AudioCodes One Voice[™] Operations Center

One Voice Operations Center Migration

Migrating from EMS/SEM Version 7.2 to One Voice Operations Center

Version 7.4



Table of Contents

1	Summary13							
2	Recommended Work Flow							
	2.1	Single	Machine Topology	15				
	2.2	Dual M	lachine Topology	17				
3	Backup Data from EMS/SEM 7.2.3000							
	3.1	Backu	p Procedure	21				
	3.2	Save D	Data in Textual Format	21				
4	Сар	Capture Version 7.2 EMS & SEM Configuration						
5	Ехр	ort Top	oology and IP Phone Configuration	25				
	5.1	Export	EMS Topology	25				
		5.1.1	Example Output	26				
	5.2	Export	IP Phone Management Server Configuration	28				
6	Che	ck and	Prepare Server Machine for Version 7.4 Installation	31				
7	Inst	all the	One Voice Operations Center	33				
	7.1	OVOC	Software Deliverables	33				
		7.1.1	Dedicated Hardware Media	33				
		7.1.2	Virtual Machine Media (VMware and Hyper-V)	33				
	7.2	Pre-ins	Stallation	34				
		7.2.1	Files Verification Requirements -Dedicated Hardware	34 35				
		7.2.3	OVOC Server Users					
	7.3 Installing the OVOC Server on Dedicated Hardware			36				
		7.3.1	DVD1-CentOS 7.3 Rev 18	36				
		7.3.2	DVD2: Oracle DB Installation					
	7 /	7.3.3 Inetalli	ng the OVOC on Virtual Server Platform	41 44				
	1.4	7 4 1	Installing the OVOC Server on the VMware Platform					
		7.4.2	Installing the OVOC Server on Microsoft Hyper-V Platform	57				
8	Con	figure	One Voice Operations Center Server	73				
		8.1.1	Connecting to the EMS Server Manager	73				
		8.1.2	General Information	74				
		8.1.3	Web Server Configuration	75				
		8.1. 4	Network Configuration					
		8.1.6	Date and Time Menu	80				
		8.1.7	Security	80				
		8.1.8 8.1.9	Enable IP Phone Management Server Client	83 83				
a	Imn	ort the	Topology and Configuration	85				
•	0 1	Import	EMS Tanalagy	05				
	ฮ. เ	9 1 1	Example Output	CO				
	92	Import	IP Phone Management Server Configuration and Users & Devices					
	5.2	import	In Those Management berver bonnguration and bacis & bevices	07				

10	Mov	e Phones from Version 7.2 Platform	91				
11	1 Configure One Voice Operations Center Web Client						
	11.1	Local User Authentication	95				
	11.2	External Authentication Servers	97				
		11.2.1 RADIUS	97 99				
	11.3	Alarms (from EMS Application)	100				
		11.3.1 Alarms Settings11.3.2 Alarms Forwarding Rules	.100 .101				
	11.4	Software Manager	104				
	11.5	Device Backup Configuration	104				
	11.6	LDAP User Authentication	105				
	11.7	SEM Client Configuration	107				
		11.7.1 Microsoft Active Directory	.107				
		11.7.2 Skype for Business SQL Server Configuration	.108				
		11.7.5 QUE Thresholds Configuration	110				
		11.7.5 Scheduled Reports Configuration (from SEM Application)	.111				
A	Арре	endix A –Backup and Restore	113				
	A.1	OVOC Server Backup	.113				
		A.1.1 Change Schedule Backup Time	.113				
	A.2	OVOC Server Restore	.114				
В	Appendix B – EMS / SEM 7.2 – Topology Import Process Limitations115						
С	Tran	sferring Files	117				

List of Figures

Figure 2.1: Migration with a Single Machine	16
Figure 2-1: Migration with a Ongle Machine	10
Figure 2-2. Migration with Dual Machines	.10
Figure 2-2: Alarm History Drompt	.22
Figure 5-2. Aldrift Filology Frompt	.22
Figure 5-1. Copy Certificate Files	.20
Figure 5-2: Export 1 opology	.29
Figure 7-1: Linux Testing Requirements	.34
Figure 7-2: File Integrity Verification	.35
Figure 7-3: Linux CentOS Installation	.37
Figure 7-4: CentOS 7	.37
Figure 7-5: CentOS Installation	.38
Figure 7-6: Linux CentOS Installation Complete	.38
Figure 7-7: Linux CentOS Network Configuration	.39
Figure 7-8: Oracle DB Installation (Linux)	.40
Figure 7-9: Oracle DB Installation - License Agreement (Linux)	.40
Figure 7-10: Oracle DB Installation (Linux) (cont)	.40
Figure 7-11: Oracle DB Installation (Linux) (cont)	41
Figure 7-12: OV/OC Server Application Installation (Linux)	41
Figure 7-12: OVOC Server Application Installation (Linux) -1 icense Agreement	 12
Figure 7-13: OVOC Server Application Installation (Linux) – Electise Agreement	. <u>ד</u> 2 12
Figure 7-14: OVOC Server Application Installation (Linux) (cont)	.72
Figure 7-15. OVOC Server Application Installation (Linux) - Java Installation	.40
Figure 7-16: Installation Complete	.43
	.45
Figure 7-18: Hosts and Clusters	.45
Figure 7-19: Deploy OVF Template Option	.46
Figure 7-20: Client Integration Plug-in	.46
Figure 7-21: Browse to OVF Package	.47
Figure 7-22: OVF Template Details Screen	.48
Figure 7-23: Virtual Machine Name and Location Screen	.48
Figure 7-24: Destination Storage Screen	.49
Figure 7-25:: Setup Networking Screen	.49
Figure 7-26: Ready to Complete Screen	.50
Figure 7-27: Deployment Progress Screen	.50
Figure 7-28: Edit Settings option	.51
Figure 7-29: CPU, Memory and Hard Disk Settings	.52
Figure 7-30: Recent Tasks	52
Figure 7-31: Power On	53
Figure 7-32: Storage Adapters	54
Figure 7 33:Turn On vSphere HA	54
Figure 7-33.1 uni On Vopinere FIA	.54
Figure 7-54. Activate FIA official Cluster Node	.00
Figure 7-35. Networking	.55
Figure 7-36: Switch Properties	.50
Figure 7-37: Protected VM	.56
Figure 7-38: Installing the OVOC server on Hyper-V – Hyper-V Manager	.58
Figure 7-39: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard	.58
Figure 7-402: Installing OVOC server on Hyper-V – Locate Folder	.59
Figure 7-413: Installing OVOC server on Hyper-V – Choose Import Type	.59
Figure 7-424: Installing OVOC server on Hyper-V – Choose Destination	.60
Figure 7-435: Installing OVOC server on Hyper-V – Choose Storage Folders	.60
Figure 7-446: File Copy Progress Bar	.61
Figure 7-45: Adjusting VM for OVOC server – Settings - Memory	.62
Figure 7-46: Adjusting VM for OVOC Server - Settings - Processor	.63
Figure 7-47: Expanding Disk Capacity	.64
Figure 7-48: Edit Virtual Hard Disk Wizard.	.65
Figure 7-49: Edit Virtual Hard Disk Wizard-Choose Action	65
Figure 7-50: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk	66
- igare - eet Eart virtuur hard Bloc virtuu Expand virtuur hard Blocking	

Figure 7-51: Edit Virtual Hard Disk Wizard-Completion	.66
Figure 7-52: Advanced Features - Network Adapter – Static MAC Address	.67
Figure 7-53: Power On Virtual Machine	.68
Figure 7-54: Connect to OVOC Server Console	.68
Figure 7-55: Hyper-V-Failover Cluster Manager Nodes	.69
Figure 7-56: Configure Role	.70
Figure 7-57: Choose Virtual Machine	.70
Figure 7-58: Confirm Virtual Machine	.71
Figure 7-59: Virtual Machine Successfully Added	.72
Figure 8-1: General Information	.74
Figure 8-2: Web Server Processes Status	.75
Figure 8-3: Schedule Backup Time Configuration	.75
Figure 8-4: Network Configuration	.76
Figure 8-5: Ethernet Interfaces	.76
Figure 8-6: Ethernet Redundancy	.77
Figure 8-7: DNS Configuration	.77
Figure 8-8: NAT Configuration	.77
Figure 8-9: Static Route Configuration	.78
Figure 8-10: Configure SNMP Agent	.78
Figure 8-11: NMS IP and Community String	.78
Figure 8-12: SNMP Agent	.79
Figure 8-13: Configure SNMP Agent	.79
Figure 8-14: SNMPv3 Engine ID	.79
Figure 8-15: Date and Time	.80
Figure 8-16: Security	.80
Figure 8-17: SSH	.81
Figure 8-18: One Voice Operations Center Server Manager – Change DB Password	.81
Figure 8-19: Network Options	.82
Figure 8-20: HTTPS Authentication	.82
Figure 8-21: SEM-AudioCodes Device Communication	.83
Figure 8-22: Diagnostics	.83
Figure 9-1: Import Phone Configuration Files	.88
Figure 9-2: Import Users and Devices	.88
Figure 10-1: Navigation Tree - Templates	.91
Figure 11-1: Users List	.95
Figure 11-2: User Details	.96
Figure 11-3: Tenant Operators	.96
Figure 11-4: Tenant Operator Settings	.97
Figure 11-5: RADIUS Configuration	.97
Figure 11-6: RADIUS Settings	.98
Figure 11-7: LDAP Configuration	.99
Figure 11-8: LDAP Settings	.99
Figure 11-9: Alarm Settings	100
Figure 11-10: Version 7.4 Alarms Settings1	100
Figure 11-11: Version 7.2: Alarm Forwarding Rules1	101
Figure 11-12: Version 7.2: Destination Rules Configuration1	101
Figure 11-13: Version 7.4: Alarm Forwarding Rules1	102
Figure 11-14: Rule Name1	102
Figure 11-15: Alarm Forwarding Rule Conditions1	102
Figure 11-16: Alarm Forwarding Destinations1	103
Figure 11-17:Version 7.2: Backup Configuration1	104
Figure 11-18: Version 7.4: Backup Configuration1	105
Figure 11-19: LDAP Authentication and Authorization1	105
Figure 11-20: Authentication Page1	106
Figure 11-21: Version 7.2: Active Directory Configuration1	107
Figure 11-22: Version 7.4 Active Directory Configuration1	108
Figure 11-23: SEM - Network tab Skype for Business Device Definition1	108
Figure 11-24: OVOC - Skype for Business Device Definition1	109
Figure 11-25: Version 7.2: QoE Thresholds Configuration1	109

Figure 11-26: Version 7.4: QoE Thresholds Configuration	110
Figure 11-27: Version 7.2: Alarm Rules Configuration	110
Figure 11-28: Version 7.4: Alarm Rules Configuration	111
Figure 11-29: Version 7.2: SEM Scheduled Reports	111
Figure 11-30: Version 7.4: Statistics Reports	111

List of Tables

Table 7-1: VMware Virtual Machine Settings	51
Table 7-2: Microsoft Hyper-V Virtual Machine Settings	61



This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: October-29-2018

WEEE EU Directive

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

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 Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Manual Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500 E-SBC User's Manual
Mediant 500L E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
One Voice Operations Center Server Installation, Operation and Maintenance Manual
One Voice Operations Center Integration with Northbound Interfaces
One Voice Operations Center User's Manual
IP Phone Manager Pro Administrator's Manual
IP Phone Manager Express Administrator's Manual
One Voice Operations Center Product Description
One Voice Operations Center Alarms Guide
One Voice Operations Center Security Guidelines
ARM User's Manual

Document Revision Record

LTRT	Description					
91052	Initial document release for Version 7.4					
91053	Update for correcting link to the AudioCodes Services portal for downloading the IP Phone Manager Pro Export Configuration script.					
91054	Update regarding the migration of the SSL.conf file.					
91055	Update to note in Section "Summary"; Update to note in Section "Topology and Configuration import".					

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 Web site at <u>https://online.audiocodes.com/documentation-feedback</u>.



This page is intentionally left blank.

1 Summary

This document is designed for customers with EMS/SEM Version 7.2.3000 who wish to upgrade to the new One Voice Operations Center 7.4 Version.

Warning:

- Verify that all devices that you wish to migrate are loaded with firmware versions that are supported by the OVOC platform (refer to the OVOC IOM for details).
- If your Version 7.2.3000 platform was configured for HA, do not proceed with this migration.
- For a full listing of open issues for Version 7.4, refer to the One Voice Operations Center Release Notes.
- Performance Monitoring Historical Data is not migrated because Version 7.4 does not currently support Performance Monitoring.

If you are new customer and the first management solution to use is One Voice Operations Center Version7.4, refer to the One Voice Operations Center IOM & One Voice Operations Center User Manual Guides.

When upgrading to One Voice Operations Center 7.4 Version, the following data can be preserved using a provided topology script:

- Topology
- License Pool allocations

The document below describes the manual procedure that should be taken to preserve other system settings. Note the following:

- Endpoints reporting QoE data using SIP Publish (RFC 6035) are not migrated as part of the topology.
- Data collected by the system, namely: alarms, SEM calls, statistics, reports, performance monitoring data CANNOT be automatically transferred from Version 7.2 to Version 7.4. This data will be lost and therefore users should keep the latest backup file to retrieve it. In addition, specific data can be saved & stored in human readable format, which does not require an EMS/SEM installation to view.
- Properties files changes: in case, customers make changes using the properties files, they should contact AudioCodes support for assistance.
- Bare Metal HA is not supported in One Voice Operations Center Version 7.4.
- If your network is composed of devices that are located behind a NAT, note that the IP & port saved in the topology file might be changed after the device is connected to the network.

For more information, see the following:

- Appendix A –Backup and Restore
- Appendix B EMS / SEM 7.2 Topology Import Process Limitations



This page is intentionally left blank.

2 Recommended Work Flow

- Migration Hardware Topology: You can run the migration process using either the existing machine or run it on a new machine, regardless of whether you are running on dedicated hardware or on a virtual machine:
 - For Single machine topology: you are required to remove all devices from the network (not including phones). In the event of failover, you need to restore the existing machine to the Version 7.2 installation.
 - For Dual machine topology: you need to disconnect the Version 7.2 machine from the network. In the event of failover, you need to disconnect the Version 7.4 platform from the network and then reconnect the Version 7.2 machine.



Warning: If you are deploying two machine topology, under no circumstances should the Version 7.2.3000 and Version 7.4 platforms be simultaneously connected to the network.

Migration Stages: It is recommended to perform the migration process in two stages, in the first stage to migrate only a few devices and phones and to check their basic operations (without importing topology). For example, if a License Pool is used, ensure the device is managed in the new One Voice Operations Center application. Also you should create all the relevant links. In the second stage, you should import the topology (including all devices and phones and users).

2.1 Single Machine Topology

This section describes the migration process when a single machine is deployed.



Figure 2-1: Migration with a Single Machine

Use the following references to the above workflow:

- 1. Step 1: Backup Version 7.2 (see Chapter 3).
- 2. Step 2: Capture Version 7.2 EMS client and server configurations (see Chapter 4).
- **3. Step 3:** Export Version 7.2 Topology and Configuration (see Chapter 5).
- 4. Step 4: Remove all devices from Version 7.2 platform (not including phones and users). This is necessary to ensure the smooth migration to the Version 7.4 platform. Do the following:
 - a. In the EMS GUI, Right-click the region in the MG Tree, and then from the submenu, choose option **Remove Multiple MGs**.
 - **b.** Perform the above step for each existing region.



Warning: When devices are removed from the Version 7.2 platform, all data is removed from the EMS database including alarm history. Therefore ensure that you have backed up the database before proceeding.

- 5. **Step 5:** Check and prepare the server machine for Version 7.4 Installation (see Chapter 6).
- 6. Step 6: Install One Voice Operations Center Version 7.4 (see Chapter 7).
- 7. **Step 7:** Configure One Voice Operations Center Server (see Chapter 8).
- 8. Step 8: Add 1-2 devices and import phones and users to default tenant.
- 9. Step 9: Perform basic testing on these devices and phones/users.



Note: Once you have completed the basic testing, it's highly recommended to remove the manually added devices before commencing the import process.

- 10. Step 10: Import EMS topology and phone configuration and users (see Chapter 9).
- **11. Step 11:** Verify that the topology import was successful and that all phones/users have been registered to the Version 7.4 platform.
- **12. Step 12:** Configure OVOC web client (see Chapter 11).

Note:



- In the event of failure, restore the Version 7.2 installation (see Appendix A.2).
- If your phones are deployed in a **non-Skype for Business** environment, you should import both **phones** and **users**. If your phones are deployed in a **Skype for Business Environment**, you should only import **phones**.

2.2 Dual Machine Topology

This section describes the upgrade process when two machines are deployed.





Use the following references to the above workflow:

- **1. Step 1:** Backup Version 7.2 (see Chapter 3).
- 2. Step 2: Capture Version 7.2 EMS client and server configurations (see Chapter 4).
- 3. Step 3: Export Version 7.2 Topology and Configuration (see Chapter 5).
- 4. Step 4: Install One Voice Operations Center Version 7.4 (see Chapter 7).
- 5. Step 5: Configure One Voice Operations Center Server (see Chapter 8).
- 6. Step 6: Add 3-4 devices to default tenant.
- 7. **Step 7:** Reconfigure the QOE server IP address on the devices using an incremental ini download (ini parameter QOEServerIp).
- 8. **Step 8:** Perform basic testing on these devices.



Note: Once you have completed the basic testing, it's highly recommended to remove the manually added devices before commencing the import process in Step 11.

9. Step 9: Remove devices from the Version 7.2 platform (not including phones and users).

This is necessary to ensure the smooth migration to the Version 7.4 platform. Do the following:

- a. In the EMS GUI, Right-click the region in the MG Tree, and then from the submenu, choose option **Remove Multiple MGs**.
- **b.** Perform the above step for each existing region.



