Installation Operation and Maintenance Manual

AudioCodes One Voice Operations Center

EMS, SEM and IP Phone Manager

Version 7.2

Table of Contents

List of Figures

List of Tables

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 and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: May-11-2017

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 service are generally provided by AudioCodes’ Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

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

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
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAM Integration Guide
Element Management System (EMS) User’s Manual
SEM User's Manual
IP Phone Management Server Administrator's Manual
IP Phone Manager Express Administrator's Manual
AudioCodes One Voice Operations Center Product Description
OVOC Security Guidelines
Element Management System (EMS) Online Help
Mediant 500 Gateway and E-SBC Performance Monitors and Alarms Guide
Mediant 800 Gateway and E-SBC Mediant Software SBC CloudBond 365 and CCE Alarms Guide
Mediant 1000B Gateway and E-SBC Performance Monitors and Alarms Guide
Mediant 2600-4000-9000-SW SBC Series Performance Monitors and Alarms Guide
Mediant 3000 with TP-6310 Performance Monitoring and Alarms Guide
Mediant 3000 with TP-8410 Performance Monitoring and Alarms Guide
Mediant MSBR Series Performance Monitors and Alarms Guide

1 Overview

The EMS provides customers with the capability to easily and rapidly provision, deploy and manage AudioCodes devices.

Provisioning, deploying and managing these devices with the EMS are performed from a centralized management station in a user-friendly Graphic User Interface (GUI).

This document describes the installation of the EMS server and its components.

It is intended for anyone responsible for installing and maintaining AudioCodes' EMS server and the EMS server database.

This page is intentionally left blank.

Part I

Pre-installation Information

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

2 Managed VoIP Equipment

The following products (and product versions) can be managed by this EMS / SEM release:

- Mediant 9000 SBC – versions 7.2 (including support for MTC), 7.0, 6.8
- Mediant 4000 SBC – versions 7.2, 7.0, 6.8
- Mediant 4000B SBC – version 7.2, 7.0
- Mediant 2600 E-SBC – versions 7.2, 7.0, 6.8
- Mediant 2600B E-SBC – version 7.2, 7.0
- Mediant Server Addition (SE) SBC – versions 7.2, 7.0 and 6.8
- Mediant Virtual Addition (VE) SBC – versions 7.2 (**including support for MTC**), 7.0 and 6.8
- Mediant 3000 Media Gateways (TP-8410 and TP-6310) – versions 7.0 (SIP), 6.8 (SIP) and 6.6 (SIP and MEGACO)
- Mediant 2000 Media Gateways – version 6.6
- *Mediant 1000 Gateway – version 6.6 (SIP and MEGACO)
- Mediant 1000B Gateway and E-SBC – versions **7.2** 7.0, 6.8 and 6.6
- Mediant 1000B MSBR – versions 6.8
- Mediant 800B Gateway and E-SBC – versions **7.2** 7.0, 6.8 and 6.6
- **Mediant 500 E-SBC –** version **7.2**
- **Mediant 500L E-SBC –** version **7.2**
- Mediant 800B MSBR – versions **7.2**, 6.8 and 6.6
- *Mediant 600 – version 6.6
- Mediant 500L MSBR, Mediant 500 MSBR – version **7.2**, 6.8
- MediaPack MP-11x series – version 6.6 (SIP and MEGACO)
- MediaPack MP-124 Rev. **D** and **E** – version 6.6 (SIP and MEGACO
- **MP-20x B –** version **7.2**
- **MP-1288 –** version **7.2**
- *Mediant 800B SBA, *Mediant 1000B SBA, and *Mediant 2600B SBA devices with SBA version 1.1.12.x and above and gateway versions **7.2**, **7.0**, 6.8
- 400 HD Series: from version 2.0.13 (Skype for Business) and from version 2.2.2 (Non-Lync): 420HD, 430HD and 440HD and 405.
- 400 HD Series from version 3.0 (Skype for Business): **450 HD**
- **CloudBond 365 Series:** version **7.4**: Standard Edition (Mediant 800B platform); Standard Plus Edition (Mediant 800B platform); Pro Edition (Mediant Server platform); Enterprise Edition (Mediant Server platform); Virtualized Edition (Mediant Server platform).
- **Mediant 800 CCE Appliance** and **Mediant Server CCE Appliance** [1]

[1] Contact AudioCodes regarding version support for these products.

Note:

- * Refers to products that are not supported by the SEM.
- All versions VoIP equipment work with the SIP control protocol.
- **Bold** refers to new product support and version support.

3 Hardware and Software Specifications

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

3.1 EMS Server and Client Requirements

This section lists the platform and software required to run the EMS dedicated hardware version and the VMware and Hyper-V version.

Table 3-1: EMS- Minimal Platform Requirements

Resource	EMS/SEM Server			EMS Client
	Dedicated EMS Server - Linux OS	Virtual EMS - Low Profile	Virtual EMS - High Profile	
Hardware	HP ProLiant DL360p Gen8	–	–	Monitor resolution: 1152*864 or higher
Operating System	Linux CentOS 64-bit, kernel version 5.9, Rev7 For EMS HA: Linux CentOS 64-bit, kernel version 5.9, Rev8	Linux CentOS 64-bit, kernel version 5.9 Rev7 (Rev8 for EMS-HA).	Linux CentOS 64-bit, kernel version 5.9 Rev7	Windows™ 10/Windows 8/Windows 8.1/ Windows 7/ Windows 7 Enterprise/ Windows Server 2012 R2 Standard
Virtualization platform	–	VMware: ESXi 6.0, 5.0 and 4.1		–
		VMware HA cluster: VMware ESXi 5.5		
		Microsoft Hyper-V Windows server 2012R2		
Memory	32 GB RAM	8 GB RAM	32 GB RAM	512 MB RAM
Disk space	Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0	500 GB	1.2 TB	300 MB
Processor	CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each)	1 core not less than 2.5 GHz	6 cores not less than 2 GHz	
DVD-ROM	Local	–	–	–

- The working space requirements on the EMS server are as follows:
    - Linux: Executable bash
- The EMS server works with the Java Development Kit (JDK) version 1.8 (JDK 1.8 for Linux™). The EMS client works with the JRE version 1.8 for Windows™.
- The Oracle database used is version *11g.*
- Supported browsers for client applications are as follows:
    - Internet Explorer version 11 and higher
    - Mozilla Firefox version 38 and higher
    - Google Chrome version 43 and higher

Note:

- The JDK and Oracle database component versions mentioned above are provided as part of the EMS server and EMS client installation images.
- The Java Runtime Environment (JRE) is not provided in the client installation and therefore you must install it on your PC in order to launch the EMS client using the Java Webstart.
- The above browsers are supported to run the following client applications: EMS/devices Single Sign-on, JAWS, NBIF, SEM and IP Phone Manager.

3.2 Bandwidth Requirements

This section lists the EMS and SEM bandwidth requirements.

3.2.1 EMS Bandwidth Requirements

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

3.2.2 SEM Bandwidth Requirements

The following table describes the upload bandwidth speed requirements for monitoring the different CPE devices using the SEM. The bandwidth requirement is for EMS/SEM Server <-> Device communication.

Table 3-2: SEM Bandwidth Requirements

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
SBC		
MP-118	_	_
MP-124	_	_

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
Mediant 800 Mediant 850	60	135 Kbits/sec
Mediant 1000	150	330 Kbits / sec
Mediant 2000	_	_
Mediant 2600	600	1.3 Mbit/sec
Mediant 3000	1024	2.2 Mbit/sec
Mediant 4000	4,000	8.6 Mbit/sec
Gateway		
MP-118	8	15 Kbits/sec
MP-124	24	45 Kbits/sec
Mediant 800 Mediant 850	60	110 Kbits/sec
Mediant 1000	120	220 Kbits/sec
Mediant 2000	480	880 Kbits/sec
Mediant 2600	_	_
Mediant 3000	2048	3.6 Mbit/sec
Mediant 4000	_	_
Endpoints	_	56 Kbits/sec

3.3 Performance and Data Storage

The following table shows the performance and data storage capabilities for the EMS managed devices, EMS for IP Phones managed devices and for the SEM.

Table 3-3: Performance and Data Storage

Machine Specifications	HP DL360p G8	VMware/Microsoft Hyper-V - Low Profile	VMware/Microsoft Hyper-V – High Profile
EMS Managed Devices	5000	100	5000
Maximum number of managed endpoints in EMS (IP Phone Manager only).	-	-	30,000 (VMware only).
SEM			
Maximum Number of CAPS (calls attempts per second) per device.	160	30	120
Maximum number of CAPS per server (SBC and Skype for Business).	300	30	120
Maximum concurrent sessions	30,000	3,000	12,000
Maximum number of devices per region	500	100	300
Maximum number of managed devices.	3,000	100	1,200
Maximum number of links between devices.	6,000	200	2,400
Call Details Storage - Detailed information per Call	Up to two months or 80 million calls.	Up to two months or 6 million rows.	Up to two months or 80 million rows.
Calls Statistics Storage - Statistic information storage.	Up to six months or 150 million intervals.	Up to six months or 12 million rows.	Up to six months or 150 million rows.
Maximum number of managed endpoints in both EMS (IP Phone Manager) and SEM.	10000	1000	5000
Maximum number of CAPS per endpoint.	10	1	5

3.4 Microsoft Lync Monitoring SQL Server Prerequisites

Following are the Microsoft Lync Monitoring SQL Server prerequisites:

- The server must be defined to accept login in 'Mix Authentication' mode.
- The server must be configured to collect calls before the SEM can connect to it and extract Lync calls.
- Call Detail Records (CDRs) and Quality of Experience (QoE) Data policies must be configured to capture data.
- Network administrators must be granted the correct database permissions (refer to the *SEM User's Manual*).
- Excel macros must be enabled so that the SQL queries and reports can be run. This was tested with Excel 2010.
- Detailed minimum requirements for Microsoft Lync SQL Server can be found in the following link:

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

This page is intentionally left blank.

4 EMS Software Deliverables

This section describes the EMS software deliverables.

4.1 Dedicated Hardware Installation – DVDs 1-4

This section describes the DVDs supplied in the EMS software delivery.

- **DVD1:** Operating System DVD for Linux:
    - Linux (CentOS) 5.9 Installation for EMS server, REV7

      The following machine is currently supported:
        - HP DL360p G8 - Linux (CentOS) 64-bit kernel version 5.9 Installation for EMS server, Linux CentOS 5.9 REV7 or REV8 for EMS-HA.
- **DVD2:** Oracle Installation: Oracle installation version *11g* DVD for the Linux platform.
- **DVD3:** Software Installation and Documentation DVD for Linux:

  The DVD ‘SW Installation and Documentation’ DVD comprises the following folders:
    - Documentation – All documentation related to the present EMS version. The documentation folder includes the following documents and sub-folders:
        - EMS Release Notes Document – includes the list of the new features introduced in the current software version as well as version restrictions and limitations.
        - EMS Server IOM Manual – Installation, Operation and Maintenance Guide.
        - EMS Product Description Document
        - EMS User's Manual Document
        - OAMP Integration Guide Document
        - 'GWs_OAM_Guides' folder – document set describing Provisioning parameters and Alarm/Performance measurements parameters supported for each one of the products or product families.
        - 'Private_Labeling' folder – includes all the information required for the OEM to create a new private labeling DVD. EmsClientInstall – EMS client software to be installed on the operator’s Windows™ based workstation.
    - 'EmsClientInstall'-EMS client software to install on the designated client workstation PC.
    - 'EmsServerInstall' – EMS server software, to install on the dedicated Linux based EMS server machine.
- **DVD4:** (relevant for future releases) EMS Server Patches: Upgrade patches DVD containing OS (Linux) patches, Oracle patches, java patches or any other EMS required patches. This DVD enables the upgrading of the required EMS patches without the EMS application upgrade.

4.2 VMware – DVD 5

The EMS software delivery for the VMware DVD includes the following folders:

- VMware for clean install
- EMS client Install
- Documentation

4.3 Hyper-V – DVD 5

The EMS software delivery for the Hyper-V DVD includes the following folders:

- Hyper-V for clean install
- EMS client Install
- Documentation

Part II

EMS Server Installation

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

5 Testing Installation Requirements - Dedicated Hardware

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

5.1 Hardware Requirements

- **Operating System** – the Linux Operating Systems are supported.

  To determine the system OS, enter the following command:

```
uname
```

  This command returns **Linux**. Proceed to the following section :

  - Testing Hardware Requirements on Linux OS (see Section 5.1.1 on page 33).

5.1.1 Testing Hardware Requirements on the Linux Platform

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

- **RAM** - A minimum of <machine type_RAM> GB is required (see Chapter 3 on page 23). 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
```

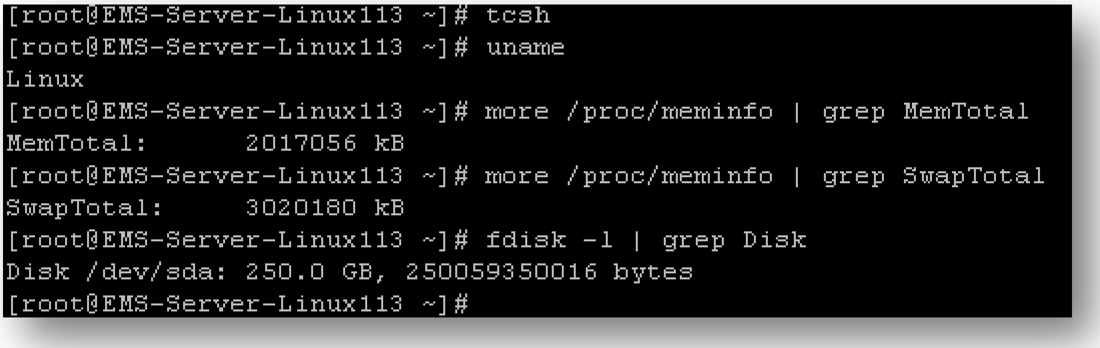
Disk Space – A minimum of <machine type_disk space> GB is required (see Chapter 3 on page 23). To determine the amount of disk space on your system, enter the following command:

```
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 5-1: 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.

6 Installing the EMS Server on Dedicated Hardware

The EMS 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:** EMS application: EMS server application installation DVD .
- **DVD4:** (relevant for future releases) EMS Server Patches: Upgrade patches DVD containing OS (Linux) patches, Oracle patches, java patches or any other EMS required patches. This DVD enables the upgrading of the EMS required patches without the EMS application upgrade.

While a clean installation requires the first three DVDs (DVD1, DVD2 and DVD3), an EMS application upgrade requires only the 'EMS server application (DVD3)'. The 'Patches upgrade' requires only the 'EMS server Patches (DVD4)'.

6.1 ISO Files Verification

If you have received an ISO file from AudioCodes instead of a burned DVD, its contents must be verified 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 6.1.2).

6.1.1 Windows

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

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

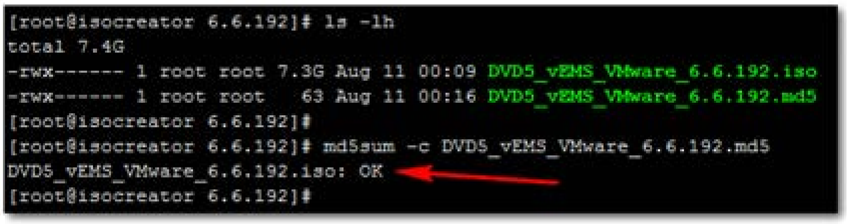
6.1.2 Linux

Copy the checksum and the ISO 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 6-1: ISO File Integrity Verification



```
[root@isocreator 6.6.192]# ls -lh
total 7.4G
-rwx------ 1 root root 7.3G Aug 11 00:09 DVD5_vEMS_VMware_6.6.192.iso
-rwx------ 1 root root   63 Aug 11 00:16 DVD5_vEMS_VMware_6.6.192.md5
[root@isocreator 6.6.192]#
[root@isocreator 6.6.192]# md5sum -c DVD5_vEMS_VMware_6.6.192.md5
DVD5_vEMS_VMware_6.6.192.iso: OK
[root@isocreator 6.6.192]#
```

6.2 Installing the EMS Server on the Linux Platform

This section describes how to install the EMS server on the Linux platform.

6.2.1 DVD1: Linux CentOS 5.9

The procedure below describes how to install Linux CentOS 5.9. This procedure takes approximately 20 minutes.

Note: If you are installing the EMS server on an HP ProLiant DL360p Gen8 server, before commencing this procedure, you must configure RAID-0 (see Appendix C on page 227).

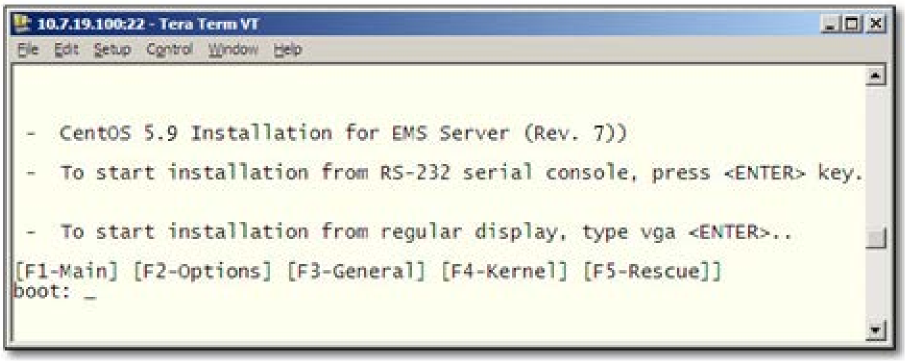
➢ To perform DVD1 installation:

1. Insert the **DVD1-Linux for EMS Rev7** (CentOS 5.9) into the DVD ROM.
2. Connect the EMS server through the serial port with a terminal application and login with 'root' user. Default password is *root*.
3. Perform EMS server machine reboot by specifying the following command:

```
reboot
```

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

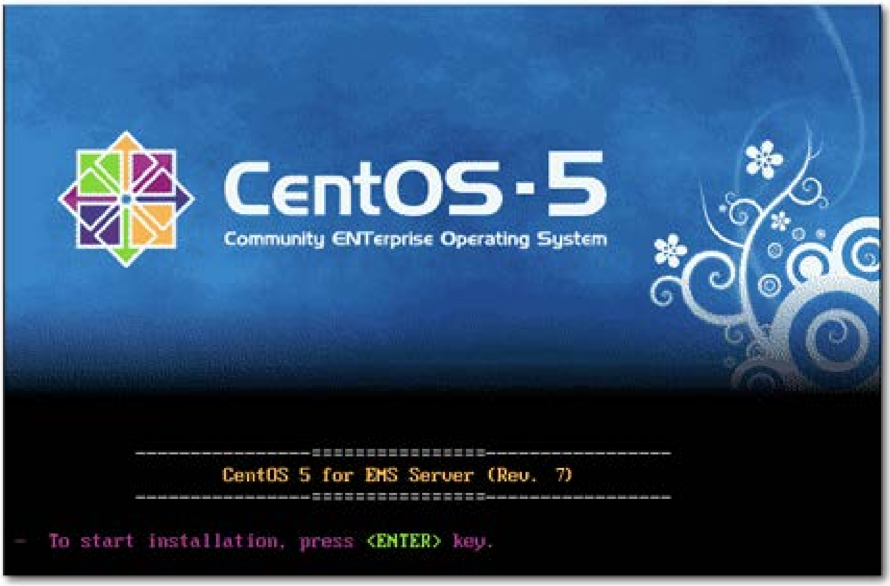
Figure 6-2: Linux CentOS Installation



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

```
-  CentOS 5.9 Installation for EMS Server (Rev. 7))
-  To start installation from RS-232 serial console, press <ENTER> key.

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

Figure 6-3: CentOS 5

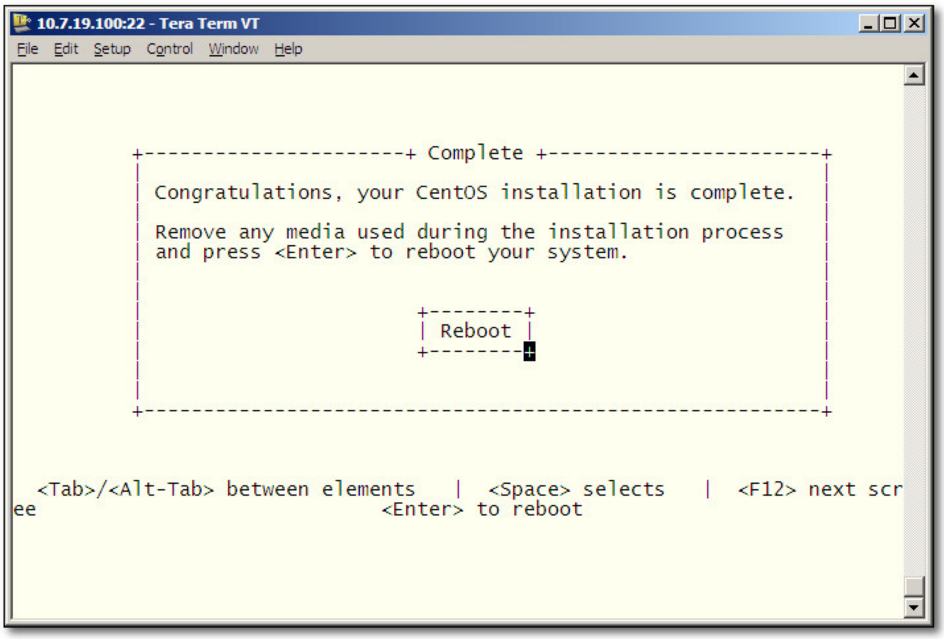


```
---------------================---------------
        CentOS 5 for EMS Server (Rev. 7)
---------------================---------------

-  To start installation, press <ENTER> key.
```

6. Wait for the installation to complete.
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 6-4: Linux CentOS Installation Complete

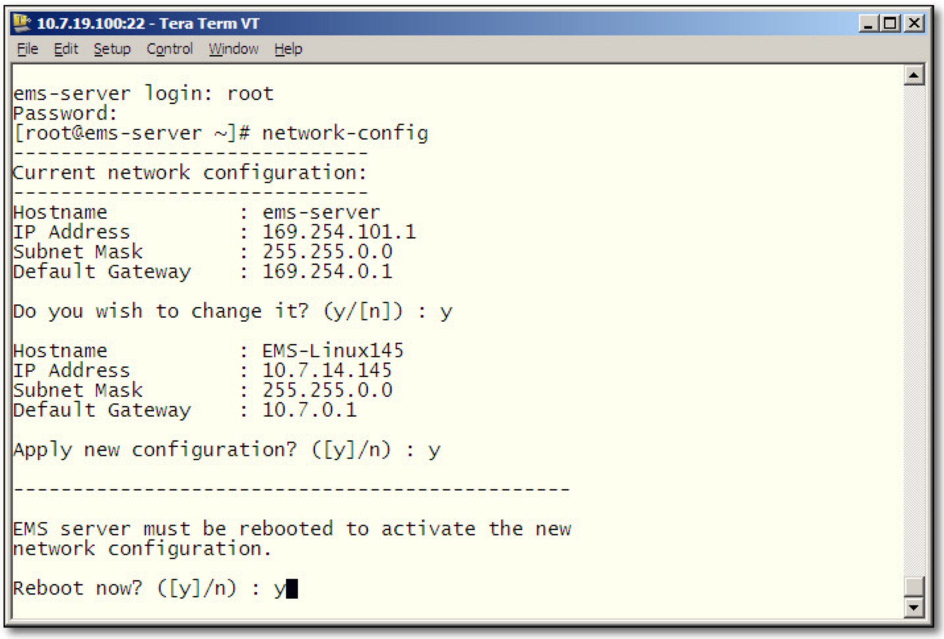


```
          +----------------------+ Complete +-----------------------+
          |                                                         |
          | Congratulations, your CentOS installation is complete.  |
          |                                                         |
          | Remove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



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

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

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

Figure 6-5: Linux CentOS Network Configuration


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

```
ems-server login: root
Password:
[root@ems-server ~]# network-config
------------------------------
Current network configuration:
------------------------------
Hostname            : ems-server
IP Address          : 169.254.101.1
Subnet Mask         : 255.255.0.0
Default Gateway     : 169.254.0.1

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

Hostname            : EMS-Linux145
IP Address          : 10.7.14.145
Subnet Mask         : 255.255.0.0
Default Gateway     : 10.7.0.1

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

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

EMS server must be rebooted to activate the new
network configuration.

Reboot now? ([y]/n) : y
```

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**.

6.2.2 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 EMS 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
```

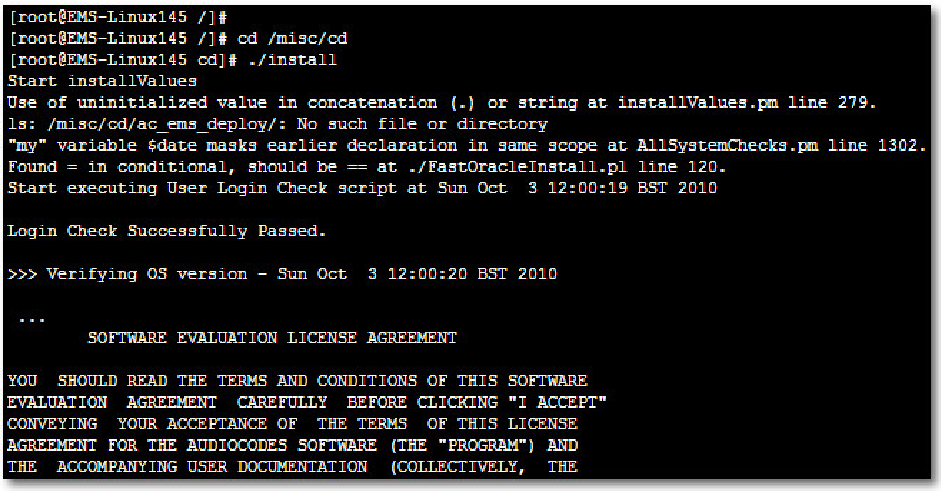
4. On some machines, you need to mount the CDROM in order to make it available:

```
mount /misc/cd
```

5. Run the installation script from its location:

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

Figure 6-6: Oracle DB Installation (Linux)

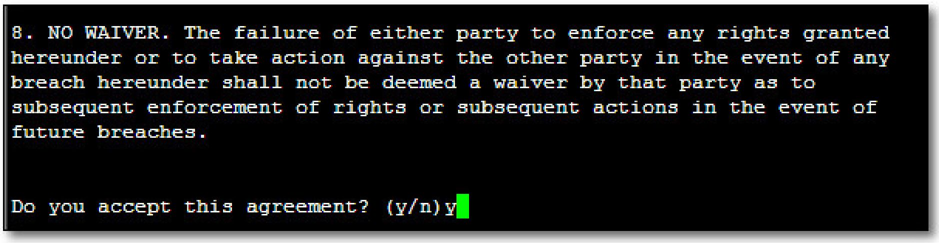


```
[root@EMS-Linux145 /]#
[root@EMS-Linux145 /]# cd /misc/cd
[root@EMS-Linux145 cd]# ./install
Start installValues
Use of uninitialized value in concatenation (.) or string at installValues.pm line 279.
ls: /misc/cd/ac_ems_deploy/: No such file or directory
"my" variable $date masks earlier declaration 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.

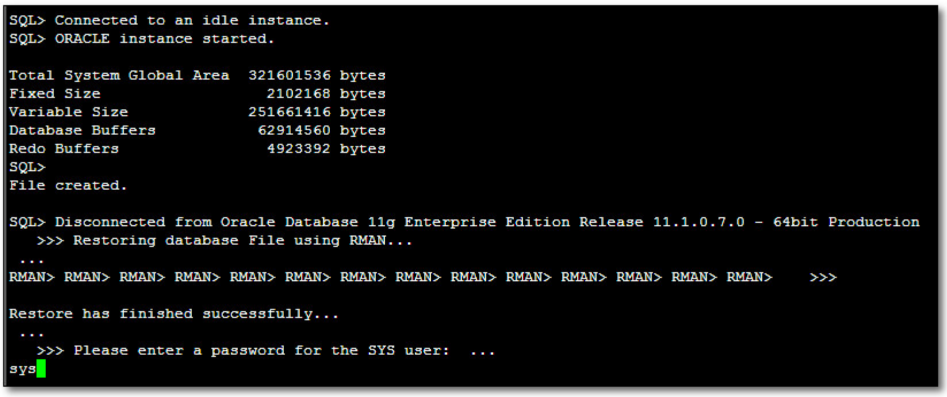
Figure 6-7: Oracle DB Installation - License Agreement (Linux)



```
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.

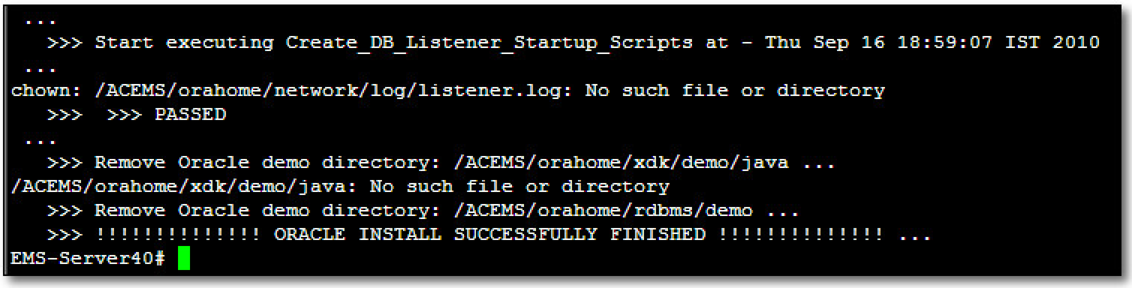
Figure 6-8: Oracle DB Installation (Linux) (cont)



```
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 6-9: 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#
```

6.2.3 DVD3: EMS Server Application Installation

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

➢ To perform DVD3 installation:

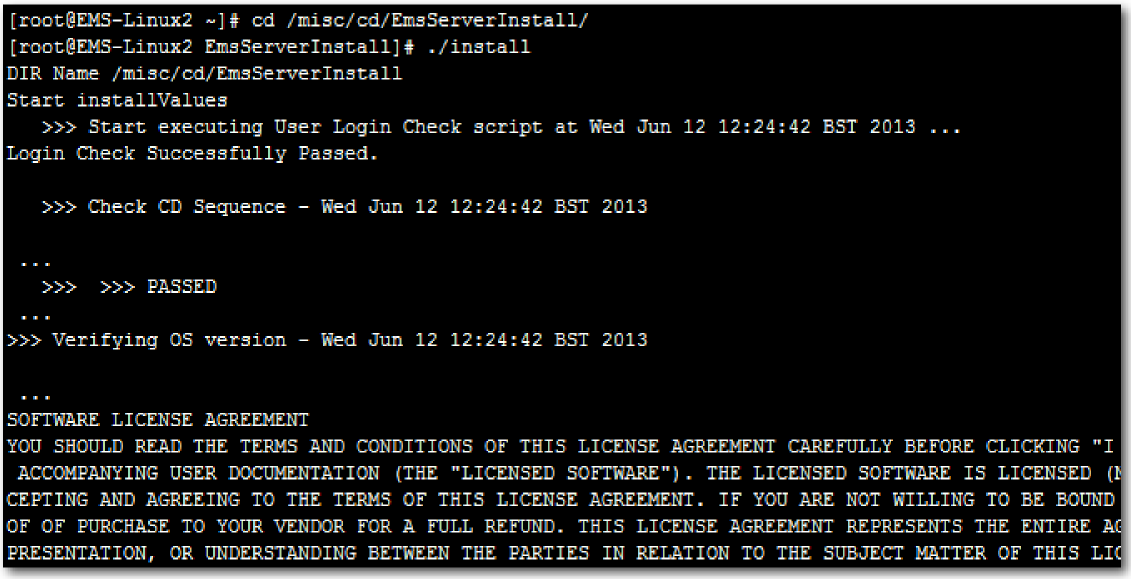
1. Insert **DVD3-EMS Server Application Installation** into the DVD ROM.
2. Login into the EMS server by SSH, as 'acems' user, and enter the password *acems*.
3. Switch to 'root' user and provide *root* password (default password is *root*):

```
su – root
```

4. Run the installation script from its location:

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

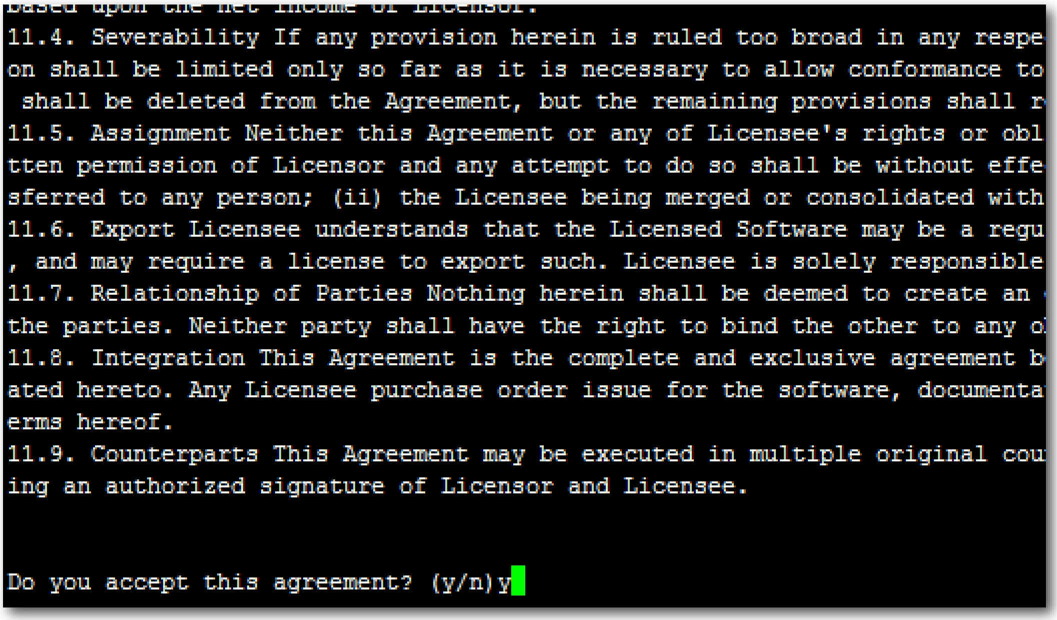
Figure 6-10: EMS Server Application Installation (Linux)



```
[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 (
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.

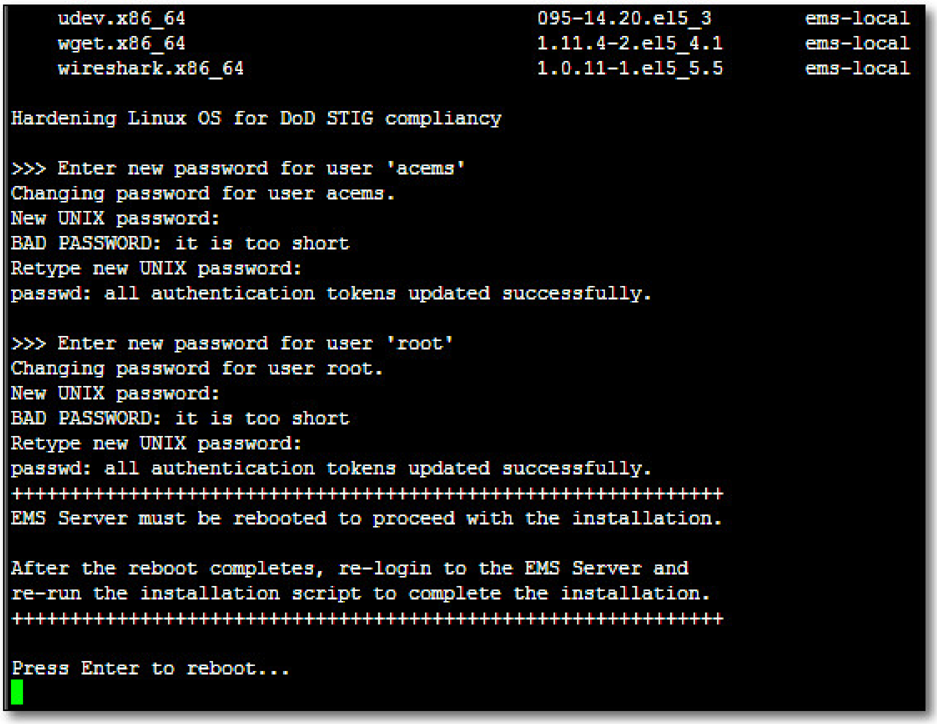
Figure 6-11: EMS Server Application Installation (Linux) – License Agreement



```
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 EMS server machine; press Enter.

Figure 6-12: EMS Server Application Installation (Linux) (cont)

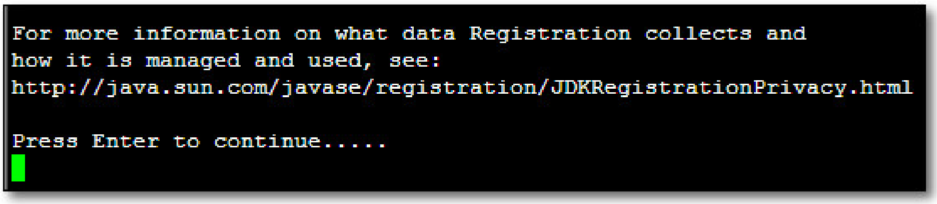


```
    udev.x86_64                            095-14.20.el5_3        ems-local
    wget.x86_64                            1.11.4-2.el5_4.1       ems-local
    wireshark.x86_64                       1.0.11-1.el5_5.5       ems-local

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 EMS server has successfully rebooted, repeat steps 2 – 4.

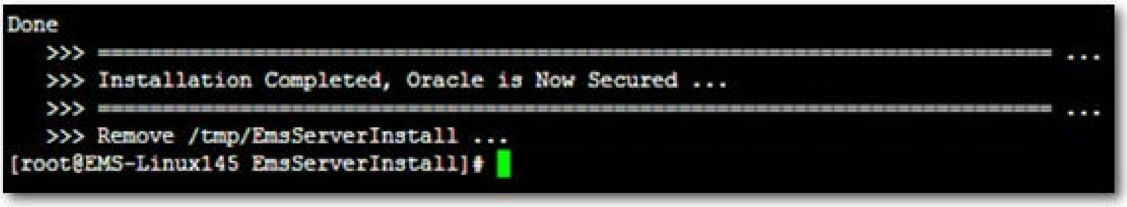
8. At the end of Java installation, press Enter to continue.

Figure 6-13: EMS 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 reboot the EMS server by typing **reboot**.



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

10. When the EMS server has successfully restarted login into the EMS 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 that the Date and Time are set correctly (see Section 18.3 to set the date and time).

13. Verify that the EMS server is up and running (see Chapter 13 and login by client to verify a successful installation).

6.3 EMS Server Users

EMS 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 EMS server includes the following OS user permissions:

- 'root' user: User permissions for installation, upgrade, maintenance using EMS server manager and EMS 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 EMS 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.

This page is intentionally left blank.

7 Installing the EMS on Virtual Server Platform

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

- Installing the EMS server on the VMware platform (see Section 7.1 on page 47).
- Installing the EMS server on Microsoft Hyper-V platform (see Section 7.2 on page 60).

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

7.1 Installing the EMS Server on the VMware Platform

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

- Installing the Virtual Machine (VM) (see Section 7.1.1).
- Configuring the Virtual machine hardware settings (see Section 7.2.2).
- Connecting EMS server to network (see Section 7.1.3).
- Configuring EMS Virtual Machines (VMs) in a VMware Cluster (see Section 7.1.4)

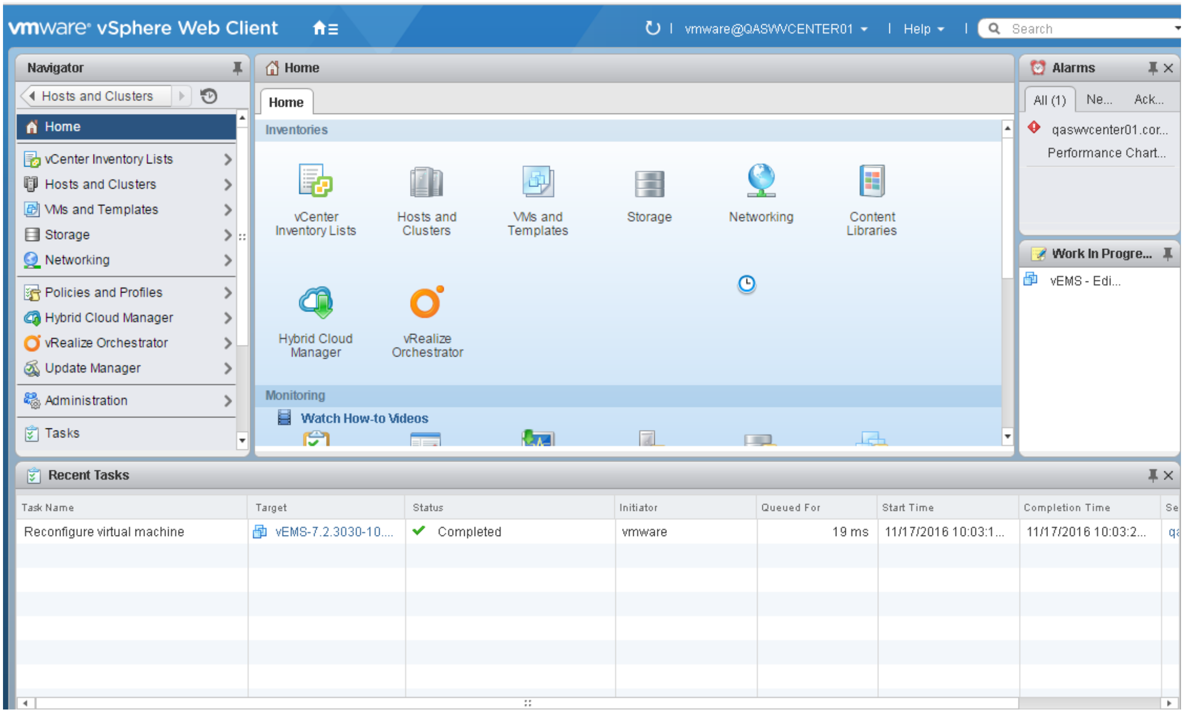
7.1.1 Installing the VMware Virtual Machine

This section describes how to install the EMS 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 5.1.1). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed.

➢ **To install the EMS Server on VMware vSphere:**

1. Insert the vEMS installation DVD (**DVD5**) into the disk drive on the PC where the vSphere client is installed.
2. Login to the VMware vSphere Web client.

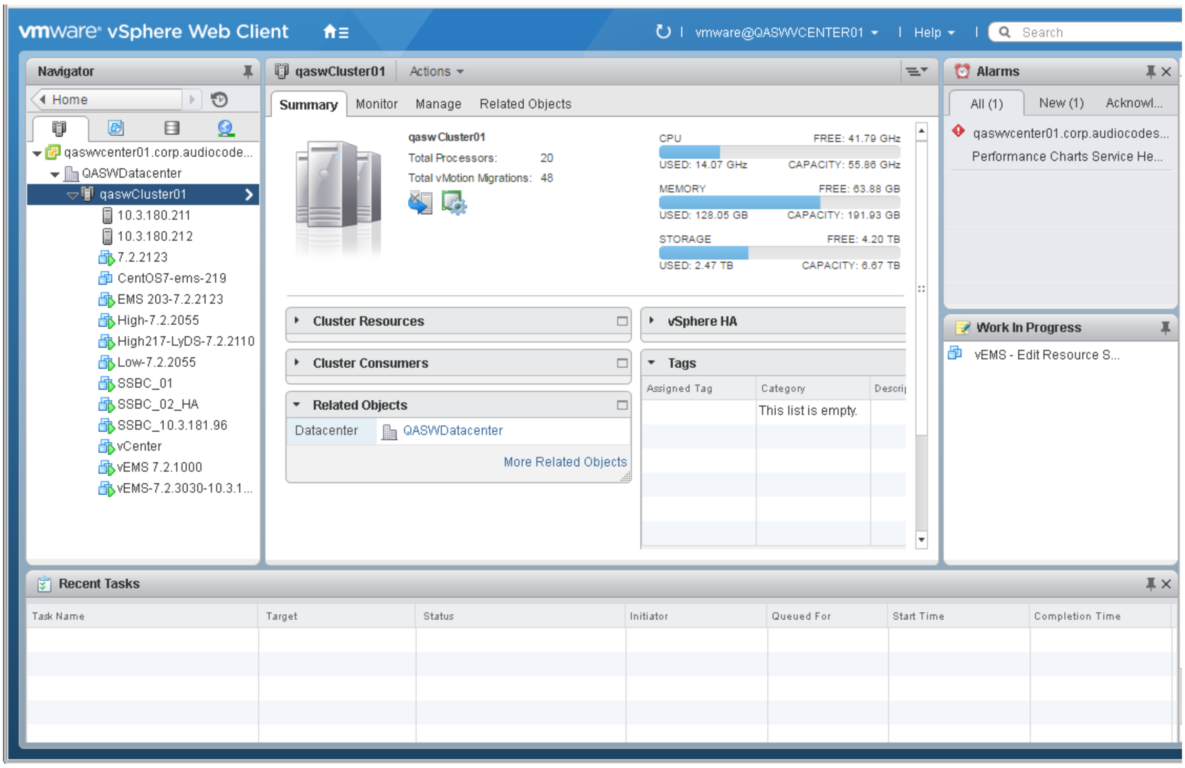
Figure 7-1: Vmware vSphere Web Client



Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Se
Reconfigure virtual machine	vEMS-7.2.3030-10....	✓ Completed	vmware	19 ms	11/17/2016 10:03:1...	11/17/2016 10:03:2...	qa

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

Figure 7-2: Hosts and Clusters



qaswCluster01
Total Processors: 20
Total vMotion Migrations: 48

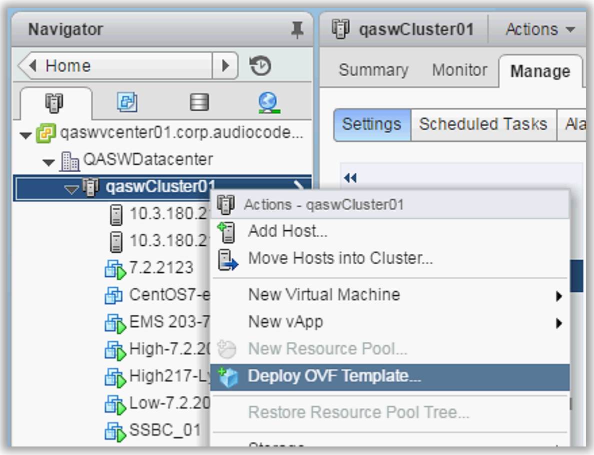
CPU FREE: 41.79 GHz
USED: 14.07 GHz CAPACITY: 55.86 GHz
MEMORY FREE: 63.88 GB
USED: 128.05 GB CAPACITY: 191.93 GB
STORAGE FREE: 4.20 TB
USED: 2.47 TB CAPACITY: 6.67 TB

Datacenter	QASWDatacenter

Assigned Tag	Category	Descri
	This list is empty.	

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time

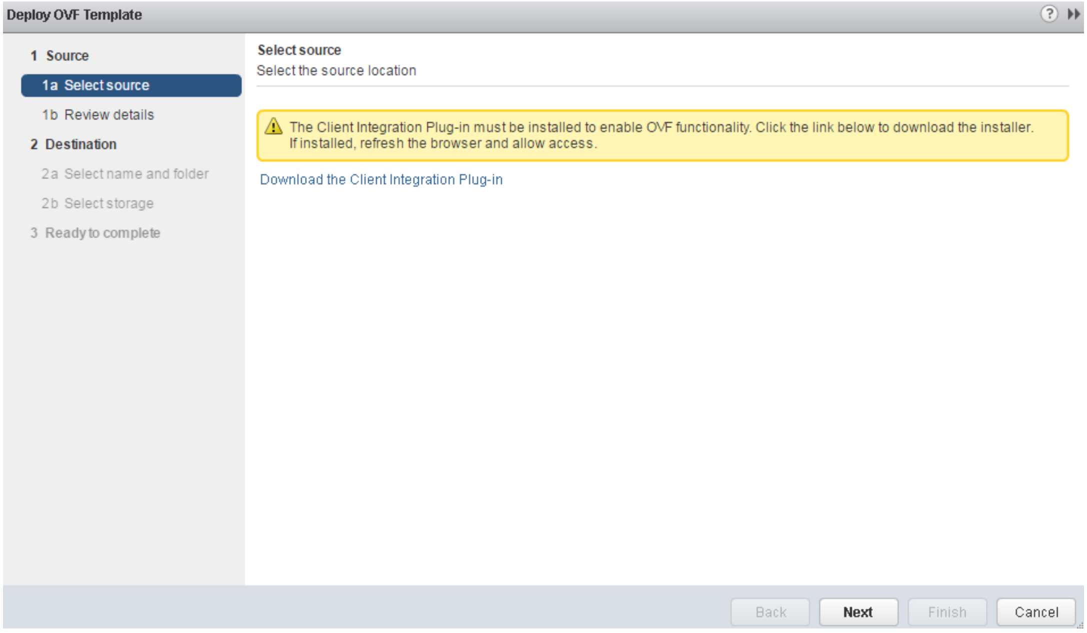
Figure 7-3: Deploy OVF Template Option



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 7-4: Client Integration Plug-in

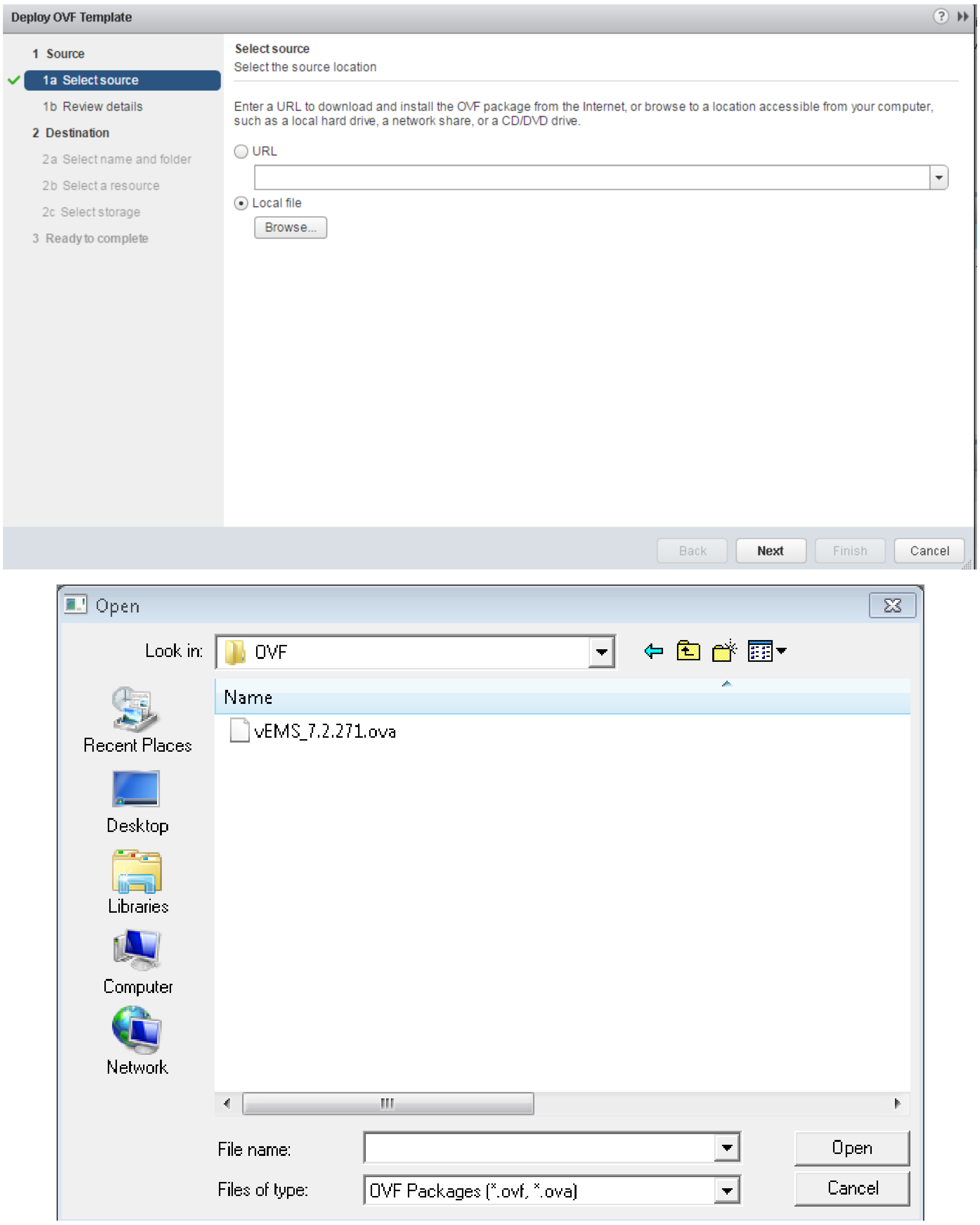


Select source
Select the source location

The Client Integration Plug-in must be installed to enable OVF functionality. Click the link below to download the installer. If installed, refresh the browser and allow access.

Download the Client Integration Plug-in

Figure 7-5: Browse to OVF Package



Deploy OVF Template

1 Source
1a Select source
1b Review details
2 Destination
2a Select name and folder
2b Select a resource
2c Select storage
3 Ready to complete

Select source
Select the source location

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

● Local file

Browse...

Back | Next | Finish | Cancel

Open

Look in: OVF

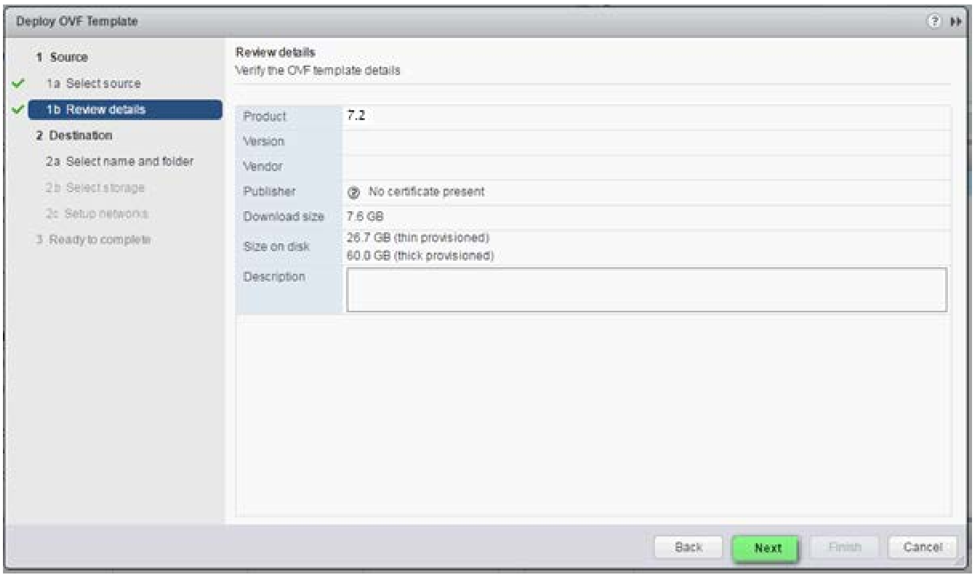
Name
vEMS_7.2.271.ova

File name:
Files of type: OVF Packages (*.ovf, *.ova)

Open | Cancel

5. Browse to the OVF file with extension OVA from the DVD disk, and click **Next**.

Figure 7-6: OVF Template Details Screen



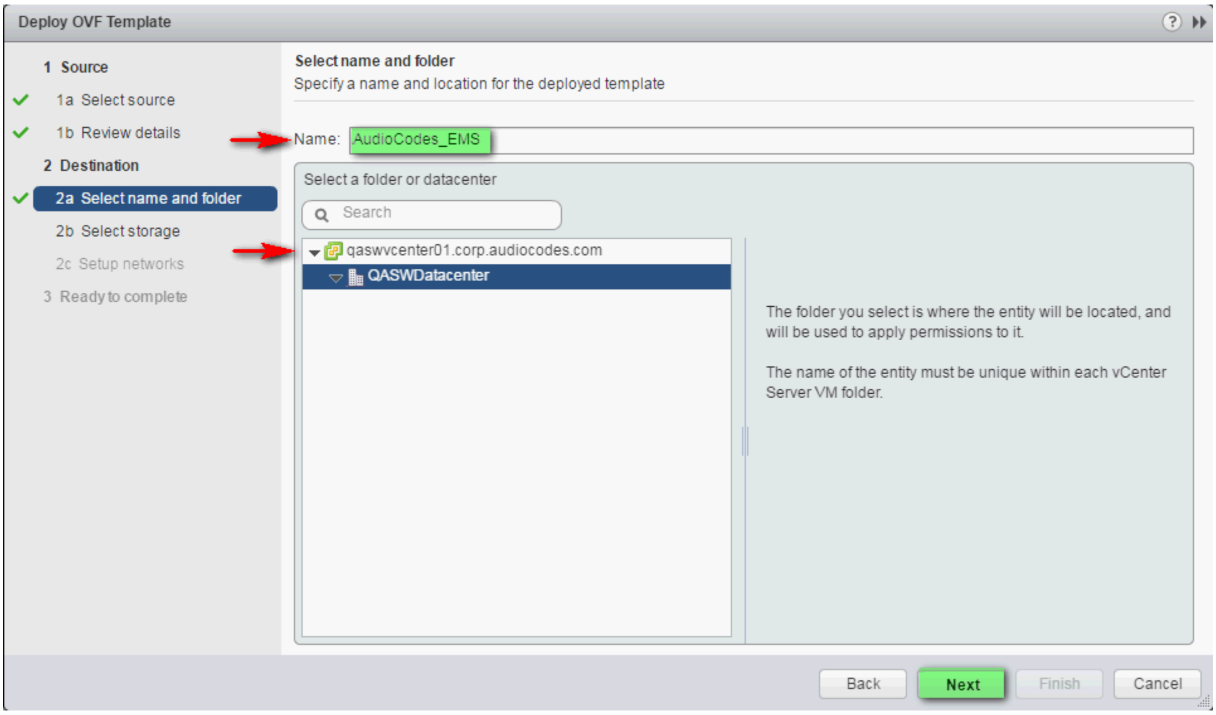
Review details

Verify the OVF template details

Product	7.2
Version	
Vendor	
Publisher	No certificate present
Download size	7.6 GB
Size on disk	26.7 GB (thin provisioned) 60.0 GB (thick provisioned)
Description	

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

Figure 7-7: Virtual Machine Name and Location Screen



Select name and folder

Specify a name and location for the deployed template

Name: AudioCodes_EMS

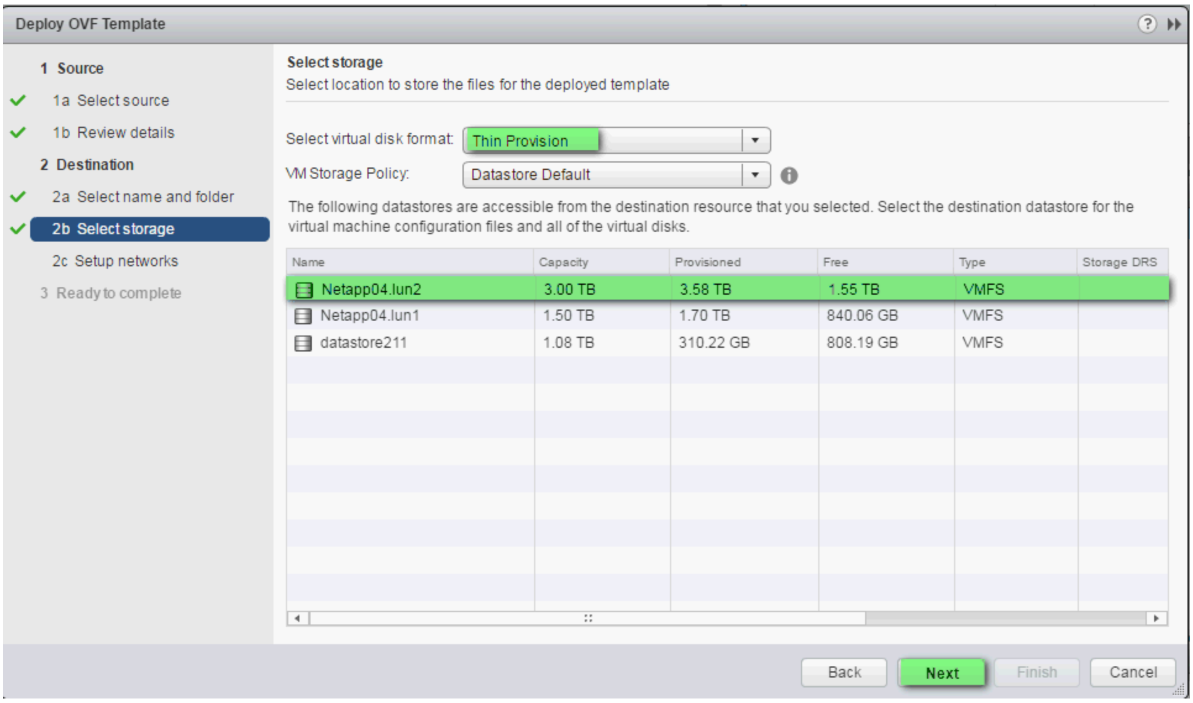
Select a folder or datacenter

The folder you select is where the entity will be located, and will be used to apply permissions to it.

