 8.0.2000
- OVOC 8.0.3000
- OVOC REST API
- OVOC Version 7.6
- OVOC Version 7.8
- OVOC Version 7.8.1000
- OVOC Version 7.8.2000
- OVOC_3000_Fix
- OVOC_8.0.3180
- OVOC_Version 8.2
  - logs

Filename	Filesize	Filetype	Last modified
..			
logs.tar.zip	42,806,948	WinZip File	06/15/22 15:20:13

Selected 1 file. Total size: 42,806,948 bytes

Remote site: /home/acems

- /
  - ACEMS
  - bin
  - boot
  - data
  - dev
  - etc
  - home
    - acems
    - emsadmin
    - hsconfig
    - LogsTemp
    - nbif
    - postgres
    - tun-ws
  - lib
  - lib64
  - media
  - meta
  - mnt
  - opt
    - ACEMS
  - proc
  - root
  - run
  - sbin
  - srv
  - sys
  - tmp

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
boardCertFiles		File folder	06/15/22 14:15:45	drwxr--r--	acems dba
.bash_history	122	BASH_HISTORY File	06/15/22 15:00:36	-rw-------	acems nbif
.bash_logout	18	BASH_LOGOUT File	08/02/16 19:00:07	-rw-r--r--	acems nbif
.bash_profile	193	BASH_PROFILE File	08/02/16 19:00:07	-rw-r--r--	acems nbif
.bashrc	241	BASHRC File	06/15/22 14:20:11	-rw-r--r--	acems nbif
.psql_history	1,974	PSQL_HISTORY File	06/15/22 13:04:25	-rw-------	acems nbif
.zshrc	658	ZSHRC File	11/06/16 01:03:20	-rw-r--r--	acems nbif
DVD3_EMS_8.2.181.iso	1,875,456,...	WinZip File	06/02/22 12:53:49	-rw-r--r--	acems nbif
DVD3_EMS_8.2.220.iso	1,875,562,...	WinZip File	06/15/22 14:04:36	-rwxr-xr-x	acems nbif
logs.tar.zip	42,806,948	WinZip File	06/15/22 15:11:18	-rw-r--r--	root root
topologyDBExportV2.sql	3,658	SQL File	06/15/22 15:11:08	-rwxrwxrwx	root root

10 files and 1 directory. Total size: 3,793,832,308 bytes

Queue: empty

35 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
```

36 Self-Signed Certificates

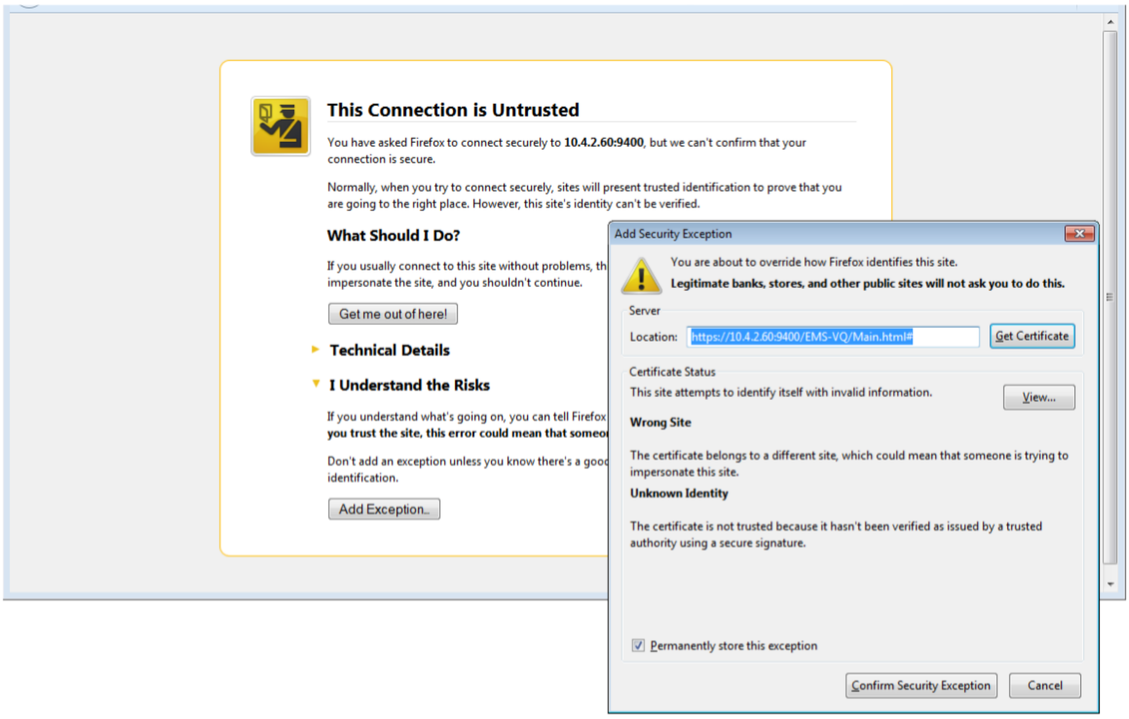
When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

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 36-1: Mozilla Firefox Settings



This Connection is Untrusted

You have asked Firefox to connect securely to **10.4.2.60:9400**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, th
impersonate the site, and you shouldn't continue.

I Understand the Risks

If you understand what's going on, you can tell Firefox
you trust the site, this error could mean that someo

Don't add an exception unless you know there's a good
identification.

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.4.2.60:9400/EMS-VQ/Main.html#

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

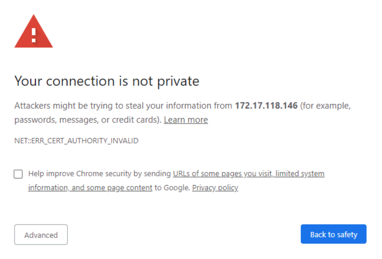
☑ Permanently store this exception

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 36-2: Chrome Browser Settings



Your connection is not private

Attackers might be trying to steal your information from **172.17.118.146** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

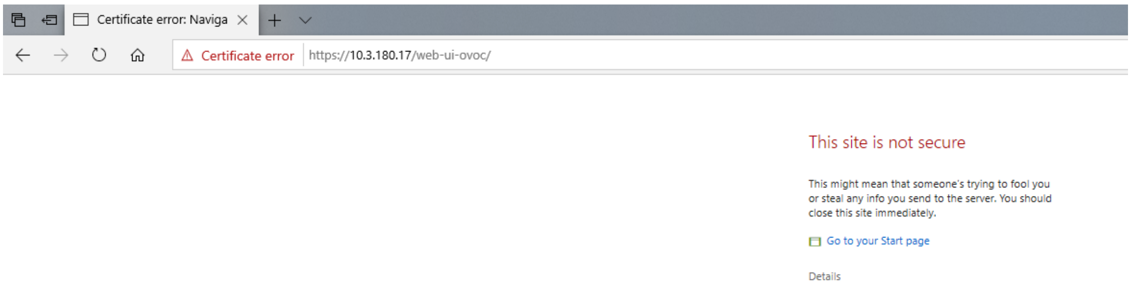
□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

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 36-3: Microsoft Edge Browser



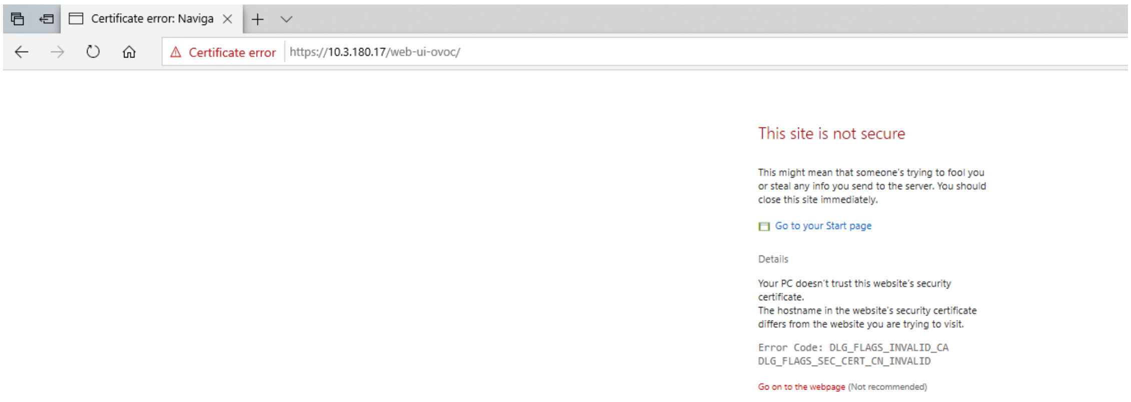
This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Figure 36-4: Go on to the Web Page



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