Warning: When devices are removed from the Version 7.2 platform, all data is removed from the EMS database including alarm history. Therefore ensure that you have backed up the database (see Step 1) before proceeding.

- 10. Step 10: Disconnect the Version 7.2 platform from the network.
- **11. Step 11:** Import device topology (see Section 9.1).
- 12. Step 12: Verify that the device topology import was successful.
- **13. Step 13:** Import phone's configuration and users (see Section 9.2).
- **14. Step 14:** Verify phone configuration/users import was successful.
- **15.** Step 15: Move phones to Version 7.4 (see Chapter 1010).
- **16. Step 16:** Verify all phones have been registered to the Version 7.4 platform.
- 17. Step 17: Configure OVOC web client (see Chapter 11).

Note:

- In the event of failure, disconnect the Version 7.4 machine from the network and restore the Version 7.2 machine. In addition, you need to do the following:
- Restore the IP address of the Version 7.2 machine i.e. configure the 'SNMP Trap Manager' parameter on the managed devices with the EMS Version 7.2 IP address. This action can be performed using an incremental ini download.

Restore the devices original QOE server IP address as described in step 7.

 If your phones are deployed in a non-Skype for Business environment, you should import both phones and users. If your phones are deployed in a Skype for Business Environment, you should only import phones. This page is intentionally left blank.

3 Backup Data from EMS/SEM 7.2.3000

You need to run the backup procedures described in this chapter to backup data from the Version 7.2.3000 platform such as Call data and alarms and to store the backup files in an external location.



Warning: All the data exported in the procedures described below cannot be imported to the Version 7.4 platform. If you do not backup this data, then it will be lost.

3.1 Backup Procedure

Before starting migration from 7.2.3000 server to 7.4, make sure to extract all backup files to an external machine. These files can be transferred to an external location directly from their default location by SCP or SFTP client using 'acems' user. These backup files are as follows:

- /data/NBIF/emsBackup/emsServerBackup_<time&date>.tar file.
- All files in /data/NBIF/emsBackup/RmanBackup directory (including control.ctl and init.ora files)

For the full backup procedure, refer to Appendix A.

3.2 Save Data in Textual Format

This procedure describes how to export data in textual format to a CSV file in human readable format. To view this information, you do not need to install any EMS/SEM software CSV file.



Note: The procedure below is not applicable if you keep two server machines until the end of the migration process.

To save machine alarms, in EMS client

- 1. In the main EMS menu, choose **Faults** -> **Alarms History**.
- 2. Filter the relevant alarms.
- 3. In the main menu, choose File > Save Records As.

Save Records As ms Entries out of \$912 Advanced Filter: 🕞 Journal: 🐼 Ala							
Print.	Ctrl+P	09-Mar-2017	10:36	To: 05-Jun-2017	11:10 C		
Exit	Escape	G Name	Source	Action/Alarm Name	Details	Region	
clear	11: 10: 47 Jun 05	172.17.118.58	EMS Server	GW Connection Alarm	Connection establish	AutoDetect	
) info	11: 10: 47 Jun 05	172.17.118.58	EMS Server	(Event) Software Replaced	The software of the previous version: 7.20	AutoDetect	
critical	11:09:22 Jun 05	172.17.118.58	EMS Server	GW Connection Alarm	Connection Lost	AutoDetect	
) info	04: 00: 17 Jun 05	10.3.2.91	EMS Server	(Event) GW Backup Event	Backup file: null from IP: 10.3.2.91 with MG n	aliya	
clear	17: 54: 05 Jun 04	172.17.118.58	Board#1	Gateway Administrative S	Administrative state is unlocked	AutoDetect	
najor	17: 54: 05 Jun 04	172.17.118.58	Board#1	Gateway Administrative S	Network element admin state change alarm	AutoDetect	
clear	17: 54: 05 Jun 04	172.17.118.58	Board#1	Gateway Administrative S	Alarm cleared. Network element admin stat	AutoDetect	
major	17: 54: 05 Jun 04	172.17.118.58	Board#1	Gateway Administrative S	Network element admin state change alarm	AutoDetect	
clear	13:45:36 Jun 04	172.17.118.58	Board#1/Et	Ethernet Group Alarm	Alarm cleared: Ethernet Group alarm. Ether	AutoDetect	
clear	13:45:36 Jun 04	172.17.118.58	Board#1/Et	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN port	AutoDetect	
major	13:45:36 Jun 04	172.17.118.58	Board#1/Et	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 1 is D	AutoDetect	
 minor	13:45:36 Jun 04	172.17.118.58	Board#1/Et	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 1 is do	AutoDetect	
clear	13:45:36 Jun 04	172.17.118.58	EMS Server	GW Connection Alarm	Connection establish	AutoDetect	
critical	13:43:51 Jun 04	172.17.118.58	EMS Server	GW Connection Alarm	Connection Lost	AutoDetect	
clear	13:40:15 Jun 04	172.17.118.58	Board#1/Et	Ethernet Group Alarm	Alarm cleared: Ethernet Group alarm. Ether	AutoDetect	
clear	13:40:15 Jun 04	172.17.118.58	Board#1/Et	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN port	AutoDetect	
najor	13:40:15 Jun 04	172.17.118.58	Board#1/Et	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 1 is D	AutoDetect	
minor	13: 40: 15 Jun 04	172.17.118.58	Board#1/Et	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 1 is do	AutoDetect	
clear	13: 40: 15 Jun 04	172.17.118.58	EMS Server	GW Connection Alarm	Connection establish	AutoDetect	
critical	13: 38: 50 Jun 04	172.17.118.58	EMS Server	GW Connection Alarm	Connection Lost	AutoDetect	
clear	10: 41: 15 Jun 04	172.17.118.58	Board#1	Gateway Administrative S	Administrative state is unlocked	AutoDetect	

Figure 3-1: Alarms History

- If less than 1500 alarms are filtered then there is an option to save them to CSV in the EMS client machine.
- If more than 1500 alarms are filtered then there is an option to save them to CSV file in the server machine\

Figure 3-2: Alarm History Prompt



- CSV file location in the server \ACEMS\NBIF\alarms directory
- CSV file format example: alarm_result_07-06-2017_16-55-39-60939.csv

EMS - Export Journals to TXT file

To save current old machine journal records, copy journal records text files from /var/log/ems/journalX files

EMS - Export PM Files

To save current old PM files, extract all files from /ACEMS/NBIF/pmFiles/

EMS - Export Devices Backup Files

To save current old device backup files (ini/CLI), extract all files from /ACEMS/NBIF/mgBackup

SEM - Export Calls to a CSV

To save calls available in your current SEM view, click 'Save As' icon from the right top corner of the Calls Screen (up to 10.000 calls loaded into your view).

4 Capture Version 7.2 EMS & SEM Configuration

The checklist shown in the table below can be used as a guide for retrieving the Version 7.2.3000 configuration on the EMS & SEM application.

Configuration Action	Action Check	Reference	Insert Screen Capture Here
EMS Server Configuration			
General Status information		See Section 8.1.2	
Web server and web port configuration		See Section 8.1.3	
Change Schedule Backup Time		See Section 8.1.4	
Ethernet Interfaces		See Section 8.1.5.1	
Ethernet Redundancy		See Section 8.1.5.2	
DNS Client		See Section 8.1.5.3	
NAT		See Section 8.1.5.4	
Static Rules		See Section 8.1.5.5	
SNMP Agent		See Section 8.1.5.6	
SNMPv3 Engine ID		See Section 8.1.5.6.1	
NTP or date configuration		See Section 8.1.6	
SSH		See Section 8.1.7.1	
DB Password		See Section 8.1.7.2	
OS Password		See Section 8.1.7.3	
File Integrity Checker		See Section 8.1.7.4	
Software Integrity Checker		See Section 8.1.7.5	
EMS Client Configuration			
Local User Authentication		See Section 11.1	

RADIUS Authentication	See Section 11.2.1	
LDAP Authentication	See Section 11.2.2	
Alarm Settings	See Section 11.3.1	
Alarm Forwarding Rules	See Section 11.3.2	
Software Manager	See Section 11.4	
Device Backup Configuration	See Section 11.5	
LDAP User Authentication	See Section 11.6	
SEM Client Configuration		
Active Directory Configuration	See Section 11.7.1	
Skype for Business SQL Server Configuration	See Section 11.7.2	
QoE Thresholds Configuration	See Section 11.7.3	
Alarm Rules	See Section 11.7.4	
Statistics Reports	See Section 11.7.5	

5 Export Topology and IP Phone Configuration

This chapter describes how to export the EMS topology and the IP Phone Management server configuration from the Version 7.2.3000 platform.



Note: Customers with installed versions earlier than 7.2.3xx, should upgrade the application to the Version 7.2.3000 platform before exporting topology.

5.1 Export EMS Topology

This section describes how to export EMS topology from Version 7.2.3000. The topology export procedure extracts and backs up the topology configuration from the Version 7.2.3000 platform to an XML file. This file can then be imported to the new Version 7.4 server. The procedure described in this section backs up the following topology configuration:

- Regions
- AudioCodes devices
- SEM Lync devices
- SEM generic devices
- SBAs
- SEM Links
- Regions which had different permissions on Version 7.2.3000
- License Pool configuration for each managed device

To export EMS topology:

- Extract the following files to an accessible location from the Version 7.4 release DVD3 or from the AudioCodes FTP site:
 - EmsServerInstall/ac_ems_deploy/server_7.4.XXX/topologyExport.pl
 - EmsServerInstall/ac_ems_deploy/server_7.4.XXX/ topologyDBExport.sql
- **2.** Login to the Version 7.2.3000 platform as 'root' user with password *root* (default password is root):

```
su - root
```

3. Enter the following command:

cd /home/acems/

- 4. Transfer the above files to this location.
- 5. Make sure both of these files have execute permissions.

```
cd /home/acems
chmod 755 topologyExport.pl
chmod 755 topologyDBExport.sql
```

6. Execute topologyExport.pl script.

```
cd /home/acems
./topologyExport.pl
```

- 7. Copy the following files to an accessible location outside of the Server machine:
 - /home/acems/topology.xml file containing the above topology
 - /home/acems/keystore.jks

8. Copy ssl.crt and ssl.key to an outside location.

Figure 5-1: Copy Certificate Files

[root@EMS-server-17								
/etc/httpd/conf.d								
(nectOFMS common 17	appf dl#							
[roougems-server-1/	cour • a]#	T T						
total 36								
-rw-rr 1 root ro	ot 2926	Apr	12	22:03	autoindex.conf			
-rwxr-xr-x 1 root ro	ot 27	Sep	3	09:06	passphrase			
-rw-rr 1 root ro	ot 625	Feb	18	2017	php.conf			
-rw-rr 1 root ro	ot 366	Apr	12	22:04	README			
-rwxr-xr-x 1 root ro	ot 10708	Sep	11	08:14	ssl.conf			
drwxr-xr-x 2 root ro	ot 71	Sep	3	09:06	ssl.crt			
drwxr-xr-x 2 root ro	ot 24	Sep	3	09:06	ssl.key			
-rw-rr 1 root ro	ot 1252	Apr	12	14:50	userdir.conf			
-rw-rr 1 root ro	ot 824	Apr	12	14:50	welcome.conf			
[root@EMS-server-17	conf.d]#							

- **9.** If you have manually modified any of the following parameters of the **/etc/httpd/ssl.conf** file, backup this file to an external location (this file needs to be later manually updated in the Import procedure-see Chapter 9):
 - SSLProtocol
 - SSLCipherSuite.
 - SSLCertificateFile.
 - SSLCertificateKeyFile .
 - SSLCACertificateFile
- 10. Copy all Version 7.2 Software Manager files to the /home/acems directory:

```
cp -Rf /data/emsSwfiles/ /home/acems
chown -R acems /home/acems
```

11. Using an FTP server, copy these files to an external location (see Appendix C): /home/acems/emsSwfiles



Note: There are several limitations regarding the topology export procedure as described in *Appendix B*.

5.1.1 Example Output

</REGIONS>

<NODES>

<NODE><NODE_ID>137</NODE_ID><NODE_NAME>10.3.2.91</NODE_NAME><IP_AD
DRESS>10.3.2.91</IP_ADDRESS><REGION_ID>65</REGION_ID><REGION_NAME>
aliya</REGION_NAME><READ_COMMUNITY>8kXtnrBulPfiTHO3hg3LfQ==</READ_
COMMUNITY><WRITE_COMMUNITY>f/OB4MNtinsMV6rykI4hFg==</WRITE_COMMUNI
TY><SERIAL_NUMBER>5200382</SERIAL_NUMBER><HTTPS_PROXY_ENABLED>0</H
TTPS_PROXY_ENABLED><GATEWAY_USER>Admin</GATEWAY_USER><GATEWAY_PASS
WORD>fseUajPSaO6h4Ug5tO9y1g==</GATEWAY_PASSWORD><NETWORK_X_LOCATIO
N>197</NETWORK_X_LOCATION><NETWORK_Y_LOCATION>468</NETWORK_Y_LOCAT
ION></NODE>

<NODE><NODE_ID>120</NODE_ID><NODE_NAME>172.17.140.118</NODE_NAME><
IP_ADDRESS>172.17.140.118</IP_ADDRESS><REGION_ID>65</REGION_ID><RE
GION_NAME>aliya</REGION_NAME><READ_COMMUNITY>8kXtnrBulPfiTHO3hg3Lf
Q==</READ_COMMUNITY><WRITE_COMMUNITY>f/OB4MNtinsMV6rykI4hFg==</WRI
TE_COMMUNITY><SERIAL_NUMBER>5972470</SERIAL_NUMBER><SECOND_SERIAL_
NUMBER>5206735</SECOND_SERIAL_NUMBER><HTTPS_PROXY_ENABLED>0</HTTPS
PROXY_ENABLED><GATEWAY_USER>Admin</GATEWAY_USER><GATEWAY_PASSWORD
>fseUajPSa06h4Ug5t09y1g==</GATEWAY_PASSWORD><NETWORK_X_LOCATION>18
7</NETWORK_X_LOCATION><NETWORK_Y_LOCATION>70</NETWORK_Y_LOCATION>

</NODES>

<NON ACL NODES>

<NON_ACL_NODE><NODE_ID>188</NODE_ID><NODE_NAME>2.2.2.2.

<SBAs>

<SBA><NODE_ID>256</NODE_ID><SBA_ID>1</SBA_ID><FQDN_NAME>test@ac.co
m</FQDN_NAME><IP_ADDRESS>10.1.1.1</IP_ADDRESS><READ_COMMUNITY>publ
ic1</READ_COMMUNITY><WRITE_COMMUNITY>private1</WRITE_COMMUNITY><DE
SCRIPTION>test</DESCRIPTION></SBA>

</SBAs>

<LINKS>

<LINK><LINK_ID>1333261328</LINK_ID><LINK_NAME>link1</LINK_NAME><SR C_NODE_ID>91</SRC_NODE_ID><DEST_NODE_ID>188</DEST_NODE_ID><LINK_TY PE>1</LINK_TYPE><TYPE_IP_GROUP>4</TYPE_IP_GROUP><TYPE_MEDIA_REALM> 0</TYPE_MEDIA_REALM><TYPE_SUB_MEDIA_REALM>0</TYPE_SUB_MEDIA_REALM> <LINK_DIRECTION>1</LINK_DIRECTION></LINK>

</LINKS>

<POOL FEATURES>

</POOL_FEATURES>

<MT_REGIONS>

- <MT_REGION><REGION_ID>65</REGION_ID></MT_REGION>
- </MT_REGIONS>
- </TOPOLOGY>
- copy topology.xml file to /ACEMS/NBIF/topology/
- copy topology.xml file to home/acems/

5.2 Export IP Phone Management Server Configuration

This section describes how to export the IP Phone Management Server configuration from Version 7.2.3000.

Note After this procedure is performed, the following cannot be configured on the Version 7.4 platform without making manual changes to the configuration template file (contact AudioCodes technical support for details):



- Automatically configuring HTTPS
- Tenant and Site configuration
- System daylight savings time

> To export IP Phone Management server configuration:

- Download the export configuration zip file to your PC from: <u>https://services.audiocodes.com/app/answers/detail/a_id/55</u>
- 2. Unzip the downloaded file.
- Copy admin folder to the Version 7.2.3000 EMS server (with WinSCP) on /tmp folder as 'acems' user.
- **4.** Login to Version 7.2.3000 telnet (putty) as 'root' user with password *root* (default password is root):

su - root

5. Run the following commands:

```
yes | cp -r /tmp/admin/* /ACEMS/ippmanager/admin/
chown -R emsadmin /opt/ACEMS/ippmanager/*
```

6. Login to IP Phone Management server Version 7.2.3000 Web client.

Enter the following URL: http://<IP_ADDRESS>/ipp/admin/AudioCodes_files/export.php The following screen is displayed:

Figure 5-2: Export Topology

Export for importing to EMS 7.4... version

Export Conliguration	Click the button to export Configuration
2. Import the configur	ration settings to new EMS 7.4 system.
Export the users an	d devices.
-	

- 7. Click the **Export Configuration** button. The configuration file is downloaded to your PC.
- 8. Click the **Export Users** button. The configuration file is downloaded to your PC.



This page is intentionally left blank.

6 Check and Prepare Server Machine for Version 7.4 Installation

Please make sure that your machine is compatible with the Hardware Requirements described in *One Voice Operations Center Version 7.4 IOM Guide* (according to the required capacity).



Note: If your Version 7.2.3000 installation platform was installed with Bare Metal High Availability solution, it's not supported for Version 7.4 One Voice Operations Center.



This page is intentionally left blank.

7 Install the One Voice Operations Center

Install the One Voice Operations Center 7.4 software according to the instructions in the One Voice Operations Center Version 7.4 IOM Guide (according to the required capacity). After the installation, you should load the license file received from AudioCodes.



Note: If you do not have the license file, extract the server machine ID (see Section "License" in the *One Voice Operations Center Server IOM* document) and contact AudioCodes for new license.

