Migration Guide

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

audiocodes

Table of Contents

List of Figures

List of Tables

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 https://online.audiocodes.com/documentation-feedback.

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.

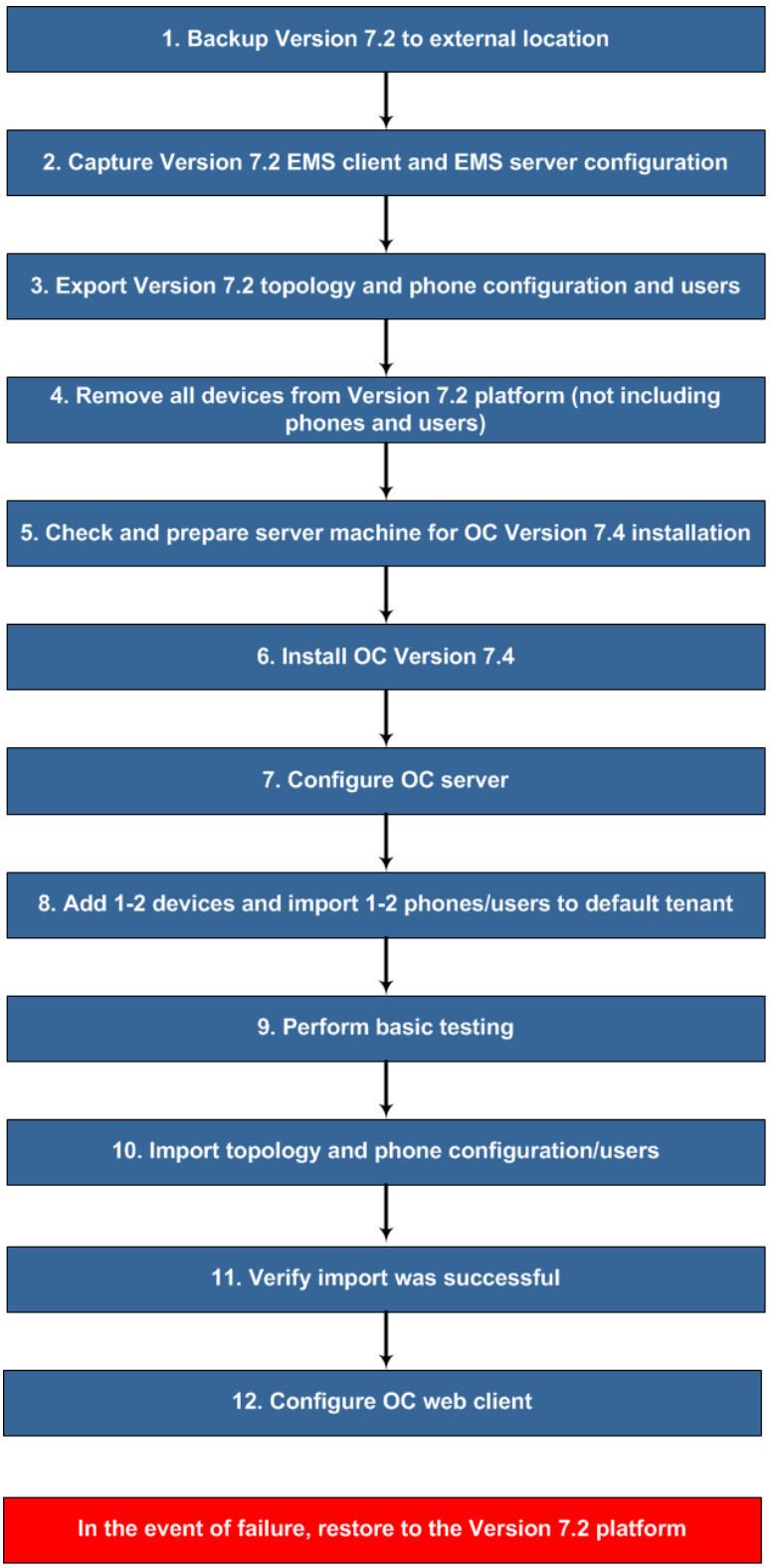
Warning: If you are deploying two machine topology, under no circumstances should the Version 7.2.3000 and Version 7.4 platforms be simultaneously connected to the network.

- **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 sub-menu, 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).

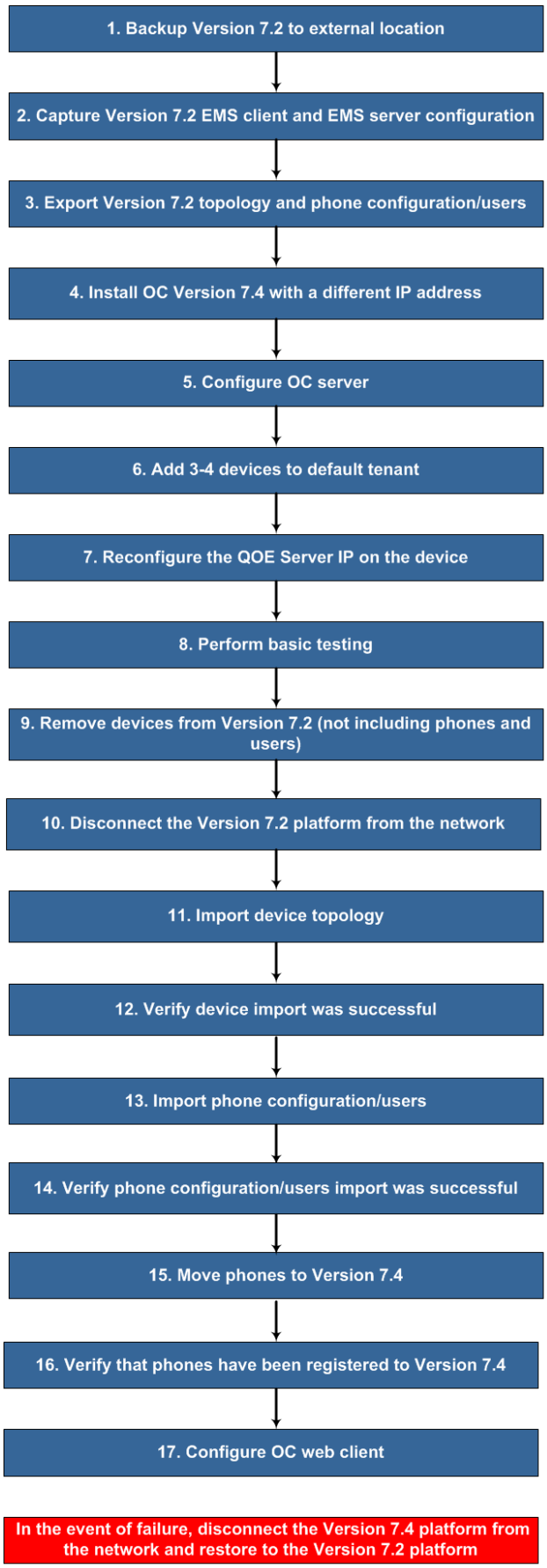
Note:

- 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.

Figure 2-2: Migration with Dual Machines



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 sub-menu, 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 devices original QOE server IP address as described in step 7.
  - √ 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.
- 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

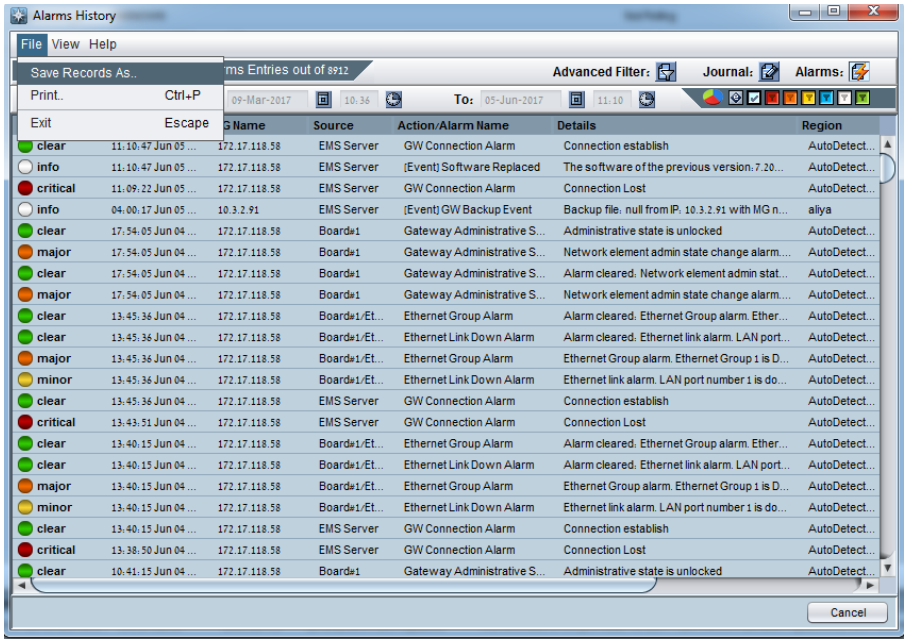
This procedure describes how to export data in textual format to a CSV file in human readable format. To view this information, you do not need to install any EMS/SEM software CSV file.

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**

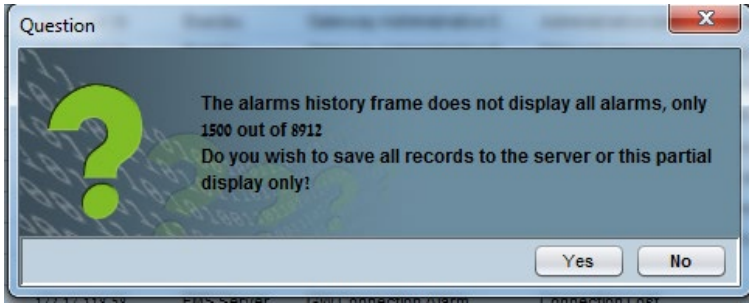
1. In the main EMS menu, choose **Faults** -> **Alarms History**.
2. Filter the relevant alarms.
3. In the main menu, choose **File** > **Save Records As**.

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:**

1. 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 conf.d]# pwd
/etc/httpd/conf.d
[root@EMS-server-17 conf.d]# ll
total 36
-rw-r--r-- 1 root root  2926 Apr 12 22:03 autoindex.conf
-rwxr-xr-x 1 root root    27 Sep  3 09:06 passphrase
-rw-r--r-- 1 root root   625 Feb 18  2017 php.conf
-rw-r--r-- 1 root root   366 Apr 12 22:04 README
-rwxr-xr-x 1 root root 10708 Sep 11 08:14 ssl.conf
drwxr-xr-x 2 root root    71 Sep  3 09:06 ssl.crt
drwxr-xr-x 2 root root    24 Sep  3 09:06 ssl.key
-rw-r--r-- 1 root root  1252 Apr 12 14:50 userdir.conf
-rw-r--r-- 1 root root   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

```
******************** Export process start ******************
Exporting topology entities...
copy keystore.jks file to /home/acems/
<?xml version='1.0' encoding='utf-8'?>
<TOPOLOGY>
<VERSION>v1</VERSION>
<REGIONS>
<REGION><REGION_ID>1</REGION_ID><REGION_NAME>AutoDetection</REGION
_NAME><REGION_DESCRIPTION> This region is intended for automatic
detection nodes </REGION_DESCRIPTION></REGION>
<REGION><REGION_ID>5</REGION_ID><REGION_NAME>gena</REGION_NAME></R
EGION>
```

```
</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
>fseUajPSaO6h4Ug5tO9y1g==</GATEWAY_PASSWORD><NETWORK_X_LOCATION>18
7</NETWORK_X_LOCATION><NETWORK_Y_LOCATION>70</NETWORK_Y_LOCATION><
/NODE>
</NODES>
<NON_ACL_NODES>
<NON_ACL_NODE><NODE_ID>188</NODE_ID><NODE_NAME>2.2.2.2</NODE_NAME>
<IP_ADDRESS>2.2.2.2</IP_ADDRESS><REGION_ID>5</REGION_ID><REGION_NA
ME>gena</REGION_NAME><NETWORK_X_LOCATION>160</NETWORK_X_LOCATION><
NETWORK_Y_LOCATION>169</NETWORK_Y_LOCATION><PRODUCT_TYPE>200</PROD
UCT_TYPE><REPORTED_NODE_ID>0</REPORTED_NODE_ID><SQL_SERVER_PORT>0<
/SQL_SERVER_PORT><SECURITY_LEVEL>0</SECURITY_LEVEL></NON_ACL_NODE>
</NON_ACL_NODES>
<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>
<LINK><LINK_ID>2385454313</LINK_ID><LINK_NAME>link2</LINK_NAME><SR
C_NODE_ID>190</SRC_NODE_ID><DEST_NODE_ID>189</DEST_NODE_ID><LINK_T
YPE>128</LINK_TYPE><TYPE_MEDIA_REALM>0</TYPE_MEDIA_REALM><TYPE_SUB
_MEDIA_REALM>0</TYPE_SUB_MEDIA_REALM><TYPE_SRC_FQDN>gggggggggggggg
g</TYPE_SRC_FQDN><TYPE_DEST_FQDN>fffffffffff</TYPE_DEST_FQDN><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/
```

```
Please transfer topology.xml from /home/acems/ to the One Voice
Operations Center 7.4 server under same /home/acems/ directory
Note: In order to preserve certificates, transfer the same way
also keystore.jks
******************** Export process finished *******************
```

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.

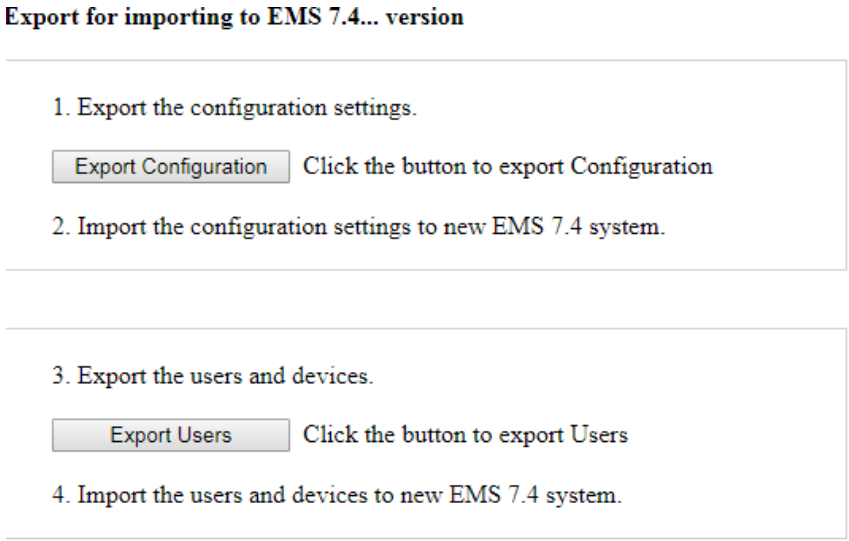
Note After this procedure is performed, the following cannot be configured on the Version 7.4 platform without making manual changes to the configuration template file (contact AudioCodes technical support for details):

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

➢ **To export IP Phone Management server configuration:**

1. Download the export configuration zip file to your PC from:
   https://services.audiocodes.com/app/answers/detail/a_id/55
2. Unzip the downloaded file.
3. 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



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 http://www.audiocodes.com/downloads.

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 -l | 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)

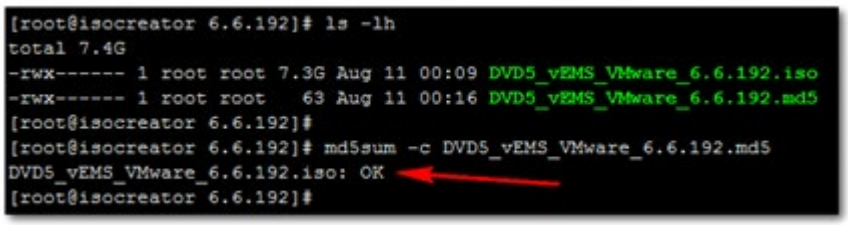
7.2.2.2 Linux

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



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

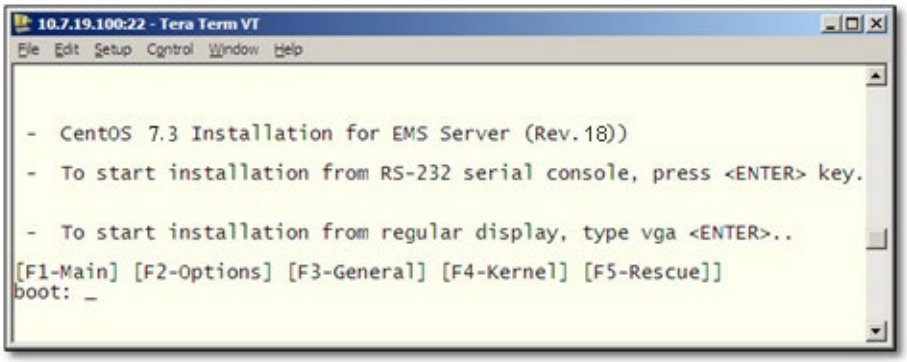
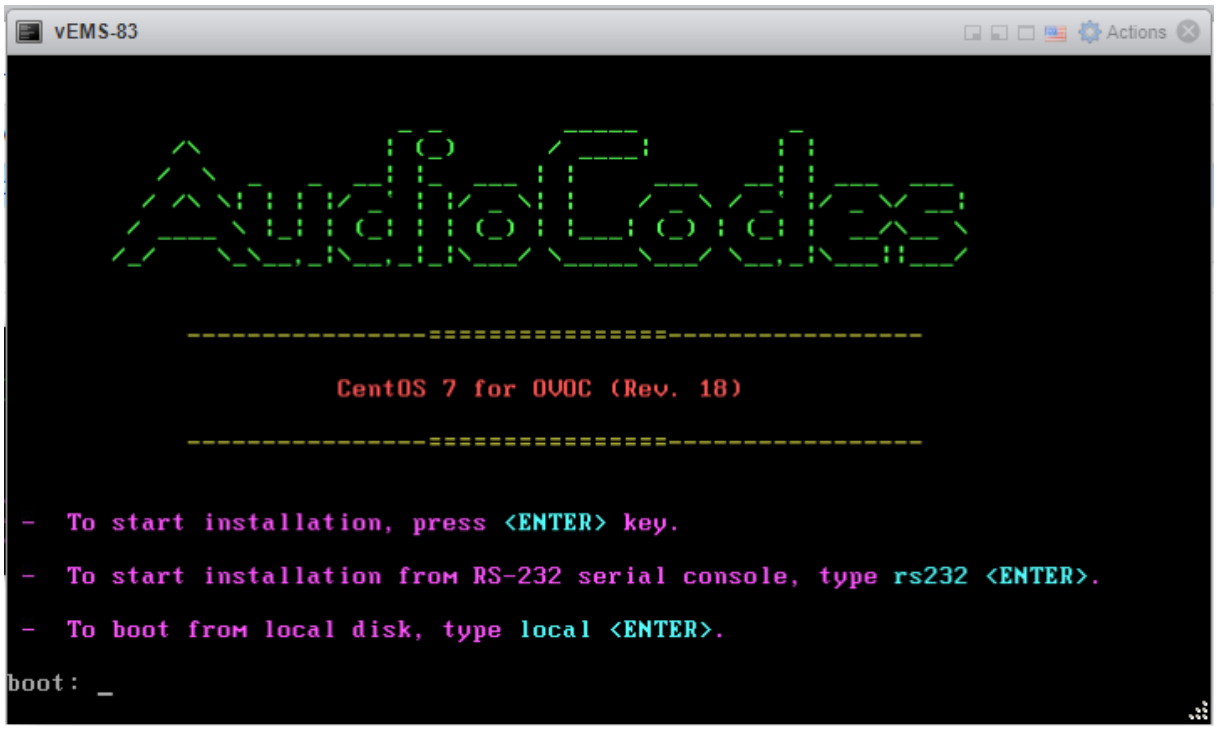
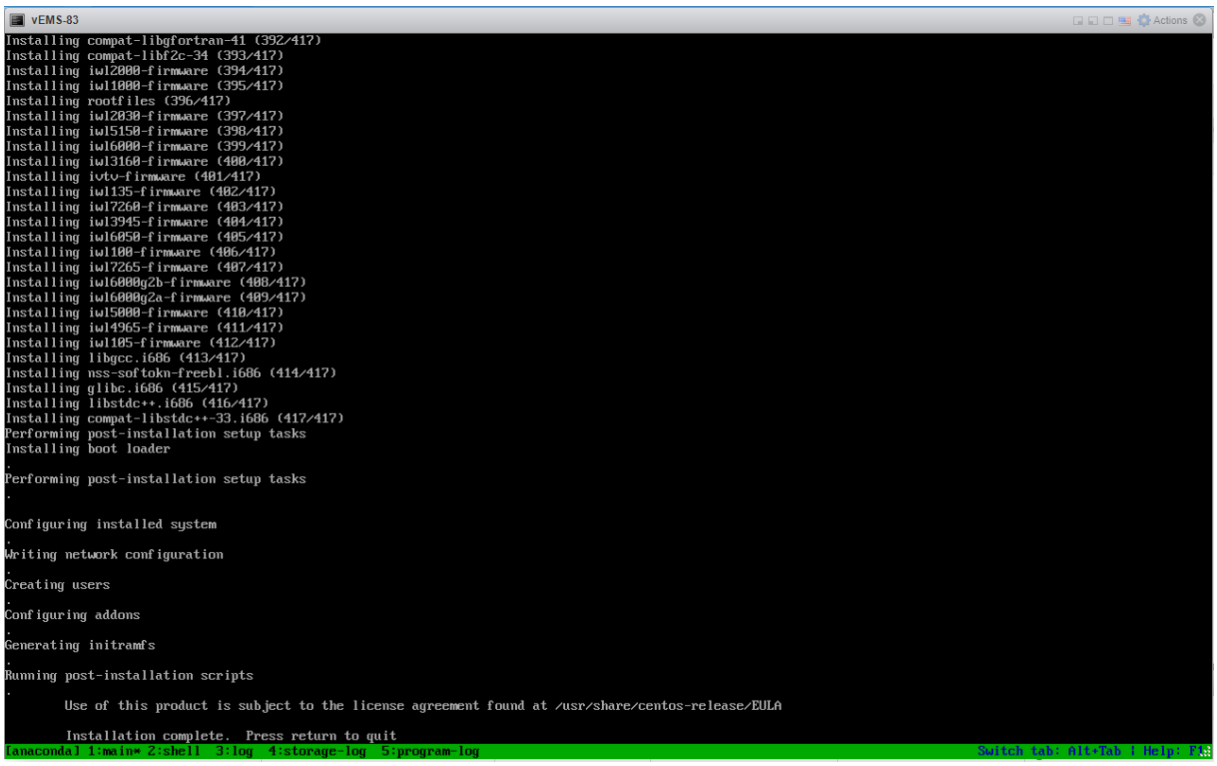


Figure 7-4: CentOS 7



6. Wait for the installation to complete.

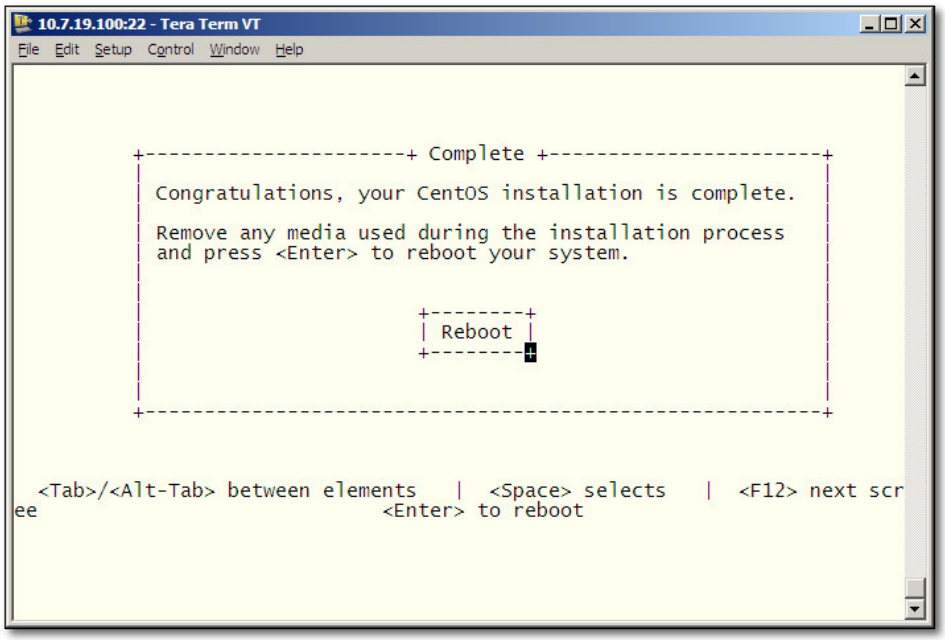
Figure 7-5: CentOS Installation



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.