The name of the entity must be unique within each vCenter Server VM folder.

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 7-8: Destination Storage Screen



Deploy OVF Template

1 Source

✓ 1a Select source

✓ 1b Review details

2 Destination

✓ 2a Select name and folder

✓ 2b Select storage

2c Setup networks

3 Ready to complete

Select storage

Select location to store the files for the deployed template

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

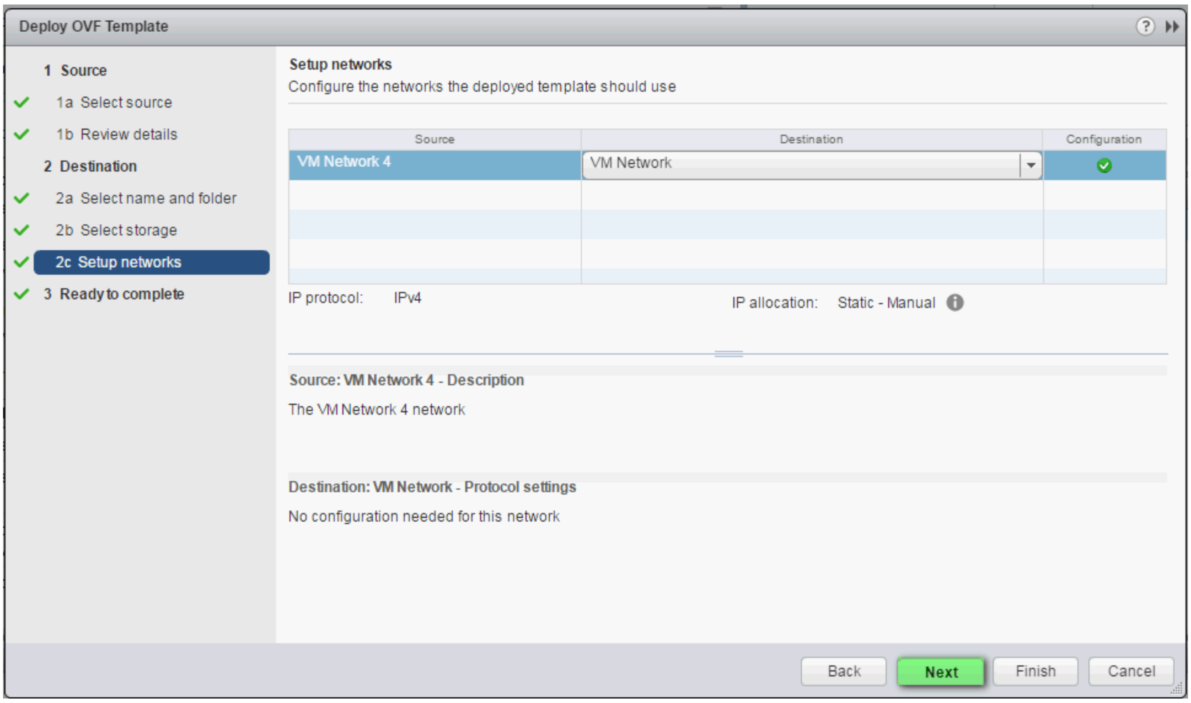
The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Storage DRS
Netapp04.lun2	3.00 TB	3.58 TB	1.55 TB	VMFS	
Netapp04.lun1	1.50 TB	1.70 TB	840.06 GB	VMFS	
datastore211	1.08 TB	310.22 GB	808.19 GB	VMFS	

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 7-9:: Setup Networking Screen



Setup networks

Configure the networks the deployed template should use

Source	Destination	Configuration
VM Network 4	VM Network	✓

IP protocol: IPv4

IP allocation: Static - Manual

Source: VM Network 4 - Description

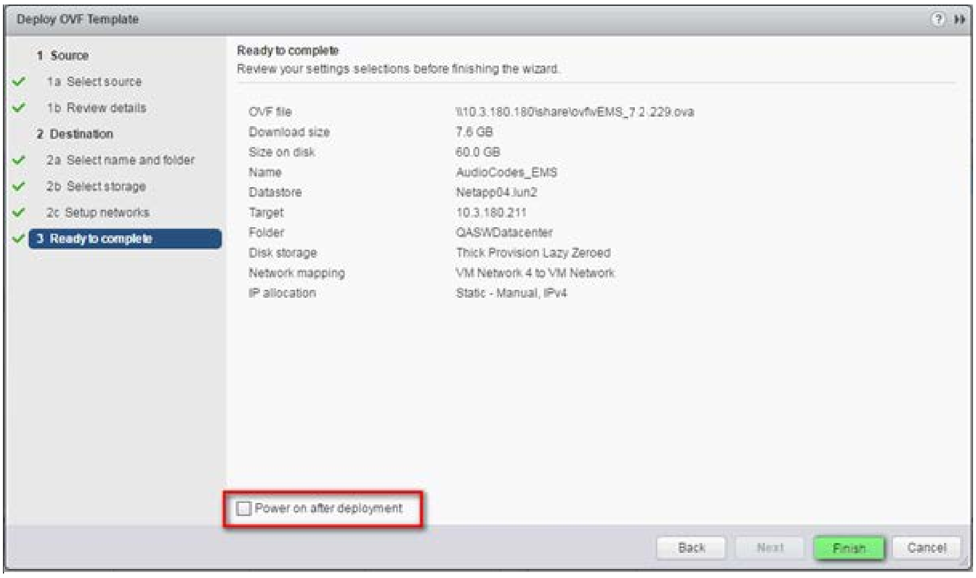
The VM Network 4 network

Destination: VM Network - Protocol settings

No configuration needed for this network

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

Figure 7-10: Ready to Complete Screen



Ready to complete

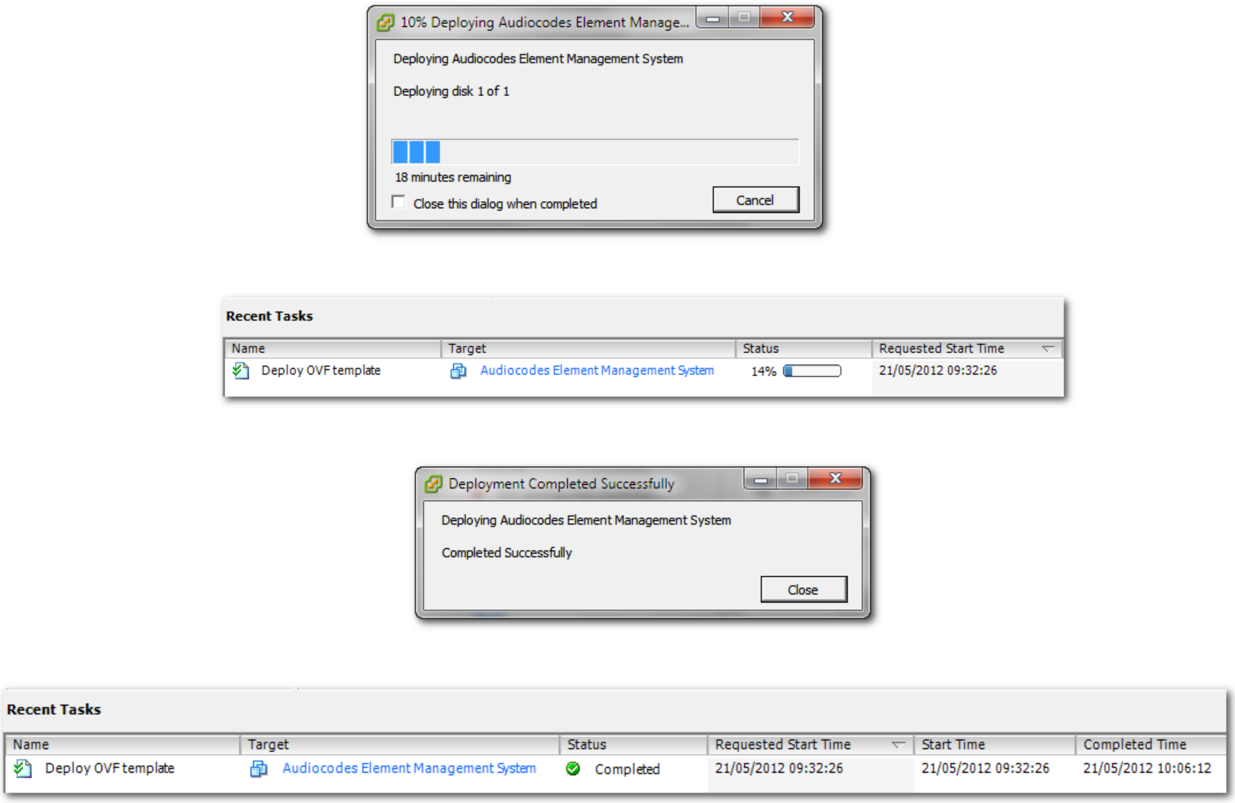
Review your settings selections before finishing the wizard.

OVF file	\\10.3.180.180\share\ovf\vEMS_7.2.229.ova
Download size	7.6 GB
Size on disk	60.0 GB
Name	AudioCodes_EMS
Datastore	Netapp04.lun2
Target	10.3.180.211
Folder	QASWDatacenter
Disk storage	Thick Provision Lazy Zeroed
Network mapping	VM Network 4 to VM Network
IP allocation	Static - Manual, IPv4

☐ Power on after deployment

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

Figure 7-11: Deployment Progress Screen



10% Deploying Audiocodes Element Manage...

Deploying Audiocodes Element Management System

Deploying disk 1 of 1

18 minutes remaining

□ Close this dialog when completed

Recent Tasks

Name	Target	Status	Requested Start Time
Deploy OVF template	Audiocodes Element Management System	14%	21/05/2012 09:32:26

Deployment Completed Successfully

Deploying Audiocodes Element Management System

Completed Successfully

Recent Tasks

Name	Target	Status	Requested Start Time	Start Time	Completed Time
Deploy OVF template	Audiocodes Element Management System	Completed	21/05/2012 09:32:26	21/05/2012 09:32:26	21/05/2012 10:06:12

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

7.1.2 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, see Chapter 3 on page 23.

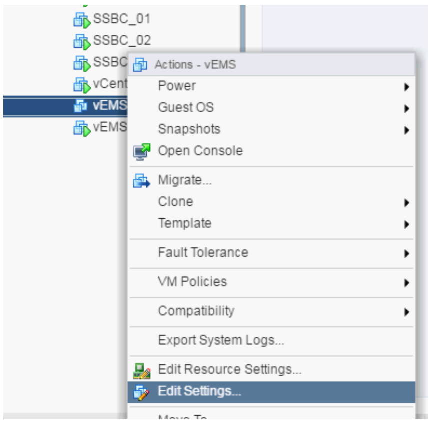
Table 7-1: Virtual Machine Configuration

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:

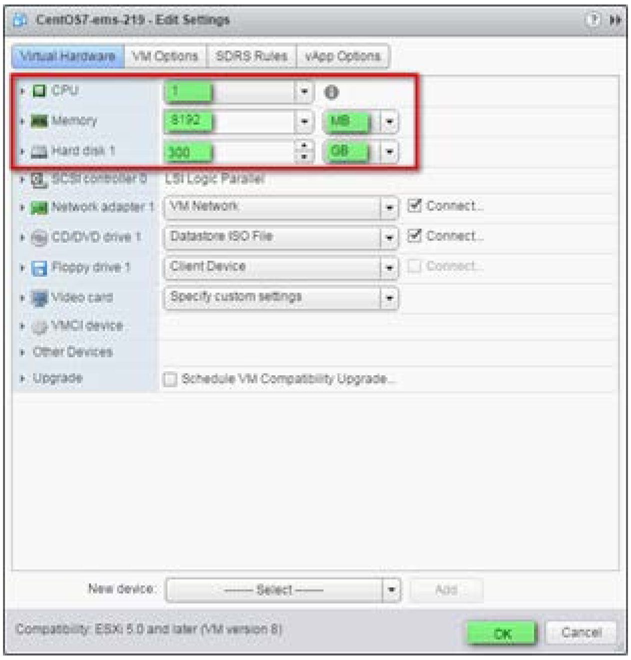
1. Before powering up the machine, go to the virtual machine **Edit Settings** option.

Figure 7-12: Edit Settings option



2. In the **CPU, Memory** and **Hardware** tabs set the required values accordingly to the desired EMS server VMware Disk Space allocation. (See Chapter 3 on page 23), and then click **OK**.

Figure 7-13: CPU, Memory and Hard Disk Settings



CPU: 1
Memory: 8192 MB
Hard disk 1: 300 GB
SCSI controller 0: LSI Logic Parallel
Network adapter 1: VM Network ☑ Connect...
CD/DVD drive 1: Datastore ISO File ☑ Connect...
Floppy drive 1: Client Device □ Connect...
Video card: Specify custom settings
VMCI device
Other Devices
Upgrade: □ Schedule VM Compatibility Upgrade...

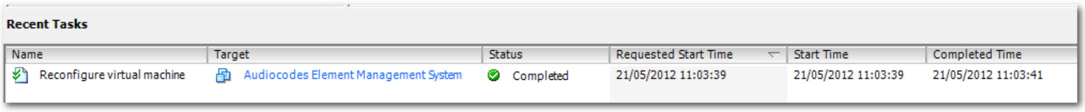
Compatibility: ESXi 5.0 and later (VM version 8)

Note:

- Once the hard disk space allocation is increased, it cannot be reduced to a lower amount.
- If you wish to create EMS 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 7.1.4).

3. **Wait** until the machine reconfiguration process has completed.

Figure 7-14: Recent Tasks



Recent Tasks

Name	Target	Status	Requested Start Time	Start Time	Completed Time
Reconfigure virtual machine	Audiocodes Element Management System	Completed	21/05/2012 11:03:39	21/05/2012 11:03:39	21/05/2012 11:03:41

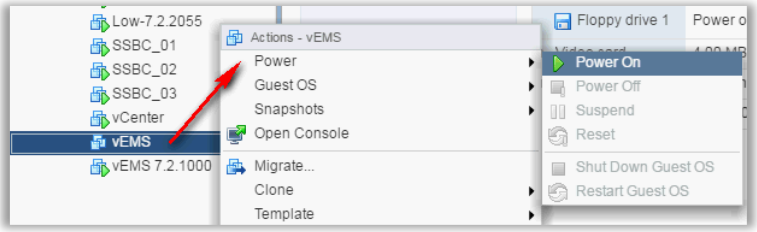
7.1.3 Connecting EMS Server to Network

After installation, the EMS 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 EMS server installation. You need to change this IP address to suit your IP addressing scheme

➢ To assign EMS Server IP address to network:

1. Power on the machine; in the vCenter tree, right-click the AudioCodes Element Management System 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 (see Chapter 3 on page 23).

Figure 7-15: 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 EMS server by SSH, as 'acems' user and enter *acems* password.
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su – root
```

5. Proceed to the network configuration using the Ems Server Manager. To run the manager type 'EmsServerManager', and then press Enter.
6. Set the EMS server network IP address as described in Section 17.1.
7. Perform configuration actions as required using the EMS Server Manager (see Chapter 12 on page 103).

7.1.4 Configuring EMS Virtual Machines (VMs) in a VMware Cluster

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

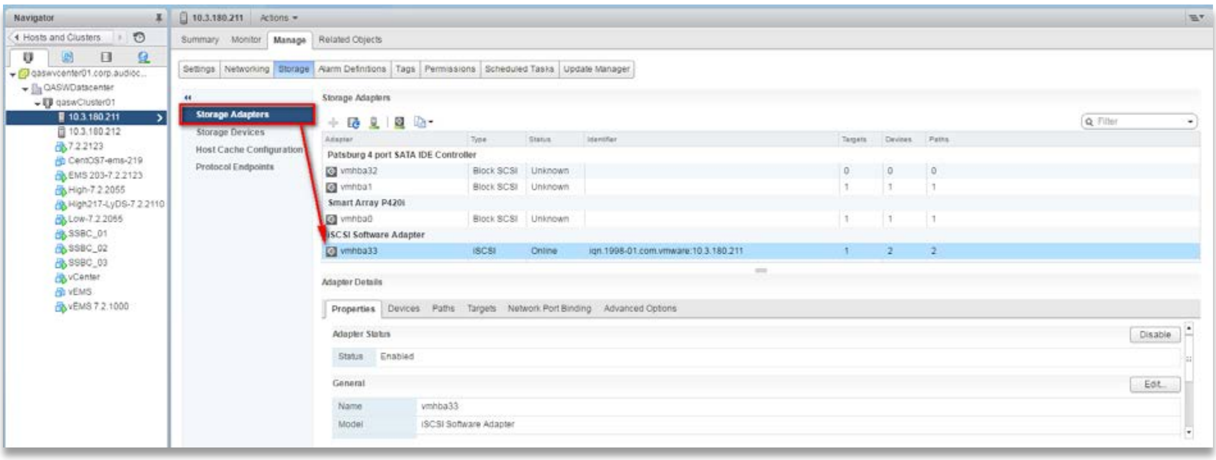
7.1.4.1 Site Requirements

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 7-16: Storage Adapters



Storage Adapters

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

Adapter Details

Adapter Status

Status: Enabled

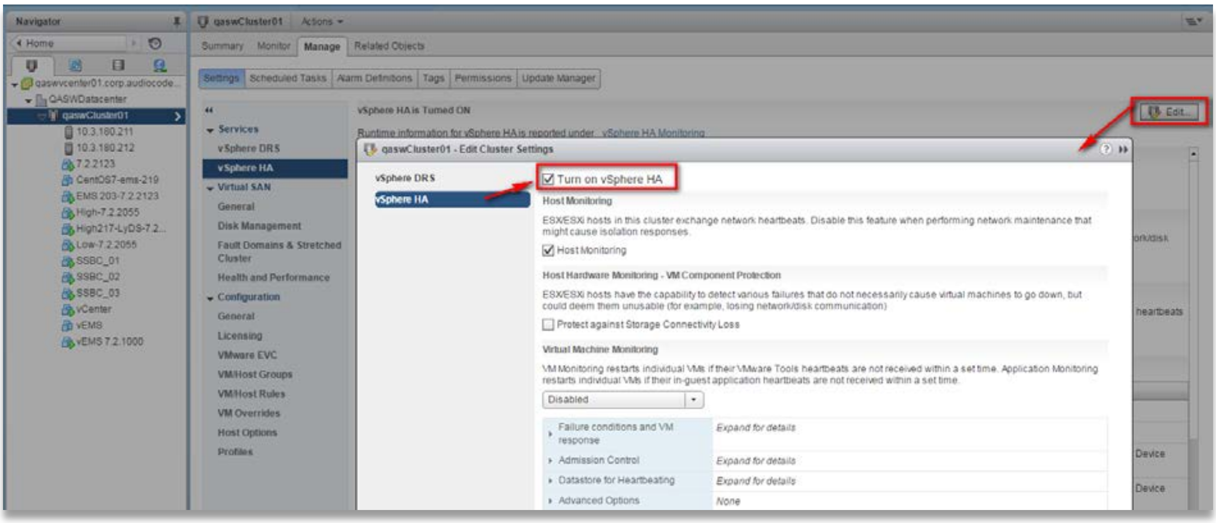
General

Name: vmhba33

Model: iSCSI Software Adapter

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

Figure 7-17:Turn On vSphere HA



vSphere HA is Turned ON

Runtime information for vSphere HA is reported under vSphere HA Monitoring

qaswCluster01 - Edit Cluster Settings

☑ Turn on vSphere HA

Host Monitoring

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

☑ Host Monitoring

Host Hardware Monitoring - VM Component Protection

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

□ Protect against Storage Connectivity Loss

Virtual Machine Monitoring

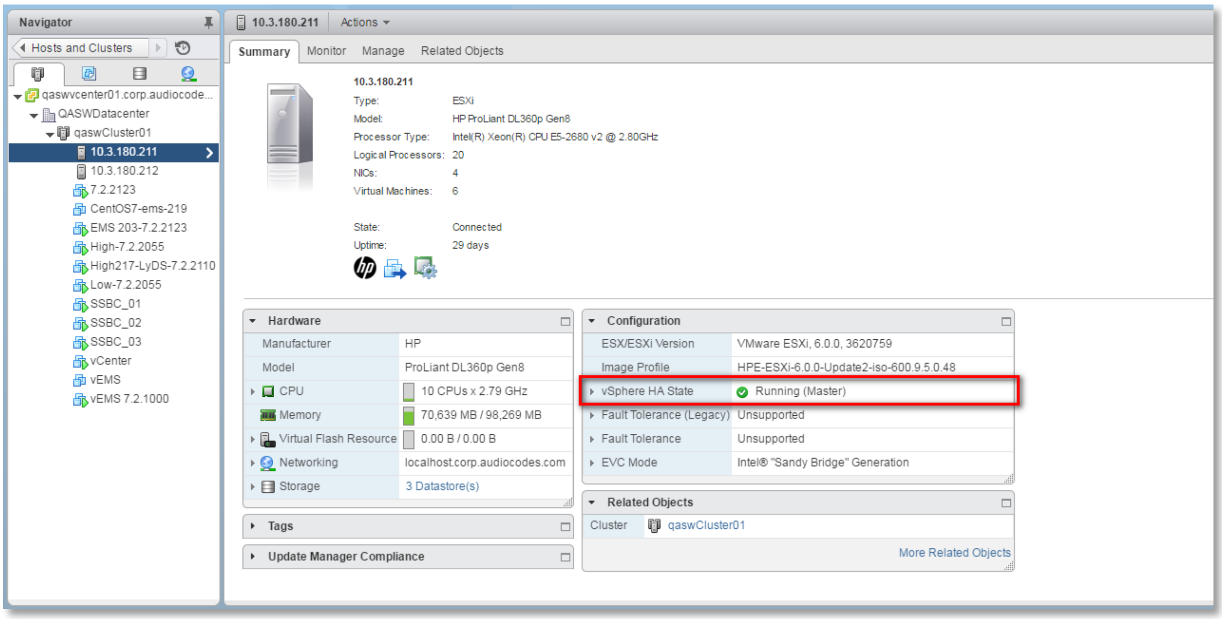
VM Monitoring restarts individual VMs if their VMware Tools heartbeats are not received within a set time. Application Monitoring restarts individual VMs if their in-guest application heartbeats are not received within a set time.

Disabled

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

- Ensure that HA is activated on each cluster node:

Figure 7-18: Activate HA on each Cluster Node



10.3.180.211

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

Hardware

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

Configuration

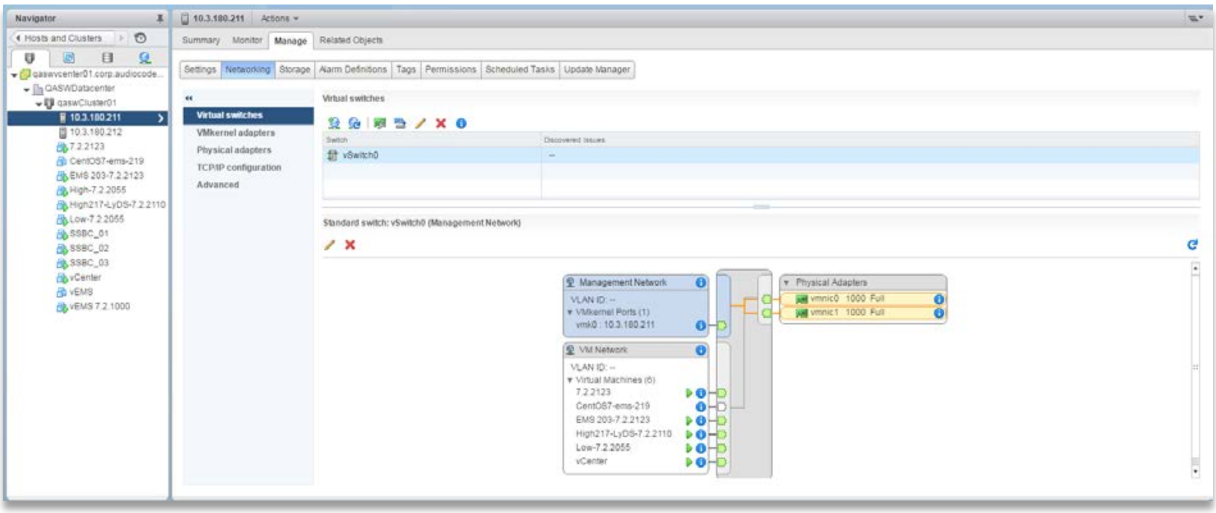
ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759
Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.0.48
vSphere HA State	Running (Master)
Fault Tolerance (Legacy)	Unsupported
Fault Tolerance	Unsupported
EVC Mode	Intel® "Sandy Bridge" Generation

Related Objects

Cluster	qaswCluster01

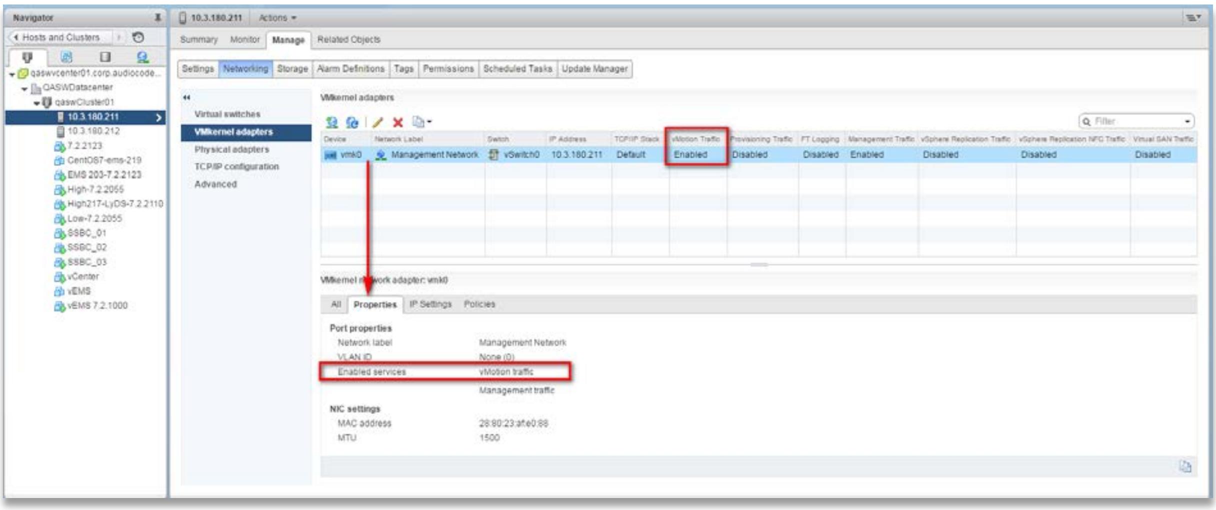
- Ensure that the networking configuration is identical on each cluster node:

Figure 7-19: 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 7-20: Switch Properties



VMkernel adapters

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

VMkernel network adapter: vmk0

All | Properties | IP Settings | Policies

Port properties

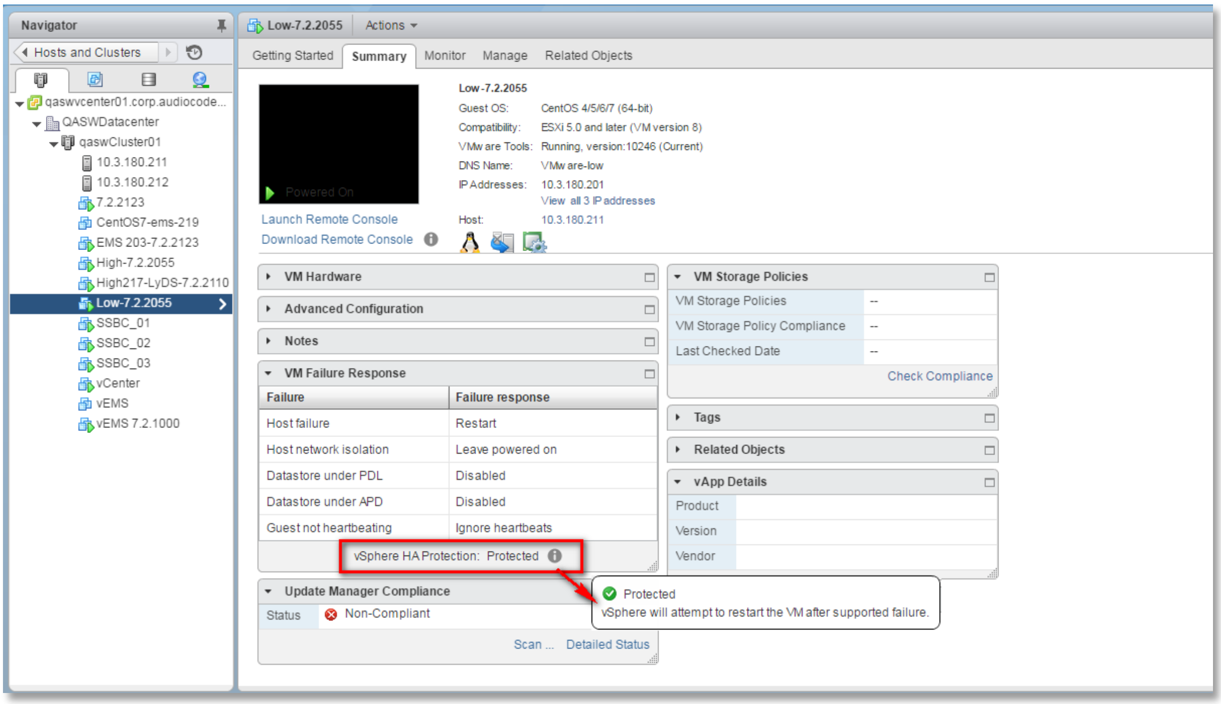
Network label	Management Network
VLAN ID	None (0)
Enabled services	vMotion traffic Management traffic

NIC settings

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

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

Figure 7-19: Protected VM



Low-7.2.2055

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

VM Failure Response

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

vSphere HA Protection: Protected

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

Update Manager Compliance

Status	Non-Compliant

VM Storage Policies

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

vApp Details

Product	
Version	
Vendor	

Note: If you wish to manually migrate the EMS VMs to another cluster node, see Appendix D.

7.1.4.2 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 EMS VM is automatically migrated to the redundant host node. During this process, the EMS VM is restarted and consequently any running EMS or SEM processes are dropped. The migration process may take several minutes.

7.2 Installing the EMS Server on Microsoft Hyper-V Platform

This section describes how to install the EMS 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 EMS supports the Failover Clustering feature in Windows Server 2012 R2 (see Chapter 3 on page 17).

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

- Install the Virtual Machine (VM) (see Section 7.2.1).
- Configure the Virtual machine hardware settings (see Section 7.2.2).
- Change MAC Addresses from 'Dynamic' to 'Static' (see Section 7.2.3).
- Connect EMS server to network (see Section 7.2.4).
- Configure VMs in a Microsoft Hyper-V cluster (see Section 7.2.5)

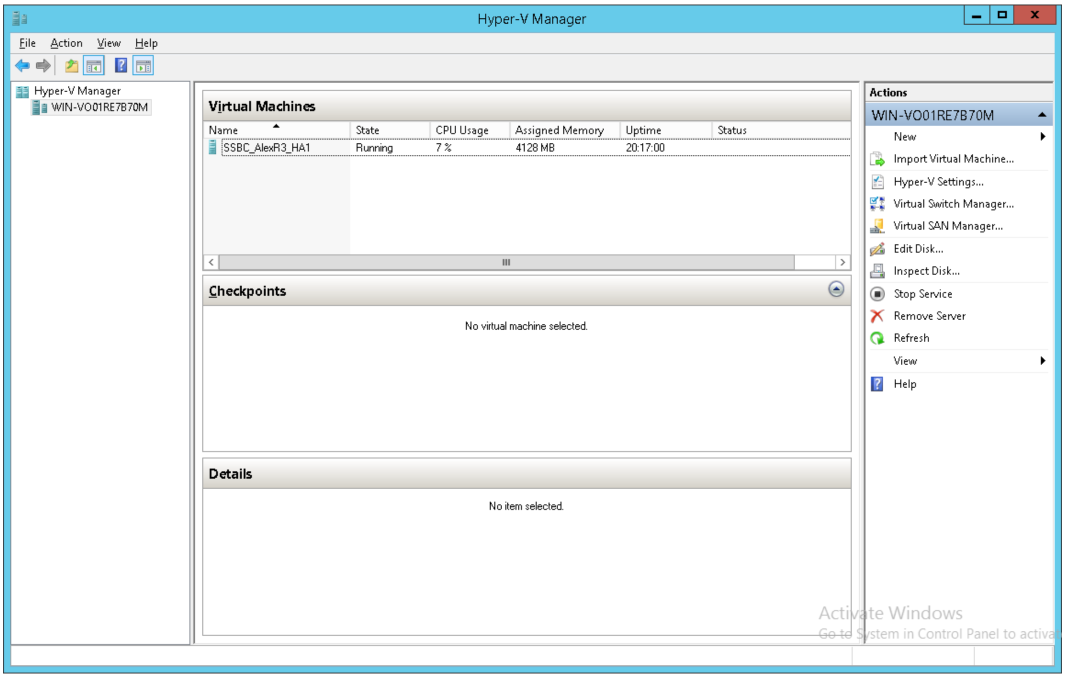
7.2.1 Installing the Microsoft Hyper-V Virtual Machine

The EMS server is distributed as a VM image (see Section 4.2 on page 30).

➢ **To install the EMS server on Microsoft Hyper-V:**

1. Extract the zip file containing the EMS server installation received from AudioCodes to a local directory on the Hyper-V server (see Appendix F on page 259 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 7-210: Installing the EMS server on Hyper-V – Hyper-V Manager



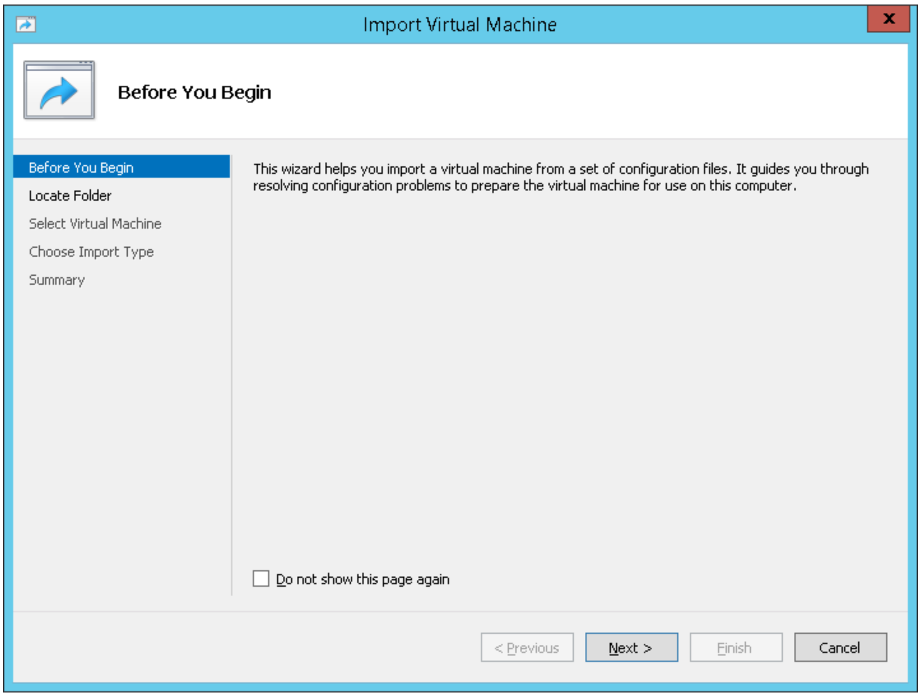
Name	State	CPU Usage	Assigned Memory	Uptime	Status
SSBC_AlexR3_HA1	Running	7 %	4128 MB	20:17:00	

No virtual machine selected.

No item selected.

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

Figure 7-221: Installing EMS server on Hyper-V – Import Virtual Machine Wizard

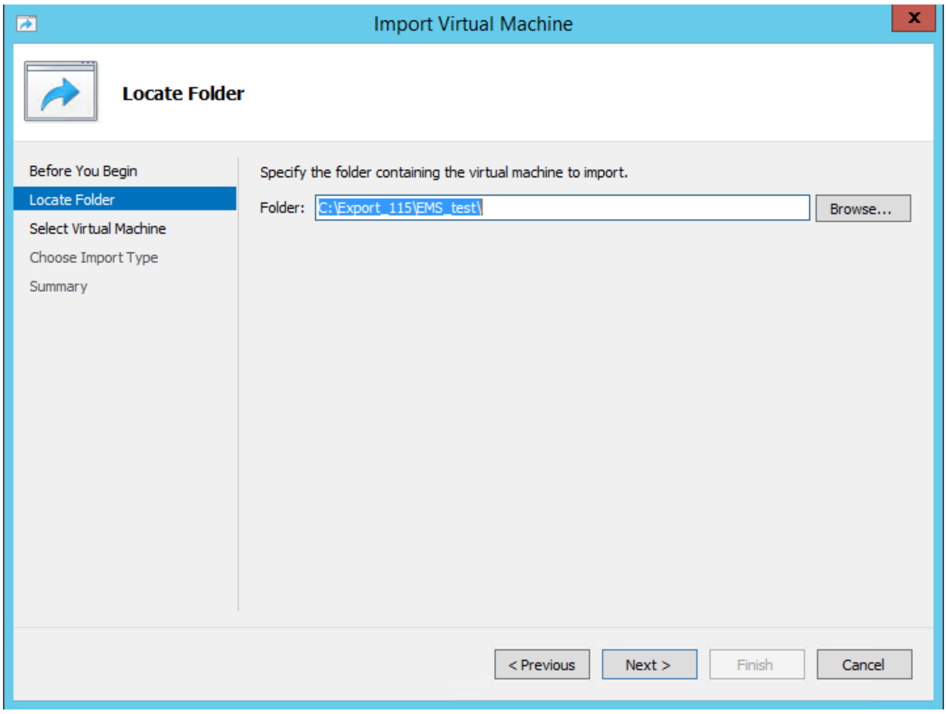


This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

□ Do not show this page again

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

Figure 7-232: Installing EMS server on Hyper-V – Locate Folder



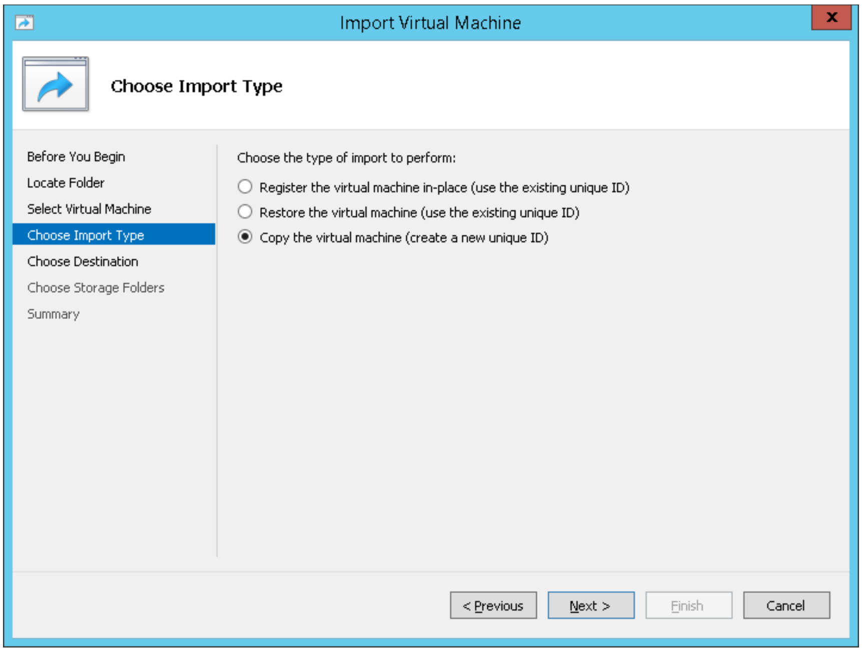
Specify the folder containing the virtual machine to import.

Folder: C:\Export_115\EMS_test\

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 7-243: Installing EMS server on Hyper-V – Choose Import Type



Choose Import Type

Choose the type of import to perform:

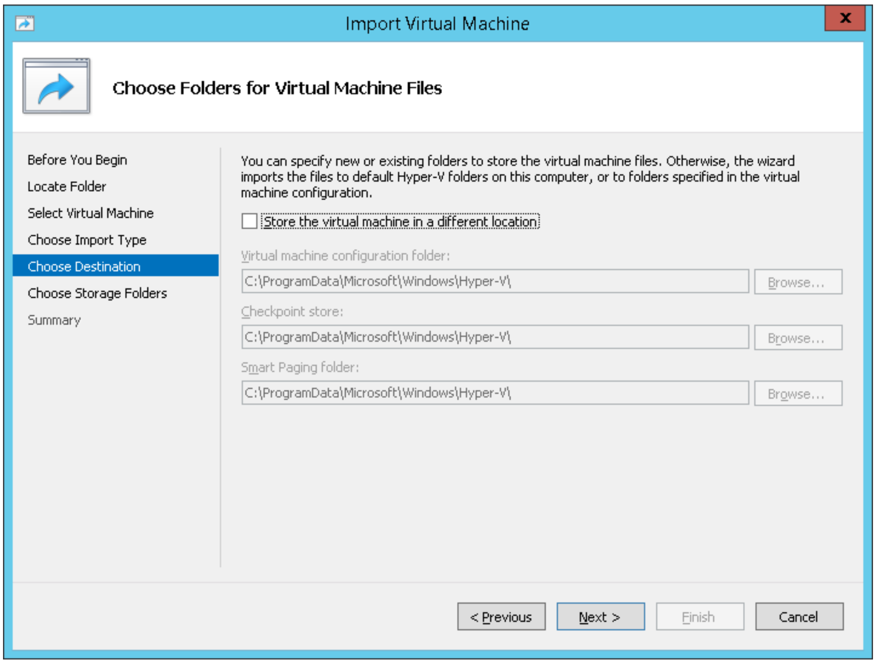
○ Register the virtual machine in-place (use the existing unique ID)

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

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

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

Figure 7-254: Installing EMS server on Hyper-V – Choose Destination



Choose Folders for Virtual Machine Files

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

□ Store the virtual machine in a different location

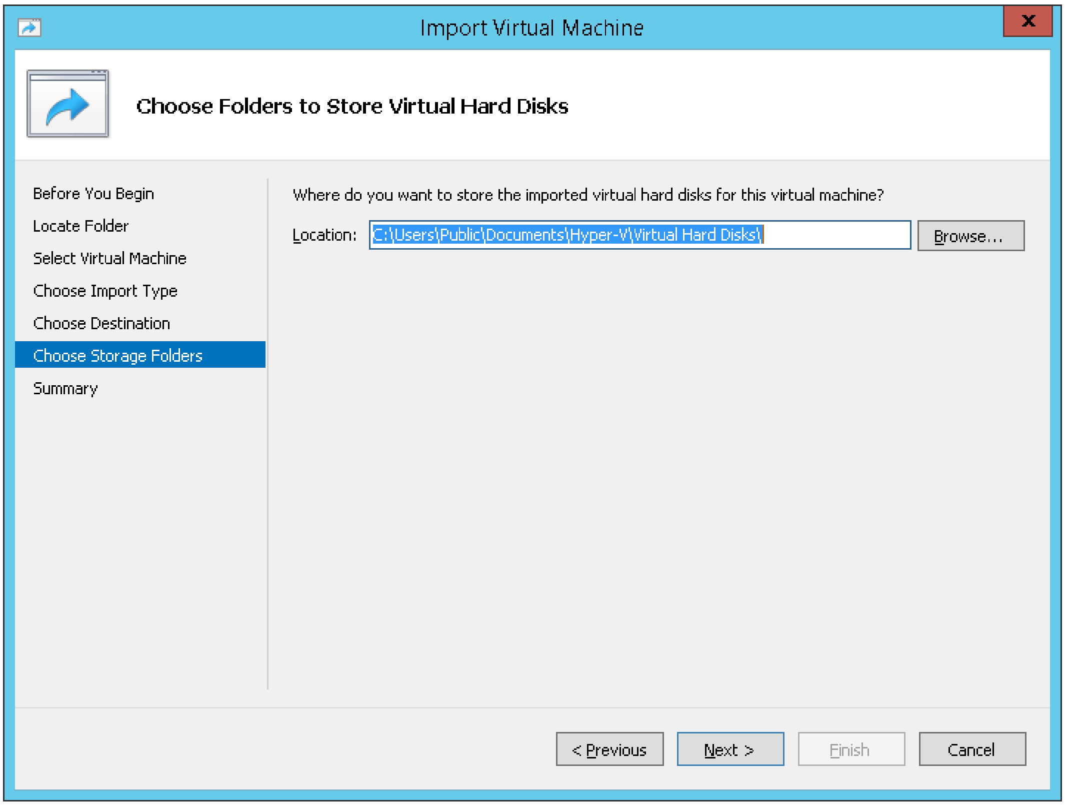
Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

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

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

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

Figure 7-265: Installing EMS server on Hyper-V – Choose Storage Folders



Import Virtual Machine

Choose Folders to Store Virtual Hard Disks

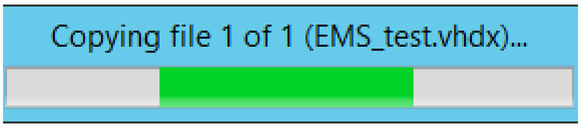
Where do you want to store the imported virtual hard disks for this virtual machine?

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

9. Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.

10. Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

Figure 7-276: File Copy Progress Bar



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

This step may take approximately 30 minutes to complete.

11. Proceed to Section 7.2.2 on page 65.

7.2.2 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, see Chapter 3 on page 23.

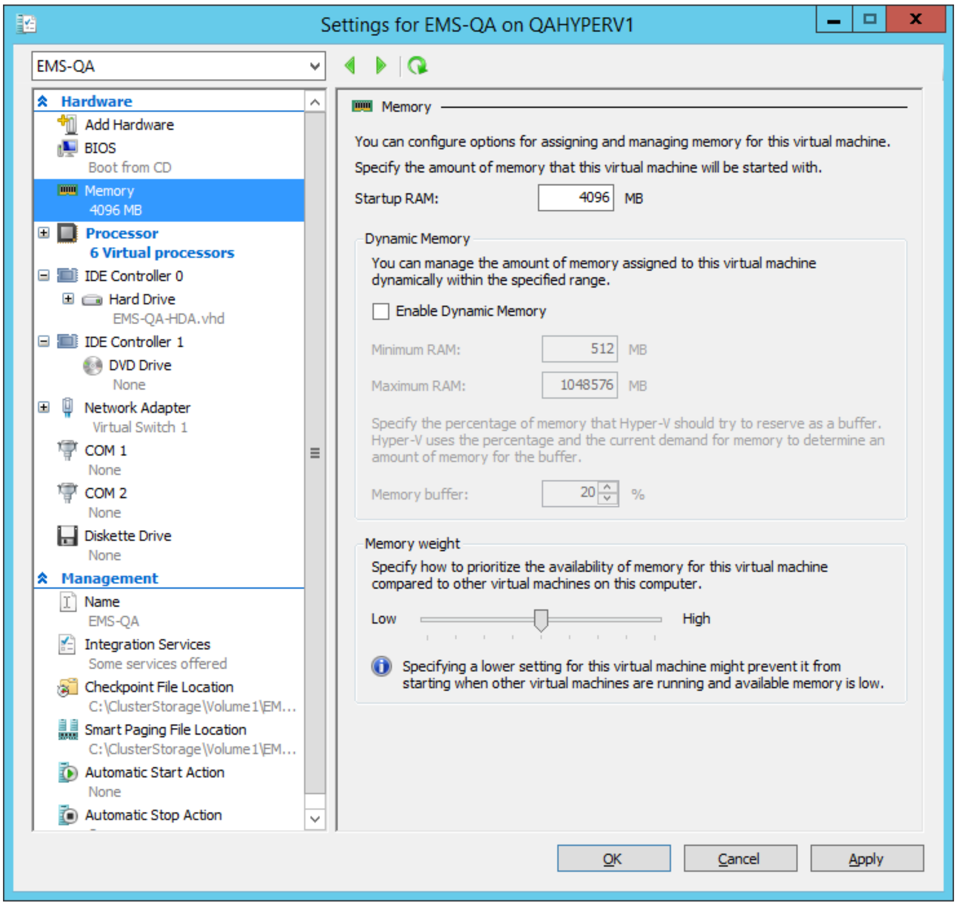
Table 7-2: Virtual Machine Configuration

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

➢ **To configure the VM for EMS server:**

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

Figure 7-287: Adjusting VM for EMS server – Settings - Memory



Settings for EMS-QA on QAHYPERV1

EMS-QA

Hardware
- Add Hardware
- BIOS
Boot from CD
- Memory
4096 MB
- Processor
6 Virtual processors
- IDE Controller 0
  - Hard Drive
EMS-QA-HDA.vhd
- IDE Controller 1
  - DVD Drive
None
- Network Adapter
Virtual Switch 1
- COM 1
None
- COM 2
None
- Diskette Drive
None

Management
- Name
EMS-QA
- Integration Services
Some services offered
- Checkpoint File Location
C:\ClusterStorage\Volume1\EM...
- Smart Paging File Location
C:\ClusterStorage\Volume1\EM...
- Automatic Start Action
None
- Automatic Stop Action

Memory

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

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

Startup RAM: 4096 MB

Dynamic Memory

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

☐ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

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

Memory buffer: 20 %

Memory weight

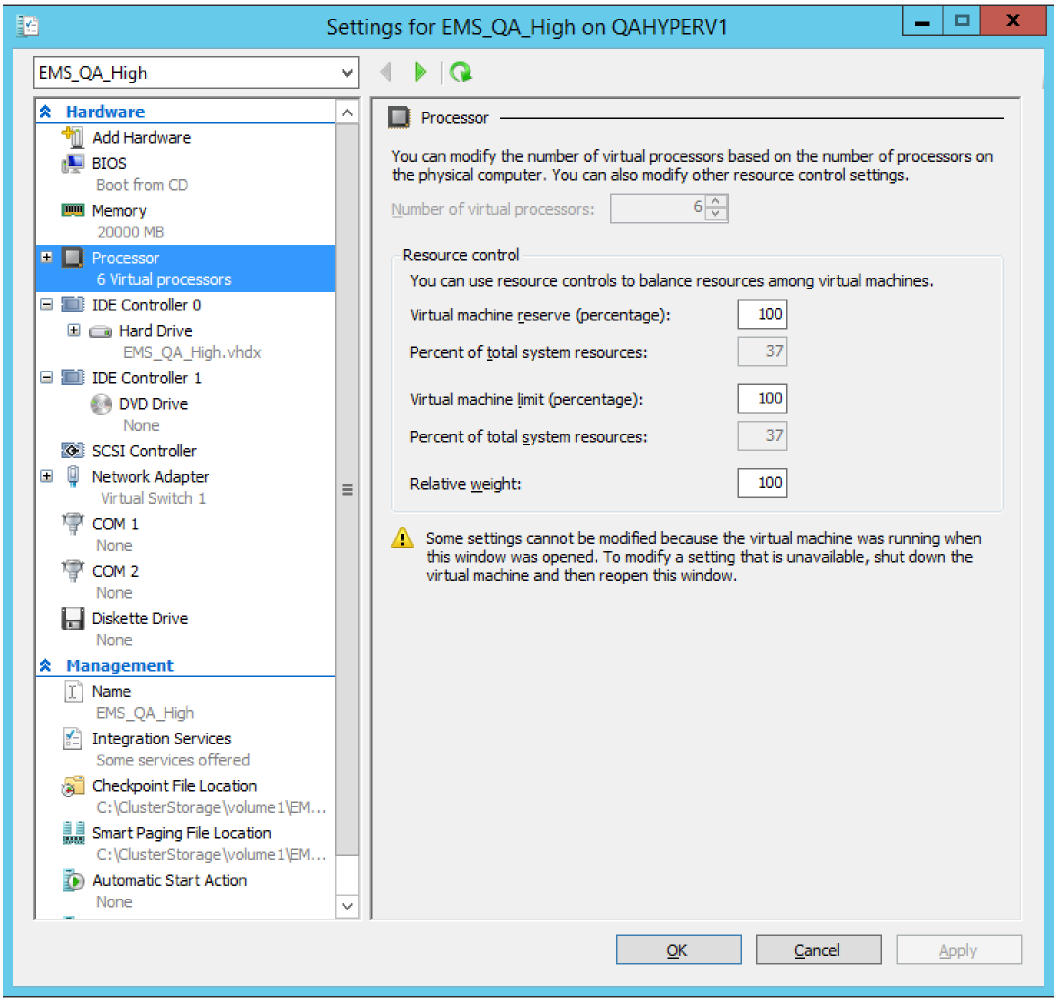
Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

Low — High

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

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

Figure 7-298: Adjusting VM for EMS server - Settings - Processor



Settings for EMS_QA_High on QAHYPERV1

EMS_QA_High

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  20000 MB
- Processor
  6 Virtual processors
- IDE Controller 0
  - Hard Drive
    EMS_QA_High.vhdx
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  Virtual Switch 1
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  EMS_QA_High
- Integration Services
  Some services offered
- Checkpoint File Location
  C:\ClusterStorage\volume1\EM...
- Smart Paging File Location
  C:\ClusterStorage\volume1\EM...
- Automatic Start Action
  None

Processor

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

Number of virtual processors: 6

Resource control

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

Virtual machine reserve (percentage): 100

Percent of total system resources: 37

Virtual machine limit (percentage): 100

Percent of total system resources: 37

Relative weight: 100

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

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

Note:

- Once the hard disk space allocation is increased, it cannot be reduced.
- If you wish to create EMS 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 7.2.5).

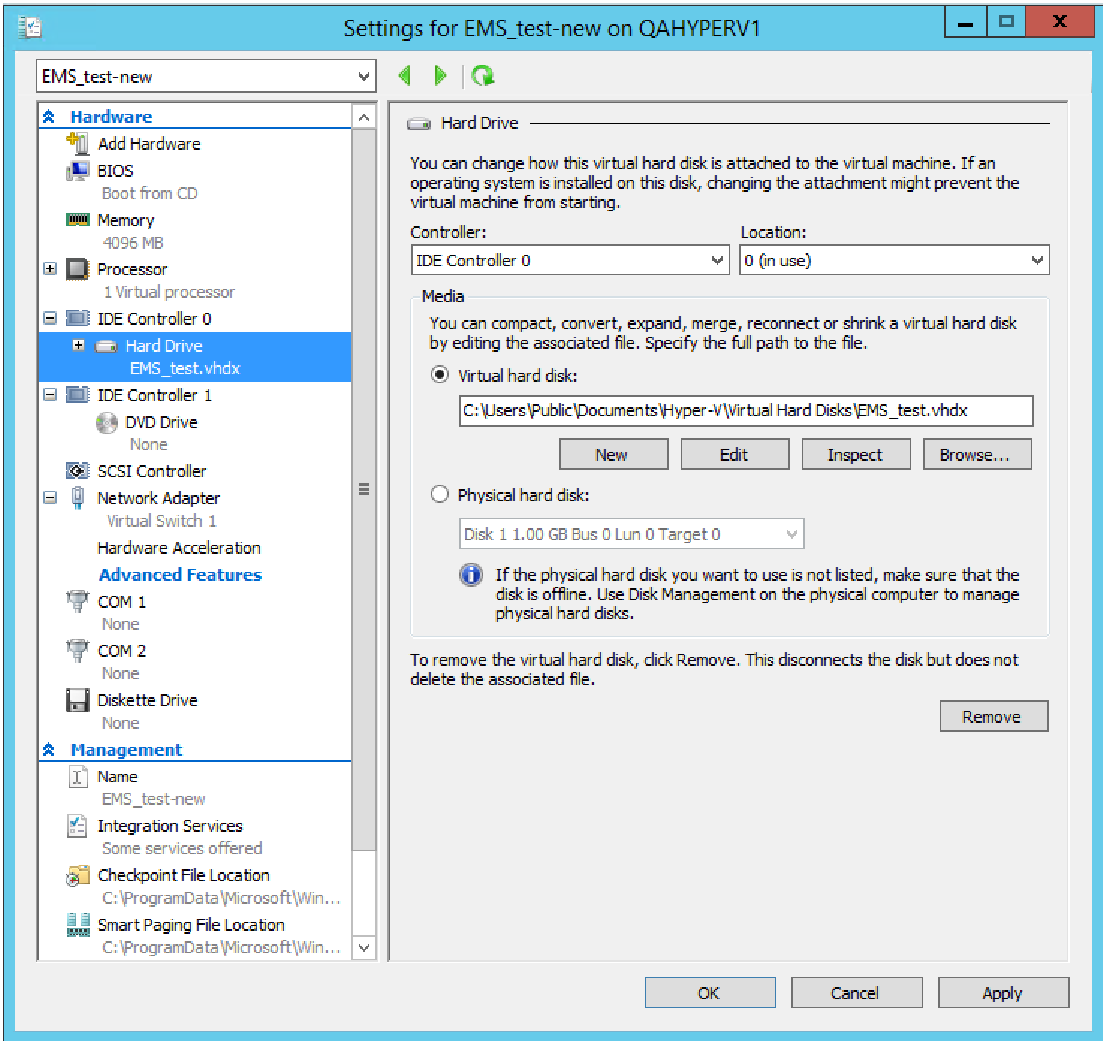
7.2.2.1 Expanding Disk Capacity

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

➢ **To expand the disk size:**

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

Figure 7-300: Expanding Disk Capacity



Settings for EMS_test-new on QAHYPERV1

EMS_test-new

Hard Drive

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

Controller: IDE Controller 0

Location: 0 (in use)

Media

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

● Virtual hard disk:

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

○ Physical hard disk:

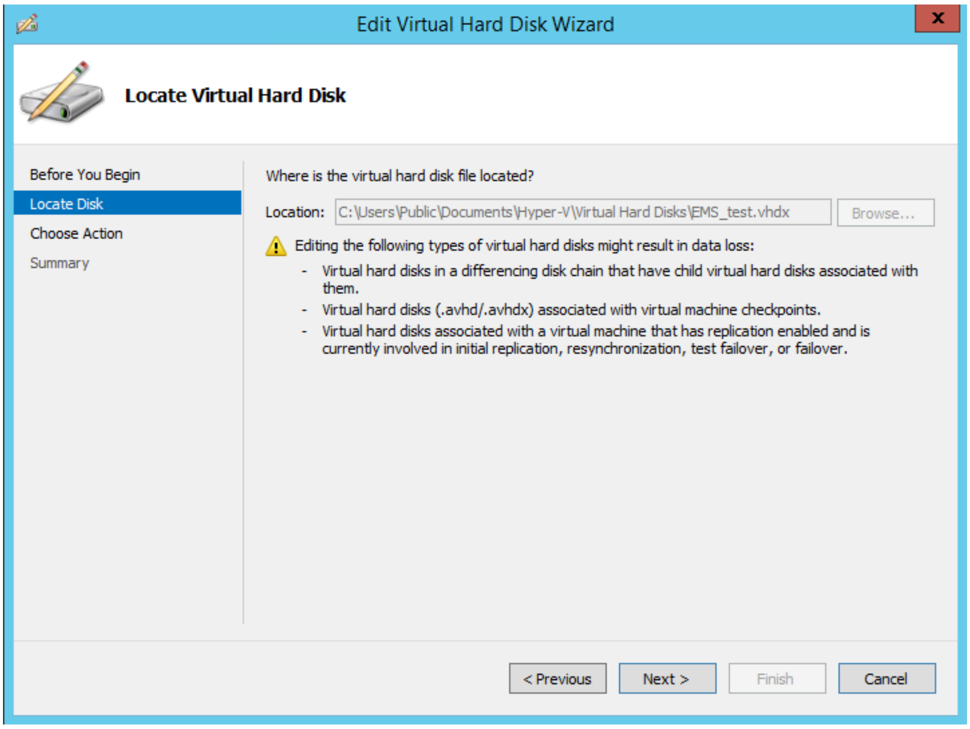
Disk 1 1.00 GB Bus 0 Lun 0 Target 0

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

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

The Edit Virtual Disk Wizard is displayed as shown below.

Figure 7-311: Edit Virtual Hard Disk Wizard



Edit Virtual Hard Disk Wizard

Locate Virtual Hard Disk

Where is the virtual hard disk file located?

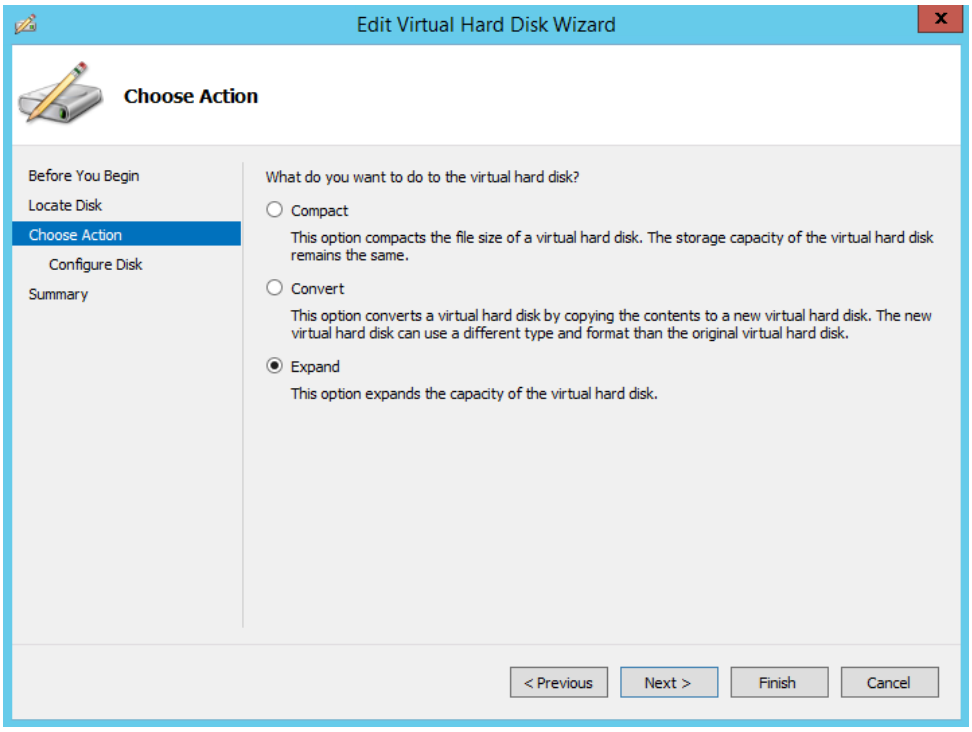
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\EMS_test.vhdx

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

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

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

Figure 7-32: Edit Virtual Hard Disk Wizard-Choose Action



Edit Virtual Hard Disk Wizard

Choose Action

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

○ Compact

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

○ Convert

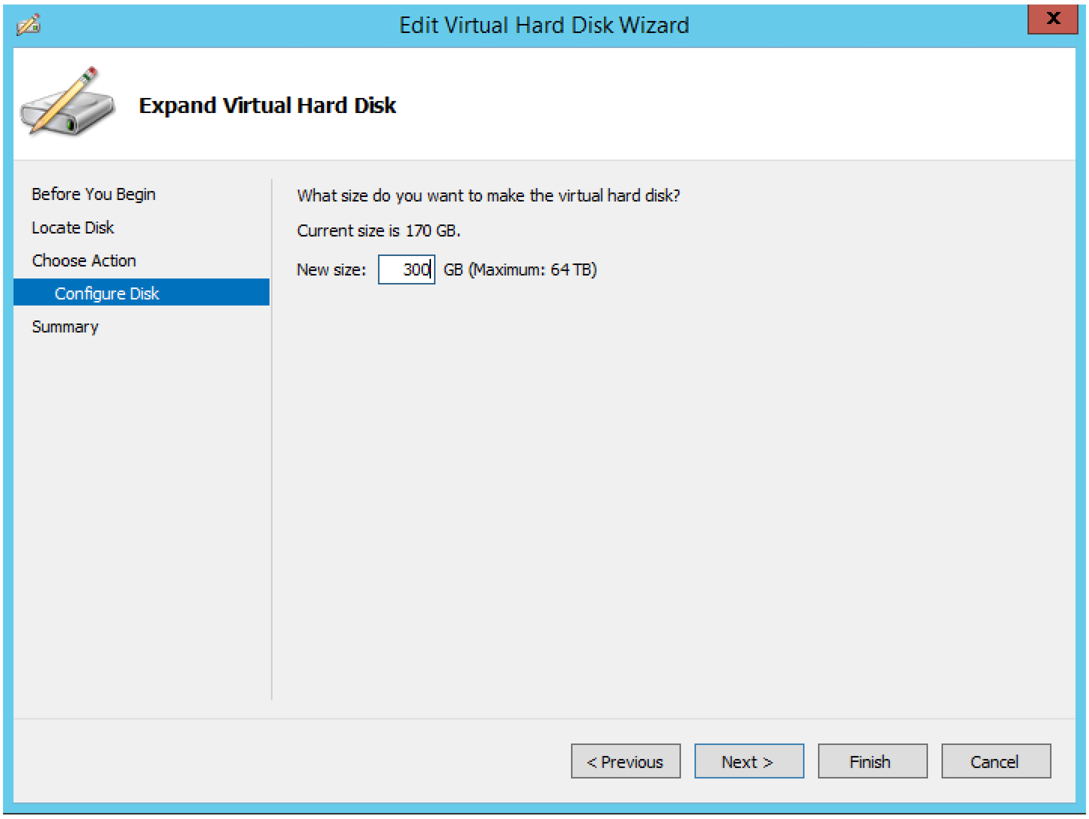
This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

● Expand

This option expands the capacity of the virtual hard disk.

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

Figure 7-33: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk



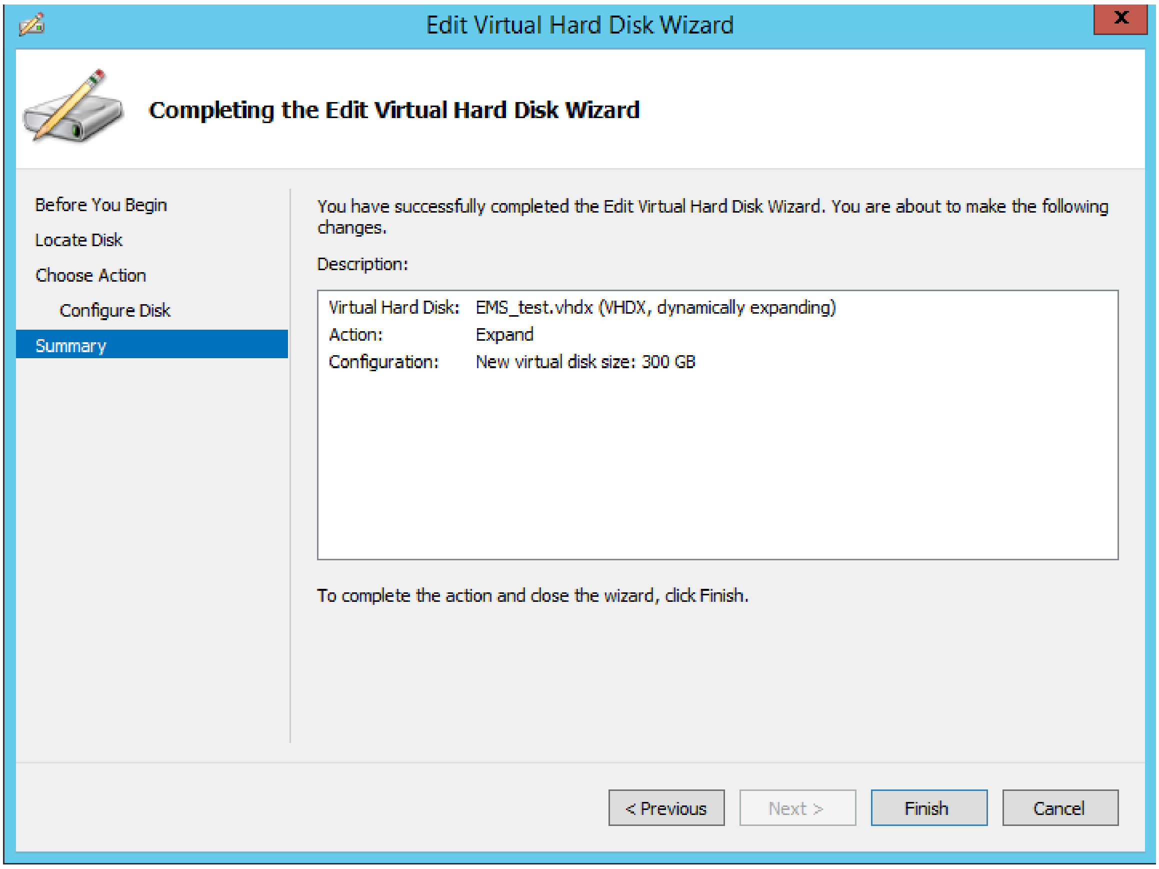
What size do you want to make the virtual hard disk?

Current size is 170 GB.

New size: 300 GB (Maximum: 64 TB)

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

Figure 7-34: Edit Virtual Hard Disk Wizard-Completion



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

Description:

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

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

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

7.2.3 Changing MAC Addresses from 'Dynamic' to 'Static'

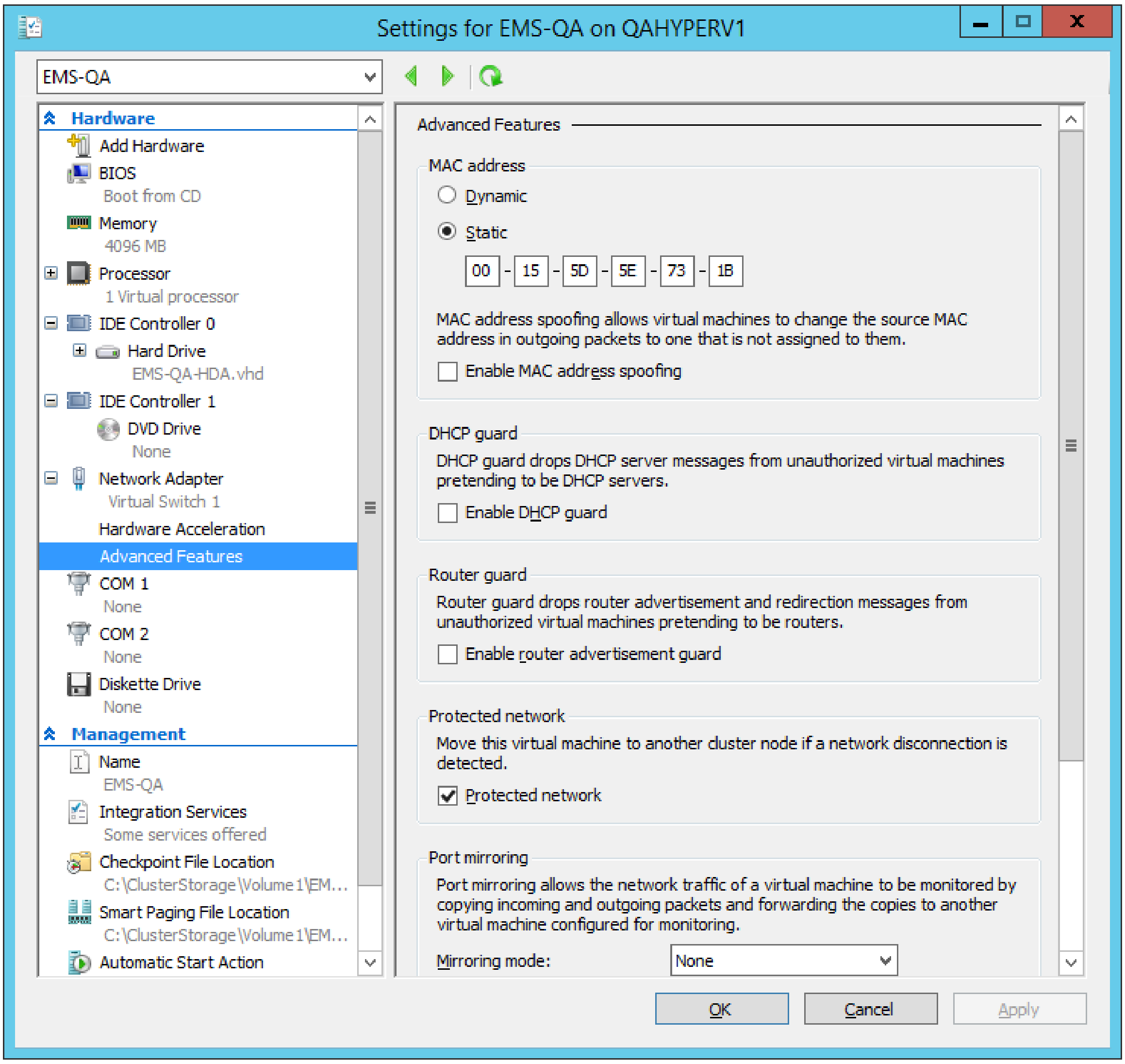
By default, the MAC addresses of the EMS server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license for features such as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

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 EMS server (see Section 16.6 on page 121).
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 7-35: Advanced Features - Network Adapter – Static MAC Address



Advanced Features

MAC address

○ Dynamic

● Static

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

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

□ Enable MAC address spoofing

DHCP guard

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

□ Enable DHCP guard

Router guard

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

□ Enable router advertisement guard

Protected network

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

☑ Protected network

Port mirroring

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

Mirroring mode: None

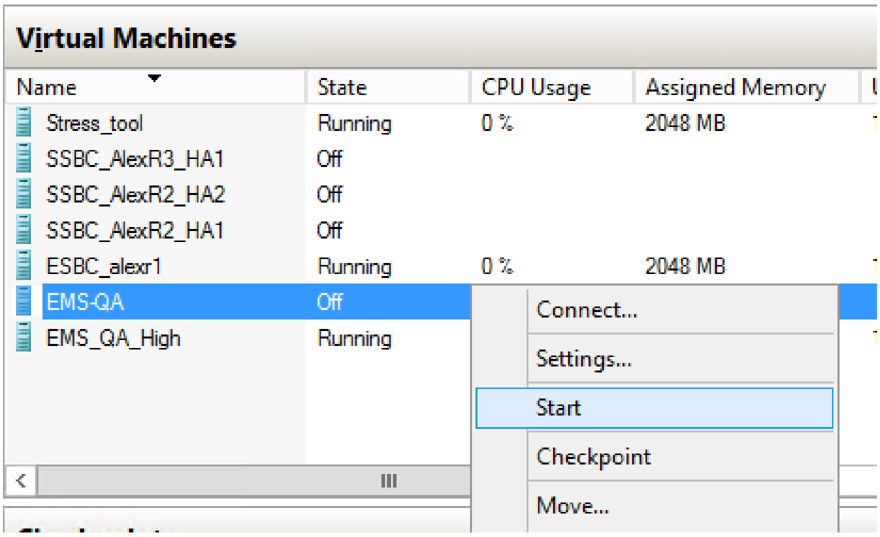
7.2.4 Connecting EMS Server to Network

After installation, the EMS 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 EMS server installation. You need to change this IP address to suit your IP addressing scheme.

➢ **To reconfigure the EMS server IP address:**

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

Figure 7-36: Power On Virtual Machine

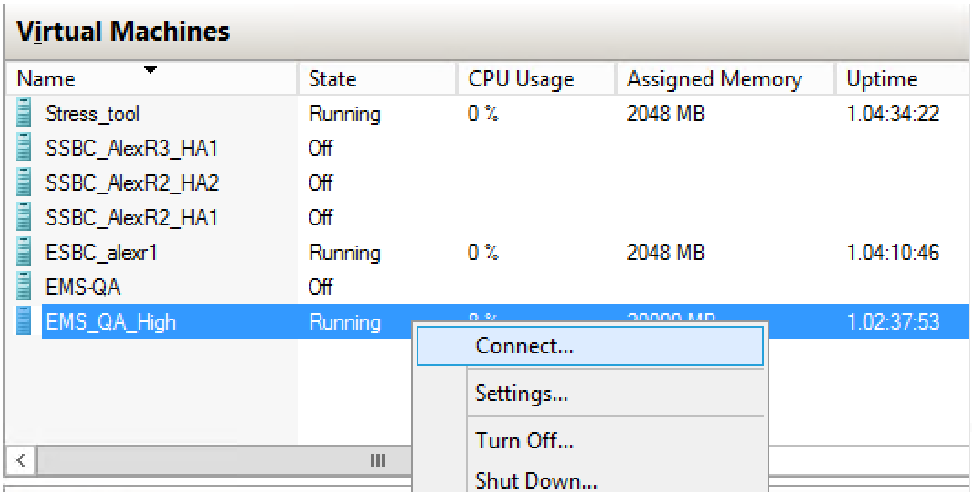


Virtual Machines

Name	State	CPU Usage	Assigned Memory
Stress_tool	Running	0 %	2048 MB
SSBC_AlexR3_HA1	Off		
SSBC_AlexR2_HA2	Off		
SSBC_AlexR2_HA1	Off		
ESBC_alexr1	Running	0 %	2048 MB
EMS-QA	Off		
EMS_QA_High	Running		

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

Figure 7-37: Connect to EMS Server Console



Virtual Machines

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

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

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