7.1 OVOC Software Deliverables

This section describes the OVOC software deliverables.

7.1.1 Dedicated Hardware Media

- **DVD1:** Operating System DVD for Linux (refer to the *One Voice Operations Center Server IOM*):
- **DVD2:** Oracle Installation: Oracle installation Version 12.1.0.2 DVD for the Linux platform.
- DVD3: The 'SW Installation and Documentation' DVD for Linux comprises the following folders:
 - OVOC'EmsServerInstall' OVOC server software, to install on the dedicated Linux based OVOC server machine.
 - 'Private_Labeling' folder includes all the information required for the OEM to create a new private labeling DVD (this folder is not available in the initial Version 7.4 release).
 - Documentation All documentation related to the present OVOC Version. The documentation folder includes the following documents and sub-folders:
 - One Voice Operations Center Release Notes Document includes the list of the new features introduced in the current software Version as well as Version restrictions and limitations.
 - One Voice Operations Center Server IOM Manual Installation, Operation and Maintenance Guide.
 - One Voice Operations Center User's Manual Document
 - One Voice Operations Center Integration with Northbound Interfaces
 document
 - 'GWs_OAM_Guides' folder document set describing Alarms supported for each product

7.1.2 Virtual Machine Media (VMware and Hyper-V)

The Virtual Machine software delivery (VMware – OVA file) (Hyper-V - Zip file) and the documentation set can be downloaded from the AudioCodes Website by registered customers at <u>http://www.audiocodes.com/downloads</u>.

7.2 **Pre-installation**

7.2.1 Testing Installation Requirements -Dedicated Hardware

Before commencing the OVOC server installation procedure, verify that your system meets the hardware, disk space, operating system and other requirements that are necessary for a successful installation.

To ensure that your machine meets the minimal hardware requirements for running the OVOC application on both dedicated and virtual hardware, run the commands described below in **tbash**.

RAM - A minimum of <machine type_RAM> GB is required (refer to the One Voice Operations Center IOM Guide). To determine the amount of random access memory installed on your system, enter the following command:

more /proc/meminfo | grep MemTotal

Swap Space - Swap space is twice the system's physical memory, or 4 GB, whichever is greater.

To determine the amount of swap space currently configured in your system, enter the following command:

more /proc/meminfo | grep SwapTotal

Disk Space – A minimum of <machine type_disk space> GB is required (refer to the One Voice Operations Center IOM Guide). To determine the amount of disk space on your system, enter the following command:

```
fdisk -l | grep Disk
```

During the application installation, you are required to reserve up to 2 GB of Temporary disk space in the **/tmp**. If you do not have enough space in the **/tmp** directory, set the **TMPDIR** and **TMP** environment variables to specify a directory with sufficient space.

DVD-ROM device - A DVD-ROM drive capable of reading ISO 9660 format.

Figure 7-1: Linux Testing Requirements

```
[root@EMS-Server-Linux113 ~]# tcsh
[root@EMS-Server-Linux113 ~]# uname
Linux
[root@EMS-Server-Linux113 ~]# more /proc/meminfo | grep MemTotal
MemTotal: 2017056 kB
[root@EMS-Server-Linux113 ~]# more /proc/meminfo | grep SwapTotal
SwapTotal: 3020180 kB
[root@EMS-Server-Linux113 ~]# fdisk -1 | grep Disk
Disk /dev/sda: 250.0 GB, 250059350016 bytes
[root@EMS-Server-Linux113 ~]#
```



Note: Use the AudioCodes' DVD1 to install the Linux Operating System.

7.2.2 Files Verification

You need to verify the contents of the ISO, Zip or OVA 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 is commonly used to check the integrity of file, and verify download. Perform the following verifications on the relevant platform:

- Windows (see below)
- Linux (see Section 7.2.2.2).

7.2.2.1 Windows

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

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

7.2.2.2 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 7-2: File Integrity Verification

[root@isocreator 6.6.192]# ls -lh total 7.4G
-rwx 1 root root 7.3G Aug 11 00:09 DVD5 vEMS VMware 6.6.192.iso
-rwx 1 root root 63 Aug 11 00:16 DVD5 vEMS VMware 6.6.192.md5
[root@isocreator 6.6.192]#
<pre>[root@isocreator 6.6.192]# md5sum -c DVD5_vEMS_VMware_6.6.192.md5</pre>
DVD5_vEMS_VMware_6.6.192.iso: OK
[root@isocreator 6.6.192]#

7.2.3 OVOC Server Users

OVOC server OS user permissions are differentiated 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 EMS Server Manager and OVOC application execution.
- acems user: The only available user for login through SSH/SFTP tasks.
- emsadmin user: User with permissions for mainly the EMS Server Manager and OVOC application for data manipulation and database access.
- oracle user: User permissions for the Oracle database access for maintenance such as installation, patches upgrade, backups and other Oracle database tasks.
- oralsnr user: User in charge of oracle listener startup.

7.3 Installing the 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.
- **DVD2:** Oracle Installation: Oracle installation DVD platform.
- **DVD3:** OVOC application: OVOC server application installation DVD.

7.3.1 **DVD1-CentOS 7.3 Rev 18**

The procedure below describes how to install Linux CentOS 7.3. This procedure takes approximately 20 minutes.



Note: Before commencing the installation, you must configure RAID-0 (see Appendix *Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen8 Servers in the One Voice Operations Center IOM Guide.*

To perform DVD1 installation:

- 1. Insert the **DVD1-CentOS 7.3 Rev 18** 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 entering 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 7-3: Linux CentOS Installation



Figure 7-4: CentOS 7

VEMS-83	🖬 🖬 🔤 🍪 Actions 🛞
CentOS 7 for OVOC (Rev. 18)	
- To start installation, press <enter> key.</enter>	
– To start installation from RS-232 serial console, type $rs23$	2 <enter>.</enter>
- To boot from local disk, type local <enter>.</enter>	
boot: _	

6. Wait for the installation to complete.

VEMS-83	🖬 🖬 🚞 🏰 Actions 🛞 .
Installing compat-libgfortran-41 (392/417)	
Installing compat-libf2c-34 (393/417)	
Installing iu/2000-firmware (394/417)	
Installing iw1000-firmware (395/417)	
Installing rootfiles (396/41/)	
Installing $ u 2030-1$ Irmware $(337/417)$	
Installing initiation (GOO Finance (GOO 417)	
Installing iuldide i Irmware (337/11/)	
Installing introfiemence (401/417)	
Installing inits finance (42/417)	
Installing iul250-finnane (403/417)	
Installing iul 2005 firmune (402/417)	
Installing iuligis firmare (405/417)	
Installing includes $(496/412)$	
Installing iul7265-firmware (407/417)	
Installing iw16000g2b-firmware (408/417)	
Installing jul6000g2a-firmware (409/417)	
Installing iw15000-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	
rerforming post-installation setup tasks	
•	
Carling installed outer	
con iguring installea system	
· Letting notions configuration	
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	
Tanaconda] 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.



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

Figure 7-6: Linux CentOS Installation Complete

👺 10.7.19.100:22 - Tera Term VT	
Eile Edit Setup Control Window Help	
++ Complete +	+
Congratulations, your CentOS installation is complete.	
Remove any media used during the installation process and press <enter> to reboot your system.</enter>	
Controller → residence intervention of P = and residence → residence → Politication of Pol	
++	
Reboot	
+	
	+
<tab>/<alt-tab> between elements <space> selects <f12> r</f12></space></alt-tab></tab>	ext scr
ee <enter> to reboot</enter>	
	•

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

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

Figure 7-7: Linux CentOS Network Configuration

墬 10.7.19.100:22 - Tera Term VT	
<u> E</u> ile <u>E</u> dit <u>S</u> etup C <u>o</u> ntrol <u>W</u> indow <u>H</u> elp	
ems-server login: root Password: [root@ems-server ~]# network-config	<u> </u>
Current network configuration:	
Hostname : ems-server IP Address : 169.254.101.1 Subnet Mask : 255.255.0.0 Default Gateway : 169.254.0.1	
Do you wish to change it? (y/[n]) : y	
Hostname : EMS-Linux145 IP Address : 10.7.14.145 Subnet Mask : 255.255.0.0 Default Gateway : 10.7.0.1	
Apply new configuration? ([y]/n) : y	
	-



Note: This script can only be used during the server installation process. Any additional Network configuration should later be performed using the EMS 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**.

7.3.2 DVD2: Oracle DB Installation

The procedure below describes how to install the Oracle database. This procedure takes approximately 30 minutes.



Note: 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 perform DVD2 installation:

- 1. Insert **DVD2-Oracle DB installation** into the DVD ROM.
- 2. Login into the OVOC server by SSH, as 'acems' user, and enter password *acems*.
- 3. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

- 4. On some machines, you need to mount the CDROM in order to make it available: mount /misc/cd
- 5. Run the installation script from its location:

```
cd /misc/cd
./install
```

Figure 7-8: Oracle DB Installation (Linux)



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

Figure 7-9: Oracle DB Installation - License Agreement (Linux)



7. Type the 'SYS' user password, type **sys** and then press Enter.

Figure 7-10: Oracle DB Installation (Linux) (cont)

SQL> Connected to an idle SQL> ORACLE instance star	instance. ted.
Total System Global Area Fixed Size Variable Size Database Buffers Redo Buffers SQL> File created.	321601536 bytes 2102168 bytes 251661416 bytes 62914560 bytes 4923392 bytes
SQL> Disconnected from Or >>> Restoring database RMAN> RMAN> RMAN> RMAN> RMAN> R	acle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production File using RMAN MAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> >>>
Restore has finished succ >>> Please enter a pas sys	essfully sword for the SYS user:

8. Wait for the installation to complete; reboot is not required at this stage.

Figure 7-11: Oracle DB Installation (Linux) (cont)



7.3.3 DVD3: OVOC Server Application Installation

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

- **To perform DVD3 installation:**
- 1. 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.
- Switch to 'root' user and provide *root* password (default password is *root*):
 su root
- 4. Run the installation script from its location:

```
cd /misc/cd/EMSServerInstall/
./install
```

Figure 7-12: OVOC Server Application Installation (Linux)



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

Figure 7-13: OVOC Server Application Installation (Linux) – License Agreement

U.I.I. III III 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.

6. 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 7-14: OVOC Server Application Installation (Linux) (cont)

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

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 s	uccessfully.	
>>> 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 s	uccessfully.	
+++++++++++++++++++++++++++++++++++++++	*********	
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		

- 7. After the OVOC server has successfully rebooted, repeat steps 2 4.
- 8. At the end of Java installation, press Enter to continue.

Figure 7-15: OVOC Server Application Installation (Linux) - Java Installation



- 9. Wait for the installation to complete and then do the following:
 - a. If you are migrating on a single machine and your deployment includes phones:
 - Type the following command:
 - # EmsServerManager
 - From the Application Maintenance > Web Servers menu, close ports 8081 and 8082.
 - **b.** Reboot the OVOC server by typing **reboot** or by using the EMS Server Manager (Application Maintenance Menu).

Figure 7-16: Installation Complete

Done	
>>>	
>>> Installation Completed, Oracle is Now Secured	
>>>	
>>> Remove /tmp/EmsServerInstall	
[root@EMS-Linux145 EmsServerInstall]#	

- **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.** Verify in the EMS Server Manager that the Date and Time are set correctly (refer to the *One Voice Operations Center IOM Manual*).
- **13.** Verify in the EMS Server Manager that the OVOC server is up and running (refer to the *One Voice Operations Center IOM Manual*) and login to Web client to verify a successful installation.

7.4 Installing the OVOC on Virtual Server Platform

This chapter describes how to install the OVOC on a Virtual Server platform. The following procedures are described:

- Installing the OVOC server on the VMware platform (see Section 7.4.1).
- Installing the OVOC server on Microsoft Hyper-V platform (see Section 7.4.2).



Note: The AudioCodes OVOC supports the VMware vSphere High Availability (HA) feature.

7.4.1 Installing the OVOC Server on the VMware Platform

The installation of the OVOC server on VMware vSphere platform includes the following procedures:

- Installing the Virtual Machine (VM) (see Section 7.4.1.1).
- Configuring the Virtual Machine Hardware Settings (see Section 7.4.1.2).
- Connecting OVOC server to network (see Section 7.4.1.3).
- Configuring OVOC Virtual Machines (VMs) in a VMware Cluster (see Section 7.4.1.4).

7.4.1.1 Installing the VMware Virtual Machine

This section describes how to install the OVOC server on the VMware vSphere platform. 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 Section 7.4.1.2). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed. The VMware Virtual Machine installation package is distributed as a VM image OVA file (see Section 7.1.2).

- > To install the OVOC Server on VMware vSphere:
- 1. Copy the OVA file containing the VMware Virtual Machine installation package received from AudioCodes to your PC (see Appendix C for instructions on how to transfer files).
- 2. Open the VMware vSphere Web Client.

vmware [®] vSphere Web Cli	ent ≜ ≣			ひ I vmware	@QASWVCEN	TER01 👻	l Help 🖌 l 🔍 S	learch	•
Navigator I	付 Home							🔯 Alarms 🛛	¥Χ
Hosts and Clusters	Home							All (1) Ne Ack	k
💣 Home	Inventories							• qaswvcenter01.co	or
😼 vCenter Inventory Lists 🔰						_	3	Performance Char	rt
Hosts and Clusters >			3		<u> </u>				_
VMs and Templates	vCenter	losts and	VMs and	Storage	Networking	Cont	ent		_
Storage > ::	Inventory Lists	Clusters	lemplates			Librai	nes	Mork In Progra	
Vetworking >								Bunc - Edi	
Policies and Profiles		O			C			Low Col	
A Hybrid Cloud Manager		Dealiza							
VRealize Orchestrator	Manager C	rchestrator							
Opdate Manager	Monitoring								
Administration >	Watch How-to Vi	leos							
😴 Tasks 🔻	្រា				F 10.	12	•		
😨 Recent Tasks								1	Į ×
Task Name	Target	Status		Initiator	Queued Fo	r	Start Time	Completion Time	Se
Reconfigure virtual machine	🚰 uoc	 Completed 		vmware		19 ms	11/17/2016 10:03:1	11/17/2016 10:03:2	qa
									- 1
•									
My Tasks ▼ Tasks Filter ▼								More Ta	asks

Figure 7-17: VMware vSphere Web Client

3. In the vCenter Navigator, select **Hosts and Clusters**. A list of Hosts and Clusters is displayed:

Figure	7-18:	Hosts	and	Clusters
--------	-------	-------	-----	----------

vmware [®] vSphere Web Cli	ient f i≘			ひ I vmware@	QASVWCENTER01		Help	🝷 I 🔍 Search 💽
Navigator I	🗊 qaswCluster01	Actions 👻				-	≞ ▼	🔯 Alarms 🛛 📕 🖈 📥
Home Generation of the second	Summary Monitor Image: Cluster Resource Image: Cluster Resource Image: Cluster Consume Related Objects Datacenter Image: Cluster Resource	Manage Related Objects pasw Chuster01 Total Processors: 20 Total Vhotion Migrations: 48 Total Vhotion Migrations: 48 Total Vhotion Migrations: 6 Es Es ASWDatacenter More Related Object		CPU USED: 14.07 GHz MEMORY USED: 128.05 GB STORAGE USED: 2.47 TB VSphere HA VSphere HA VSphere HA	CAPACITY: 55 49 CAPACITY: 51 49 CAPACITY: 191, FREE: 43, CAPACITY: 81 CAPACITY: 81 CAPACITY: 81 CAPACITY: 81 CATEgory This list is empty.	9 GHz 8 GHz 88 GB 93 GB 20 TB 87 TB		All (1) New (1) Acknowl
🕄 Recent Tasks								∓ ×
Task Name	Target	Status	In	itiator	Queued For	Star	t Tim	e Completion Time
								Ţ



Figure 7-19: Deploy OVF Template Option

4. In the Navigator, select the cluster and from the right-click menu, choose **Deploy OVF Template**.

The following screen may be displayed if the Client Integration Plug-in is not installed on your PC. Click the **Download the Client Integration Plug-in** link to download this application to your PC and then install it.

Figure 7-20: Client Integration Plug-in

Deploy OVF Template	4 (s)
1 Source	Select source Select the source location
1a Select source	
1b Review details	The Client Integration Plug-in must be installed to enable OVF functionality. Click the link below to download the installer.
2 Destination	If installed, refresh the browser and allow access.
2a Select name and folder	Download the Client Integration Plug-in
2b Select storage	
3 Ready to complete	
	Back Next Finish Cancel

Deploy OVF Template		?
1 Source 1a Select source 1b Review details 2 Destination 2a Select name and folder 2b Select a resource 2c Select storage 3 Ready to complete	Select source Select the source location Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your comp such as a local hard drive, a network share, or a CD/DVD drive. URL Council Trian Council	uter,
Dpen	Back Next Finish	Cancel
Look in: Recent Places Desktop Libraries Computer Network	OVF ↓ ♠ ♠ ♠ ●	
	File name: Open Files of type: OVF Packages (*.ovf, *.ova)	

Figure 7-21: Browse to OVF Package

5. Browse to the OVF file with extension OVA that you saved to your PC, and click **Next**.

Deploy OVF Template			(? H
1 Source ✓ 1a Selectsource	Review details Verify the OVF tem	plate details	
V 1b Review details	Product	7.4	
2 Destination	Version		
2a Select name and folder	Vendor		
2b Select storage	Publisher	No certificate present	
2c Setup networks	Download size	7.6 GB	
3 Ready to complete Si	Size on disk	26.7 GB (thin provisioned) 60.0 GB (thick provisioned)	
	Description		
		Back Next Finish	Cancel

Figure 7-22: OVF Template Details Screen

6. In the OVF Template Details screen, click **Next**.



Deploy OVF Template		(? H
Source 1a Select source 1b Review details 2 Destination	Select name and folder Specify a name and location for the deployed template Name: AudioCodes_OC	
 2 Desuriation 2a Select name and folder 2b Select storage 2c Setup networks 3 Ready to complete 	Select a folder or datacenter Select a folder or datacenter Search Image: S	The folder you select is where the entity will be located, and will be used to apply permissions to it. The name of the entity must be unique within each vCenter Server VM folder.
		Back Next Finish Cancel

7. In the Name and Location screen, enter the desired virtual machine name and choose the inventory location (the Data Center to locate the machine), and then click **Next**.

i igule i -27. Destiliation Stolage Scieen
--

Deploy OVF Template						(?)
 1 Source 1a Select source 1b Review details 2 Destination 2a Select name and folder 	Select storage Select location to store the Select virtual disk format: VM Storage Policy: The following datastores a	files for the deployed Thin Provision Datastore Default are accessible from the	template v e destination resource th)	t the destination da	tastore for the
2b Select storage 2c Setup networks	virtual machine configurat	Capacity	virtual disks.	Free	Туре	Storage DRS
3 Ready to complete	Netapp04.lun2	3.00 TB	3.58 TB	1.55 TB	VMFS	
,,	Netapp04.lun1	1.50 TB	1.70 TB	840.06 GB	VMFS	
	datastore211	1.08 TB	310.22 GB	808.19 GB	VMFS	
				Back	Next Finis	sh Cancel

- 8. In the Storage screen, do the following:
 - Select Virtual Disk Format- choose the desired provisioning option ('Thin Provisioning' is recommended),
 - Select the data store where wish to locate your machine, and click Next.