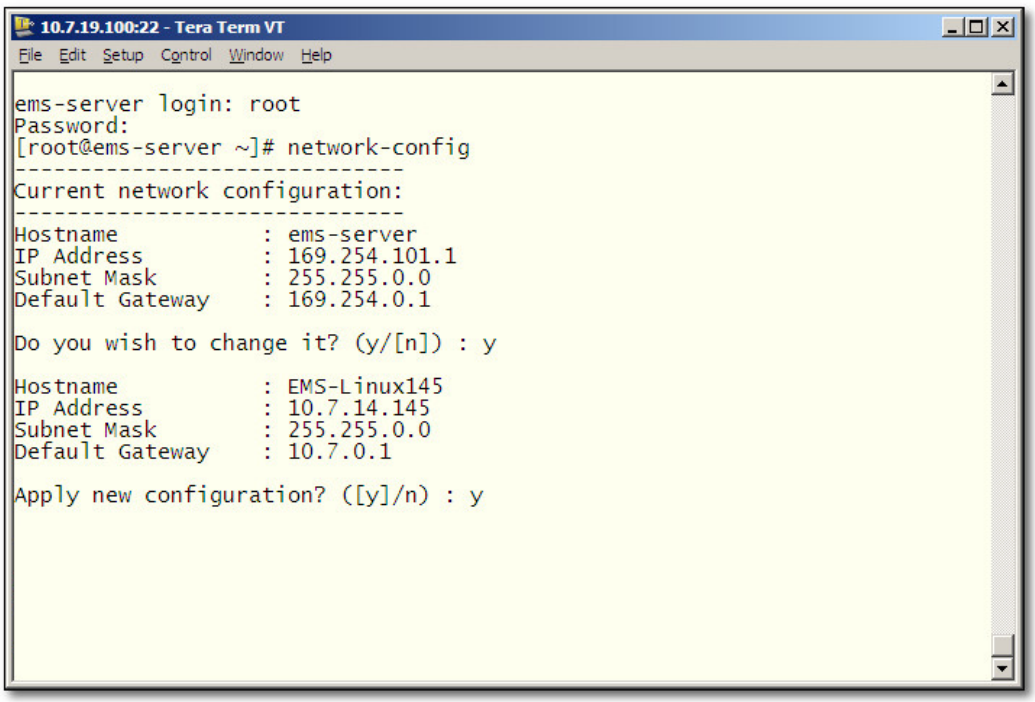
Figure 7-6: Linux CentOS Installation Complete



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



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)

```
[root@EMS-Linux145 /]#
[root@EMS-Linux145 /]# cd /misc/cd
[root@EMS-Linux145 cd]# ./install
Start installValues
Use of uninitialized value in concatenation (.) or string at installValues.pm line 279.
ls: /misc/cd/ac_ems_deploy/: No such file or directory
"my" variable $date masks earlier declaration in same scope at AllSystemChecks.pm line 1302.
Found = in conditional, should be == at ./FastOracleInstall.pl line 120.
Start executing User Login Check script at Sun Oct  3 12:00:19 BST 2010

Login Check Successfully Passed.

>>> Verifying OS version - Sun Oct  3 12:00:20 BST 2010

 ...
        SOFTWARE EVALUATION LICENSE AGREEMENT

YOU  SHOULD READ THE TERMS AND CONDITIONS OF THIS SOFTWARE
EVALUATION  AGREEMENT  CAREFULLY  BEFORE CLICKING "I ACCEPT"
CONVEYING  YOUR ACCEPTANCE OF  THE TERMS  OF THIS LICENSE
AGREEMENT FOR THE AUDIOCODES SOFTWARE (THE "PROGRAM") AND
THE  ACCOMPANYING USER DOCUMENTATION  (COLLECTIVELY,  THE
```

.

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

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

```
8. NO WAIVER. The failure of either party to enforce any rights granted
hereunder or to take action against the other party in the event of any
breach hereunder shall not be deemed a waiver by that party as to
subsequent enforcement of rights or subsequent actions in the event of
future breaches.


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

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 instance.
SQL> ORACLE instance started.

Total System Global Area  321601536 bytes
Fixed Size                  2102168 bytes
Variable Size             251661416 bytes
Database Buffers           62914560 bytes
Redo Buffers                4923392 bytes
SQL>
File created.

SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production
   >>> Restoring database File using RMAN...
 ...
RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN>    >>>

Restore has finished successfully...
 ...
   >>> Please enter a password for the SYS user:  ...
sys
```

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

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

```
 ...
   >>> Start executing Create_DB_Listener_Startup_Scripts at - Thu Sep 16 18:59:07 IST 2010
 ...
chown: /ACEMS/orahome/network/log/listener.log: No such file or directory
   >>>  >>> PASSED
 ...
   >>> Remove Oracle demo directory: /ACEMS/orahome/xdk/demo/java ...
/ACEMS/orahome/xdk/demo/java: No such file or directory
   >>> Remove Oracle demo directory: /ACEMS/orahome/rdbms/demo ...
   >>> !!!!!!!!!!!!!! ORACLE INSTALL SUCCESSFULLY FINISHED !!!!!!!!!!!!!! ...
EMS-Server40#
```

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*.
3. 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)

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

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

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

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

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

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

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


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

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)

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

Hardening Linux OS for DoD STIG compliancy

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

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

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

Press Enter to reboot...
```

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

```
For more information on what data Registration collects and
how it is managed and used, see:
http://java.sun.com/javase/registration/JDKRegistrationPrivacy.html