```
su – root
```

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

```
# EmsServerManager
```

6. Set the EMS server network IP address to suit your IP addressing scheme (see Section 17.1).

7. Perform other configuration actions as required using the EMS Server Manager (see Chapter 12 on page 103).

7.2.5 Configuring EMS Virtual Machines in a Microsoft Hyper-V Cluster

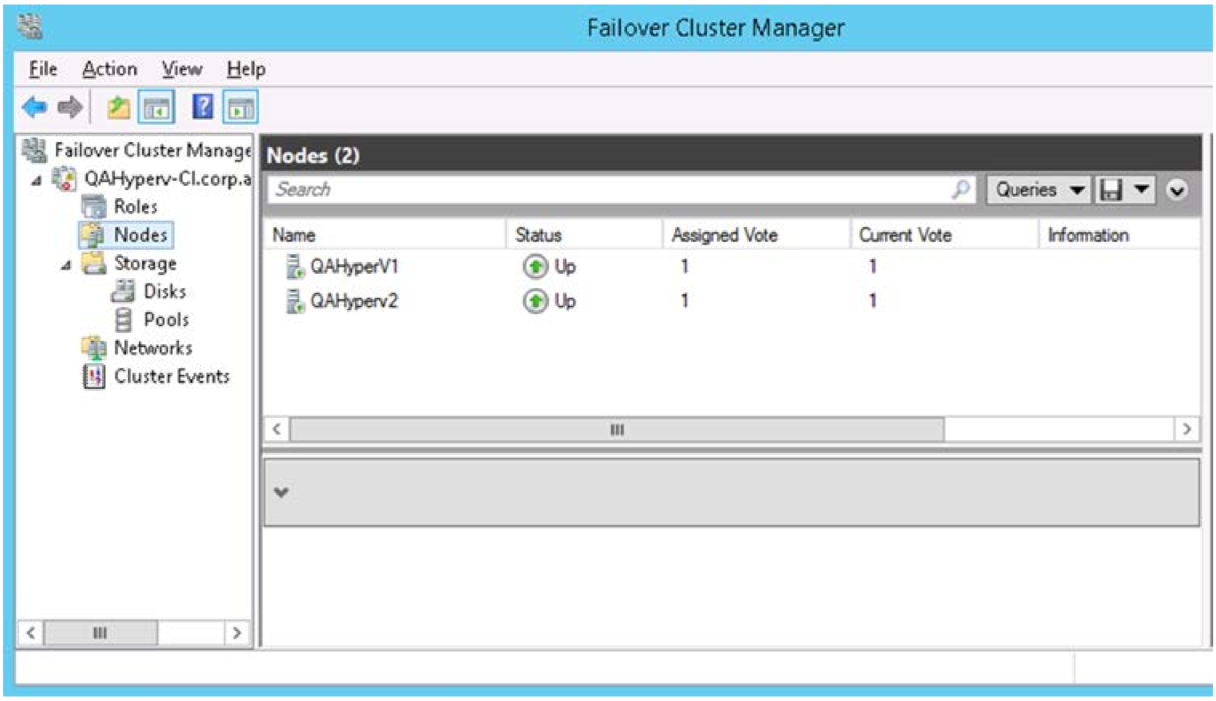
This section describes how to configure EMS VMs in a Microsoft Hyper-V cluster for HA.

7.2.5.1 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 7-38: Hyper-V-Failover Cluster Manager Nodes



Nodes (2)

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

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

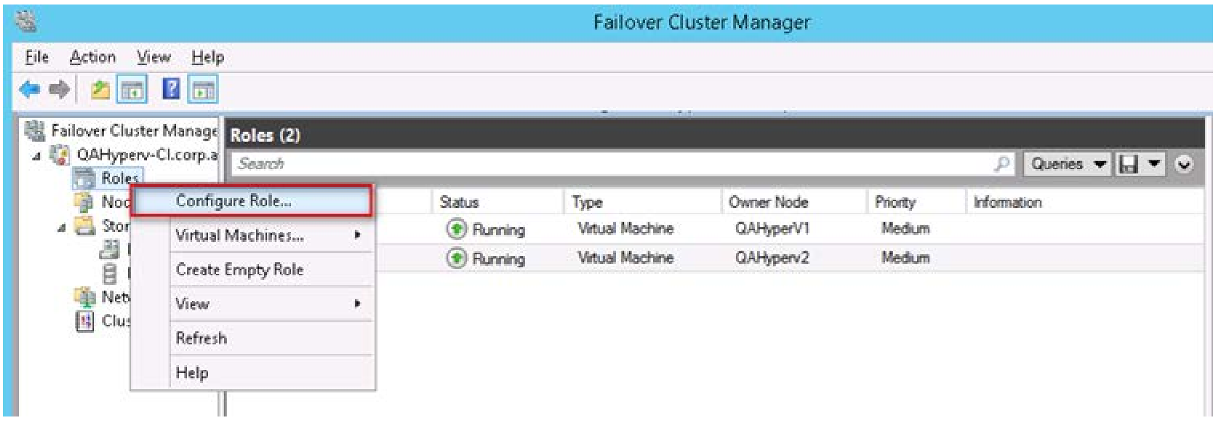
7.2.5.2 Add the EMS VM in Failover Cluster Manager

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

➢ **To add the EMS VM in Failover Cluster Manager:**

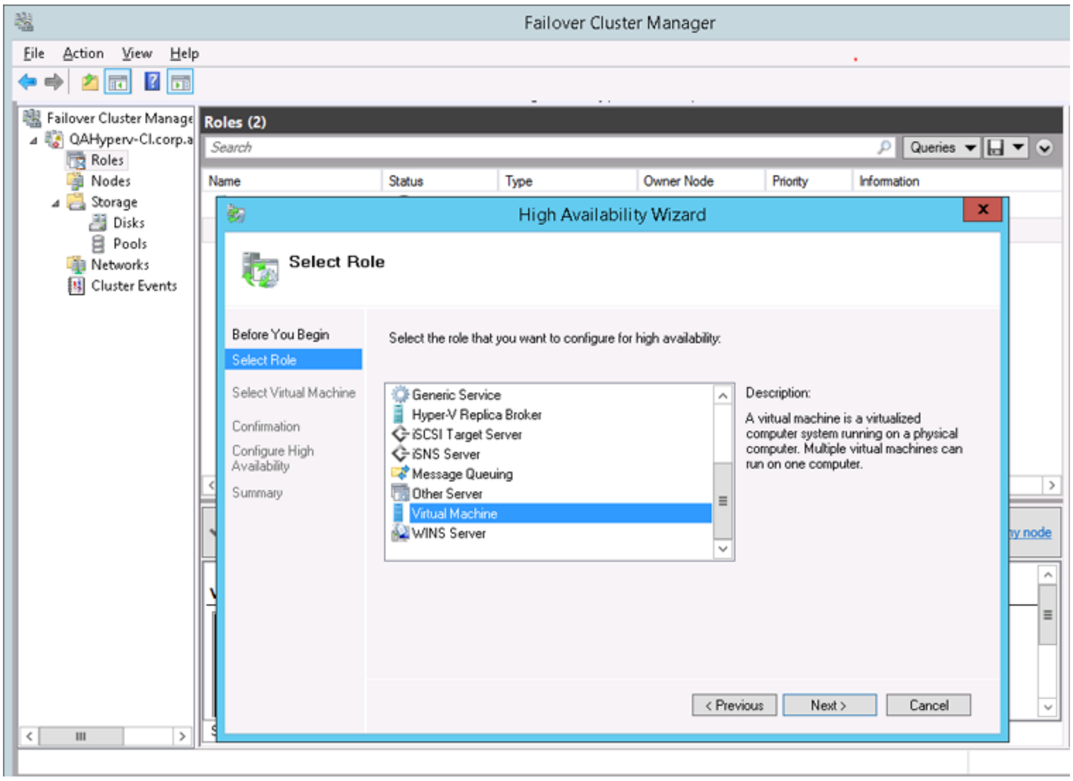
1. Right-click “Roles” and in the pop up menu, choose **Configure Role**:

Figure 7-39: Configure Role



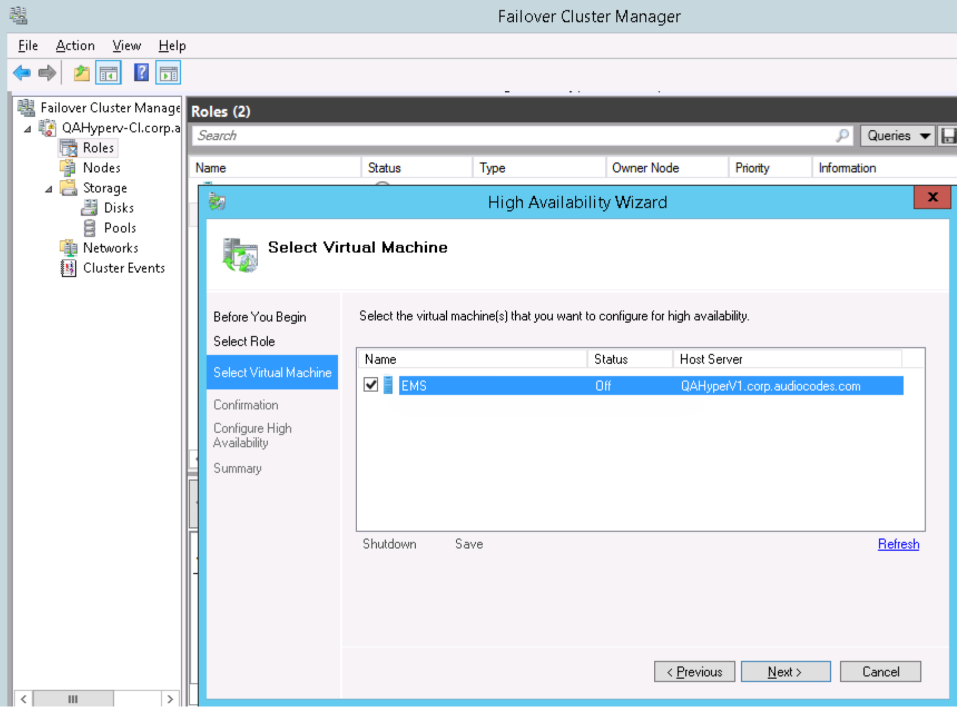
2. In the Select Role window, select the **Virtual Machine** option and then click **Next**.

Figure 7-40: Choose Virtual Machine



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

Figure 7-41: Confirm Virtual Machine



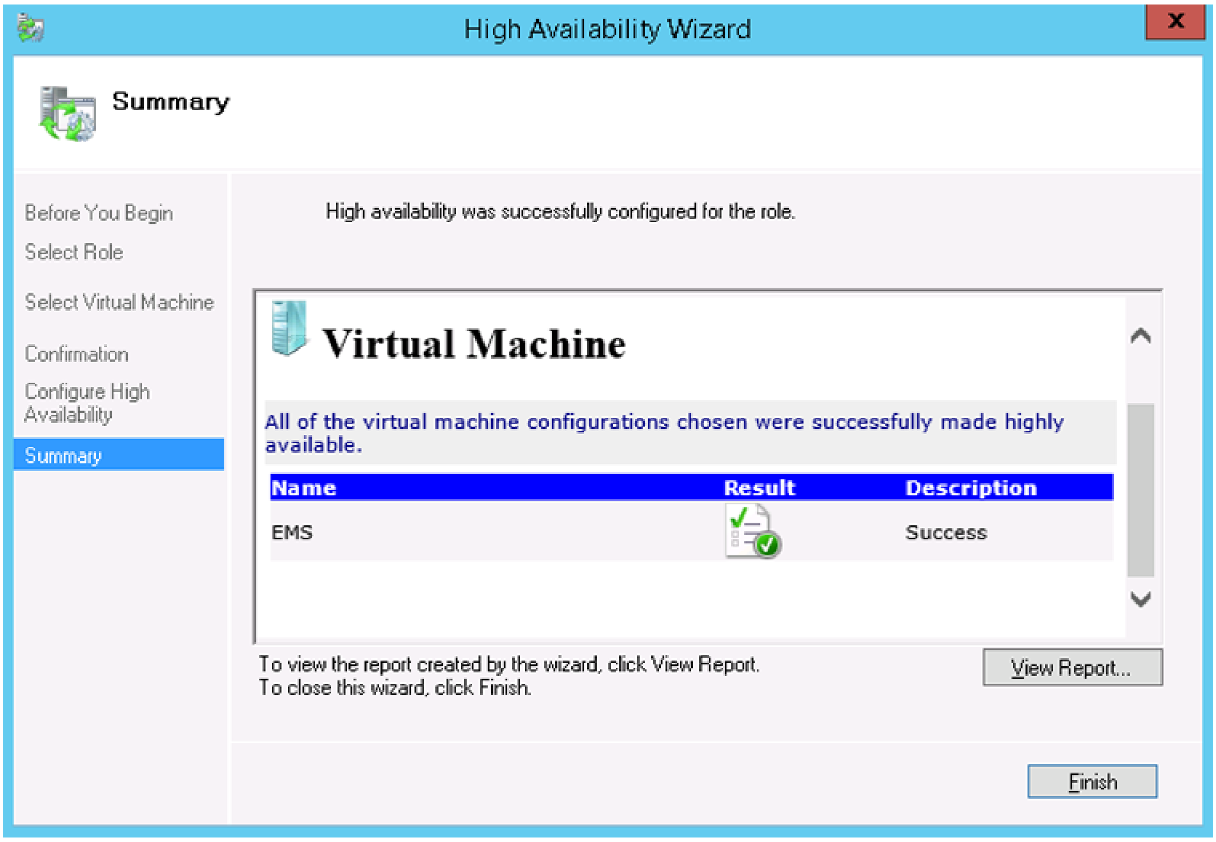
Select the virtual machine(s) that you want to configure for high availability.

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

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

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

Figure 7-42: Virtual Machine Successfully Added



High availability was successfully configured for the role.

Virtual Machine

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

Name	Result	Description
EMS	✓	Success

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

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

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

Note: If you wish to manually move the EMS VMs to another cluster node, see Appendix D on page 235.

7.2.5.3 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 EMS VM is automatically moved to the redundant server host node. During this process, the EMS VM is restarted and consequently any running EMS or SEM processes are dropped. The move process may take several minutes.

This page is intentionally left blank.

Part III

EMS Server Upgrade

This part describes the upgrade of the EMS server on dedicated hardware and on the VMware platform.

8 Upgrading the EMS Server on Dedicated Hardware

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

Important: Prior to performing the upgrade, it is highly recommended to perform a complete backup of the EMS server. For more information, see Appendix A on page 215.

You can perform the EMS version upgrade using AudioCodes supplied **DVD3**.

- For EMS versions 2.2 until version 6.6:

  A major version upgrade of the EMS from the above versions is not supported. Instead, users must perform a full installation of version 7.0 as described in Section 6 on page 35.

8.1 Upgrading the EMS Server-DVD

This section describes how to upgrade the EMS server from the AudioCodes supplied installation DVD on the Linux platform.

To upgrade the EMS server on the Linux platform to version 7.2, only DVD3 is required. Verify in the EMS Manager ‘General Info’ screen that you have installed the latest Linux revision (see Chapter 3 on page 23). If you have an older OS revision, a clean installation must be performed using all three DVDs (see Section 6.2 on page 37).

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 upgrade the EMS server on the Linux platform:

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

   ```
   su – root
   ```

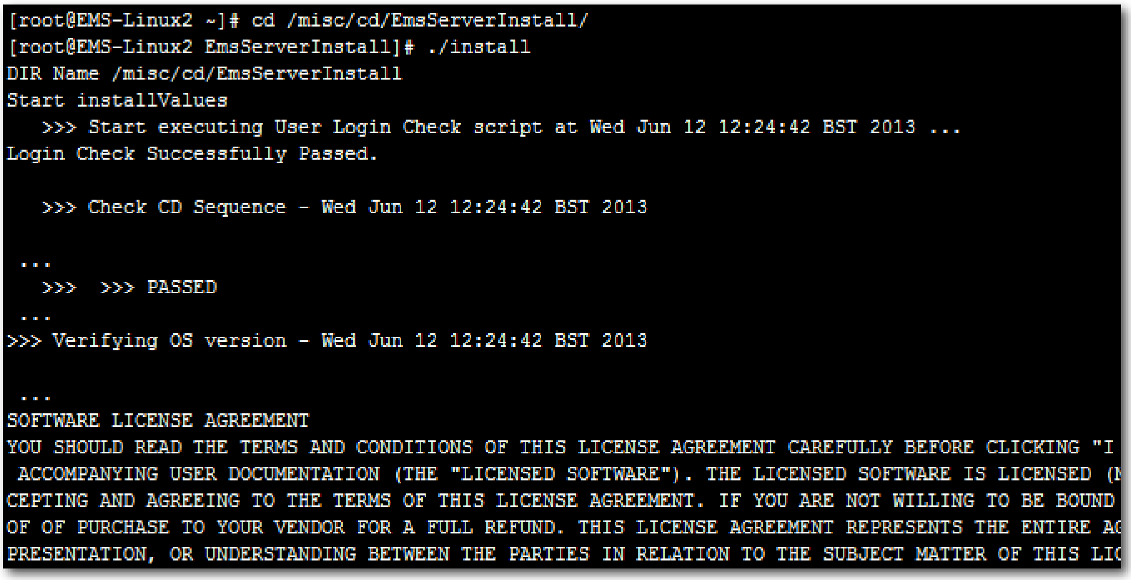
4. On some machines you need to mount the CDROM in order to make it available:

   ```
   mount /misc/cd
   ```

5. Run the installation script from its location:

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

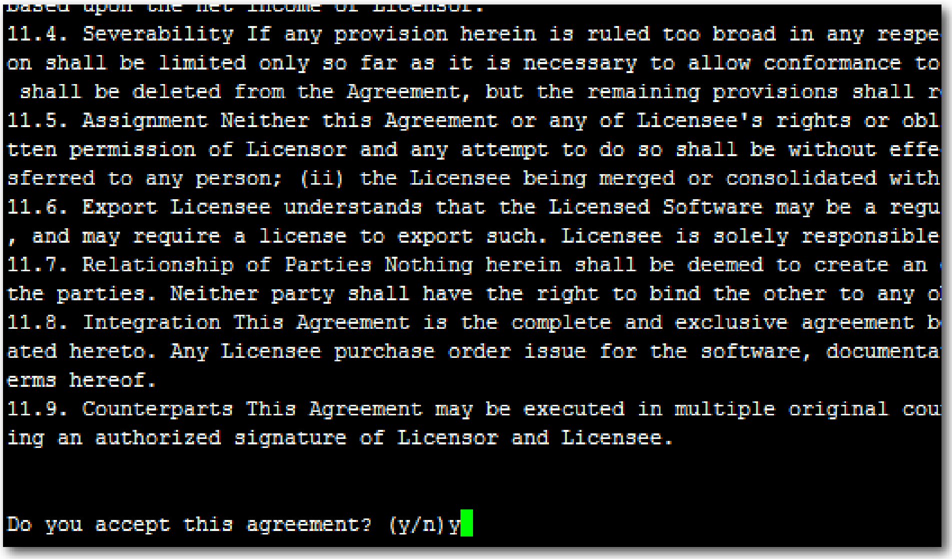
Figure 8-1: EMS Server Upgrade (Linux)



```
[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 (
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 AC
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

Figure 8-2: EMS Server Upgrade (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
```

7. OS patches are installed.

After the OS patches installation, you are prompted to press Enter to reboot.

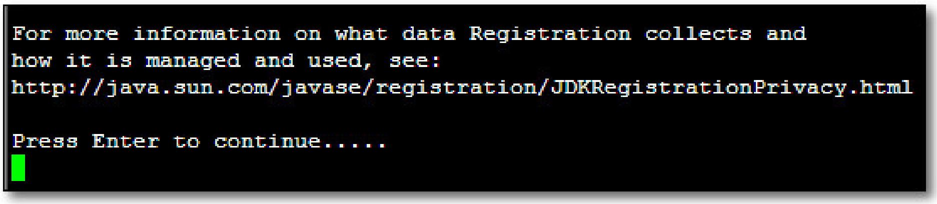
Note: This step is optional and depends upon which version you are upgrading. After the EMS server has rebooted, repeat steps 2 to 6.

8. If the EMS version you are upgrading to is packaged with a later version of Java than the one that is currently installed, type **yes**, and then press Enter to upgrade the Java version, otherwise, skip this step:

```
Java DB version 10.4.2.1.1 is currently installed.
Upgrade to version 10.6.2.1.1 ? [yes,no]yes
```

9. At the end of Java installation, press Enter to continue.

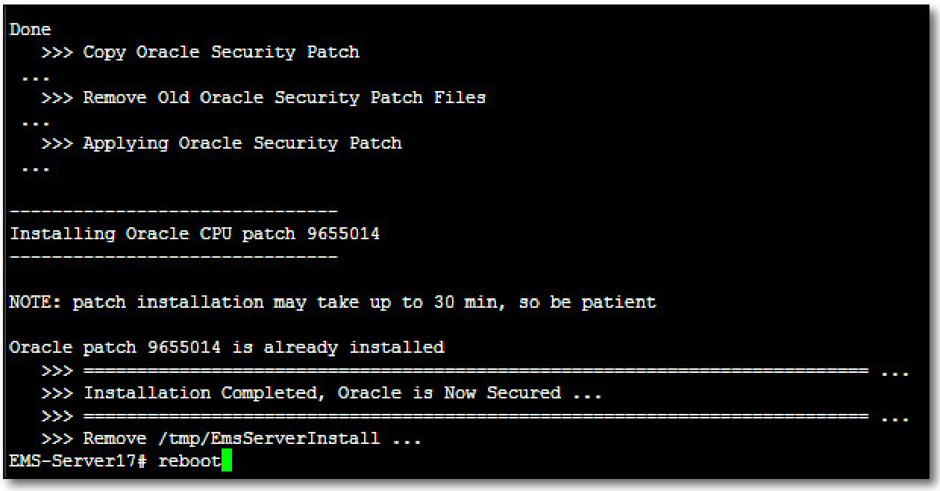
Figure 8-3: EMS Server Application Upgrade (Linux) - Java Installation



```
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.....
```

10. Wait for the installation to complete and reboot the EMS server.

Figure 8-4: EMS Server Upgrade (Linux) Complete



```
Done
   >>> Copy Oracle Security Patch
 ...
   >>> Remove Old Oracle Security Patch Files
 ...
   >>> Applying Oracle Security Patch
 ...

-------------------------------
Installing Oracle CPU patch 9655014
-------------------------------

NOTE: patch installation may take up to 30 min, so be patient

Oracle patch 9655014 is already installed
   >>> ========================================================================== ...
   >>> Installation Completed, Oracle is Now Secured ...
   >>> ========================================================================== ...
   >>> Remove /tmp/EmsServerInstall ...
EMS-Server17# reboot
```

Note: For SEM Users: each time the EMS server version is upgraded, the operator should perform CTRL – F5 (refresh) action on the SEM Page, and then relogin to the application.

8.2 Upgrading the EMS Server-ISO File

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

Before performing this procedure, you need to verify the ISO file contents (see Section 6.1.2).

➢ To upgrade using an ISO file:

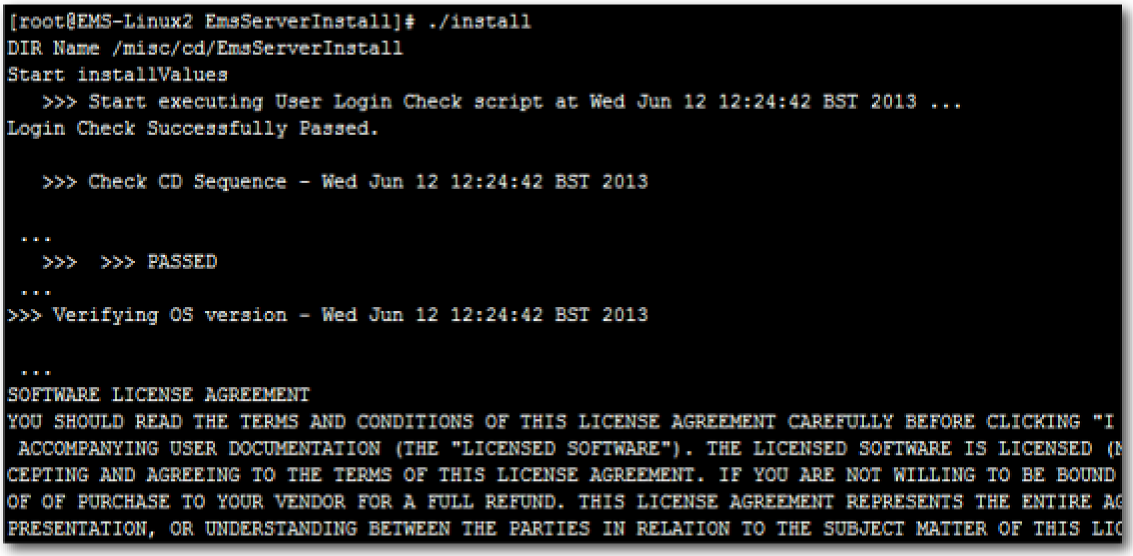
1. Use SFTP or SCP to copy the iso file to /home/acems in the server
2. Replace "7.2.xxx" in the filename with the relevant version in two of the following commands.

```
mkdir /ins
cp ~acems/DVD3_EMS_7.2.xxx.iso /ins
mkdir /tmp/cd
umount -l /tmp/cd
mount -t iso9660 -o loop,ro /ins/DVD3_EMS_7.2.xxx.iso
/tmp/cd
cd /tmp/cd/EmsServerInstall
```

3. Run the installation script from its location:

```
./install
```

Figure 8-5: EMS Server Upgrade (Linux)



```
[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
```

4. Proceed to step 6 in Section 8.1.

9 Upgrading the EMS Server on the VMware Platform

This section describes how to upgrade the EMS server on the VMware platform. This can be performed by running the Upgrade media (CD/DVD or ISO file) using either the VMware Remote Console Application (VMRC) or the VMware Server Host.

The following steps must be performed:

- Step 1: Setting up the VMware vSphere Web Client (see Section 9.1)
- Step 2: Running the VMware upgrade script (see Section 9.2)

Note:

- A Remote connection to the VMware host is established using the VMware Remote Console application (VMRC). You must download this application or use a pre-installed remote connection client to connect to the remote host.
- The procedures below show screen examples of the vSphere Web Client. However, you should refer to the VMware documentation for more information.

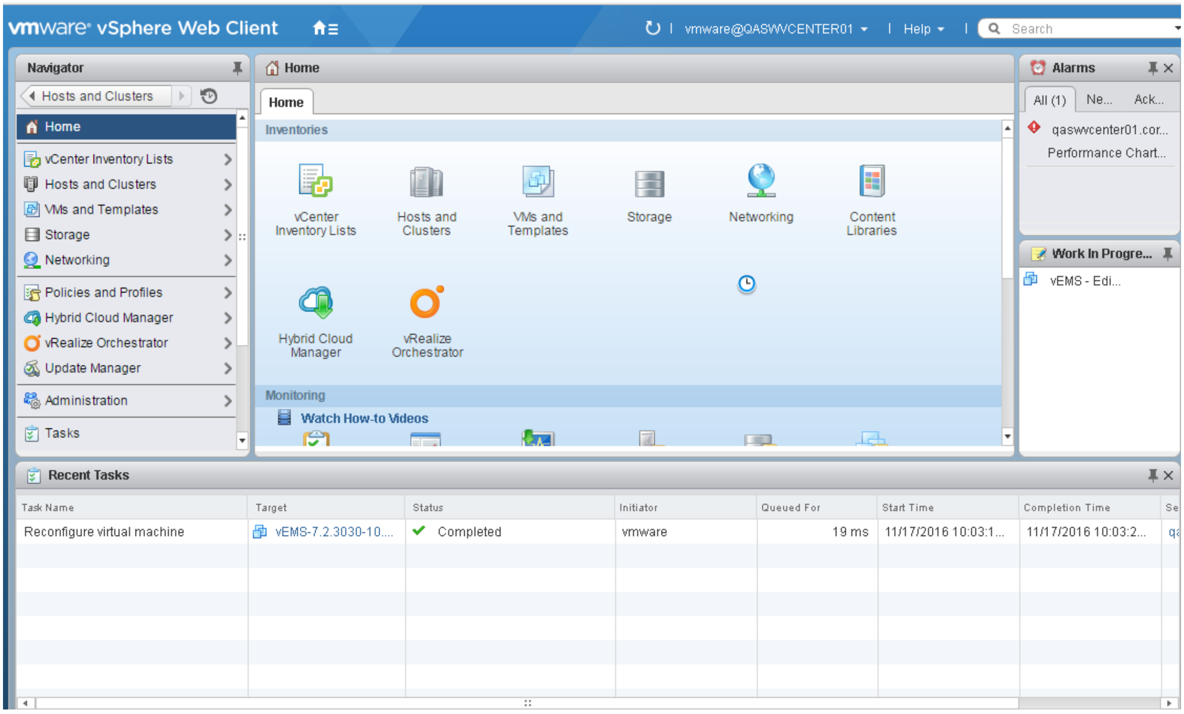
9.1 Step 1: Setting Up the VMware vSphere Web Client

This section describes how to setup the VMware vSphere Web Client.

➢ **To upgrade the EMS server on the VMware platform:**

1. Place the media **DVD3-EMS Server Application Installation** into the DVD/CD disk drive or if you are using an ISO file to the desired directory on either the machine where the VMware vSphere Web client is installed or on the VMware server host.
2. Login to the VMware vSphere Web client.

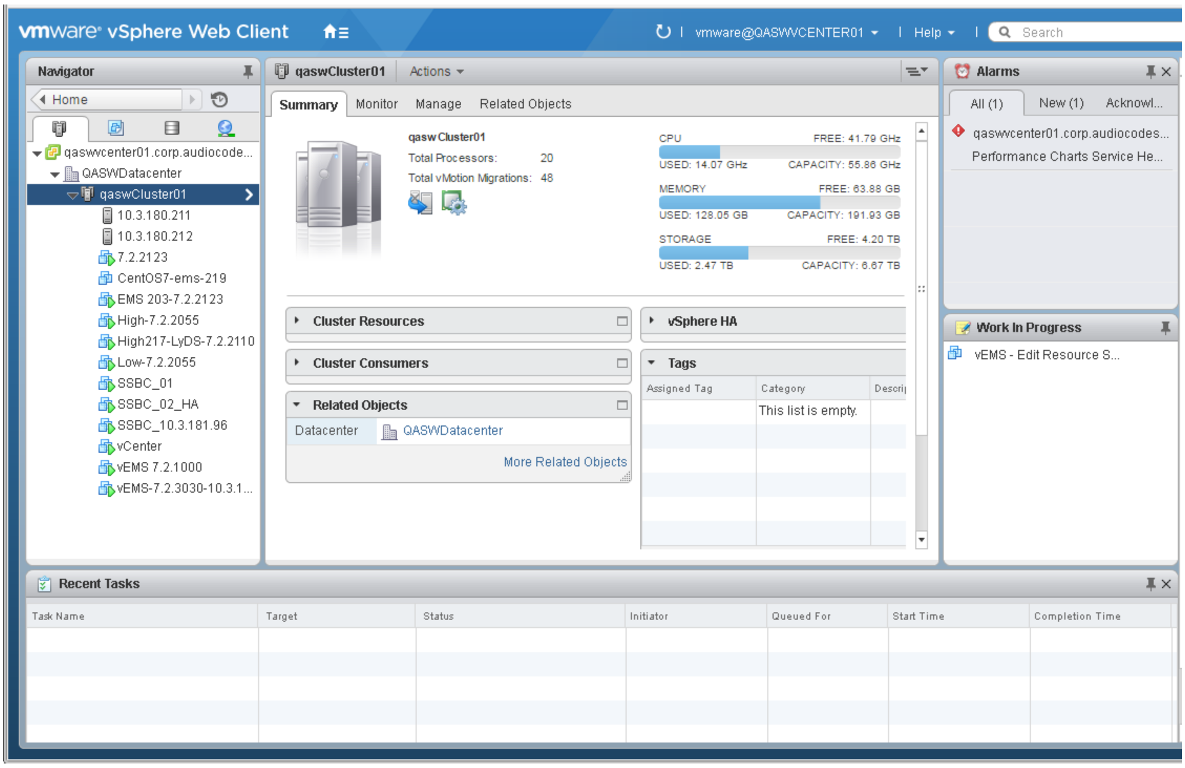
Figure 9-1: VMware vSphere Web Client



Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Se
Reconfigure virtual machine	vEMS-7.2.3030-10....	✓ Completed	vmware	19 ms	11/17/2016 10:03:1...	11/17/2016 10:03:2...	qa

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

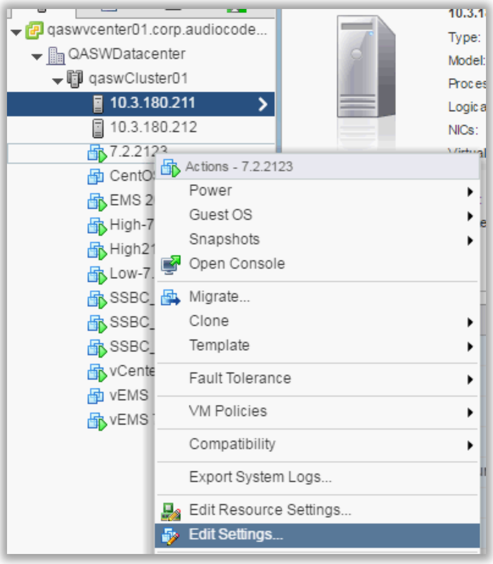
Figure 9-2: Hosts and Clusters



vmware vSphere Web Client
vmware@QASWVCENTER01 | Help | Search
Navigator
Home
qaswvcenter01.corp.audiocode...
QASWDatacenter
qaswCluster01
10.3.180.211
10.3.180.212
7.2.2123
CentOS7-ems-219
EMS 203-7.2.2123
High-7.2.2055
High217-LyDS-7.2.2110
Low-7.2.2055
SSBC_01
SSBC_02_HA
SSBC_10.3.181.96
vCenter
vEMS 7.2.1000
vEMS-7.2.3030-10.3.1...
qaswCluster01 Actions
Summary Monitor Manage Related Objects
qasw Cluster01
Total Processors: 20
Total vMotion Migrations: 48
CPU FREE: 41.79 GHz
USED: 14.07 GHz CAPACITY: 55.86 GHz
MEMORY FREE: 63.88 GB
USED: 128.05 GB CAPACITY: 191.93 GB
STORAGE FREE: 4.20 TB
USED: 2.47 TB CAPACITY: 6.67 TB
Cluster Resources
Cluster Consumers
Related Objects
Datacenter QASWDatacenter
More Related Objects
vSphere HA
Tags
Assigned Tag Category Descri
This list is empty.
Alarms
All (1) New (1) Acknowl...
qaswvcenter01.corp.audiocodes...
Performance Charts Service He...
Work In Progress
vEMS - Edit Resource S...
Recent Tasks
Task Name Target Status Initiator Queued For Start Time Completion Time

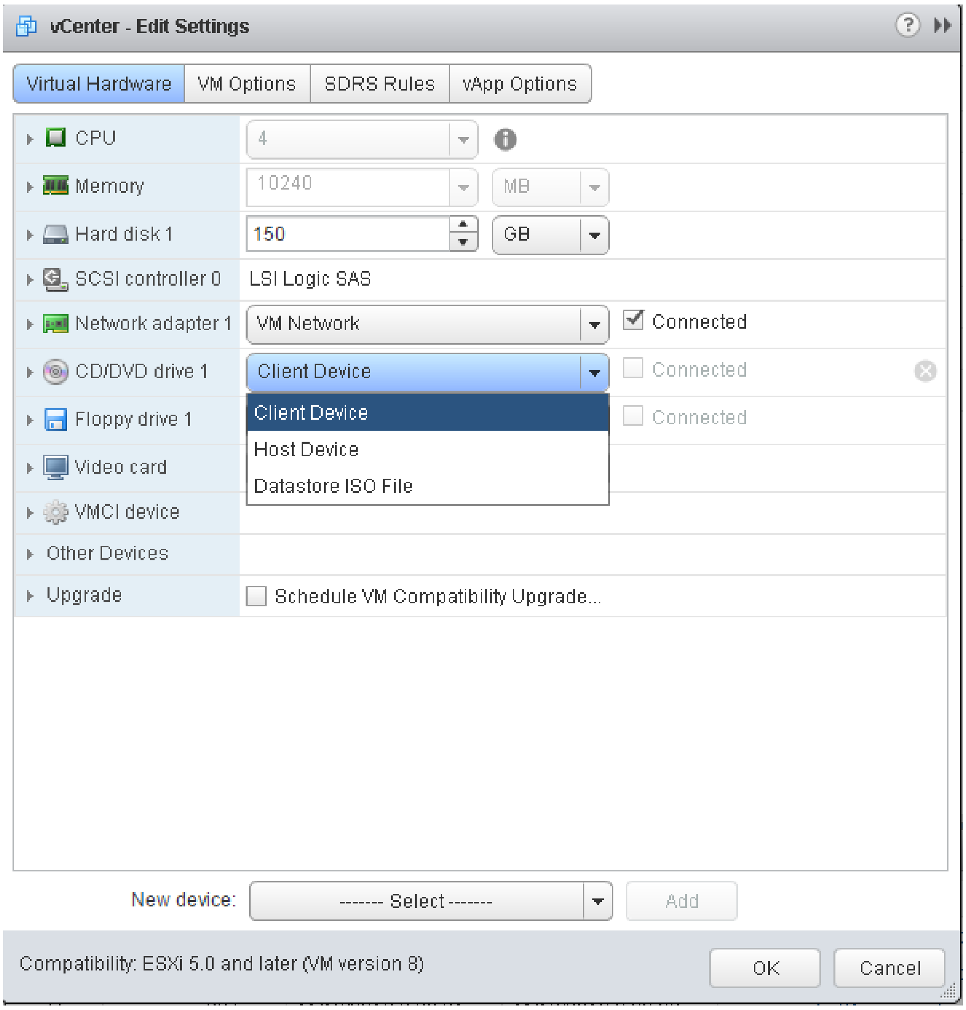
4. Right-click the AudioCodes EMS node that you wish to upgrade and choose the **Edit Settings** option.

Figure 9-3: Edit Settings Option



The vCenter Edit Settings screen is displayed.

Figure 9-4: Connection Options



CPU: 4

Memory: 10240 MB

Hard disk 1: 150 GB

SCSI controller 0: LSI Logic SAS

Network adapter 1: VM Network ☑ Connected

CD/DVD drive 1: Client Device □ Connected

Floppy drive 1: □ Connected

Video card

VMCI device

Other Devices

Upgrade: □ Schedule VM Compatibility Upgrade...

New device: ------- Select -------

Compatibility: ESXi 5.0 and later (VM version 8)

5. In the **Virtual Hardware** tab, select the CD/DVD drive item, and from the drop-down list, select the relevant option according to where you placed the Upgrade Media (CD/DVD or ISO image file):
   - **Client Device:** This option enables you to run the upgrade from the PC running the remote console (see Section 9.1.1).
   - **Host Device:** This option enables you to run the upgrade from the CD/DVD drive of the VMware server host (see Section 9.1.2).
   - **Datastore ISO file:** This option enables you to run the upgrade from the image file on the storage device of the VMware server host. When you choose this option, browse to the location of the ISO file on the VMware storage device (see Section 9.1.2).

9.1.1 Setting up Upgrade Using VMware Remote Console Application (VMRC)

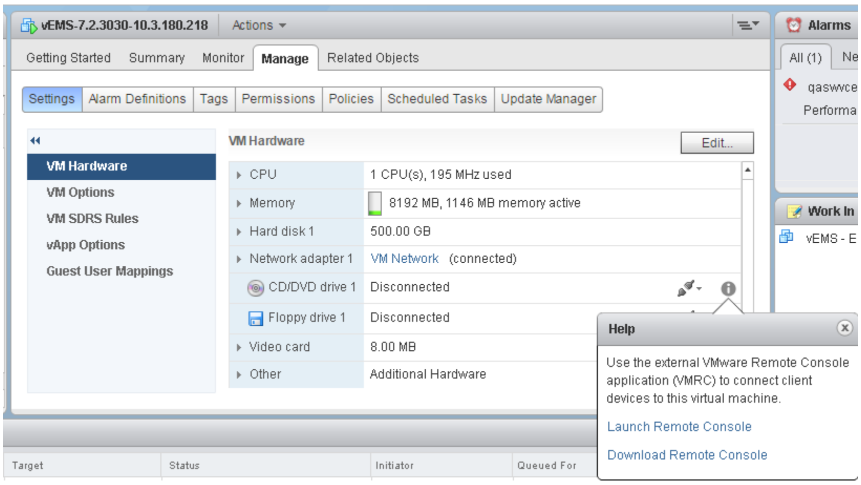
This section describes how to run the upgrade from the VMware host. This procedure requires connecting to the VMware host using the VMware Remote Console application (VMRC).

➢ **To run the upgrade using VMRC:**

1. In the **Manage** tab under **Settings**> **VM Hardware**, select the Help icon adjacent to the CD/DVD drive item and then from the pop-up, click the **Launch Remote Console** to launch the VMware Remote Console application (VMRC). If necessary, click the **Download Remote Console** link to download this application.

Note: If you already have a remote console application installed on your machine, you can use your pre-installed application.

Figure 9-5: Help Link to Launch Remote Console



CPU 1 CPU(s), 195 MHz used

Memory 8192 MB, 1146 MB memory active

Hard disk 1 500.00 GB

Network adapter 1 VM Network (connected)

CD/DVD drive 1 Disconnected

Floppy drive 1 Disconnected

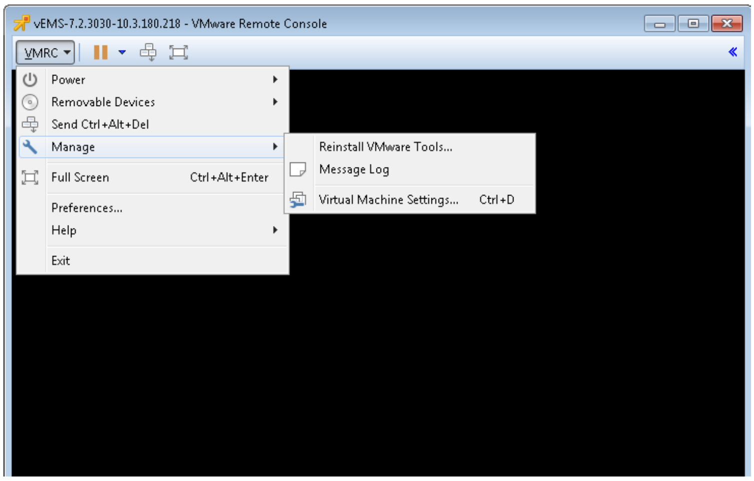
Video card 8.00 MB

Other Additional Hardware

Use the external VMware Remote Console application (VMRC) to connect client devices to this virtual machine.

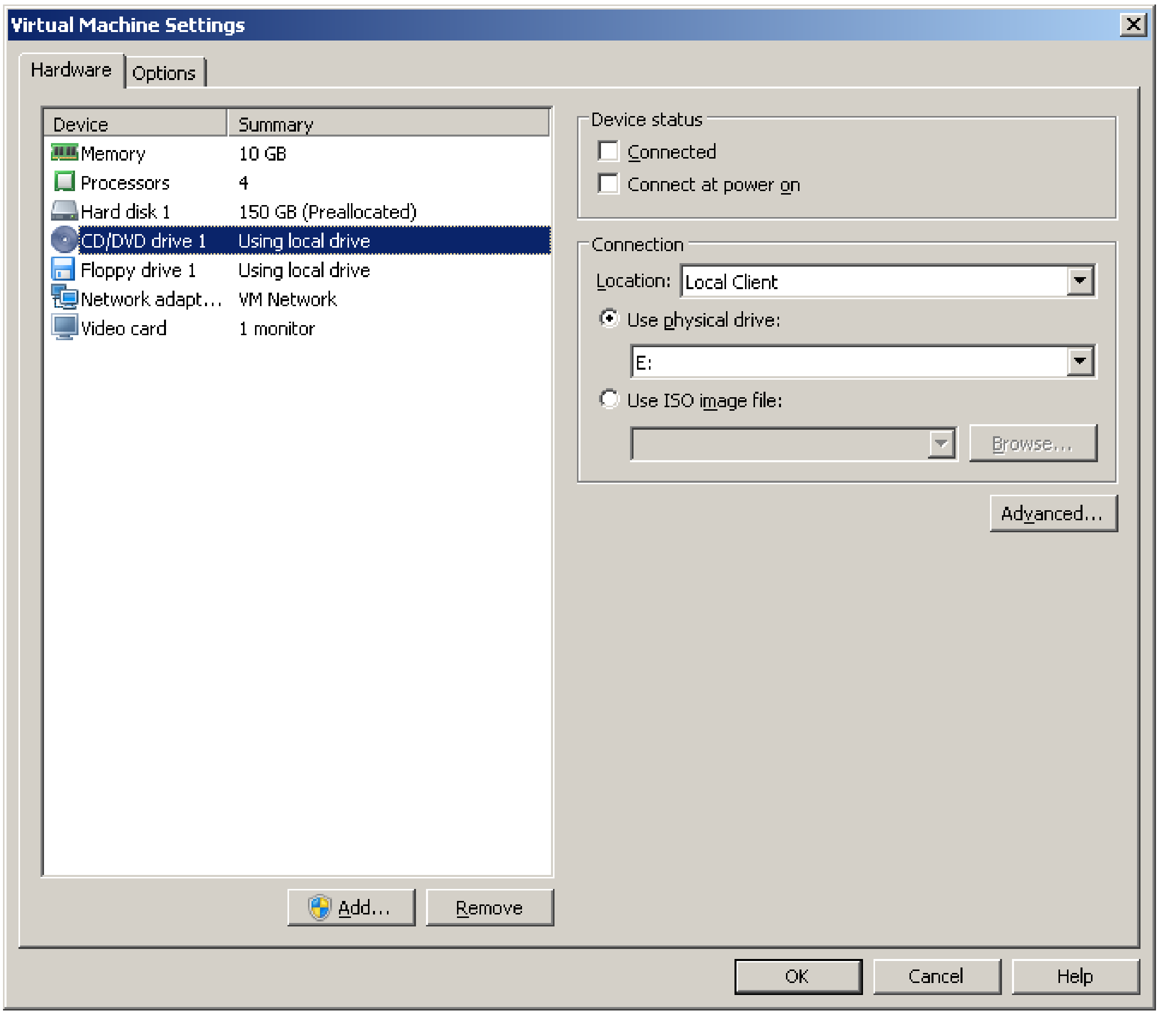
The remote console application is displayed.

Figure 9-6: Remote Console Application


vEMS-7.2.3030-10.3.180.218 - VMware Remote Console
VMRC
Power
Removable Devices
Send Ctrl+Alt+Del
Manage
Full Screen Ctrl+Alt+Enter
Preferences...
Help
Exit
Reinstall VMware Tools...
Message Log
Virtual Machine Settings... Ctrl+D

2. In the toolbar, from the VMRC drop-down list, choose **Manage** > **Virtual Machine Settings**. The Virtual Machine Settings screen is displayed:

Figure 9-7: Virtual Machine Settings



Device	Summary
Memory	10 GB
Processors	4
Hard disk 1	150 GB (Preallocated)
CD/DVD drive 1	Using local drive
Floppy drive 1	Using local drive
Network adapt...	VM Network
Video card	1 monitor

Device status

□ Connected

□ Connect at power on

Connection

Location: Local Client

● Use physical drive:

E:

○ Use ISO image file:

3. From the Location drop-down list, select **Local Client**.

4. Select the CD/DVD drive item and then choose one of the following:
   - Use physical drive: from the drop-down list, select the CD/DVD drive where you placed the Upgrade media.
   - Use ISO image file: browse to the location of the ISO image file.
5. Click **OK**.
6. Proceed to Section 9.2.

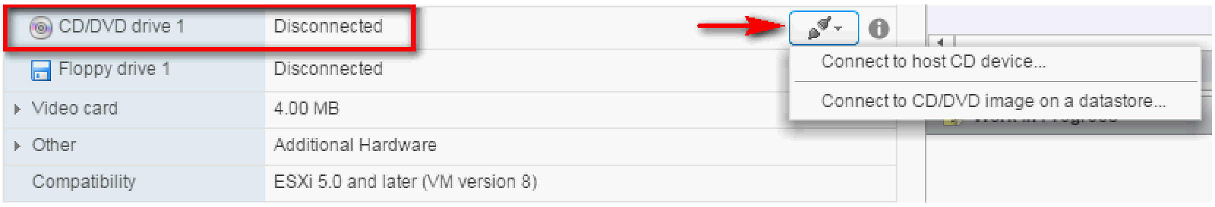
9.1.2 Setting up Upgrade Using VMware Server Host

This section describes how to run the upgrade using the VMware server host.

➢ To run the upgrade using the VMware Server host:

1. Select the **Manage** tab, right-click the Connect icon and select one of the following options:
   - Connect to host CD device
   - Connect to CD/DVD image on a datastore

Figure 9-8: Connect to Host CD Device/ Datastore ISO file

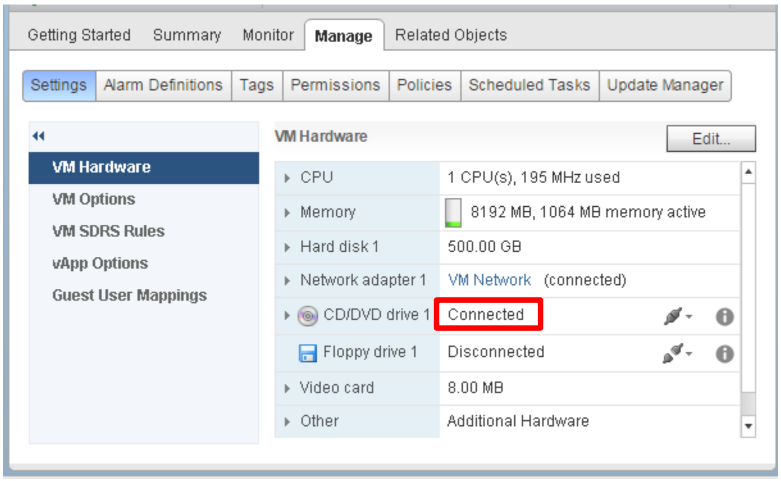


CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	4.00 MB
Other	Additional Hardware
Compatibility	ESXi 5.0 and later (VM version 8)

Connect to host CD device...
Connect to CD/DVD image on a datastore...

2. Wait until the machine reconfiguration has completed, and then verify that the 'Connected' status is displayed:

Figure 9-9: CD/DVD Drive - Connected Status



VM Hardware

CPU	1 CPU(s), 195 MHz used
Memory	8192 MB, 1064 MB memory active
Hard disk 1	500.00 GB
Network adapter 1	VM Network (connected)
CD/DVD drive 1	Connected
Floppy drive 1	Disconnected
Video card	8.00 MB
Other	Additional Hardware

3. Proceed to Section 9.2.

9.2 Step 2: Running the VMware Upgrade

This section describes how to run the VMware upgrade script.

➢ To run the VMware upgrade:

1. Open an SSH connection or the VM console.
2. Login into the EMS server as ‘acems’ user with password *acems* (or customer defined password).
3. Switch to 'root' user and provide *root* password (default password is *root*):

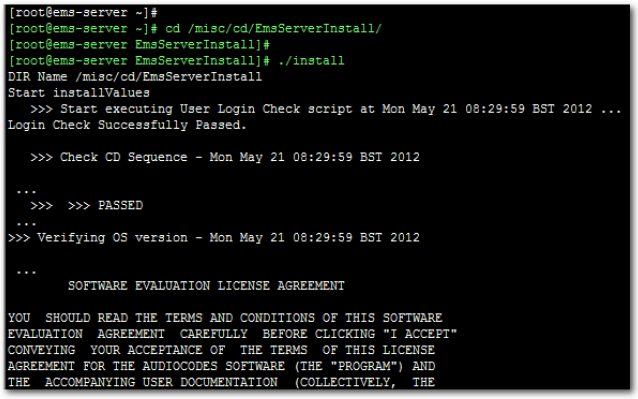
```
su – root
```

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.

4. Change directory to ‘/misc/cd/EmsServerInstall’ and run the install script.

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

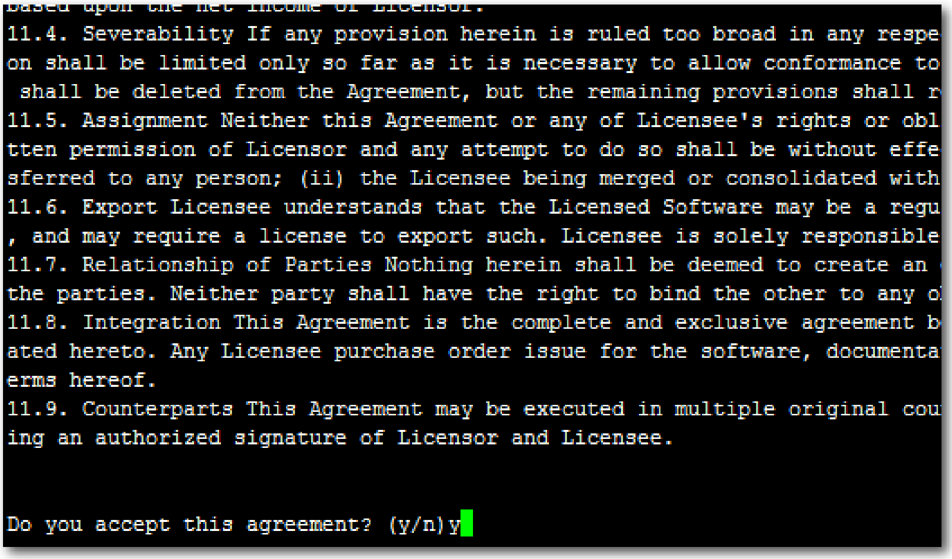
Figure 9-10: EMS Server Installation Script