Figure 7-25:: Setup Networking Screen

Deploy OVF Template				(* §
1 Source	Setup networks Configure the networks the deployed templa	ate should use		
 1b Review details 	Source	Desti	ination	Configuration
2 Destination	VMI NELWOIK 4		▼	v
 2a Select name and folder 				
✓ 2b Select storage				
✓ 2c Setup networks				
 3 Ready to complete 	IP protocol: IPv4	IP allocation	n: Static - Manual 🚯	
	Source: VM Network 4 - Description The VM Network 4 network			
	Destination: VM Network - Protocol settings			
	No configuration needed for this network			
		[Back Next Finis	sh Cancel

9. In the Network setup screen, select the network where the deployed template should apply, and click **Next**.

Deploy OVF Template				(? H
Deploy OVF Template Source I a Select source I b Review details Destination 2 a Select name and folder 2 b Select storage 2 c Setup networks 3 Ready to complete	Ready to complete Review your settings selection OVF file Download size Size on disk Name Datastore Target Folder Disk storage Network mapping IP allocation	Is before finishing the wizard. 110.3.180.180sharelovflv/OC_T.4 7.6 GB 60.0 GB AudioCodes_OC Netapp04.iun2 10.3.180.211 QASWDatacenter Thick Provision Lazy Zeroed VM Network 4 to VM Network Static - Manual, IPv4	1.255.00a	"
	Power on after deploymen		Back Next F	nish Cancel

Figure 7-26: Ready to Complete Screen

10. In the Ready to Complete screen, ensure the option 'Power on after deployment' is not selected, and click **Finish**.

Figure 7-27: Deployment Progress Screen

💋 10% Deploying OC	
Deploying	
Deploying disk 1 of 1	
18 minutes remaining	
Close this dialog when completed	Cancel

Recent Tasks			
Name	Target	Status	Requested Start Time 🛛 🗢
Deploy OVF template	Audiocodes OC	14% 💶 🗌	21/05/2012 09:32:26



Recent Tasks					
Name	Target	Status	Requested Start Time 🛛 🗸	Start Time	Completed Time
Reconfigure virtual machine	Audiocodes OC	Completed	21/05/2012 11:03:39	21/05/2012 11:03:39	21/05/2012 11:03:41

11. Wait until deployment process has completed. This process may take approximately half an hour.

7.4.1.2 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, refer to the *One Voice Operations Center IOM Manual*.

Table 7-1:	VMware	Virtual	Machine	Settings
------------	--------	---------	---------	----------

Required Parameter	Value
Disk size	Fill-in-here
Memory size	Fill-in-here
CPU cores	Fill-in-here

> To configure the virtual machine hardware settings:

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

	01	
SSBC	Actions - voc	
🔂 vCent	Power	•
🗗 VOC	Guest OS	•
🗗 voc	Snapshots	•
	🚰 Open Console	
i	💁 Migrate	
	Clone	,
	Template	•
1	Fault Tolerance	•
-	VM Policies	•
-	Compatibility	•
-	Export System Logs	
	Edit Resource Settings	
	🦻 Edit Settings	
	Mous To	

Figure 7-28: Edit Settings option

2. In the **CPU**, Memory and **Hardware** tabs set the required values accordingly to the desired OVOC server VMware Disk Space allocation. (refer to the *One Voice Operations Center IOM*), and then click **OK**.

CentOS7-ems-219 - 8	(9)					
Virtual Hardware VM C	Options	SDRS Rules	vA	pp Option	5	
CPU	1		•	0		
Memory	8192		•	MB	-	
Hard disk 1	300		+	08)		
• 🛃 SCSI controller 0	LSILog	pic Parallel	-		-	
• Metwork adapter 1	VM N	etwork.				Connect
CO/DVD drive 1	Datas	tone ISO File				Connect.
Floppy drive 1	Client	Device				Connect.
Video card	Specif	ly custom setting	5			
WMCI device						
Other Devices						
+ Upgrade	Sch	edule VM Comp	atbi	ity Upgrad	50	
New device:		Select	-			Add

Figure 7-29: CPU, Memory and Hard Disk Settings

Note:

- 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 (see Section 7.4.1.4).
- 3. Wait until the machine reconfiguration process has completed.

Figure 7-30: Recent Tasks

Recent Tasks					
Name	Target	Status	Requested Start Time 🛛 🗢	Start Time	Completed Time
Reconfigure virtual machine	Audiocodes OC	Completed	21/05/2012 11:03:39	21/05/2012 11:03:39	21/05/2012 11:03:41

7.4.1.3 Connecting OVOC Server to Network

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 assign OVOC Server IP address to network:

 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 (refer to the One Voice Operations Center IOM Manual).



Figure 7-31: Power On

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

EmsServerManager

- 6. If you are migrating on a single machine and your deployment includes phones:
 - From the Application Maintenance > Web Servers menu, close ports **8081** and **8082**.
- 7. From the Network Configuration > Server IP Address menu, set the OVOC server network IP address.
- 8. Perform other configuration actions as required using the EMS Server Manager (refer to Chapter 8).

7.4.1.4 Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

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

7.4.1.4.1 Site Requirements

Ensure that your VM cluster site meets the following requirements:

- The configuration process assumes that you have a VMware cluster which 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 (see figure below).

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

	-								
nary Monitor Manage	Related Objects								
ngs Networking Storage	Alarm Definitions Tags Per	missions Schedule	d Tasks Up	date Manager					
	Storago Adaptore								
orago Adaptore	Sibilage Adapters								
orage Auapters	- 🛯 🖸 💄 🖉							Q Filter	
orage Devices	Adapter	Туре	Status	Identifier	Targets	Devices	Paths		
ost Cache Configuration	Patsburg 4 port SATA IDE (Controller							
rotocol Endpoints	🚱 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 Details								
	Properties Devices P	aths Targets Net	work Port Bind	ding Advanced Options					
	-								
	Adapter Status							D	isable
	Status Enabled								-
	General								Edit
	Name vmh	ba33							_

Figure 7-32: Storage Adapters

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

Figure 7-33:Turn On vSphere HA

gaswCluster01 Actions -				E.
Summary Monitor Manage	Related Objects			
Settings Scheduled Tasks Ala	rm Definitions Tags Permissions Up	date Manager		
	vSphere HA is Turned ON			Edit
✓ Services	Runtime information for vSphere HA is r	eported under vSphere HA Monitoring		
v Sphere DR S	qaswCluster01 - Edit Cluster Set	tings	/ (•
vSphere HA Virtual SAN General	vSphere DRS vSphere HA	Turn on vSphere HA		
Disk Management Fault Domains & Stretched Cluster		ESX/ESXi hosts in this cluster exchan- might cause isolation responses.	ge network heartbeats. Disable this feature when performing network maintenance that	ork/disk
Health and Performance		Host Hardware Monitoring - VM Comp	onent Protection	
✓ Configuration General Liconsing		ESX/ESXI hosts have the capability to could deem them unusable (for exam Protect against Storage Connectivi	detect various failures that do not necessarily cause virtual machines to go down, but ple, losing network/disk communication) ty Loss	heartbeats
VMware EVC		Virtual Machine Monitoring		
VM/Host Groups VM/Host Rules		VM Monitoring restarts individual VMs restarts individual VMs if their in-guest Disabled	if their VMware Tools heartbeats are not received within a set time. Application Monitoring application heartbeats are not received within a set time.	
Host Options		Failure conditions and ∨M response	Expand for details	
Promes		 Admission Control 	Expand for details	Device
		 Datastore for Heartbeating 	Expand for details	Device
		 Advanced Options 	None	

Ensure that HA is activated on each cluster node:

Figure 7-34: Activate HA on each Cluster Node

10.3.180.211 Actio	ons 🔻						
Summary Monitor	Manage Rela	ted Objects					
In the second se	0.3.180.211 ype: bodel trocessor Type: ogical Processors: ICs: litual Machines: tate: ptime: ptime: ptime:	ESXi HP ProLiant DL360p Geni Intel(R) Xeon(R) CPU ES- 20 4 6 Connected 29 days	3 2680	v2 @ 2.80GHz			
▼ Hardware				 Configuration 			
Manufacturer	HP		11	ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759		
Model	ProLian	t DL360p Gen8		Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.	0.48	
CPU	10 C	PUs x 2.79 GHz		 vSphere HA State 	🥑 Running (Master)		1
Memory	70,63	39 MB / 98,269 MB		 Fault Tolerance (Legacy) 	Unsupported		
🕨 🔚 Virtual Flash Re	source 0.00	B/0.00 B		 Fault Tolerance 	Unsupported		
Metworking	localhos	st.corp.audiocodes.com		EVC Mode	Intel® "Sandy Bridge" Generation		
Storage	3 Datas	tore(s)		 Related Objects 			
 Tags 			1	Cluster 👔 qaswCluster	01		
Update Manager	Compliance				More F	Related Objects	

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

Figure 7-35: Networking

10.3.180.211 Actions -			<i>E</i> *
Summary Monitor Manage	Related Objects		
Settings Networking Storage	Alarm Definitions Tags Permissions	Scheduled Tasks Update Manager	
44	Virtual switches		
Virtual switches	3 G 🕸 🖻 / X O		
VMkernel adapters	Switch	Discovered issues	
Physical adapters	1 vSwitch0	-	
TCP/IP configuration			
Advanced			
	Standard switch: vSwitch0 (Managemen	nt Network)	
	/ X		C
		Management Network VLAN ID: V VMoemen Forts (1) wmid: 10.3 16021 VILAN ID: V/LAN ID: <	- - -

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):

many Monitor Manage	Related Ohie	orte										
manage	riterated exp	000										
ings Networking Storage	Alarm Defini	itions Tags Permissions	Scheduled Tas	iks Update Mar	nager							
	VMkernel ad	dapters										
/irtual switches	2 @	/ × 🖻-									Q Filter	
/Mkernel 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 Traf
Physical adapters ICP/IP configuration	💓 vmk0	Seal Management Network	vSwitch0	10.3.180.211	Default	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
dvanced												
	VMkernel n	work adapter: vmk0										
	All Pro	operties IP Settings Polic	cies									
	Port pror	partiae										
	Networ	k label	Management Ne	etwork								
	VLAN I	D	None (0)	_								
	Enable	d services	vMotion traffic									
			Management tra	affic								
	NIC setti	ings										
	MAC at	ddress .	28:80:23:af:e0:8	18								
	MIO		1500									

Figure 7-36: Switch Properties

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

Figure	7-37:	Protected	VM
--------	-------	-----------	----

Low-7.2.2055 Actions -						
etting Started Summary Mo	nitor Manage	Related Objects				
Powered On Launch Remote Console Download Remote Console	Low-7.4.268 Guest OS: Compatibility: E OMV are Tools: I DNS Name: DNS Name: IP Addresses: Host:	CentOS 4/5/6/7 (64-bit) SXI 5.0 and later (VM v Running, version:10246 //W are-low 0.3.180.201 //ew all 3 IP addresses 0.3.180.211	version 8) (Current)			
 VM Hardware 			▼ VM Sto	orage Policies		
 Advanced Configuration 			VM Storag	e Policies		
h Notos			VM Storag	e Policy Compliance		
r nules			Last Chec	ked Date		
 VM Failure Response 					Check Complia	ince
Failure	Failure respons	e				
Host failure	Restart		 Tags 			
Host network isolation	Leave powered	on	 Relate 	d Objects		
Datastore under PDL	Disabled		▼ vApp [Details		
Datastore under APD	Disabled		Product			
Guest not heartbeating	Ignore heartbea	s	Version			
vSphere HA Pro	tection: Protected	0	Vendor			
- Update Manager Compliand	ce	Protei	ted			
Status 😵 Non-Compliant		vSphere v	vill attempt to r	estart the VM after supp	orted failure.	
	Scan	Detailed Status				



Note: If you wish to manually migrate the OVOC VMs to another cluster node (refer to Appendix *Managing Clusters* in the *One Voice Operations Center IOM Manual*).

7.4.1.4.2 Cluster Host Node Failure

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



Note: 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 running OVOC process is dropped. The migration process may take several minutes.

7.4.2 Installing the OVOC Server on Microsoft Hyper-V Platform

This section describes how to install the OVOC server on the Microsoft Hyper-V Server 2012 R2 platform. This procedure takes approximately 30 minutes and predominantly depends on the hardware machine where the Microsoft Hyper-V platform is installed.



Note: The AudioCodes OVOC supports the Failover Clustering feature in Windows Server 2012 R2 (see Appendix *Managing Clusters* in the *One Voice Operations Center IOM Manual*).

The installation of the OVOC server on Microsoft Hyper-V includes the following procedures:

- Install the Virtual Machine (VM) (see Section 7.4.2.1).
- Configure the Virtual machine hardware settings (see Section 7.4.2.2).
- Change MAC Addresses from 'Dynamic' to 'Static' (see Section 7.4.2.3).
- Connect OVOC server to network (see Section 7.4.2.4).
- Configure VMs in a Microsoft Hyper-V cluster (see Section 7.4.2.5)

7.4.2.1 Installing the Microsoft Hyper-V Virtual Machine

The OVOC server is distributed as a VM image Zip file (see Section 7.1.2).

- > To install the OVOC server on Microsoft Hyper-V:
- 1. Extract the Zip file containing the OVOC server installation received from AudioCodes to a local directory on the Hyper-V server (see Appendix C for instructions on how to transfer files).



 Open Hyper-V Manager by clicking Start > Administrative Tools > Hyper-V Manager; the following screen opens:

100 m			Нур	er-V Manager				_ D X
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp								
🗢 🔿 🙍 🖬								
🏭 Hyper-V Manager								Actions
WIN-VO01RE7B70M	Virtual Machines				_			WIN-VO01RE7B70M
	Name	State	CPU Usage	Assigned Memory	Uptime 20.17-00	Status		New 🕨
		nunning	1/6	4120 MD	20.17.00			💫 Import Virtual Machine
								🖆 Hyper-V Settings
								🗱 Virtual Switch Manager
								🔬 Virtual SAN Manager
								💋 Edit Disk
							~	🔄 Inspect Disk
	Checkpoints						۲	Stop Service
			No virtua	al machine selected.				🗙 Remove Server
								🔉 Refresh
								View 🕨
								👔 Help
	Details							
			No	item selected.				
							Acti	ate Windows
							Go to	System in Control Panel to activa

Figure 7-38: Installing the OVOC server on Hyper-V – Hyper-V Manager

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

Figure 7-39: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard

1 M	Import Virtual Machine					
Before You Begin						
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	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.					
	< Previous Next > Einish Cancel					

4. Click Next; the Locate Folder screen opens:

i iguie / -+02. i	
	Import Virtual Machine
Locate Folde	r
Before You Begin	Specify the folder containing the virtual machine to import.
Locate Folder	Folder: C:\Export 115\cc test Browse
Select Virtual Machine	
Choose Import Type	
Summary	
	< Previous Next > Finish Cancel

Figure 7-402: Installing OVOC server on Hyper-V – Locate Folder

- 5. Enter the location of the VM installation folder, which was previously extracted, from the zip file as shown in the figure above, 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 7-413: Installing OVOC server on Hyper-V Choose Import Type

*	Import Virtual Machine				
Choose Import Type					
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	Choose the type of import to perform: Register the virtual machine in-place (use the existing unique ID) Restore the virtual machine (use the existing unique ID) © Copy the virtual machine (create a new unique ID)				
	< Previous Next > Einish Cancel				