Press Enter to continue.....
```

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

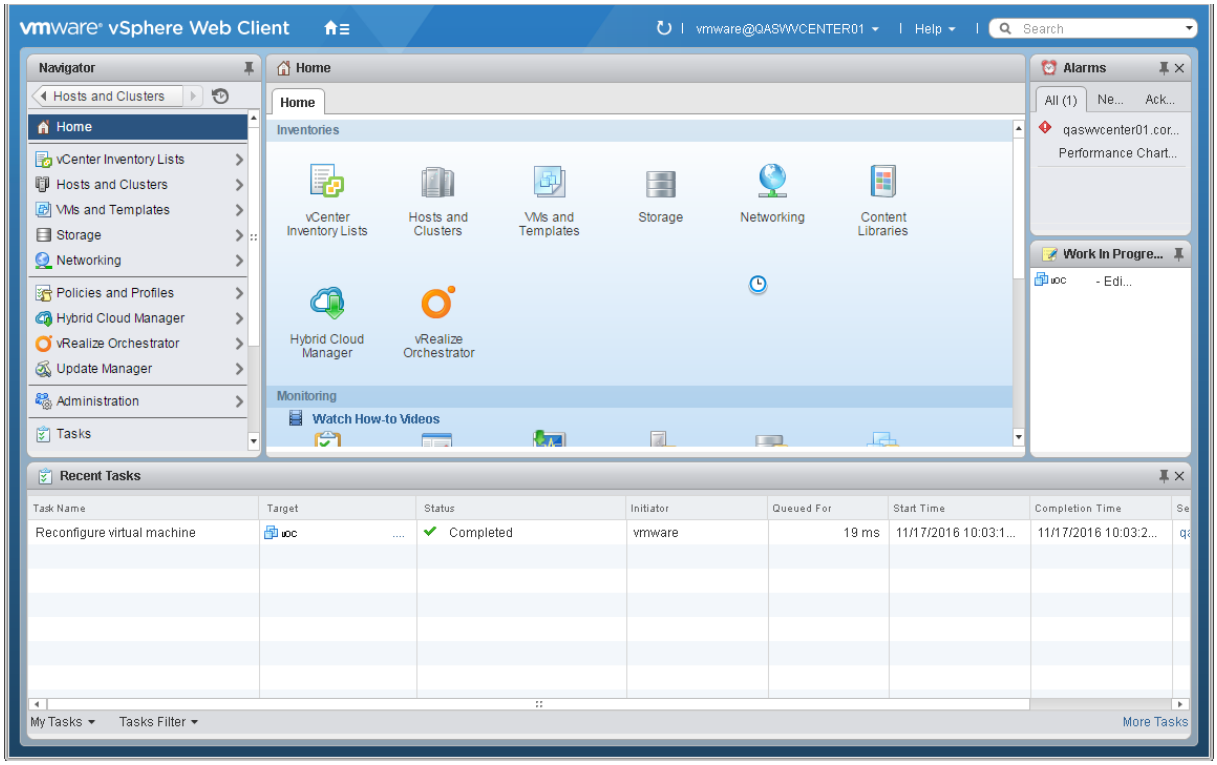
This section describes how to install the OVOC server on the VMware vSphere platform. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Section 7.4.1.2). The upgrade time depends on the hardware machine where 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.

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

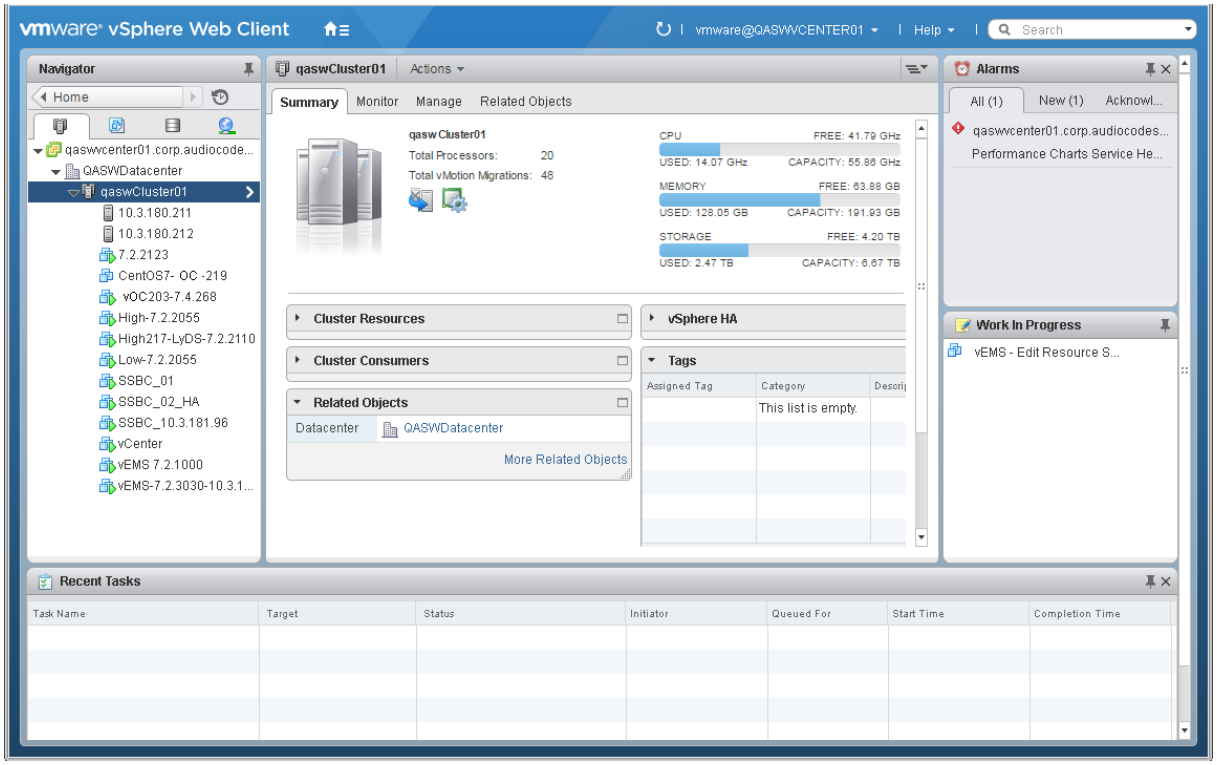
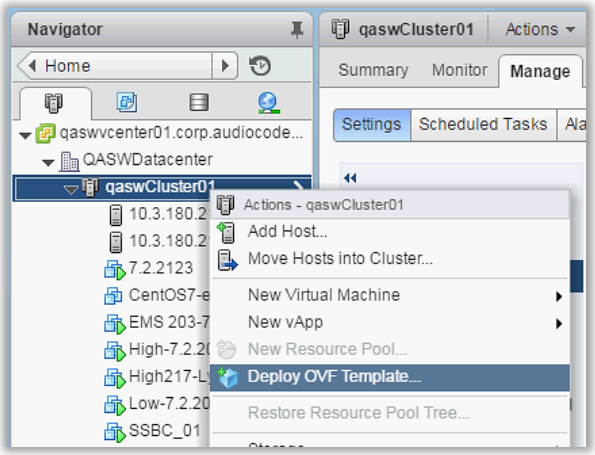


Figure 7-19: Deploy OVF Template Option



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

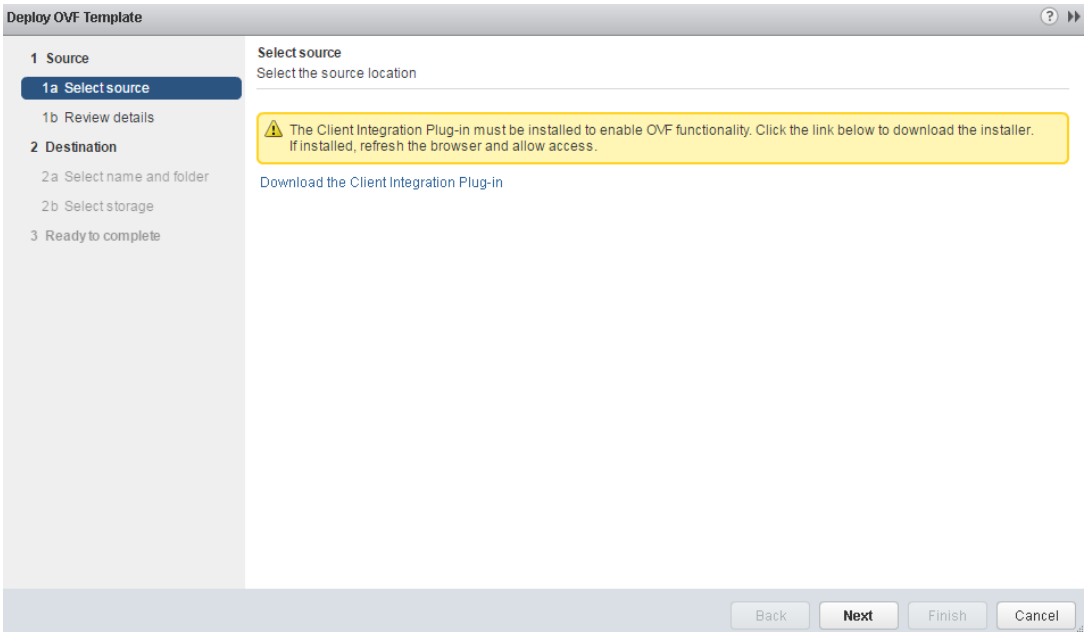
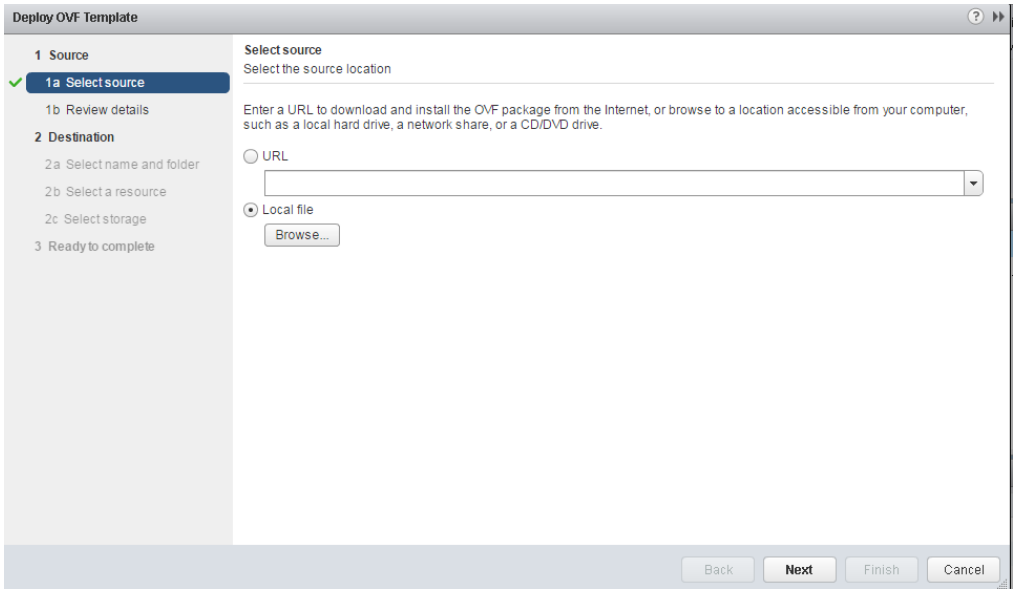
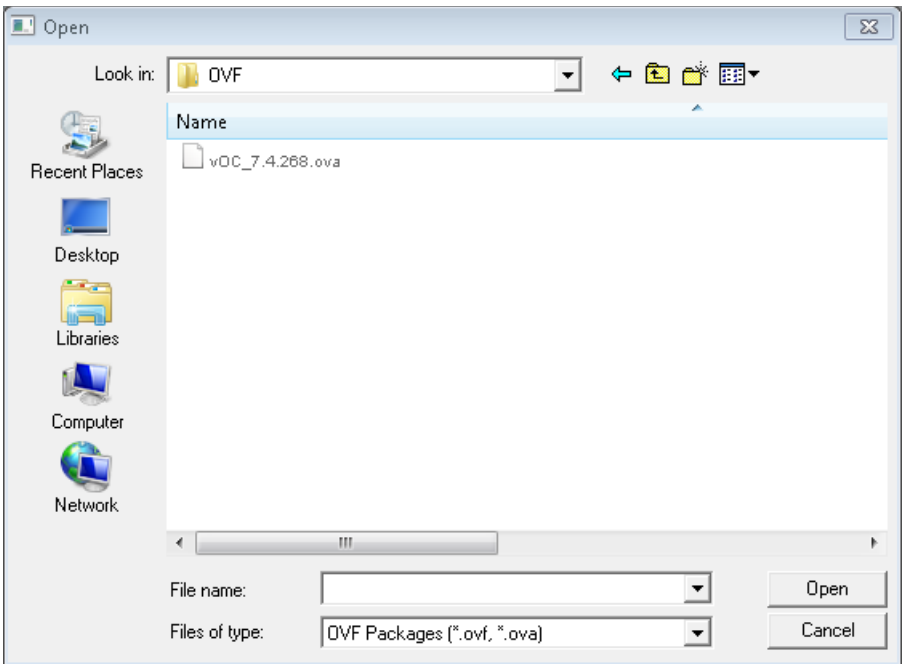


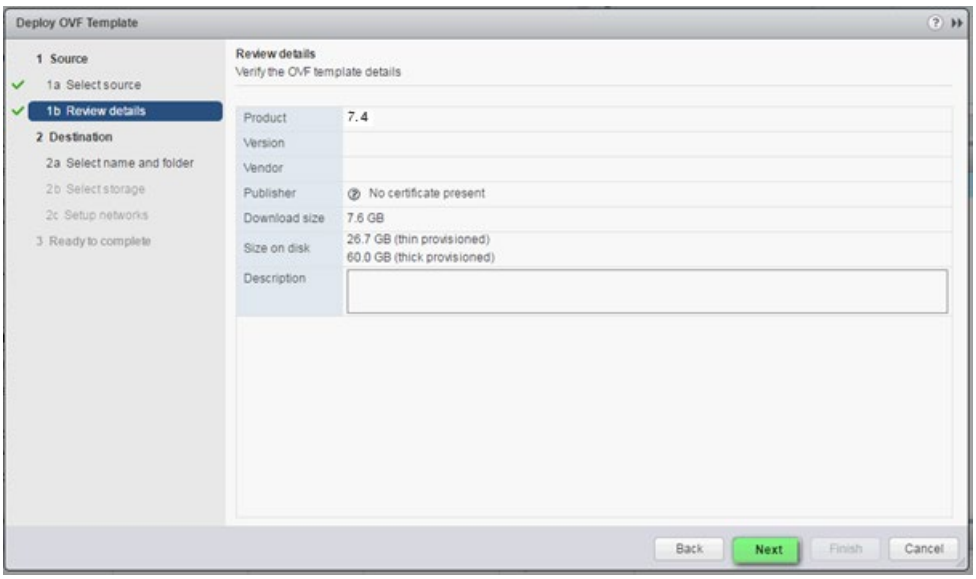
Figure 7-21: Browse to OVF Package





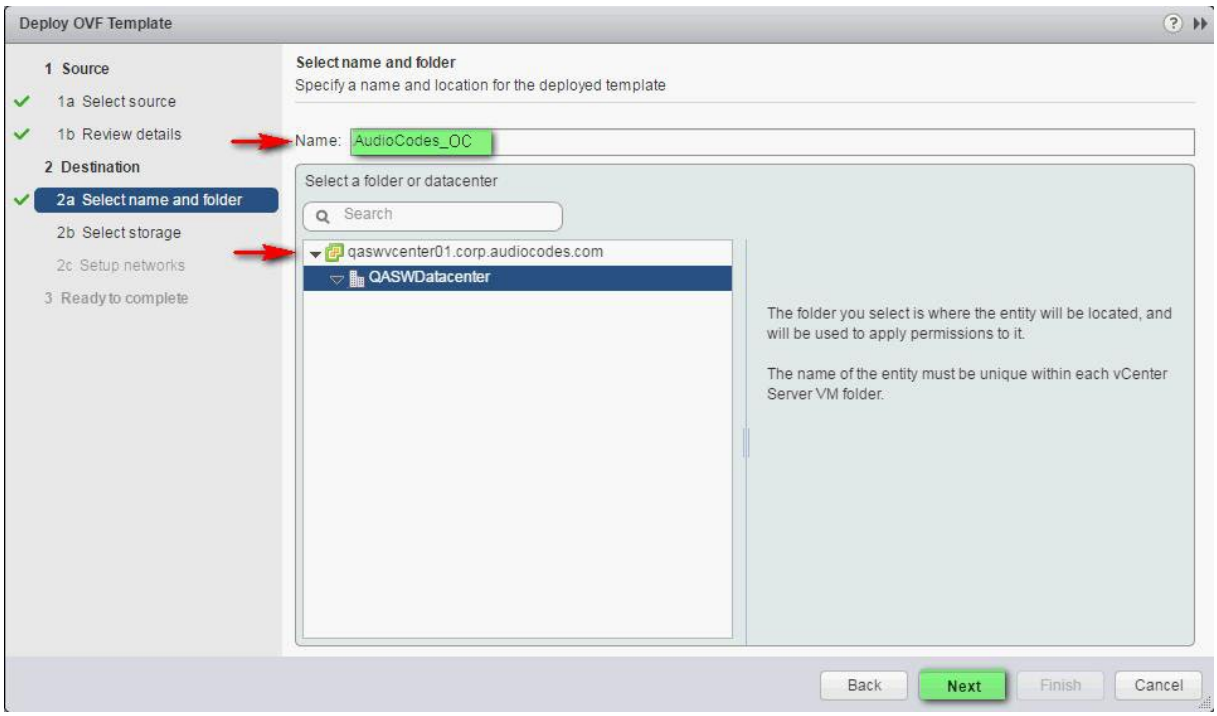
5. Browse to the OVF file with extension OVA that you saved to your PC, and click **Next**.

Figure 7-22: OVF Template Details Screen



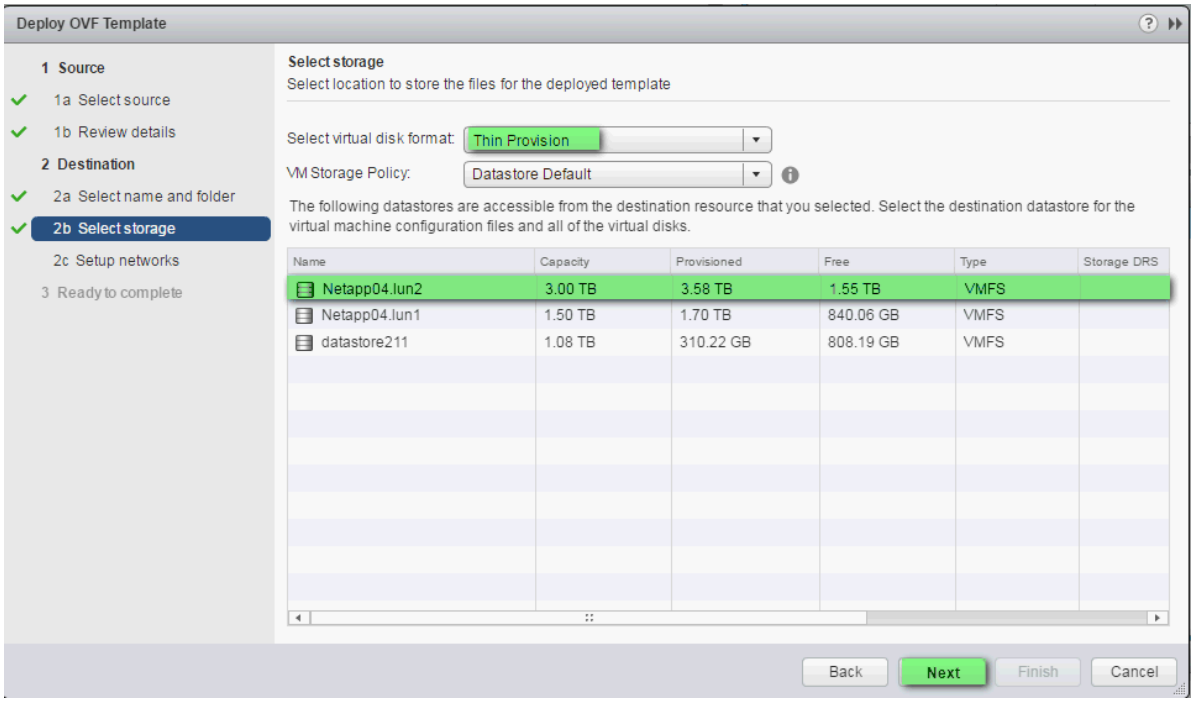
6. In the OVF Template Details screen, click **Next**.

Figure 7-23: Virtual Machine Name and Location Screen



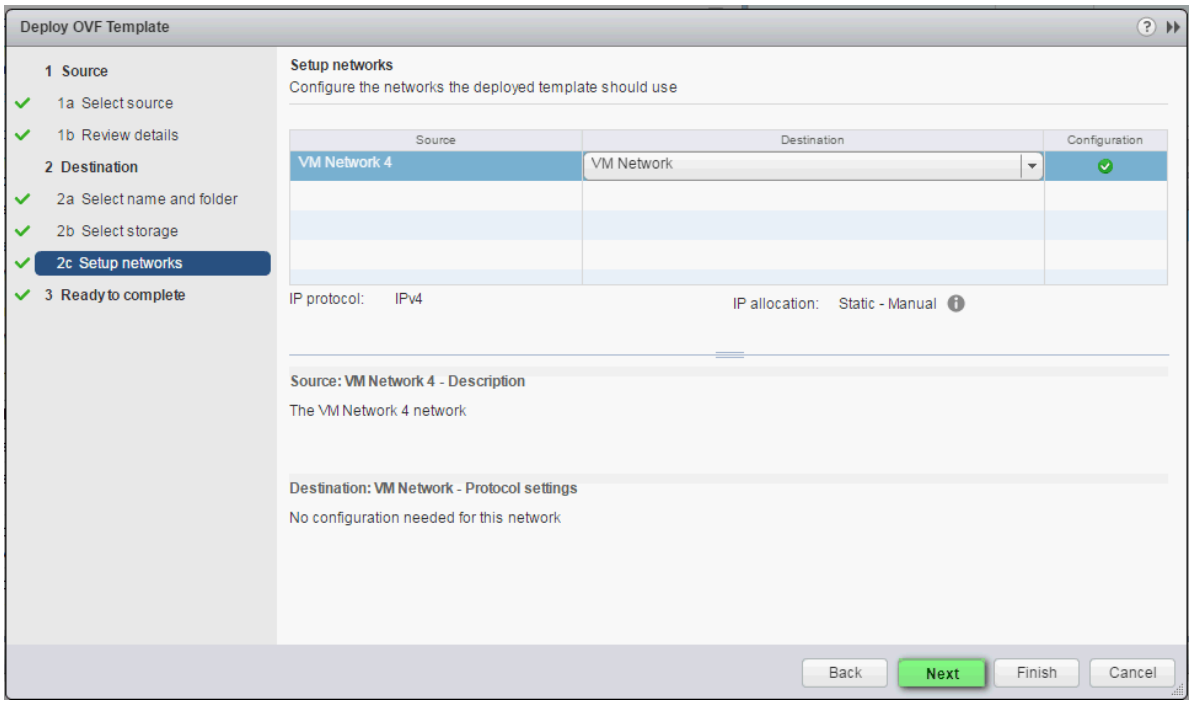
7. In the Name and Location screen, enter the desired virtual machine name and choose the inventory location (the Data Center to locate the machine), and then click **Next**.

Figure 7-24: Destination Storage Screen



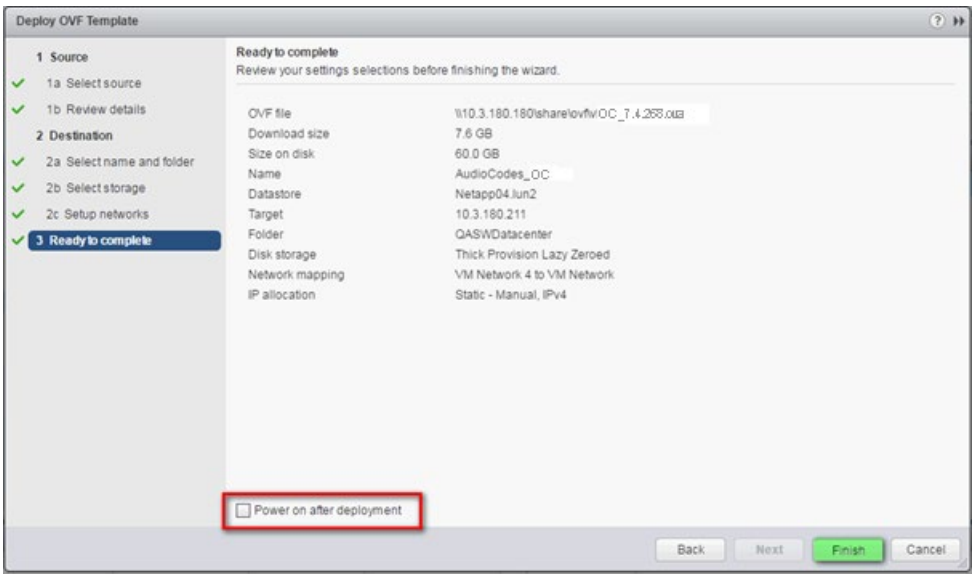
8. In the Storage screen, do the following:
   - Select Virtual Disk Format- choose the desired provisioning option ('Thin Provisioning' is recommended),
   - Select the data store where wish to locate your machine, and click **Next**.

Figure 7-25:: Setup Networking Screen



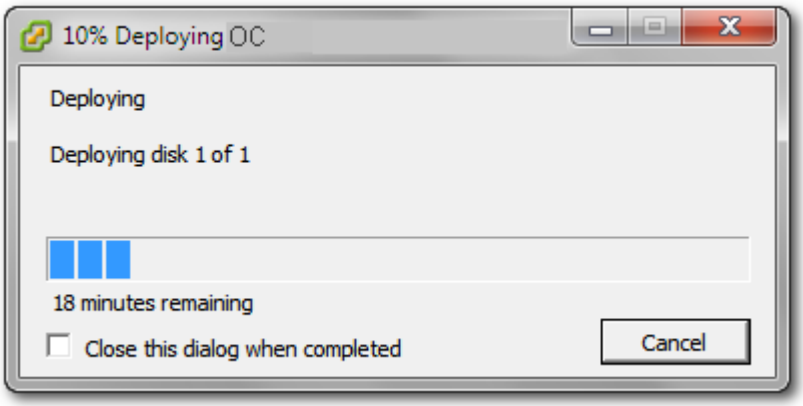
9. In the Network setup screen, select the network where the deployed template should apply, and click **Next**.

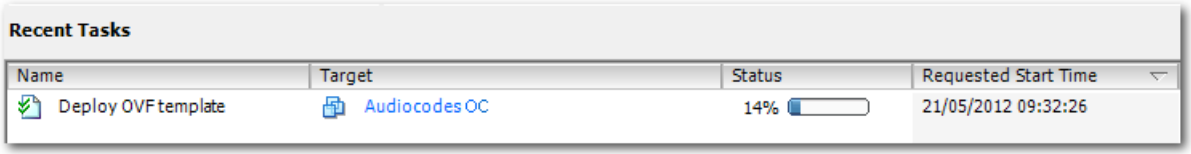
Figure 7-26: Ready to Complete Screen

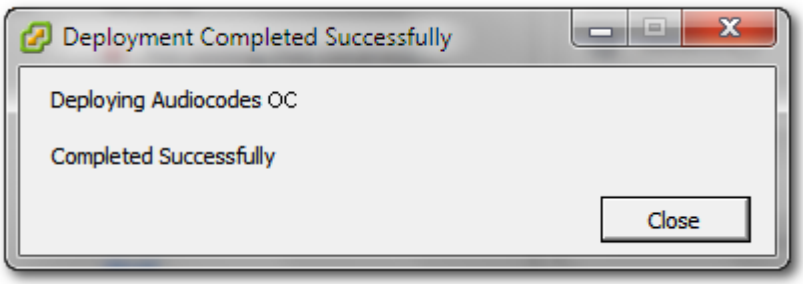


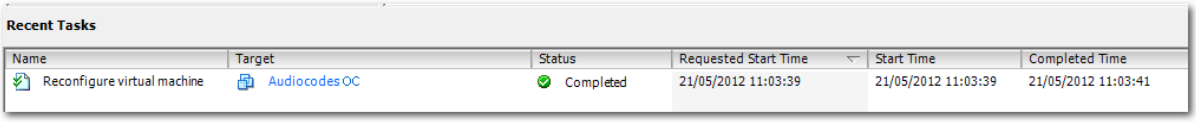
10. In the Ready to Complete screen, ensure the option 'Power on after deployment' is not selected, and click **Finish**.

Figure 7-27: Deployment Progress Screen









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*.

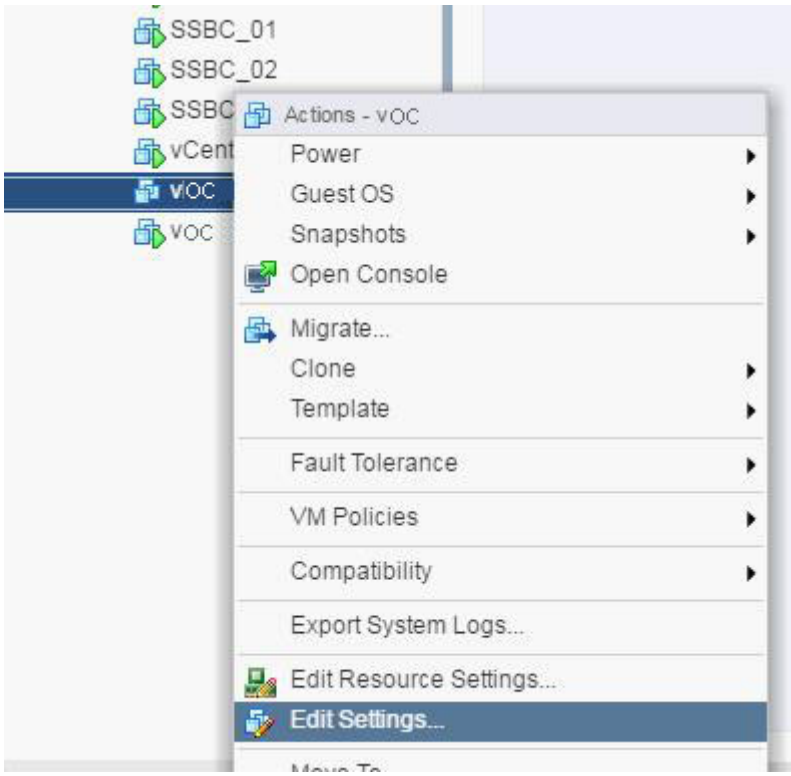
Table 7-1: VMware Virtual Machine Settings

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:**

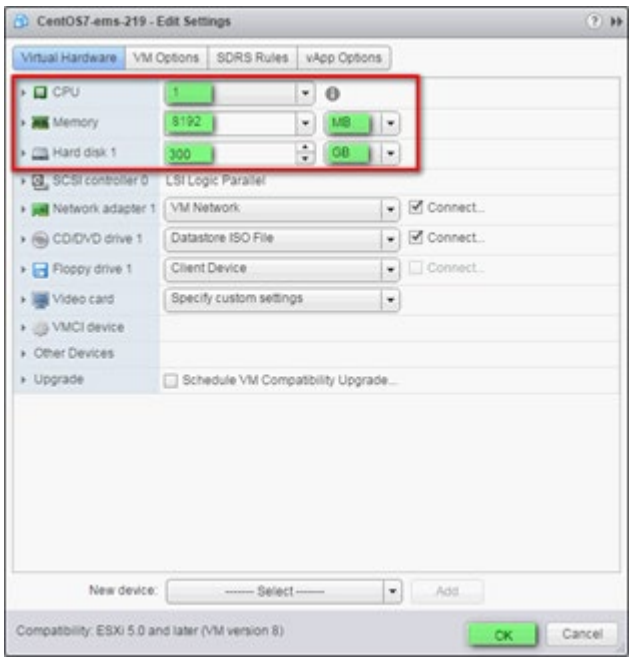
1. Before powering up the machine, go to the virtual machine **Edit Settings** option.

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**.

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

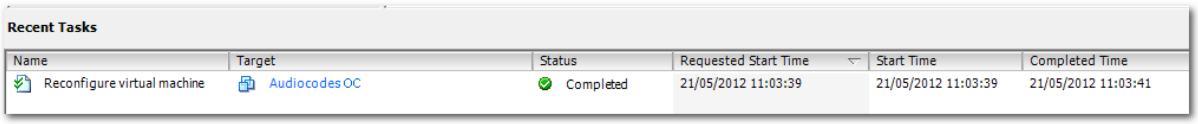


Note:

- 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

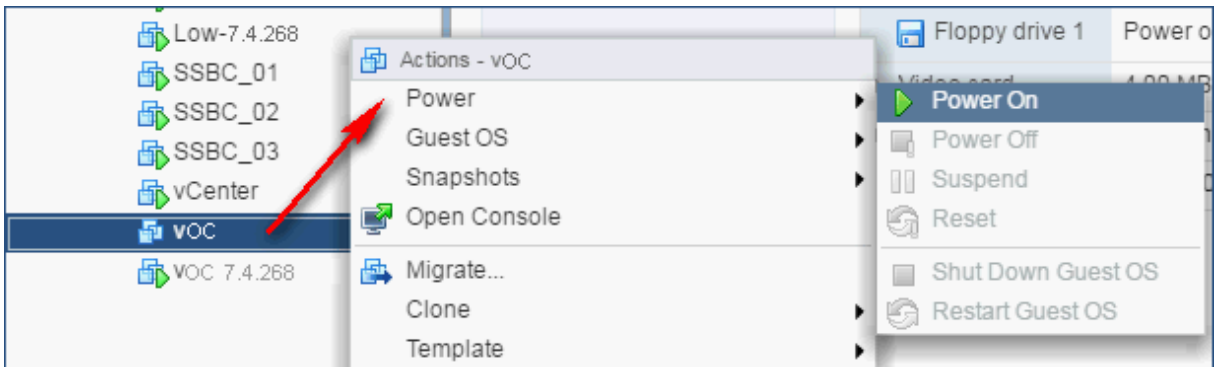
7.4.1.3 Connecting OVOC Server to Network

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:**