```
[root@ems-server ~]#
[root@ems-server ~]# cd /misc/cd/EmsServerInstall/
[root@ems-server EmsServerInstall]#
[root@ems-server EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
   >>> Start executing User Login Check script at Mon May 21 08:29:59 BST 2012 ...
Login Check Successfully Passed.

   >>> Check CD Sequence - Mon May 21 08:29:59 BST 2012

 ...
   >>>  >>> PASSED
 ...
>>> Verifying OS version - Mon May 21 08:29:59 BST 2012

 ...
        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
```

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

Figure 9-11: EMS Server Upgrade (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. OS patches are installed.

   After the OS patches installation, you are prompted to press Enter to reboot.

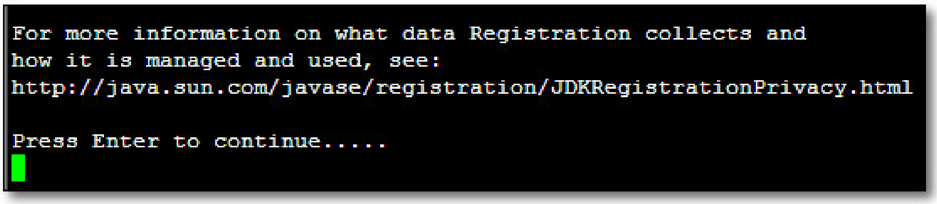
Note: This step is optional and depends upon which version you are upgrading. After the EMS server has rebooted, repeat steps 2 to 5.

7. If the EMS version you are upgrading to is packaged with a later version of Java than the one that is currently installed, type **yes**, and then press Enter to upgrade the Java version, otherwise, skip this step:

```
Java DB version 10.4.2.1.1 is currently installed.
Upgrade to version 10.6.2.1.1 ? [yes,no]yes
```

8. At the end of Java installation, press Enter to continue.

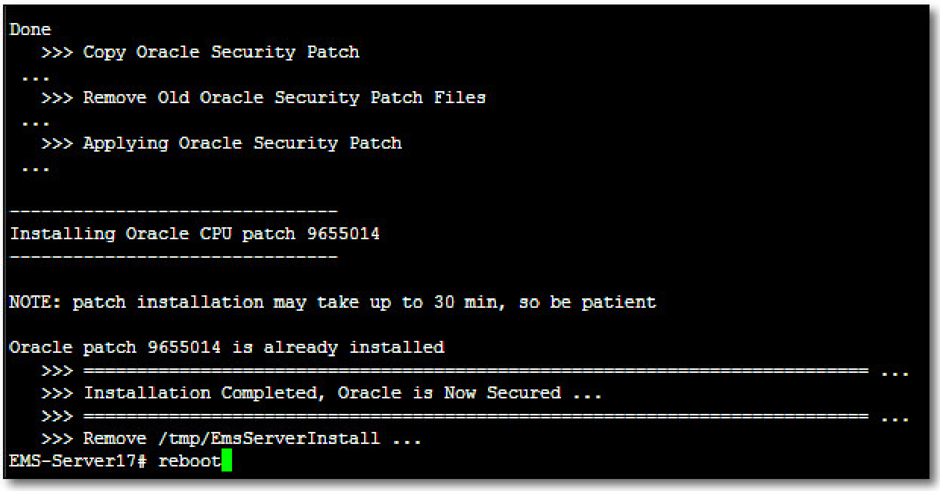
Figure 9-12: EMS Server Application Upgrade (Linux) - Java Installation



```
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 reboot the EMS server.

Figure 9-13: EMS Server Upgrade (Linux) Complete



```
Done
   >>> Copy Oracle Security Patch
 ...
   >>> Remove Old Oracle Security Patch Files
 ...
   >>> Applying Oracle Security Patch
 ...

-------------------------------
Installing Oracle CPU patch 9655014
-------------------------------

NOTE: patch installation may take up to 30 min, so be patient

Oracle patch 9655014 is already installed
   >>> ========================================================================== ...
   >>> Installation Completed, Oracle is Now Secured ...
   >>> ========================================================================== ...
   >>> Remove /tmp/EmsServerInstall ...
EMS-Server17# reboot
```

Note: For SEM Users: each time the EMS server version is upgraded, the operator should perform CTRL – F5 (refresh) action on the SEM Page, and then re-login to the application.

.

This page is intentionally left blank.

Part IV

EMS Server Machine Backup and Restore

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

10 EMS Server Backup

There are two main backup processes that run on the EMS 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), EMS Software Manager content and server_xxx directory’s content.

  To change the weekly backup’s time and date, see Section 16.3.
- **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. 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)

This page is intentionally left blank.

11 EMS Server Restore

This section describes how to restore the EMS 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 EMS 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 EMS server:

1. Install (or upgrade) EMS to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.

   For more details, see Chapter 8 on page 81.

2. Use the EMS Server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.

   For more details, see Chapter 12 on page 103.

3. Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
4. Copy all backup files to /data/NBIF directory by SCP or SFTP client using the 'acems' user.
5. In EMS Server Manager, go to the Application Maintenance menu and select the **Restore** option.
6. Follow the instructions during the process. For more details, see Section 16.4 on page 118.
7. After the restore process has completed, you will be asked to reboot the machine.
8. If you installed custom certificates prior to the restore, you must reinstall these certificates (see Appendix E).

This page is intentionally left blank.

Part V

EMS Server Manager

This part describes the EMS server machine maintenance using the EMS Server Management utility.

The EMS Server Management utility is a CLI interface that is used to configure networking parameters and security settings and to perform various maintenance actions on the EMS server.

Warning: Do not perform EMS Server Manager actions directly through the Linux OS shell. If you perform such actions, EMS application functionality may be harmed.

Note: To exit the EMS Server Manager to Linux OS shell level, press **q**.

12 Getting Started

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

12.1.1 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 EMS 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 EMS server by SSH, as ‘acems’ user and enter password *acems*.
2. Switch to 'root' user and provide root password (default password is root):

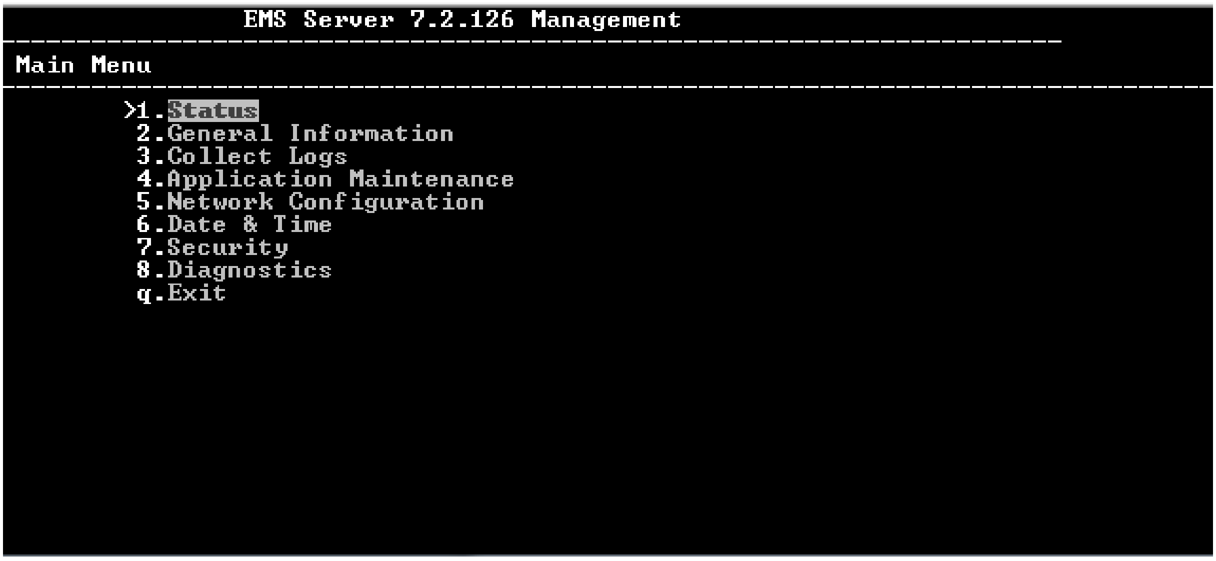
   ```
   su – root
   ```

3. Type the following command:

   ```
   # EmsServerManager
   ```

The EMS Server Manager menu is displayed:

Figure 12-1: EMS Server Manager Menu



```
                  EMS Server 7.2.126 Management
-----------------------------------------------------------------------
Main Menu
------------------------------------------------------------------------------------------
         >1.Status
          2.General Information
          3.Collect Logs
          4.Application Maintenance
          5.Network Configuration
          6.Date & Time
          7.Security
          8.Diagnostics
          q.Exit
```

Important:

- Whenever prompted to enter **Host Name**, provide letters or numbers.
- Ensure IP addresses contain all correct digits.
- For menu options where reboot is required, the EMS server automatically reboots after changes confirmation.

  For some of the configuration options, you are prompted to authorize the changes. There are three options: Yes, No, Quit (y,n,q). **Yes** implements the changes, **No** cancels the changes and returns you to the initial prompt for the selected menu option and **Quit** returns you to the previous menu.

The following describes the full menu options for the EMS Management utility:

- **Status** – Shows the status of current EMS processes (see Chapter 13)
- **General Information** – Provides the general EMS server current information from the Linux operating system, including EMS Version, EMS Server Process Status, Oracle Server Status, Apache Server Status, Java Version, Memory size and Time Zone. See Chapter 14.
- **Collect Logs** – Collates all important logs into a single compressed file (see Chapter 15):
  - General Info
  - Collect Logs

- **Application Maintenance** – Manages system maintenance actions (see Chapter 16):
  - Start / Stop the Application
  - Web Servers
  - Change Schedule Backup Time
  - Restore
  - High Availability
  - License
  - Shutdown the machine
  - Reboot the machine
- **Network Configuration** – Provides all basic, advanced network management and interface updates (see Chapter 17):
  - Server IP Address (The server will be rebooted)
  - Ethernet Interfaces (The server will be rebooted)
  - Ethernet Redundancy (The server will be rebooted)
  - DNS Client
  - NAT
  - Static Routes
  - SNMP Agent
  - SNMPv3 Engine ID
- **Date & Time** – Configures time and date settings (see Chapter 18):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (see Chapter 19):
  - EMS user
  - SSH
  - DB Password (EMS and SEM applications will be stopped)
  - OS Users Passwords
  - File Integrity Checker
  - Software Integrity Checker (AIDE) and Prelinking
  - USB Storage
  - Network Options
  - Audit Agent Options (the server will be rebooted)
  - HTTPS Authentication
  - Enable SEM client secured connection (EMS application will be restarted).

    - Enable IP Phone Manager client and JAWS secured communication (Apache will be restarted).
    - Server Certificates Update
    - SEM-AudioCodes device communication

- **Diagnostics** – Manages system debugging and troubleshooting (see Chapter 20):
    - Server Syslog
    - Devices Syslog
    - Devices Debug

12.1.2 Using the EMS Server Manager

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

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

This page is intentionally left blank.

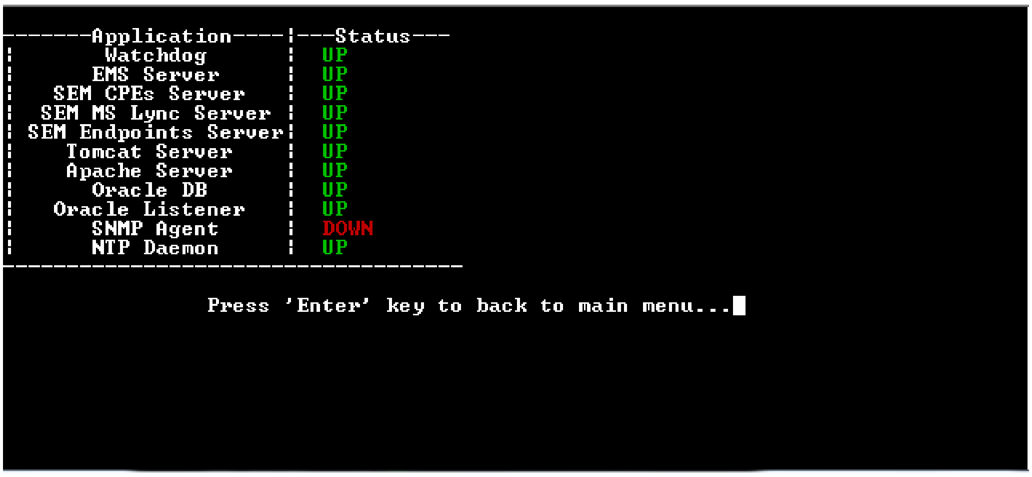
13 Viewing Process Statuses

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

➢ To view the statuses of the current EMS applications:

1. From the EMS Server Management root menu, choose **Status**, and then press Enter; the following is displayed:

Figure 13-1: Application Status



```
-------Application----|---Status---
|       Watchdog       |  UP
|      EMS Server      |  UP
|   SEM CPEs Server    |  UP
|  SEM MS Lync Server  |  UP
| SEM Endpoints Server|  UP
|     Tomcat Server    |  UP
|     Apache Server    |  UP
|      Oracle DB       |  UP
|   Oracle Listener    |  UP
|      SNMP Agent      |  DOWN
|      NTP Daemon      |  UP
------------------------------------

               Press 'Enter' key to back to main menu...
```

The following table describes the application statuses.

Table 13-1: Application Statuses

Application	Status
Watchdog	Indicates the status of the EMS Watchdog process.
EMS Server	Indicates the status of the EMS Server process.
SEM CPEs Server	Indicates the status of the XML based SEM communication between the devices and the SEM CPEs Server.
SEM MS Lync Server	Indicates the status of the SEM MS Lync Server, which manages the HTTP/S connection with the MS-SQL Server.
SEM Endpoints Server	Indicates the status of the Endpoint Server, which manages the UDP connection with the Endpoints (IP Phones) for SIP Publish RFC 6035 messages.
Tomcat Server	Indicates the status of the Tomcat server, which manages the connection with the SEM Web client.
Apache Server	Indicates the status of the Apache server, which manages the following connections: HTTP/S connection with the AudioCodes device,

Application	Status
	The EMS Server-Client connection. The HTTP connection that is used by Endpoints for downloading firmware and configuration files from the EMS server.
Oracle DB	Indicates the status of the Oracle Database process.
Oracle Listener	Indicates the status of the Oracle Listener process.
SNMP Agent	Indicates the status of the Linux SNMP Agent process. This agent is not responsible for the SNMPv2/SNMPv3 connection with the AudioCodes devices.
NTP Daemon	Indicates the status of the NTP Daemon process.

14 Viewing General Information

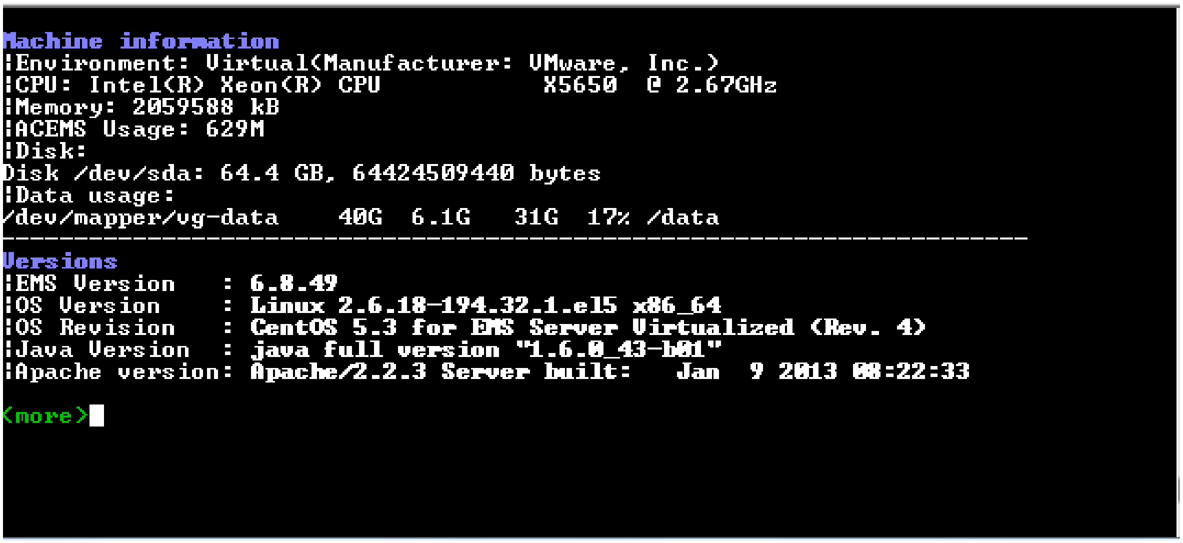
This section describes the General Information and Logs collection options. The General Information option provides detailed information about the EMS server configuration and current status variables. The following information is provided:

- Components versions: EMS, Linux, Java, Apache
- Components Statuses: EMS server process and security, Watchdog, Apache, Oracle, SNMP agent, Tomcat and SEM.
- Memory size and disk usage
- Network configuration
- Time Zone and NTP configuration
- User logged in and session type

➢ To view General Information:

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

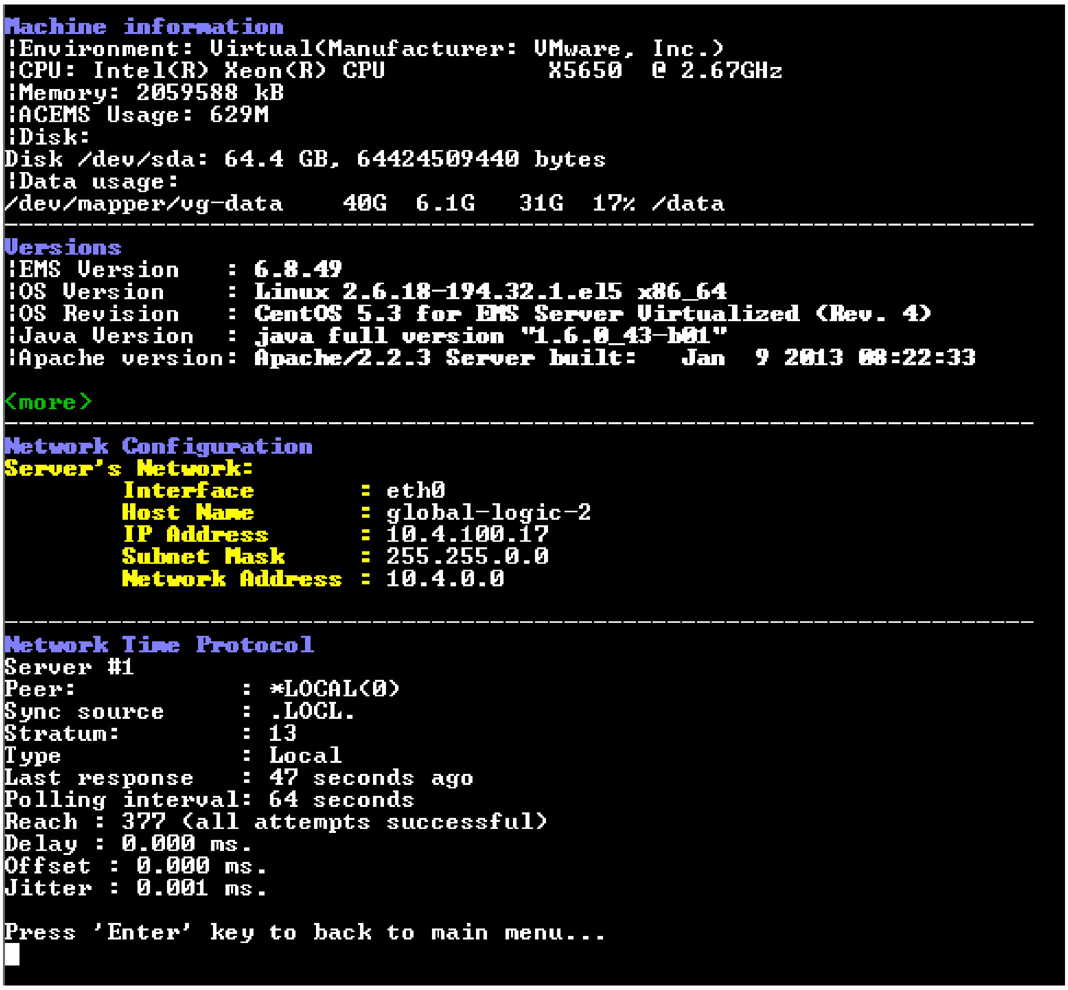
Figure 14-1: General Information



```
Machine information
|Environment: Virtual(Manufacturer: VMware, Inc.)
|CPU: Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
|Memory: 2059588 kB
|ACEMS Usage: 629M
|Disk:
Disk /dev/sda: 64.4 GB, 64424509440 bytes
|Data usage:
/dev/mapper/vg-data    40G  6.1G   31G  17% /data
----------------------------------------------------------------------
Versions
|EMS Version    : 6.8.49
|OS Version     : Linux 2.6.18-194.32.1.el5 x86_64
|OS Revision    : CentOS 5.3 for EMS Server Virtualized (Rev. 4)
|Java Version   : java full version "1.6.0_43-b01"
|Apache version: Apache/2.2.3 Server built:   Jan  9 2013 08:22:33

<more>
```

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

Figure 14-2: General Information



```
Machine information
¦Environment: Virtual(Manufacturer: VMware, Inc.)
¦CPU: Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
¦Memory: 2059588 kB
¦ACEMS Usage: 629M
¦Disk:
Disk /dev/sda: 64.4 GB, 64424509440 bytes
¦Data usage:
/dev/mapper/vg-data    40G  6.1G   31G  17% /data
----------------------------------------------------------------------
Versions
¦EMS Version    : 6.8.49
¦OS Version     : Linux 2.6.18-194.32.1.el5 x86_64
¦OS Revision    : CentOS 5.3 for EMS Server Virtualized (Rev. 4)
¦Java Version   : java full version "1.6.0_43-b01"
¦Apache version: Apache/2.2.3 Server built:   Jan  9 2013 08:22:33

<more>
----------------------------------------------------------------------
Network Configuration
Server's Network:
        Interface        : eth0
        Host Name        : global-logic-2
        IP Address       : 10.4.100.17
        Subnet Mask      : 255.255.0.0
        Network Address  : 10.4.0.0

----------------------------------------------------------------------
Network Time Protocol
Server #1
Peer:            : *LOCAL(0)
Sync source      : .LOCL.
Stratum:         : 13
Type             : Local
Last response    : 47 seconds ago
Polling interval: 64 seconds
Reach : 377 (all attempts successful)
Delay : 0.000 ms.
Offset : 0.000 ms.
Jitter : 0.001 ms.

Press 'Enter' key to back to main menu...
```

15 Collecting Logs

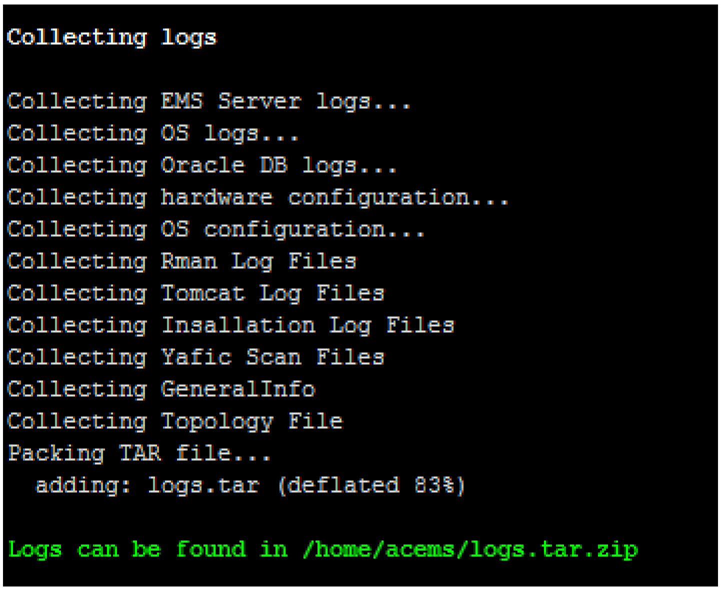
This option enables you to collect important log files. All log files are collected in a single file log.tar that is created under the user home directory. The log file size is approximately 5MB. The following log files are collected:

- EMS Server Application logs
- Server's Syslog Messages
- Oracle Database logs
- Tomcat logs
- Hardware information (including disk)
- Relevant network configuration files (including static routes)

➢ To collect logs:

- From the EMS Server Management root menu, choose **Collect Logs**, and then press Enter; the EMS server commences the log collection process:

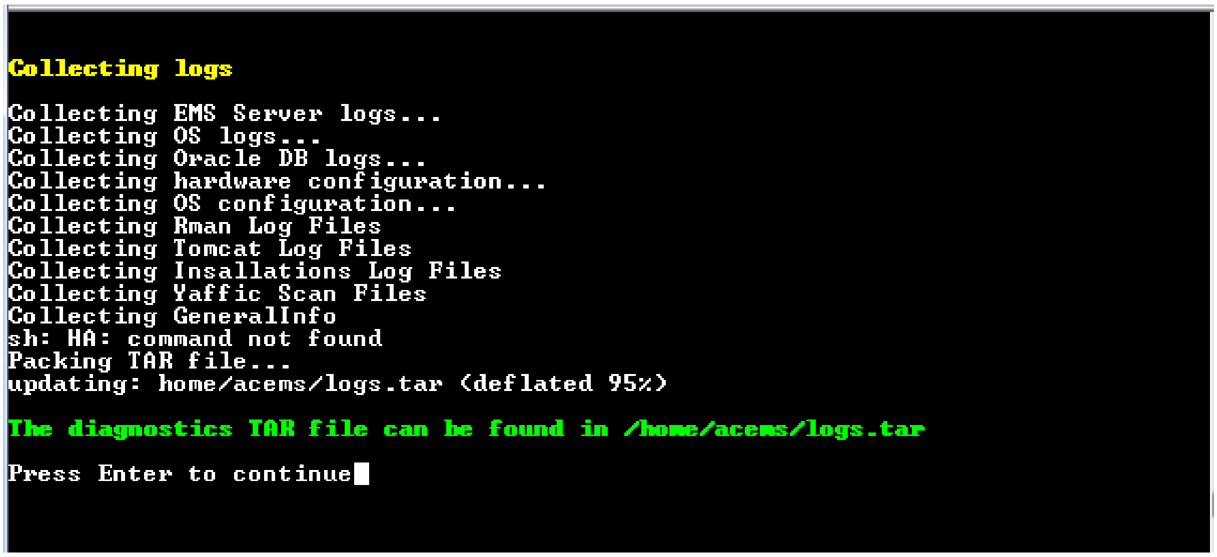
Figure 15-1: EMS Server Manager – Collect Logs



```
Collecting logs

Collecting EMS Server logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Insallation Log Files
Collecting Yafic Scan Files
Collecting GeneralInfo
Collecting Topology File
Packing TAR file...
  adding: logs.tar (deflated 83%)

Logs can be found in /home/acems/logs.tar.zip
```

This process can take a few minutes. Once the file generation has completed, a message is displayed on the screen informing you that a Diagnostic tar file has been created and the location of the tar file:

Figure 15-2: TAR File Location



```
Collecting logs

Collecting EMS Server logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Insallations Log Files
Collecting Yaffic Scan Files
Collecting GeneralInfo
sh: HA: command not found
Packing TAR file...
updating: home/acems/logs.tar (deflated 95%)

The diagnostics TAR file can be found in /home/acems/logs.tar

Press Enter to continue
```

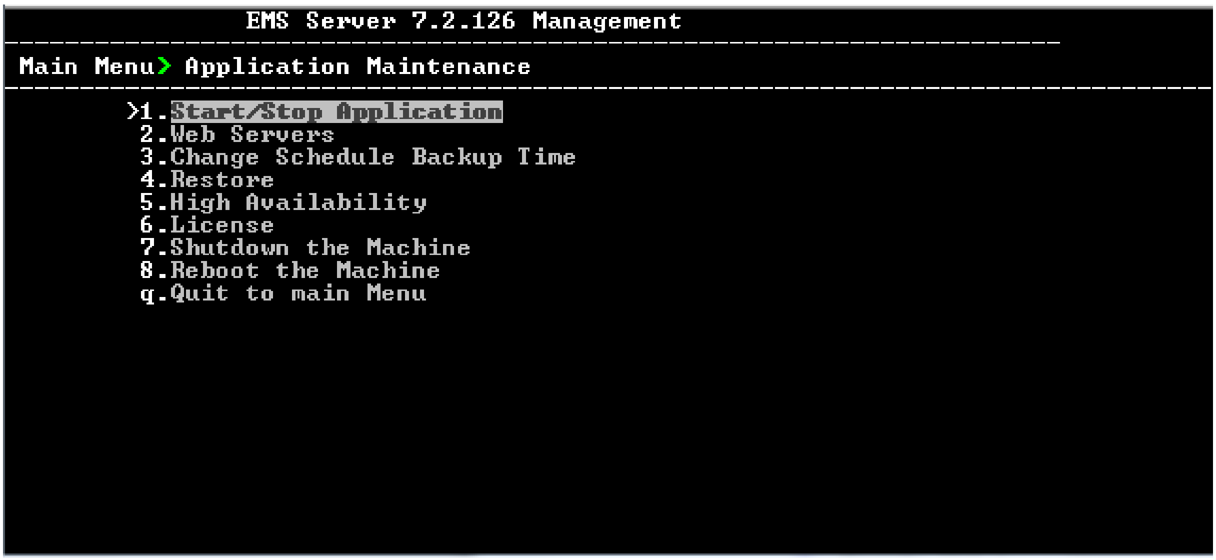
16 Application Maintenance

This section describes the application maintenance.

➢ **To configure application maintenance:**

- From the EMS Server Manager root menu, choose **Application Maintenance**; the following is displayed:

Figure 16-1: Application Maintenance



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Application Maintenance
--------------------------------------------------------------------------------
        >1.Start/Stop Application
         2.Web Servers
         3.Change Schedule Backup Time
         4.Restore
         5.High Availability
         6.License
         7.Shutdown the Machine
         8.Reboot the Machine
         q.Quit to main Menu
```

This menu includes the following options:

- Start/Stop Application (see Section 16.1 on page 115).
- Web Servers (see Section 16.2on page 116).
- Change Schedule Backup Time (see Section 16.316.3 on page 118).
- Restore (see Section 16.4 on page 118)
- High Availability (see Chapter 21 on page 175).
- License (see Section 16.5 on page 119).
- Shutdown the Machine (see Section 16.6 on page 121).
- Reboot the Machine (see Section 16.7 on page 121).

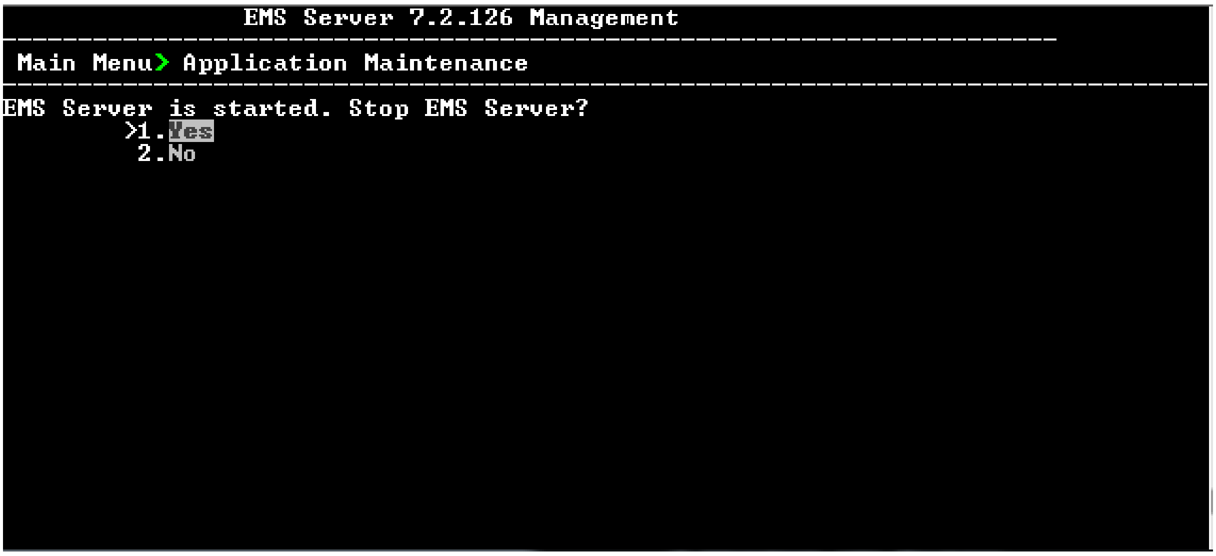
16.1 Start /Stop the Application

This section describes how to start or stop the application.

➢ **To start/stop the application:**

1. From the Application Maintenance menu, choose **Start / Stop the Application**, and then press Enter; the following is displayed:

Figure 16-2: Start or Stop the EMS Server



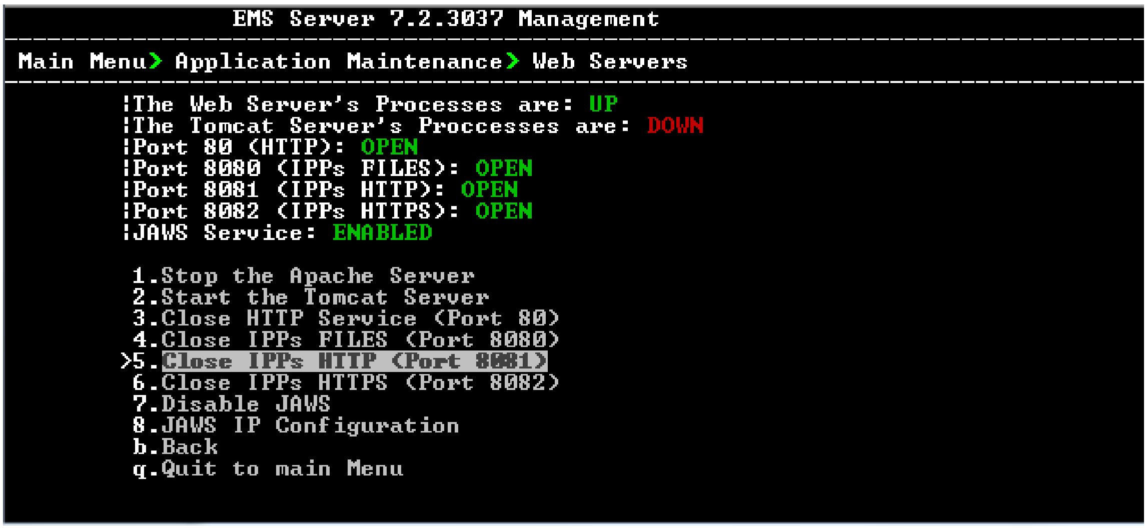
```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Application Maintenance
--------------------------------------------------------------------------------
EMS Server is started. Stop EMS Server?
        >1.Yes
         2.No
```

2. Select **Yes** to start the EMS server or **No** to stop it.

16.2 Web Servers

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

Figure 16-3: – Web Servers



```
                EMS Server 7.2.3037 Management
--------------------------------------------------------------------------------
 Main Menu> Application Maintenance> Web Servers
--------------------------------------------------------------------------------
        |The Web Server's Processes are: UP
        |The Tomcat Server's Proccesses are: DOWN
        |Port 80 (HTTP): OPEN
        |Port 8080 (IPPs FILES): OPEN
        |Port 8081 (IPPs HTTP): OPEN
        |Port 8082 (IPPs HTTPS): OPEN
        |JAWS Service: ENABLED

         1.Stop the Apache Server
         2.Start the Tomcat Server
         3.Close HTTP Service (Port 80)
         4.Close IPPs FILES (Port 8080)
        >5.Close IPPs HTTP (Port 8081)
         6.Close IPPs HTTPS (Port 8082)
         7.Disable JAWS
         8.JAWS IP Configuration
         b.Back
         q.Quit to main Menu
```

16.2.1 Apache and Tomcat Server Processes

This section describes how to open and close the Apache and Tomcat Web server connections.

➢ **To stop the Apache server:**

- In the Web Servers menu, choose option **Stop/Start Apache Server**, and then press Enter.

➢ To stop the Tomcat server:

- In the Web Servers menu, choose option **Stop/Start Tomcat Server**, and then press Enter.

16.2.2 HTTP/HTTPS Services

This section describes how to open and close the different HTTP/HTTPS services.

➢ To open/close HTTP Service (Port 80):

- In the Web Servers menu, choose option **Open/Close HTTP Service (Port 80)**, and then press Enter.

  This HTTP port is used for the connection between the EMS server and all AudioCodes devices, with the JAWS client and with the IP Phone Management Server Web browser.

➢ To open/close IPPs FILES (Port 8080):

- In the Web Servers menu, choose option **Open/Close IPPs FILES (Port 8080)**, and then press Enter.

  This HTTP port is used for downloading firmware and configuration files from the EMS server to the endpoints.

➢ To open/close IPPs HTTP (Port 8081):

- In the Web Servers menu, choose option **Open/Close IPPs HTTP (Port 8081)**, and then press Enter.

  This HTTP port is used for sending REST updates from the endpoints to the EMS server, such as alarms and statuses.

➢ To open/close IPPs HTTPS (Port 8082):

- In the Web Servers menu, choose option **Open/Close IPPs HTTPS (Port 8082)**, and then press Enter.

  This HTTPS port is used for sending secure REST updates from the endpoints to the EMS server, such as alarms and statuses (HTTPS without certificate authentication).

➢ To enable/disable JAWS client:

- In the Web Servers menu, choose option **Enable/Disable JAWS**, and then press Enter.

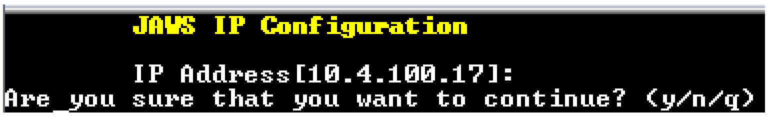
16.2.2.1 JAWS IP Configuration

By default, logging into the EMS server using JAWS can only be performed through the EMS server's first interface only. This option allows you to configure an alternative interface for the JAWS login.

➢ To change the JAWS login interface:

1. From the Web Server configuration menu, choose option **6**, and then press Enter.
2. Type the desired interface IP address, press Enter, and then confirm by typing **y**.

Figure 16-4: JAWS IP Configuration



```
          JAWS  IP  Configuration

          IP Address[10.4.100.17]:
Are you sure that you want to continue? (y/n/q)
```

16.3 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.
3. Copy all files in /data/NBIF/emsBackup/RmanBackup/ directory to an external machine.
4. Copy /data/NBIF/emsBackup/emsServerBackup_<time&date>.tar file to an external machine.

   Where <time&date> is only an example; replace this path with your filename.

16.4 Restore

This step describes how to restore the EMS server.

➢ To restore the EMS server:

1. Copy all files that you backed up in Section 16.3 to the /data/NBIF directory on the Restore server. Overwrite existing files if required.
2. From the EMS server Application Maintenance menu, choose **Restore**; a script is started.
3. Follow the instructions; you might need to press Enter a few times.
4. After the restore operation has completed and then reboot the EMS server (see Section 17.1).

16.5 License

The License menu enables you to view the details of the existing license or upload a new license.

The OVOC Server License (SBC License pool, EMS for IP Phones, SEM device and IP Phone Management) should have a valid license loaded to the server in order for it to be fully operational.

In order to obtain a valid license for your OVOC Server License you should activate your product through AudioCodes License Activation tool at htttp://www.audiocodes.com/swactivation. You will need your Product Key (see below) and the Server Machine ID (see below) for this activation process:**Product Key:** the Product Key string represents the customer order for the EMS and SEM products. For more information, contact your AudioCodes partner.

- **Machine ID:** the Machine ID should be taken from the server as shown in the screen below (enter this ID in the Fingerprint field in the Activation form).
- **License Status:** indicates whether the EMS license is enabled (see Section 16.5.1 below).
- **Expiration Date:** indicates the expiration date of the EMS time license. If an expiration date is not configured, this field displays 'Unlimited' (see below).

  The timezone is determined by the configured date and time in the Date & Time menu (see Section 18.2).

You will receive an e-mail with your product license file.

Note:

- When you order AudioCodes devices (Mediant SBC and Mediant Gateway AudioCodes products), ensure that for those devices that you wish to manage using EMS, a valid feature key is enabled with the "EMS" parameter. Note that this feature key is a separate license to the OVOC Server license that is described in this Section.
- The Mediant 3000 and MP-1288 products are not supported by the SBC License Pool Manager.

16.5.1 EMS Time License

The EMS and SEM license may control the time period for which the product can be used. When the time license is enabled and the configured license time expires, the connection to the EMS/SEM server is denied. The time based license affects all the features in the EMS and SEM including the SBC License Pool, EMS for IP Phones and SEM. When the EMS server time license approaches or reaches its expiration date, the 'EMS License' alarm is raised (Refer to the relevant product *Performance Monitors and Alarms Guide)*.

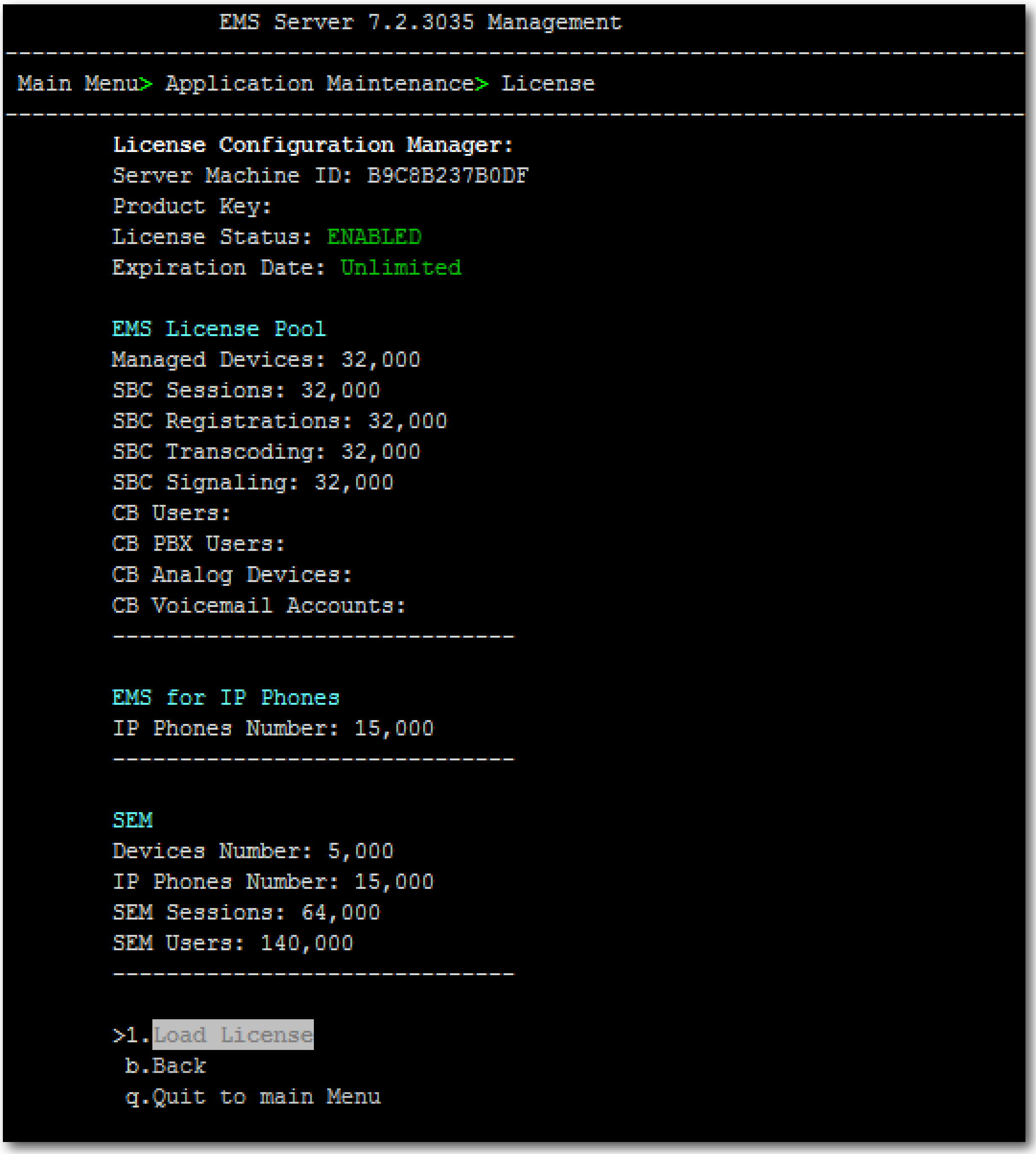
➢ **To view the license details or upload a new license:**

1. Copy the license file that you have obtained from AudioCodes to the following path on the EMS server machine:

/home/acems/<License_File>

2. From the Application Maintenance menu, choose **License** option, and then press Enter; the current SEM License Manager details are displayed:

Figure 16-5: License Manager



```
               EMS Server 7.2.3035 Management
-----------------------------------------------------------------------------
 Main Menu> Application Maintenance> License
-----------------------------------------------------------------------------
        License Configuration Manager:
        Server Machine ID: B9C8B237B0DF
        Product Key:
        License Status: ENABLED
        Expiration Date: Unlimited

        EMS License Pool
        Managed Devices: 32,000
        SBC Sessions: 32,000
        SBC Registrations: 32,000
        SBC Transcoding: 32,000
        SBC Signaling: 32,000
        CB Users:
        CB PBX Users:
        CB Analog Devices:
        CB Voicemail Accounts:
        ------------------------------

        EMS for IP Phones
        IP Phones Number: 15,000
        ------------------------------

        SEM
        Devices Number: 5,000
        IP Phones Number: 15,000
        SEM Sessions: 64,000
        SEM Users: 140,000
        ------------------------------

        >1.Load License
         b.Back
         q.Quit to main Menu
```

- **EMS (SBC) License Pool:**
  - The supported number of managed devices
  - The supported number of managed SBC sessions
  - The supported number of managed SBC user registrations
  - The supported number of managed SBC transcoding sessions
  - The supported number of managed SBC signaling sessions
  - The supported number of managed CB users
  - The supported number of managed CloudBond (CB) PBX users

    - ♦ The supported number of managed CB Analog devices (for future support)
    - ♦ The supported number of managed CB Voicemail accounts
- **EMS for IP Phones:**
    - ♦ The supported number of IP Phones that can be managed by the EMS.
- **SEM:**
    - ♦ The supported number of devices that can be managed by the SEM.
    - ♦ The supported number of IP Phones that can be managed by the SEM.
    - ♦ The supported number of simultaneous call sessions that can be managed by the SEM.
    - ♦ The supported number of users that can be managed by the SEM.

3. To load a new license, choose option **1**.
4. Enter the license file path and name.
5. Restart the EMS server.

16.6 Shutdown the EMS Server Machine

This section describes how to shut down the EMS Server machine.

➢ To shut down the EMS server machine:

1. From the Application Maintenance menu, choose **Shutdown the Machine**, and then press Enter.
2. Type **y** to confirm the shutdown; the EMS server machine is shutdown.

16.7 Reboot the EMS Server Machine

This section describes how to reboot the EMS server machine.

➢ To reboot the EMS server machine:

1. From the Application Maintenance menu, choose **Reboot the Machine**, and then press Enter.
2. Type **y** to confirm the reboot; the EMS server machine is rebooted.

This page is intentionally left blank.

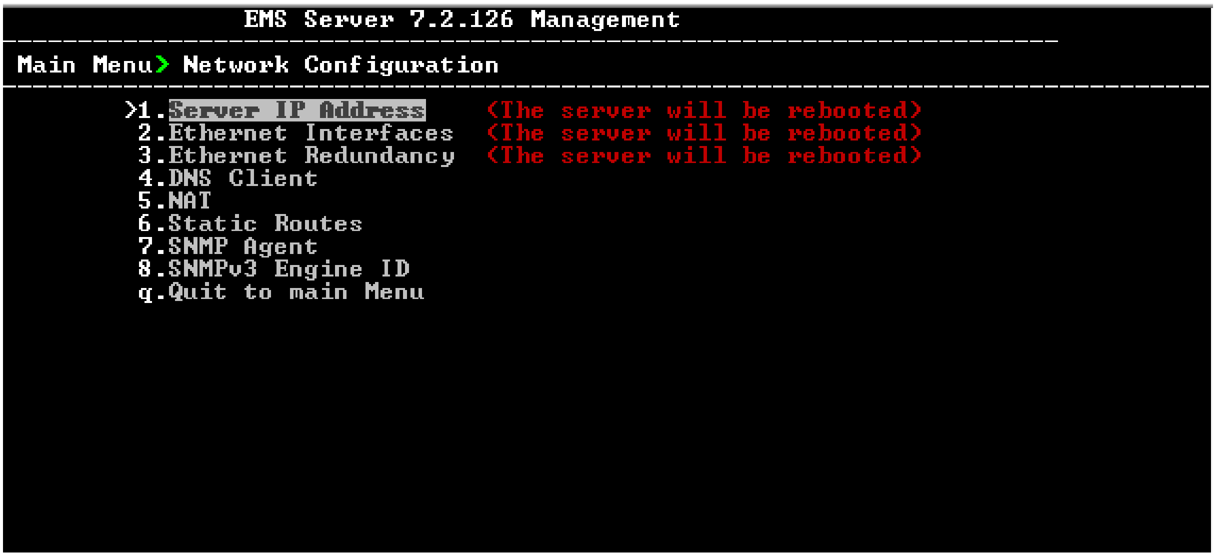
17 Network Configuration

This section describes the networking options in the EMS Server Manager.

➢ To run the network configuration:

- From the EMS Server Manager root menu, choose **Network Configuration**; the following is displayed:

Figure 17-1: Network Configuration



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Network Configuration
--------------------------------------------------------------------------------
        >1.Server IP Address     (The server will be rebooted)
         2.Ethernet Interfaces   (The server will be rebooted)
         3.Ethernet Redundancy   (The server will be rebooted)
         4.DNS Client
         5.NAT
         6.Static Routes
         7.SNMP Agent
         8.SNMPv3 Engine ID
         q.Quit to main Menu
```

This menu includes the following options:

- Server IP Address (the server will be rebooted) (see Section 17.1 on page 123).
- Ethernet Interfaces (the server will be rebooted) (see Section 17.2 on page 125).
- Ethernet Redundancy (the server will be rebooted) (see Section 17.3 on page 128).
- DNS Client (see Section 17.4 on page 133).
- NAT (see Section 17.5 on page 134).
- Static Routes (see Section 17.6 on page 134).
- SNMP Agent (see Section 17.7 on page 135).
- SNMPv3 Engine ID (see Section 17.8 on page 135).