```
Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID
```

Go on to the webpage (Not recommended)

37 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.

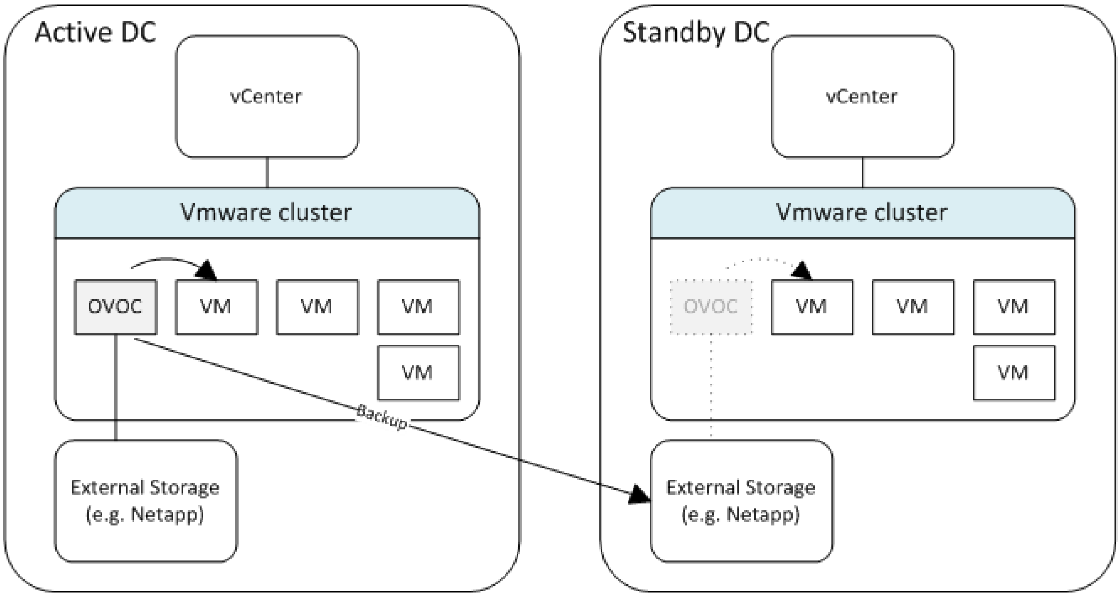
Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

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 37-1: 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 189.

- 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 191).
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 37-1: 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

Naimi Park

6 Ofra Haza Street

Or Yehuda, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-94196