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 7-424: Installing OVOC server on Hyper-V – Choose Destination
```

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

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

Figure 7-435: Installing OVOC server on Hyper-V – Choose Storage Folders

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

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 7-446: File Copy Progress Bar



This step may take approximately 30 minutes to complete.

11. Proceed to Section 7.4.2.2 on page 61.

7.4.2.2 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, refer to the *One Voice Operations Center IOM Manual*.

Table 7-2: Microsoft Hyper-V Virtual Machine Settings

Required Parameter	Value
Disk size	Fill-in-here
Memory size	Fill-in-here
CPU cores	Fill-in-here

> 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 7-45: Adjusting	VM for OVOC server –	Settings - Memory
------------------------	----------------------	-------------------

1	Settings for OC-QA on QAHYPERV1
OC-QA	✓ 4 ▶ Q.
 ★ Hardware ★ Add Hardware ★ BIOS Boot from CD ★ Memory 4096 MB ★ Processor 	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
6 Virtual processors ■ IDE Controller 0 ■ Hard Drive OCQA+IDA.vhd ■ IDE Controller 1 ● DVD Drive	You can manage the amount of memory assigned to this virtual machine dynamically within the specified range. Enable Dynamic Memory Minimum RAM: 512
None None None Network Adapter Virtual Switch 1 COM 1 None COM 2 COM 2	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 huffer: 20 - 26
None None Diskette Drive None None Management Name Occod	Memory weight Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer. Low High
Checkpoint File Location C:\ClusterStorage\Volume1\0C Smart Paging File Location C:\ClusterStorage\Volume1\0C	③ Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.
Automatic Start Action None Automatic Stop Action	✓ OK Cancel Apply

- 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.

😰 Se	ttings for OC_QA_High on QAHYPERV1
OC_QA_High	✓ ▲ ▶ Q.
 ★ Hardware ★ Add Hardware ▲ BIOS Boot from CD ➡ Memory 20000 MB ➡ Processor 6 Virtual processors ➡ IDE Controller 0 ➡ Hard Drive OC_QA_High.vhdx ➡ IDE Controller 1 ▲ DVD Drive None SCSI Controller ➡ Network Adapter Virtual Switch 1 	▲ Processor You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings. Number of virtual processors: 6 ♦ Resource control You can use resource controls to balance resources among virtual machines. Virtual machine reserve (percentage): 100 Percent of total system resources: 37 Virtual machine limit (percentage): 100 Percent of total system resources: 37 Relative weight: 100
 COM 1 None COM 2 None Diskette Drive None Management Name OC_QA_High Integration Services Some services offered Checkpoint File Location C:\ClusterStorage\volume1\OC Smart Paging File Location C:\ClusterStorage\volume1\OC Smart Paging File Location C:\ClusterStorage\volume1\OC Automatic Start Action None 	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.
	QK <u>C</u> ancel Apply

Figure 7-46: Adjusting VM for OVOC Server - Settings - Processor

- 4. Set the 'Number of virtual processors' parameters as required.
- 5. Set the 'Virtual machine reserve (percentage)' parameter to **100%**, and then click **Apply**.

Note:

- 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 (see Section 7.4.2.5).

7.4.2.2.1 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 7-47: Expanding Disk Capacity

1 <u>23</u>	Se	ettings for OC_test-new on QAHYPERV1
OC_test-new	~	
 ★ Hardware ★ Add Hardware ▲ BIOS Boot from CD ➡ BHOS Boot from CD ➡ Memory 4096 MB ➡ Processor 1 Virtual processor ■ IDE Controller 0 ♥ ▲ Hard Drive OC_test.vhdx ➡ IDE Controller 1 ▲ DVD Drive None ♥ SCSI Controller ➡ SCSI Controller ➡ Network Adapter Virtual Switch 1 Hardware Acceleration Advanced Features ♥ COM 1 		 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: Location: IDE Controller 0 (in use) (in use) (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. (in virtual hard disk: (:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\OC_test.vhdx New Edit Inspect Browse 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.
COM 2 None Diskette Drive None Management Name OC_test-new Minegration Services Some services offered Checkpoint File Location C:\ProgramData\Microsoft\Win Smart Paging File Location C:\ProgramData\Microsoft\Win	~	To remove the virtual hard disk, dick Remove. This disconnects the disk but does not delete the associated file.
		OK Cancel Apply

The Edit Virtual Disk Wizard is displayed as shown below.

Figure 7-48: Edit Virtual Hard Disk Wizard

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

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

Figure 7-49: Edit Virtual Hard Disk Wizard-Choose Action

💋 Edit Virtual Hard Disk Wizard 🛃				
Choose Actio	on			
Before You Begin Locate Disk Choose Action Configure Disk Summary	 What do you want to do to the virtual hard disk? Compact This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard or 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. 	disk ew		
	< Previous Next > Finish Cancel			

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

Figure 7-50: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk

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

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

Figure 7-51: Edit Virtual Hard Disk Wizard-Completion

ø	Edit Virtual Hard Disk Wizard
Completing t	the Edit Virtual Hard Disk Wizard
Before You Begin Locate Disk Choose Action Configure Disk	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)
Summary	Action: Expand Configuration: New virtual disk size: 300 GB
	To complete the action and dose the wizard, dick 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.

7.4.2.3 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 (refer to the One Voice Operations Center IOM Manual).
- 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 7-52: Advanced Features - Network Adapter – Static MAC Address



7.4.2.4 Connecting OVOC Server to Network

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**.

Virtual Machines					
Name	State	CPU	Usage	Assigned Memory	l
Stress_tool SSBC_AlexR3_HA1 SSBC_AlexR2_HA2 SSBC_AlexR2_HA1	Running Off Off Off	0 %		2048 MB	1
ESBC_alexr1	Running	0 %		2048 MB	1
OC-QA OC_QA_High	Off Running		Connect Settings		1
			Start Checkpoi	nt	
<	III	_	Move		

Figure 7-53: Power On Virtual Machine

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

Figure 7-54: Connect to OVOC Server Console

Virtual Machines				
Name	State	CPU Usage	Assigned Memory	Uptime
Stress_tool SSBC_AlexR3_HA1 SSBC_AlexR2_HA2 SSBC_AlexR2_HA1 ESBC_alexr1	Running Off Off Off Bunning	0%	2048 MB	1.04:34:22
OC-QA	Off		2010110	
CC_QA_High	Running	Connect		1.02:37:53
		Settings		
<		Turn Off		
		Shut Down		

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

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

su - root

5. Type the following command:

EmsServerManager

- 6. If you are migrating on a single machine and your deployment includes phones:
 - From the Application Maintenance > Web Servers menu, close ports **8081** and **8082**.
- 7. From the Network Configuration > Server IP Address menu, set the OVOC server network IP address.
- 8. Perform other configuration actions as required using the EMS Server Manager (refer to Chapter 8).

7.4.2.5 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.

7.4.2.5.1 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.

4		Faile	over Cluster Manag	ger	
<u>File</u> <u>Action</u> <u>View</u> <u>Help</u>	p				
Failover Cluster Manage	Nodes (2) Search			P	Queries 🔻 🕁 👻
Nodes	Name	Status	Assigned Vote	Current Vote	Information
⊿ 📇 Storage	R QAHyperV1	🛞 Up	1	1	
Disks Pools Networks	QAHyperv2	 Φ 	1	1	
	<	ш			>
	•				
< III >					

Figure 7-55: Hyper-V-Failover Cluster Manager Nodes

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

7.4.2.5.2 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 7-56: Configure Role

6			Failover Clu	ster Manager		
ile <u>A</u> ction <u>V</u> i	iew <u>H</u> elp					
• 🔿 🙍 📰	? 🗊					
Eailover Cluste	er Managel Balan (2)					
A CAHyperv	-Cl.corp.a					P Queries 👻 🛃 💌
Noc	Configure Role	Status	Туре	Owner Node	Priority	Information
🔺 🔜 Stor	Virtual Machines +	(1) Running	Virtual Machine	QAHyperV1	Medium	
8	Create Empty Role	Running	Virtual Machine	QAHyperv2	Medium	
Net Net	View +					
i Clus	Refresh					
	2 million (2					

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

Figure 7-57: Choose Virtual Machine

Eile Action View Help Image: Select Role Imag	
Image: Select Role	
Roles (2) Soles (2) Soles (2) Soles (2) Name Name Status Type Owner Node Piols Pools Networks Cluster Events Before You Begin Select Role Select Role Select Hole Select Witual Machine Confirmation	
Roles Pools Name Status Type Owner Node Pools High Availability Wizard Networks Select Role Cluster Events Select Role Before You Begin Select the role that you want to configure for high availability. Select Role Select Role Before You Begin Select the role that you want to configure for high availability. Select Role Select Role Configuration A vitual machine is a vitualized	
Storage Disks Pools Disks Pools Retworks Select Role Before You Begin Select the role that you want to configure for high availability. Select Role Select Witual Machine Configuration	••
Pools Pools Networks Cluster Events Before You Begin Select Role Select the role that you want to configure for high availability. Select Role Select Witual Machine Select Vitual Machine Configure for high availability. A vitual machine is a vitualized	
Before You Begin Select the role that you want to configure for high availability. Select Role Select Vitual Machine Confirmation Image: Provide and Provide a	
Constitution Constitution Availability Summary Constitution Constit	y node
< III >> Cancel	~

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

· 唱			Failover C	luster Manag	ger		
<u>File Action View Help</u>)				-		
 Failover Cluster Manage QAHyperv-Cl.corp.a Roles Nodes Storage Disks Pools Networks Cluster Events 	Roles (2) Search Name	Status tual Machine	Type High Availa	Owner N ability Wizard	ode Pr	iority Ir	♀ Queries ▼ formation
	Before You Begin Select Role Confirmation Configure High Availability Summary	Select the virtual ma	achine(s) that you wa	nnt to configure fo Status Off	r high availability Host Server QAHyperV1.	corp.audiocode	es.com
		Shutdown S	ave				<u>Refresh</u>
<				[< <u>P</u> revious	<u>N</u> ext >	Cancel

Figure 7-58: Confirm Virtual Machine

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

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

Figure 7-59: Virtual Machine Successfully Added

8 7	High Availability Wizard	x
Summary		
Before You Begin Select Role	High availability was successfully configured for the role.	
Select Virtual Machine Confirmation	Virtual Machine	^
Configure High Availability	All of the virtual machine configurations chosen were successfully made highly	
Summary	available.	
	OC Success	
		~
	To view the report created by the wizard, click View Report. <u>View Report</u> To close this wizard, click Finish.	t
	<u> </u>	h

4. Click **Finish** to confirm your choice.

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



Note: If you wish to manually move the OVOC VMs to another cluster node, refer to Appendix *One Voice Operations Center IOM Manual*.

7.4.2.5.3 Cluster Host Node Failure

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



Note: 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.
8 Configure One Voice Operations Center Server

This chapter describes how to mirror the One Voice Operations Center server configuration with the Version 7.2 EMS & SEM configuration using the EMS Server Manager utility.

Note

- When working with One Voice Operations Center 7.4 Version, you should login as System Admin operator. Navigation to menu items are identical on the Version 7.2 platform to the Version 7.4 platform, unless indicated otherwise.
- The EMS Server management configuration is not backed up to the Version 7.4 platform. Therefore you must manually capture all actions performed using the EMS Server Manager on the Version 7.2 platform and replicate these actions on the Version 7.4 platform.

8.1.1 Connecting to the EMS Server Manager

You can either run the EMS Server Manager utility 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 Server Manager Configuration includes the following menu items (that are relevant to the Migration process):

- General Info (see Section 8.1.2)
- Web server and Web port configuration (see Section 8.1.3)
- Change Schedule Backup Time (see Section 8.1.4)
- All network configuration (see Section 8.1.5)
- NTP or date configuration (see Section 8.1.6)
- Security configuration (see Section 8.1.7)



Note General info can be used as a generic summary. Review all options and apply the non-default configuration to the new machine. You can use the checklist in Chapter 4 to assist you in this task.

8.1.2 General Information

1. From the One Voice Operations Center Server Management root menu, choose **General Information**, and then press Enter; the following is displayed:.

Figure 8-1: General Information

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
Collecting information
Machine information
Environment: Virtual(Manufacturer: VMware, Inc.)
Product Name: VMware Virtual Platform
<pre>(CPU: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz, total cores: 1</pre>
Memory: 7982 MB
Network:
Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)
ACEMS Usage: 1.2G
Disk:
Disk /dev/sda: 182.5 GB, 182536110080 bytes
Data usage:
/dev/mapper/vg-data 76G 22G 51G 30% /data
Versions
EMS Version : 7.2.3075
OS Version : Linux 2.6.18-409.el5 x86 64
OS Revision : CentOS 5 for EMS Server Virtualized (Rev. 8)
Java Version : java full version "1.8.0 111-b14"
Apache version: Apache/2.2.3 Server built: Sep 16 2014 11:05:09
Server's NAT : Not configured
Server's Certificate : Default
<more></more>

- **2.** Collect the following information:
 - Server NAT
 - Server Certificate
 - Network Configuration
 - Time & Date
 - NTP

8.1.3 Web Server Configuration

1. From the Application maintenance menu, choose **Web Servers**, and then press Enter; the following is displayed:

Figure 8-2: Web Server Processes Status



- 2. Collect the current state information regarding the following ports:
 - Port 80
 - Port 8080
 - Port 8081
 - Port 8082
 - JAWS service (not relevant in Version 7.4)
 - JAW IP Configuration (not relevant in Version 7.4)
- 3. Configure the above states on the Version 7.4 platform.

8.1.4 Schedule Backup Time

1. From the Application Maintenance menu, choose **Change Schedule Backup Time**.

Figure 8-3: Schedule Backup Time Configuration



- 2. Note the current schedule backup day & time.
- **3.** On the Version 7.4 server, update this time accordingly. If the backup time is different from the default (Saturday at 2 AM) then update it.

8.1.5 Network Configuration

From the One Voice Operations Center Server Manager root menu, choose Network Configuration; the following is displayed:

Figure 8-4: Network Configuration



8.1.5.1 Ethernet Interfaces

1. From the Network Configuration menu, choose **Ethernet Interfaces**, and then press Enter; the following is displayed:

Figure 8-5: 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. Add or remove the same interfaces on the Version 7.4 platform.

8.1.5.2 Ethernet Redundancy

1. From the Network Configuration menu, choose **Ethernet Redundancy**, and then press Enter; the following is displayed:

Figure 8-6: Ethernet Redundancy



2. Configure interfaces redundancy for the Version 7.4 platform.

8.1.5.3 DNS Client

1. From the Network Configuration menu, choose **DNS Client**, press Enter, and then in the sub-menu, choose **Configure DNS**; the following is displayed:

Figure 8-7: DNS Configuration



2. Configure DNS client for the Version 7.4 platform.

8.1.5.4 NAT

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

Figure 8-8: NAT Configuration



2. Configure the NAT IP for the Version 7.4 platform.

8.1.5.5 Static Routes

1. From the Network Configuration menu, choose Static Routes, and then press Enter; the Static Routes Configuration is displayed:

Figure 8	3-9:	Static	Route	Configuration
----------	------	--------	-------	---------------

Main Menu> Net	work Configurat:	ion> Static Route	25			
Static	Routes Configura	ation				
Kernel IP routi	ing table					
Destination	Gateway	Genmask	Flags	MSS Window	irtt	Iface
172.17.118.0	0.0.0.0	255.255.255.0	U	0 0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0 0	0	eth0
0.0.0.0	172.17.118.1	0.0.0.0	UG	0 0	0	eth0
>1.Add	Static Route					
2.Remo	ove Static Route					
b.Back						
q.Quit	; to main Menu					

2. Configure static routes for the Version 7.4 platform according to the new network subnets.

8.1.5.6 SNMP Agent

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

Figure 8-10: Configure 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

2. Note the NMS IP and community string.

Figure 8-11: NMS IP and Community String

Configure SNMP Agent
NMS IP : 10.1.1.1
Community string : public

3. On the Version 7.4 platform, from the Network Configuration menu, choose **SNMP** Agent, and then press Enter.



Figure 8-12: SNMP Agent

4. Choose option 1.

Figure 8-13: Configure SNMP Agent



- 5. Choose option 2 Linux Traps Forwarding Configuration.
- 6. Configure the NMS IP and community string parameters from the Version 7.2 platform on the Version 7.4 platform.

8.1.5.6.1 SNMPv3 Engine ID

If you changed the SNMPv3 Engine ID on the Version 7.2 platform and wish to use the same ID then on the Version 7.4 platform then perform the procedure below.

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