17.1 Server IP Address

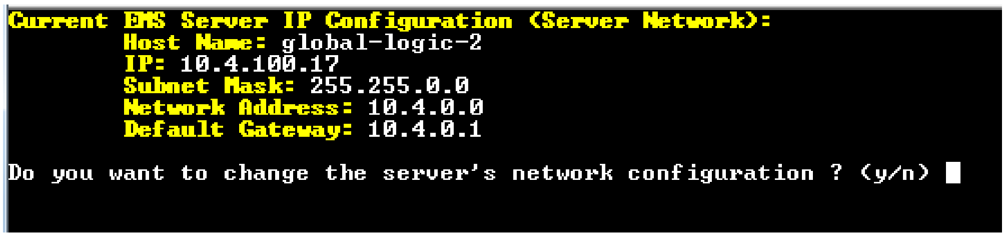
This option enables you to update the EMS server's IP address. This option also enables you to modify the EMS server host name.

Note: When this operation has completed, the EMS automatically reboots for the changes to take effect.

➢ To change Server's IP address:

1. From the Network Configuration menu, choose **Server IP Address**, and then press Enter; the following is displayed:

Figure 17-2: EMS Server Manager – Change Server's IP Address



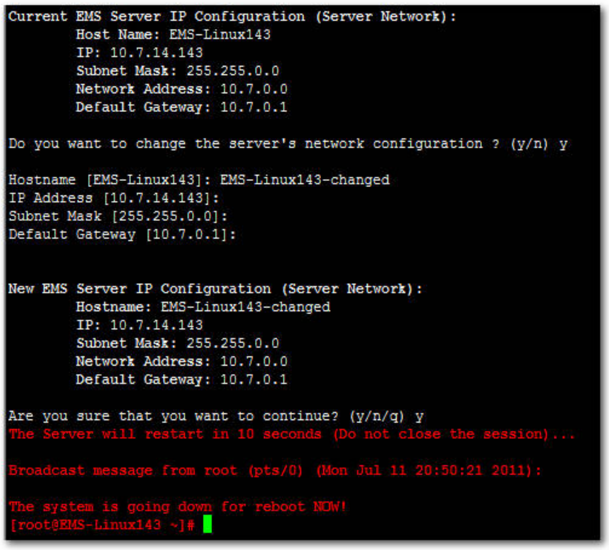
```
Current EMS Server IP Configuration (Server Network):
        Host Name: global-logic-2
        IP: 10.4.100.17
        Subnet Mask: 255.255.0.0
        Network Address: 10.4.0.0
        Default Gateway: 10.4.0.1

Do you want to change the server's network configuration ? (y/n)
```

2. Configure IP configuration parameters as desired.

   Each time you press Enter, the different IP configuration parameters of the EMS server are displayed. These parameters include the Server Host Name, IP address, Subnet Mask, Network Address and Default Gateway.

3. Type **y** to confirm the changes, and then press Enter.

Figure 17-3: IP Configuration Complete



```
Current EMS Server IP Configuration (Server Network):
        Host Name: EMS-Linux143
        IP: 10.7.14.143
        Subnet Mask: 255.255.0.0
        Network Address: 10.7.0.0
        Default Gateway: 10.7.0.1

Do you want to change the server's network configuration ? (y/n) y

Hostname [EMS-Linux143]: EMS-Linux143-changed
IP Address [10.7.14.143]:
Subnet Mask [255.255.0.0]:
Default Gateway [10.7.0.1]:


New EMS Server IP Configuration (Server Network):
        Hostname: EMS-Linux143-changed
        IP: 10.7.14.143
        Subnet Mask: 255.255.0.0
        Network Address: 10.7.0.0
        Default Gateway: 10.7.0.1

Are you sure that you want to continue? (y/n/q) y
The Server will restart in 10 seconds (Do not close the session)...

Broadcast message from root (pts/0) (Mon Jul 11 20:50:21 2011):

The system is going down for reboot NOW!
[root@EMS-Linux143 ~]#
```

Upon confirmation, the EMS automatically reboots for the changes to take effect.

17.2 Ethernet Interfaces

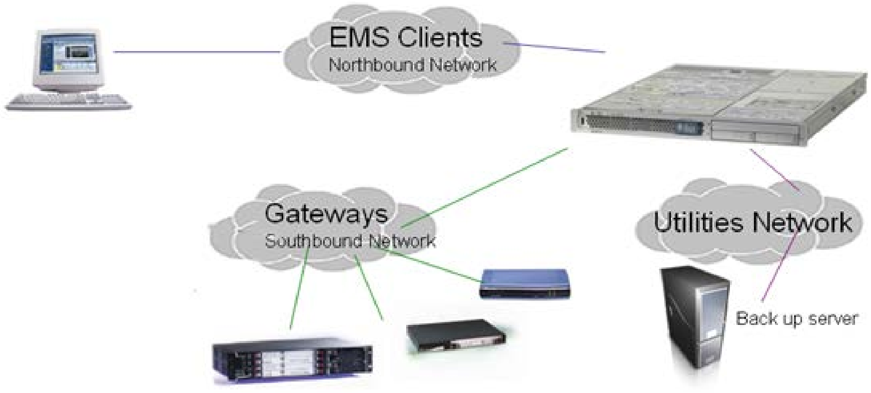
This section describes how to configure Ethernet interfaces.

17.2.1 EMS Client Login on all EMS Server Network Interfaces

The EMS server can be configured with up to four network interfaces (connected to different subnets) as described above. You can connect to any one of the above interfaces directly from the EMS client login dialog.

The “Server IP” field in EMS client login dialog is set to the desired EMS server network interface IP address.

Figure 17-4: EMS Server: Triple Ethernet Interfaces



In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound Network' to each one of the subnets. For Static Routes configuration, see Section 17.6 on page 134.

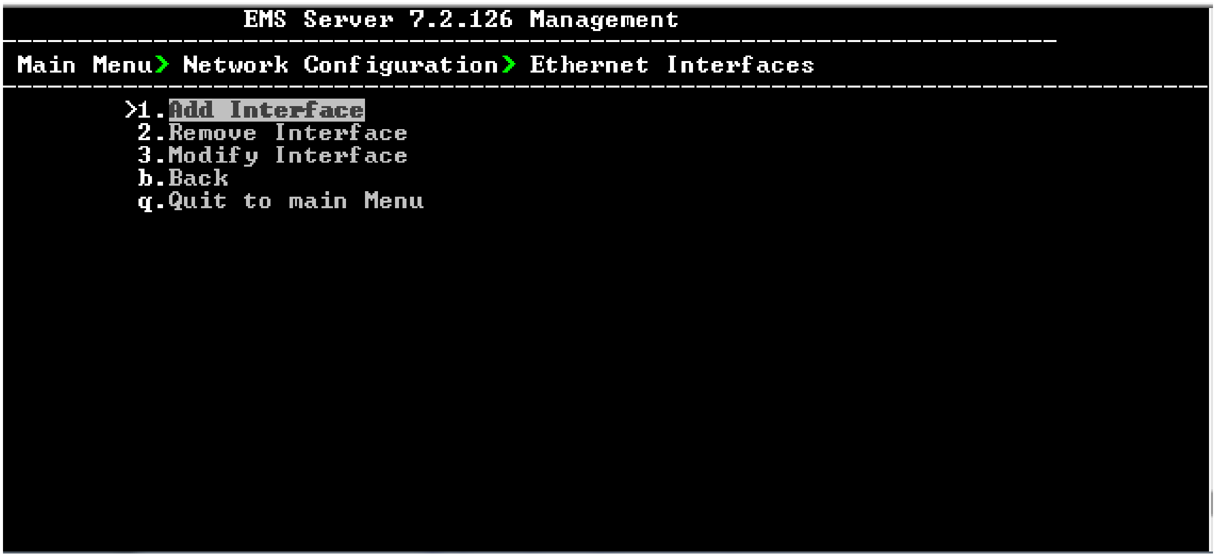
To ensure that the network configuration is performed successfully, test that the EMS is successfully connected to each one of the gateways by running the following basic tests:

- Adding the gateway to the EMS application
- Reviewing its status screen
- Performing basic configuration action (set of ‘MG Location’ in Media Gateways Provisioning Frame / General Setting tab)
- Ensuring that the EMS receives traps from the gateway by adding TP boards in one of the empty slots and ensuring that the ‘Operational Info’ Event is received.

➢ To configure Ethernet Interfaces:

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

Figure 17-5: EMS Server Manager – Configure Ethernet Interfaces



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
Main Menu> Network Configuration> Ethernet Interfaces
--------------------------------------------------------------------------------
        >1.Add Interface
         2.Remove Interface
         3.Modify Interface
         b.Back
         q.Quit to main Menu
```

2. Choose from one of the following options:
   - **Add Interface** – Adds a new interface to the EMS server (see Section 17.2.2 on page 126).
   - **Remove Interface** – Removes an existing interface from the EMS server (see Section 17.2.3 on page 127).
   - **Modify Interface** – Modifies an existing interface from the EMS server (see Chapter 3 on page 127).

17.2.2 Add Interface

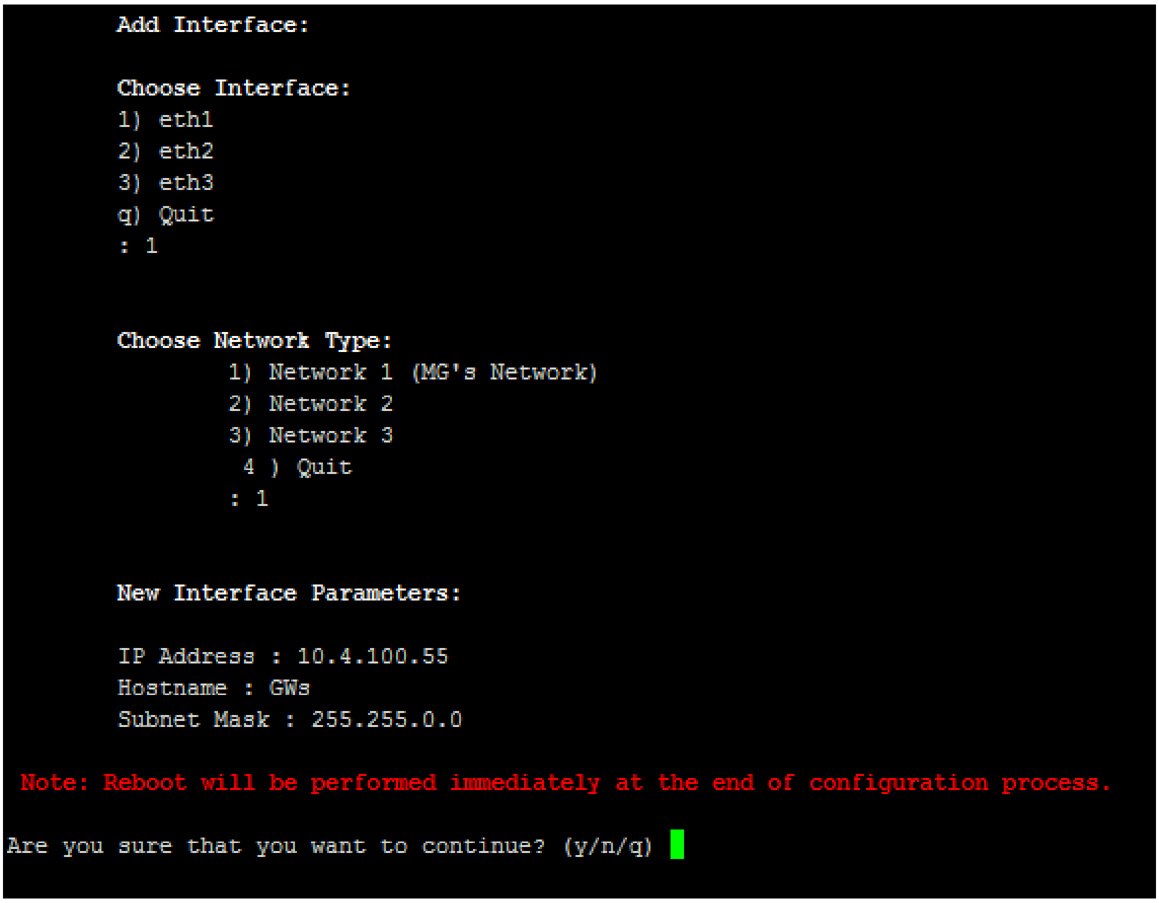
This section describes how to add a new interface.

➢ To add a New Interface:

1. From the Ethernet Interfaces menu, choose option **1**; a list of currently available interfaces (not yet configured) is displayed.
2. Choose an interface (on HP machines the interfaces are called 'eth0', 'eth1', etc).
3. Choose the Network Type.
4. Enter values for the following interface parameters and confirm:
   - IP Address
   - Hostname
   - Subnet Mask

   The new interface parameters are displayed.
5. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

Figure 17-9: Add Interface Parameters



```
        Add Interface:

        Choose Interface:
        1) eth1
        2) eth2
        3) eth3
        q) Quit
        : 1


        Choose Network Type:
                1) Network 1 (MG's Network)
                2) Network 2
                3) Network 3
                 4 ) Quit
                : 1


        New Interface Parameters:

        IP Address : 10.4.100.55
        Hostname : GWs
        Subnet Mask : 255.255.0.0

 Note: Reboot will be performed immediately at the end of configuration process.

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

17.2.3 Remove Interface

This section describes how to remove an interface.

➢ To remove an existing interface:

1. From the Ethernet Interfaces menu, choose option **2**; the following is displayed:
2. Choose the interface to remove.
3. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

17.2.4 Modify Interface

This section describes how to modify an existing interface.

➢ To modify an existing interface:

1. From the Ethernet Interfaces menu, choose option **3**.
2. Choose the interface to modify; the following is displayed:
3. Change the interface parameters.
4. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

17.3 Ethernet Redundancy

This section describes how to configure Ethernet Redundancy.

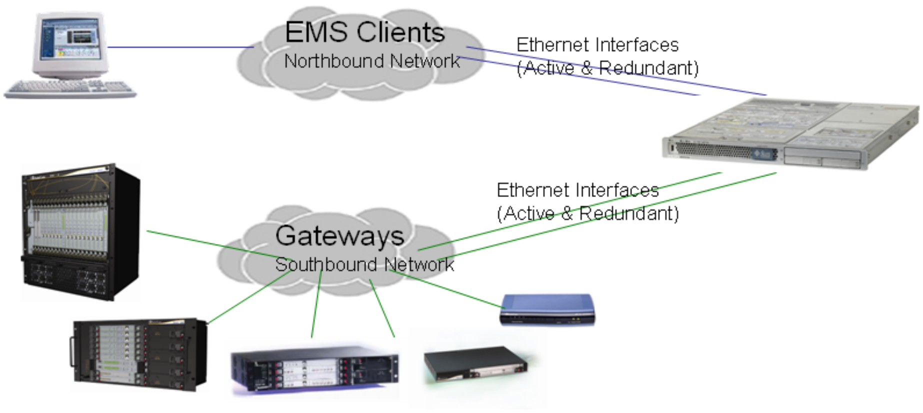
Physical Ethernet Interfaces Redundancy provides failover when you have multiple network interface cards that are connected to the same IP link.

The EMS server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, EMS Clients [Northbound] and Gateways [Southbound]).

This option enables you to configure Ethernet ports redundancy.

Note: When the operation is finished, the EMS server automatically reboots for the changes to take effect.

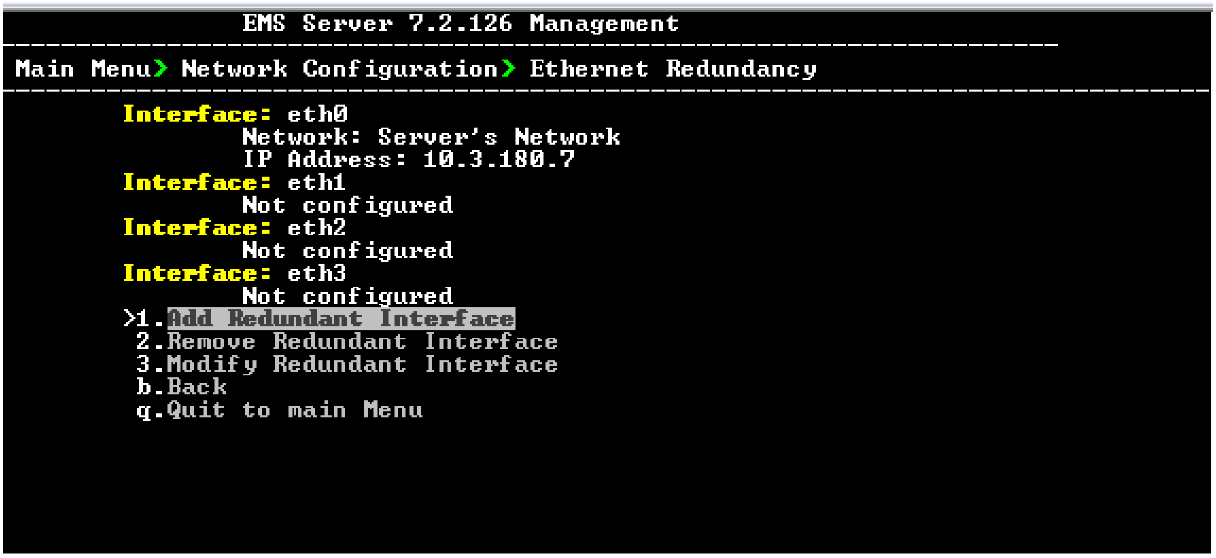
Figure 17-6: Physical Ethernet Interfaces Redundancy



➢ To configure Ethernet Redundancy:

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

Figure 17-7: Ethernet Redundancy Configuration



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Network Configuration> Ethernet Redundancy
--------------------------------------------------------------------------------
        Interface: eth0
                Network: Server's Network
                IP Address: 10.3.180.7
        Interface: eth1
                Not configured
        Interface: eth2
                Not configured
        Interface: eth3
                Not configured
        >1.Add Redundant Interface
         2.Remove Redundant Interface
         3.Modify Redundant Interface
         b.Back
         q.Quit to main Menu
```

2. This menu includes the following options:

   - Add Redundant Interface (see Section 17.3.1 on page 129.
   - Remove Redundant Interface (see Section 17.3.2 on page 131).
   - Modify Redundant Interface (see Section 17.3.3 on page 132).

17.3.1 Add Redundant Interface

Remove a redundant interface under the following circumstances:

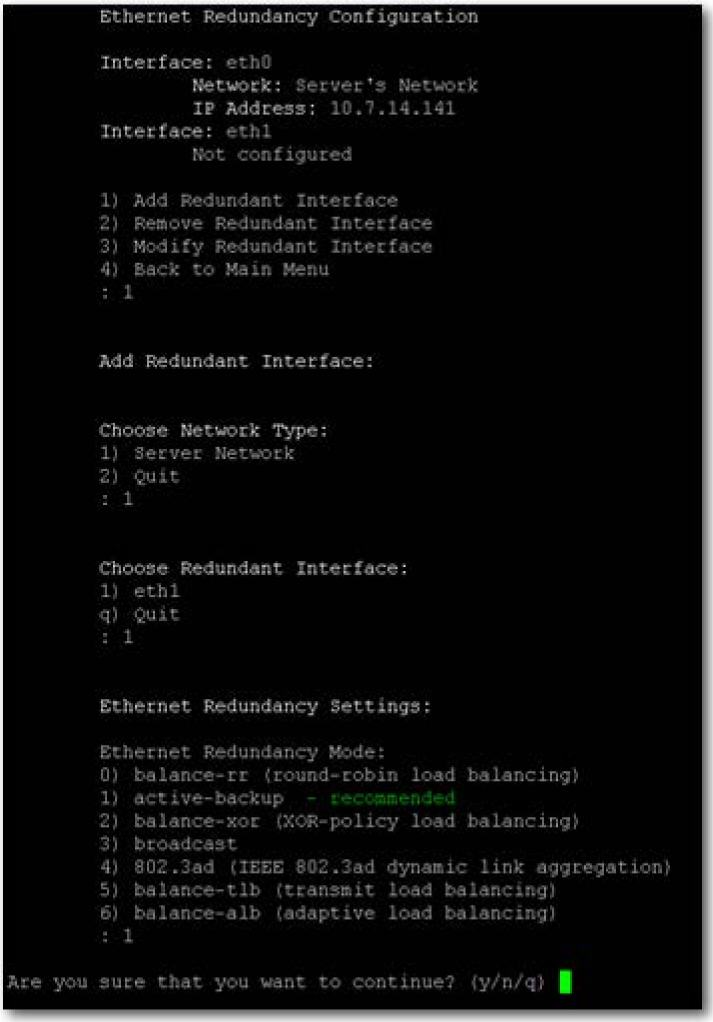
- You have configured an Ethernet interface (see Section 17.3.1).
- Your default router can respond to a ‘ping’ command, due to a heartbeat procedure between interfaces and the default router (to verify activity).

➢ To add a redundant interface:

1. From the Ethernet Redundancy menu, choose option **1**.
2. Choose the network type for which to create a new redundant interface (for example, 'EMS Client-Server Network').
3. Choose the interface in the selected network that you wish to make redundant (for example, 'bge1', 'bge2', 'bge3').
4. Choose the redundancy mode (for example, 'balance-rr', 'active-backup').

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

Figure 17-8: Add Redundant Interface (Linux)



```
        Ethernet Redundancy Configuration

        Interface: eth0
                Network: Server's Network
                IP Address: 10.7.14.141
        Interface: eth1
                Not configured

        1) Add Redundant Interface
        2) Remove Redundant Interface
        3) Modify Redundant Interface
        4) Back to Main Menu
        : 1


        Add Redundant Interface:


        Choose Network Type:
        1) Server Network
        2) Quit
        : 1


        Choose Redundant Interface:
        1) eth1
        q) Quit
        : 1


        Ethernet Redundancy Settings:

        Ethernet Redundancy Mode:
        0) balance-rr (round-robin load balancing)
        1) active-backup  - recommended
        2) balance-xor (XOR-policy load balancing)
        3) broadcast
        4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
        5) balance-tlb (transmit load balancing)
        6) balance-alb (adaptive load balancing)
        : 1

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

17.3.2 Remove Ethernet Redundancy

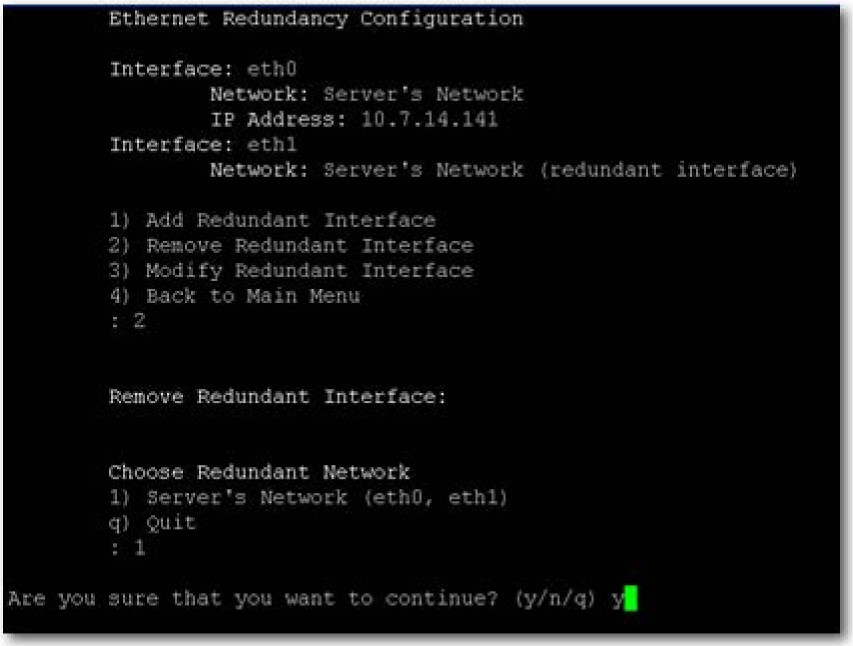
This section describes how to remove an Ethernet redundancy interface.

➢ To remove the Ethernet Redundancy interface:

1. From the Ethernet Redundancy menu, choose option **2**.
2. Choose the network redundancy to remove.

   The current Ethernet redundancy configuration is displayed.
3. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

Figure 17-9: Ethernet Redundancy Interface to Disable



```
        Ethernet Redundancy Configuration

        Interface: eth0
                Network: Server's Network
                IP Address: 10.7.14.141
        Interface: eth1
                Network: Server's Network (redundant interface)

        1) Add Redundant Interface
        2) Remove Redundant Interface
        3) Modify Redundant Interface
        4) Back to Main Menu
        : 2


        Remove Redundant Interface:


        Choose Redundant Network
        1) Server's Network (eth0, eth1)
        q) Quit
        : 1

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

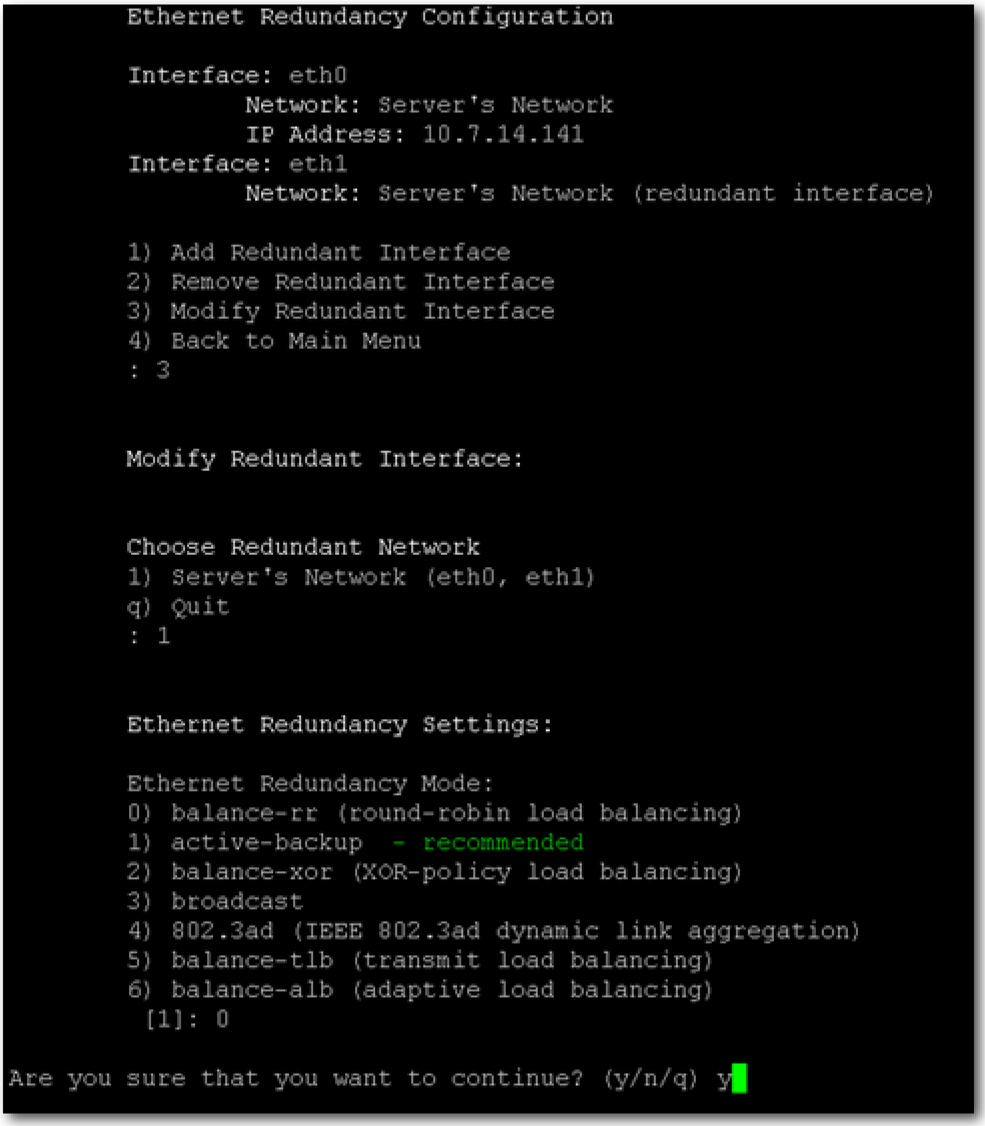
17.3.3 Modify Redundant Interface

This section describes how to modify a redundant interface.

➢ To modify redundant interface and change redundancy settings:

1. From the Ethernet Redundancy, choose option **3**.
2. Choose the Ethernet redundancy interface to modify.
3. Change the redundancy settings.
4. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

Figure 17-10: Modify Redundant Interface (Linux)



```
        Ethernet Redundancy Configuration

        Interface: eth0
                Network: Server's Network
                IP Address: 10.7.14.141
        Interface: eth1
                Network: Server's Network (redundant interface)

        1) Add Redundant Interface
        2) Remove Redundant Interface
        3) Modify Redundant Interface
        4) Back to Main Menu
        : 3


        Modify Redundant Interface:


        Choose Redundant Network
        1) Server's Network (eth0, eth1)
        q) Quit
        : 1


        Ethernet Redundancy Settings:

        Ethernet Redundancy Mode:
        0) balance-rr (round-robin load balancing)
        1) active-backup  - recommended
        2) balance-xor (XOR-policy load balancing)
        3) broadcast
        4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
        5) balance-tlb (transmit load balancing)
        6) balance-alb (adaptive load balancing)
         [1]: 0

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

17.4 DNS Client

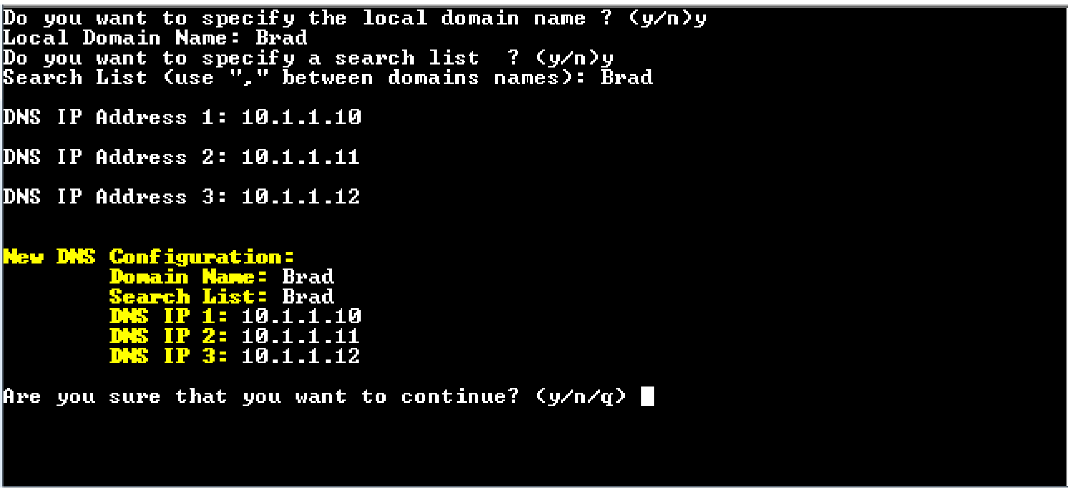
Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

This option enables you to configure the client side (Resolver). If there is no existing DNS configuration, the option **Configure DNS** is displayed. If already configured, the option **Modify DNS** is displayed.

➢ To Configure the DNS Client:

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

Figure 17-11: DNS Setup



```
Do you want to specify the local domain name ? (y/n)y
Local Domain Name: Brad
Do you want to specify a search list  ? (y/n)y
Search List (use "," between domains names): Brad

DNS IP Address 1: 10.1.1.10

DNS IP Address 2: 10.1.1.11

DNS IP Address 3: 10.1.1.12


New DNS Configuration:
        Domain Name: Brad
        Search List: Brad
        DNS IP 1: 10.1.1.10
        DNS IP 2: 10.1.1.11
        DNS IP 3: 10.1.1.12

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

2. Specify the location domain. Type **y** to specify the local domain name or type **n**, and then press Enter.
3. Specify a search list; type **y** to specify a list of domains (use a comma delimiter to separate search entries in the list) or type **n**, and then press Enter.
4. Specify DNS IP addresses **1, 2** and **3**.
5. Type **y** to confirm your configuration; the new configuration is displayed.

17.5 NAT

NAT is the process of modifying network address information in datagram packet headers traversing a traffic routing device for the purpose of remapping a given address space to another.

➢ To configure NAT:

1. From the Network Configuration menu, choose **NAT**, and then press Enter.
2. Enable a NAT address; type **y**.
3. Enter the NAT address, and then press Enter.
4. Type **y** to confirm the changes.
5. Stop and start the EMS server for the changes to take effect.

➢ To remove NAT configuration:

1. Enter the value **-1**.
2. Type **y** to confirm the changes.
3. Stop and start the EMS server for the changes to take effect.

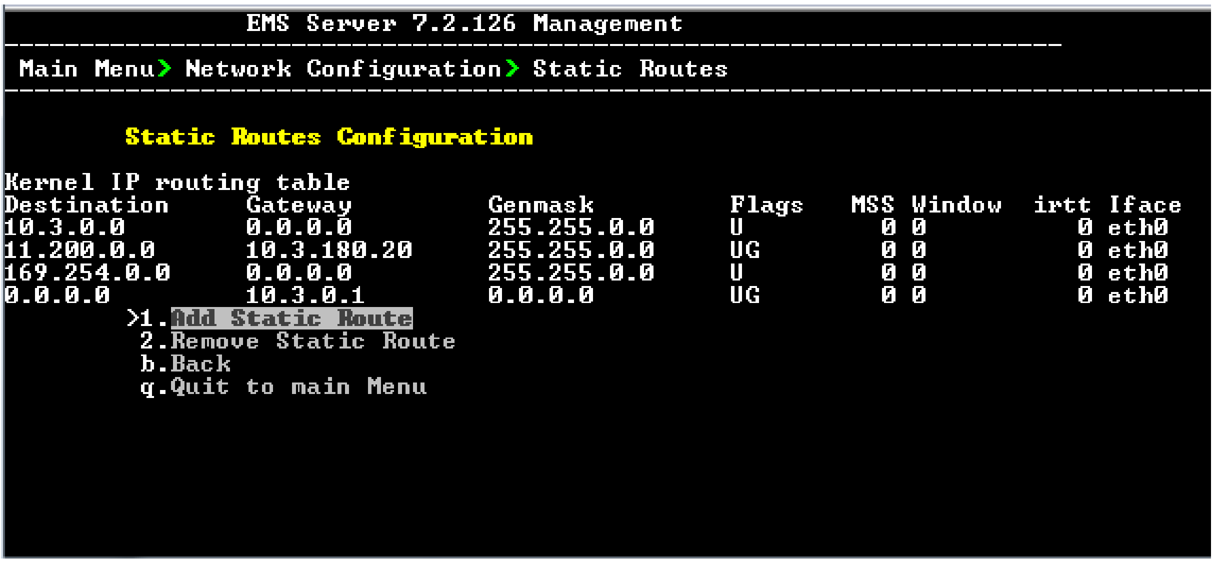
17.6 Static Routes

This option enables you to add or remove static route rules. Static routes are usually only used in conjunction with /etc/defaultrouter. Static routes may be required for network topology, where you don’t want to traverse your default Gateway/Router. In this case, you will probably wish to make the routes permanent by adding the static routing rules.

➢ To configure static routes:

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

Figure 17-12: Routing Table and Menu



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Network Configuration> Static Routes
--------------------------------------------------------------------------------

        Static Routes Configuration

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.3.0.0        0.0.0.0         255.255.0.0     U         0 0          0 eth0
11.200.0.0      10.3.180.20     255.255.0.0     UG        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         10.3.0.1        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. From the Static Routes configuration screen, choose one of the following options:
   - Add a Static Route
   - Remove a Static Route

➢ To add a static route:

1. From the Static Routes menu, choose option **1**.
2. Enter the Destination Network Address.
3. Enter the router's IP address.
4. Type **y** to confirm the changes.

➢ To remove a static route:

1. From the Static Routes menu, choose option **2**.
2. Enter the Destination Network Address for the static route you wish to remove.
3. Enter the router's IP address.
4. Type **y** to confirm the changes.

17.7 SNMP Agent

The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP).

This option enables you to configure the SNMP agent on the EMS server and determines whether or not to forward system alarms from the EMS server to the NMS.

➢ To configure SNMP Agent:

1. From the Network Configuration menu, choose **SNMP Agent**, and then press Enter.
2. Enter the NMS IP.
3. Enter the Community string.

   The new configuration is applied.

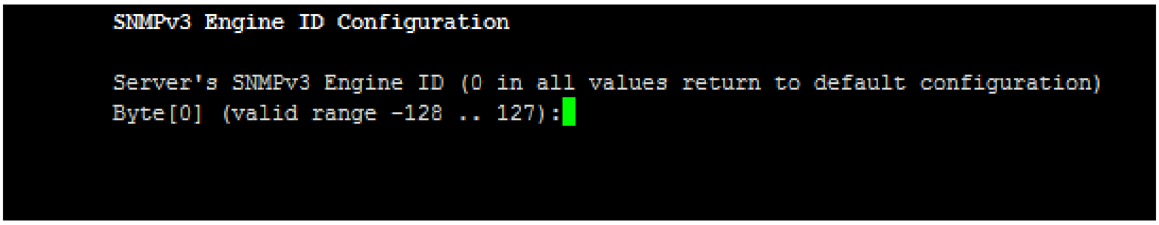
17.8 Server SNMPv3 Engine ID

The EMS server Engine ID is used by the SNMPv3 protocol when alarms are forwarded from the EMS to an NMS. By default, the EMS server SNMPv3 Engine ID is automatically created from the EMS server IP address. This option enables the user to customize the EMS server Engine ID according to their NMS configuration.

➢ To configure the SNMPv3 Engine ID:

1. From the Network Configuration menu, choose **SNMPv3 Engine ID**, and then press Enter; the following is displayed:

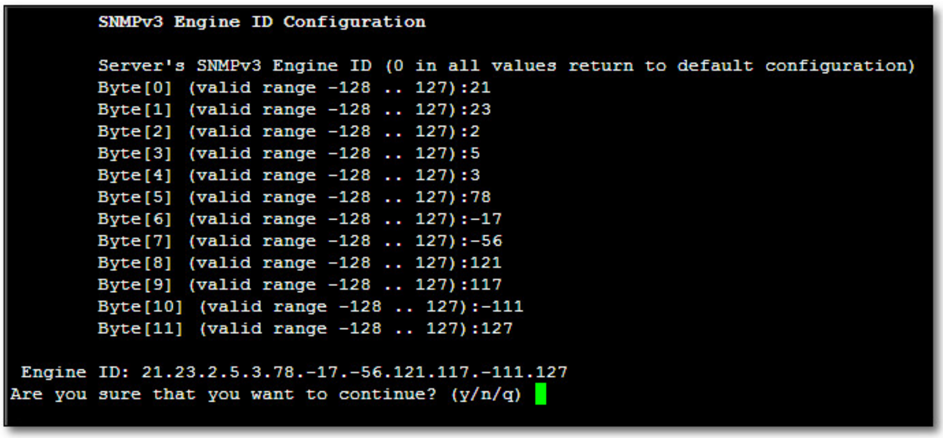
Figure 17-13: EMS Server Manager – Configure SNMPv3 Engine ID



```
        SNMPv3 Engine ID Configuration

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

2. Enter '12' separate bytes ranges of the Engine ID (each valid range from between -128 to 127). In each case, press Enter to confirm the current value insertion and then proceed to the next one.
3. When all Engine ID bytes are provided, type **y** to confirm the configuration. To return to the root menu of the EMS Server Manager, press **q**.

Figure 17-14: SNMPv3 Engine ID Configuration – Complete Configuration



```
        SNMPv3 Engine ID Configuration

        Server's SNMPv3 Engine ID (0 in all values return to default configuration)
        Byte[0] (valid range -128 .. 127):21
        Byte[1] (valid range -128 .. 127):23
        Byte[2] (valid range -128 .. 127):2
        Byte[3] (valid range -128 .. 127):5
        Byte[4] (valid range -128 .. 127):3
        Byte[5] (valid range -128 .. 127):78
        Byte[6] (valid range -128 .. 127):-17
        Byte[7] (valid range -128 .. 127):-56
        Byte[8] (valid range -128 .. 127):121
        Byte[9] (valid range -128 .. 127):117
        Byte[10] (valid range -128 .. 127):-111
        Byte[11] (valid range -128 .. 127):127

 Engine ID: 21.23.2.5.3.78.-17.-56.121.117.-111.127
Are you sure that you want to continue? (y/n/q)
```

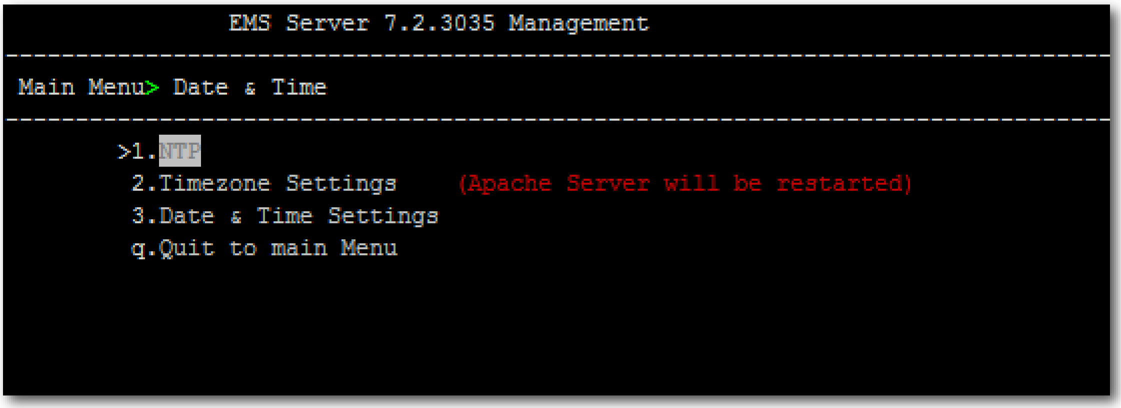
18 Date and Time Settings

This option enables you to change the system time and date.

➢ **To change system time and date:**

- From the EMS Server Management root menu, choose **Date & Time**, and then press Enter; the following is displayed:

Figure 18-1: EMS Server Manager - Change System Time & Date



```
                EMS Server 7.2.3035 Management
--------------------------------------------------------------------------------
 Main Menu> Date & Time
--------------------------------------------------------------------------------
        >1.NTP
         2.Timezone Settings     (Apache Server will be restarted)
         3.Date & Time Settings
         q.Quit to main Menu
```

This menu includes the following options:

- NTP
- Timezone Settings
- Date & Time Settings

See Chapter 18 on page 140.

18.1 NTP

Network Time Protocol (NTP) is used to synchronize the time and date of the EMS server (and all its components) with other devices in the IP network.

This option enables you to configure the EMS server to obtain its clock from an external NTP clock source and other devices that are connected to the EMS server in the IP network can synchronize with this clock source. These devices can be any device containing an NTP server or client.

Alternatively, you can configure the NTP server to allow other devices in the IP network to synchronize their clocks according to the EMS server clock.

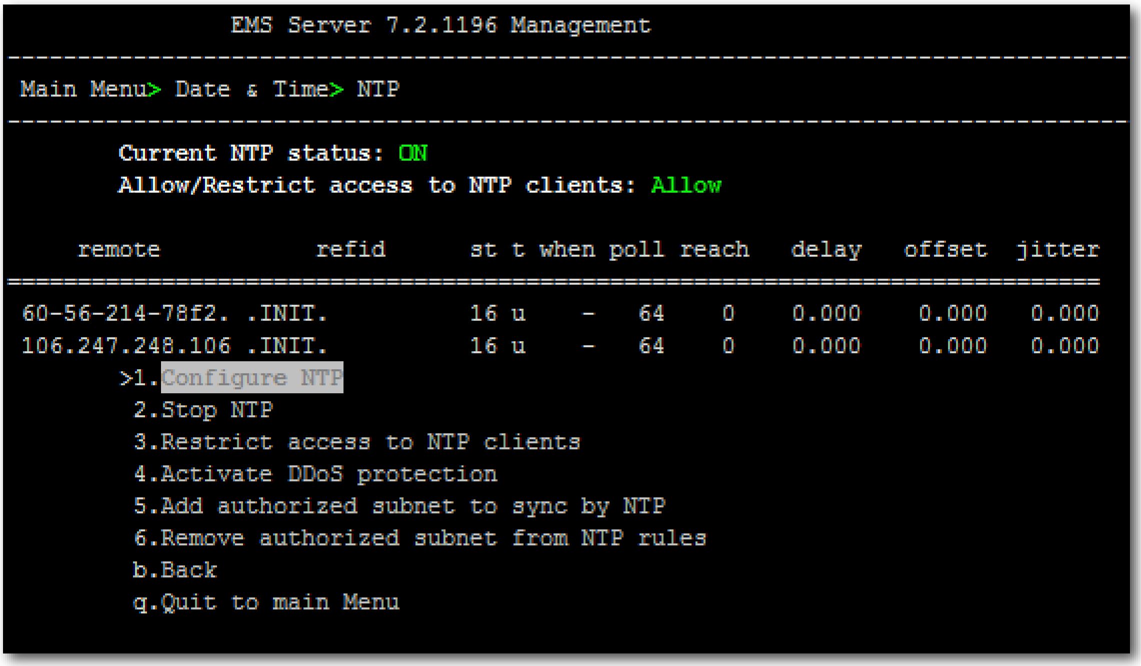
Note:

- It is recommended to configure the EMS server to synchronize with an external clock source because the EMS server clock is less precise than other NTP devices.
- When working with the Session Experience Manager (SEM), you should configure the same NTP server on both the EMS server and the AudioCodes device.
- When connecting the Lync Front-End server to the SEM, ensure that the same NTP server clock is used on both the EMS server and Microsoft Lync server.
- If you configure NTP server on the device, it is recommended to configure the same NTP server settings on the device and the EMS server.

To configure NTP:

1. From the Date & Time menu, choose **NTP**, and then press Enter; the following is displayed:

Figure 18-2: EMS Server Manager - Configure NTP



```
                EMS Server 7.2.1196 Management
--------------------------------------------------------------------------------
 Main Menu> Date & Time> NTP
--------------------------------------------------------------------------------
        Current NTP status: ON
        Allow/Restrict access to NTP clients: Allow

    remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 60-56-214-78f2. .INIT.          16 u    -   64    0    0.000    0.000   0.000
 106.247.248.106 .INIT.          16 u    -   64    0    0.000    0.000   0.000
        >1.Configure NTP
         2.Stop NTP
         3.Restrict access to NTP clients
         4.Activate DDoS protection
         5.Add authorized subnet to sync by NTP
         6.Remove authorized subnet from NTP rules
         b.Back
         q.Quit to main Menu
```

2. From the NTP menu, choose option **1** to configure NTP.
3. At the prompt, do one of the following:
   - Type **y** for the EMS server to act as both the NTP server and NTP client. Enter the IP addresses of the NTP servers to serve as the clock reference source for the NTP client (Up to four NTP servers can be configured).
   - Type **n** for the EMS server to act as the NTP server only. The EMS server is configured as a Stand-alone NTP server. The NTP process daemon starts and the NTP status information is displayed on the screen.

18.1.1 Stopping and Starting the NTP Server

This section describes how to stop and start the NTP server.

➢ **To start NTP services:**

- From the NTP menu, choose option **2**, and then choose one of the following options:
  - If NTP Service is on: **Stop NTP**
  - If NTP Service is off: **Start NTP**

  The NTP daemon process starts; when the process completes, you return to the NTP menu.

18.1.2 Restrict Access to NTP Clients

This section describes how to restrict access to NTP clients.

➢ **To allow access to NTP clients:**

- From the NTP menu, choose option **3** to allow or restrict access to NTP clients; the screen is updated accordingly.

18.2 Timezone Settings

This option enables you to change the timezone of the EMS server.

> **Note:** The Apache server is automatically restarted after the timezone changes are confirmed.

➢ **To change the system timezone:**

1. From the Date & Time menu, choose **Time Zone Settings**, and then press Enter.
2. Enter the required time zone.
3. Type **y** to confirm the changes; the EMS server restarts the Apache server for the changes to take effect.

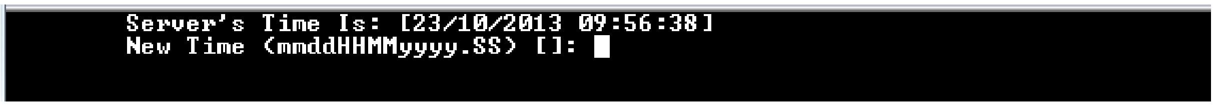
18.3 Date and Time

This option enables you to set the date and time.

➢ To set the date and time:

1. From the Date & Time menu, choose **Date & Time Settings**, and then press Enter; the current server time is displayed:

Figure 18-3: Change System Time and Date Prompt



```
Server's Time Is: [23/10/2013 09:56:38]
New Time (mmddHHMMyyyy.SS) []:
```

2. Enter the new time as shown in the following example:

```
mmddHHMMyyyy.SS :
month(08),day(16),Hour(16),Minute(08),year(2007),”.”
Second.
```

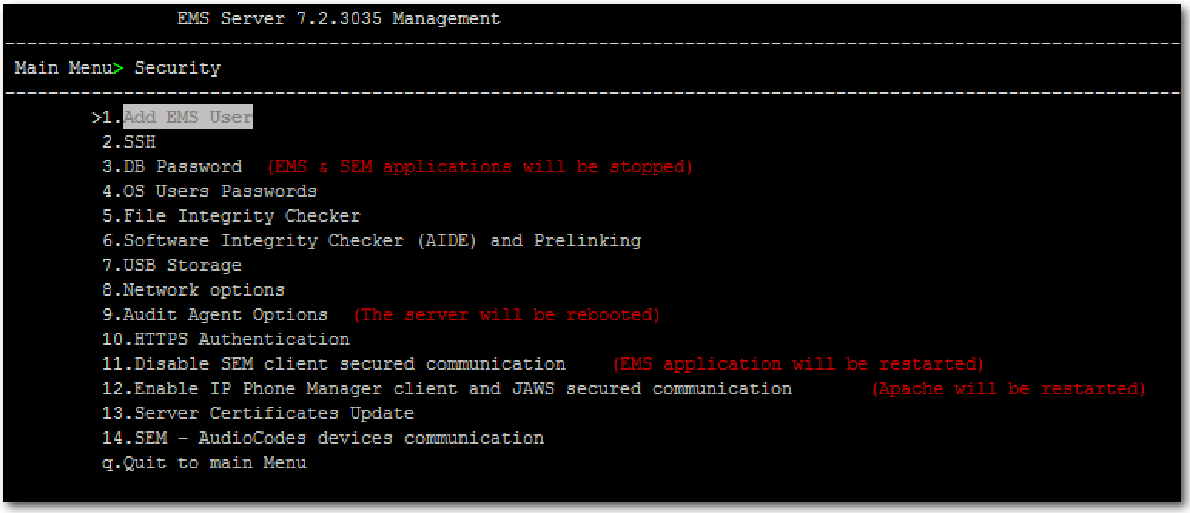
19 Security

The EMS Management security options enable you to perform security actions, such as configuring the SSH Server Configuration Manager, and user's administration.

➢ To configure security settings:

- From the EMS Server Manager root menu, choose **Security**, and then press Enter, the following is displayed:

Figure 19-1: Security Settings



```
                EMS Server 7.2.3035 Management
------------------------------------------------------------------------------------------------------------
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
```

This menu includes the following options:

- Add EMS User (see Section 19.1 on page 142).
- SSH (see Section 19.2 on page 135).
- DB Password (EMS and SEM applications will be stopped) (see Section 19.3 on page 151).
- OS Users Password (see Section 19.4on page 152).
- File Integrity Checker (see Section 19.5 on page 155).
- Software Integrity Checker (AIDE) and Pre-linking (see Section 19.6 on page 155).
- USB Storage (see Section 19.7 on page 156).
- Network options (see Section 19.8 on page 156).
- Audit Agent Options (see Section 19.9 on page 157).
- HTTPS Authentication (see Section 19.10.1 on page 159).
- Enable SEM client secured connection (EMS application will be restarted) (see Section 19.10.2 on page 160).

- Enable IP Phone Manager client and JAWS secured communication (Apache will be restarted) (see Section 19.10.3 on page 160).
- Server Certificates Update (see Section 19.10.4 on page 160)
- SEM-AudioCodes devices communication (see Section 19.10.2 on page 168).

19.1 EMS User

This option enables you to add a new administrator user to the EMS server database. This user can then log into the EMS client. This option is advised to use for the operator's definition only in cases where all the EMS application users are blocked and there is no way to perform an application login.

➢ To add an EMS user:

1. From the Security menu, choose **Add EMS User**, and then press Enter.
2. Enter the name of the user you wish to add.
3. Enter a password for the user.
4. Type **y** to confirm your changes.

Note: Note and retain these passwords for future access.

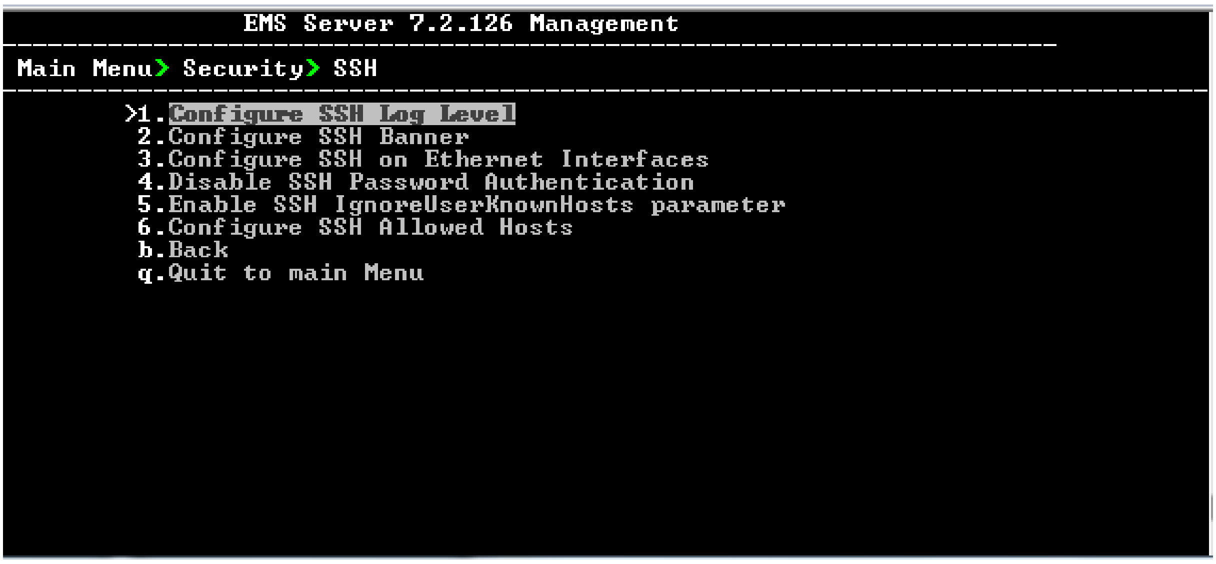
19.2 SSH

This section describes how to configure the EMS server SSH connection properties using the SSH Server Configuration Manager.

➢ To configure SSH:

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

Figure 19-2: SSH Configuration



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
Main Menu> Security> SSH
--------------------------------------------------------------------------------
        >1.Configure SSH Log Level
         2.Configure SSH Banner
         3.Configure SSH on Ethernet Interfaces
         4.Disable SSH Password Authentication
         5.Enable SSH IgnoreUserKnownHosts parameter
         6.Configure SSH Allowed Hosts
         b.Back
         q.Quit to main Menu
```

This menu includes the following options:

- Configure SSH Log Level (see Section 19.2.1 on page 143).
- Configure SSH Banner (see Section 19.2.2 on page 144).
- Configure SSH on Ethernet Interfaces (see Section 19.2.3 on page 145).
- Disable SSH Password Authentication (see Section 19.2.4 on page 147).
- Enable SSH Ignore User Known Hosts Parameter (see Section 19.2.5 on page 147).
- Configure SSH Allowed Hosts (see Section 19.2.6 on page 148).

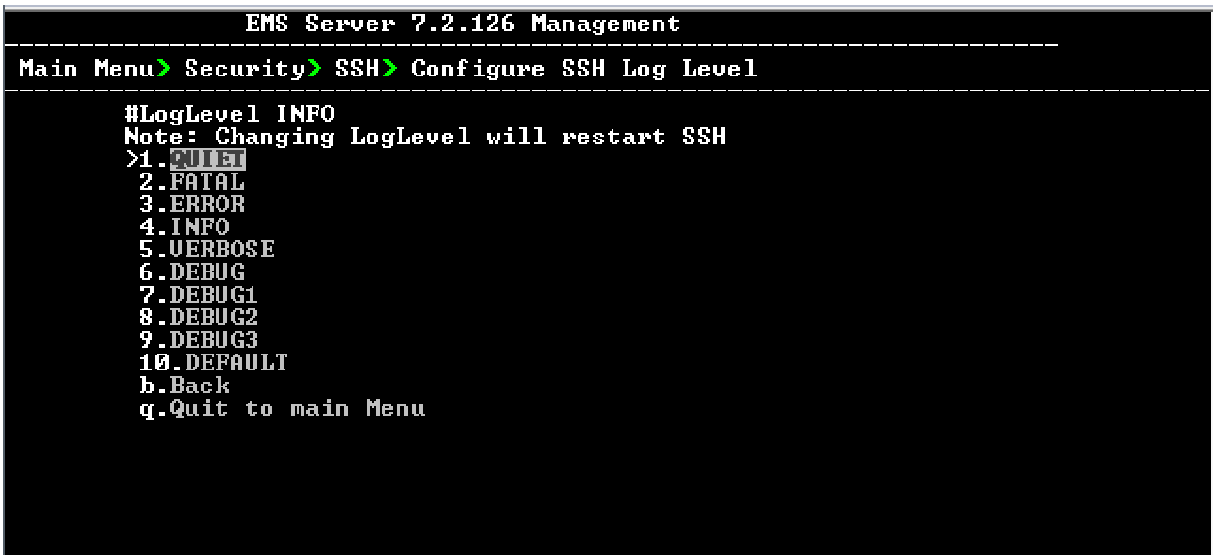
19.2.1 SSH Log Level

You can configure the log level of the SSH daemon server. The log files are found at the location '/var/log/secure' (older records are stored in secure.1, secure.2 etc.).

➢ To configure the SSH Log Level:

1. From the SSH menu, choose option **1**, and then press Enter; the following is displayed:

Figure 19-3: SSH Log Level Manager



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Log Level
--------------------------------------------------------------------------------
        #LogLevel INFO
        Note: Changing LogLevel will restart SSH
        >1.QUIET
         2.FATAL
         3.ERROR
         4.INFO
         5.VERBOSE
         6.DEBUG
         7.DEBUG1
         8.DEBUG2
         9.DEBUG3
         10.DEFAULT
         b.Back
         q.Quit to main Menu
```

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press Enter.