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

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

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

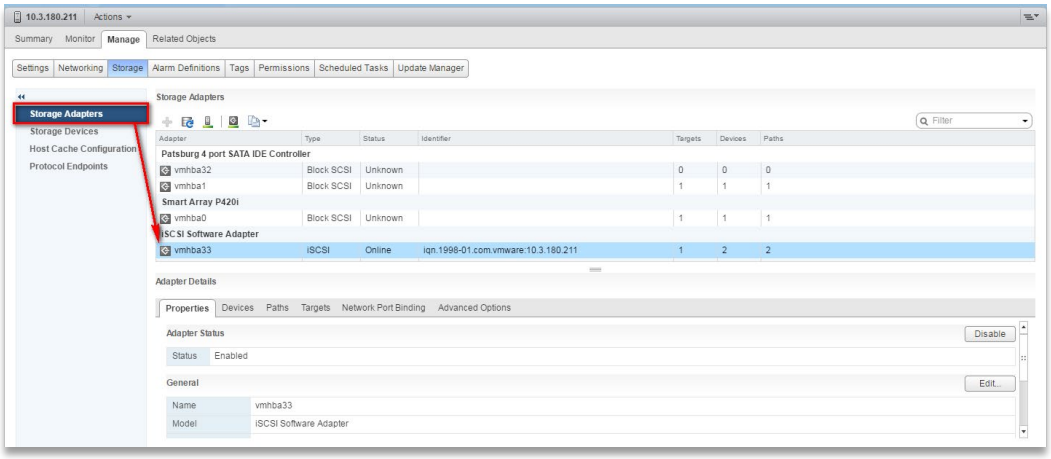
7.4.1.4.1 Site Requirements

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.

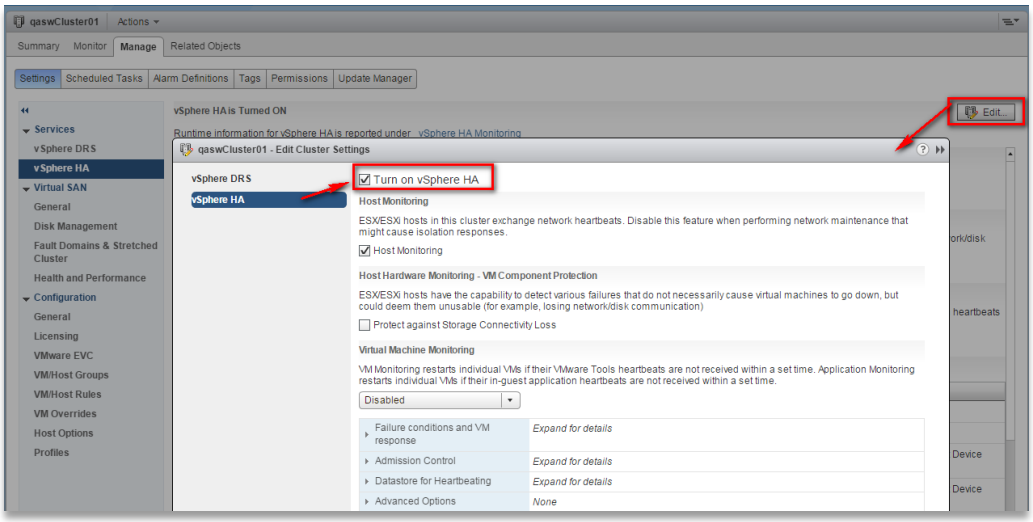
  For example, a datastore “QASWDatacenter” which contains a cluster named “qaswCluster01” and is combined of two ESXi servers (see figure below).
- Verify that Shared Storage is defined and mounted for all cluster members:

Figure 7-32: Storage Adapters



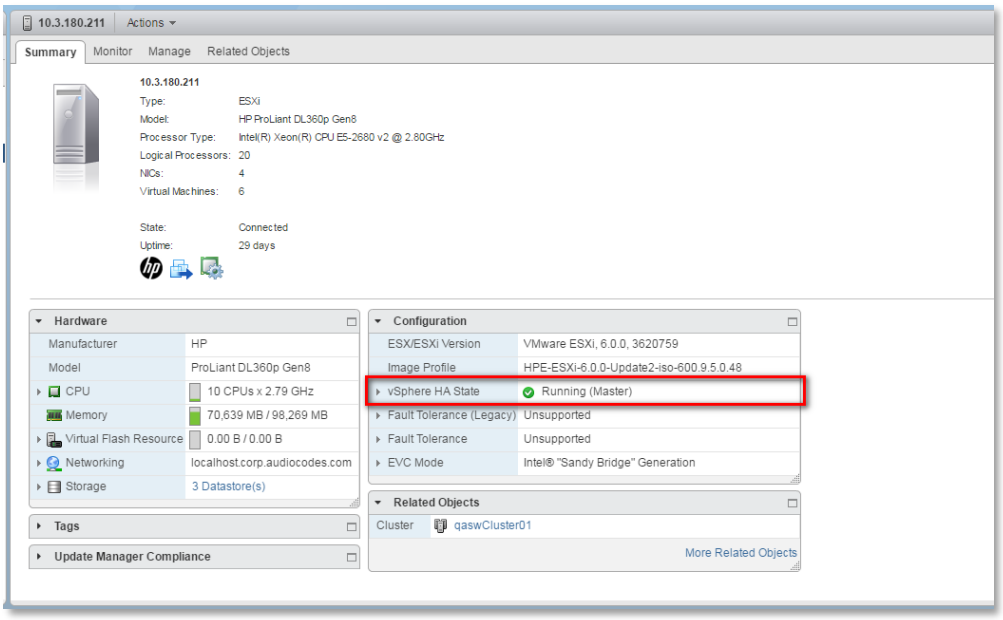
- Ensure that the 'Turn On vSphere HA' check box is selected:

Figure 7-33:Turn On vSphere HA



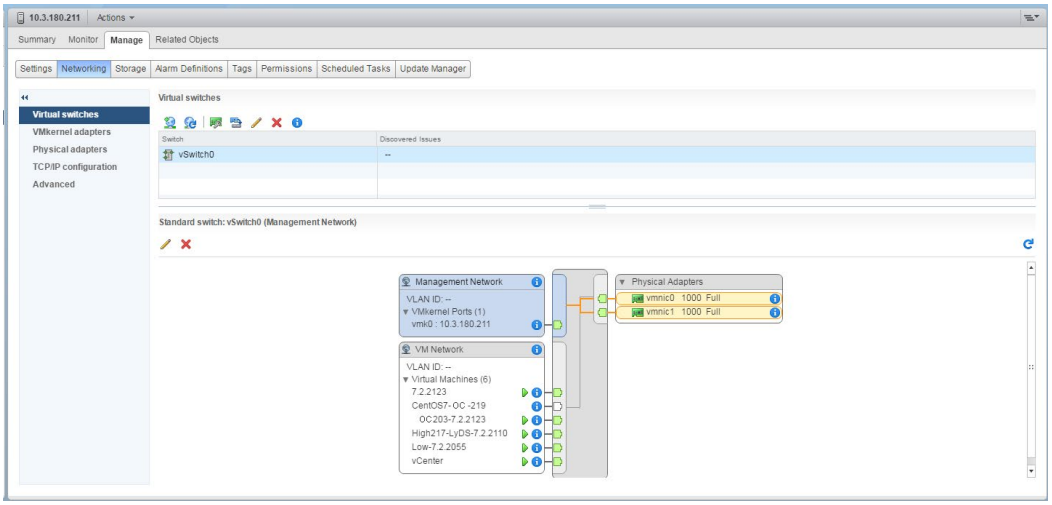
- Ensure that HA is activated on each cluster node:

Figure 7-34: Activate HA on each Cluster Node



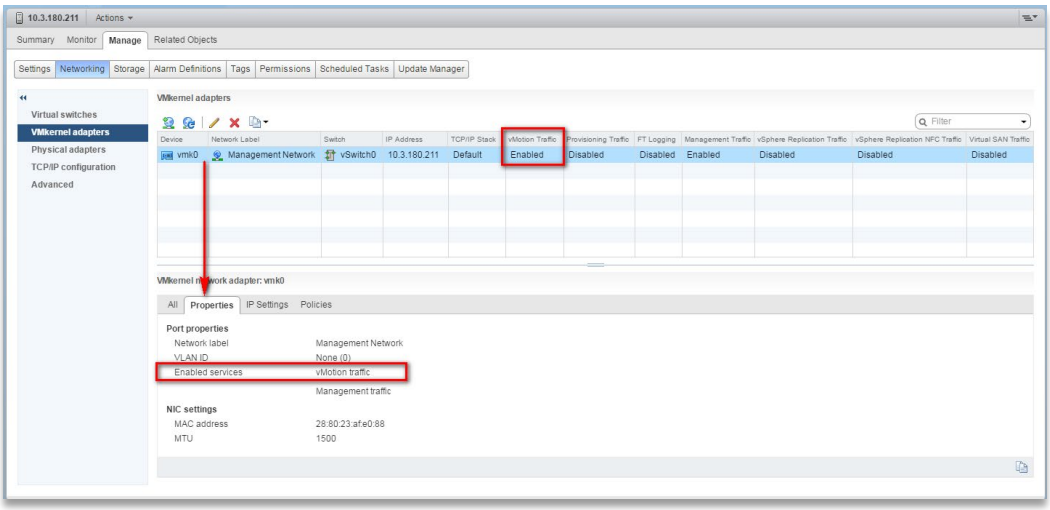
- Ensure that the networking configuration is identical on each cluster node:

Figure 7-35: Networking



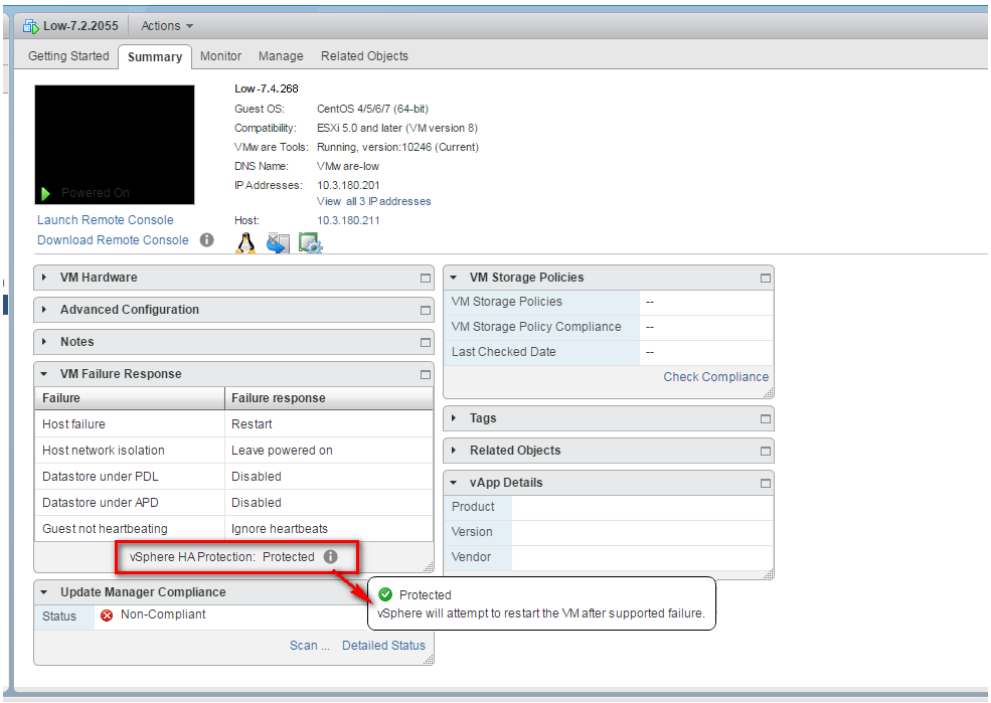
- Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

Figure 7-36: 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



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

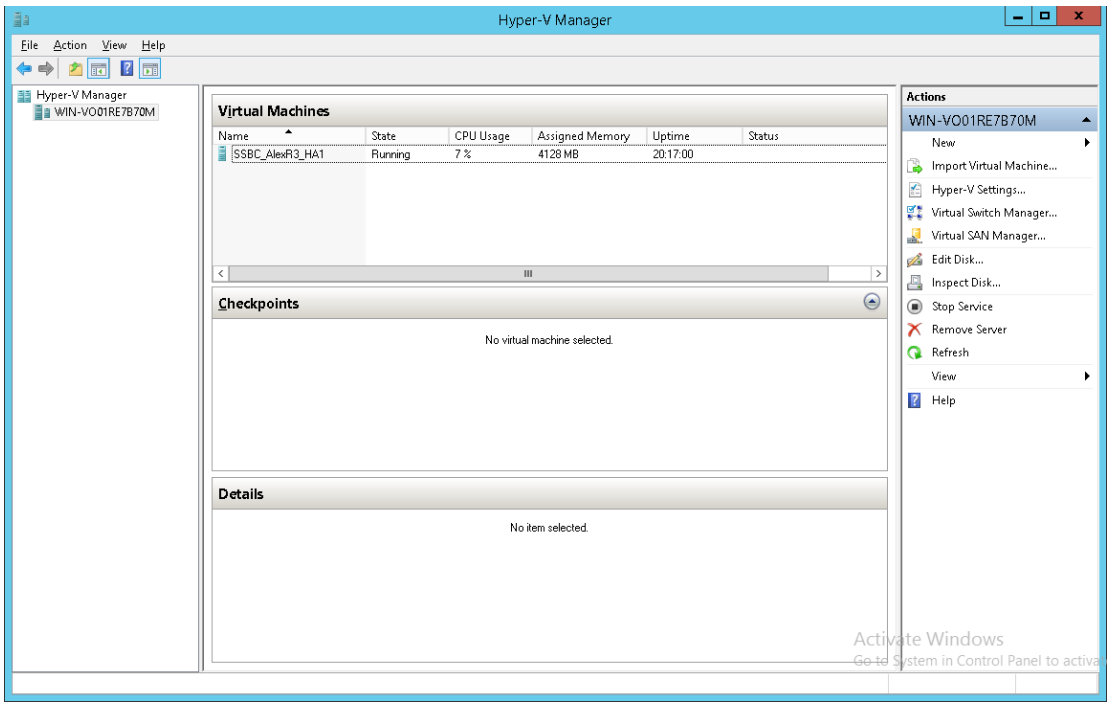
The OVOC server is distributed as a VM image Zip file (see Section 7.1.2).

➢ **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).

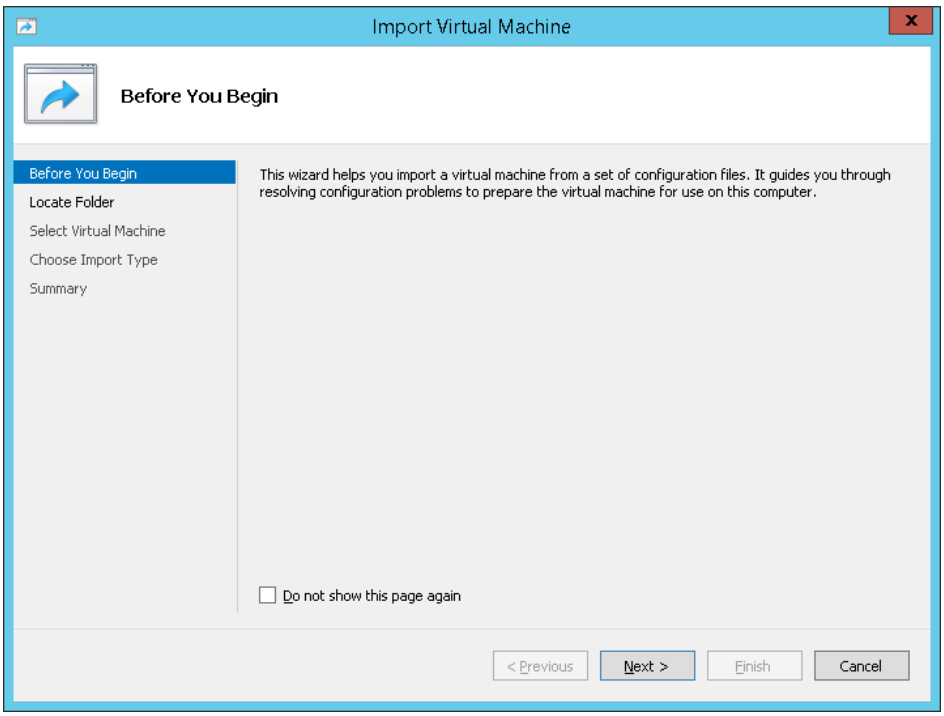
2. Open Hyper-V Manager by clicking **Start** > **Administrative Tools** > **Hyper-V Manager**; the following screen opens:

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



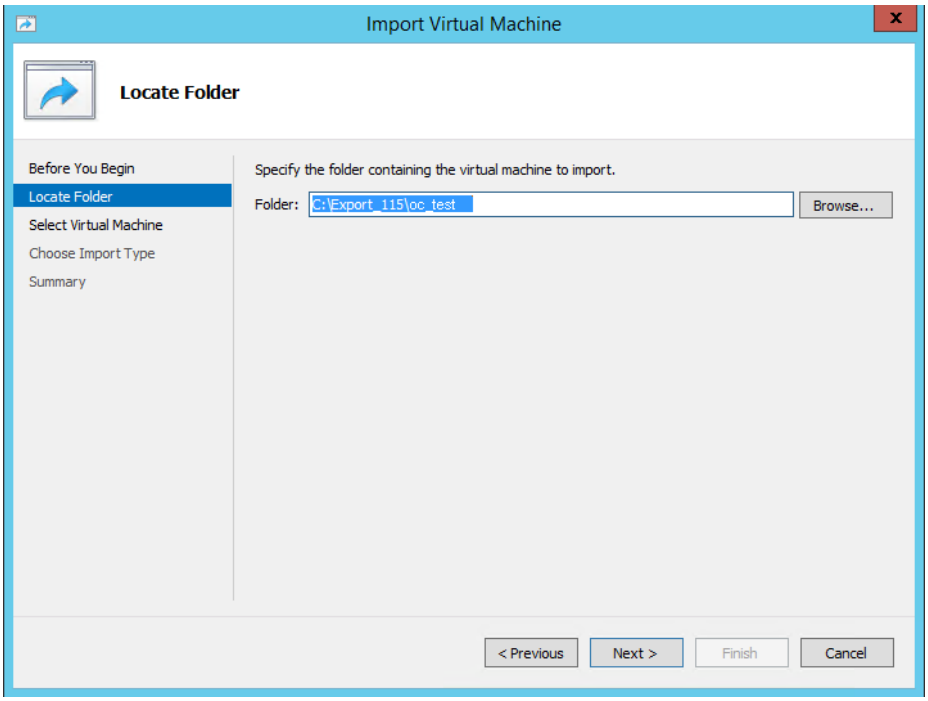
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

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



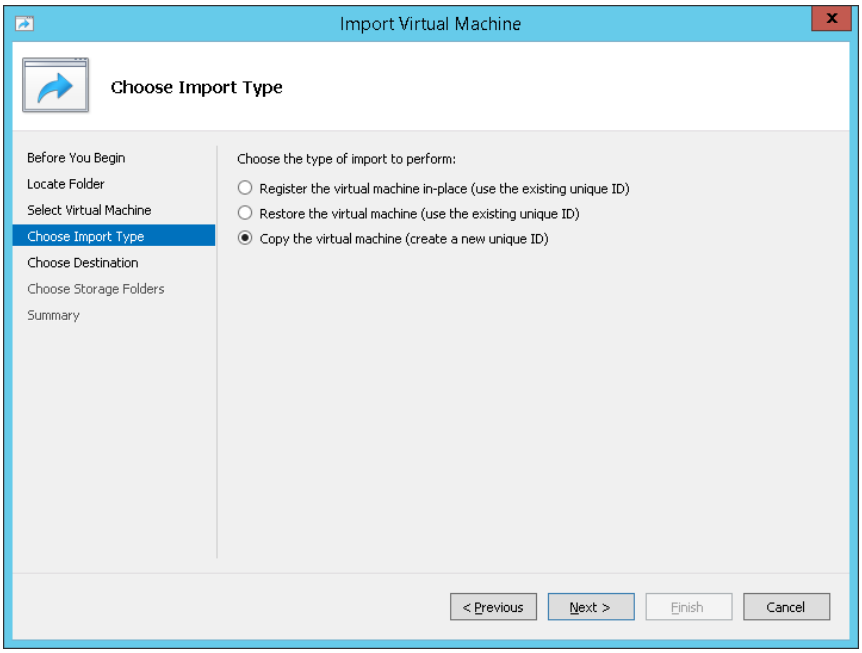
4. Click **Next**; the Locate Folder screen opens:

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



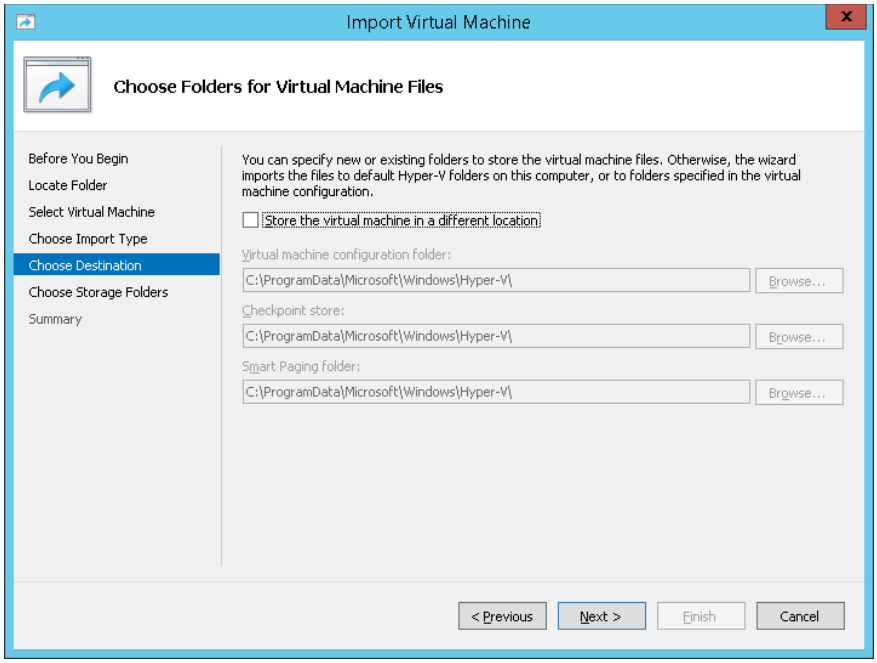
5. Enter the location of the VM installation folder, which was previously extracted, from the zip file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

Figure 7-413: Installing OVOC server on Hyper-V – Choose Import Type



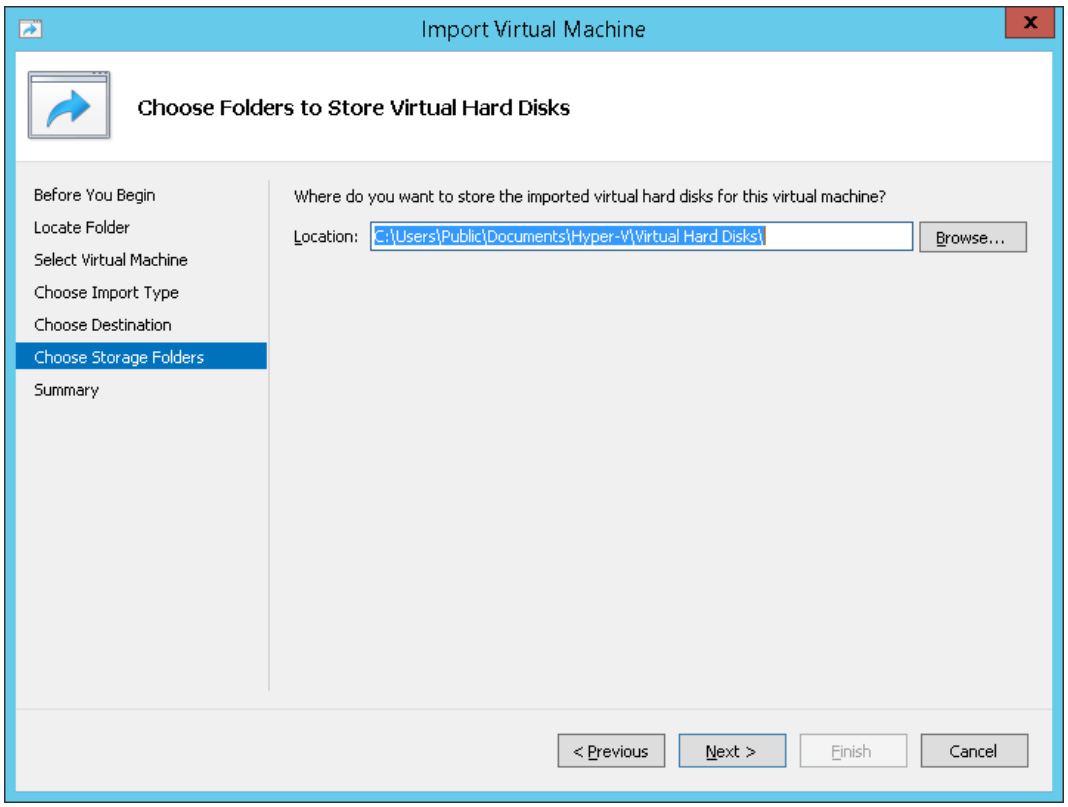
7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

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



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

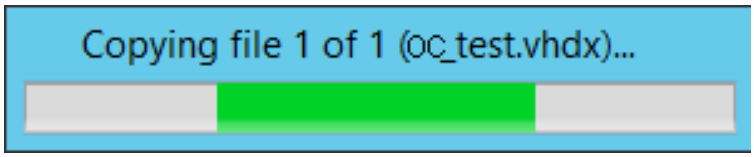
Figure 7-435: Installing OVOC server on Hyper-V – Choose Storage Folders



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.*

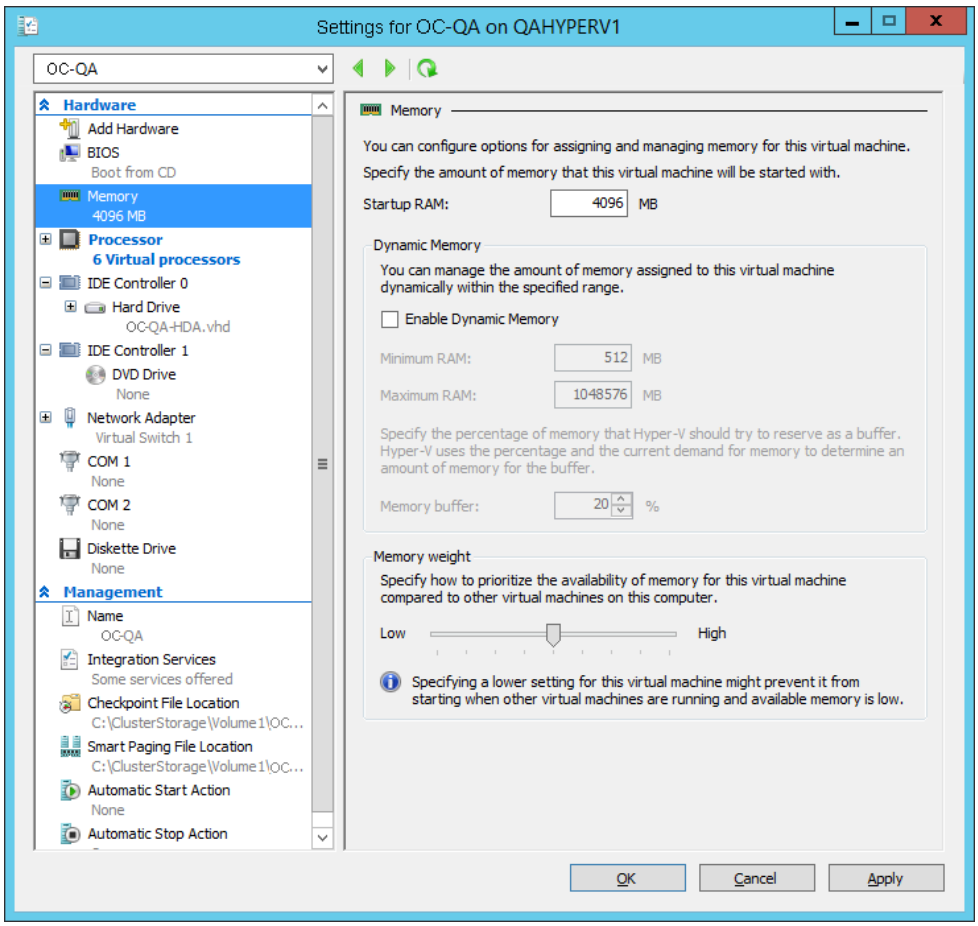
Table 7-2: Microsoft Hyper-V Virtual Machine Settings

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:

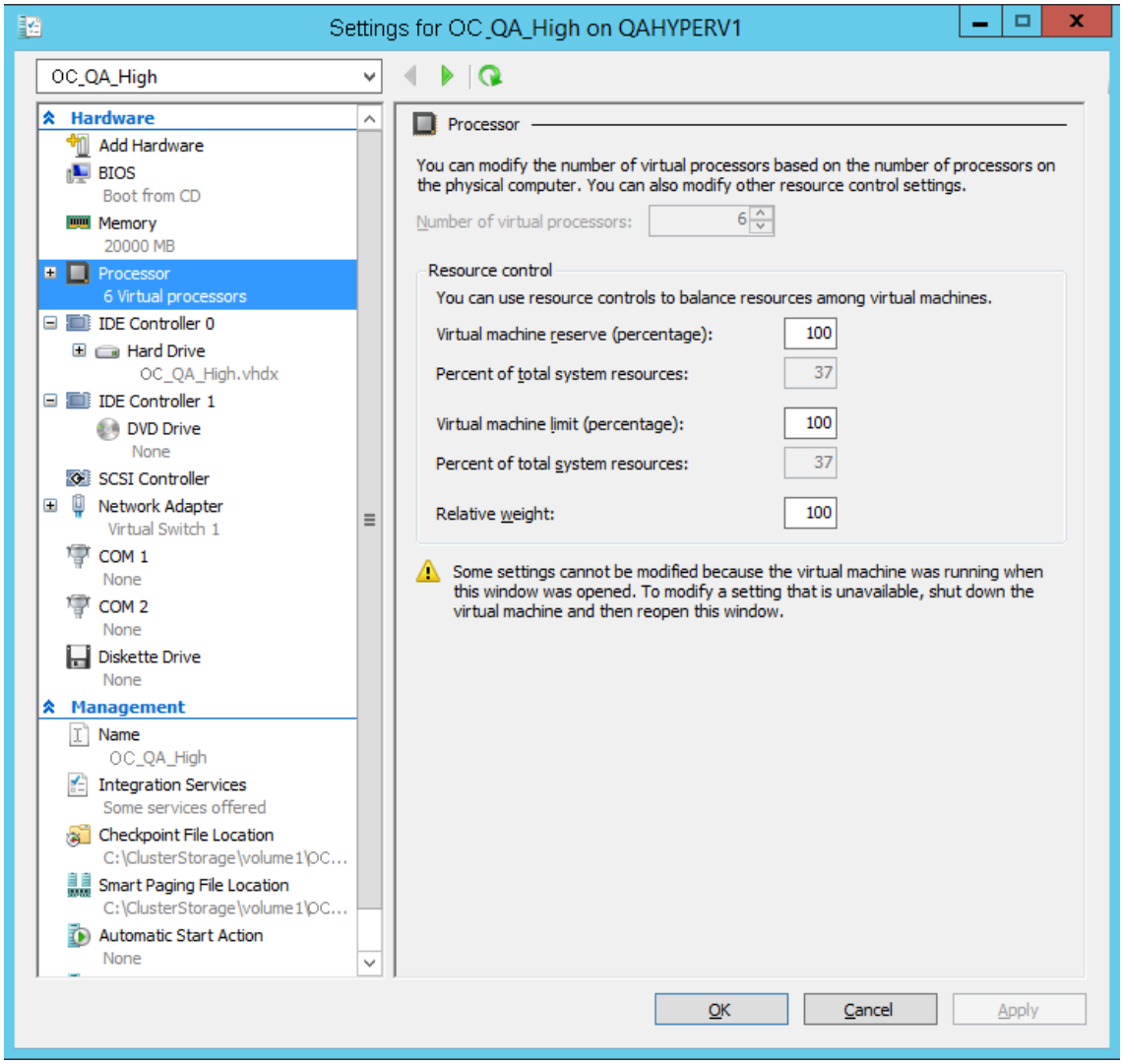
1. Locate the new OVOC server VM in the tree in the Hyper-V Manager, right-click it, and then select Settings; the Virtual Machine Settings screen opens:

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



2. In the Hardware pane, select **Memory**, as shown above, enter the 'Startup RAM' parameter as required, and then click **Apply**.
3. In the Hardware pane, select **Processor**; the Processor screen shown in the figure below opens.

Figure 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).

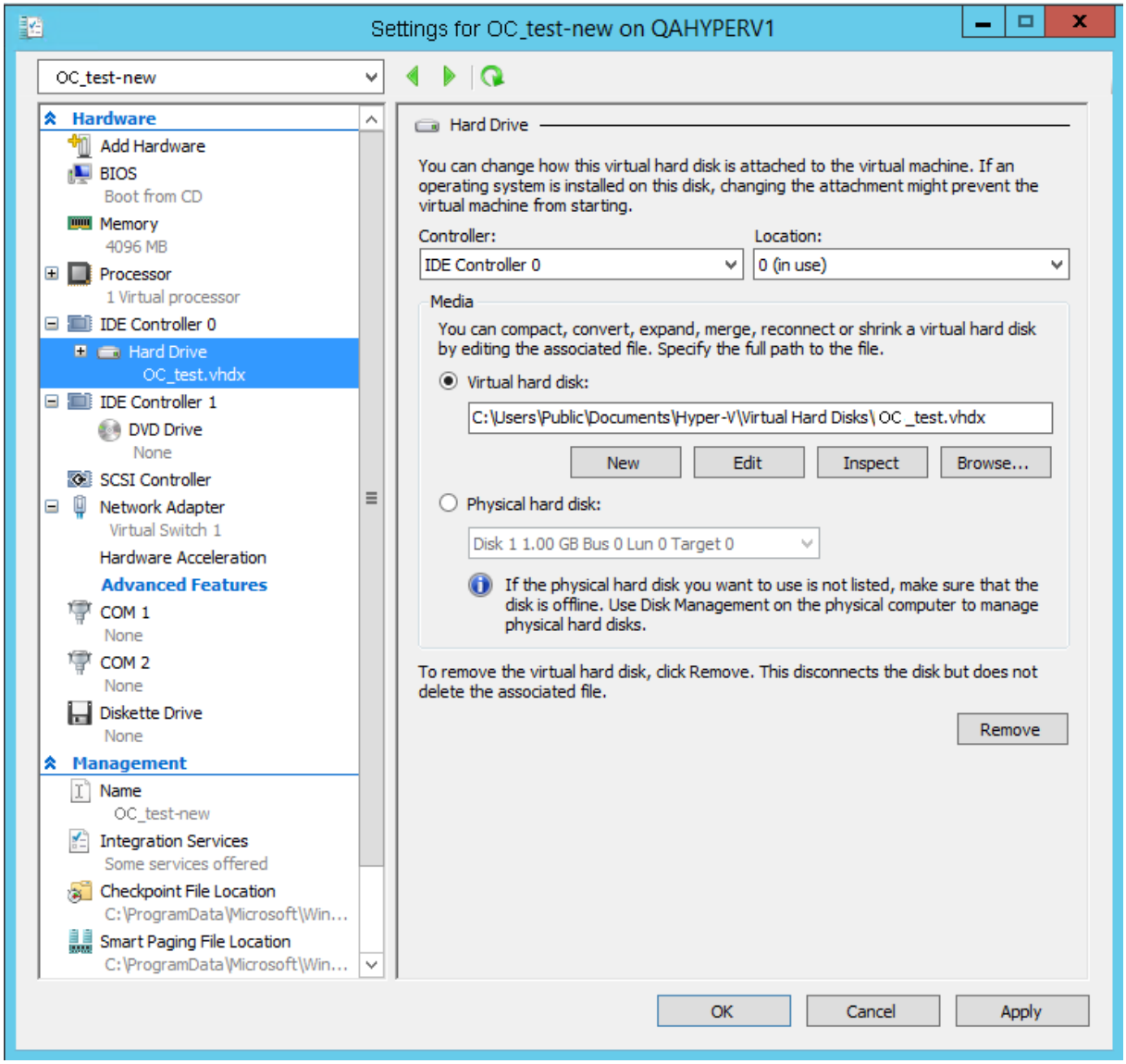
7.4.2.2.1 Expanding Disk Capacity

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:**

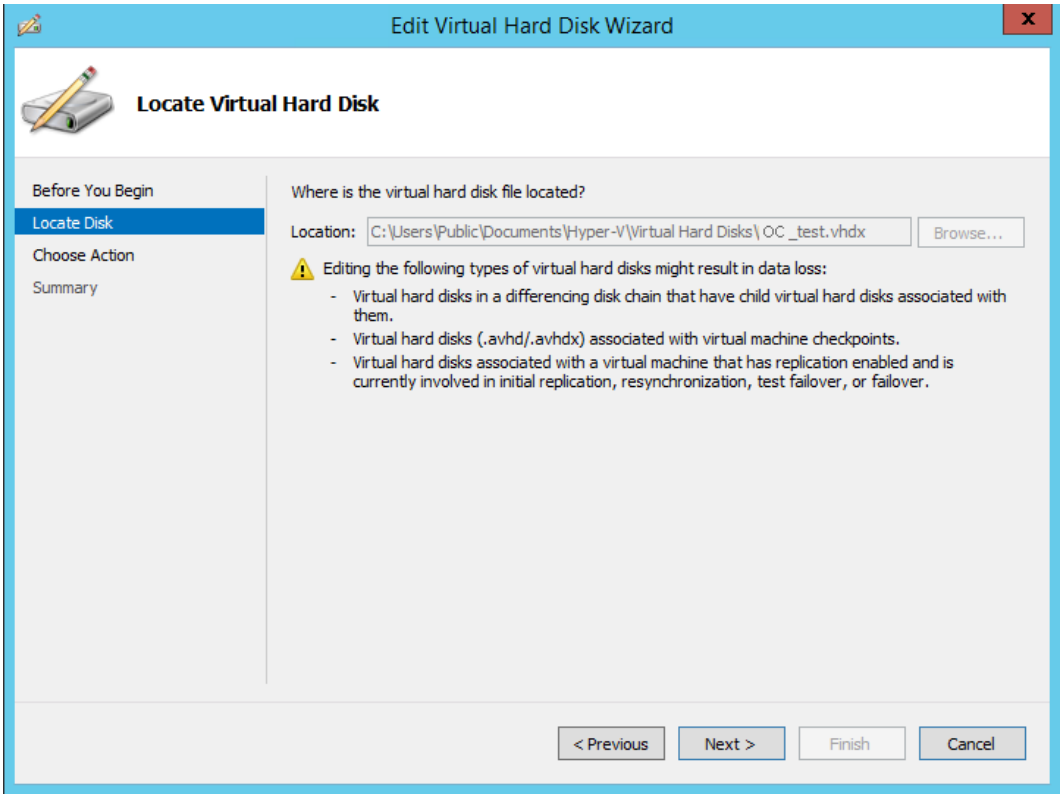
1. Make sure that the target OVOC server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

Figure 7-47: Expanding Disk Capacity



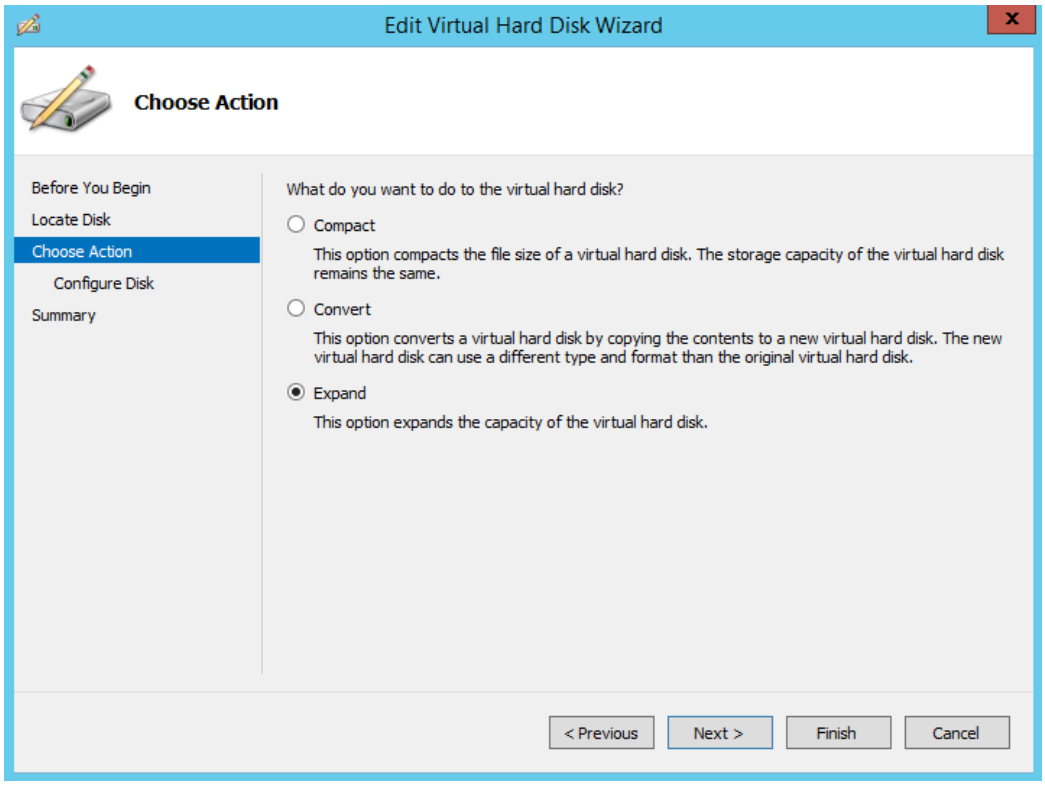
The Edit Virtual Disk Wizard is displayed as shown below.

Figure 7-48: Edit Virtual Hard Disk Wizard



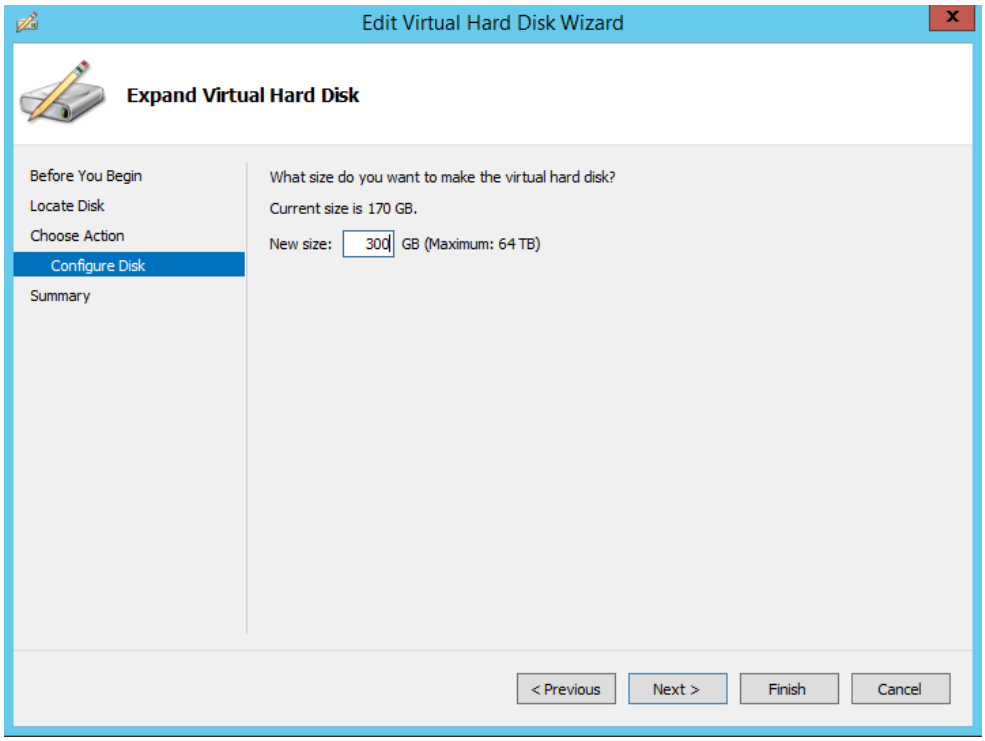
3. Click **Next**; the Choose Action screen is displayed:

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



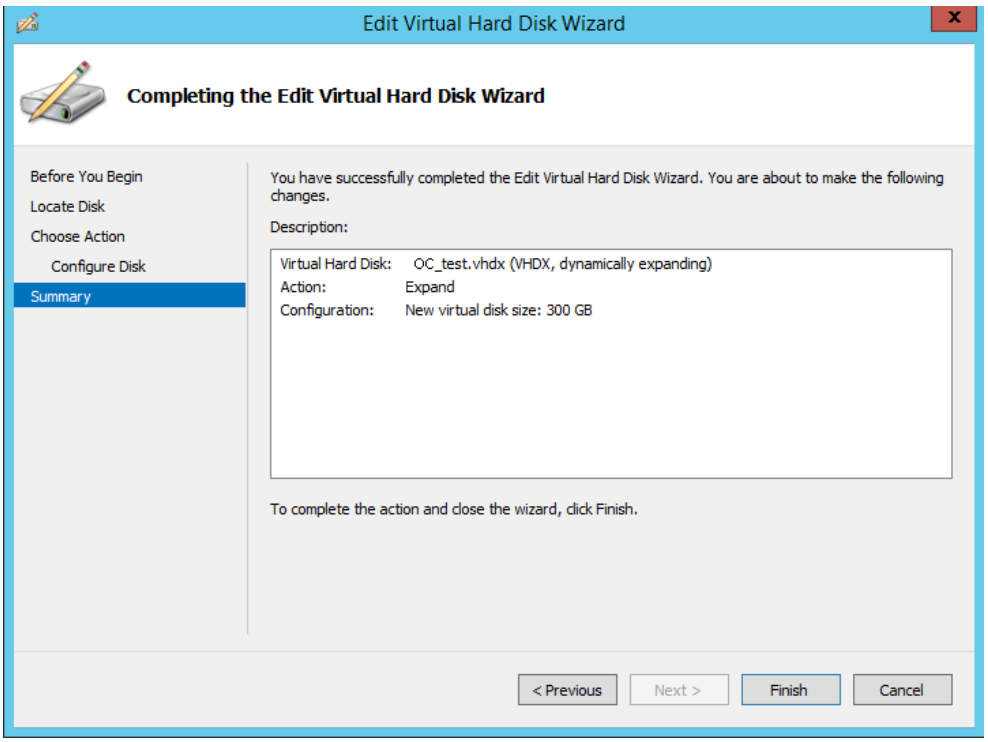
4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

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



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



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'

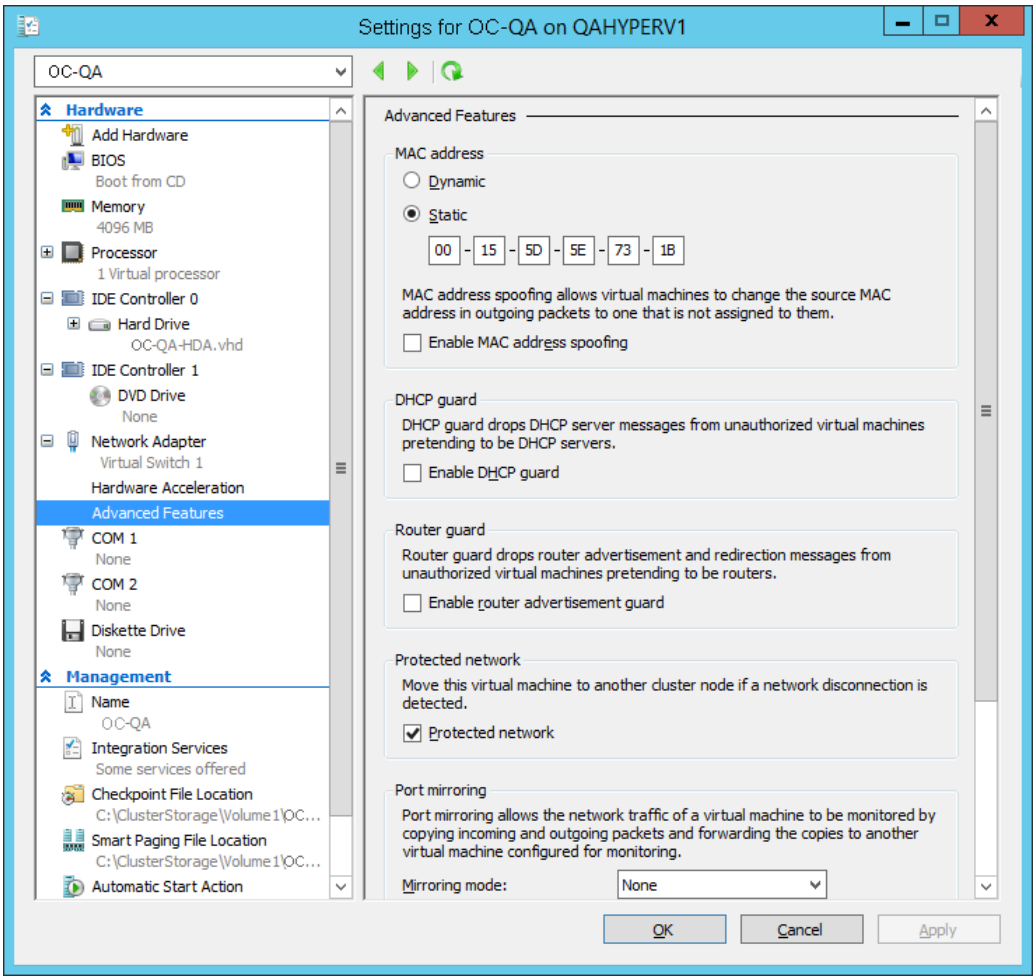
By default, the MAC addresses of the OVOC server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license.

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



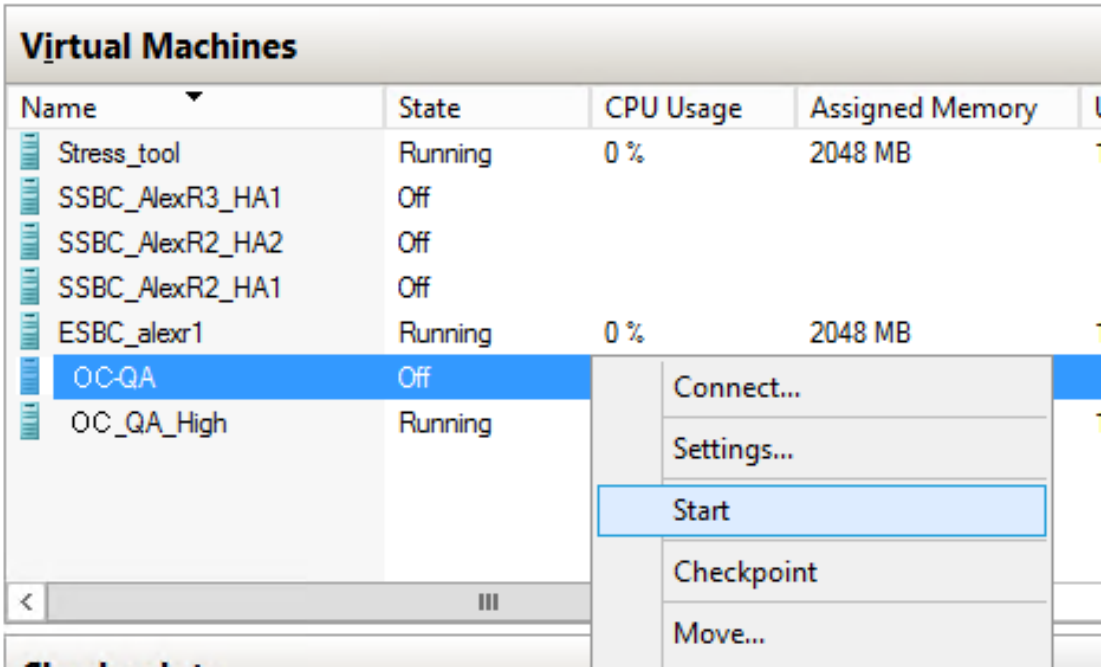
7.4.2.4 Connecting OVOC Server to Network

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:**

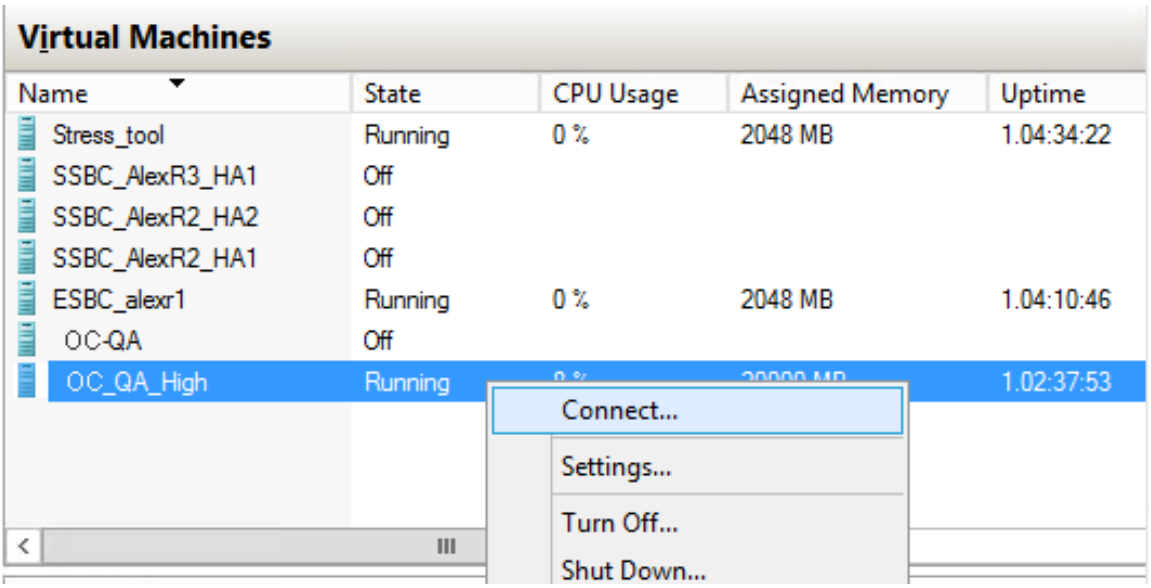
1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

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



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

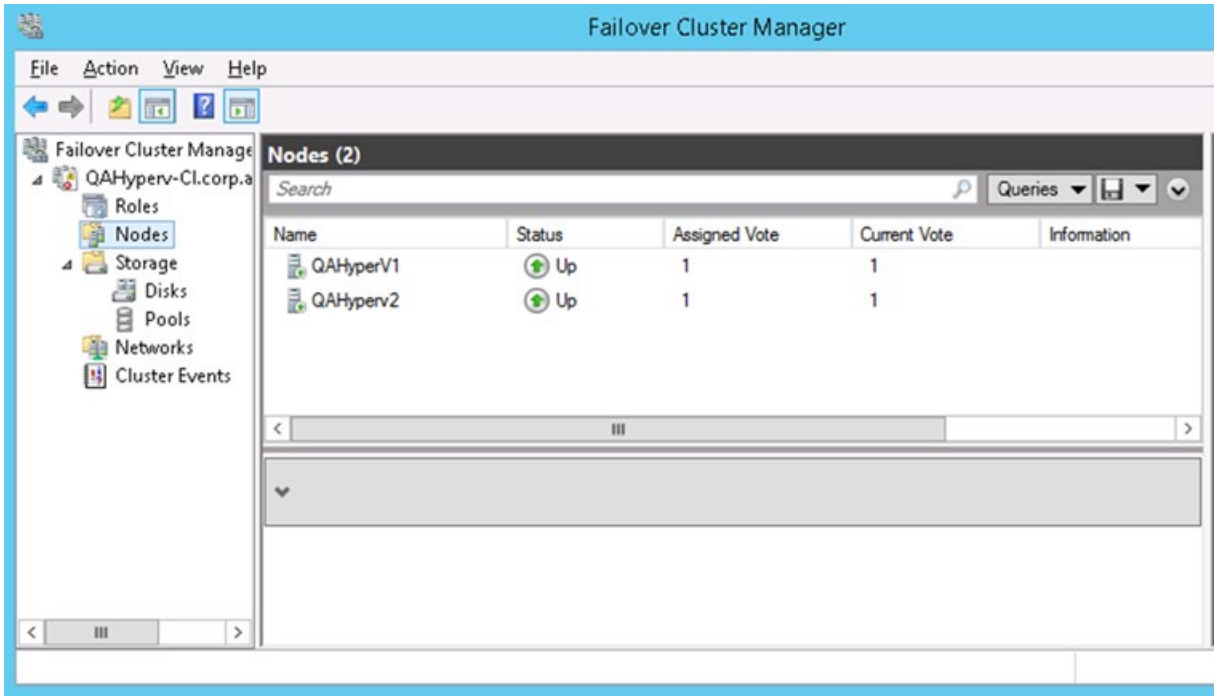
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

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.

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.

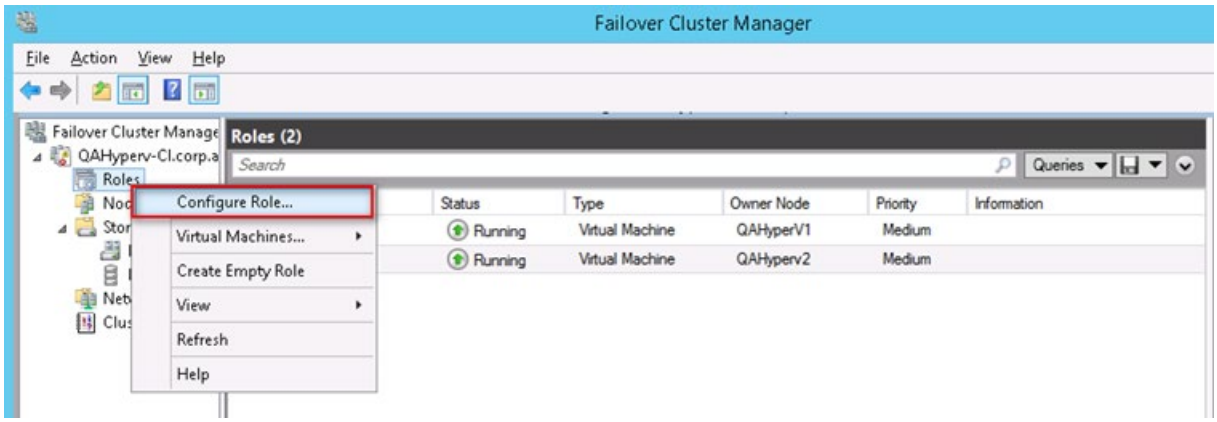
7.4.2.5.2 Add the OVOC VM in Failover Cluster Manager

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:**

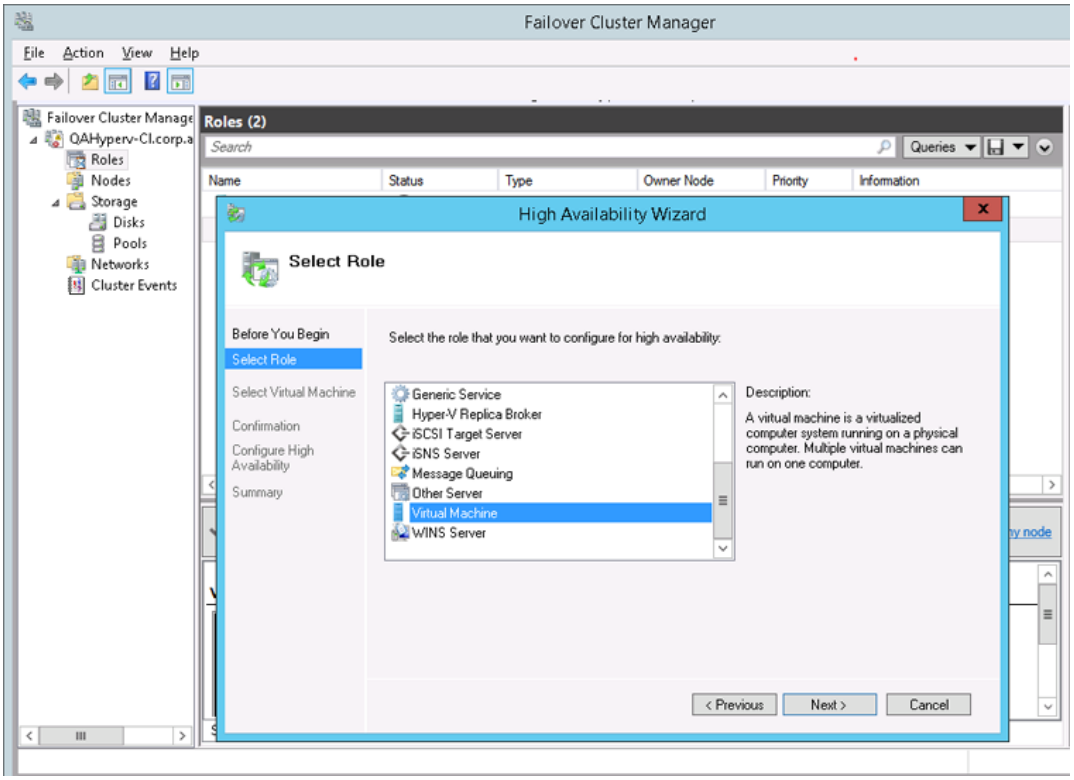
1. Right-click “Roles” and in the pop up menu, choose **Configure Role**:

Figure 7-56: Configure Role



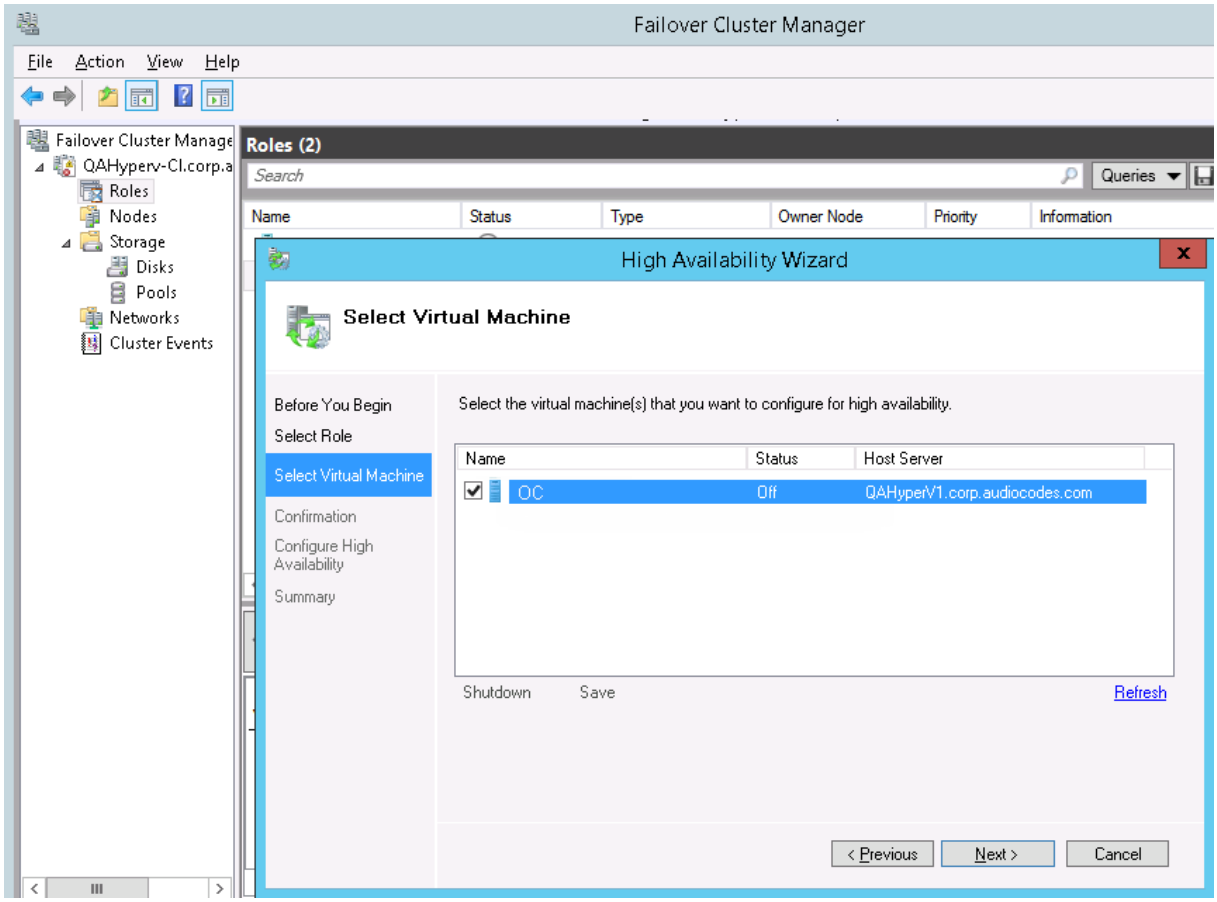
2. In the Select Role window, select the **Virtual Machine** option and then click **Next**.

Figure 7-57: Choose Virtual Machine



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

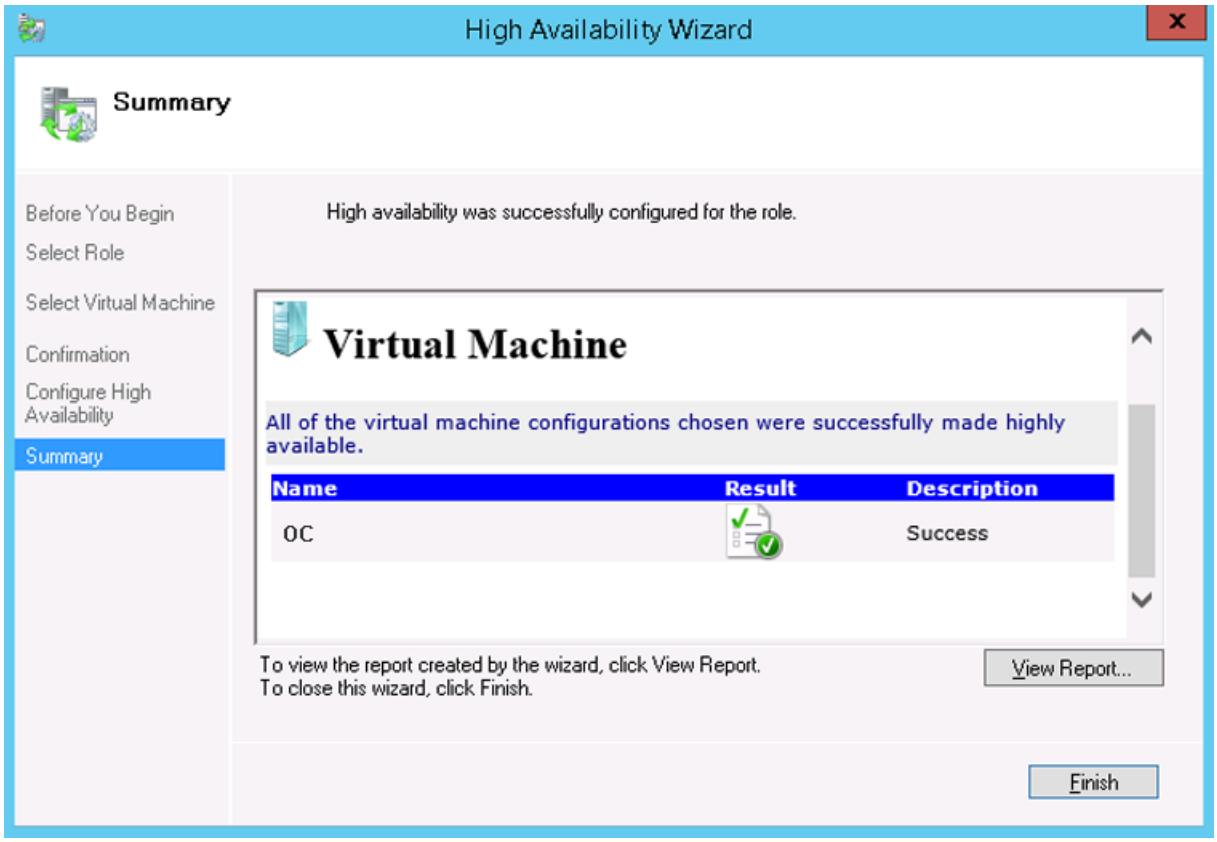
Figure 7-58: Confirm Virtual Machine



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



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
|CPU: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz, total cores: 1
|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>
```