```
SNMPv3 Engine ID Configuration
Server's SNMPv3 Engine ID (0 in all values return to default configuration)
Byte[0] (valid range -128 .. 127):
```

2. Choose option 3 SNMPv3 Engine ID and change accordingly.

8.1.6 Date and Time Menu

 From the One Voice Operations Center Server Management root menu, choose Date & Time, and then press Enter; the following is displayed:

Figure 8-15: Date and Time

EMS Server 7.2.3	8075 Management
Main Menu> Date & Time	
>1.NTP 2.Timezone Settings 3.Date & Time Settings q.Quit to main Menu	(Apache Server will be restarted)

2. Update the same NTP, time zone and current date on the Version 7.4 platform.

8.1.7 Security

1. From the One Voice Operations Center Server Manager root menu, choose **Security**, and then press Enter, the following is displayed:

Figure 8-16: Security



8.1.7.1 SSH

1. From the Security menu, choose **SSH**; the following is displayed:



2. Configure identically on the Version 7.4 platform.

8.1.7.2 DB Password

1. From the Security menu, choose **DB Password**, and then press enter.

Figure 8-18: One Voice Operations Center Server Manager – Change DB Password



2. Configure an identical DB Password on the 7.4 platform (default is "pass_1234).

8.1.7.3 OS Password

- 1. From the Security menu, choose **OS Users Passwords**, and then press Enter.
- 2. Configure an identical password on the Version 7.4 platform.

8.1.7.4 File Integrity Checker

- 1. From the Security menu, choose **File Integrity Checker**, and then press Enter.
- 2. Configure identically on the Version 7.4 platform.

8.1.7.5 Software Integrity Checker

- 1. From the Security menu, choose **Software Integrity Checker (AIDE) and Pre-linking**; the current status of these two processes is displayed.
- 2. Configure identically on the Version 7.4 platform.

8.1.7.6 USB Storage

- 1. From the Security menu, choose **USB Storage**.
- 2. Configure identically on the Version 7.4 platform.

8.1.7.7 Network Options

1. From the Security menu, choose **Network Options**; the following screen is displayed.

Figure 8-19: Network Options



2. Configure identically on the Version 7.4 platform.

8.1.7.8 Audit Agent Options

- 1. From the Security menu, choose Auditd Options.
- 2. Configure identically on the Version 7.4 platform.

8.1.7.9 HTTPS Authentication

1. In the Security menu, choose the **HTTPS Authentication** option

	Figure 6-20: HTTPS Authentication
Main	Menu> Security> HTTPS Authentication
HTTPS	Authentication: One-Way
	>1.Set Mutual Authentication
	2.Set One-Way Authentication
	b.Back
	q.Quit to main Menu

Figure 8-20: HTTPS Authentication

2. Configure identically on the Version 7.4 platform.

8.1.7.10 Enable/Disable SEM client Secured Communication

- 1. From the Security menu, choose **Enable SEM client secured connection**.
- 2. Configure identically on the Version 7.4 platform.

8.1.8 Enable IP Phone Management Server Client

- 1. From the Security menu, choose **IP Phone Manager client secured communication**.
- 2. Configure identically on the Version 7.4 platform (note JAWS is not applicable to the Version 7.4 platform).

8.1.8.1 SEM - AudioCodes Devices Communication

1. From the Security menu, select **SEM – AudioCodes device communication**.

Figure	8-21:	SEM-A	udioCodes	Device	Communication
i igui o	~		441000400	001100	oominumoution

Main	Menu>	Secur	ity>	SEM -	Audio	Codes	device	es co	ommuni	ication	
SEM -	Audio	odes	devi	ces co	mmuni	catior	: TCP				
	>1.	CP	SEM 3					d)			
	2.1	ILS (SEM :								
	3.1	LS/TC	;P	(SE		ver wi		resta			
	b.E	Back									
	q.()uit t	o ma:	in Men	a						

2. Configure identically on the Version 7.4 platform.

8.1.9 Diagnostics

1. From the One Voice Operations Center Server Manager Root menu, choose **Diagnostics**, and then press Enter, the following is displayed:

Figure 8-22: Diagnostics

Main Menu> Diagnostics	
>1.Server Syslog 2.Devices Syslog 3.Devices Debug q.Quit to main Menu	(The server may be rebooted)

2. Configure identically on Version 7.4 platform.



This page is intentionally left blank.

9 Import the Topology and Configuration

This chapter describes how to import the EMS Topology and the IP Phone Management server configuration to the Version 7.4 platform.

Note:

• The import process creates tenants based on the existing region names and also creates a region under each tenant with the same name. Consequently you should customize your site tenant and region definitions following the import process.



- If your phones are deployed in a non-Skype for Business environment, you should import both phones and users. If your phones are deployed in a Skype for Business Environment, you should only import phones.
- If you have configured SNMP Trusted Managers on devices and you wish these devices to be automatically added to OVOC, then the Trusted Manager IP address should be the IP address of the OVOC server. If a device is configured with a Trusted Manager IP address that is not the OVOC server IP address, then such devices must be added manually to OVOC.

9.1 Import EMS Topology

The topology import procedure takes the topology.xml file created during the topology export process (see Chapter 5) and imports all topology entities to the new One Voice Operations Center 7.4 released server.

> To import the EMS topology:

1. Login to the Version 7.4 platform Login as 'root' user with password *root* (default password is root):

su - root

2. Change Directory to /home/acems:

cd /home/acems

- **3.** Copy the exported topology output files topology.xml and keystore.jks to this directory.
- 4. Change Directory to ACEMS/server_7.4.XXX: cd /ACEMS/server_7.4.XXX
- **5.** Execute topologyImport.pl (this process stops the One Voice Operations Center server application):

```
./topologyImport.pl
```

- 6. Approve/Decline the copy of keystore.jks file, which overrides the current /opt/ssl/keystore.jks (the current file will be backed up before the copy is executed).
- 7. Copy **ssl.crt** and **ssl.key** to **/etc/httpd/conf.d** (backed up in Export procedure in Section 5.1).
- 8. If you manually updated /etc/httpd/ssl.conf on the Version 7.2 platform, using an editor tool, update this file with the following values according to your Version 7.2 configuration:
 - SSLProtocol
 - SSLCipherSuite.
 - SSLCertificateFile.
 - SSLCertificateKeyFile .

SSLCACertificateFile



Warning: Do not directly overwrite the Version 7.2 **/etc/httpd/ssl.conf** file to the Version 7.4 platform.

9. Restart the One Voice Operations Center server application using EMS Server Manager.

9.1.1 Example Output

```
Topology file processed entities:
Importing topology entities:
07 Jun 2017 13:35:43:632 Start SNMP Handler
07 Jun 2017 13:35:43:660 Start entity manager initialization
07 Jun 2017 13:35:45:764 Entity manager initialization completed
07 Jun 2017 13:35:45:824 isVQM:false *** current
dir:/opt/ACEMS/server 7.4.223 mibsRoot: externals/mibs/
07 Jun 2017 13:35:45:824 Loading mibs for Refresh. Allocating 100
threads 07 Jun 2017 13:35:46:856 Loading mibs for unknown machine.
Allocating 10 threads .....
07 Jun 2017 13:35:46:857 Loading mibs for MP machine
07 Jun 2017 13:35:46:857 Loading mibs for MP v6.6 machine.
07 Jun 2017 13:35:49:270 Loading mibs for MP v6.8 machine.
07 Jun 2017 13:35:51:424 Loading mibs for MP v7.0 machine.
Loading mibs for MP v7.2 machine.
Loading mibs for MP v7.2.100 machine.
Loading mibs for MP v7.4 machine.
07 Jun 2017 13:35:58:245 All mibs loaded successfully.
07 Jun 2017 13:35:58:245 Finish SNMP Handler
07 Jun 2017 13:36:10:182 Alert Rule profile Added
07 Jun 2017 13:36:10:249 Quality Threshold profile Added
07 Jun 2017 13:36:10:251 Quality Threshold profile Added
07 Jun 2017 13:36:10:328 Quality Threshold profile Added
07 Jun 2017 13:36:10:329 new tenant was Inserted
07 Jun 2017 13:36:10:352 new tenant was added
07 Jun 2017 13:36:10:665 Alert Rule profile Added
07 Jun 2017 13:36:10:674 Quality Threshold profile Added
07 Jun 2017 13:36:10:677 Quality Threshold profile Added
07 Jun 2017 13:36:10:690 Quality Threshold profile Added
```

```
07 Jun 2017 13:36:10:690 new tenant was Inserted
07 Jun 2017 13:36:10:700 new tenant was added
07 Jun 2017 13:36:10:885 Alert Rule profile Added
07 Jun 2017 13:36:10:894 Ouality Threshold profile Added
07 Jun 2017 13:36:10:896 Quality Threshold profile Added
07 Jun 2017 13:36:10:904 Quality Threshold profile Added
07 Jun 2017 13:36:10:904 new tenant was Inserted
07 Jun 2017 13:36:10:911 new tenant was added
07 Jun 2017 13:36:11:005 Alert Rule profile Added
07 Jun 2017 13:36:11:011 Quality Threshold profile Added
07 Jun 2017 13:36:11:013 Quality Threshold profile Added
07 Jun 2017 13:36:11:019 Quality Threshold profile Added
07 Jun 2017 13:36:11:020 new tenant was Inserted
07 Jun 2017 13:36:11:031 new tenant was added
regions added: 4/4 : 100%
.....Failed to add node ID:257 Message:null
Failed to add node ID:254 Message: Cannot add node with serial
number 5867475.
This serial number already exists.
nodes added: 11/13 : 85%
non acl nodes added: 3/3 : 100%
links added: 2/2 :100%
features added: 0/0 :100%
Are you sure that you want to override /opt/ssl/keystore.jks?
(y/n) y
Please restart One Voice Operations Center application using
EMSServerManager!
```

Refer to the "entity type" summary (regions, devices, etc ...) to verify that all the entities are added to the new One Voice Operations Center. In case of failures, approach AudioCodes support team.

9.2 Import IP Phone Management Server Configuration and Users & Devices

The configuration import procedure takes the IP Phone configuration file created during configuration export process (see Section 5.1) and imports all topology entities into the new One Voice Operations Center 7.4 released server:

- > To import IP Phone Management Server Configuration and Users & Devices:
- 1. Login to IP Phone Management server Version 7.4 Web client.
- 2. Open the Import Configuration page (Setup tab > Import/Export > Import Configuration).



One Voice Operation Center	= SETUP MONITOR TROUBLESHOOT 🤨 IPP Manager Server 🖉 \shay+	0
VC IPP MANAGER SERVER		
Vuers & Devices Phones Configuration Import Configuration Export Configuration Import Certification Import Users & Devices Export Users & Devices System E	 Import Phone Configuration Files: Citck the Browse(Choose File button and select the import *.zip file from your file system. Citck the Import button. The file is imported into the IP Phone Management Server The server import Sata of Tematar's regions, Sites, Templates, System Settings, Template Placeholders, Tenant Placeholders, Site Placeholders, Phone Firmware Files. The import result will be displayed as tables of the imported configurations. Mote: Importing a large file can take a few seconds or minutes. Please be patient and wait until the operation has successfully been finished. Import from file: 	

- 3. Import the configuration file that you downloaded in Section 5.2.
- Open the Import Users & Devices page (Setup tab > Import/Export > Import Users & Devices).

Figure 9-2: Import Users and Devices

MudioCodes One Voice Operation Center ≡	SETUP MONITOR TROUBLESHOOT 🥸 IPP Manager Server	ß	\shay -	0
C IPP MANAGER SERVER				
Users & Devices Manage Users Manage Multiple Users Manage Multiple Devices Phones Configuration Import / Export	Import Users and Devices information This page lets you import a CSV file containing users and devices information into the server. Browse to the file and then click the import button.			
Import Configuration Export Configuration Export Users & Devices Export Users & Devices	MURISCUE TO THE SETELLED.			J

5. Import the Users file that you downloaded in Section 5.2.

6. If you are migrating on a single machine:

- a. Type the following command: # EmsServerManager
- From the Application Maintenance > Web Servers menu, close ports 8081 and 8082.

The phones will restart when they receive their new configuration files.



This page is intentionally left blank.

10 Move Phones from Version 7.2 Platform

This chapter describes how to move phones from the Version 7.2 platform to the Version 7.4 platform. This procedure describes how to create a template file for moving phones that are currently deployed in a region in the Version 7.2 platform to a corresponding new tenant in the Version 7.4 platform. You need to create a separate template file for each defined region.

Note:

- This procedure is only relevant when the migration process is implemented with dual machine topology (both servers must be connected to the network).
- Move phones one region at a time; each region will be moved to a tenant with the same name as the region.
- For new phones that will be added directly on the Version 7.4 platform: update the DHCP option 160 to use the new IP address of the OVOC server.

Perform the following procedure for each region:

- 1. In the Navigation tree, select Phones Configuration > Templates.
- 2. In the IP Phones Configuration Templates page, click the Generate Global Configuration Template button.
- 3. Create a new template MOVE_TO_OVOC_<YOUR_REGION_NAME>.

A HD Second to 8			- 1	
	Navigation Tree		_	\odot
	Dashboard	+		
	Regions	+		
	Users	+		
	Phones Configuration			
	Templates			
	System Settings			
	Default Placeholders Value	es		
	Templates Placeholders			
	Region Placeholders			
	Devices Placeholders			
	Phone Configuration Files			
	Phone Firmware Files			
	License	+		
	Custom Disconstine			

Figure 10-1: Navigation Tree - Templates

- 4. Click the Edit configuration template button; the template opens in an integral editor:
- 5. Edit the template MOVE TO OVOC <YOUR REGION NAME> data to change the IP