   The SSH daemon restarts automatically.

   The Log Level status is updated on the screen to the configured value.

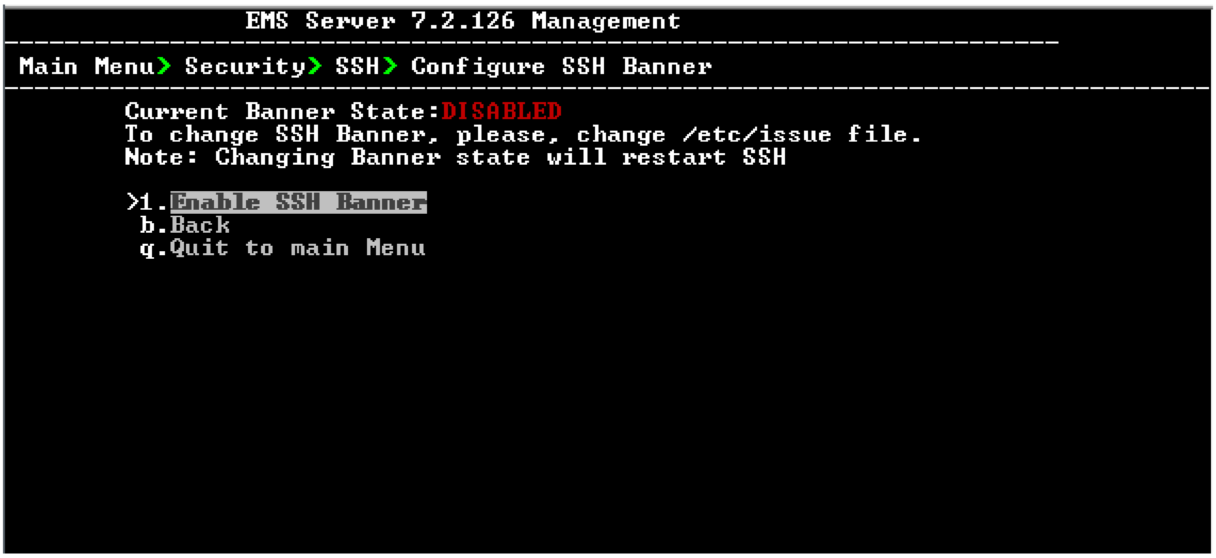
19.2.2 SSH Banner

The SSH Banner displays a pre-defined text message each time the user connects to the EMS server using an SSH connection. You can customize this message. By default this option is disabled.

➢ To configure the SSH banner:

1. From the SSH menu, choose option **2**, and then press Enter; the following is displayed:

Figure 19-4: SSH Banner Manager



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Banner
--------------------------------------------------------------------------------
        Current Banner State:DISABLED
        To change SSH Banner, please, change /etc/issue file.
        Note: Changing Banner state will restart SSH

        >1.Enable SSH Banner
         b.Back
         q.Quit to main Menu
```

2. Edit a '/etc/issue' file with the desired text.
3. Choose option **1** to enable or disable the SSH banner.

   Whenever you change the banner state, SSH is restarted.

   The 'Current Banner State' is displayed in the screen.

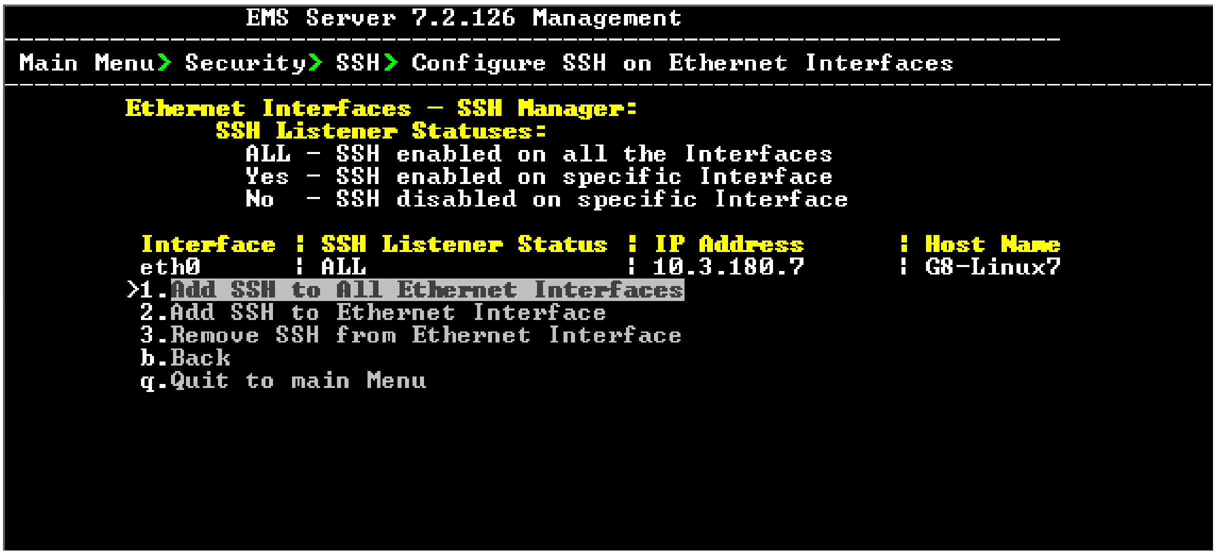
19.2.3 SSH on Ethernet Interfaces

You can allow or deny SSH access separately for each network interface enabled on the EMS server.

➢ To configure SSH on Ethernet interfaces:

- From the SSH menu, choose option **3**, and then press Enter; the following is displayed:

Figure 19-5: Configure SSH on Ethernet Interfaces



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH on Ethernet Interfaces
--------------------------------------------------------------------------------
        Ethernet Interfaces - SSH Manager:
              SSH Listener Statuses:
                ALL - SSH enabled on all the Interfaces
                Yes - SSH enabled on specific Interface
                No  - SSH disabled on specific Interface

         Interface | SSH Listener Status | IP Address       | Host Name
         eth0      | ALL                 | 10.3.180.7       | G8-Linux7
        >1.Add SSH to All Ethernet Interfaces
         2.Add SSH to Ethernet Interface
         3.Remove SSH from Ethernet Interface
         b.Back
         q.Quit to main Menu
```

This menu includes the following options:

- Add SSH to All Ethernet Interfaces (see Section 19.2.3.1 on page 145.
- Add SSH to Ethernet Interface (see Section 19.2.3.2 on page 146).
- Remove SSH from Ethernet Interface (see Section 19.2.3.3 on page 146).

19.2.3.1 Add SSH to All Ethernet Interfaces

This option enables SSH access for all network interfaces currently enabled on the EMS server.

➢ To add SSH to All Ethernet Interfaces:

- From the Configure SSH on Ethernet Interfaces menu, choose option **1**, and then press Enter.

  The SSH daemon restarts automatically to update this configuration action.

  The column 'SSH Listener Status' displays ALL for all interfaces.

19.2.3.2 Add SSH to Ethernet Interface

This option enables you to allow SSH access separately for each network interface.

➢ **To add SSH to Ethernet Interfaces:**

1. From the Configure SSH on Ethernet Interfaces menu, choose option **2**, and then press Enter.

   After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.

2. Enter the appropriate interface number, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

   The column 'SSH Listener Status' displays 'YES' for the configured interface.

19.2.3.3 Remove SSH from Ethernet Interface

This option enables you to deny SSH access separately for each network interface.

➢ **To deny SSH from a specific Ethernet Interface:**

1. From the Configure SSH on Ethernet Interfaces menu, choose option **3**, and then press Enter.

   All the interfaces to which SSH access is currently enabled are displayed.

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

   The SSH daemon restarts automatically to update this configuration action.

   The column 'SSH Listener Status' displays 'No' for the denied interface.

Note: If you attempt to deny SSH access for the only enabled interface, a message is displayed informing you that such an action is not allowed.

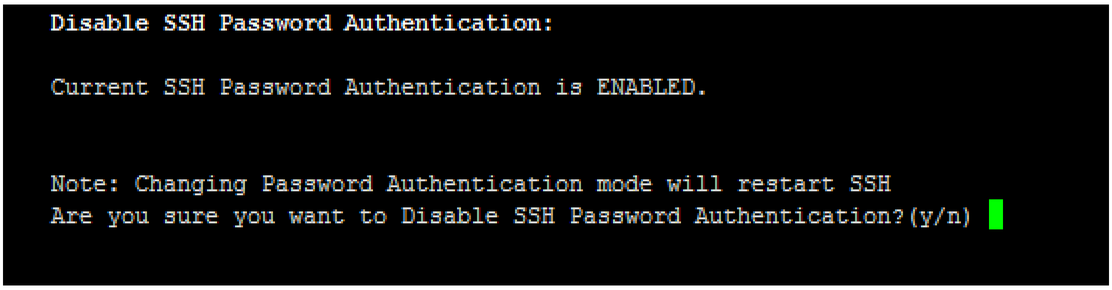
19.2.4 Enable/Disable SSH Password Authentication

This option enables you to disable the username/password authentication method for all network interfaces enabled on the EMS server.

➢ To disable SSH Password Authentication:

1. From the SSH menu, choose option **4**, and then press Enter; the following is displayed:

Figure 19-6: Disable Password Authentication



```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.


Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Disable SSH Password Authentication?(y/n)
```

2. Type **y** to disable SSH password authentication or **n** to enable, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

Note: Once you perform this action, you cannot reconnect to the EMS server using User/Password authentication. Therefore, before you disable this authentication method, ensure that you provision an alternative SSH connection method. For example, using an RSA keys pair. For detailed instructions on how to perform such an action, see www.junauza.com or search the internet for an alternative method.

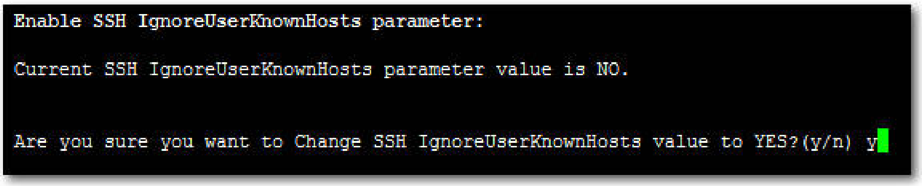
19.2.5 Enable SSH IgnoreUserKnownHosts Parameter

This option enables you to disable the use of the '$HOME/.ssh/known_host' file with stored remote servers fingerprints.

➢ To enable SSH IgnoreUserKnowHosts parameter:

1. From the SSH menu, choose option **5**, and then press Enter; the following is displayed:

Figure 19-7: SSH IgnoreUserKnowHosts Parameter - Confirm



```
Enable SSH IgnoreUserKnownHosts parameter:

Current SSH IgnoreUserKnownHosts parameter value is NO.


Are you sure you want to Change SSH IgnoreUserKnownHosts value to YES?(y/n) y
```

2. Type **y** to change this parameter value to either 'YES' or **'**NO' or type **n** to leave as is, and then press Enter.

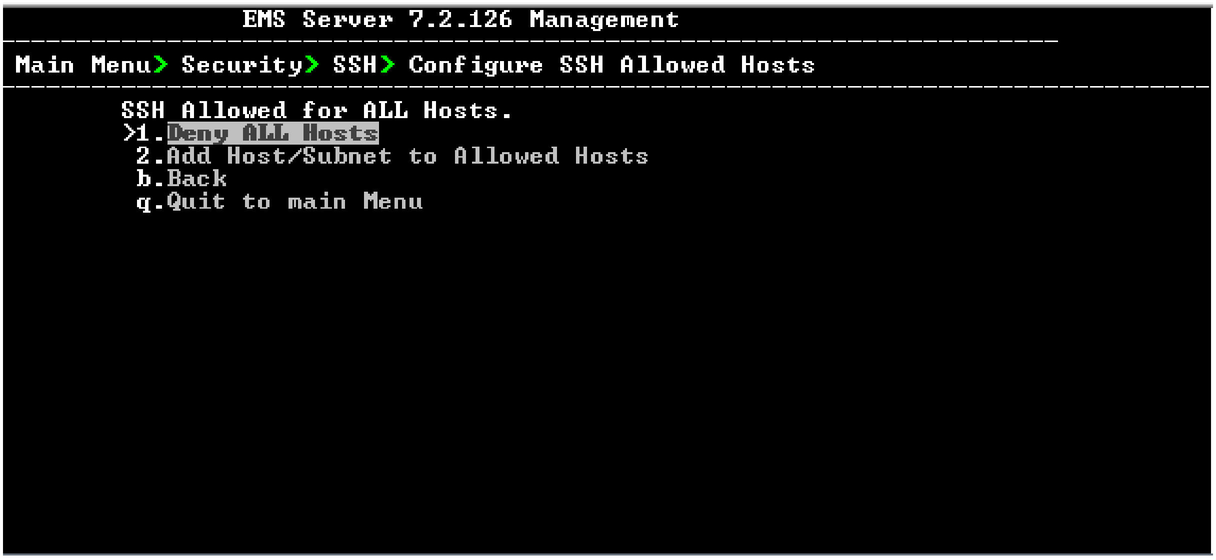
19.2.6 SSH Allowed Hosts

This option enables you to define which hosts are allowed to connect to the EMS server through SSH.

To Configure SSH Allowed Hosts:

- From the SSH menu, choose option **6**, and then press Enter; the following is displayed:

Figure 19-8: Configure SSH Allowed Hosts



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
Main Menu> Security> SSH> Configure SSH Allowed Hosts
----------------------------------------------------------------------------------
       SSH Allowed for ALL Hosts.
       >1.Deny ALL Hosts
        2.Add Host/Subnet to Allowed Hosts
        b.Back
        q.Quit to main Menu
```

This menu includes the following options:

- Allow ALL Hosts (see Section 19.2.6.1 on page 148).
- Deny ALL Hosts (see Section 19.2.6.2 on page 149).
- Add Host/Subnet to Allowed Hosts (see Section 19.2.6.3 on page 149).
- Remove Host/Subnet from Allowed Hosts (see Section 19.2.6.4 on page 150).

19.2.6.1 Allow ALL Hosts

This option enables all remote hosts to access this EMS server through the SSH connection.

To allow ALL Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

   The appropriate status is displayed in the screen.

19.2.6.2 Deny ALL Hosts

This option enables you to deny all remote hosts access to this EMS server through the SSH connection.

➢ **To deny all remote hosts access:**

1. From the Configure SSH Allowed Hosts menu, choose option **2**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

   The appropriate status is displayed in the screen.

> **Note:** When this action is performed, the EMS server is disconnected and you cannot reconnect to the EMS server through SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM connection.

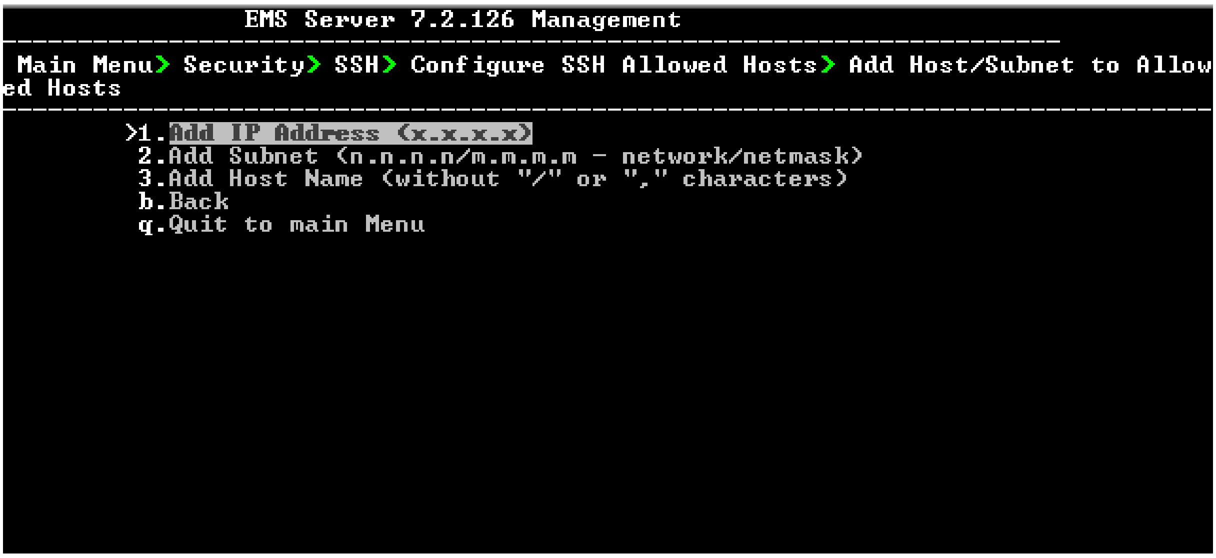
19.2.6.3 Add Hosts to Allowed Hosts

This option enables you to allow different SSH access methods to different remote hosts. You can provide the desired remote host IP, subnet or host name in order to connect to the EMS server through SSH.

➢ **To add Hosts to Allowed Hosts:**

1. From the Configure SSH Allowed Hosts menu, choose option **3**, and then press Enter; the following is displayed:

Figure 19-9: Add Host/Subnet to Allowed Hosts



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allow
ed Hosts
--------------------------------------------------------------------------------
        >1.Add IP Address (x.x.x.x)
         2.Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
         3.Add Host Name (without "/" or "," characters)
         b.Back
         q.Quit to main Menu
```

2. Choose the desired option, and then press Enter.
3. Enter the desired IP address, subnet or host name, and then press Enter.

Note: When adding a Host Name, ensure the following:

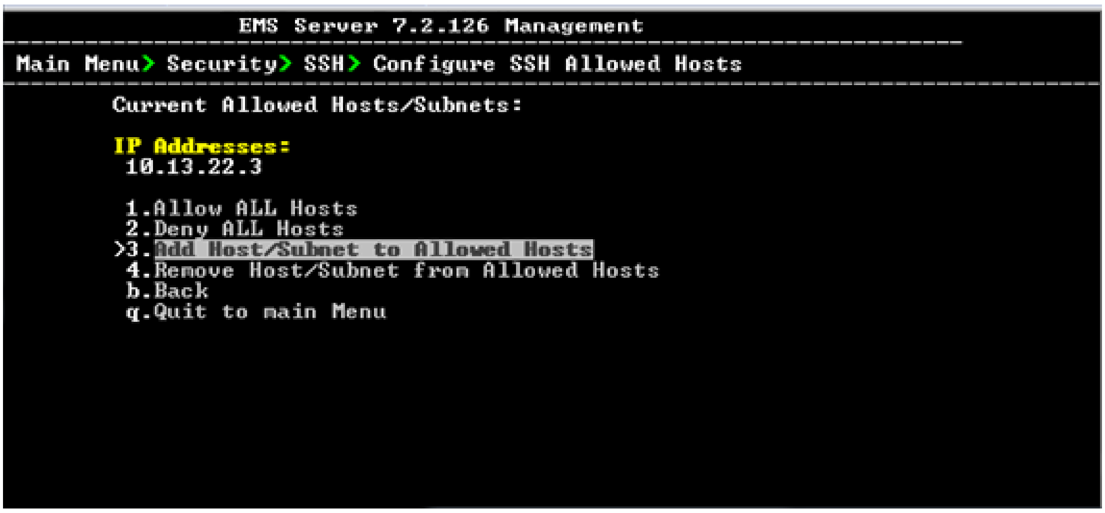
- Verify your remote host name appears in the DNS server database and your EMS server has an access to the DNS server.
- Provide the host name of the desired network interface defined in “/etc/hosts” file.

4. Type **y** to confirm the entry, and then press Enter again.

   If the entry is already included in the list of allowed hosts, an appropriate notification is displayed.

   When the allowed hosts entry has been successfully added, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:

Figure 19-10: Add Host/Subnet to Allowed Hosts-Configured Host



```
                  EMS Server 7.2.126 Management
------------------------------------------------------------------------
Main Menu> Security> SSH> Configure SSH Allowed Hosts
------------------------------------------------------------------------
        Current Allowed Hosts/Subnets:

        IP Addresses:
         10.13.22.3

         1.Allow ALL Hosts
         2.Deny ALL Hosts
        >3.Add Host/Subnet to Allowed Hosts
         4.Remove Host/Subnet from Allowed Hosts
         b.Back
         q.Quit to main Menu
```

19.2.6.4 Remove Host/Subnet from Allowed Hosts

If you have already configured a list of allowed hosts IP addresses, you can then remove one or more of these host addresses from the list.

➢ **To remove an existing allowed host's IP address:**

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter; the following is displayed:
2. Choose the desired entry to remove from the Allowed Hosts list, i.e. to deny access to the EMS server through SSH connection, and then press Enter again.
3. Type **y** to confirm the entry, and then press Enter again.

   When the allowed hosts entry has been successfully removed, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:

> **Note:** When you remove either the only existing IP address, Subnet or Host Name in the Allowed Hosts in the Allowed Hosts list, there are no remote hosts with access (i.e. for each respective option) to connect to the EMS server using SSH. When this action is performed, you are disconnected from the EMS server and may not be able to reconnect through SSH. Therefore, prior to disabling SSH access, ensure that alternative connection methods have been provisioned, for example, serial management connection or KVM connection.

19.3 DB Password

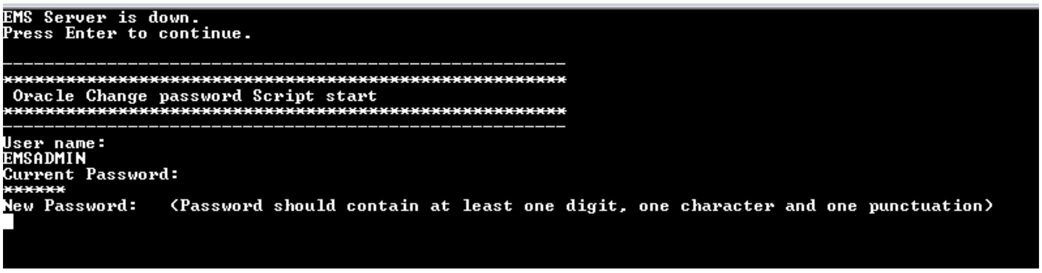
This option enables you to change the default Oracle Database password "pass_1234". The EMS server shuts down automatically before changing the Oracle Database password.

➢ To change the DB Password:

1. From the Security menu, choose **DB Password,** and then press Enter; the EMS server is rebooted.

2. Press Enter until the New Password prompt is displayed.

Figure 19-11: EMS Server Manager – Change DB Password



```
EMS Server is down.
Press Enter to continue.

------------------------------------------------------
******************************************************
 Oracle Change password Script start
******************************************************
------------------------------------------------------
User name:
EMSADMIN
Current Password:
******
New Password:   (Password should contain at least one digit, one character and one punctuation)
```

3. Enter the new password, which should contain at least one digit, one character and one punctuation.

> **Note:**
>
> - The EMS server is rebooted when you change the Oracle Database password.
> - Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the EMS Oracle Database without them.

4. After validation, a message is displayed indicating that the password was changed successfully.

19.4 OS Users Passwords

This section describes how to change the OS password settings.

➢ **To change OS passwords:**

1. From the Security menu, choose **OS Users Passwords**, and then press Enter.
2. Proceed to one of the following procedures:
   - General Password Settings (see Section 19.4.1 on page 152.
   - Operating System User Security Extensions (see Section 19.4.2 on page 153).

19.4.1 General Password Settings

This option enables you to change the OS general password settings, such as 'Minimum Acceptable Password Length' and 'Enable User Block on Failed Login'. This feature also enables you to modify settings for a specific user, such as 'User's Password' and 'Password Validity Max Period'.

➢ **To modify general password settings:**

1. The Change General Password Settings prompt is displayed; type **y**, and then press Enter.

```
Do you want to change general password settings? (y/n)y
```

2. The Minimum Acceptable Password Length prompt is displayed; type **10**, and then press Enter.

```
Minimum Acceptable Password Length [10]:  10
```

3. The Enable User Block on Failed Login prompt is displayed; type **y**, and then press Enter.

```
Enable User Block on Failed Login (y/n) [y] y
```

4. The Maximum Login Retries prompt is displayed; type **3**, and then press Enter.

```
Maximum Login Retries [3]: 3
```

5. The Failed Login Locking Timeout prompt is displayed; type **900**, and then press Enter.

```
Failed Login Locking Timeout [900]:900
```

6. You are prompted if you wish to continue; type **y**, and then press Enter.

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

19.4.2 Operating System Users Security Extensions

This feature enables the administrator to configure the following additional user security extensions:

- Maximum allowed numbers of simultaneous open sessions.
- Inactivity time period (days) before the OS user is locked.

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure in Figure 19-12).

➢ **To configure operating system users security extensions:**

1. The Change General Password Settings prompt is displayed; type **n**, and then press Enter.

```
Do you want to change general password settings ? (y/n) n
```

2. The Change password for a specific user prompt is displayed; type **y**, and then press Enter.

```
Do you want to change password for specific user ? (y/n) y
```

3. Enter the Username upon which you wish to configure, and then press Enter.

```
Enter Username [acems]:
```

4. The change User Password prompt is displayed; type **n**, and then press Enter.

```
Do you want to change its password ?  (y/n) n
```

5. An additional Password prompt is displayed, type **y**, and then press Enter.

```
Do you want to change its login and password properties? (y/n)
y
```

6. The Password Validity prompt is displayed; press Enter.

```
Password Validity Max Period (days) [90]:
```

7. The Password Update prompt is displayed; press Enter.

```
Password Update Min Period (days) [1]:
```

8. The Password Warning prompt is displayed; press Enter.

```
Password Warning Max Period (days) [7]:
```

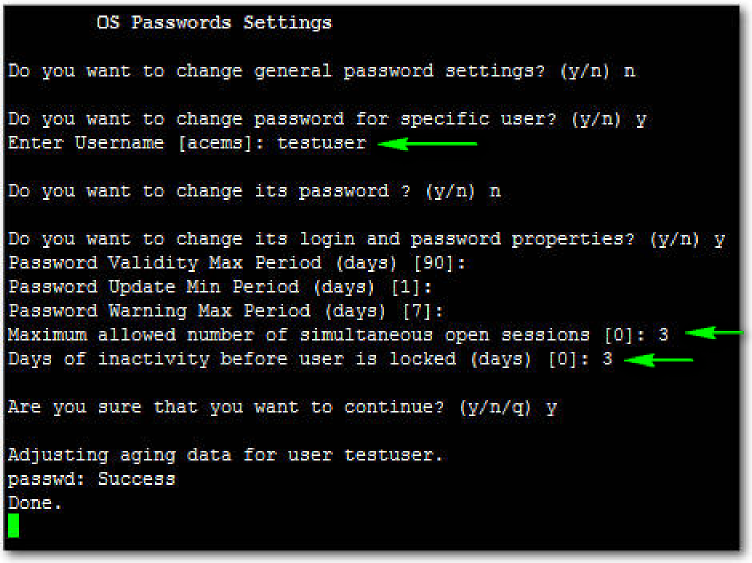
9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user.

```
Maximum allowed number of simultaneous open sessions [0]:
```

10. The Inactivity Days prompt is displayed; enter the number of inactivity days before the user is locked. For example, if you'd like to suspend a specific user if they have not connected to the EMS server for a week, enter 7 days.

```
Days of inactivity before user is locked (days) [0]:
```

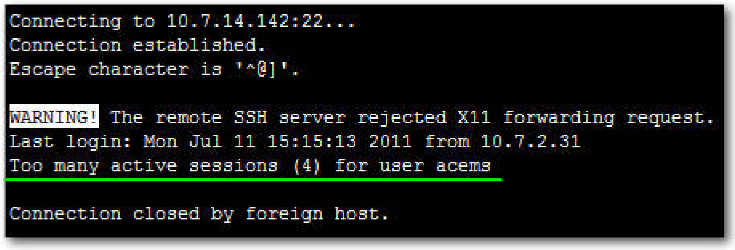
Figure 19-12: OS Passwords Settings with Security Extensions



```
        OS Passwords Settings

Do you want to change general password settings? (y/n) n

Do you want to change password for specific user? (y/n) y
Enter Username [acems]: testuser

Do you want to change its password ? (y/n) n

Do you want to change its login and password properties? (y/n) y
Password Validity Max Period (days) [90]:
Password Update Min Period (days) [1]:
Password Warning Max Period (days) [7]:
Maximum allowed number of simultaneous open sessions [0]: 3
Days of inactivity before user is locked (days) [0]: 3

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

Adjusting aging data for user testuser.
passwd: Success
Done.
```

If the user attempts to open more than three SSH sessions simultaneously, they are prompted and immediately disconnected from the fourth session as displayed in the figure below.

Figure 19-13: Maximum Active SSH Sessions



```
Connecting to 10.7.14.142:22...
Connection established.
Escape character is '^@]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Jul 11 15:15:13 2011 from 10.7.2.31
Too many active sessions (4) for user acems

Connection closed by foreign host.
```

Note: By default you can connect through SSH to the EMS server with user *acems* **only**. If you configure an inactivity days limitation on this user, the situation may arise, for example, where a user is away for an extended period and has no active user to access the EMS server. Therefore, we strongly recommend to use this limitation very carefully and preferably to configure this option for each user to connect to the EMS server through SSH other than with the *acems* user.

19.5 File Integrity Checker

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported through EMS Security Events. The File Integrity checker tool runs on the EMS server machine.

- From the Security menu, choose **File Integrity Checker**, and then press Enter; the File Integrity Checker is started or stopped.

19.6 Software Integrity Checker (AIDE) and Pre-linking

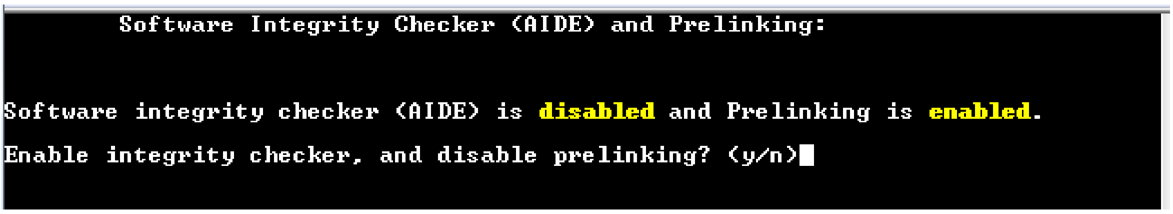
AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

Pre-linking is designed to decrease process startup time by loading each shared library into an address for which the linking of needed symbols has already been performed. After a binary has been pre-linked, the address where the shared libraries are loaded will no longer be random on a per-process basis. This is undesirable because it provides a stable address for an attacker to use during an exploitation attempt.

➢ To start AIDE and disable pre-linking:

1. From the Security menu, choose **Software Integrity Checker (AIDE) and Pre-linking**; the current status of these two processes is displayed:

Figure 19-14: Software Integrity Checker (AIDE) and Pre-linking



```
       Software Integrity Checker (AIDE) and Prelinking:


Software integrity checker (AIDE) is disabled and Prelinking is enabled.

Enable integrity checker, and disable prelinking? (y/n)
```

2. Do one of the following:
   - Type **y** to enable AIDE and disable pre-linking
   - Type **n** to disable AIDE and enable pre-linking.

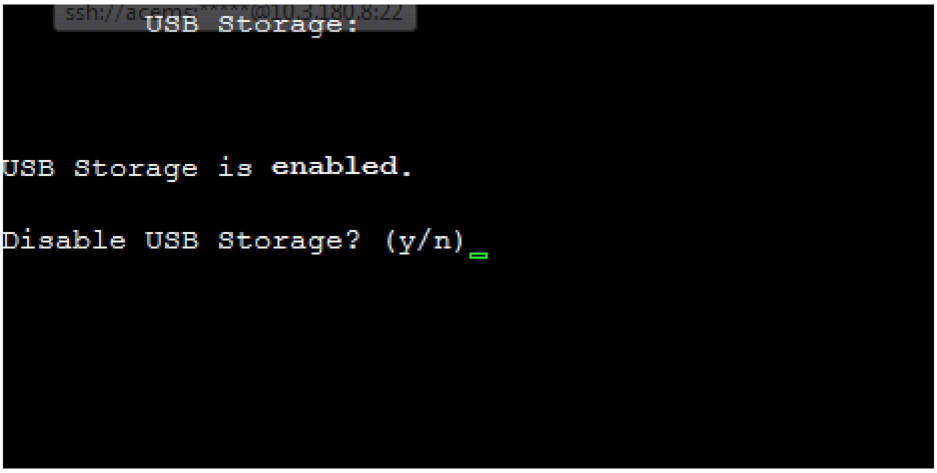
19.7 USB Storage

This menu option allows enabling or disabling the EMS Server's USB storage access as required.

➢ To enable USB storage:

1. From the Security menu, choose **USB Storage**; the following prompt is displayed:

Figure 19-15: USB Storage



```
     USB Storage:


USB Storage is enabled.

Disable USB Storage? (y/n)_
```

2. Enable or disable USB storage as required.

19.8 Network Options

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

- **Ignore Internet Control Message Protocol (ICMP) Echo requests:**

  This option ensures that the EMS server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.

- **Ignore ICMP Echo and Timestamp requests:**

  This option ensures that the EMS server does not respond to an ICMP timestamp request to query for the current time. This reduces exposure to spoofing of the system time.

- **Send ICMP Redirect Messages:**

  This option disables the sending of ICMP Redirect Messages, which are generally sent only by routers.

- **Ignore ICMP Redirect Messages:**

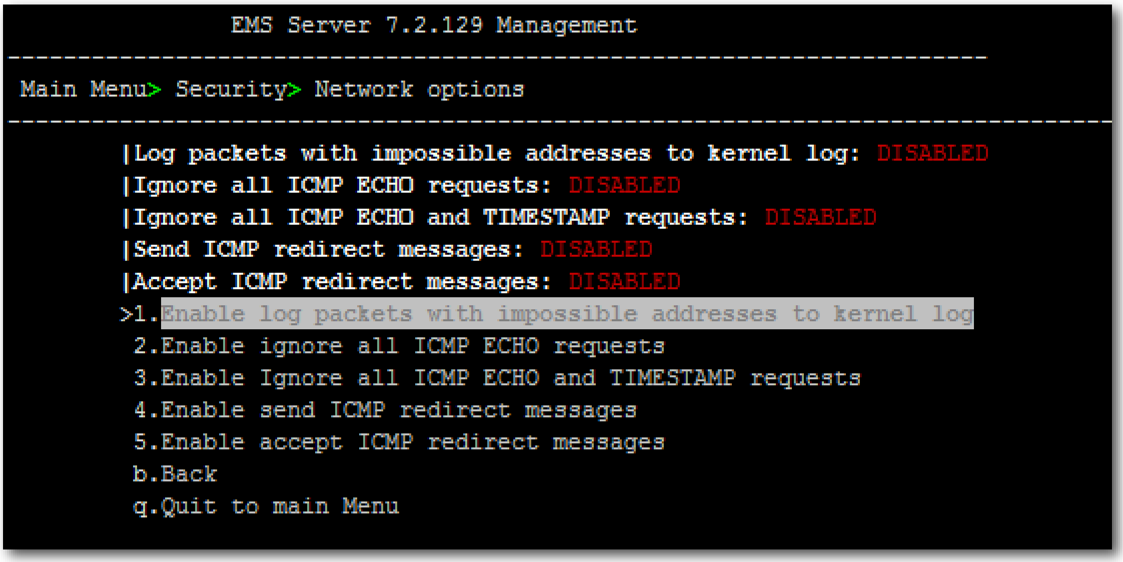
  This option ensures that the EMS server does not respond to ICMP Redirect broadcasts, and therefore such replies are always discarded.

  This prevents an intruder from attempting to redirect traffic from the EMS server to a different gateway or a non-existent gateway.

➢ To enable network options:

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

Figure 19-16: Network Options



```
              EMS Server 7.2.129 Management
-----------------------------------------------------------------------
 Main Menu> Security> Network options
-------------------------------------------------------------------------------
        |Log packets with impossible addresses to kernel log: DISABLED
        |Ignore all ICMP ECHO requests: DISABLED
        |Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
        |Send ICMP redirect messages: DISABLED
        |Accept ICMP redirect messages: DISABLED
        >1.Enable log packets with impossible addresses to kernel log
         2.Enable ignore all ICMP ECHO requests
         3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
         4.Enable send ICMP redirect messages
         5.Enable accept ICMP redirect messages
         b.Back
         q.Quit to main Menu
```

2. Set the required network options.

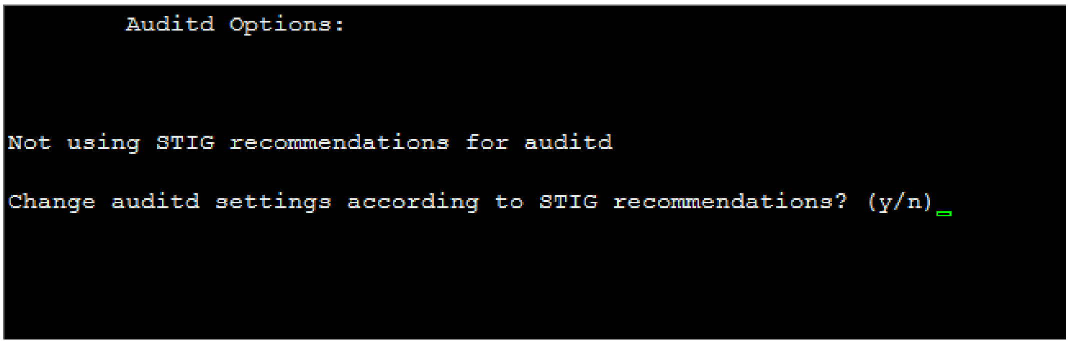
19.9 Auditd Options

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

➢ To set Auditd options according to STIG:

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

Figure 19-17: Auditd Options



```
        Auditd Options:


Not using STIG recommendations for auditd

Change auditd settings according to STIG recommendations? (y/n)_
```

2. Enable or disable Auditd options as required.

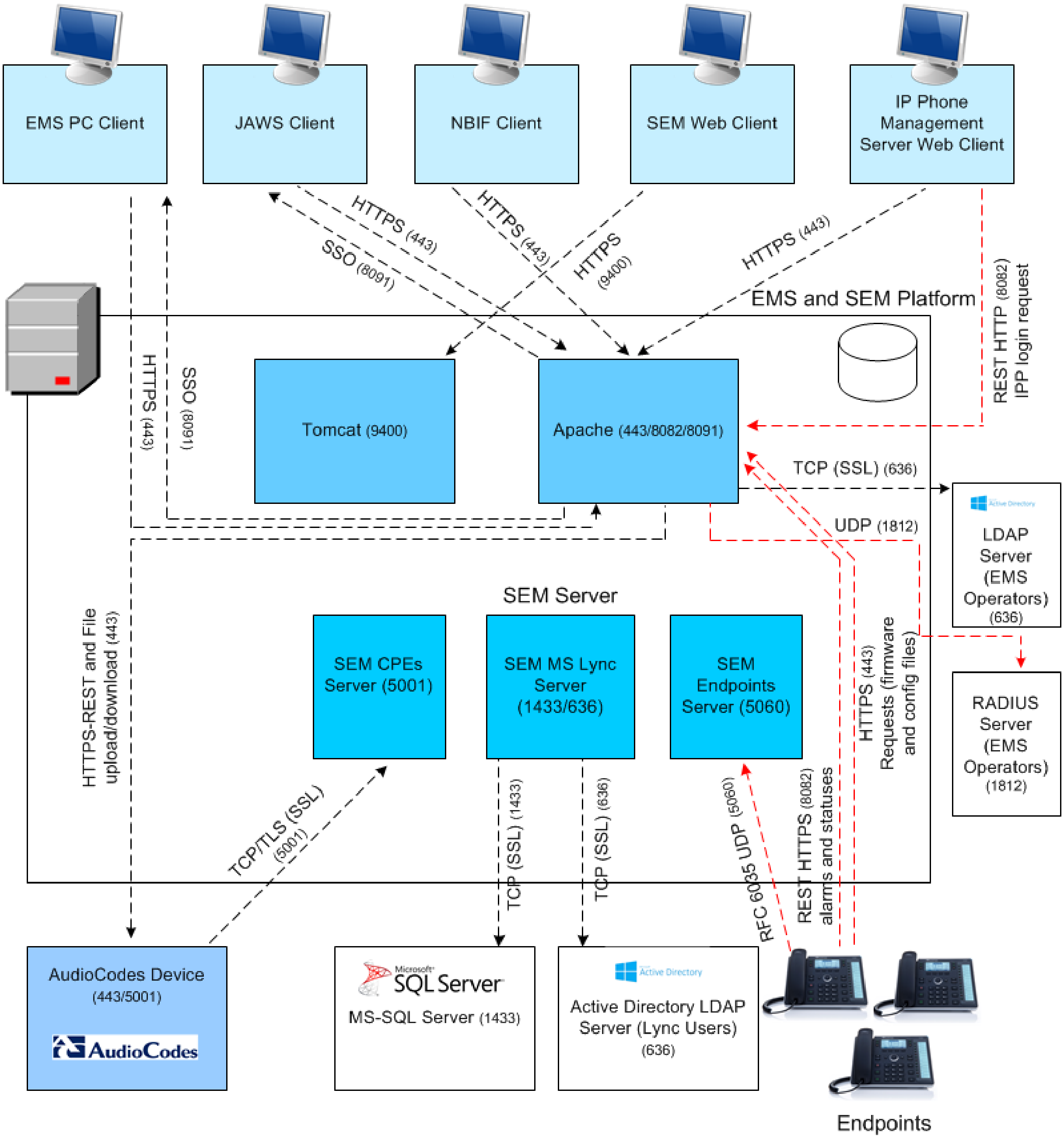
   Audit records are saved in the following /var/log/audit/ directory.

19.10 HTTPS/SSL/TLS Security

This section describes the configuration settings for the HTTPS/SSL/TLS connections.

The figure below shows the maximum security that can be implemented in the OVOC environment. For most connections, the HTTPS/SSL/TLS protocols can be implemented; those connections where these protocols are not supported are indicated in red.

Figure 19-18: OVOC Maximum Security Implementation


EMS PC Client
JAWS Client
NBIF Client
SEM Web Client
IP Phone Management Server Web Client
HTTPS (443)
SSO (8091)
HTTPS (443)
HTTPS (9400)
HTTPS (443)
EMS and SEM Platform
REST HTTP (8082) IPP login request
HTTPS (443)
SSO (8091)
Tomcat (9400)
Apache (443/8082/8091)
TCP (SSL) (636)
UDP (1812)
LDAP Server (EMS Operators) (636)
RADIUS Server (EMS Operators) (1812)
SEM Server
SEM CPEs Server (5001)
SEM MS Lync Server (1433/636)
SEM Endpoints Server (5060)
HTTPS-REST and File upload/download (443)
HTTPS (443) Requests (firmware and config files)
TCP/TLS (SSL) (5001)
TCP (SSL) (1433)
TCP (SSL) (636)
RFC 6035 UDP (5060)
REST HTTPS (8082) alarms and statuses
AudioCodes Device (443/5001)
AudioCodes
SQL Server
MS-SQL Server (1433)
Active Directory
Active Directory LDAP Server (Lync Users) (636)
Endpoints

Note: The above figure shows all the HTTPS/SSL/TLS connections in the OVOC network. Use this figure as an overview to the procedures described below. Note that not all of the connections shown in the above figure have corresponding procedures. For more information, refer to the OVOC Security Guidelines document..

19.10.1 HTTPS Authentication

This option enables you to configure whether certificates are used to authenticate the connection between the EMS server and the devices in one direction or in both directions:

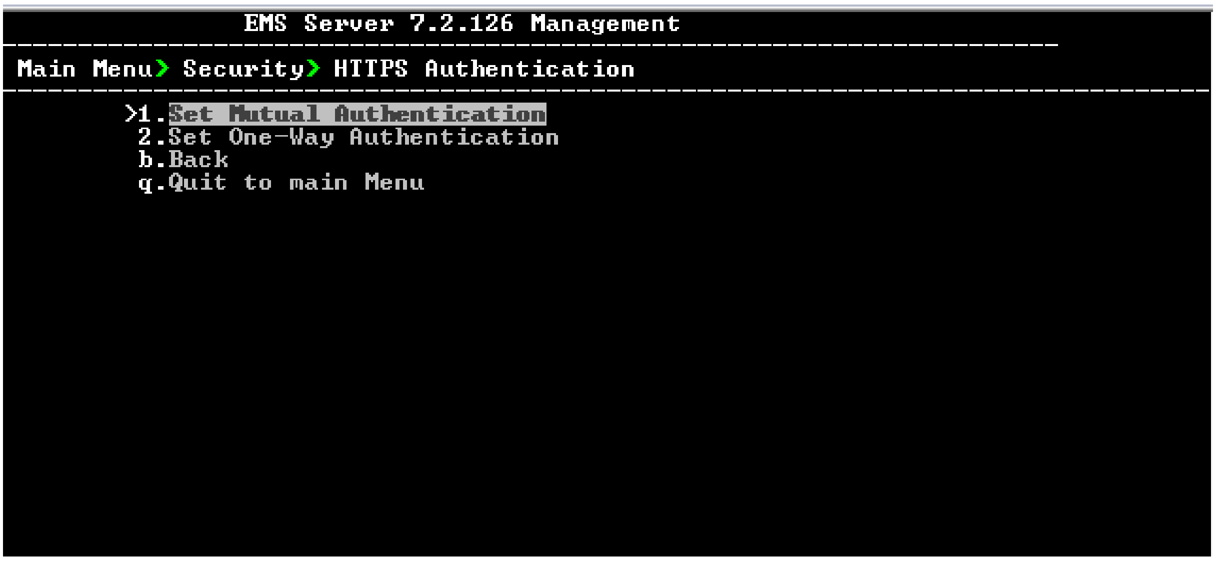
- **Mutual Authentication:** the EMS authenticates the device connection request using certificates and the device authenticates the EMS connection request using certificates. When this option is configured:
  - The same root CA must sign the certificate that is loaded to the device and certificate that is loaded to the EMS server.
  - Mutual authentication must also be enabled on the device (see Section E.5.2.5).
- **One-way Authentication option:** the EMS does not authenticate the device connection request using certificates; only the device authenticates the EMS connection request.

Note: You can use the procedure described in Section 19.10.4 to load the certificate file to the EMS server.

To enable HTTPS authentication:

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

19-19: HTTPS Authentication



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
Main Menu> Security> HTTPS Authentication
--------------------------------------------------------------------------------
        >1.Set Mutual Authentication
         2.Set One-Way Authentication
         b.Back
         q.Quit to main Menu
```

2. Choose one of the following options:
   - 1-Set Mutual Authentication
   - 2. Set One-Way Authentication

19.10.2 Enable SEM Client Secured Connection

This menu option enables you to secure the connection between the SEM client browser and the Tomcat server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 9400 (instead of port 8400-HTTP).

➢ **To enable a secure connection between SEM client browser and Tomcat server:**

- From the Security menu, choose **Enable SEM client secured connection**; the connection is secured.

19.10.3 Enable IP Phone Manager Client JAWS and NBIF Secured Communication

This menu option enables you to secure the connection between the IP Phone Manager client browser, JAWS/NBIF clients and the Apache server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 443 (instead of port 80-HTTP).

➢ **To enable a secure connection between the IP Phone Manager client browser/JAWS and EMS server:**

- From the Security menu, choose **IP Phone Manager client and JAWS secured communication**; the connection is secured.

19.10.4 Server Certificates Update

This menu option enables you to automatically generate custom SSL server certificates.

Note: If you are using self-generated certificates and private key, you can skip to step 4.

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

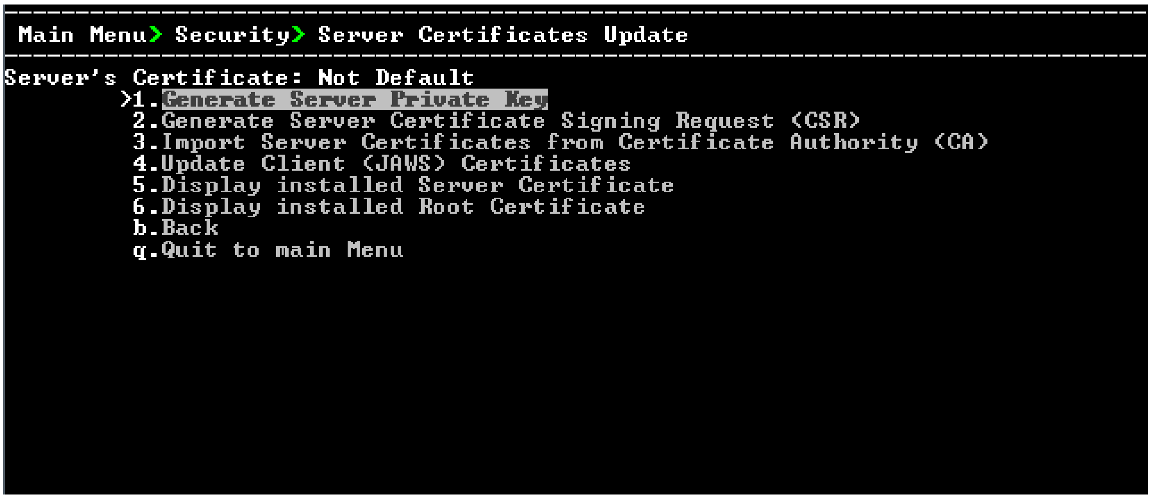
1. **Step 1:** Generate Server Private Key.
2. **Step 2:** Generate Server Certificate Signing Request (CSR).
3. **Step 3:** Transfer the generated CSR file to your PC and send to CA.
4. **Step 4:** Transfer certificates files received from CA back to EMS server.
5. **Step 5:** Import new certificates on EMS server.
6. **Step 6:** Verify the installed Server certificate.
7. **Step 7:** Verify the installed Root certificate.

8. **Step 8:** Update Client Java Web Start certificates (when using non-default certificates, following an upgrade of the EMS server).
9. **Step 9:** Perform Supplementary procedures to complete certificate update process (refer to Appendix E).

➢ To generate server certificates:

1. From the Security menu, choose **Server Certificates Update**.

19-20:Server Certificate Updates



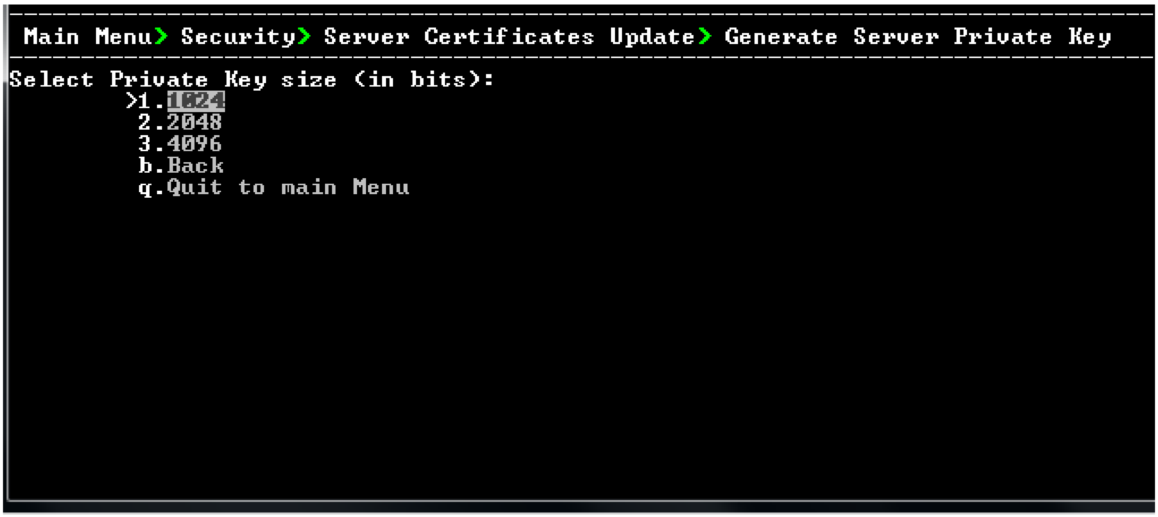
```
 Main Menu> Security> Server Certificates Update
Server's Certificate: Not Default
        >1.Generate Server Private Key
         2.Generate Server Certificate Signing Request (CSR)
         3.Import Server Certificates from Certificate Authority (CA)
         4.Update Client (JAWS) Certificates
         5.Display installed Server Certificate
         6.Display installed Root Certificate
         b.Back
         q.Quit to main Menu
```

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

➢ Step 1: Generate a server private key:

1. Select option **1**. The following screen is displayed:

Figure 19-21: Generate Server Private Key

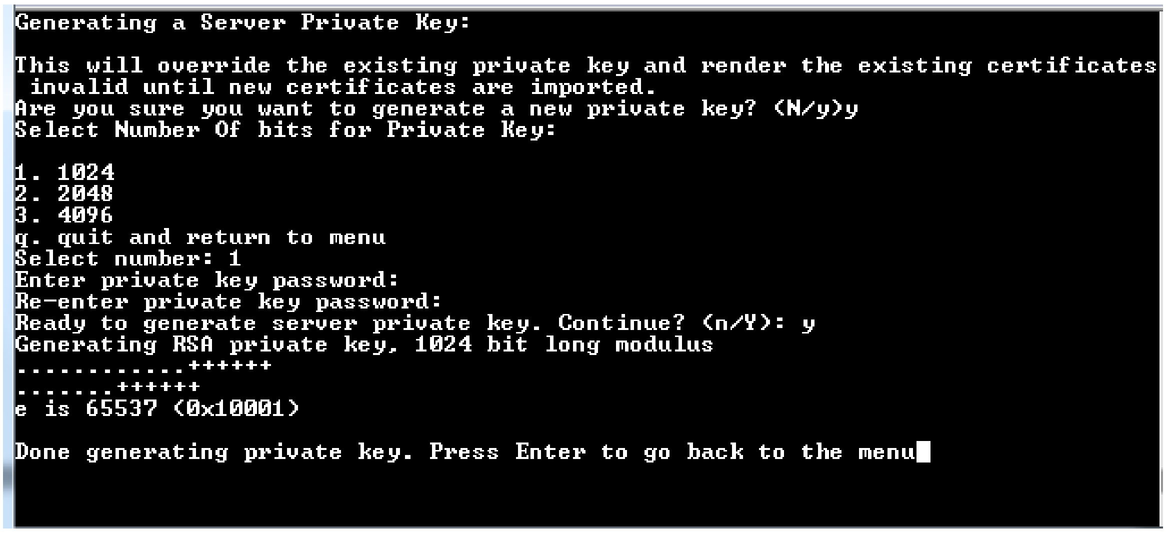


```
 Main Menu> Security> Server Certificates Update> Generate Server Private Key
Select Private Key size (in bits):
        >1.1024
         2.2048
         3.4096
         b.Back
         q.Quit to main Menu
```

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

The private key is generated.

Figure 19-22: Server Private Key Generated



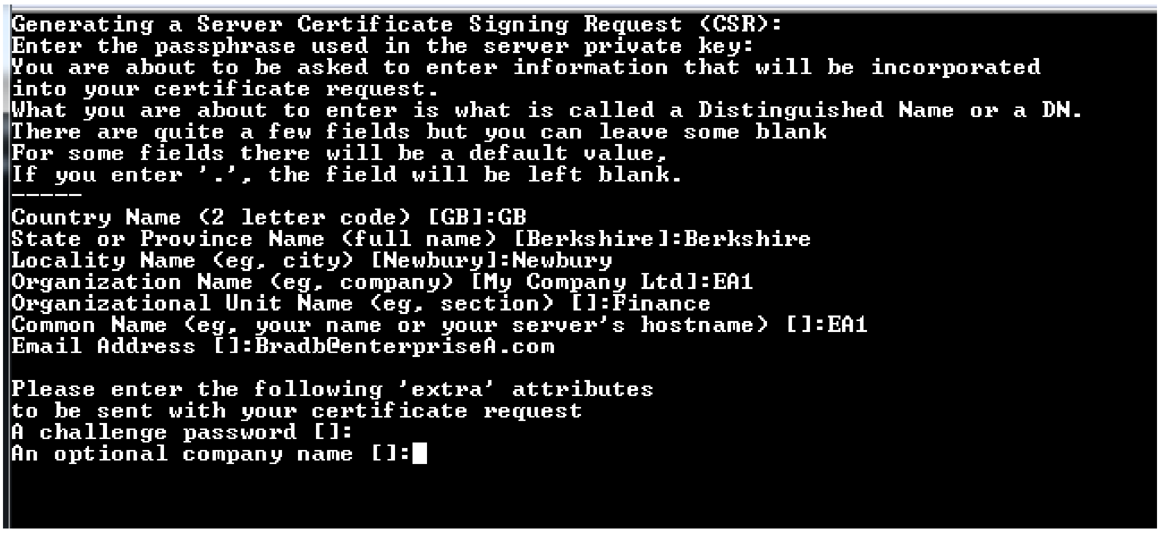
```
Generating a Server Private Key:

This will override the existing private key and render the existing certificates
 invalid until new certificates are imported.
Are you sure you want to generate a new private key? (N/y)y
Select Number Of bits for Private Key:

1. 1024
2. 2048
3. 4096
q. quit and return to menu
Select number: 1
Enter private key password:
Re-enter private key password:
Ready to generate server private key. Continue? (n/Y): y
Generating RSA private key, 1024 bit long modulus
............++++++
.......++++++
e is 65537 (0x10001)

Done generating private key. Press Enter to go back to the menu
```

➢ Step 2: Generate a CSR for the server:

1. Select option **2**.
2. Enter the private key password (the password that you entered in the procedure above).
3. Enter the Country Name code, state or province, locality, organization name, organization unit name, common name (server host name) and email address.
4. Enter a challenge password and optionally a company name.

   You are notified that a server Certificate Signing Request has successfully been generated and saved to the specified location.

Figure 19-23: Generating a Server Certificate Signing Request (CSR)

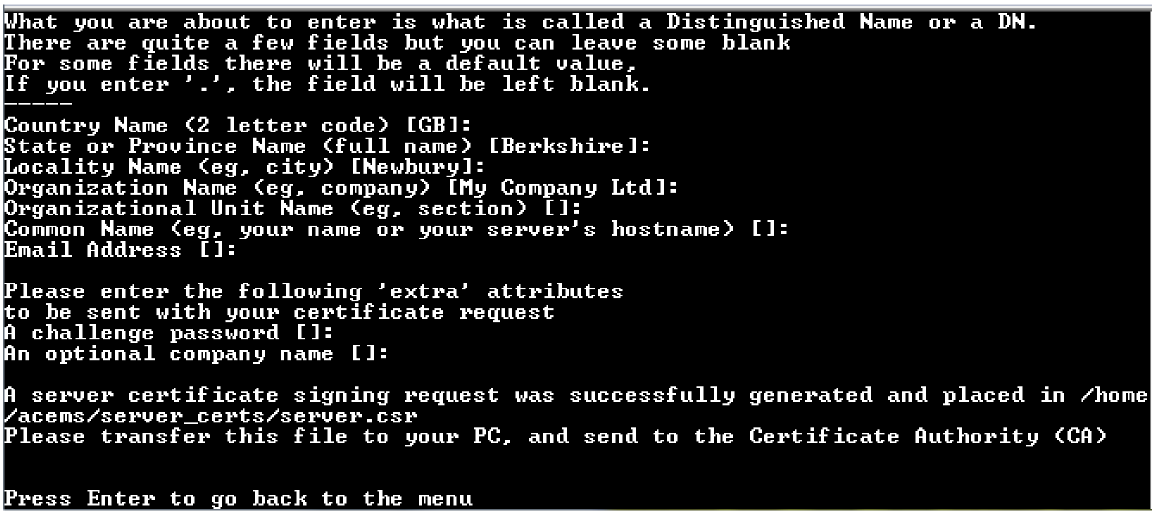


```
Generating a Server Certificate Signing Request (CSR):
Enter the passphrase used in the server private key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name (full name) [Berkshire]:Berkshire
Locality Name (eg, city) [Newbury]:Newbury
Organization Name (eg, company) [My Company Ltd]:EA1
Organizational Unit Name (eg, section) []:Finance
Common Name (eg, your name or your server's hostname) []:EA1
Email Address []:Bradb@enterpriseA.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

➢ Step 3: Transfer the CSR file to your PC and send to CA:

- Transfer the CSR file from the /home/acems/server_cert/server.csr directory to your PC and then sent it to the Certificate Authority (CA). For instructions on transferring files, see Appendix F.