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

```
-----------------------------------------------------
Main Menu> Application Maintenance> Web Servers
-----------------------------------------------------
        |The Web Server's Processes are: UP
        |The Tomcat Server's Proccesses are: UP
        |Port 80 (HTTP): OPEN
        |Port 8080 (IPPs FILES): OPEN
        |Port 8081 (IPPs HTTP): OPEN
        |Port 8082 (IPPs HTTPS): OPEN
        |JAWS Service: ENABLED
```

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

```
---- Scheduling backup ---
The data will be exported once a week,to a file named emsServerBackup_<yymmdd>.tar and to RmanBackup directory
you should backup these files to another machine.
The backup files can be used later only for the same EMS version.

 Current Schedule: Saturday at 2:00

choose a day of the week to perform weekly backup (0-6)
or type q to exit back to previous menu
 0-Sunday,1-Monday,2-Tuesday,3-Wednesday,4-Thursday,5-Friday,6-Saturday (q-quit)
```

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

```
Main Menu> Network Configuration
>1.Server IP Address      (The server will be rebooted)
 2.Ethernet Interfaces    (The server will be rebooted)
 3.Ethernet Redundancy    (The server will be rebooted)
 4.DNS Client
 5.NAT
 6.Static Routes
 7.SNMP Agent
 8.SNMPv3 Engine ID
 q.Quit to main Menu
```

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

```
-------------------------------------------------------
Main Menu> Network Configuration> Ethernet Redundancy
-------------------------------------------------------
        Interface: ens32
                Network: Server's Network
                IP Address: 172.17.118.165
        >1.Add Redundant Interface
         2.Remove Redundant Interface
         3.Modify Redundant Interface
         b.Back
         q.Quit to main Menu
```

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

```
-------------------------------------------------------
Main Menu> Network Configuration> DNS Client
-------------------------------------------------------
        nameserver 10.1.1.11
        nameserver 10.1.1.10

        >1.Configure DNS
         b.Back
         q.Quit to main Menu
```

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

```
NAT Configuration

Server's NAT Address (-1 to disable this feature) [-1]:
```

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 8-9: Static Route Configuration

```
-----------------------------------------------------------------------------------
 Main Menu> Network Configuration> Static Routes
-----------------------------------------------------------------------------------

        Static Routes Configuration

Kernel IP routing 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.Remove 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.

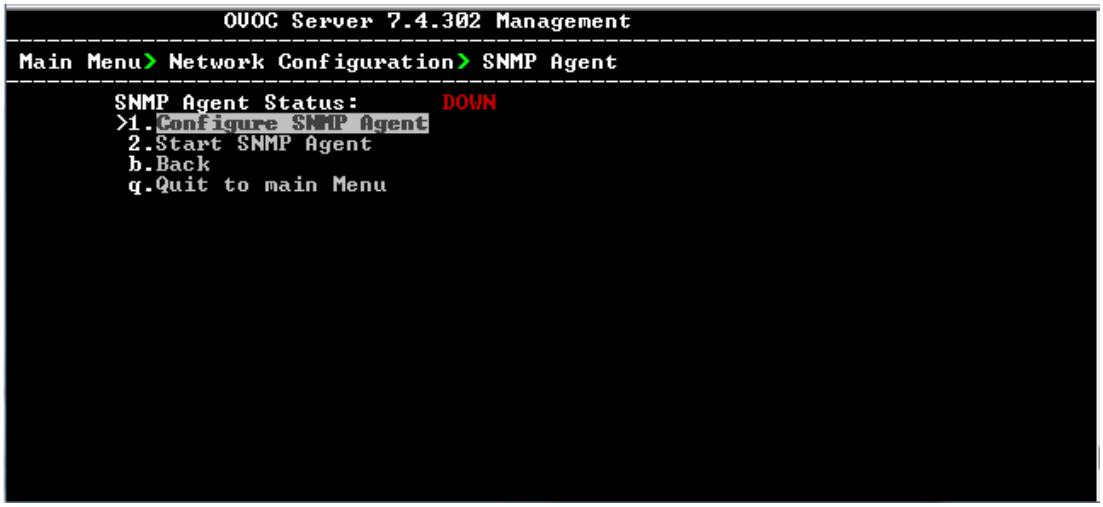
Figure 8-11: NMS IP and Community String

```
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

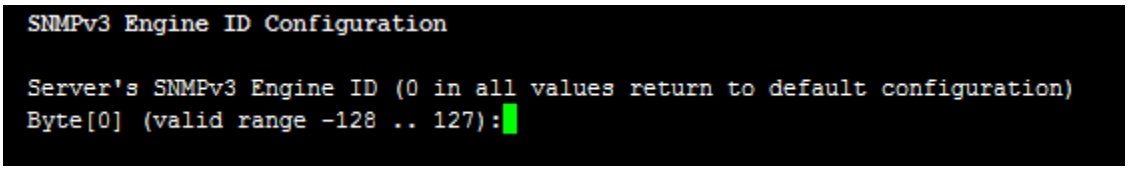
5. Choose option **2 Linux Traps Forwarding Configuration**.
6. Configure the NMS IP and community string parameters from the Version 7.2 platform on the Version 7.4 platform.

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.

Figure 8-14: SNMPv3 Engine ID



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

8.1.6 Date and Time Menu

1. 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 7.2.3075 Management
-----------------------------------------------------------------------
Main Menu> Date & Time
-----------------------------------------------------------------------
        >1.NTP
         2.Timezone Settings     (Apache Server will be restarted)
         3.Date & Time Settings
         q.Quit to main Menu
```

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

```
-----------------------------------------------------------------------------------------------
Main Menu> Security
-----------------------------------------------------------------------------------------------
         1.Add EMS User
        >2.SSH
         3.DB Password  (EMS & SEM applications will be stopped)
         4.OS Users Passwords
         5.File Integrity Checker
         6.Software Integrity Checker (AIDE) and Prelinking
         7.USB Storage
         8.Network options
         9.Audit Agent Options  (The server will be rebooted)
         10.HTTPS Authentication
         11.Disable SEM client secured communication    (EMS application will be restarted)
         12.Enable IP Phone Manager client and JAWS secured communication       (Apache will be restarted)
         13.Server Certificates Update
         14.SEM - AudioCodes devices communication
         q.Quit to main Menu
```

8.1.7.1 SSH

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

Figure 8-17: SSH

```
-----------------------------------------------------------
Main Menu> Security> SSH
-----------------------------------------------------------
        >1.Configure SSH Log Level
         2.Configure SSH Banner
         3.Configure SSH on Ethernet Interfaces
         4.Disable SSH Password Authentication
         5.Enable SSH IgnoreUserKnownHosts parameter
         6.Configure SSH Allowed Hosts
         b.Back
         q.Quit to main Menu
```

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

```
Do you really want to change DB password? Press Esc to quit or any key to continue...
-----------------------------------------------------
*****************************************************
 Oracle Change password Script start
*****************************************************
-----------------------------------------------------
User name:
EMSADMIN
Current Password:
******
The password should be at least 15 characters long, contain at least two digits, two lowercase
and two  uppercase  charactets,  two  punctuation  characters  and  should differ by more than
4 characters from the previous passwords.
New 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

```
Main Menu> Security> Network options

        |Log packets with impossible addresses to kernel log: DISABLED
        |Ignore all ICMP ECHO requests: DISABLED
        |Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
        |Send ICMP redirect messages: DISABLED
        |Accept ICMP redirect messages: DISABLED
        >1.Enable log packets with impossible addresses to kernel log
         2.Enable ignore all ICMP ECHO requests
         3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
         4.Enable send ICMP redirect messages
         5.Enable accept ICMP redirect messages
         b.Back
         q.Quit to main Menu
```

2. 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 8-20: 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
```

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-AudioCodes Device Communication

```
-----------------------------------------------------------------
 Main Menu> Security> SEM - AudioCodes devices communication
-----------------------------------------------------------------
SEM - AudioCodes devices communication: TCP
        >1.TCP   (SEM Server will be restarted)
         2.TLS   (SEM Server will be restarted)
         3.TLS/TCP       (SEM Server will be restarted)
         b.Back
         q.Quit to main Menu
```

2. 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        (The server may be rebooted)
         2.Devices Syslog
         3.Devices Debug
         q.Quit to main Menu
```

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

```
******************** Import process start *******************
Shutting down One Voice Operations Center server...
Topology file processed entities:
Regions: 4
MT Regions: 4
Nodes: 13
Non ACL Nodes: 3
Links: 2
Nodes with LP Features: 0
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
Import Regions...
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 Quality 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%
Import Devices (can take up to 7.0 Minute/s)...
.....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%
Import Links...
links added: 2/2 :100%
Import License Pool...
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!
******************** Import process finish ******************

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.
```

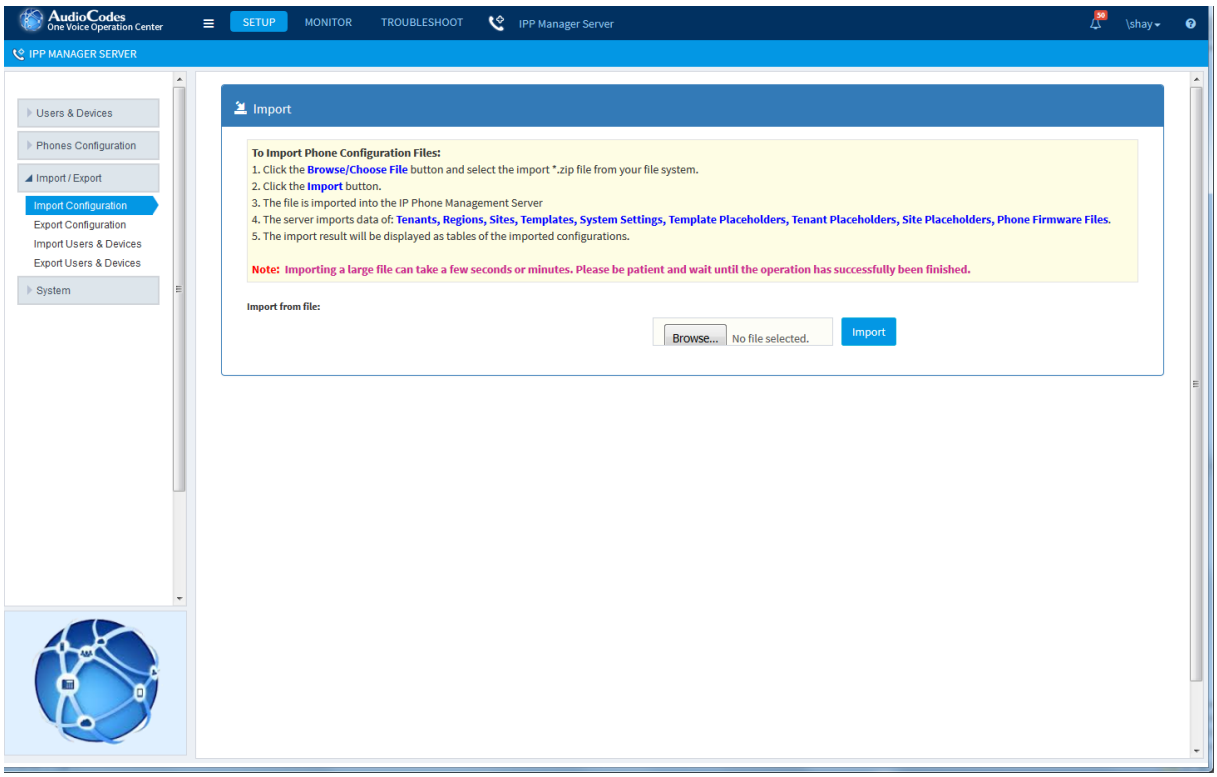
9.2 Import IP Phone Management Server Configuration and Users & Devices

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:**

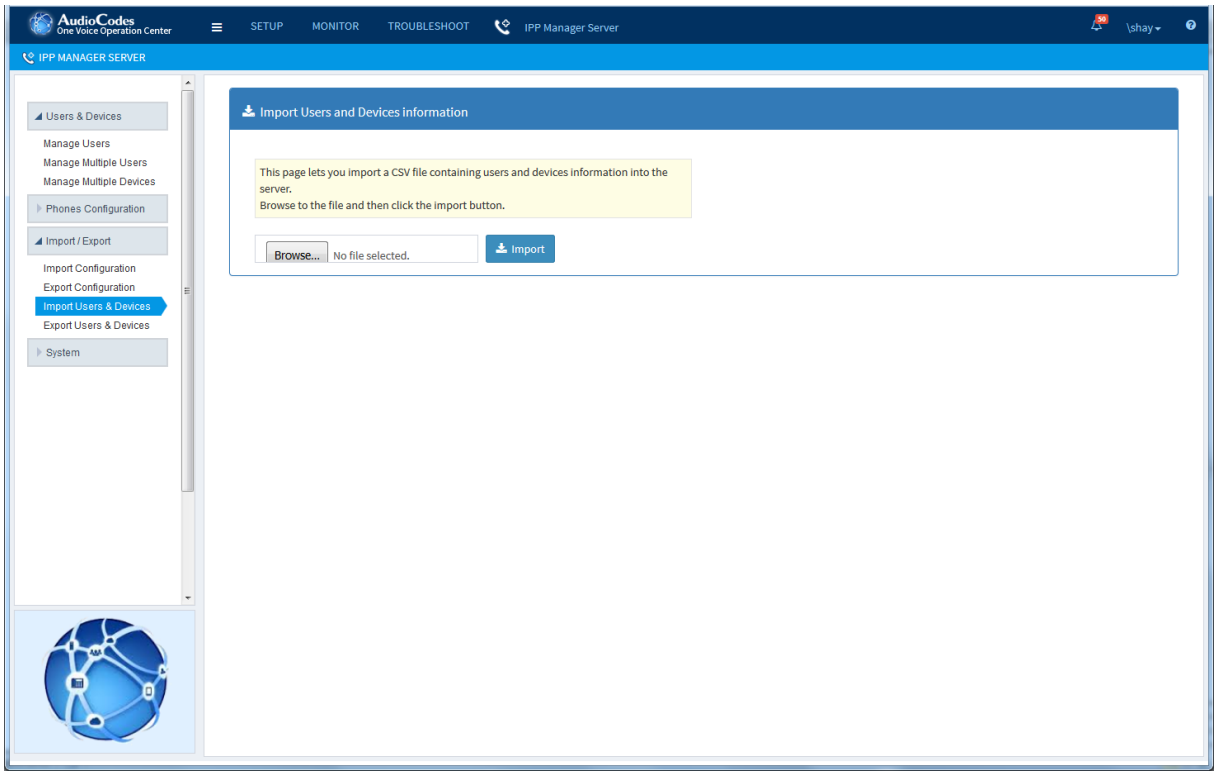
1. Login to IP Phone Management server Version 7.4 Web client.
2. Open the Import Configuration page (Setup tab > Import/Export > Import Configuration).