```
address and <YOUR REGION NAME>):
<?xml Version="1.0" encoding="ISO-8859-1"?>
<ipphonetamplate>
                <type>audiocodes 440HD</type>
                <description >AudioCodes 440HD
LYNC</description>
                <file config>
                                 <type>global file</type>
                                 <profile>global</profile>
                                 <encrypt mode>0</encrypt mode>
                                 <name>Audiocodes 440HD global
LYNC.cfg</name>
                                 <destinationDir>%ITCS destinat
ion%</destinationDir>
                                 <data>
<! [CDATA]
11>
                                 </data>
                </file config>
                <file config>
                                 <type>file</type>
                                 <profile>user</profile>
                                 <encrypt mode>0</encrypt mode>
                                 <name>%ITCS mac%.cfg</name>
                                 <destinationDir>%ITCS destinat
ion%</destinationDir>
<data><![CDATA[
provisioning/configuration/url=http://X.X.X.X/ipp/dhcpoption16
0.cfg
11>
</data>
                </file_config>
</ipphonetamplate>
  If you want the devices to enter a specific tenant change
the row in the template from:
provisioning/configuration/url=http://X.X.X.X/ipp/dhcpoption16
0.cfg
to:
provisioning/configuration/url=http:// X.X.X.X/ipp/tenant/<
REGION NAME>
   Apply the template to the desired devices: Users->Manage
Multiple Devices. Action: change template and choose:
"MOVE TO OVOC <REGION NAME>"
```

6. Click **Save**; the modified template is saved in its URL location on the server, for example:

http://10.59.0.200/ipp/tenant/< REGION_NAME>/admin/AudioCodes.php.

In the IP Phones Configuration Templates page, the name of an edited template is displayed in green.



This page is intentionally left blank.

11 Configure One Voice Operations Center Web Client

This chapter describes how to migrate the Version 7.2.3000 EMS client configuration to the Version 7.4 OVOC Web client configuration.

11.1 Local User Authentication

To move operators to the new Version 7.4 platform, manually copy all previously defined Operators on the Version 7.2 platform (EMS Main Menu: Security > Users List).

View Tools	Faults Security H	lelp				
ree	Users List	ada lafa	A 👼 A . A .	* • · ·	Cloba	x
Globe	File View Acti	ons Help				S
ACL-Holl	ሴ 💩 💐 🖢	i 🚯 🚹 🖉				
III PPC	Basic Info	Regions Info				
ACL-US	User Name	Security Level	Login Type	Full Name	Status	Valid II
	demo3	Monitoring	User/Password Lo		NOTACTIVE	4
	demo4	Monitoring	User/Password Lo		NOT ACTIVE	
OVR	demo5	Monitoring	User/Password Lo		NOT ACTIVE	
MSMarina	demo6	Monitoring	User/Password Lo		NOT ACTIVE	
Marketing	kast	Administration	User/Password Lo		NOT ACTIVE	
RD-Solut	operator11	Operation	User/Password Lo		NOT ACTIVE	
Dperation	hadarv	Administration	User/Password Lo		NOT ACTIVE	
RND-CB	shai	Administration	User/Password Lo		NOTACTIVE	
Training	glmaks	Administration	User/Password Lo		NOTACTIVE	
DHCPRE	operator5	Operation	User/Password Lo		NOT ACTIVE	
France	-	Administration	Hoor/Boooword Lo		NOT ACTIVE	7 Þ 3
					ОК	Close

Figure 11-1: Users List

If for specific Operators, security levels were defined for specific Regions, then the security levels should now be configured per Tenant Operator on the Version 7.4 platform:

File View	Actions Help		
🗄 🙆 🍯	V 늖 🚯 👍 🧹		
Basic Int	fo Regions Info		
User Name	Security Level	Login Type	Full Name
demo3	User Details		×
demo4	Basic Info Advanced Info	Regions Info	
demo5			
demo6			5
kast	Set All Regions	Select	
operator:	Region	Security Level	
hadarv	ACL-Hona-Kona	Not Visible	
shai			
glmaks	ACL-Israel	Monitoring	
operator:	ACL-US	Monitoring 🔹 💌	
-	AutoDetection	Not Visible 💌	
	Demo	Monitoring	
	DHCPREGION	Monitoring	
	•		7 F
		ОК	Cancel
l			

Figure 11-2: User Details

Open the Operators screen on the Version 7.4 platform (System tab > Administration > Security > Operators) to adopt the user security levels to the new multi-tenancy definitions. For more information, refer to the One Voice Operations Center User's Manual.



ATORS		ACTIONS C Delete					
ADMINISTRATION <<	LOGIN NAME	OPERATOR TYPE	SECURITY LEVEL	STATUS	LAST SUCC	>> OPERATORS SUMMARY	
ENSE	acladmin	System	ADMIN	NOT ACTIVE	26-jul-17 1 *	OPERATORS STATUS	
	dev	System	ADMIN	NOT ACTIVE	02-Jul-17 1		Active
CURITY	amil	System	ADMIN	NOT ACTIVE	23-Jul-17 1		(1, 10.00 9
Authentication	orenp	System	ADMIN	NOT ACTIVE	25-Jul-17 1		
Operators	shay	System	ADMIN	NOT ACTIVE	17-Jul-17 1		
	ran	System	ADMIN	NOT ACTIVE	10-Jul-17 1		
	alan	System	ADMIN	NOT ACTIVE		Not Active	
	brad	System	ADMIN	NOT ACTIVE		(3, 50.00 /e)	
	mike	System	ADMIN	NOT ACTIVE		SECURITY LEVEL	
	Brad	System	ADMIN	ACTIVE	26-Jul-17 1		
						C	Admii (10, 100.00

SETTINGS TASKS			
OPERATORS	🗢 Add 🔻 🥒 Edit	📦 Actions 🕶 📋 Delete	
SETTING NAVIGATION	PERATOR SETTINGS		×
LICENSE	BASIC INFO	ADVANCED INFO	
STORAGE	Assigned Tenants:	^	·
SECURITY			
Authentication		defaultTenant	
Operators		newTenant	1
▶ TEMPLATES		DefaultTenant	
ALARMS		testTenant	
		myTenant	
FILE MANAGER		device_tenant	
EXTERNAL APPLICATIONS		GenaTenant	
DEVICE BACKUP		newDefaultTenant	
		Type to search Select	Cancel
		OK Cancel	

Figure 11-4: Tenant Operator Settings

11.2 External Authentication Servers

If EMS is defined to work with external Authentication servers, save the Authentication Servers configuration.



Note: TACACS server is not supported in Version 7.4.

11.2.1 RADIUS

- 1. Open the Authentication and Authorization Settings on the Version 7.2 platform (open the EMS menu: Security > Authentication & Authorization).
- 2. From the drop-down list, select **RADIUS Authentication**.

AudioCodes' EMS - gena is logged with Administration authorizatio	n to server 10.1.8.23.(Last login time:20)	16-05-26 18:06:21)		
File View Tools Faults Security Help				
Authentication & Authorization Settings				
		👔 land	e SEM	IP Ph
Authentication Type	RADIUS Authentication			1 E
	EMS Authentication		_	l l l l
Synchronizing M5K/M8K CLI with EMS Users	RADIUS Authentication			
DADUIS Authentication	TACACS+ Authentication			
RADIOS Autrenucation	LDAP Authentication			
			Others	Total
User Login Type (User/Password or CAC)	User/Password Login		(@Connected)	2
Current Active Radius Server	1) (0 Connected)	7
Guilent Adults Certer	*		(0 Connected)	0
1st RADIUS enabled	\checkmark		(0 Connected)	5
			(0 Connected)	5
1st RADIUS Auth Server IP	1.1.1.1		0 (0 Connected)	3
1st RADIUS Auth Server Port	1812		0 (0 Connected)	0
			0 (0 Connected)	0
1st RADIUS Auth Server Secret	abc123		(1 Connected)	1
and RADIUS enabled			(1 Connected)	1
			(u connected)	U
2nd RADIUS Auth Server IP	2.2.2.2) (0 Connected)	0
		((0 Connected)	0

Figure 11-5: RADIUS Configuration

- **3.** Open the Authentication screen on the Version 7.4 platform (System tab > Administration > Security > Authentication).
- 4. From the drop-down list, select **RADIUS**.

NISTRATION CONFIGURATI	ON TASKS				
IENTICATION					
ADMINISTRATION <	Authentication Type RADIUS	¥			
ICENSE	RADIUS AUTHENTICATION SE	TTINGS			
ECURITY	RADIUS retransmit timeout (m	isec) 3000			
Operators	RADIUS auth number of retrie	s 1]	
	Enable display of RADIUS reply	y message		1	
	Default Auth level	Operator RADIUS sequent	•		
	server IP	Server port	Server secret		
	1st:	1812			
	2st:	1812			
	Bst:	1812			
		Submit			

Figure 11-6: RADIUS Settings

11.2.2 LDAP

R

- 1. Open the Authentication and Authorization Settings on the Version 7.2 platform (open the EMS menu: Security > Authentication & Authorization).
- 2. From the drop-down list, select LDAP Authentication.

Figure 11-7: LDA	P Configuration
------------------	-----------------

	AudioCodes' EMS - gena is logged with Administration authoriz	ation to server 10.1.8.23.(Last login time:2016-05-26 18:06:21)	
F	ile View Tools Faults Security Help		
1	Authentication & Authorization Settings		
	Authentication Type Synchronizing MsK-MsK CLI with EMS Us LDAP Authentication User Login Type (User/Password or CAC)	LDAP Authentication	ance
	LDAP Authentication Server IP	10.10.10.10	0 (0)
	LDAP Authentication Server Port	389	0 (0 0
	LDAP Connectivity DN	aaaaaaa	0 (0)
	LDAP Connectivity Password		0 (0)
	User DN Search Base	bbbbbbbb	0 (0 0
	EMS Super Administrator User Group Name	EMS_SuperAdmin	0 (0 (
	EMS Administrator User Group Name	EMS_Admin	0 (0
	EMS Operator User Group Name	EMS_Operator	0 (0)
	EMS Monitor User Group Name	EMS_Monitor	0(1)
	Default Security Level on LDAP Group Absence	Reject	0 (0)
	LDAP Server Number Of Retries	3	0 (0)
	LDAP Server SSL Enabled	Plain Connection	

- **3.** Open the Authentication screen on the Version 7.4 platform (System tab > Administration > Security > Authentication).
- 4. From the drop-down list, select LDAP.

		Figure 11	-8: LDAP Settings	
des ration Center	NETWORK ALARMS STATISTICS	CALLS USERS SYSTEM		
CONFIGURA	TION TASKS			
ATION				
MINISTRATION <<	Authentication Type LDAP •			
	AUTHORIZATION LEVEL SETTINGS		LDAP AUTHENTICATION SETTINGS	
	Administrator User Group Name	EMS_Admin	LDAP Authentication Server IP	0.0.0.0
rs	Operator User Group Name	EMS_Operator	LDAP Authentication Server Port	389
	Monitor User Group Name	EMS_Monitor	LDAP Connectivity DN	domain
	Default Security Level	Reject	LDAP Connectivity Password	
			LDAP Server Number of Retries	3
			User Dn Search Base	base
			SSL	
			Certificate	T

Figure 11-8: LDAP Settings

AUTHENTIC/ ADM LICENSE 5. Configure the required parameters using the Version 7.2 platform as reference.

11.3 Alarms (from EMS Application)

11.3.1 Alarms Settings

1. Open the Global alarm settings on the Version 7.2 platform (In the main EMS menu: Faults > Alarms Setting).

Events Automatic Clearing	
Enable Events Automatic Clearing	V
Events Automatic Clearing Period (days)	3
Alarms Automatic Clearing	
Enable Alarms Automatic Clearing	
Alarms Automatic Clearing Period (days)	30
Marms Suppression	
Enable Alarms Suppression	
Alarms Suppression Counter Threshold	20
Alarms Suppression Interval (seconds)	2
Note that this configuration applies to the same	alarm type from the same source
EMS Keep-Alive	
Enable EMS Keep-Alive trap	
EMS Keep-Alive trap interval (seconds)	60
Destination Provisionin	g

Figure 11-9: Alarm Settings

2. Open the Alarms screen on the Version 7.4 platform (System tab > Configuration > Alarms).

One Voice Operation Center		SYSTEM	
ADMINISTRATION CONFIG	TASKS		
ALARMS			
CONFIGURATION	c		
> TEMPLATES	ALARMS AUTOMATIC CLEARING	ALARMS SUPPRESSION	
ALARMS	Alarms Automatic Clearing	Alarms Suppression	8
FILE MANAGER	Alarms Automatic Clearing Period (days) 30	Alarms Suppression Counter Threshold	20
EXTERNAL APPLICATIONS		Alarms Suppression Interval (seconds)	600
	EVENTS AUTOMATIC CLEARING	Note that this configuration applies to the alarms	of same type and source
DEVICE BACKUP	Events Automatic Clearing	OVOC KEEP-ALIVE	
	Events Automatic Clearing Period (days)	OVOC Keep-Alive	
		OVOC Keep-Alive trap interval(seconds)	60
		Note: Pay attention to define alarm for rule with	event
		Submit	

Figure 11-10: Version 7.4 Alarms Settings

3. Configure the required settings using the Version 7.2 platform as reference.

11.3.2 Alarms Forwarding Rules

1. Alarms forwarding rules need to be reconfigured manually on the new Version 7.4 machine (EMS Main menu: Faults > Alarms Forwarding Configuration).

🔛 Alarn	ns Forwarding Configurat	ion				terinary.	×
File Vi	iew Actions Help						
🛨 😒							
Active	Destination Name	Destination Type 🔺	Allow	Alarm Forward	EventForward	Severities	
	Email	EMAIL	×	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical	
	aliya	EMAIL	×	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical	
	test1	SNMP	×	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical	
V	SNMP	SNMP		EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critic	al
	MaksTest	SNMP	×	IP Phone	IP Phone	info, warning, minor, major, critical	
	gal	SNMP	 	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical	
	Syslog	SYSLOG	×	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical	
						ОК Са	ncel

Figure 11-11: Version 7.2: Alarm Forwarding Rules

2. Double-click to open each rule specific configuration rule.

Destination Rule Configuration	_	_	_	_	_	_		×
Destination Type	SNMP							
Destination Rule Name						_	Destination Host IP Address 10.1.2.38	
Decandation reality	SNMP						Destination Host Port 162	
Allow Forward	Preve	ent Forwa	ď				SNMP v2c Trap Community public	
Alarm Origin	*	EMS	SEM	MGW	IP Phone	e	Enable SNMPv3 Configuration	
	Alarms	 ✓ 		 ✓ ✓ 	✓		Security Name	
	Evenus	V	•	v	v		County Name	
Alarm Names	AllAlarm	IS					Security Level No Security	T
							Authentication Protocol None	T
							Authentication Key	
Alarm Types						E.	Privacy Protocol None	▼
		,					Privacy Key	
Severities								
	e e							
Source								
Source MGW List	Select	NGW						
	Pegion		MGW Name	ID A	ddroee	_		
	AllRegio	ns	AIMGW	IF A	uuress			
								OK Cancel

Figure 11-12: Version 7.2: Destination Rules Configuration

Caudiocodes

3. Open the Alarm-forwarding rules screen (Alarms tab > Forwarding) on the Version 7.4 platform.

Figure 11-13: Version 7.4:	Alarm Forwarding Rules
----------------------------	------------------------

Cone Voice Operation Center		MS STATISTICS C				
ACTIVE JOURNAL ALL	FORWARDING					
FORWARDING	🕒 Add 🖉 Edit	Delete CRefresh				
RULE NAME	A	CTIVE	DESTINATION TYPE	DESTINATION	TENANT	
roman2		×	SNMP	1.1.1.1	System	*
roman3		×	SNMP	1.1.1.1	System	
aliya		~	SNMP	10.4.2.60	System	
TEST_EITAN_1		×	SNMP	1.2.3.4	Customer1	

- 4. Click **Add** to add a new rule.
- 5. Configure the required parameters using the Version 7.2 platform as reference:
 - **a.** Allow/prevent configuration and enable/disable rule can be configured under top section.

Figure 11-14: Rule Name

Rule Name	
Forward matching alarms/events	Prevent forwarding of matching alarms/events
Contraction (Disable Date	

- Enable/Disable Rule
 - **b.** Configure devices and other topology filtered elements under "Topology Conditions" section.
 - c. Other forwarding conditions can be configured under "Rule Conditions" section.

Figure 11-15: Alarm Forwarding Rule Conditions

Rule Name		
Forward matching alarms/even Enable/Disable Rule	ts Prevent forwarding of n	natching alarms/events
TOPOLOGY CONDITIONS		DESTINATION
Alarm Origin	All Selected	~
Event Origin	All Selected	~
Severities	All Selected	~
Alarm Names	All Selected	~
Alarm Types	All Selected	~
Source		

d. Destination type and configuration can be configured under "Destination" section.

Prevent forwarding of n	natching alarms/events
RULE CONDITIONS	
SNMP	
Destination Details	
NMP v2	
No security	
No protocol	
No protocol	
	Prevent forwarding of n RULE CONDITIONS SNMP Destination Details No Protocol No protocol

Figure 11-16: Alarm Forwarding Destinations

11.4 Software Manager

On the new One Voice Operations Center Version 7.4 machine, add files that you extracted from the Version 7.2 platform in Section 5.1 to the Software Manager (System tab > Configuration > File Manager).



Note: If devices were added to the Version 7.2 platform and not connected to the network then you must download their configuration and firmware files manually on the Version 7.4 platform (from the Network Topology page).

11.5 Device Backup Configuration

1. Open the devices backup configuration settings on the Version 7.2 platform (In the main EMS menu: Tools > MG Backup Manager).

File Viev	v Tools Faults S	Security Hel	p			······,				
MG Tree	🞇 MG Backup Ma	anager				1 mm			• *	1
▼ 🔐 G ▶ #	Backup Summ	ary	3 Backup Settings		×				_	
	MG Name	IP /	Enable Periodic Backup	Yes	•		File Type	File Size (Bytes)		
▶ 🔡	NJ-MSBG-SBC	172	Packup History Size			BC_172.28.1.10_p_80_iniFile_0401-Dec-11-2015.ini	INI	14422		
▶ 👬	M1KA	10.	Dackup History Size	· ·		.10.5_p_84_iniFile_0400-May-24-2017.ini	NI	23642)	
▶ ■	NJ-GW	172	Number of Retries	3	v	28.1.3_p_84_iniFile_0402-Jun-05-2017.ini	INI	26804		
	10.3.4.62	10.				3.4.62_p_68_iniFile_0401-Mar-30-2017.ini	INI	3791		
	172.17.116.69	172		ОК	Cancel	172.17.116.69_p_68_iniFile_0401-Jun-03-2017.ini	INI	9437		
	172.22.3.155-3227	172				3227461_172.22.3.155_p_80_cliScriptFile_0402-M	CLI	26234		
	172.17.116.69	172.17.116.69	Periodic	2017-05-30 07:01:16	172.17.116.6	59_172.17.116.69_p_68_iniFile_0401-May-30-2017.ini	INI	12928		
	10.3.4.61	10.3.4.61	Periodic	2017-03-20 06: 01: 08	10.3.4.61_1	0.3.4.61_p_46_iniFile_0401-Mar-20-2017.ini	INI	9157		tic detection nodes
88	10.3.151.222	10.3.151.222	Periodic	2017-05-19 07:01:20	10.3.151.222	2_10.3.151.222_p_46_iniFile_0401-May-19-2017.ini	INI	7333		
▶ 3	10.4.100.35	10.4.100.35	Periodic	2017-05-22 07:00:06	10.4.100.35	_10.4.100.35_p_5_iniFile_0400-May-22-2017.ini	INI	10126		
-	172.22.3.155-3227	172.22.3.155	Periodic	2017-05-06 07:02:06	172.22.3.15	5-3227461_172.22.3.155_p_80_iniFile_0402-May-06	INI	5610		
88	M1KA	10.15.10.5	Periodic	2017-05-18 07:00:18	M1KA_10.1	5.10.5_p_84_iniFile_0400-May-18-2017.ini	INI	22333		
	Uzi-SBC	10 15 54 100	Perindic	2016-05-17 07-00-29	Uzi-SBC 1	0.15.54.100 p.82 iniFile 0400-Mav-17-2016 ini	INI	13897		5
								Refresh	Close	

Figure 11-17:Version 7.2: Backup Configuration

2. Open the Device Backup screen on the Version 7.4 platform (System tab > Configuration > Device Backup).

		CALLS LISERS SYSTEM	-	ARM 0 =
One Voice Operation Center				
Administration Controlium				
DEVICE BACKUP				
CONFIGURATION 🛠				
▶ TEMPLATES	DEVICE BACKUP			
ALARMS	Enable Periodic backup			
	Number of backup files per device	5		
P FILE MANAGER	Number of retries	2		
EXTERNAL APPLICATIONS				
DEVICE BACKUP		Submit		

Figure 11-18: Version 7.4: Backup Configuration

3. Configure the required parameters using the Version 7.2 platform as reference.

11.6 LDAP User Authentication

- 1. On the Version 7.2 platform, open the LDAP Authentication & Authorization Settings screen (EMS Main menu: Security > Authentication & Authorization).
- 2. From the Authentication drop-down list, select LDAP Authentication.
 - Figure 11-19: LDAP Authentication and Authorization

	DAR Authoritation	Ă
Authentication Type Synchronizing MsK/MsK CLI with EMS U	Jsers	
LDAP Authentication		1
User Login Type (User/Password or CAC)	User/Password Login	
LDAP Authentication Server IP	10.3.180.11	
LDAP Authentication Server Port	636	
LDAP Connectivity DN	Admin2@QA-EMS.LOCAL	
LDAP Connectivity Password		
User DN Search Base	OU=QA,DC=QA-EMS,DC=LOCAL	
EMS Super Administrator User Group Name	EMS_SuperAdmin	
EMS Administrator User Group Name	EMS_Admin	