Figure 19-24: Transfer CSR File to PC



```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

A server certificate signing request was successfully generated and placed in /home
/acems/server_certs/server.csr
Please transfer this file to your PC, and send to the Certificate Authority (CA)


Press Enter to go back to the menu
```

➢ Step 4: Transfer server certificates from the CA:

- Transfer the files that you received from the CA to the /home/acems/server_certs directory. The root certificate should have the name root.crt and that the server certificate should have the name server.crt. If you received intermediate certificates, then rename them to ca1.crt and ca2.crt. Make sure that all certificates are in PEM format.
  For instructions on transferring files, see Appendix F.

Note: If your certificates are self-generated (you did not perform steps 1-3), the /home/acems/server_certs directory does not exist; create it using the following commands:

```
mkdir /home/acems/server_certs
chmod 777 /home/acems/server_certs
```

➢ Step 5: Import certificates:

- Select option **3** and follow the prompts.

  The certificate file is installed.

Note:

- If you have installed an HA system and wish to install Custom server certificates, the HA system must first be uninstalled, and then you must perform this procedure separately on both server machines (as stand-alone machines).
- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format and appear as follows:

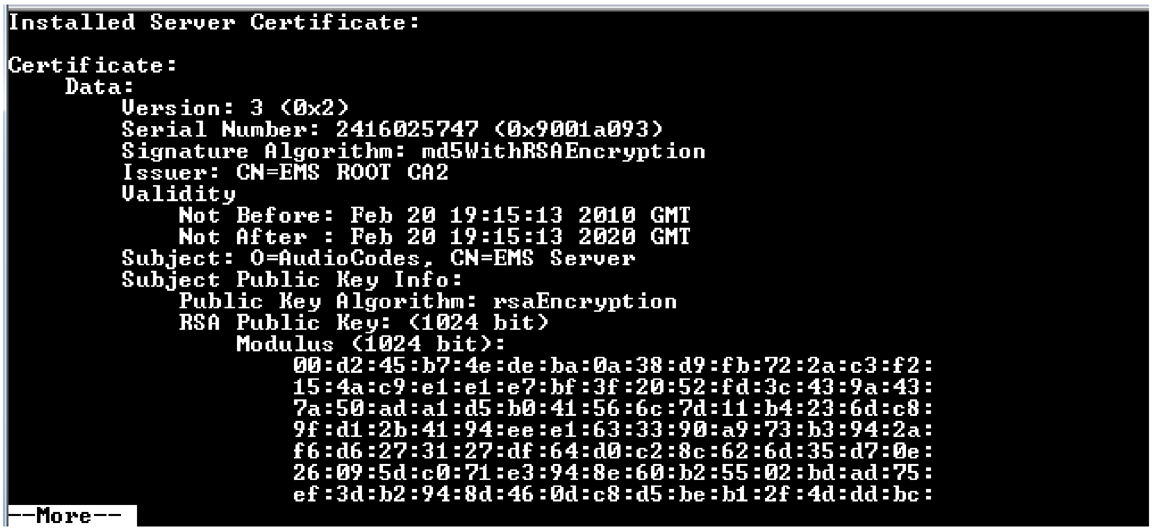
```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UEAxM
M

RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0MFowKjE
T

...

Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol
0

L6V8lzUYOfHrEiq/6g==

-----END CERTIFICATE-----
```

➢ Step 6: Verify the installed server certificate:

- Select option **4**.

  The installed server certificate is displayed:

Figure 19-25: Installed Server Certificate

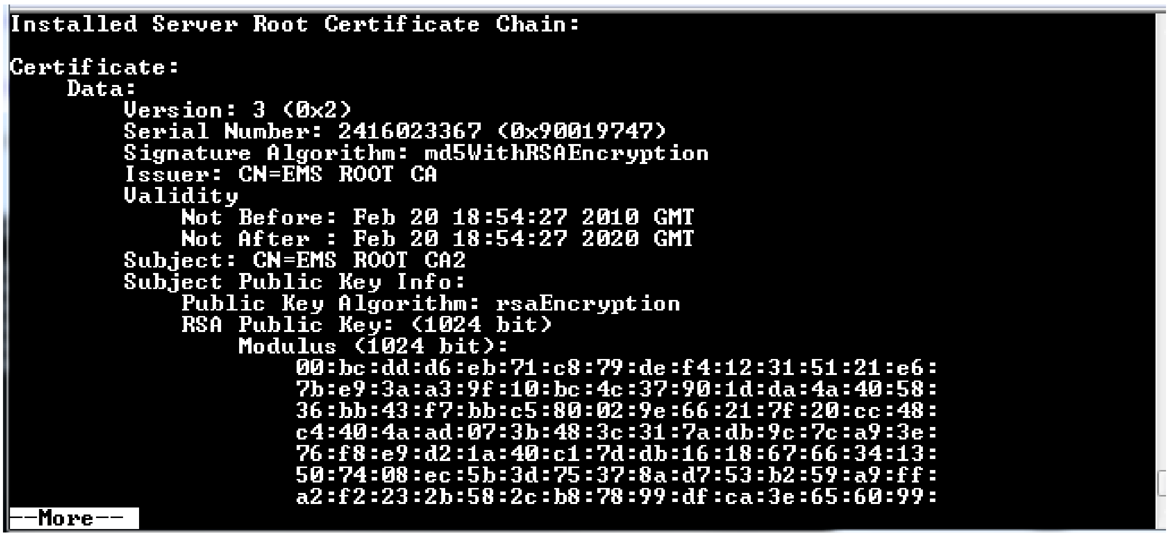


```
Installed Server Certificate:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2416025747 (0x9001a093)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=EMS ROOT CA2
        Validity
            Not Before: Feb 20 19:15:13 2010 GMT
            Not After : Feb 20 19:15:13 2020 GMT
        Subject: O=AudioCodes, CN=EMS Server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d2:45:b7:4e:de:ba:0a:38:d9:fb:72:2a:c3:f2:
                    15:4a:c9:e1:e1:e7:bf:3f:20:52:fd:3c:43:9a:43:
                    7a:50:ad:a1:d5:b0:41:56:6c:7d:11:b4:23:6d:c8:
                    9f:d1:2b:41:94:ee:e1:63:33:90:a9:73:b3:94:2a:
                    f6:d6:27:31:27:df:64:d0:c2:8c:62:6d:35:d7:0e:
                    26:09:5d:c0:71:e3:94:8e:60:b2:55:02:bd:ad:75:
                    ef:3d:b2:94:8d:46:0d:c8:d5:be:b1:2f:4d:dd:bc:
--More--
```

➢ Step 7: Verify the installed root certificate:

- Select Option **5**. The installed root certificate is displayed:

Figure 19-26: Installed Root Certificate



```
Installed Server Root Certificate Chain:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2416023367 (0x90019747)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=EMS ROOT CA
        Validity
            Not Before: Feb 20 18:54:27 2010 GMT
            Not After : Feb 20 18:54:27 2020 GMT
        Subject: CN=EMS ROOT CA2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bc:dd:d6:eb:71:c8:79:de:f4:12:31:51:21:e6:
                    7b:e9:3a:a3:9f:10:bc:4c:37:90:1d:da:4a:40:58:
                    36:bb:43:f7:bb:c5:80:02:9e:66:21:7f:20:cc:48:
                    c4:40:4a:ad:07:3b:48:3c:31:7a:db:9c:7c:a9:3e:
                    76:f8:e9:d2:1a:40:c1:7d:db:16:18:67:66:34:13:
                    50:74:08:ec:5b:3d:75:37:8a:d7:53:b2:59:a9:ff:
                    a2:f2:23:2b:58:2c:b8:78:99:df:ca:3e:65:60:99:
--More--
```

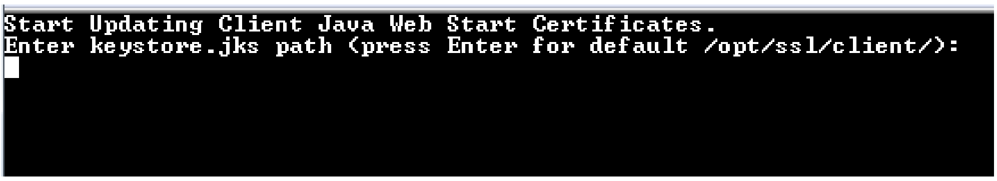
➢ Step 8: Update Client Java Web Start certificates:

Note:

- This option is only relevant when using non-default certificates, following an upgrade of the EMS server.
- The other components of the certificate configuration are maintained following an upgrade of the EMS server.

1. Select Option **4**.

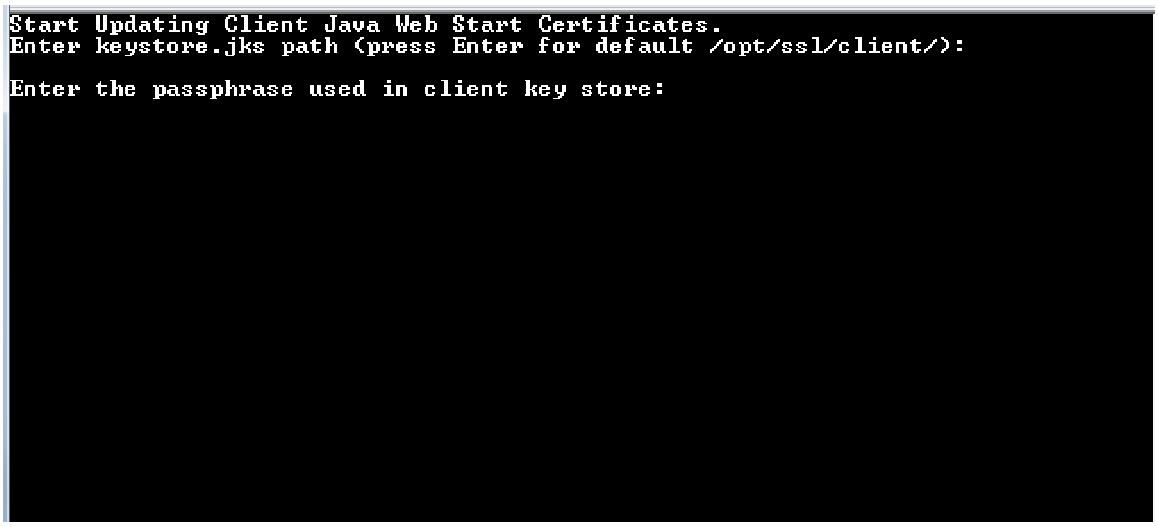
Figure 19-27: Update Client Java Web Start Certificates



```
Start Updating Client Java Web Start Certificates.
Enter keystore.jks path (press Enter for default /opt/ssl/client/):
```

2. Enter the path of the Java KeyStore file (press Enter to use the default path).

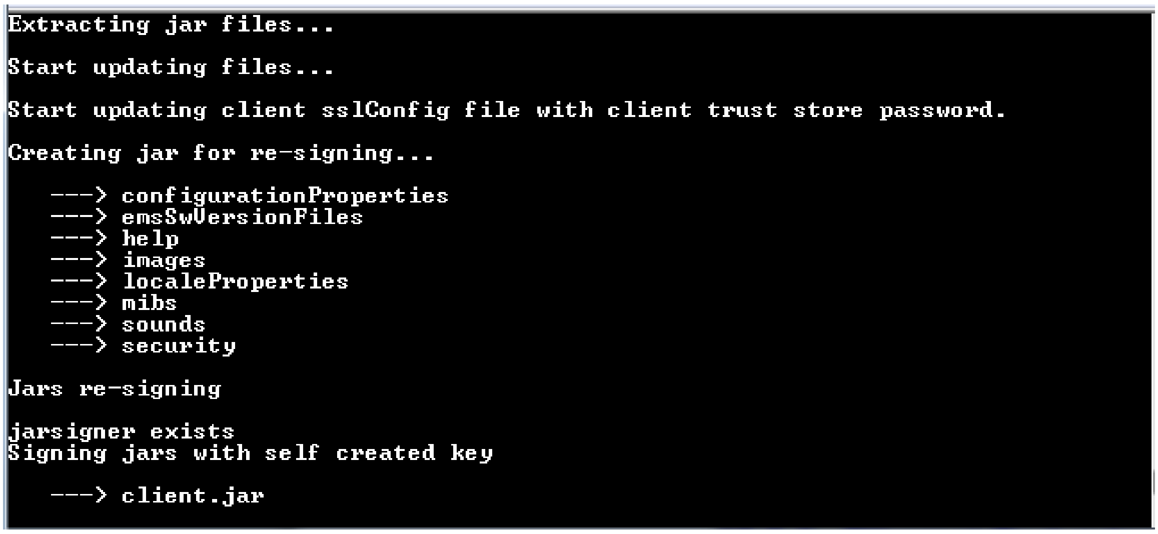
Figure 19-28: Enter Java Web Start Passphrase



```
Start Updating Client Java Web Start Certificates.
Enter keystore.jks path (press Enter for default /opt/ssl/client/):

Enter the passphrase used in client key store:
```

3. Enter the passphrase of the client KeyStore (default "password").

Figure 19-29: Java Files Updating



```
Extracting jar files...

Start updating files...

Start updating client sslConfig file with client trust store password.

Creating jar for re-signing...

   ---> configurationProperties
   ---> emsSwVersionFiles
   ---> help
   ---> images
   ---> localeProperties
   ---> mibs
   ---> sounds
   ---> security

Jars re-signing

jarsigner exists
Signing jars with self created key

   ---> client.jar
```

The Java files are updated. The progress of the updates are displayed on the screen.

➢ Step 9: Perform Supplementary procedures to complete certificate update process

- Refer to the supplementary procedures in Appendix E on page 241 to complete the certificate update process.

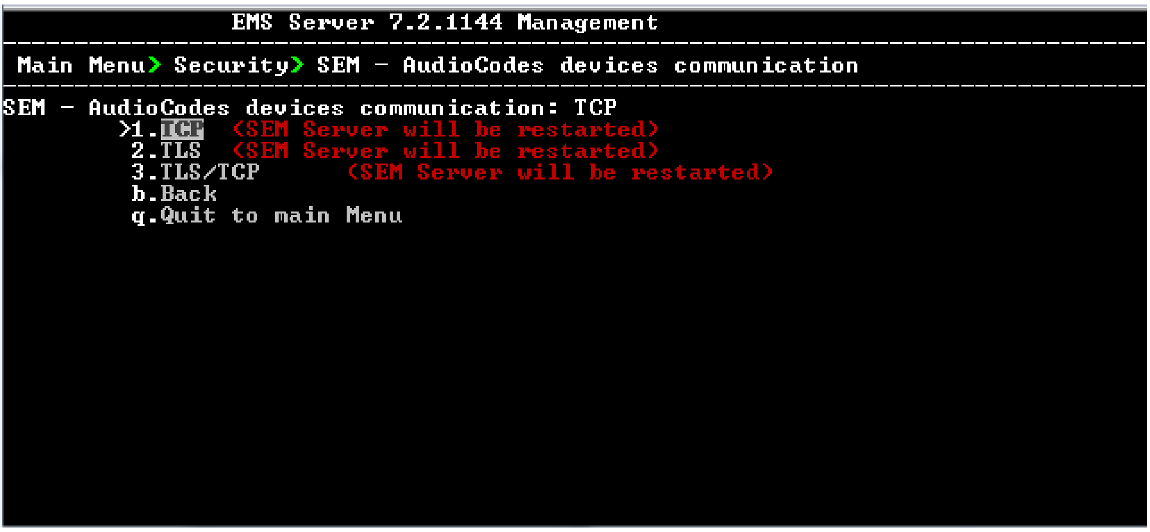
19.10.5 SEM - AudioCodes Devices Communication

This option allows you to configure the transport type for the XML based SEM communication from the AudioCodes devices to the SEM server. You can enable the TCP port (port 5000), the TLS port (port 5001) connections or both port connections.

➢ To configure the SEM - AudioCodes device communication:

1. From the EMS Server Manager Root menu, select **SEM – AudioCodes device communication**.

Figure 19-30: SEM - AudioCodes Device Communication



```
                EMS Server 7.2.1144 Management
------------------------------------------------------------------------------------
 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. Choose one of the following transport types:
   - TCP (opens port 5000)
   - TLS (opens port 5001)
   - TLS/TCP (this setting opens both ports 5000 and 5001)

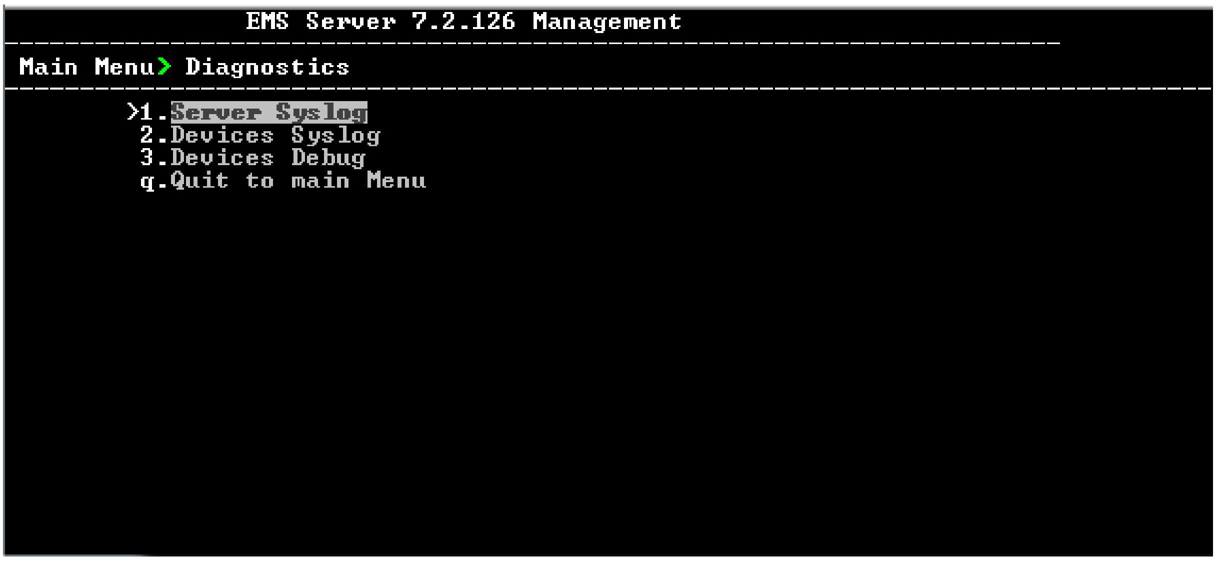
20 Diagnostics

This section describes the diagnostics procedures provided by the EMS server Manager.

➢ To run EMS Server diagnostics:

- From the EMS Server Manager Root menu, choose **Diagnostics**, and then press Enter, the following is displayed:

Figure 20-1: Diagnostics



```
                EMS Server 7.2.126 Management
-----------------------------------------------------------------------
Main Menu> Diagnostics
--------------------------------------------------------------------------------
        >1.Server Syslog
         2.Devices Syslog
         3.Devices Debug
         q.Quit to main Menu
```

This menu includes the following options:

- Server Syslog Configuration (see Section 20.1 on page 171).
- Devices Syslog Configuration (see Section 20.2 on page 171).
- Devices Debug Configuration (see Section 20.3 on page 172).

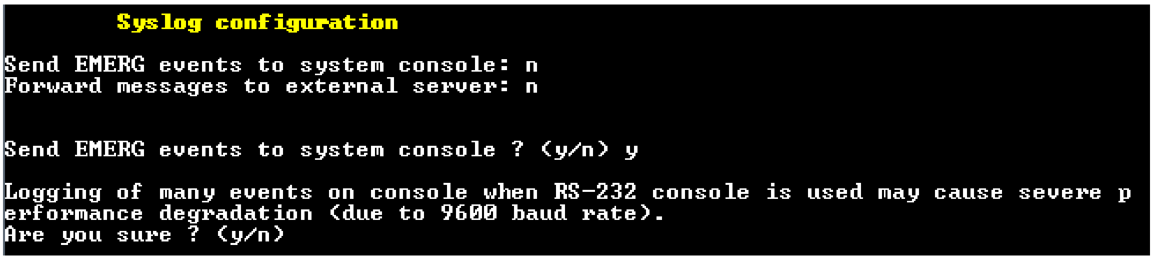
20.1 Server Syslog Configuration

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

➢ To send EMERG event to the syslog console and other events to an external server:

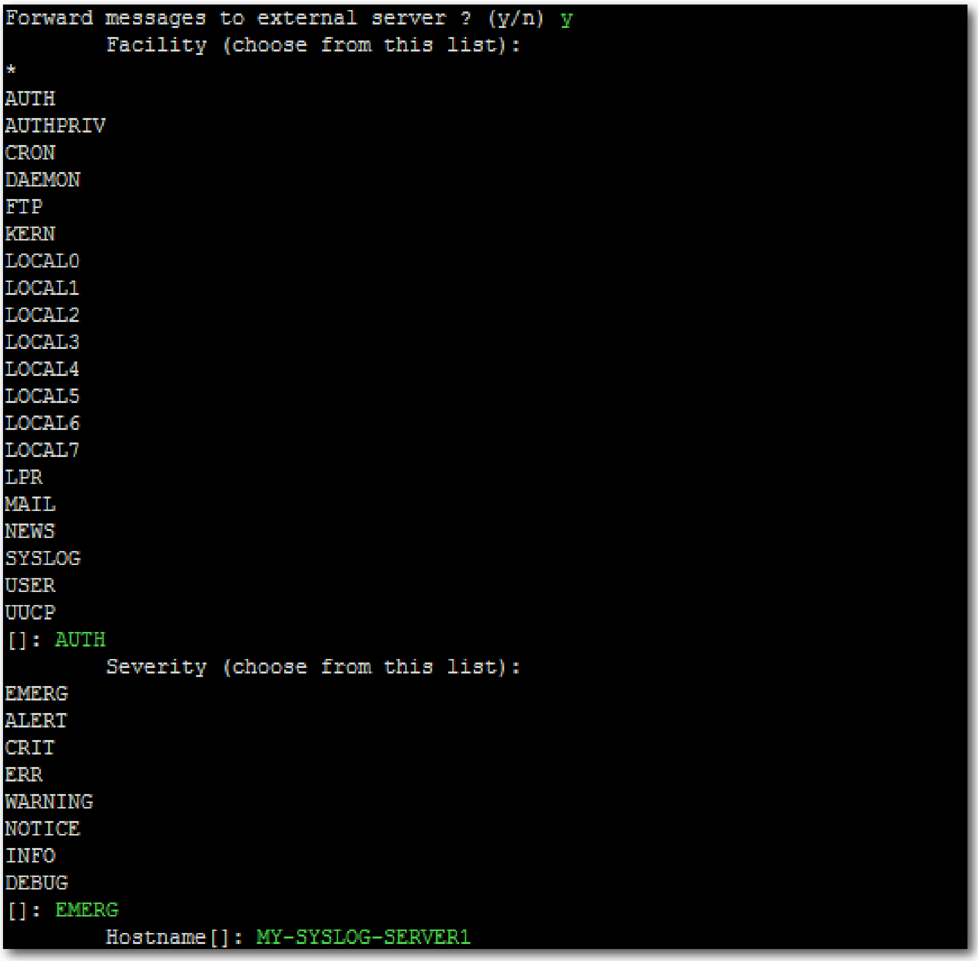
1. From the Diagnostics menu, choose **Server Syslog**, and then press Enter.
2. To send EMERG events to the system console, type **y**, press Enter, and then confirm by typing **y** again.

Figure 20-2: Syslog Configuration



```
        Syslog configuration

Send EMERG events to system console: n
Forward messages to external server: n


Send EMERG events to system console ? (y/n) y

Logging of many events on console when RS-232 console is used may cause severe p
erformance degradation (due to 9600 baud rate).
Are you sure ? (y/n)
```

Figure 20-3: Forward Messages to an External Server



```
Forward messages to external server ? (y/n) y
        Facility (choose from this list):
*
AUTH
AUTHPRIV
CRON
DAEMON
FTP
KERN
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: AUTH
        Severity (choose from this list):
EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG
[]: EMERG
        Hostname[]: MY-SYSLOG-SERVER1
```

3. You are prompted to forward messages to an external server, type **y**, and then press Enter.
4. Type the desired **Facility** from the list (case-sensitive), and then press Enter.
5. Type the desired **Severity**.
6. Type the external server Hostname or IP address.

20.2 Devices Syslog Configuration

The capture of the device's Syslog can be logged directly to the EMS server without the need for a third-party Syslog server in the same local network. The EMS server Manager is used to enable this feature.

Note: This feature is only relevant for CPE products. Syslog is captured according to the device's configured Syslog parameters. For more information, see the relevant device's *SIP User's manual*.

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the EMS server machine.

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

/data/NBIF/mgDebug/syslog

The syslog file is automatically rotated once a week or when it reaches 100 MB. Up to four syslog files are stored.

➢ To enable device syslog logging:

1. From the Diagnostics menu, choose **Devices Syslog**, and then press Enter.
2. You are prompted whether you wish to send EMER events to system console; type **Y** or **N**.
3. You are prompted whether you wish to send events to an external server; type **Y** or **N**.

20.3 Devices Debug Configuration

Debug recordings packets from all managed machines can be logged directly to the EMS server without the need for a 3rd party network sniffer in the same local network.

> **Note:** This feature is only relevant for CPE products. Debug recording packets are collected according to the device's configured Debug parameters. For more information, see the relevant device's *User's Manual*.

The EMS server runs the Wireshark network sniffer, which listens on a particular configured port. The sniffer records the packets to a network capture file in the Debug Recording (DR) directory. You can then access this file from your PC through FTP.

The EMS Server Manager is used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the EMS server IP.

The DR capture file is located in the following EMS server directory:

/data/NBIF/mgDebug/DebugRecording

The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close i.e. if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the EMS server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

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

1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.

   A message is displayed indicating that debug recording is either enabled or disabled.

2. Type **y**, and then press Enter.

   Recording files are saved in /data/NBIF/mgDebug directory on the server.

> **Note:** It is highly recommended to disable the 'TP Debug Recording' feature when you have completed recording because this feature heavily utilizes system resources.

Part VI

HA (High Availability)

This section describes the EMS HA Configuration options.

21 Getting Started with HA (High Availability)

EMS servers High Availability is supported for EMS server applications running on the Linux platform.

Two EMS server machines are required to support High Availability: one machine serving as the Primary machine and the other serving as the Secondary machine. When the EMS application is active and running, all data stored in the EMS server machine and database is replicated from the Primary machine to the Secondary machine. Upon Primary machine failure recognition (either on the EMS application or on the Network), activity is automatically transferred from the Primary server machine to the Secondary server machine.

Two models of High Availability are supported:

- Both EMS servers are located in the same subnet. There is a single EMS server IP address - Global (Virtual) IP address defined for all the Network Components (EMS clients and Managed Gateways). Each of the EMS server machines has an internal Private IP address and the active EMS server machine performs binding to the Global (Virtual) IP address. This setup currently does not support working with gateways behind a NAT.
- Each one of the EMS servers is located in a different network subnet and has its own IP address. During the EMS client login dialog, the user should provision both IP addresses (Geo HA), and the EMS client application will constantly search for the currently active EMS server machine. All the managed gateways relevant applications (such as Trap Sending, NTP Server, and OCSP Server) should be aware of two possible EMS server machine addresses.

The HA Configuration menu option enables you to configure EMS server machines high availability, perform HA-related actions and review the HA status for both servers.

Prior to configuring HA, both machines should be installed with an identical EMS server version and an identical operating system and network configuration.

21.1 EMS HA Pre-requisites

Before implementing an EMS HA configuration, ensure that both EMS servers have an identical configuration according to the following:

- Both servers have identical hardware. See EMS Server and Client Requirements section for supported machines (see Chapter 3 on page 23).
- An identical Linux OS is installed on both servers.
- An identical EMS version is installed on both servers.
- An identical database password should be configured on both servers.
- An identical interface configuration and the same subnets are connected to each server (N/A for Geo HA).
- An identical redundancy configuration on identical interfaces.
- The EMS application is down (use the EMS Server Manager to shut down the EMS application).
- SSH communication between the Secondary and the Primary servers exists.
- Network Bandwidth requirements between two EMS servers are as follows:
    - Initial Synchronization process: at least 80 Mbps

      During the initial sync process, the entire /data partition is synchronized between the active and redundant servers. This partition size is 1.7 TB on HP DL360p G8 servers. A network speed of at least 80 Mbps is required to complete the initial sync process in up to 5 hours on G8 servers.

      Assuming a slower network, the process will take longer. For example, on G8 servers:
        - 100Mbps -> up to 40 hours
        - 1Gbps -> up to 4 hours
    - Ongoing server Synchronization: 10 Mbps.
    - Ping between two servers: the ping time between each EMS server machine should not exceed 200 msec.
- During the HA configuration process, entire /data partition is duplicated from the primary server to the secondary server. If any of the servers contain previous backup files, these files are deleted on the secondary server. These files should be backed up on an external storage machine prior to the HA configuration.
- If you are using custom certificates (see Appendix E on page 241), they must be preinstalled on both primary and secondary machines before commencing the HA process.

21.2 EMS HA Data Synchronization

The data synchronization is performed using a distributed replicated block device for the Linux operating system. This process allows a real-time mirror of the local block devices on a remote machine.

The replicated EMS data includes the following:

- EMS Database
- EMS NBIF files including the following:
  - Backup files
  - Alarms files
  - Topology files
  - Performance files
  - MG backup files
  - Debug recording
- EMS Software files (EMS Software Manager files)
  - MG configuration files, for upgrade and management
  - MG Auxiliary files

The initial synchronization time between two EMS server machines is estimated at 1.5-4 hours, depending on network speed/quality and servers' disk size. Every change that is performed on the primary server is immediately synchronized to the secondary server.

21.2.1 Replicate EMS Server Manager Actions

Any actions performed using the EMS Server Manager prior to the HA configuration should be manually updated on both EMS server machines. EMS Server Manager actions are logged in the following file:

```
/var/log/ems/EmsServerManager.txt
```

Note: The EMS HA process does not automatically replicate actions executed using the EMS Server Manager on the primary server to the secondary server.

21.3 EMS Server Manager

This section describes specific details in reference to the maintenance procedures available in the EMS Server Manager.

The EMS Server Manager displays dynamic menus. Each menu is displayed differently according to the current server's state.

The following menu items are not displayed on the Primary server:

- Start/Stop Application
- Change Server's IP Address
- Configure Ethernet Interfaces

- Configure Ethernet Redundancy
- Configure NAT
- Restore the EMS Server
- DB Password

The following menu items are not displayed on the Secondary server:

- Start/Stop Application
- Change Server's IP Address
- Configure Ethernet Interfaces
- Configure Ethernet Redundancy
- Configure NAT
- Add EMS User
- Restore the EMS Server
- DB Password

In some cases, the menu will only be updated after running EMS Server Manager again. For instance, after HA installation, the Start/Stop EMS Server option is hidden after exiting the EMS Server Manager and running it again.

21.4 EMS Client

Once the switchover has successfully completed, the EMS client logs in again to the active server and a "Server Startup" alarm is displayed.

21.5 EMS Server Upgrade

EMS server version upgrade cannot be performed while HA is configured.

To upgrade the servers, HA must be uninstalled prior to the upgrade. It is recommended to firstly uninstall the secondary server, and then the primary server.

- To uninstall HA, see Section 22.6 on page 192.
- To upgrade the EMS server, see Section 8.1 on page 81.

21.5.1 Upgrading to Version 7.2.1000

The procedure below is designated for customers with EMS HA installed on any version prior to 7.2.1000 who wish to upgrade their servers to 7.2.1000. This procedure requires the following actions:

1. Upgrade of the EMS servers to Version 7.2.1000.
2. Backup of all data.
3. Upgrade of the Linux Operating System to CentOS 5.9 Rev8.
4. Restore of data to new installation.

Note: For maintaining EMS HA and all data, it is mandatory for you to perform the procedure below if you are upgrading to EMS Version 7.2.1000 CentOS 5.9 Rev8.

➢ **Do the following:**

1. Uninstall HA from Secondary server and reboot it. After reboot make sure all processes are up in EMS Server Manager Status (see Chapter 13).
2. Uninstall HA from Primary server and reboot it. After reboot make sure all processes are up in EMS Server Manager Status (see Chapter 13).
3. Upgrade each one of the servers to 7.2.1000. After reboot make sure all processes are up in Ems Server Manager Status.
4. On the server which was the Primary server prior to uninstalling HA, configure the server to create a new weekly backup on the next full hour e.g. 1200 (following the time of completing this procedure) using the Change Schedule Backup Time option (see Section 16.3).
5. Wait for backup process to complete. This can be verified by typing the following command:

   ```
    ll /data/NBIF/emsBackup/RmanBackup/init.ora" command.
   ```

   When the init.ora file recieves the current timestamp, this implies that the Backup process has completed. For example:

   ```
   [root@EMS-12 ~]# ll
   /data/NBIF/emsBackup/RmanBackup/init.ora
   -rw-r--r-- 1 oracle dba 1449 May  2 02:08
   /data/NBIF/emsBackup/RmanBackup/init.ora
   ```

6. Copy all backup files to an external server:

   ```
   /data/NBIF/emsBackup/emsServerBackup_xxx.tar
   /data/NBIF/emsBackup/RmanBackup/*
   ```

7. Perform clean installations:
   a. Install the Linux CentOS 5.9 Rev8 Operating System.
   b. Install EMS 7.2.1000 (the same version that you installed in Step 3 above) on both servers. After reboot, make sure all processes are up in EMS Server Manager / Status (see Chapter 13).
8. Copy all backup files to the Primary server and run the EMS Server Manager Restore procedure (see Section 16.4).
9. After reboot make sure all processes are up in the EmsServerManager Status (see Chapter 13). Make sure all data from latest backup was properly restored.
10. Install HA on the Primary server and wait for all processes to be up again in EMS Server Manager Status (see Chapter 13). This step can take several minutes.
11. Install HA on the Secondary server and wait for sync to complete.

21.6 EMS Server Restore

EMS server restore cannot be performed while HA is configured.

To restore the EMS server, HA must be uninstalled prior to the restore.

It is recommended to firstly uninstall the secondary server, and only then the primary server. After restoring the server, HA should be reconfigured.

To uninstall HA, see Section 22.6 on page 192.

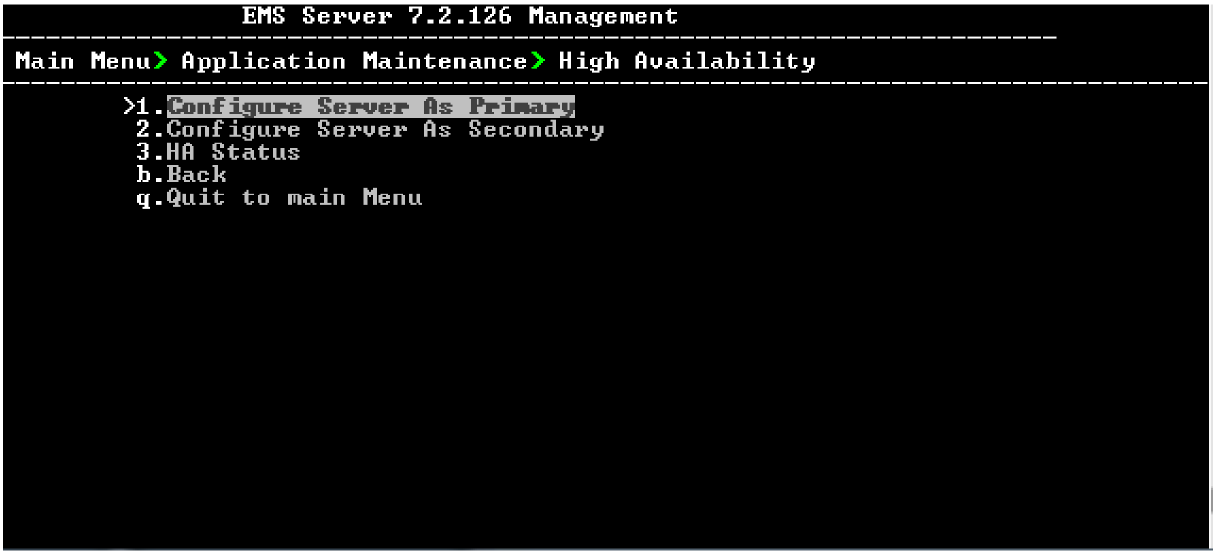
22 EMS HA Configuration

This section describes the EMS HA Installation.

➢ To configure the primary server:

1. In the EMS Server Manager root menu, choose **Application Maintenance**, in the sub-menu, choose **High Availability**, and then press Enter; the following is displayed:

Figure 22-1: EMS Server Manager - HA Configuration



```
                EMS Server 7.2.126 Management
----------------------------------------------------------------------
Main Menu> Application Maintenance> High Availability
--------------------------------------------------------------------------------
        >1.Configure Server As Primary
         2.Configure Server As Secondary
         3.HA Status
         b.Back
         q.Quit to main Menu
```

This menu includes the following options:

- Primary Server Installation in Global IP Model (see Section 22.1 on page 182).
- Primary Server Installation in in Geo HA model (see Section 22.2 on page 184).
- Secondary Server Installation (see Section 22.3 on page 184).
- HA Status (see Section 22.4 on page 188).

22.1 Primary Server HA Installation in Global IP Model

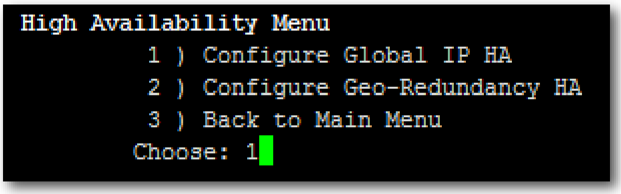
This section describes how to install the HA application on the designated Primary server in the Global IP address model.

Note: When alarms are forwarded from the EMS, you can configure the global IP address as a source address. For more information, refer to the *EMS User's Manual*.

➢ To install the HA primary server in Global IP Model:

1. In the High Availability menu, choose option **1** to run the Primary server HA installation, and then press Enter.
2. After the HA packages are installed, you are prompted for the HA model:

Figure 22-2: Primary HA Server Menu

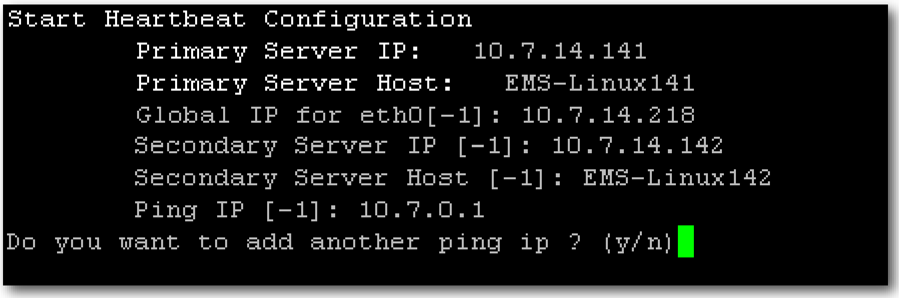


```
High Availability Menu
         1 ) Configure Global IP HA
         2 ) Configure Geo-Redundancy HA
         3 ) Back to Main Menu
        Choose: 1
```

For the Global IP HA model, both EMS servers are located in the same subnet.

3. In the High Availability sub-menu, choose option **1** (**Configure Global IP HA**).
4. You are now prompted for the following network parameters:
   - 'Global IP' for each configured interface (physical or logical IF).
   - Secondary server's Host name and IP address.
   - Ping Nodes - If you have several interfaces configured, you can add another 'ping node' (for more information, see Section 22.2.1 on page 186).

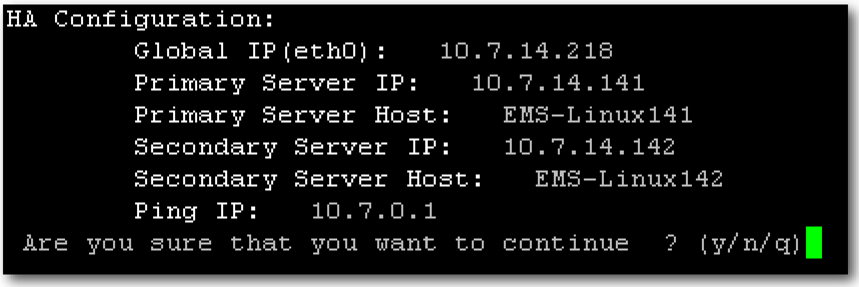
Figure 22-3: Primary HA Server Sub-menu



```
Start Heartbeat Configuration
        Primary Server IP:   10.7.14.141
        Primary Server Host:   EMS-Linux141
        Global IP for eth0[-1]: 10.7.14.218
        Secondary Server IP [-1]: 10.7.14.142
        Secondary Server Host [-1]: EMS-Linux142
        Ping IP [-1]: 10.7.0.1
Do you want to add another ping ip ? (y/n)
```

The current configuration is displayed for confirmation:

Figure 22-4: HA Configuration Display



```
HA Configuration:
        Global IP(eth0):   10.7.14.218
        Primary Server IP:   10.7.14.141
        Primary Server Host:   EMS-Linux141
        Secondary Server IP:   10.7.14.142
        Secondary Server Host:   EMS-Linux142
        Ping IP:   10.7.0.1
 Are you sure that you want to continue  ? (y/n/q)
```

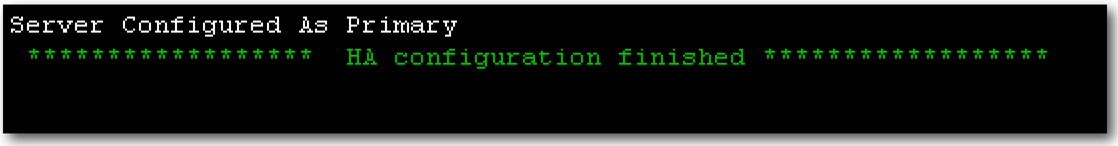
- Type **y** to continue the installation process
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- "/data: device is busy" – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing**. In the case where the /data partition isn't busy, the above message is not displayed.
- When prompted, press Enter to continue.
- When prompted "To abort waiting type 'yes' [1]:" – you can wait or press 'yes' to continue.

When the installation process for the Primary server has completed, the following message is displayed:

Figure 22-5: HA Server Configured as Primary Server - Confirmation



```
Server Configured As Primary
 ******************  HA configuration finished ******************
```

Note: After the installation process has completed, it takes several minutes until the HA status changes to "Online" and the EMS server status changes to 'EMS server is running'.

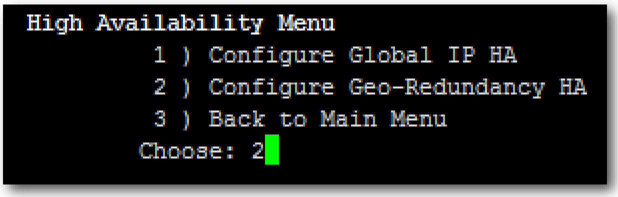
22.2 Primary Server HA Installation in Geo HA Model

This section describes how to install the HA application on the designated Primary server in the Geo HA model.

➢ To install the HA primary server in Geo HA model:

1. In the High Availability menu, choose option **1** to run the Primary server HA installation, and then press Enter.
2. After the HA packages are installed, you are prompted for the HA model:

Figure 22-6: Primary HA Server Menu

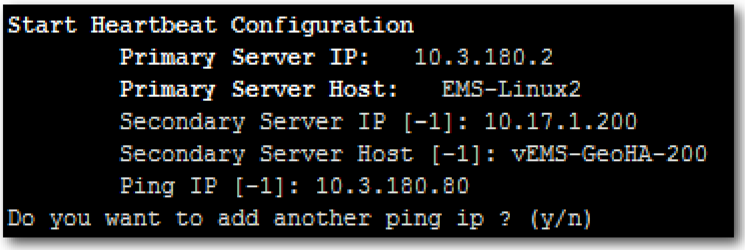


```
High Availability Menu
         1 ) Configure Global IP HA
         2 ) Configure Geo-Redundancy HA
         3 ) Back to Main Menu
        Choose: 2
```

For the Geo HA model, EMS servers are located in different subnets.

3. In the High Availability sub-menu, choose option **2** (**Configure Geo-Redundancy HA**).
4. You are now prompted for the following network parameters:
   - Secondary server's Host name and IP address.
   - Ping Nodes - If you have several interfaces configured, you can add another 'ping node' (for more information, see Section 22.2.1 on page 186).

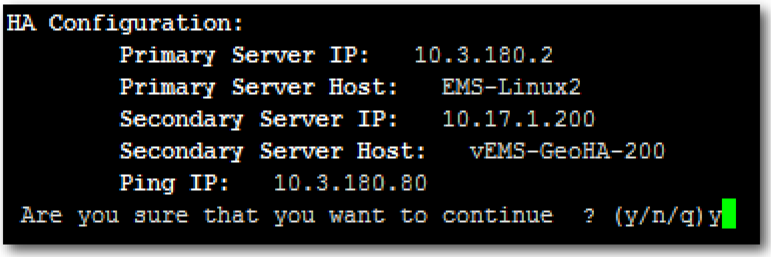
Figure 22-7: Primary HA Server Sub-menu



```
Start Heartbeat Configuration
        Primary Server IP:    10.3.180.2
        Primary Server Host:    EMS-Linux2
        Secondary Server IP [-1]: 10.17.1.200
        Secondary Server Host [-1]: vEMS-GeoHA-200
        Ping IP [-1]: 10.3.180.80
Do you want to add another ping ip ? (y/n)
```

The current configuration is displayed for confirmation:

Figure 22-8: HA Configuration Display



```
HA Configuration:
        Primary Server IP:   10.3.180.2
        Primary Server Host:   EMS-Linux2
        Secondary Server IP:   10.17.1.200
        Secondary Server Host:   vEMS-GeoHA-200
        Ping IP:   10.3.180.80
 Are you sure that you want to continue  ? (y/n/q)y
```

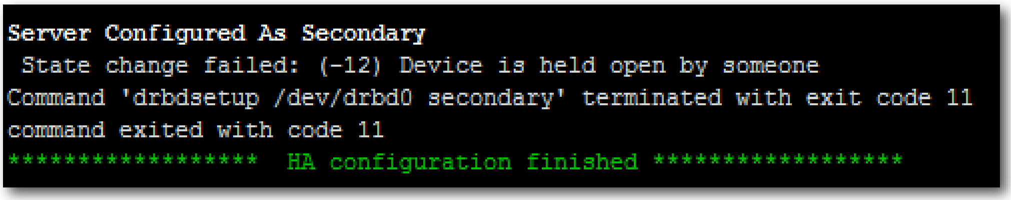
- Type **y** to continue the installation process.
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- "/data: device is busy" – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing**. In the event where the /data partition isn't busy, the above message is not displayed.
- When prompted, press Enter to continue.
- When prompted "To abort waiting type 'yes' [1]:" – you can wait or press 'yes' to continue.

When the installation process for the Primary server has completed, the following message is displayed:

Figure 22-9: HA Server Configured as Primary Server - Confirmation



```
Server Configured As Secondary
 State change failed: (-12) Device is held open by someone
Command 'drbdsetup /dev/drbd0 secondary' terminated with exit code 11
command exited with code 11
******************  HA configuration finished ******************
```

Note: After the installation process has completed, it takes several minutes until the HA status changes to 'Online' and the EMS server status changes to 'EMS server is running'.

22.2.1 Ping Nodes

The purpose of these nodes (IP address) is to ensure network connection along all EMS server configured interfaces. When an IP address is configured as “ping node”, this implies that the HA process sends ICMP packets (at a constant interval) to this address (through the appropriate Server Ethernet interface). If no response is returned from this ping node (during a constant period of time), the HA process determines that the specific network interface connection is down and acts accordingly (i.e. initiates a possible switchover). The ping node should be a reliable host in the network, such as router or any other machine which accurately reflects the network status.

It is possible to configure several “ping nodes”, where each ping node is considered to be a single point of failure. Consequently if there is no connection to one of the ping nodes, a switchover is performed (unless the Secondary server cannot takeover due to the same or different network problems or during initial synchronization between the Primary and Secondary server).

Note: It’s recommended to configure a separate ping node for each configured physical Ethernet interface (to the router connected to each of the subnets); however, if Ethernet Redundancy is configured between these two interfaces, then it’s sufficient to configure a single ping node.

22.3 Secondary Server HA Installation

This section describes how to install the High Availability (HA) application on the designated Secondary server.

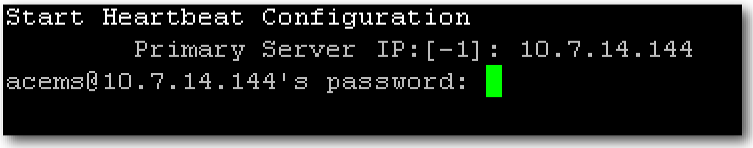
➢ To install the secondary server:

1. In the High Availability menu, choose option **2** to run the Secondary HA Server installation, and then press Enter.

> **Note:** The Secondary server configuration MUST be performed after the Primary server configuration has completed and its status is 'EMS Server is running'.

2. After the HA packages are installed, you are prompted for the 'Primary IP' and *acems* user password (you might also be prompted to answer **yes** before connecting).

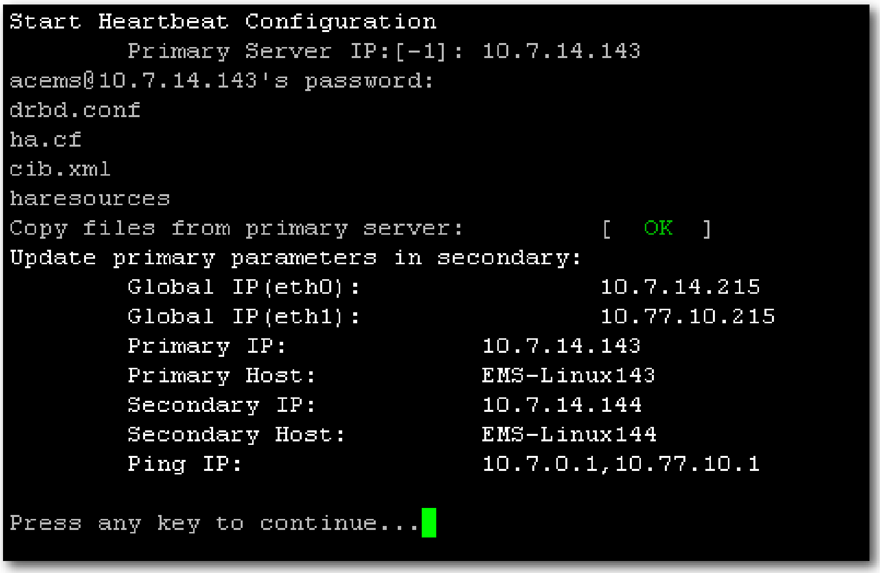
Figure 22-10: Primary HA Server IP



```
Start Heartbeat Configuration
        Primary Server IP:[-1]: 10.7.14.144
acems@10.7.14.144's password: █
```

The Secondary server copies the HA configuration files from the Primary server and then starts the installation process.

Figure 22-11: Secondary HA Server Configuration



```
Start Heartbeat Configuration
        Primary Server IP:[-1]: 10.7.14.143
acems@10.7.14.143's password:
drbd.conf
ha.cf
cib.xml
haresources
Copy files from primary server:          [  OK  ]
Update primary parameters in secondary:
        Global IP(eth0):                  10.7.14.215
        Global IP(eth1):                  10.77.10.215
        Primary IP:             10.7.14.143
        Primary Host:           EMS-Linux143
        Secondary IP:           10.7.14.144
        Secondary Host:         EMS-Linux144
        Ping IP:                10.7.0.1,10.77.10.1

Press any key to continue...█
```

3. When prompted '[need to type **yes** to confirm]' press **yes**.
4. When prompted 'Press any key to continue...' press Enter.

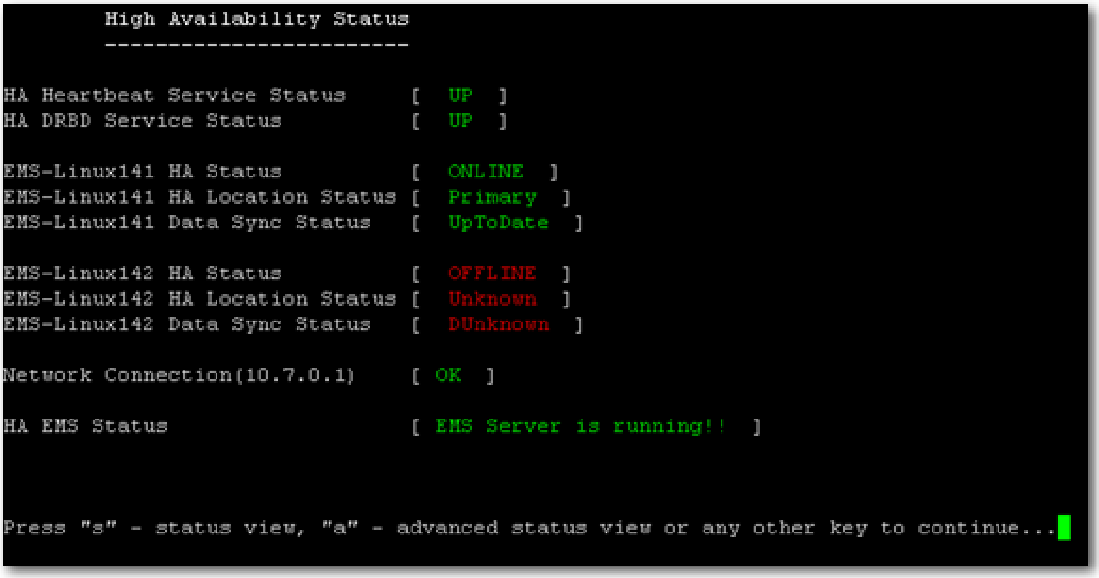
22.4 HA Status

The 'HA status' displays both servers’ High Availability parameters.

➢ **To verify the EMS HA status:**

- In the High Availability menu, choose option **3** (**HA Status**), and then press Enter; the following status view is displayed (Example only):

Figure 22-12: EMS HA Status - Example Display



```
        High Availability Status
        ------------------------

HA Heartbeat Service Status     [  UP  ]
HA DRBD Service Status          [  UP  ]

EMS-Linux141 HA Status          [  ONLINE  ]
EMS-Linux141 HA Location Status [  Primary  ]
EMS-Linux141 Data Sync Status   [  UpToDate  ]

EMS-Linux142 HA Status          [  OFFLINE  ]
EMS-Linux142 HA Location Status [  Unknown  ]
EMS-Linux142 Data Sync Status   [  DUnknown  ]

Network Connection(10.7.0.1)    [ OK  ]

HA EMS Status                   [ EMS Server is running!!  ]



Press "s" - status view, "a" - advanced status view or any other key to continue...
```

- **HA Heartbeat Service Status:** Whether the heartbeat service is installed and running.
- **HA DRBD Service Status:** Whether the data replication service is installed and running.
- **<HOST_NAME > HA Status:** The following states are available:
  - ONLINE – HA is enabled and heartbeat packets have been sent.
  - OFFLINE – HA is disabled or does not exist (this state usually appears for several minutes after the new installation).
  - IN Progress – HA has started (this state usually appears for several seconds immediately after the new installation).
- **<HOST_NAME > HA Location Status:** the following states are available:
  - Unknown – Cannot resolve if the EMS server is Primary or Secondary
  - Primary - The current working server
  - Secondary - the redundant server
- **<HOST_NAME > HA Data Sync Status:** the following states are available:
  - DUnknown - Cannot resolve whether the EMS server data is synchronized with the other server
  - UpToDate – The replicated data is synchronized with the Primary server
  - Inconsistent – The replicated data is in the progress of synchronizing with the Primary server
- **Network Connection (<Ping Node>):**- For each configured ping node, this status verifies if there is a network connection to it.
- **HA EMS Status:** The current state of the EMS server and watchdog processes:
  - The EMS server is running – the EMS server process is up.
  - The EMS is not installed
  - The EMS server is not running – the EMS watchdog is trying to start the EMS server.
  - The EMS watchdog is not running.
  - Unknown, Not Primary Server – This state is always displayed on the Secondary server. In addition, it displays when HA is not configured.

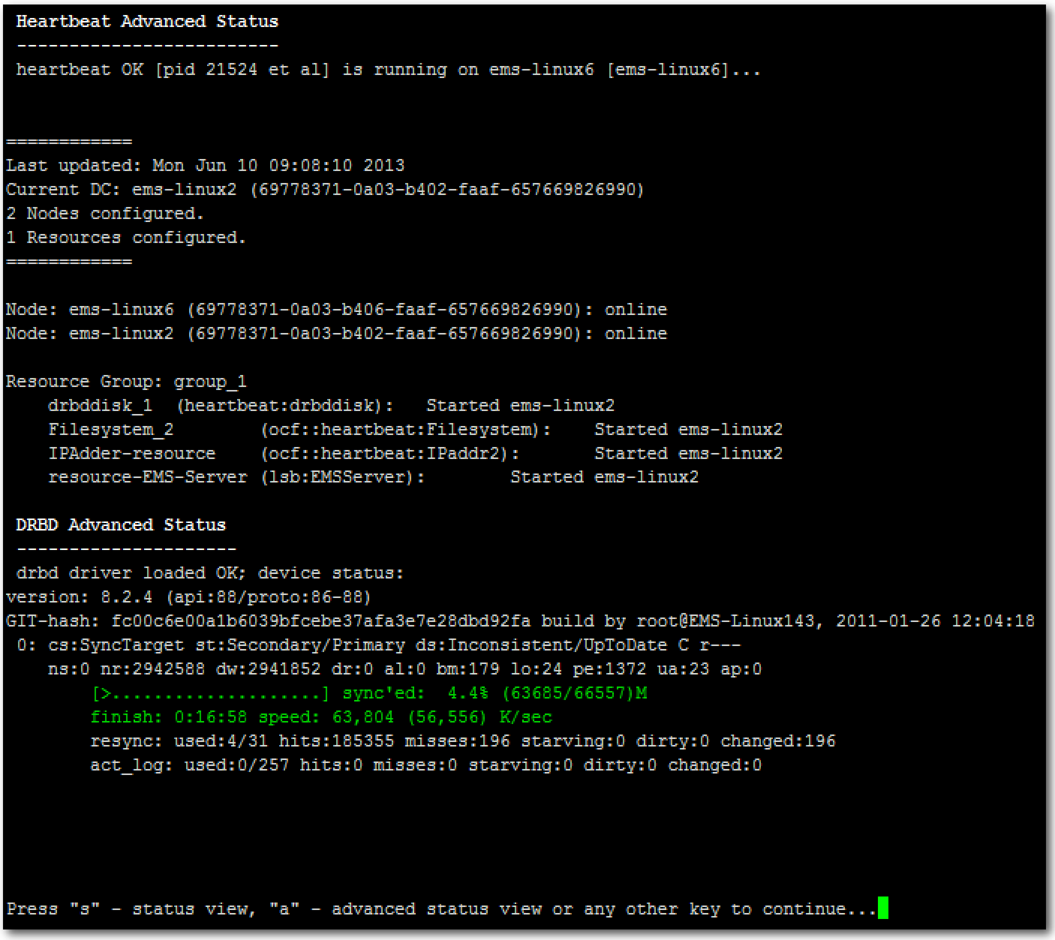
22.4.1 Advanced Status View

This section describes the advanced status view.

➢ **To view the advanced status:**

- In the High Availability Status screen, press **a**; the following is displayed:

Figure 22-13: Advanced Status View



```
 Heartbeat Advanced Status
 -------------------------
 heartbeat OK [pid 21524 et al] is running on ems-linux6 [ems-linux6]...