Figure 9-1: Import Phone Configuration Files



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

Figure 9-2: Import Users and Devices



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
   ```
   b. 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.

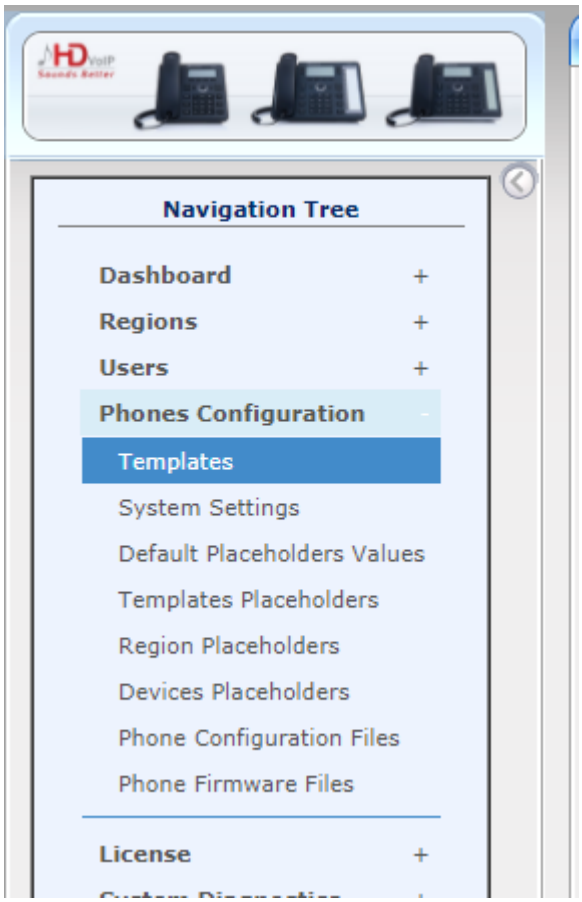
Note:

- 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>.

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[
]]>
                                </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
]]>
</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/dhcpoption160.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.

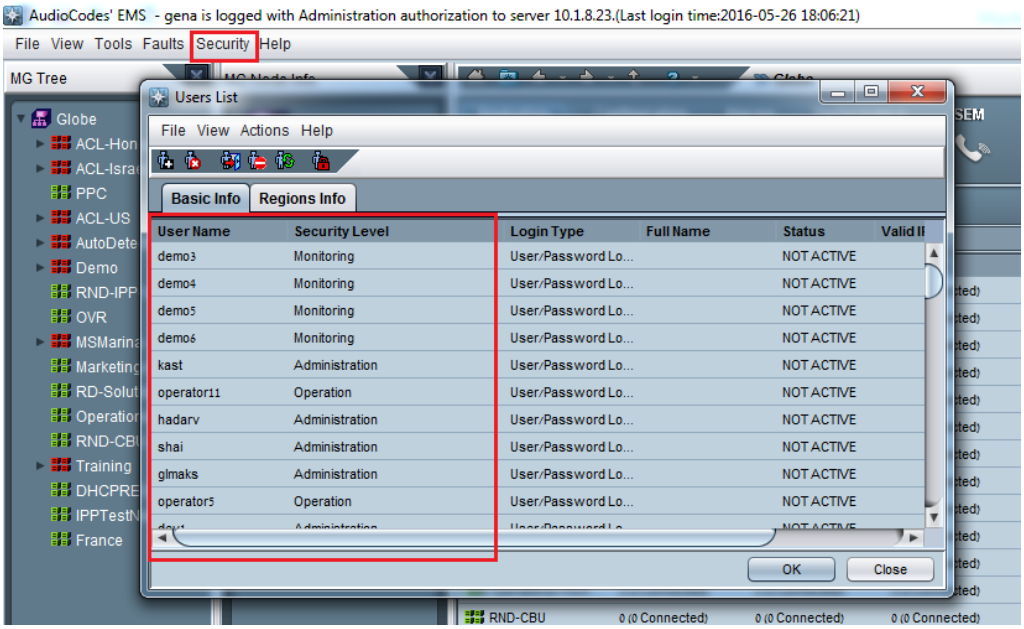
11 Configure One Voice Operations Center Web Client

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

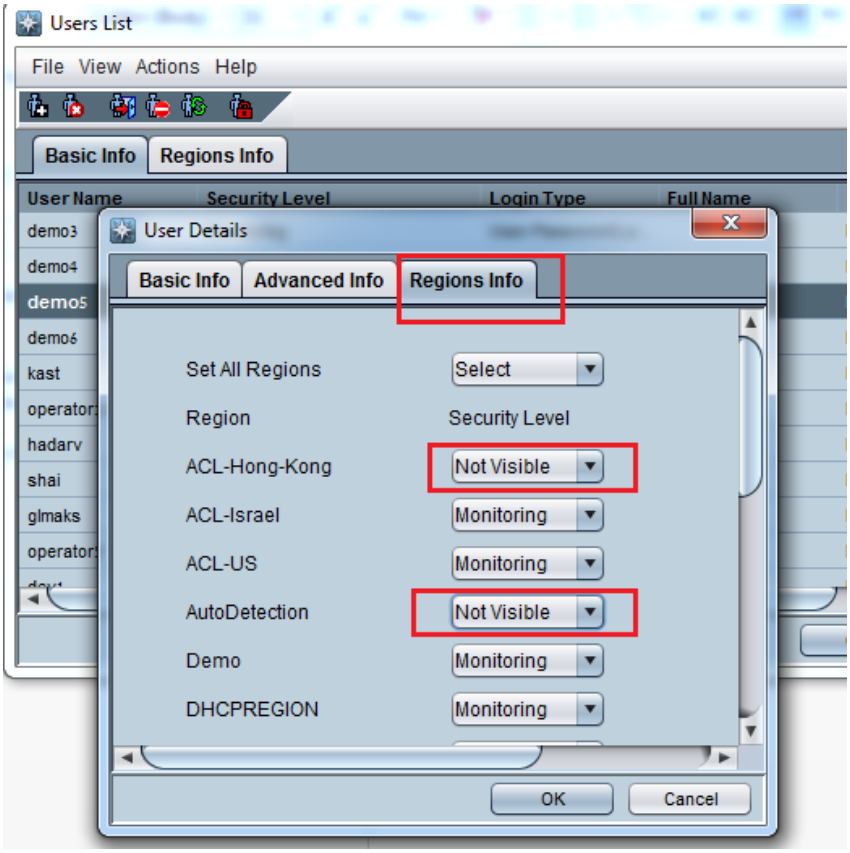
- To move operators to the new Version 7.4 platform, manually copy all previously defined Operators on the Version 7.2 platform (EMS Main Menu: Security > Users List).

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:

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.*

Figure 11-3: Tenant Operators

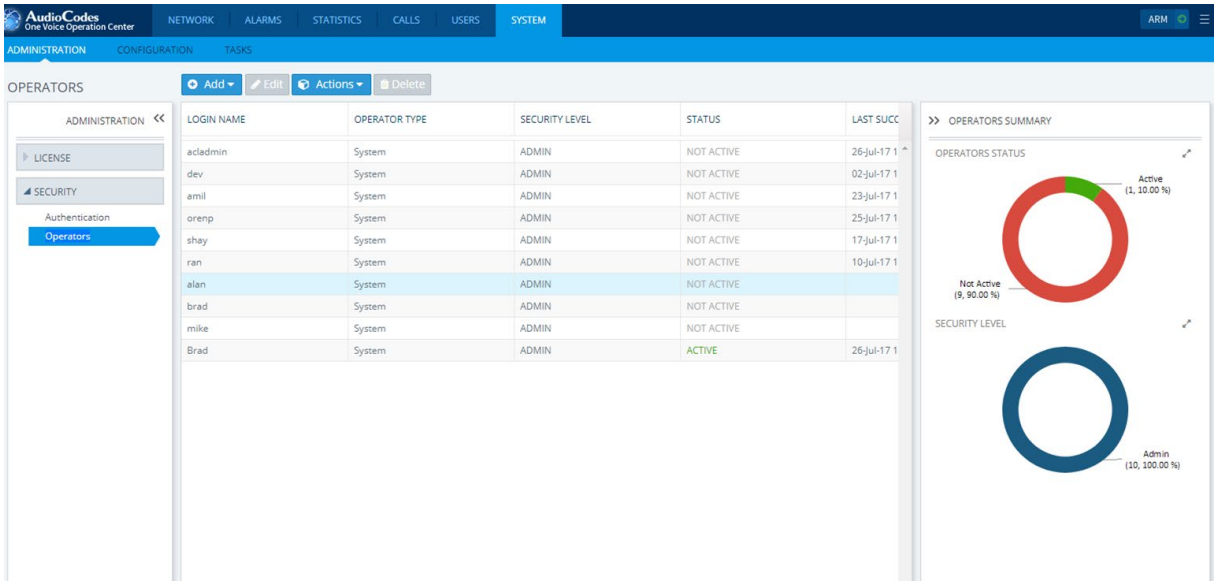
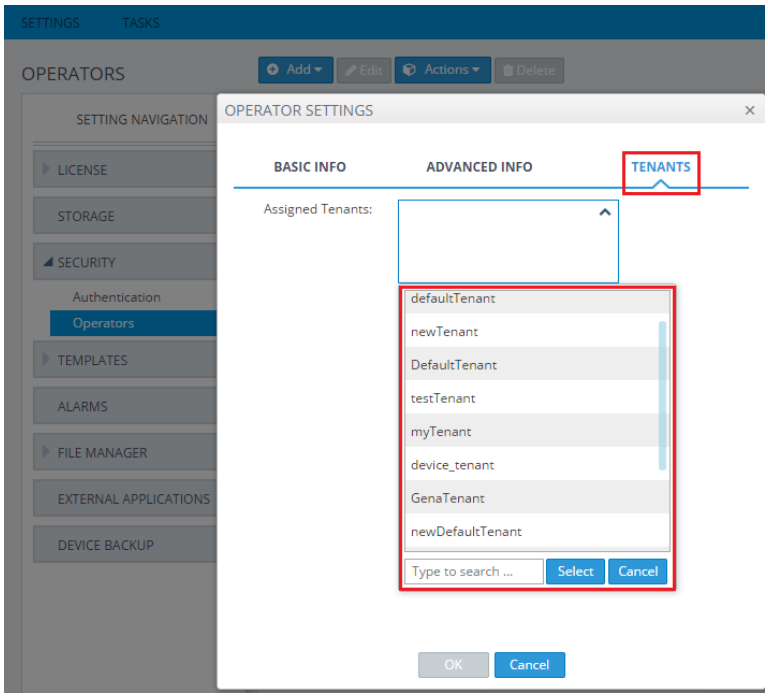


Figure 11-4: Tenant Operator Settings



11.2 External Authentication Servers

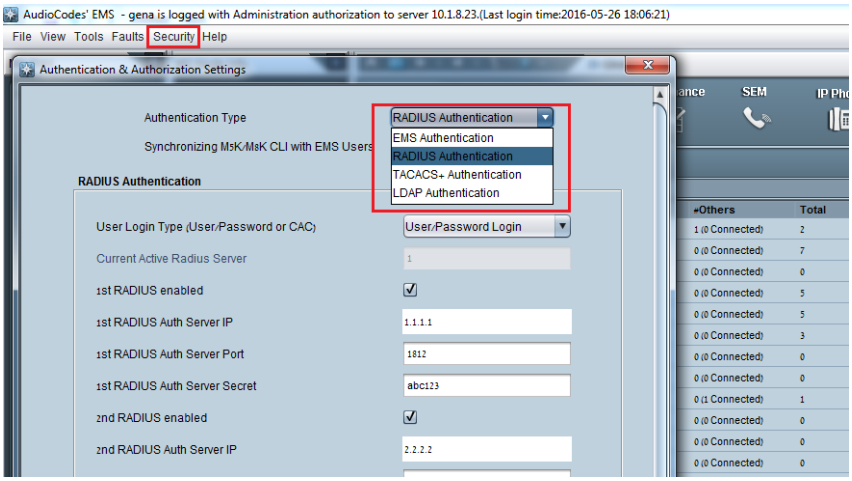
If EMS is defined to work with external Authentication servers, save the Authentication Servers configuration.

Note: TACACS server is not supported in Version 7.4.

11.2.1 RADIUS

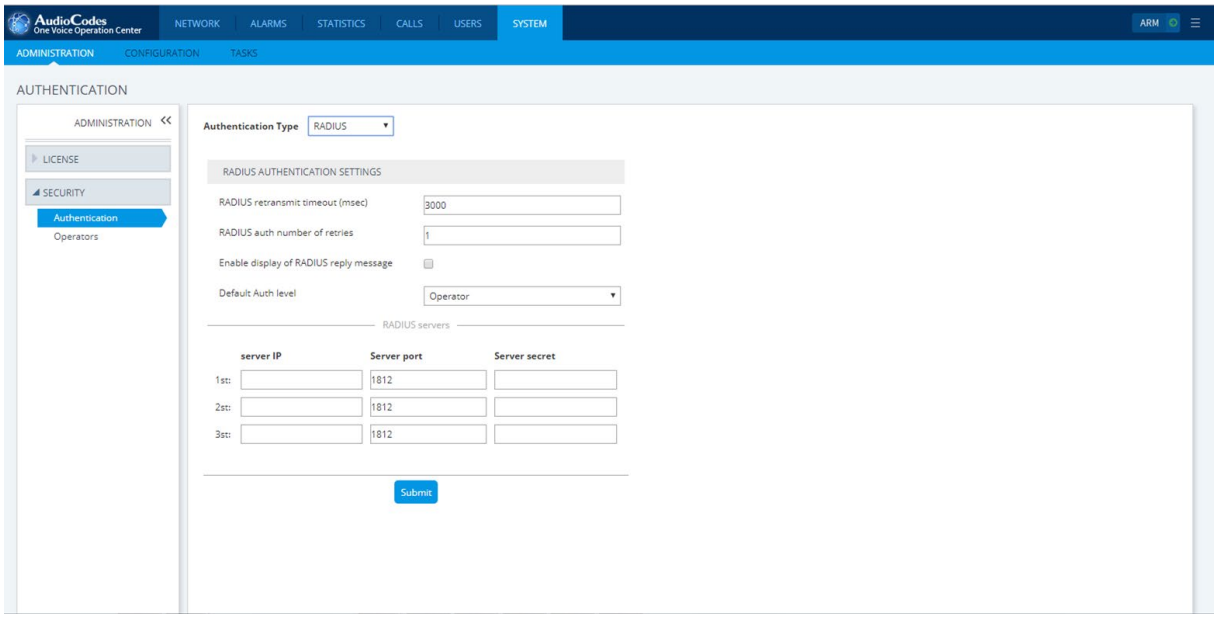
1. Open the Authentication and Authorization Settings on the Version 7.2 platform (open the EMS menu: Security > Authentication & Authorization).
2. From the drop-down list, select **RADIUS Authentication**.

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**.

Figure 11-6: RADIUS Settings

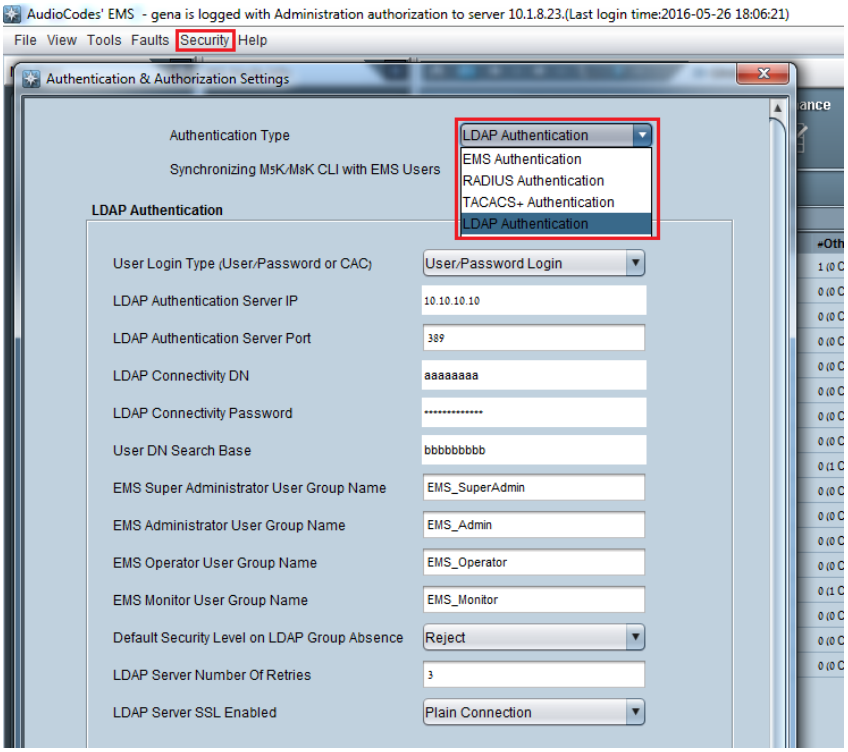


5. Configure the required parameters using the Version 7.2 platform as reference.

11.2.2 LDAP

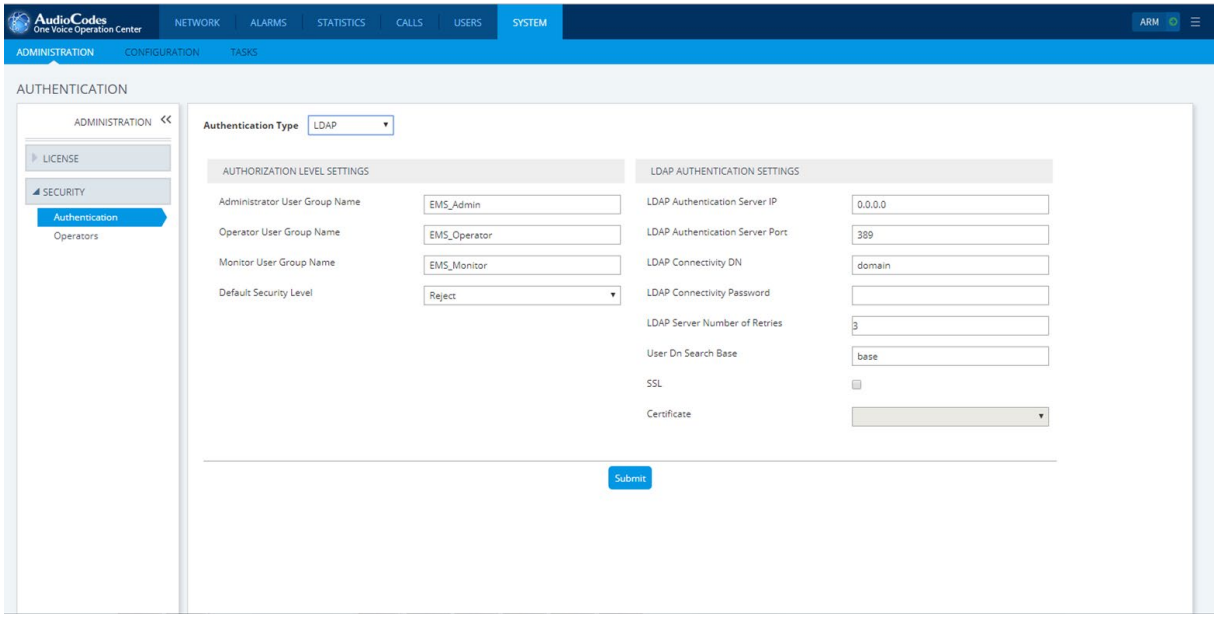
1. Open the Authentication and Authorization Settings on the Version 7.2 platform (open the EMS menu: Security > Authentication & Authorization).
2. From the drop-down list, select **LDAP Authentication**.

Figure 11-7: LDAP Configuration



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



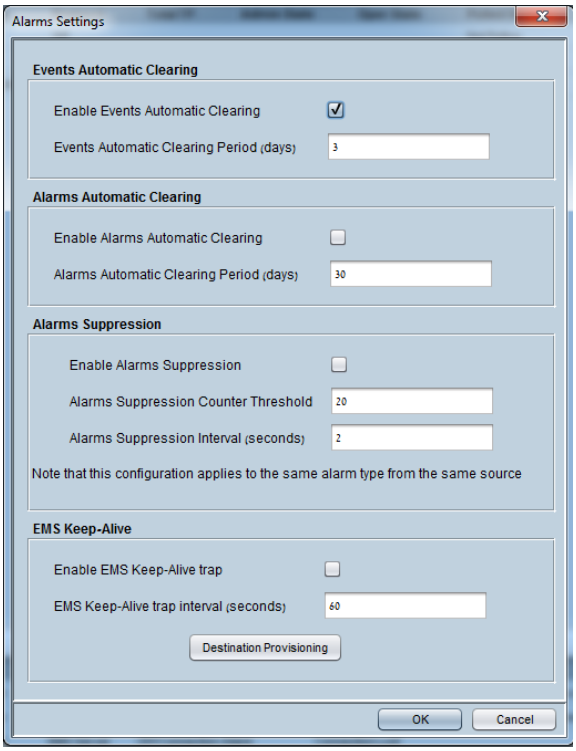
5. Configure the required parameters using the Version 7.2 platform as reference.

11.3 Alarms (from EMS Application)

11.3.1 Alarms Settings

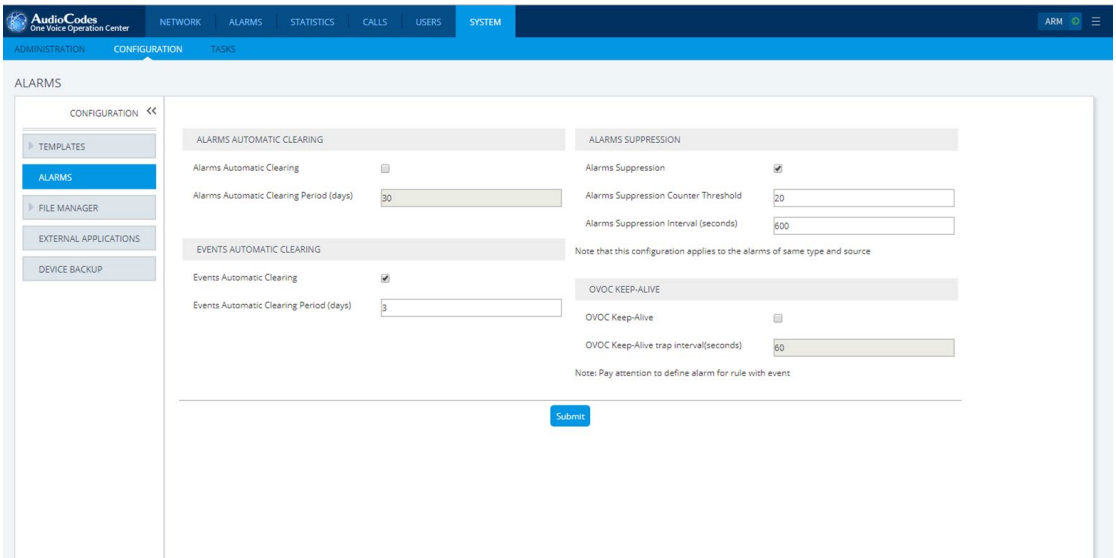
1. Open the Global alarm settings on the Version 7.2 platform (In the main EMS menu: Faults > Alarms Setting).

Figure 11-9: Alarm Settings



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

Figure 11-10: Version 7.4 Alarms Settings

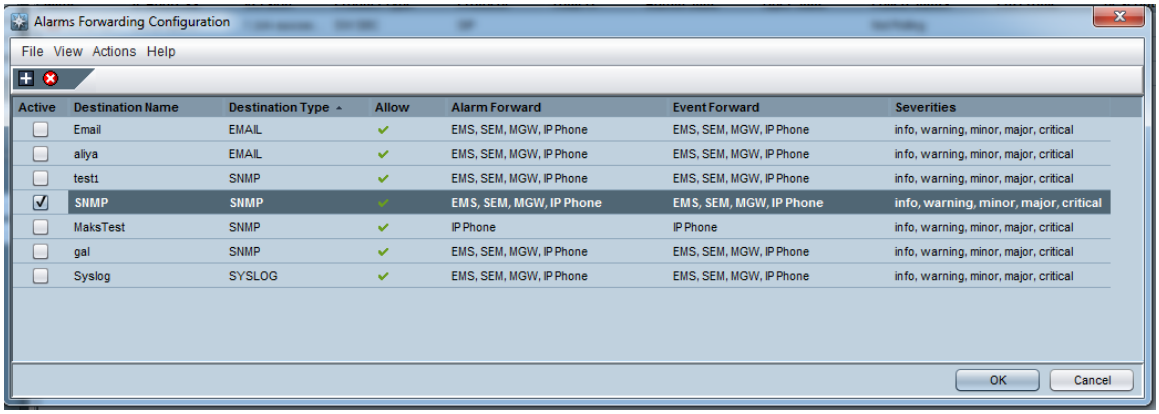


3. Configure the required settings using the Version 7.2 platform as reference.

11.3.2 Alarms Forwarding Rules

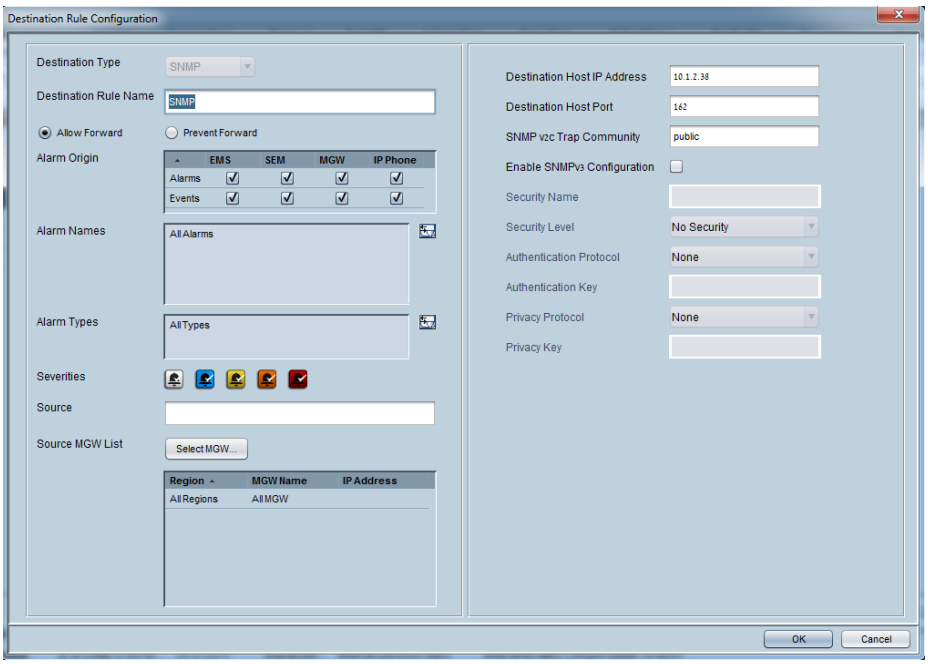
1. Alarms forwarding rules need to be reconfigured manually on the new Version 7.4 machine (EMS Main menu: Faults > Alarms Forwarding Configuration).

Figure 11-11: Version 7.2: Alarm Forwarding Rules



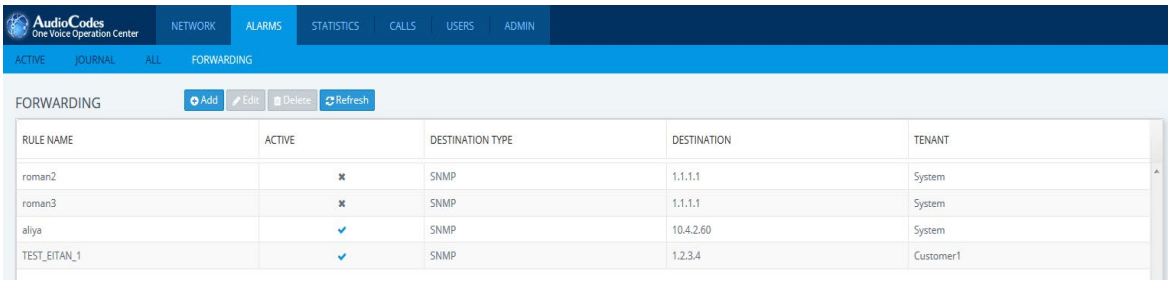
2. Double-click to open each rule specific configuration rule.

Figure 11-12: Version 7.2: Destination Rules Configuration



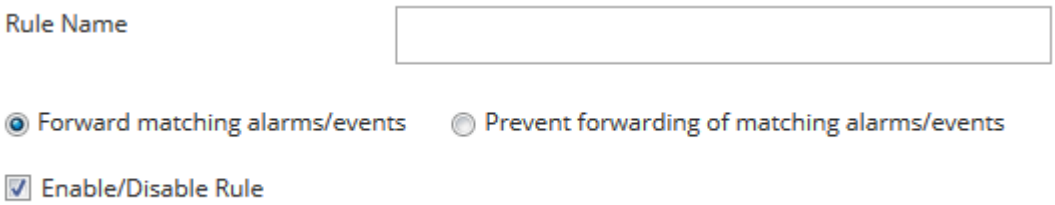
3. Open the Alarm-forwarding rules screen (Alarms tab > Forwarding) on the Version 7.4 platform.

Figure 11-13: Version 7.4: Alarm Forwarding Rules



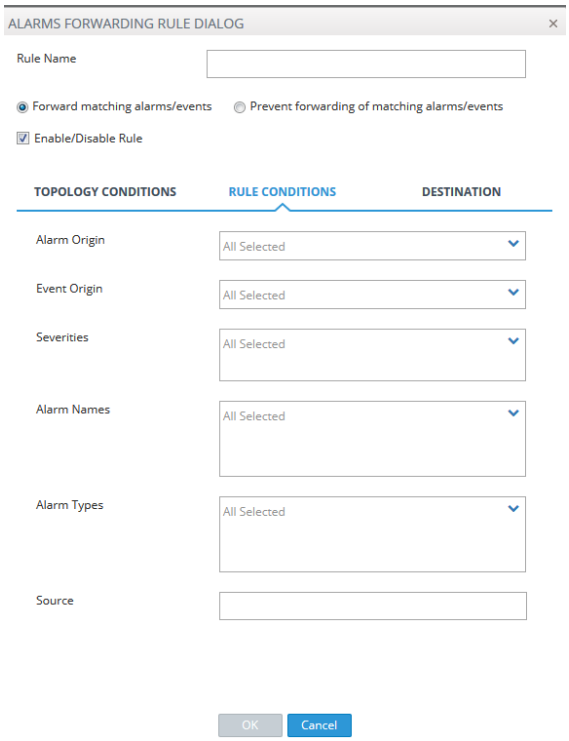
4. Click **Add** to add a new rule.
5. Configure the required parameters using the Version 7.2 platform as reference:
   a. Allow/prevent configuration and enable/disable rule can be configured under top section.

Figure 11-14: Rule Name



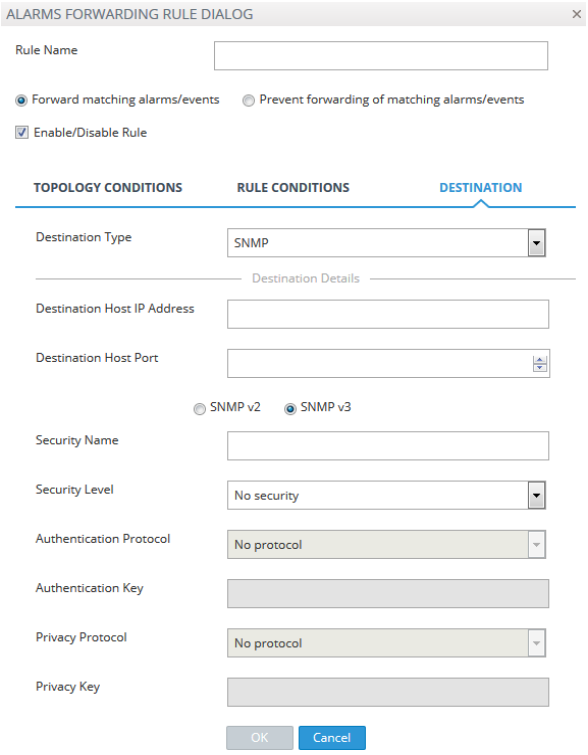