EMS Operator User Group Name	EMS_Operator	
EMS Monitor User Group Name	EMS_Monitor	
Default Security Level on LDAP Group Absence	Reject	
LDAP Server Number Of Retries	3	
LDAP Server SSL Enabled	SSL With Certificate	
LDAP Client Certificate	EMS-QA-rootCA.cer	
•(ОКС	ancel

- 3. Note the LDAP Authentication settings.
- 4. Open the Authentication page on the Version 7.4 platform (System tab > Administration > Security > Authentication).
- 5. From the Authentication Type drop-down list, select LDAP.

Figure 11-20: Authentication Page

ADMINISTRATION 《	Authentication Type LDAP				
LICENSE			I DAD ALITUENTICATION SETTINGS		
Summary	Administration developments				
Tenants Allocations	Administrator User Group Name	EMS_Admin	LDAP Authentication Server IP	0.0.0.0	
SECURITY	Operator User Group Name	EMS_Operator	LDAP Authentication Server Port	389	
Authentication Operators	Monitor User Group Name	EMS_Monitor	LDAP Connectivity DN	domain	
	Default Security Level	Reject	LDAP Connectivity Password		
			LDAP Server Number of Retries	3	
			User Dn Search Base	base	
			SSL	V	
			Certificate		
			ubmit		

SEM Client Configuration 11.7

11.7.1 **Microsoft Active Directory**

On the SEM Version 7.2 platform, open the Active Directory Settings screen (Users tab 1. > Active Directories folder).

Figure 1	1-21: Version 7.2: Active Directory Configuration
Active Directory Setting	S .
General Settings	
Server name	Enterprise-AD
Host	new.corp.enterprise.com
Port	389
DN	new.corp.enterprise.com
Base Object	dc=corp,dc=enterprise,dc=com
Security Settings	
Password	***
SSL	Disable
Certificate File	Browse
Scheduler Settings	
Sync Time	Start Sync Each 1 + Hours
Last Sync Time	
Full Sync Time	Start Full Sync At 00 🔻 : 00 💌 Each 1 📥 Days
Last Full Sync Time	

Open the Active Directory Settings on the Version 7.4 platform (Users tab > Active Directories) and then click **Edit**. 2.

ACTIVE DIRECTO	DRY SETTINGS	×
GENERAL		
Tenant	Tenant 1	•
Name	Host Port 389	
Base object		
Bind DN		
Password		
Enable SSL	. Certificate file	•
Test connec	tivity (NA)	
UPDATES		
Check for upo	lates every 1 hours	
Perform full u	Indate even / 2	
	days	
dl		
	OK Cancel	

Figure 11-22: Version 7.4 Active Directory Configuration

3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.2 Skype for Business SQL Server Configuration

1. On the SEM Version 7.2 platform, open the Network Device Definition screen for the Skype for Business device (Network tab).

Figure 11-23	3: SEM - N	etwork tab	Skype for	Business	Device Definition
--------------	------------	------------	-----------	-----------------	-------------------

Net	Network Device Definition X		
	◯ Generic Device		
	Device Type	Front End Server 👻	
	FQDN		
	IP		
	Name		
	SQL Server IP		
۲	SQL Port	1433	
\bigcirc	SQL Instance Name		
	SQL Server User		
	SQL Server Password		
	SSL	Disable 🗸	
	Certificate File	Browse	
	Region	AutoDetection 👻	
		Apply Close	

Open the Lync Device Details screen in the Version 7.4 platform, (Network tab > Topology), select the Skype for Business device and then click Edit.
LYN	C DEVICE DETAILS		×
	Name	SFB	
	Tenant	Singapore 🔻	
	Region	AutoDetection 🔻	
	Device Type	MS LYNC FE	
	FQDN	enterpriseSFB.corp.enterprise.com	
	SQL Server IP	10.1.1.64	
۲	SQL Port	1433	
•	SQL Instance Name		
	SQL Server User		
	SQL Server Password		
	SSL	DISABLED •	
	ОК	Cancel	

Figure 11-24: OVOC - Skype for Business Device Definition

3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.3 QoE Thresholds Configuration

Open the QoE Thresholds page (Utilities tab > QoE Thresholds) on the Version 7.2 platform.

Session Experience Manager							☆ Network	Statis	tics	Calls List	Lus ers	یک Alarms	Reports	Utilities			
	Server Storage Cot. Thresholds Server Configuration																
	II	Refresh															🔒 System Profile 🖠
				MOS Fair- Poor TH	MOS Good- Fair TH	Delay Fair- Poor TH	Delay Good- Fair TH	P.Loss Fair- Poor TH	P.Loss Good-Fair TH	Jitter Fair- Poor TH	Jitter Good- Fair TH	Echo Fair- Poor TH	Echo Good- Fair TH				
	습 1	7 OrenP - test		3	3.5	70	50	30	5	20	5	3	0	Devices / Links / Endpoin	ts 📀	\otimes	dfgdfg
	습 ۲	7 test						0.8	0.6					Devices / Links / Endpoin	ts 🧭	8	
	\$ 1	High Sensitivity Thresho	-	2.9	3.6	400	140	4.3	1.5	70	35	11	27	Devices / Links / Endpoin	ts 🥥		
			1.00											and the second s	0	0	

Figure 11-25: Version 7.2: QoE Thresholds Configuration

 Open the QOE Thresholds page on the Version 7.4 platform (Calls tab > QOE Thresholds).



			5 5.4		_									·
	odes NETWO				USERS									
CALLS LIST	QOE THRESHOLDS	QOE STATUS & ALARM	s		-									
QOE THRE	SHOLDS	Add 🖋 Edit 💼 E	elete 🛛 😂 Refre	esh										
DEFAULTS	NAME	DESCRIPTION	MOS		DELAY (M	SEC)	PLOSS (%)		JITTER (MS	SEC)	ECHO (DB)	>> QOE THRESHOLDS SUMMARY	
	High Sensitivity Thres		+3.6+	+2.9+	+140+	+400+	+1.5+	→ 4.3 →	+35+	→ 70 →	+27+	+11+	0 selected	
	Low Sensitivity Thres		+3.4 →	+2.7→	→ 200→	→ 1200 →	+2.7+	+6.6+	→ 45 →	→ 90 →	÷23÷	→ 9 →		
000	Medium Sensitivity T		+3.5+	+2.8+	+160+	→ 500 →	+2+	+5+	+40+	→ 80 →	+25 →	+10+		
	High Sensitivity Thres		+3.6 +	+ 2.9 +	+140+	→ 400 →	+1.5+	→ 4.3 →	+35+	→ 70 →	→ 27 →	→ 11 →		
	Low Sensitivity Thres		+3.4+	+ 2.7 →	→ 200 →	<mark>→</mark> 1200 →	+2.7→	→ 6.6 →	+45+	→ 90 →	÷23→	→ 9 →		
000	Medium Sensitivity T		+3.5+	+2.8+	+160+	→ 500 →	+2+	→ 5 →	+40+	+ 80 +	+25+	+10+		
H 4 (1)	×			20 ,	 items per 	r page					Ite	ms 1-6 out of		

Figure 11-26: Version 7.4: QoE Thresholds Configuration

3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.4 Alarm Rules Configuration

1. Open the Alarms Rules Configuration on the Version 7.2 platform (Alarms tab > Alarm Rules).

Figure 11-27	: Version	7.2: Alarm	Rules	Configuration
--------------	-----------	------------	-------	---------------

Ses		sperience Manager	* Netw		U Statistics	Calls		and the series of the series o		L ms	Reports	Utili	ties				
Time	Time Range: From: Last 3 hours 🔤 To: New 🧃 39 Devices All Selected + 32 Links All Selected + 373 Endpoints All Selected + All / Ilone																
A	Active Alarma History Alarma Alarma Rules																
			Frequency	Time Window (min)	Calls #	Failed Calls %		Poor Quality Calls %		Avg Call Duration (sec)		Total Bandwidth (Kb/s					
						Critical	Major	Critical	Major	Critical	Major	Critical	Major	Critical	Major		
u	ink	IL Edge to NJ FE,NJ FE to Edge ,IL Mediation to SBC ,IP PB>	60	120	50	15	5	0	0	0	0	0	0	0	0	0	\oslash
Li	ink	Client Access, SSW Connection	15	60	50	10	5	10	5	3	5	0	0	0	0	•	\oslash
N	ode	VMAS,Mobility-ESBC,VMAS-Demo	15	60	50	10	5	10	8	3	5	0	0	0	0	•	\oslash
N	oda	E.980	15	60	50	15	5	15	5	0	0	0	0	0	0	0	0

2. Open the QOE Status and Alarms page on the Version 7.4 platform (Calls tab > QOE Status & Alarms tab).

	des eration Center	NETWORK	ALARMS	STATISTICS	CALLS	JSERS SYSTEM							
CALLS LIST	QOE THRESHO	.DS QOE	STATUS & ALAR	MS									
QOE STATUS & ALARMS OAdd													
DEFAULTS	NAME	LAST RUNT	MONITORI	MINIMUM	FAILED CALLS PR	POOR QUALITY	AVERAGE CALL	BANDWIDTH RU	MAX CONCURRE	DESCRIPTI	>> QOE ALARMS SUMMARY		
	ALARM RULE	27-Jul-17 2	15	50	+2+ +10+	+2+ +10+ *	+5+ +3+ [*]	+0+ +1+	+0+ +1+		O selected		
	ALARM RULE	27-Jul-17 2	15	50	+2+ +10+	+2→ +10→ *	+5+ +3+ [#]	+0+ +1+	+0+ +1+				
0	S4B failed	27-Jul-17 2	15	50	+2+ +10+ ▲	+2+ +10+ *	→5→ →3→ [▲]	⇒5→ →10→	+5+ +10+				

Figure 11-28: Version 7.4: Alarm Rules Configuration

3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.5 Scheduled Reports Configuration (from SEM Application)

 Open the SEM Scheduled Reports configuration on the Version 7.2 platform (Reports > Scheduled Reports).

SEM Reports Scheduled Reports SEM Report Name Report Topic Report Report Name Report Topic Report Call Statistics by Device Network Status Rep SEM Report test Session Experience Manager Session Experience Manager Report Name Report Topic Report Statistics by Device Network Status Rep SEM Report test Set Report Report Name Report Topic Report Statistics by Device Network Status Rep SEM Report test Set Report Set Report Set Report Topic Report Call Statistics by Device Network Status Rep SEM Report cat qui qui Hourly 1 0 Secure O O Secure 15000 Jan 24 Call Statistics By Device Network Status Rep SEM Report Call_Stats Heaving 1 00005 Feb 16 Call Statistics by Device Network Status Rep SEM Report cat qui qui Hourly 1 0 Secure O O Secure 150000 Jan 24 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 14 Call Statistics by Device Network Status Rep SEM Report cat gui Heaving 1200005 Feb 16 Call Statistics by Device Network Status Rep SEM Report statbylink Heaving 123 Status 20 O Sub report 1200005 Feb 16 Call Statistics By Device Network Status Rep SEM Report statbylink Heaving 123 Status 20 O Sub 1222020 May 24 Call Statistics By Device Network Status Rep SEM Report statbylink Heaving 123 Status 20 O Sub 1222020 May 24 Call Statistics By Device Network Status Rep SEM Report statbylink Heaving 123 Status 20 O Sub 1222020 May 24 Call Status 20 O Sub 1222020 May 24 Call Statu	ŝ	ession Experie	nce Manager				
Image: Search Image: Report Topic Report Name Report Topic Group Scheduler Name Descrip Name Call Statistics by Device Name Statistics Provide Name Descrip Name Report Name Name Descrip Name Session Experience Manager		SEM Reports Sch	heduled Reports				
Report Name Report Topic Group Report Name Scheduler Forup Descrip Name Session Experience Manager		🛗 Search	Refr	resh			
Call Statistics by Device Network Status Res SEM Report test Session Experience Manager Network Status Res SEM Report Last Set Report Soldeduct Reports Scheduld Reports Scheduld Reports Report Name Report Scheduldr Report Name Report Scheduldr Report Name Report Scheduldr Gall Statistics by Device Name/er Description Scheduldr Num of Run Num of Run Num of Run Scheduldr Call Statistics by Device Network Status Rep Scheduldr Description Call Statistics by Device Network Status Rep Scheduldr Num of Run Call Statistics by Device Network Status Rep Status Rep Scheduldr Call Statistics by Device Network Status Rep Status Rep Scheduldr Call Statistics by Device Network Status Rep Status Rep Status Rep Call Statistics by Device Name/Status Rep Status Rep Status Rep Call Statistics by Device Network Status Rep Status Rep Status Rep Call Statistics by Device Network Status Rep Status Rep Status Rep Call Statistics by Device Netwok Status Rep		Report Name	Report Topic Rep Name Gro	oort Schedule up Name	r Descrip		
Session Experience Manager Million Statistics		Call Statistics by Device	Network Status Rep SE!	M Report test			
Session Experience Manager Mrtwork Selection Calls List List <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>							
Schedulde Reports Bester h Reformation Schedulder Description Scheduling Frequency Num to Run Num of Run Times Generated Reports User Last Run Time Next Run Time Cell Statistics by Device Network Status Rep SEM Report q1 q1 Hourly 1 0 Status 0 0 orep 180000 Jan 24 Call Statistics by Device Network Status Rep SEM Report q1 q1 Hourly 1 1 Status 0 0 0 orep 180000 Jan 24 0 Call Statistics by Device Network Status Rep SEM Report q1 et al. Status 0 0 0 orep 180000 Jan 24 0 Call Statistics by Device Network Status Rep SEM Report 100000 Fab 16 0 0 0 0 orep 100000 Fab 16 0	Session Experience Manager		米 etwork Statistic	s Calls List	and the set of the set	Alarms Reports	Utilities
Mare Report Report Scheduling Num to Run Num to Run Generated Times Centrated Reports User Last Run Time Next Run Time Call Statistics by Device Network Status Rep Scheduling Num to Run 1 0 Stream © © support support Image: Stream Image: Stream <td< td=""><td>SEM Reports Scheduled Reports</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	SEM Reports Scheduled Reports						
Report Name Report Topic Name Report Topic Group Report Name Scheduler (Group Description Scheduling Frequency Num to Run Num of Run Times Generated Report User Last Run Time Next Run Time Call Statistics by Device Network Status Rep SEM Report qq1 qq1 Hourly 1 0 Status © © scrept support	📸 Search 🧱 Refresh						
Call Statistics by Device Network Status Rep SEM Report optimization optimal instation optimization	Report Name Report Topic Report Scheduler Name Group Name	Description Sch	quency Num to Run	Num of Run Generated Times Reports		User Last Run Time	Next Run Time
Call Statistica by Device Network Status Rep: SEM Report Call Statistica by Device Network Status Rep: SEM Report Call Statistica by Device Network Status Rep: SEM Report 100:000 Jun 24 Call Statistica by Device Network Status Rep: SEM Report Text Weekly 4 Status © Ø O orep 100:000 Jun 24 Call Statistica by Device Network Status Rep: SEM Report Text Weekly 4 Status Ø Ø orep 100:000 Jun 24 Call Statistica by Device Network Status Rep: SEM Report Text Weekly 4 Status Ø Ø orep 100:000 Jun 24 Call Statistica by Device Network Status Rep: SEM Report Text Tex	Call Statistics by Device Network Status Rep SEM Report qq1	qq1 Hou	uriy 1	0 Show	6 0 8	support	
Call Statistics by Device Network Status Rep. SEM Report Test Weekly 4 Show © Ø orep 100000 Feb 16 Call Statistics by Device Network Status Rep. SEM Report statistics by Device Ø Ø O Ø usit 220200 May 24	Call Statistics by Device Network Status Rep SEM Report Call_Stats	Hou	urly 1	1 Show	۲ ال	orenp 18:00:00 Jan 2	14
Call Statistics by Link Network Status Rep SEM Report status/link Hourly 123 Show 🖸 🖉 🐼 usit 22:02:00 May 24	Call Statistics by Device Network Status Rep SEM Report Test	Wee	ekly	4 Show	• • •	orenp 10:00:00 Feb 1	6
	Call Statistics by Link Network Status Rep SEM Report statbylink	Hou	urly	123 Show	• • •	usit 22:02:00 May 2	24

Figure 11-29: Version 7.2: SEM Scheduled Reports

2. Open the Reports tab on the Version 7.4 platform (Statistics tab > Reports tab).

	3													
	Codes te Operation Ce	nter	NETWORK	ALARMS	STATISTICS	CALLS	USERS	ADMIN						
DEVICES	LINKS	SITES	ENDPOINT	S REPOR	RTS 🛃									

Figure 11-30: Version 7.4: Statistics Reports

3. Configure the required scheduled reports using the Version 7.2 platform as reference.



This page is intentionally left blank.

A Appendix A – Backup and Restore

A.1 OVOC Server Backup

There are two main backup processes that run on the OVOC server:

Weekly backup: runs once a week at a pre-configured date & time (default is Saturday 02:00). In this process, the whole database is backed up into several "RMAN" files that are located in /data/NBIF/EMSBackup/RmanBackup directory. In addition, many other configuration and software files are backed up to a TAR file in the /data/NBIF/EMSBackup directory. In general, this TAR file contains the entire /data/NBIF directory's content (except 'EMSBackup' directory), OVOC Software Manager content and server_xxx directory's content.

To change the weekly backup's time and date, see Section A.1.1.

Daily backup: runs daily except on the scheduled week day (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.



Warning: The Backup process does not backup configurations performed using EMS 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.

Do the following:

1. Copy all files in /data/NBIF/EMSBackup/emsSServerBackup_<time&date>_<Version>.tar file directory to an external machine.

Where:

- <time&date> is only an example; replace this path with your filename.
- <Version> is the Version number of the server release
- 2. Copy all files in /data/NBIF/EMSBackup/RmanBackup directory (including control.ctl and init.ora files) to an external machine.

A.1.1 Change Schedule Backup Time

This step describes how to reschedule the backup time.

- To schedule backup time:
- 1. From the Application Maintenance menu, choose Change Schedule Backup Time.
- 2. Choose the day of the week that you wish to perform the backup.

A.2 OVOC Server Restore

This section describes how to restore the OVOC server. This can be done on the original machine that the backup files were created from or on any other machine.

Note:



- 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 (see Chapter 8).
- **3.** Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
- 4. Copy all the files you backed up in A.1 to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
- 5. In EMS Server Manager, go to the Application Maintenance menu and select the **Restore** option.
- 6. Follow the instructions during the process; you might need to press Enter a few times.
- 7. After the restore operation has completed, you are prompted to reboot the OVOC server.

B Appendix B – EMS / SEM 7.2 – Topology Import Process Limitations

- Since the Version 7.4 release support tenants topology level, the process will create a new default tenant (if no default tenant was already defined)
- It is recommended to perform this procedure on server without previous topology configuration.
- Import regions:
 - Regions which were not in previous 7.2.3000 multi-tenancy (defined specific operators visibility on these regions), will be created under the default tenant
 - Regions which were in previous 7.2.3000 multi-tenancy (defined specific operators visibility on these regions), will be created each in new tenant with same name (if such tenant name already exists, it will not be created!)
 - If region name already exist in the tenant, it will not be created!
- Import Devices/Lync devices/Generic devices:
 - Create all devices/Lync devices/Generic devices to the same region they were belong to in previous 7.2.3000 server (if the region failed to be created, relevant devices will not be created)
 - Device will not be created if any constraint is violated such as serial number already exists etc.
- Import SBAs:
 - Create SBAs under his relevant device
- Import Links:
 - Create link only if both devices were successfully created
- Import License Pool:
 - Add license pool configuration only for devices which were successfully added.



This page is intentionally left blank.

C Transferring Files

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



Note: FTP by default is disabled in 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, you drag the relevant file from the left pane i.e. in your PC directory to the right pane i.e. the /home/acems directory on the OVOC server host machine.

International Headquarters

1 Hayarden Street, Airport City Lod 7019900, Israel Tel: +972-3-976-4000 Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive, Somerset, NJ 08873 Tel: +1-732-469-0880 Fax: +1-732-469-2298

Contact us: <u>https://www.audiocodes.com/corporate/offices-worldwide</u> **Website:** <u>https://www.audiocodes.com/</u>

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-91055