   b. Configure devices and other topology filtered elements under “Topology Conditions” section.
   c. Other forwarding conditions can be configured under “Rule Conditions” section.

Figure 11-15: Alarm Forwarding Rule Conditions



d. Destination type and configuration can be configured under “Destination” section.

Figure 11-16: Alarm Forwarding Destinations



11.4 Software Manager

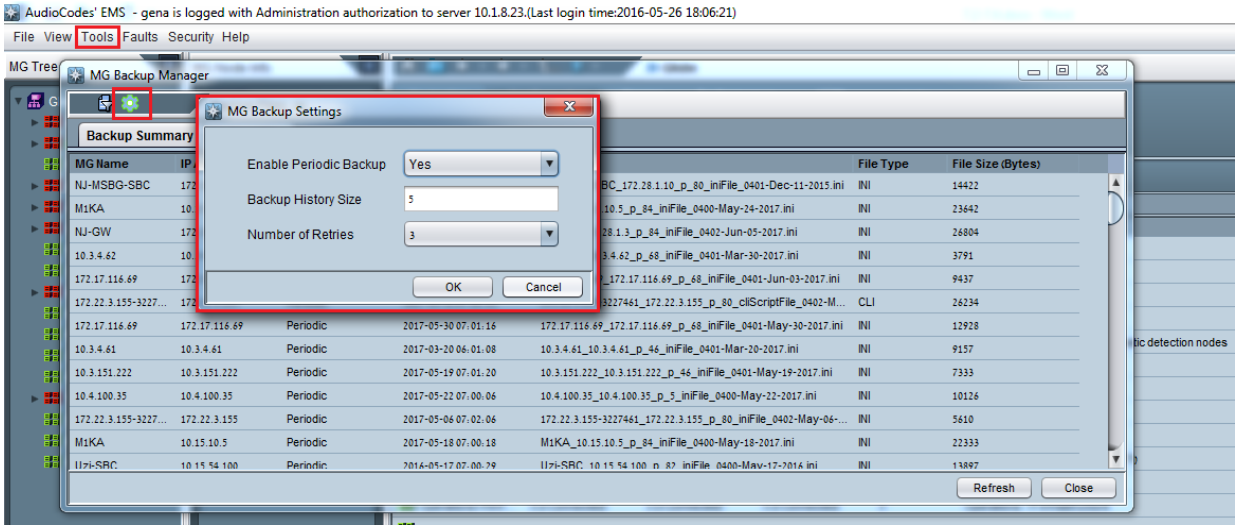
- On the new One Voice Operations Center Version 7.4 machine, add files that you extracted from the Version 7.2 platform in Section 5.1 to the Software Manager (System tab > Configuration > File Manager).

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

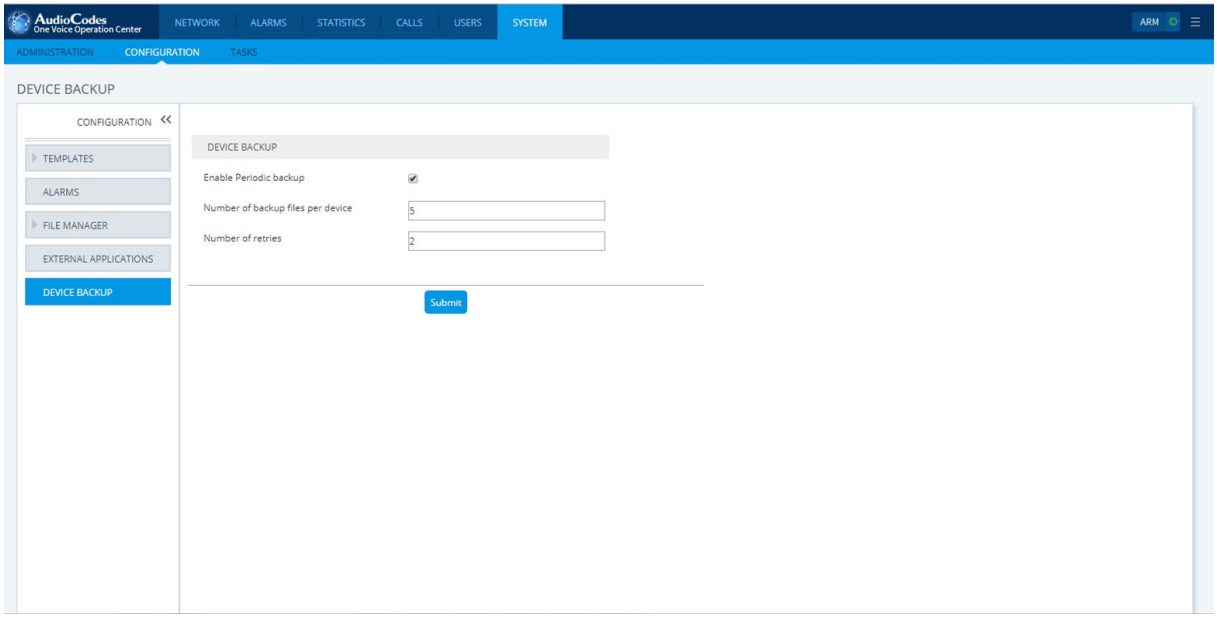
1. Open the devices backup configuration settings on the Version 7.2 platform (In the main EMS menu: Tools > MG Backup Manager).

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).

Figure 11-18: Version 7.4: Backup Configuration

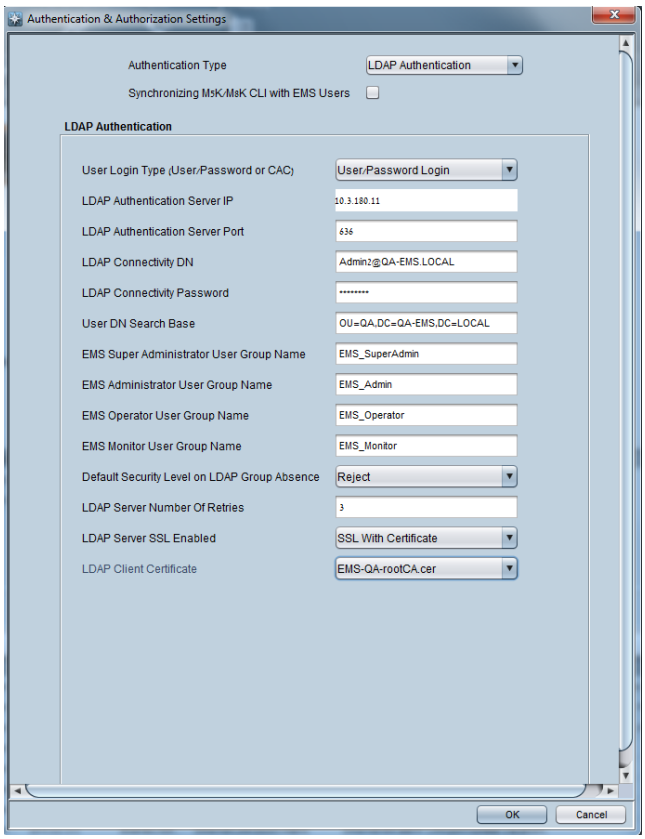


3. Configure the required parameters using the Version 7.2 platform as reference.

11.6 LDAP User Authentication

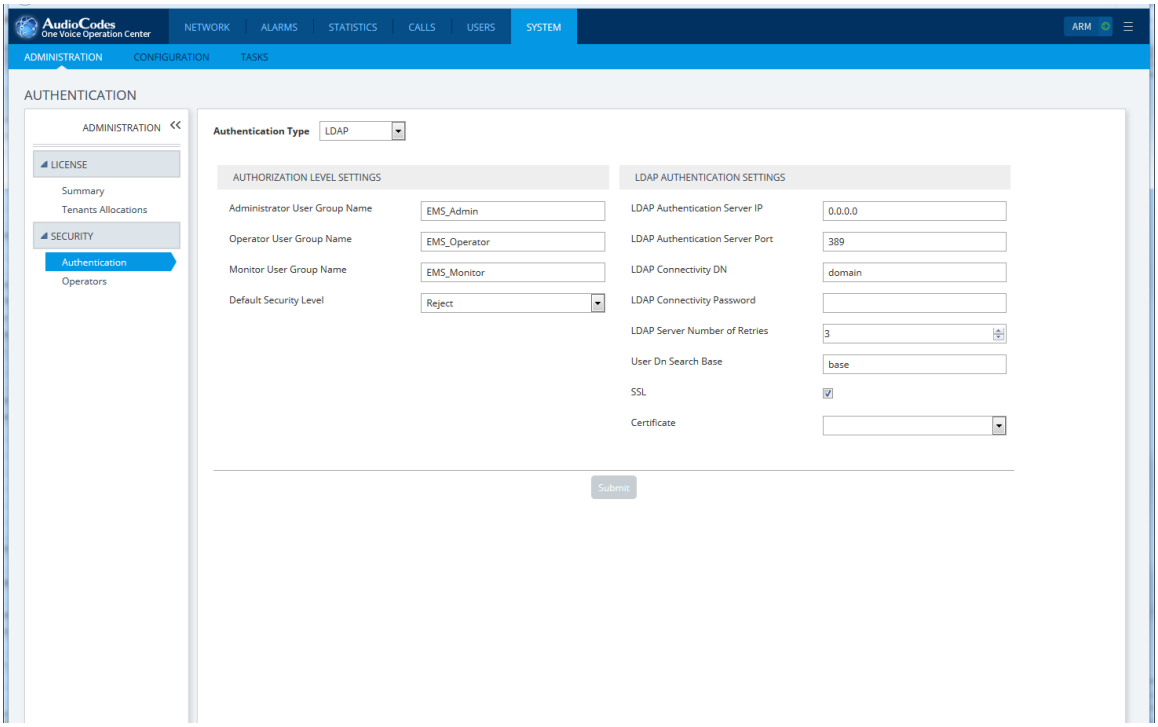
1. On the Version 7.2 platform, open the LDAP Authentication & Authorization Settings screen (EMS Main menu: Security > Authentication & Authorization).
2. From the Authentication drop-down list, select **LDAP Authentication**.

Figure 11-19: LDAP Authentication and Authorization



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



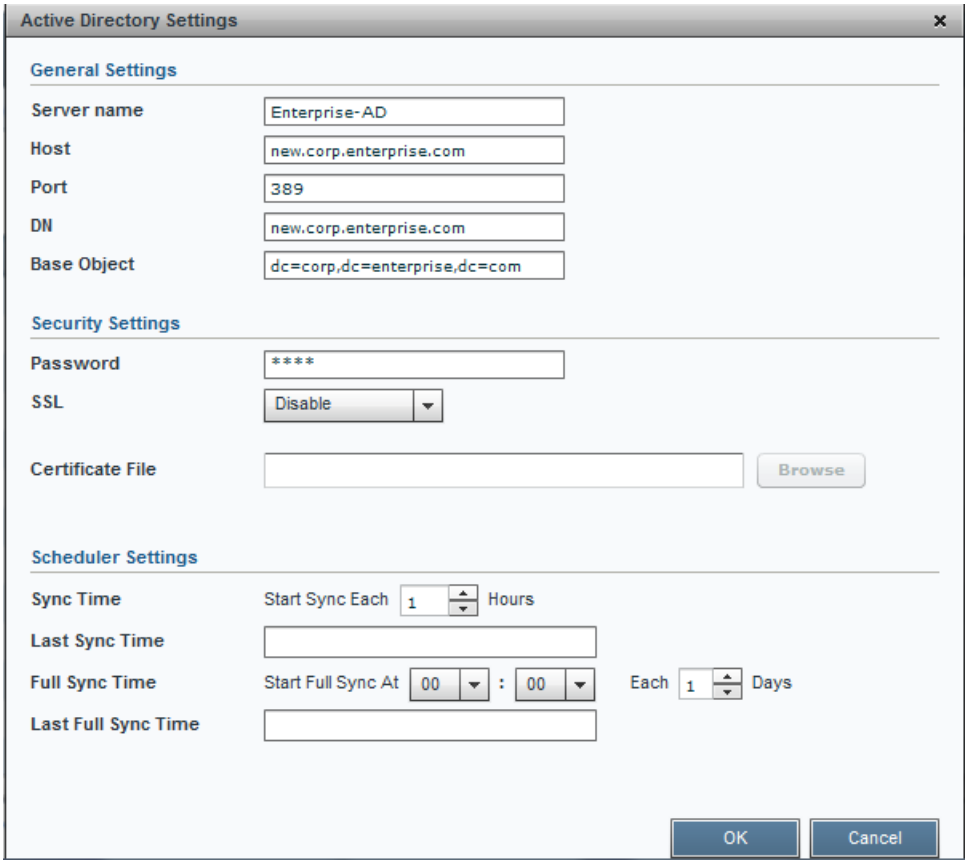
6. Configure the required parameters using the Version 7.2 platform as reference.

11.7 SEM Client Configuration

11.7.1 Microsoft Active Directory

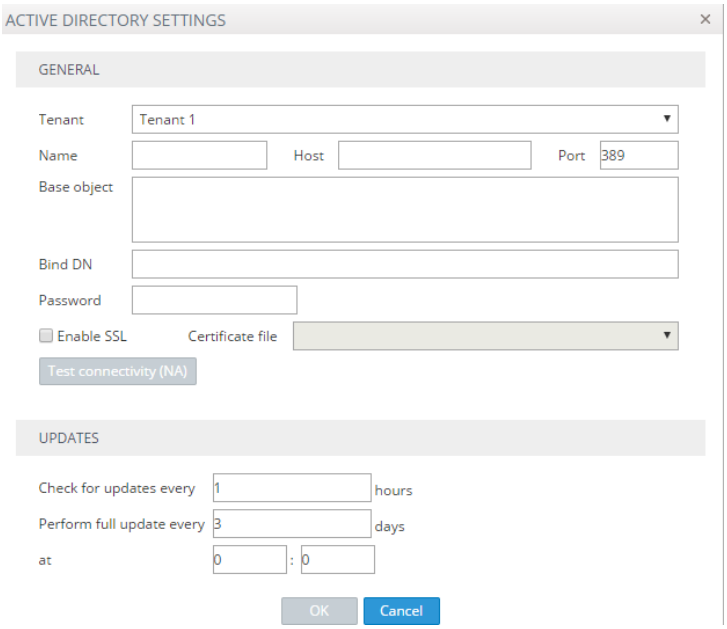
1. On the SEM Version 7.2 platform, open the Active Directory Settings screen (Users tab > Active Directories folder).

Figure 11-21: Version 7.2: Active Directory Configuration



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

Figure 11-22: Version 7.4 Active Directory Configuration

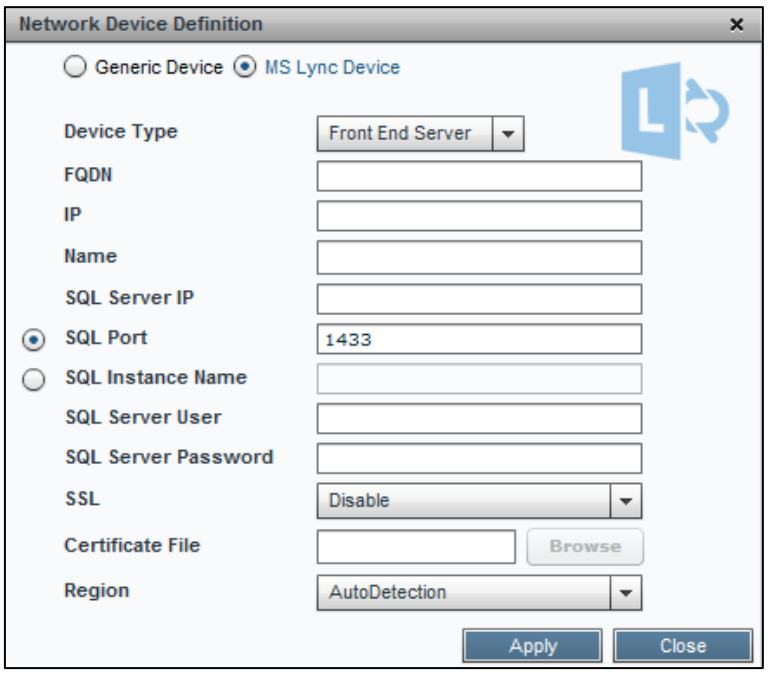


3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.2 Skype for Business SQL Server Configuration

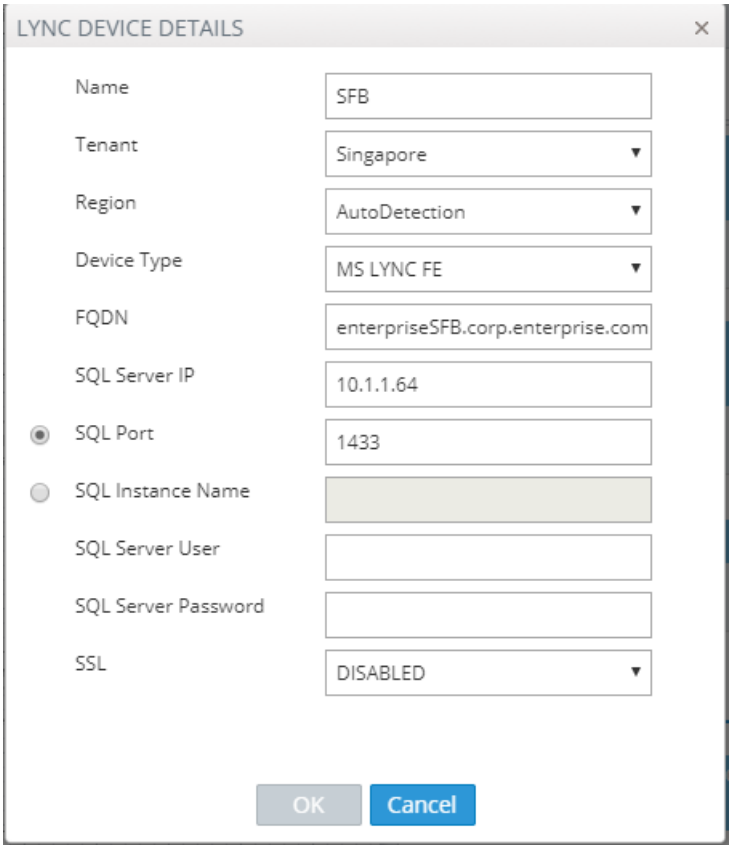
1. On the SEM Version 7.2 platform, open the Network Device Definition screen for the Skype for Business device (Network tab).

Figure 11-23: SEM - Network tab Skype for Business Device Definition



2. 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**.

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



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

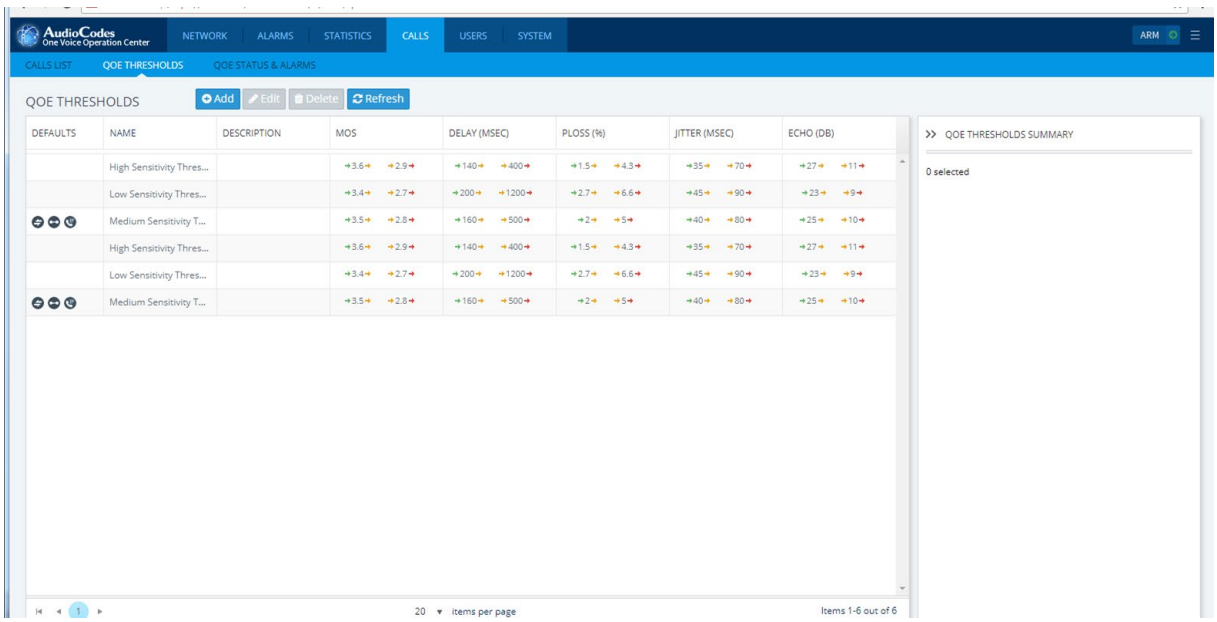
11.7.3 QoE Thresholds Configuration

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

Figure 11-25: Version 7.2: QoE Thresholds Configuration

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

Figure 11-26: Version 7.4: QoE Thresholds Configuration

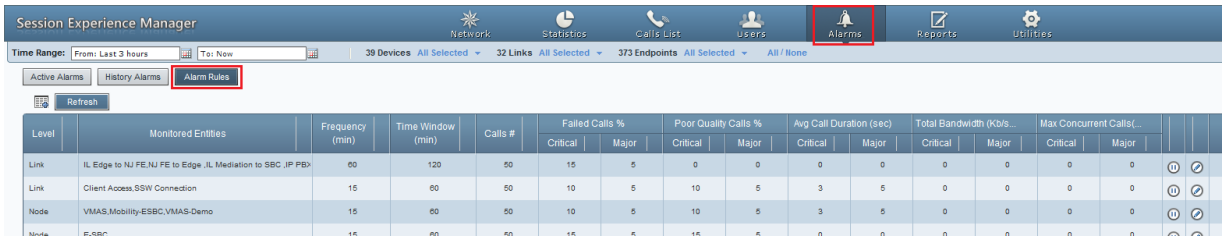


3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.4 Alarm Rules Configuration

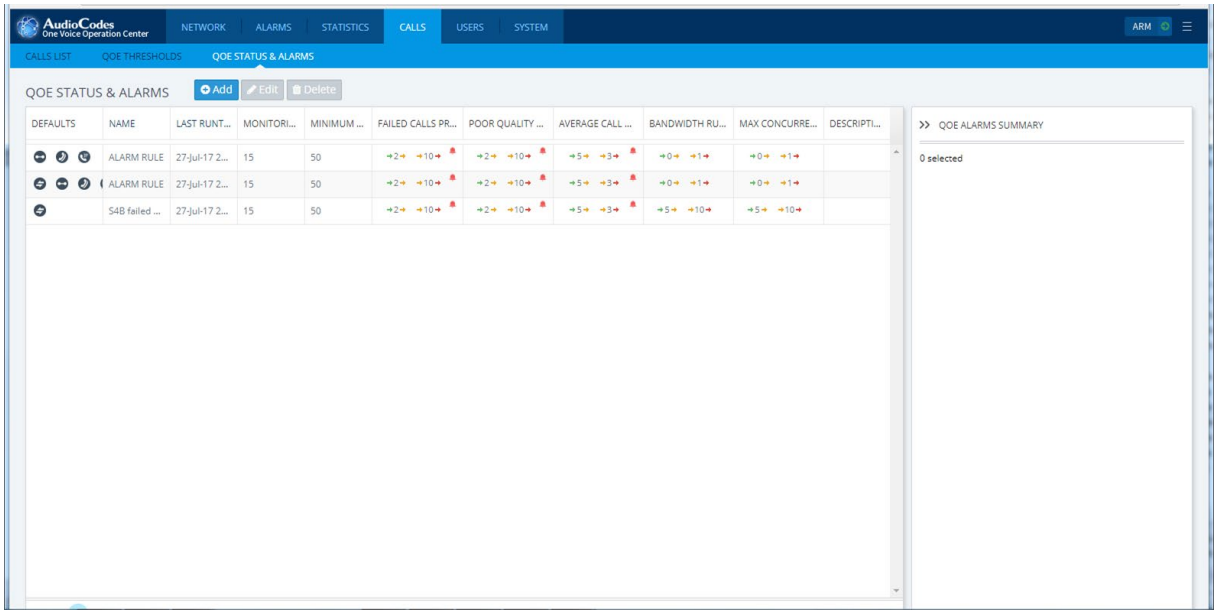
1. Open the Alarms Rules Configuration on the Version 7.2 platform (Alarms tab > Alarm Rules).

Figure 11-27: Version 7.2: Alarm Rules Configuration



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

Figure 11-28: Version 7.4: Alarm Rules Configuration

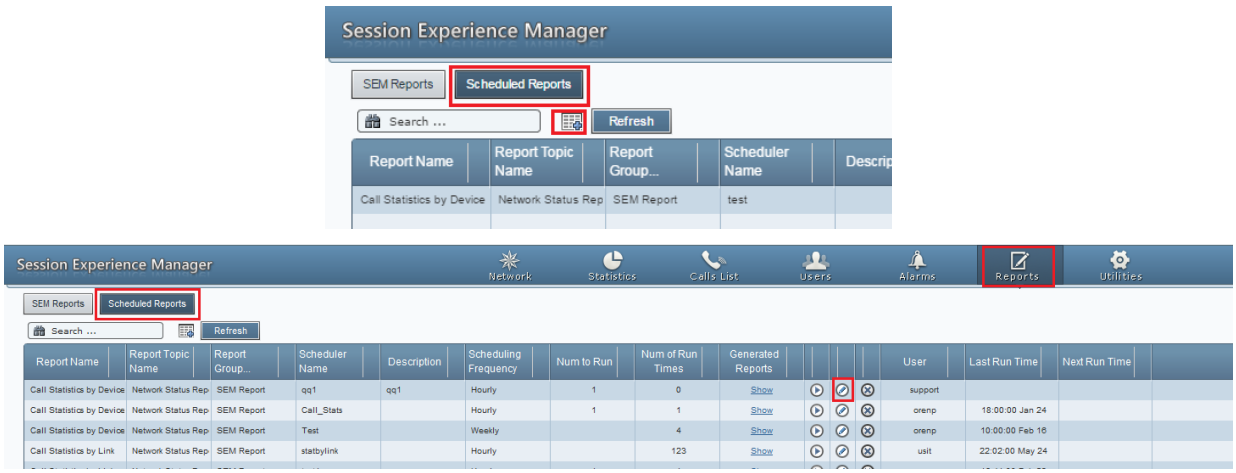


3. Configure the required parameters using the Version 7.2 platform as reference.

11.7.5 Scheduled Reports Configuration (from SEM Application)

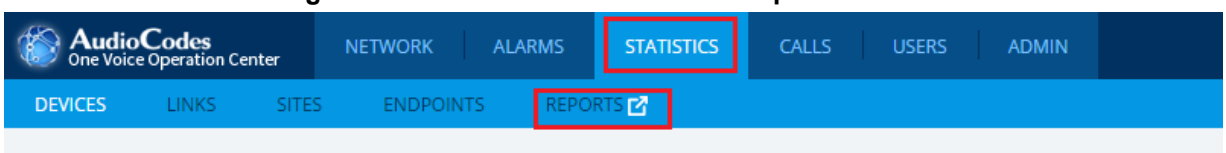
1. Open the SEM Scheduled Reports configuration on the Version 7.2 platform (Reports > Scheduled Reports).

Figure 11-29: Version 7.2: SEM Scheduled Reports



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

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: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-91055