============
Last updated: Mon Jun 10 09:08:10 2013
Current DC: ems-linux2 (69778371-0a03-b402-faaf-657669826990)
2 Nodes configured.
1 Resources configured.
============

Node: ems-linux6 (69778371-0a03-b406-faaf-657669826990): online
Node: ems-linux2 (69778371-0a03-b402-faaf-657669826990): online

Resource Group: group_1
    drbddisk_1  (heartbeat:drbddisk):   Started ems-linux2
    Filesystem_2        (ocf::heartbeat:Filesystem):    Started ems-linux2
    IPAdder-resource    (ocf::heartbeat:IPaddr2):       Started ems-linux2
    resource-EMS-Server (lsb:EMSServer):        Started ems-linux2

 DRBD Advanced Status
 ---------------------
 drbd driver loaded OK; device status:
version: 8.2.4 (api:88/proto:86-88)
GIT-hash: fc00c6e00a1b6039bfcebe37afa3e7e28dbd92fa build by root@EMS-Linux143, 2011-01-26 12:04:18
 0: cs:SyncTarget st:Secondary/Primary ds:Inconsistent/UpToDate C r---
    ns:0 nr:2942588 dw:2941852 dr:0 al:0 bm:179 lo:24 pe:1372 ua:23 ap:0
        [>....................] sync'ed:  4.4% (63685/66557)M
        finish: 0:16:58 speed: 63,804 (56,556) K/sec
        resync: used:4/31 hits:185355 misses:196 starving:0 dirty:0 changed:196
        act_log: used:0/257 hits:0 misses:0 starving:0 dirty:0 changed:0




Press "s" - status view, "a" - advanced status view or any other key to continue...
```

The advanced status view provides a more detailed view of the EMS HA status. This command is particularly important during the initial synchronization between the primary and secondary EMS servers when the precise percentage of the stage of the EMS HA synchronization process is displayed (highlighted in green in the above figure).

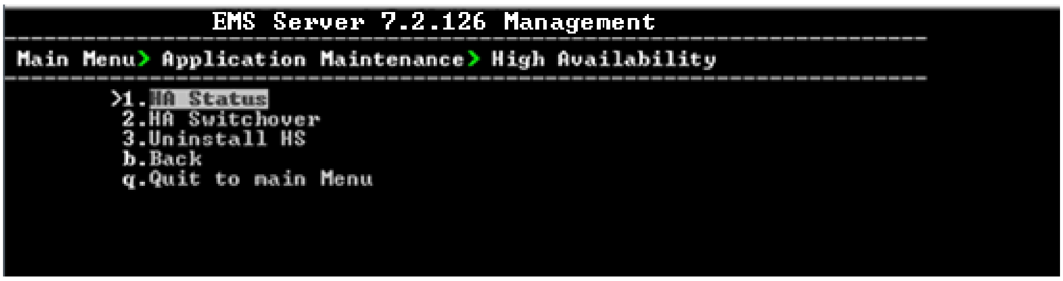
22.5 EMS Server Manual Switchover

Manual switchover can be performed from either the Primary HA or Secondary HA server.

➢ To manually switchover to the active EMS server:

1. In the High Availability menu, choose option **2** (**HA Switchover**), and then press Enter.

Figure 22-14: Manual Switchover

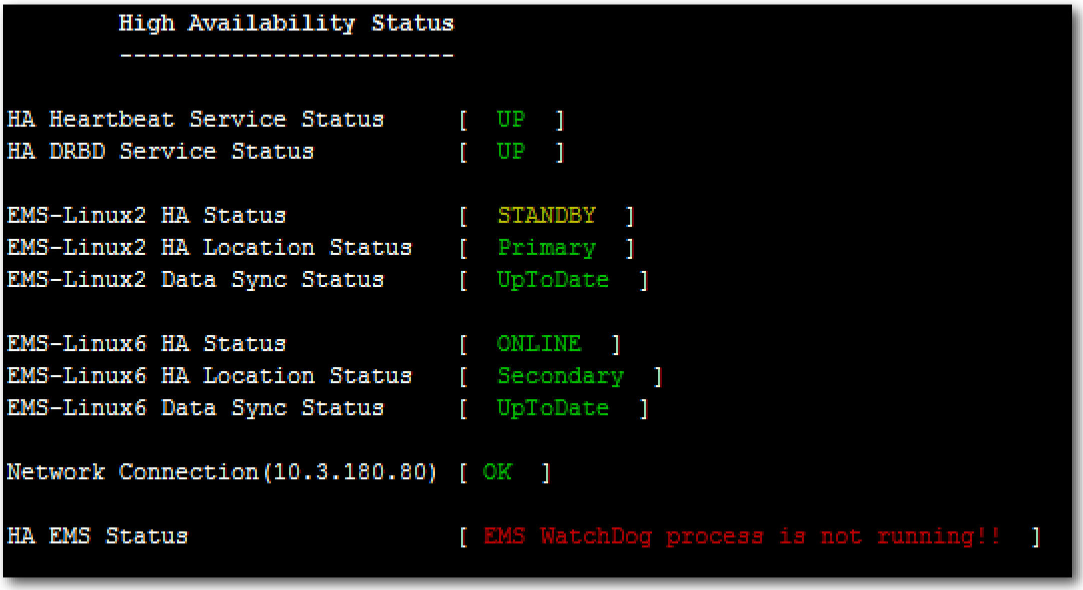


```
                EMS Server 7.2.126 Management
------------------------------------------------------------------------
Main Menu> Application Maintenance> High Availability
------------------------------------------------------------------------
        >1.HA Status
         2.HA Switchover
         3.Uninstall HS
         b.Back
         q.Quit to main Menu
```

2. Type **y** to confirm your selection.

   During the manual switchover process, the "switchover in process…" message is displayed in the EMS server machine where the command was activated. If you run the 'HA Status' command on the other server, it will display the HA status of the Primary server as STANDBY until the Secondary server becomes the Primary server.

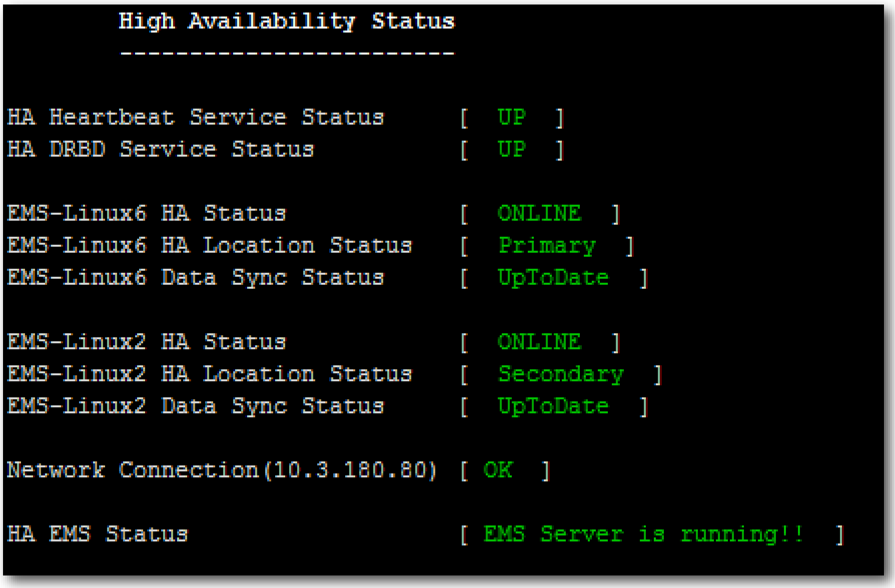
Figure 22-15: Switchover Status



```
        High Availability Status
        ------------------------

HA Heartbeat Service Status     [  UP  ]
HA DRBD Service Status          [  UP  ]

EMS-Linux2 HA Status            [  STANDBY  ]
EMS-Linux2 HA Location Status   [  Primary  ]
EMS-Linux2 Data Sync Status     [  UpToDate  ]

EMS-Linux6 HA Status            [  ONLINE  ]
EMS-Linux6 HA Location Status   [  Secondary  ]
EMS-Linux6 Data Sync Status     [  UpToDate  ]

Network Connection(10.3.180.80) [ OK  ]

HA EMS Status                   [ EMS WatchDog process is not running!!  ]
```

After the Secondary server becomes the Primary server, a few minutes are required until the EMS application is up and running.

Figure 22-16: Status after Switchover



```
        High Availability Status
        ------------------------

HA Heartbeat Service Status      [  UP  ]
HA DRBD Service Status           [  UP  ]

EMS-Linux6 HA Status             [  ONLINE  ]
EMS-Linux6 HA Location Status    [  Primary  ]
EMS-Linux6 Data Sync Status      [  UpToDate  ]

EMS-Linux2 HA Status             [  ONLINE  ]
EMS-Linux2 HA Location Status    [  Secondary  ]
EMS-Linux2 Data Sync Status      [  UpToDate  ]

Network Connection(10.3.180.80)  [ OK  ]

HA EMS Status                    [ EMS Server is running!!  ]
```

22.6 EMS HA Uninstall

The user should uninstall the EMS HA application on both the Primary and Secondary servers under the following circumstances:

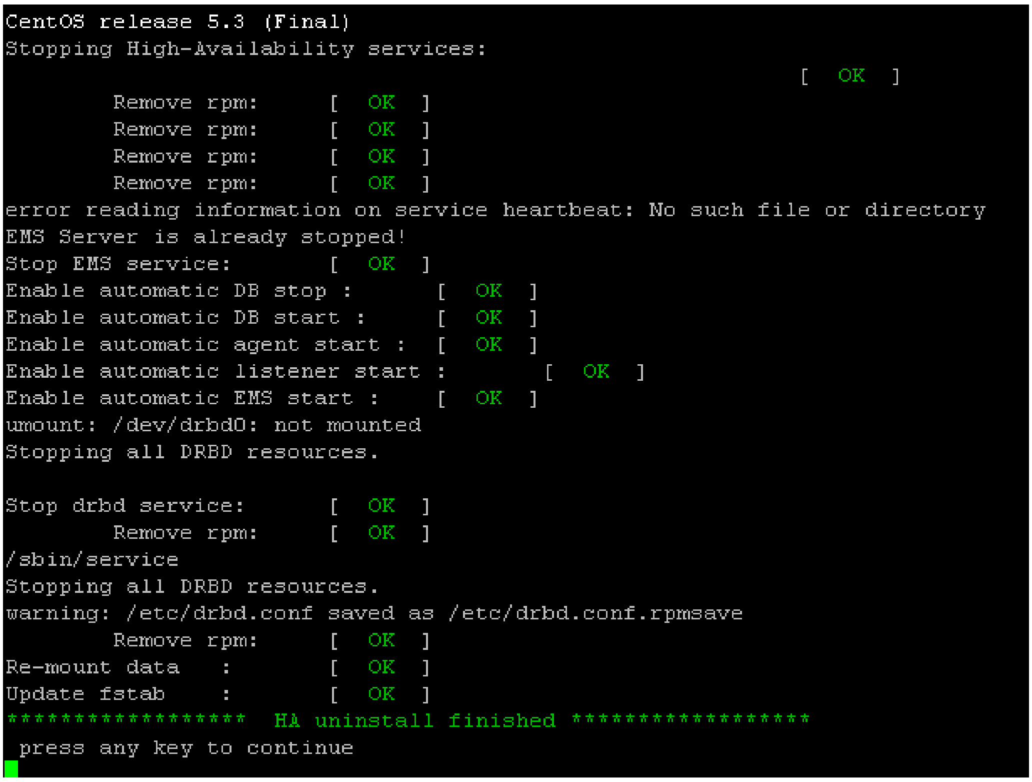
- EMS software version upgrade
- EMS server network configuration changes
- Custom certificate installations

➢ To uninstall EMS HA:

- In the High Availability menu, choose option **3** (**Uninstall HA**), and then press Enter.

The uninstall process takes 1-2 minutes with the following output:

Figure 22-17: Uninstall EMS HA Status Display



```
CentOS release 5.3 (Final)
Stopping High-Availability services:
                                                            [  OK  ]
        Remove rpm:      [  OK  ]
        Remove rpm:      [  OK  ]
        Remove rpm:      [  OK  ]
        Remove rpm:      [  OK  ]
error reading information on service heartbeat: No such file or directory
EMS Server is already stopped!
Stop EMS service:        [  OK  ]
Enable automatic DB stop :       [  OK  ]
Enable automatic DB start :      [  OK  ]
Enable automatic agent start :   [  OK  ]
Enable automatic listener start :        [  OK  ]
Enable automatic EMS start :     [  OK  ]
umount: /dev/drbd0: not mounted
Stopping all DRBD resources.

Stop drbd service:       [  OK  ]
        Remove rpm:      [  OK  ]
/sbin/service
Stopping all DRBD resources.
warning: /etc/drbd.conf saved as /etc/drbd.conf.rpmsave
        Remove rpm:      [  OK  ]
Re-mount data    :       [  OK  ]
Update fstab     :       [  OK  ]
******************  HA uninstall finished ******************
 press any key to continue
```

Note: The EMS application doesn’t start automatically after this process has completed. To start the EMS, reboot the EMS server or quit the EMS Server Manager and run it again using the 'Start EMS Server' option (see 16.1 on page 115).

This page is intentionally left blank.

Part VII

Configuring the Firewall and Installing the EMS Client

This part describes how to configure the EMS firewall and install the EMS client.

23 Configuring the Firewall

The EMS interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. You need to define firewall rules to secure communications for the OVOC client-server processes. Each of these processes use different communication ports. By default, all ports are open on the EMS server side. When installing the EMS server, you need to configure its network and open the ports in your Enterprise LAN according to your site requirements; based on the firewall configuration rules (representing these port connections) that are described in the table and figure below.

Table 23-1: Firewall Configuration Rules

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
EMS Clients and EMS Server					
EMS Client PC ↔ EMS Server	TCP	✓	22	SSH communication between EMS server and client PC. Initiator: client PC	EMS server side / Bi-directional.
	TCP	×	80	HTTP for JAWS. Initiator: client PC	
JAWS and NBIF Clients ↔ EMS Server	TCP	✓	443	HTTPS for PC client/ JAWS and NBIF. Initiator: Client	EMS server side / Bi-directional.
EMS Server ↔ Single Sign-on Connection to Device Web	TCP (HTTP)	×	8090	Direct HTTP connection between the device's embedded Web interface (Management PC) and the EMS server. Initiator: EMS Server	EMS server side / Bi-directional
	TCP (HTTPS)	✓	8091	Direct HTTPS connection between the device's embedded Web interface (Management PC) and the EMS server. Initiator: EMS Server	EMS server side / Bi-directional.

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
EMS Server and Devices					
Device ↔ EMS Server (SNMP)	UDP	✓	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Initiator: EMS server	EMS server side / Bi-directional
	UDP	✓	162	SNMP trap listening port on the EMS. Initiator: AudioCodes device	EMS server side / Receive only.
	UDP	✓	161	SNMP Trap Manager port on the device that is used to send traps to the EMS. Initiator: EMS server	MG side / Bi-directional
Device↔ EMS Server (NTP Server)	UDP (NTP server)	×	123	NTP server synchronization. Initiator: MG (and EMS Server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional
Device ↔ EMS Server (REST communication /upload/download)	TCP (HTTP)	×	80	HTTP connection for files transfer. Initiator: EMS server	EMS server side / Bi-directional
	TCP (HTTPS)	✓	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: EMS server	EMS server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Endpoints (IP Phones)					
EMS Server ↔ IP Phone Management Server	TCP (HTTP)	✗	80	HTTP connection between the EMS server and the IP Phone Management Server Web browser. Initiator: Client browser	EMS server side / Bi-Directional.
	TCP (HTTPS)	✓	443	HTTPS connection between the EMS server and the IP Phone Management Server Web browser. Initiator: Client browser	EMS server side / Bi-Directional.
				HTTPS connection used by endpoints for downloading firmware and configuration files from the EMS server. Initiator: Endpoints	
EMS Server ↔ Endpoints (IP Phones)	HTTP	✗	8080	HTTP connection that is used by endpoints for downloading firmware and configuration files from the EMS server. Initiator: Endpoint	EMS server side / Bi-directional

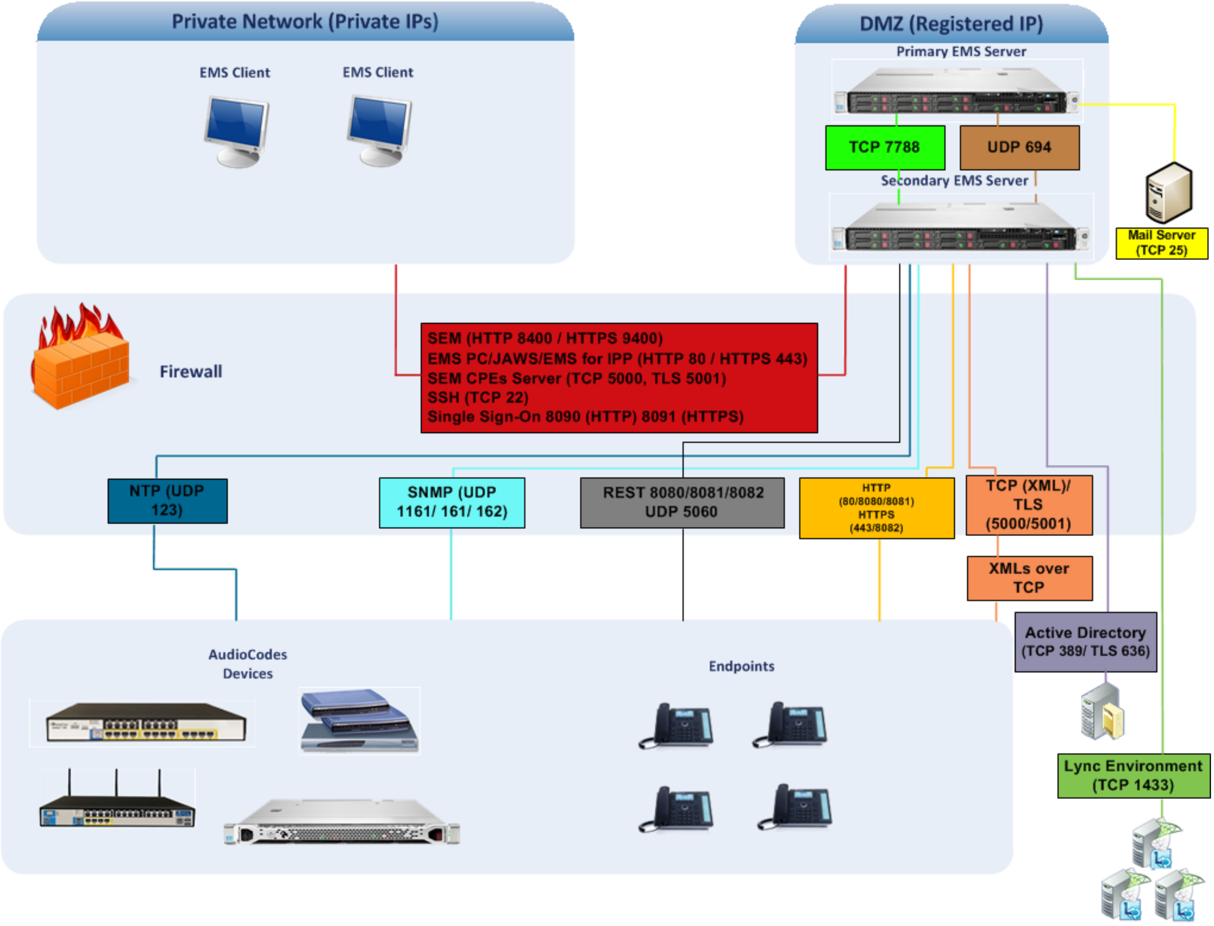
Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	TCP (HTTP)	✗	8081	HTTP connection used for sending REST updates from the endpoints to the EMS server, such as alarms and statuses. Initiator: Endpoint	EMS server side / Bi-directional
	TCP (HTTPS)	✓	8082	HTTPS connection used for sending secure REST updates from the IP phone to the EMS server, such as alarms and statuses (SSL authentication without certificate).	EMS server side / Bi-directional
SEM Server and Devices					
Media Gateways ↔ SEM server	TCP	✗	5000	XML based SEM communication. Initiator: Media Gateway	EMS server side / Bi-directional
	TCP (TLS)	✓	5001	XML based SEM TLS secured communication. Initiator: Media Gateway	EMS server side / Bi-directional
SEM Client					
SEM client ↔ Tomcat server	TCP (HTTP)	✗	8400	SEM HTTP connection between the user's browser and Tomcat server. Initiator: Client's PC.	EMS server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	TCP (HTTPS)	✓	9400	SEM HTTPS connection between the user's browser and Tomcat server. Initiator: Client.	EMS server side / Bi-directional
MS-SQL Server					
SEM server ↔ Lync MS-SQL Server	TCP	✓	1433	Connection between the EMS server and the MS-SQL Lync server. This port should be configured with SSL. Initiator: EMS server	Lync SQL server side / Bi-directional
LDAP Active Directory Server					
SEM server ↔ Active Directory LDAP server (Microsoft Lync user authentication with SEM)	TCP	×	389	Connection between the SEM server and the Active Directory LDAP server. Initiator: EMS server	Active Directory server side/ Bi-directional
	TCP (TLS)	✓	636	Connection between the SEM server and the Active Directory LDAP server with SSL configured. Initiator: EMS server	Active Directory server side/ Bi-directional
EMS server ↔ Active Directory LDAP Server (EMS user authentication)	TCP	×	389	Connection between the EMS server and the Active Directory LDAP server (EMS Users). Initiator: EMS server	Active Directory server side/ Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	TCP (TLS)	✓	636	Connection between the EMS server and the Active Directory LDAP server (EMS Users) with SSL configured. Initiator: EMS server	Active Directory server side/ Bi-directional
RADIUS Server					
EMS server ↔ RADIUS server	TCP	×	1812	Direct connection between the EMS server and the RADIUS server (when EMS user is authenticated using RADIUS server). Initiator: EMS server	EMS server side / Bi-directional
EMS HA					
Primary EMS Server ↔ Secondary EMS Server (HA Setup)	TCP	×	7788	Database replication between the servers. Initiator: Both servers	Both EMS servers / Bi-directional
	UDP	×	694	Heartbeat packets between the servers. Initiator: Both servers	
Mail and Syslog Servers					
EMS server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server Initiator: EMS server	Mail server side / Bi-directional
EMS server ↔ Syslog Server	TCP	×	514	Trap Forwarding to Syslog server. Initiator: EMS server	Syslog server side /Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
RFC 6035					
SEM Server ↔ Endpoints	UDP	✗	5060	SIP Publish reports sent to the SEM server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics. Initiator: Endpoint	SEM server / Bi-directional

Figure 23-1: Firewall Configuration Schema


Private Network (Private IPs)
EMS Client
EMS Client
DMZ (Registered IP)
Primary EMS Server
TCP 7788
UDP 694
Secondary EMS Server
Mail Server (TCP 25)
Firewall
SEM (HTTP 8400 / HTTPS 9400)
EMS PC/JAWS/EMS for IPP (HTTP 80 / HTTPS 443)
SEM CPEs Server (TCP 5000, TLS 5001)
SSH (TCP 22)
Single Sign-On 8090 (HTTP) 8091 (HTTPS)
NTP (UDP 123)
SNMP (UDP 1161/ 161/ 162)
REST 8080/8081/8082 UDP 5060
HTTP (80/8080/8081) HTTPS (443/8082)
TCP (XML)/ TLS (5000/5001)
XMLs over TCP
Active Directory (TCP 389/ TLS 636)
Lync Environment (TCP 1433)
AudioCodes Devices
Endpoints

Note: The above figure displays images of devices. For the full list of supported products, see Chapter 2 on page 21.

- NOC ↔ EMS (Server) ports

Table 23-2: OAM Flows: NOC ↔Device/ IP Phone/ SBA/ EMS

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
NOC/OSS	**Device/SBA/IP Phone/**EMS	SFTP	1024 - 65535	20
		FTP	1024 - 65535	21
		SSH	1024 - 65535	22
		Telnet	1024 - 65535	23
		NTP	123	123
		-	-	-
		HTTP/HTTPS	N/A	80,443

Table 23-3: OAM Flows: Device/ IP Phone/ SBA/ EMS↔ NOC

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
Device/IP Phone/ SBA/EMS	NOC/OSS	NTP	123	123
		SNMP Trap	1024 – 65535	162
		-	-	-

This page is intentionally left blank.

24 Installing the EMS Client

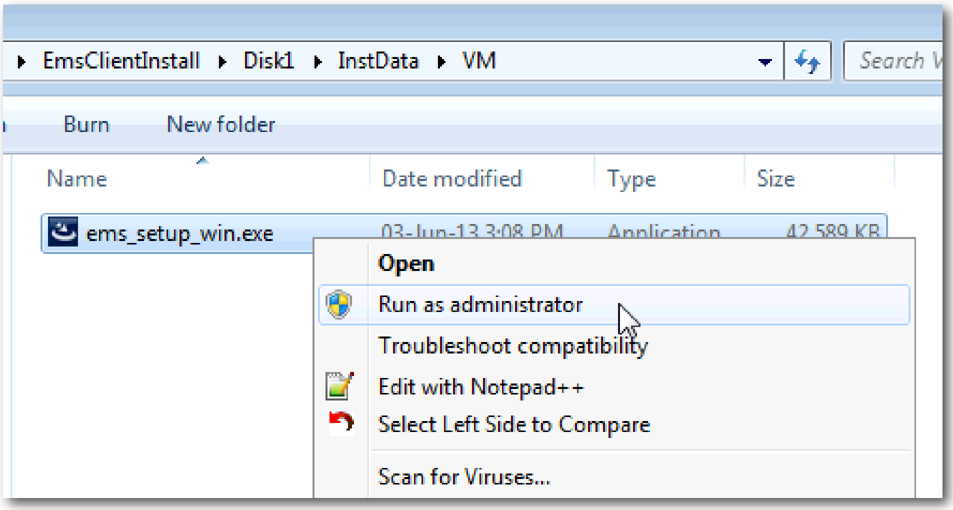
This section describes how to install the EMS Client on a PC or Laptop.

Note: Before you run the EMS Client exe file, ensure that you extract the entire Disk1 EMS client directory to your PC/laptop in the same relative path as the Disk image, and only then, run the exe file from this location.

➢ To install the EMS client on a PC or Laptop:

1. Insert AudioCodes' EMS installation disk into the CDROM.
2. Open the EmsClientInstall\Disk1\InstData\VM directory.
3. Do one of the following:
   - On **Windows 7**:
     a. Right-click the EMS client Installation file ac_ems_setup_win.exe, and then choose **Run as administrator**; the EMS client installation setup is displayed.
     b. Follow the prompts to install the EMS client.

Figure 24-1: EMS Client Installation-Run as Administrator

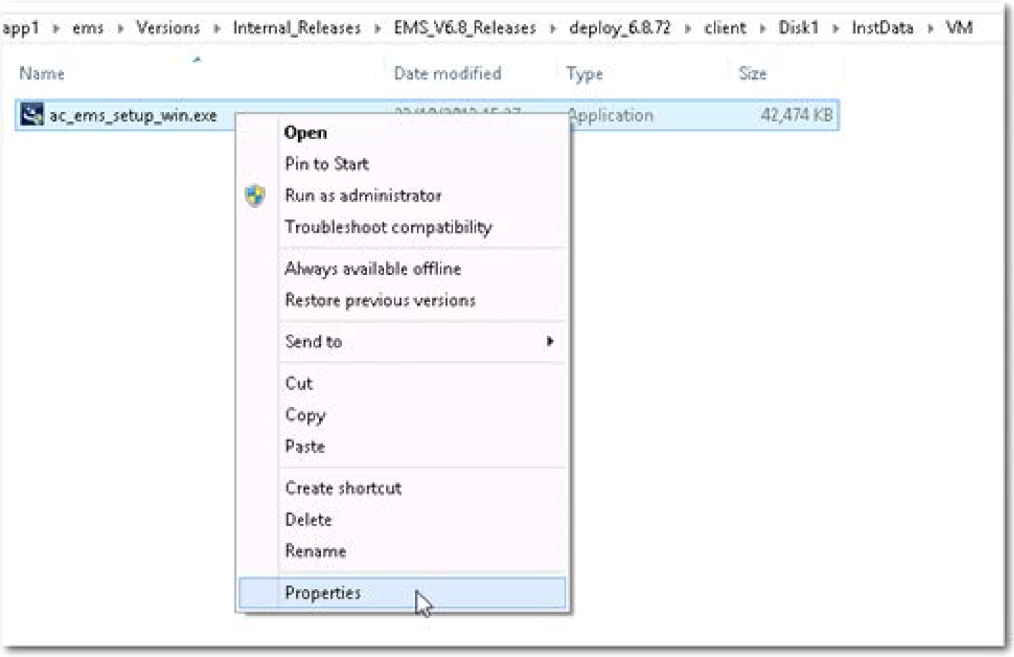


Upon the completion of the installation process, the EMS client icon is added to the desktop.

- On **Windows 8**:

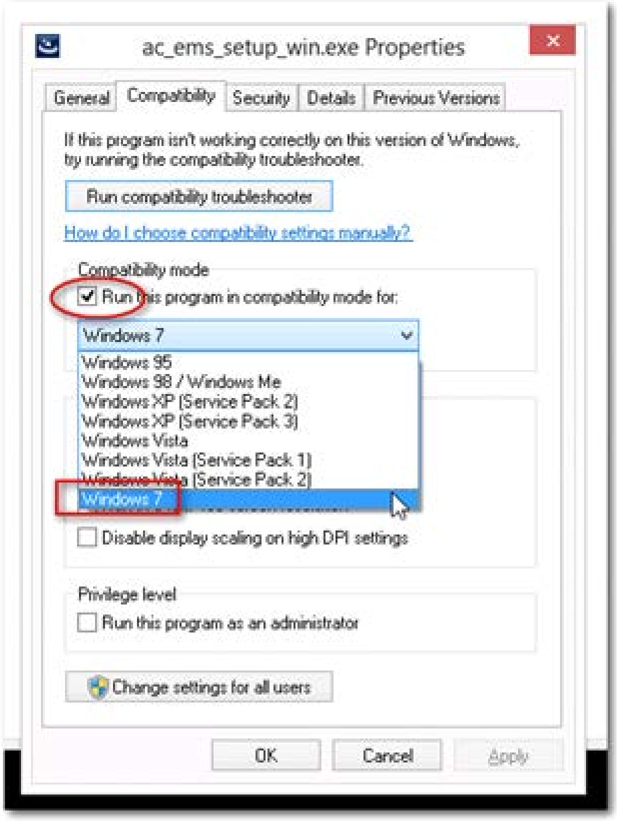
a. Right-click the installation exe file, and then choose **Properties**; the Properties window is displayed:

Figure 24-2: EMS Client Installation File-Windows 8 Properties



b. Select the **Compatibility** tab, and then select the checkbox **Run this program in compatibility mode for**.

Figure 24-3: EMS Client Installation File-Compatibility Tab



ac_ems_setup_win.exe Properties

If this program isn't working correctly on this version of Windows, try running the compatibility troubleshooter.

Compatibility mode

☑ Run this program in compatibility mode for:

Windows 7

□ Disable display scaling on high DPI settings

Privilege level

□ Run this program as an administrator

General
Compatibility
Security
Details
Previous Versions
Run compatibility troubleshooter
How do I choose compatibility settings manually?
Windows 95
Windows 98 / Windows Me
Windows XP (Service Pack 2)
Windows XP (Service Pack 3)
Windows Vista
Windows Vista (Service Pack 1)
Windows Vista (Service Pack 2)
Windows 7
Change settings for all users
OK
Cancel
Apply

c. In the Windows 7 pane, select **Windows 7**.

d. Click **OK**.

e. Right-click the EMS client installation file ac_ems_setup_win.exe, and then choose **Run as administrator**; the EMS client installation setup is displayed.

f. Follow the prompts to install the EMS client.

Upon the completion of the installation process, the EMS client icon is added to the desktop.

Note: If you have replaced the “AudioCodes-issued” certificates with external CA certificates, and wish to uninstall the previous EMS client, ensure that you backup the **clientNssDb** files: **cert8.db**, **key3.db**, and **secmod.db**.

24.1 Running the EMS Client on a PC or Laptop

This section describes how to run the EMS client on a PC or Laptop

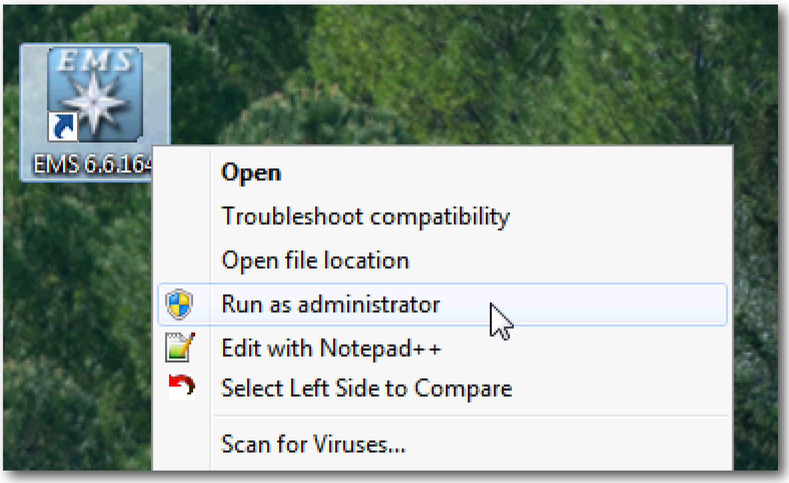
➢ To run the EMS on Windows XP or older:

- Double-click the EMS client icon on your desktop or run **Start** > **Programs** > **EMS Client**.

➢ To run the EMS on Windows 7 or later:

- Right-click the EMS client icon on your desktop, and then choose **Run as Administrator**.

Figure 24-4: Running EMS Client-Run as Administrator



24.2 Initial Login

This section describes how to initially login to the EMS client.

➢ To initially login to the EMS client:

1. Log in as user 'acladmin' with password 'pass_1234' or 'pass_12345'.

Note: First-time access defaults are case sensitive. After you login to the EMS for the first-time, you are prompted to change the default password. If you incorrectly define these or the field Server IP Address, a prompt is displayed indicating that the fields should be redefined correctly.

2. In the main screen, open the ‘Users List’ and add new users according to your requirements.

24.3 Installing and Running the EMS Client on a PC using Java Web Start (JAWS)

Java Web Start (JAWS) enables you to install the EMS client (compatible with your EMS server version) without using any CDs.

➢ To install the EMS client on a PC using JAWS:

1. Open a browser and type the EMS server IP in the Address field and add /jaws as suffix, for example:

   http://10.7.6.18/jaws/

2. Follow the online instructions.

➢ To run the EMS client after JAWS install through URL:

- Specify the path http://<server_ip>/jaws.

  An ‘EMS Login Screen’ is opened.

  For example: http://10.7.6.18/jaws/

This page is intentionally left blank.

Part VIII

Appendix

This part describes additional EMS server procedures.

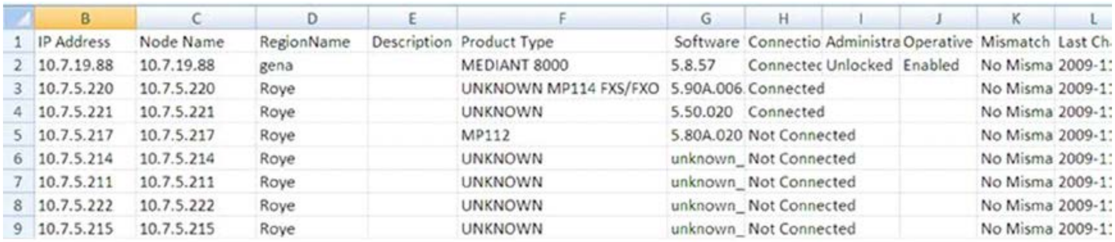
A Site Preparation

This appendix describes the procedures for backing up the EMS server.

Note: It is highly recommended to perform a complete backup of the EMS server prior to performing an installation or upgrade, according to the procedures described below.

- EMS server data backup should be performed prior to machine formatting. The Backup files should be transferred to another machine prior to the EMS server installation. Note, that these backup files cannot be used for other versions. They should be kept in case the user fails to install the new version, and decides to roll back to the previous version.
- EMS Users: all the users' names and permissions should be saved. After the new EMS version is installed, these users should be defined manually with default passwords. To perform this task, in the EMS menu, choose Security > User's List menu.
- EMS Tree: the user can export the gateways tree using the File > MGs Report command (example of the file is attached). This file is a CSV file and does not preserve secured information such as passwords. Therefore, we recommend extending it manually with columns including: SNMP read and write community strings, or SNMPv3 user details. This information will be required during the device's definition in the newly installed EMS system. It's also highly recommended to perform gateway removal and adding and to ensure that the EMS <-> GW connection has been established.

Figure A-1: Save MGs Tree Command



	B	C	D	E	F	G	H	I	J	K	L
1	IP Address	Node Name	RegionName	Description	Product Type	Software	Connectio	Administra	Operative	Mismatch	Last Ch
2	10.7.19.88	10.7.19.88	gena		MEDIANT 8000	5.8.57	Connectec	Unlocked	Enabled	No Misma	2009-1
3	10.7.5.220	10.7.5.220	Roye		UNKNOWN MP114 FXS/FXO	5.90A.006	Connected			No Misma	2009-1
4	10.7.5.221	10.7.5.221	Roye		UNKNOWN	5.50.020	Connected			No Misma	2009-1
5	10.7.5.217	10.7.5.217	Roye		MP112	5.80A.020	Not Connected			No Misma	2009-1
6	10.7.5.214	10.7.5.214	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1
7	10.7.5.211	10.7.5.211	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1
8	10.7.5.222	10.7.5.222	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1
9	10.7.5.215	10.7.5.215	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1

This page is intentionally left blank.

B EMS Application Acceptance Tests

This appendix describes the EMS Application Acceptance tests.

B.1 Introduction

The following series of tests are defined as acceptance tests for the EMS application and cover all the major areas and features of the application.

The tests should run sequentially as a single test with dependencies. For example, you can’t add a media gateway to the EMS before you have added a software file.

It is also recommended to integrate the below test plan in the Acceptance Test Plan (ATP) of the complete solution of which the EMS is a component. The ATP is typically developed by the solution integrator and covers all solution components (e.g. Softswitch, Media Gateway, IP routers etc). The ATP typically verifies “end to end” functionality, for example, the calls running through the solution. The below test plan should be integrated in the ATP as part of this “end to end” functionality testing (e.g. you may send and receive calls through the media gateway, perform media gateway board switchover and verify that calls are recovered on the redundant board).

Prior to running the tests described below, the tester should have a basic understanding of how to operate the product. Next to each test case there is a reference to the relevant chapter in the documentation. The tester should read these chapters to acquire the required tools to run this test. Running this test can also be considered as an excellent hand’s-on initial training session.

B.2 Configuration

This section describes the EMS application configuration acceptance tests.

B.2.1 Client Installation

Table B-1: Acceptance Test – Client Installation

Step Name	Description	Expected Result
Install	Install the client software	Verify that all the instructions are clear.

B.2.2 Server Installation

Table B-2: Acceptance Test – Server Installation

Step Name	Description	Expected Result
Server	Run the full procedure that installs the DB software, creates the DB, creates the schema and installs the EMS server.	The EMS server directory exists under /ACEMS.
Reboot	Reboot the EMS server	The EMS server starts automatically.
Connect	Connect to the EMS server with the EMS client	The connection should succeed.

B.2.3 Add Auxiliary File

Table B-3: Acceptance Test – Add Auxiliary File

Step Name	Description	Expected Result
Software Manager	Open the Software Manager Tools >> SW manager	The Software Manager window opens.
Auxiliary Tab	Choose the auxiliary tab	A new tab is opened with all the available auxiliary files.
Add Auxiliary File	Choose an auxiliary file that you usually work with such as: Call Progress Tone	A new file was added to the SW Manager.
Add file browser	Click the Add file Button (Plus sign)	Software File added to the Software Manager.

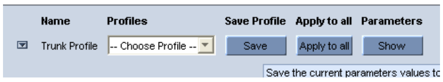
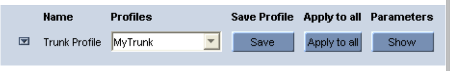
B.2.4 Add Media Gateway

Table B-4: Acceptance Test – Add MG

Step Name	Description	Expected Result
Add MG	Add MG to the EMS	The media gateway appears in the EMS GUI.
MG Status	Click on the Media Gateway	The Media Gateway status is available in the GUI, including all LEDS and boards.

B.2.5 Entity Profile – Digital CPE Devices

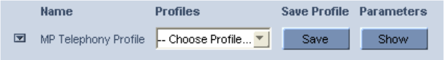
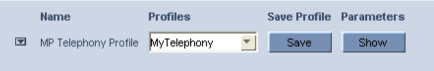
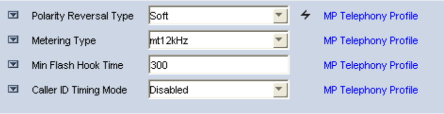
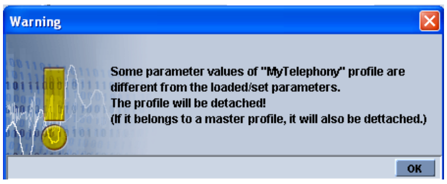
Table B-5: Acceptance Test – Entity Profile: Digital CPE Devices

Step Name	Description	Expected Result
Go to trunk level	Drill down to trunk level	Trunks list appears according to board type.
Trunk Properties	Open trunk#1 properties	The frame provisioning opens and all the parameters are available.
Trunk Configuration	Configure the trunk	The new set of values appears on the provisioning screen.
Apply	Apply the new configuration	Action successful and there were no errors and no purple tabs.
Save profile	Save the profile, choose an appropriate name.  Name Profiles Save Profile Apply to all Parameters Save Apply to all Show Trunk Profile -- Choose Profile -- Save the current parameters values tc	The new profile appears in the profiles list.  Name Profiles Save Profile Apply to all Parameters Save Apply to all Show Trunk Profile MyTrunk
Apply to All	Download this configuration easily to all trunks by using the apply to all	Open trunk#2 and verify the configuration is equal to trunk#1.

Note: Digital CPE devices include the following products: Mediant 500 MSBR, Mediant 500L MSBR, Mediant 600, Mediant 800B MSBR, Mediant 800B Gateway and E-SBC, Mediant 1000B MSBR, Mediant 1000B Gateway and E-SBC, Mediant 1000, Mediant 2000 and Mediant 3000.

B.2.6 Entity Profile – Analog CPE Devices

Table B-6: Acceptance Test – Analog CPE Devices

Step Name	Description	Expected Result
Go to telephony frame	Click on the telephony button	Telephony configuration is displayed.
Save profile	Save the profile, choose an appropriate name  Name · Profiles · Save Profile · Parameters MP Telephony Profile · -- Choose Profile... · Save · Show	The new profile is displayed in the profiles list.  Name · Profiles · Save Profile · Parameters MP Telephony Profile · MyTelephony · Save · Show
Expose profile parameters	Press on the “show profile parameters” button	All profiles parameters are marked with the profile name.  Polarity Reversal Type · Soft · MP Telephony Profile Metering Type · mt12kHz · MP Telephony Profile Min Flash Hook Time · 300 · MP Telephony Profile Caller ID Timing Mode · Disabled · MP Telephony Profile
Detach profile	Change one of the profile parameters, and then press **Apply**.	A detach profile pop up message is displayed.  Warning Some parameter values of "MyTelephony" profile are different from the loaded/set parameters. The profile will be detached! (If it belongs to a master profile, it will also be dettached.) OK

Note: Analog CPE devices include the following products: MediaPack, Mediant 600, Mediant 500 MSBR, Mediant 500L MSBR, Mediant 800B MSBR, Mediant 800B Gateway and E-SBC, Mediant 1000B MSBR; Mediant 1000B Gateway and E-SBC and Mediant 1000.

B.3 Faults

B.3.1 Alarm Receiver

Figure B-1: Alarm Receiver

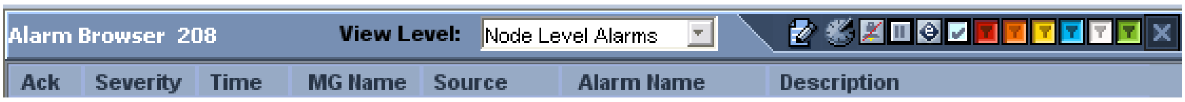


Table B-7: Acceptance Test – Alarm Receiver

Step Name	Description	Expected Result
Raise Alarm	Lock one of the elements in the MG, such as the trunk.	The alarm is received in the EMS.
Clear Alarm	Unlock one of the elements in the media gateway, such as a trunk.	The clear alarm is received in the EMS.

B.3.2 Delete Alarms

Table B-8: Acceptance Test – Delete Alarms

Step Name	Description	Expected Result
Delete Alarms	Right-click the alarms in the alarm browser and delete all the alarms	The alarm browser in empty.

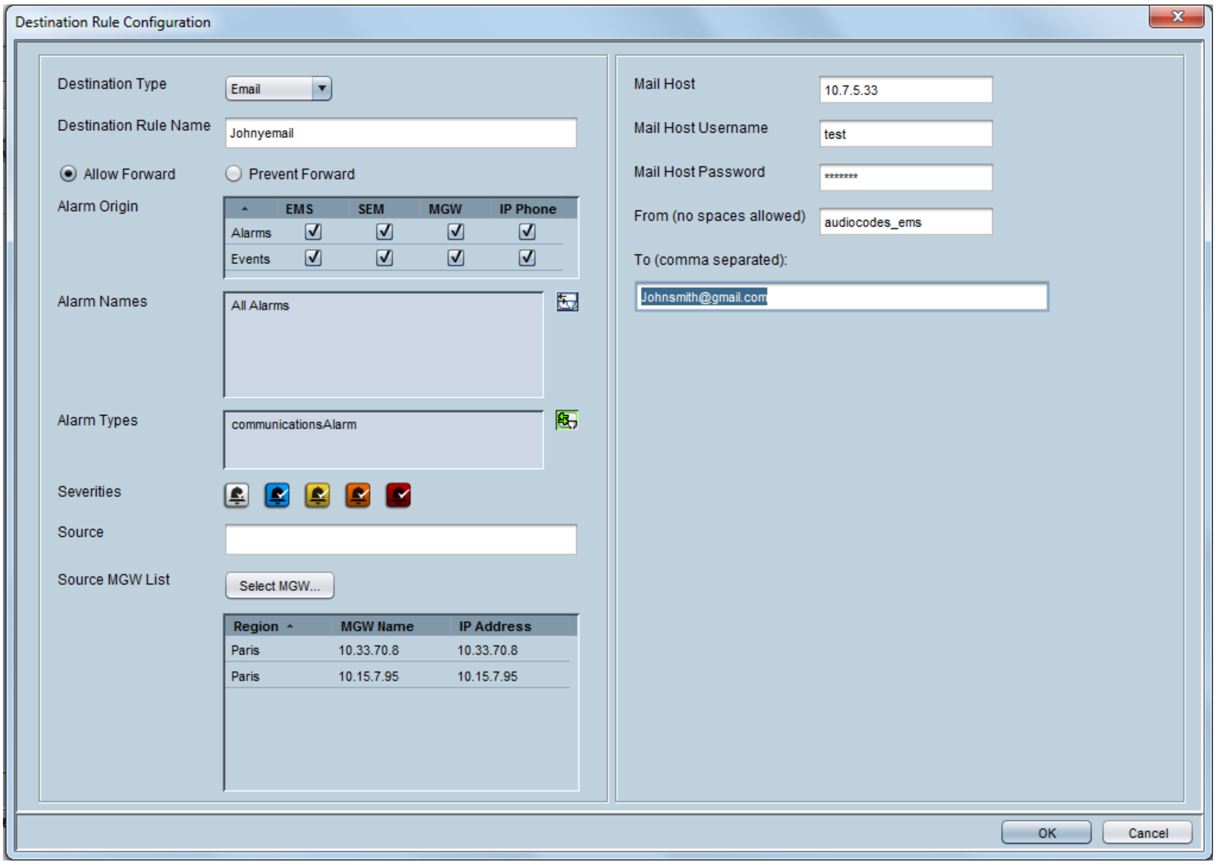
B.3.3 Acknowledge Alarm

Table B-9: Acceptance Test – Acknowledge Alarm

Step Name	Description	Expected Result
Check Box	Click on the Acknowledge check box	The alarm is marked as acknowledge.

B.3.4 Forwarding Alarms

Figure B-2: Destination Rule Configuration



Destination Rule Configuration

Destination Type: Email

Destination Rule Name: Johnyemail

● Allow Forward ○ Prevent Forward

Alarm Origin

	EMS	SEM	MGW	IP Phone
Alarms	☑	☑	☑	☑
Events	☑	☑	☑	☑

Alarm Names: All Alarms

Alarm Types: communicationsAlarm

Severities

Source:

Source MGW List: Select MGW...

Region	MGW Name	IP Address
Paris	10.33.70.8	10.33.70.8
Paris	10.15.7.95	10.15.7.95

Mail Host: 10.7.5.33

Mail Host Username: test

Mail Host Password: *******

From (no spaces allowed): audiocodes_ems

To (comma separated): Johnsmith@gmail.com

Table B-10: Acceptance Test – Forwarding Alarms

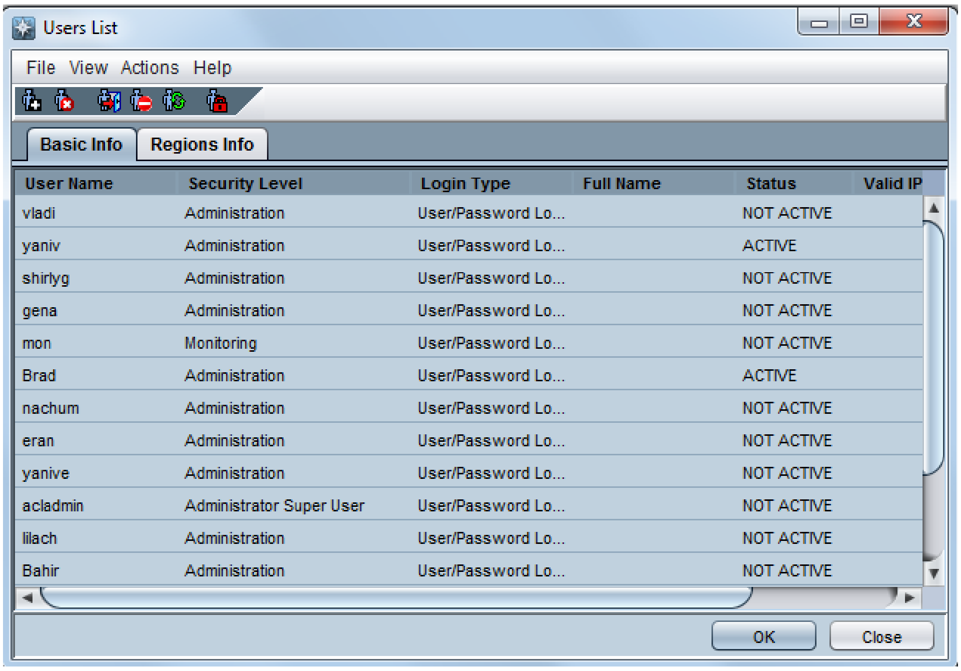
Step Name	Description	Expected Result
IP	Enable the Alarm Forwarding feature Tools >> trap configuration Add rule	Verify that you receive the Traps in the requested IP address on port 162.
Port	Change the Port number	Verify that you receive the Traps in the requested IP address on the new port.

B.4 Security

This section describes the EMS application security tests.

B.4.1 Users List

Figure B-3: Users List



User Name	Security Level	Login Type	Full Name	Status	Valid IP
vladi	Administration	User/Password Lo...		NOT ACTIVE	
yaniv	Administration	User/Password Lo...		ACTIVE	
shirlyg	Administration	User/Password Lo...		NOT ACTIVE	
gena	Administration	User/Password Lo...		NOT ACTIVE	
mon	Monitoring	User/Password Lo...		NOT ACTIVE	
Brad	Administration	User/Password Lo...		ACTIVE	
nachum	Administration	User/Password Lo...		NOT ACTIVE	
eran	Administration	User/Password Lo...		NOT ACTIVE	
yanive	Administration	User/Password Lo...		NOT ACTIVE	
acladmin	Administrator Super User	User/Password Lo...		NOT ACTIVE	
lilach	Administration	User/Password Lo...		NOT ACTIVE	
Bahir	Administration	User/Password Lo...		NOT ACTIVE	

Table B-11: Acceptance Test – Add an Operator

Step Name	Description	Expected Result
Add	Add a new operator, and then press the OK key in the screen.	Verify the new operator was added to the operators table frame.

B.4.2 Non Repetitive Passwords

Table B-12: Acceptance Test – Non Repetitive Passwords

Step Name	Description	Expected Result
Change password	Change password and try to enter the old password.	The old password is not valid. The password has been used before, please choose another one."

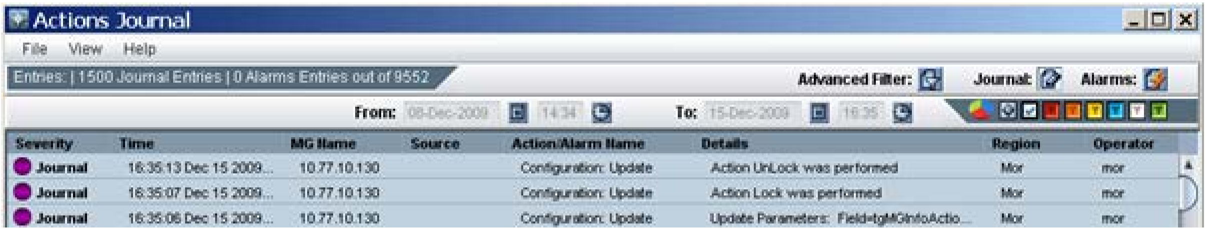
B.4.3 Removing Operator

Table B-13: Acceptance Test – Removing Operator

Step Name	Description	Expected Result
Remove	Remove a user from the operators table by selecting the remove button in the operators table.	A pop up window prompts you whether you wish to remove the user.
Verify	Select the **OK** button.	Verify that the user you selected was removed from the operators table.

B.4.4 Journal Activity

Figure B-4: Actions Journal



Entries: | 1500 Journal Entries | 0 Alarms Entries out of 9552

From: 08-Dec-2009 14:34 To: 15-Dec-2009 16:35

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator
Journal	16:35:13 Dec 15 2009...	10.77.10.130		Configuration: Update	Action UnLock was performed	Mor	mor
Journal	16:35:07 Dec 15 2009...	10.77.10.130		Configuration: Update	Action Lock was performed	Mor	mor
Journal	16:35:06 Dec 15 2009...	10.77.10.130		Configuration: Update	Update Parameters: Field=tgMGInfoActio...	Mor	mor

Table B-14: Acceptance Test – Journal Activity

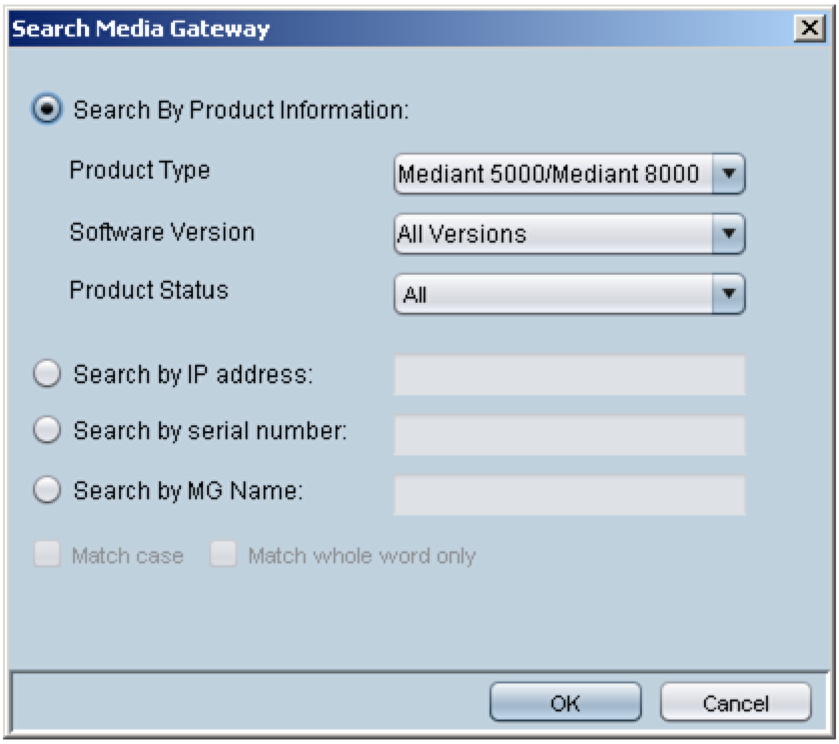
Step Name	Description	Expected Result
Activity	Open the action journal.	Check that all actions that you performed until now are registered.
Filter	Use the filter: time, user and action.	Time, user, action filter are working OK.

B.5 Utilities

This section describes the EMS application utilities acceptance tests.

B.5.1 MG Search

Figure B-5: Media Gateway Search



Search Media Gateway

● Search By Product Information:

Product Type: Mediant 5000/Mediant 8000

Software Version: All Versions

Product Status: All

○ Search by IP address:

○ Search by serial number:

○ Search by MG Name:

□ Match case □ Match whole word only

Table B-15: Acceptance Test – MG Search

Step Name	Description	Expected Result
Search Box	Open the MG search dialog by choosing Tools >> Search MG in the EMS Main menu.	Search MG tool opens.
IP	Search /MG/Unknown machine by IP address.	Displays a dialog with a list of results according to selected criteria.
Serial Number	Search /MG/Unknown machine by serial number.	Displays a dialog with a list of results according to selected criteria.
MG Name	Search /MG/Unknown machine by MG Name.	Displays a dialog with a list of results according to selected criteria.
Additional Search Options	Search /MG/Unknown machine by matching case or by matching a whole word.	Displays a dialog with a list of results according to selected criteria.

B.5.2 Online Help

Table B-16: Acceptance Test – Online Help

Step Name	Description	Expected Result
Alarms	Select one alarm and verify that the help opens in the correct context in the online help	Relevant information, clear and user friendly.
Status	Stand on one MG status screen and open the online help	Relevant information, clear and user friendly.
Provisioning	Stand on one tab in the provisioning windows and open the online help	Relevant information, clear and user friendly.

B.5.3 Backup and Recovery

Table B-17: Acceptance Test – Backup and Recovery

Step Name	Description	Expected Result
Backup	Create backup file in the EMS server according to the EMS Installation & Maintenance manual	A backup will be created in the same folder.
Recovery	Perform recovery on the new machine according to the EMS Installation & Maintenance manual	The new server is identical to the previous server.

C Configuring RAID-0 for AudioCodes EMS on HP ProLiant DL360p Gen8 Servers

This appendix describes the required equipment and the steps for configuring the HP ProLiant server to support RAID-0 Disk Array configuration for the EMS server installation.

Note: This procedure erases any residual data on the designated disk drives.

C.1 Prerequisites

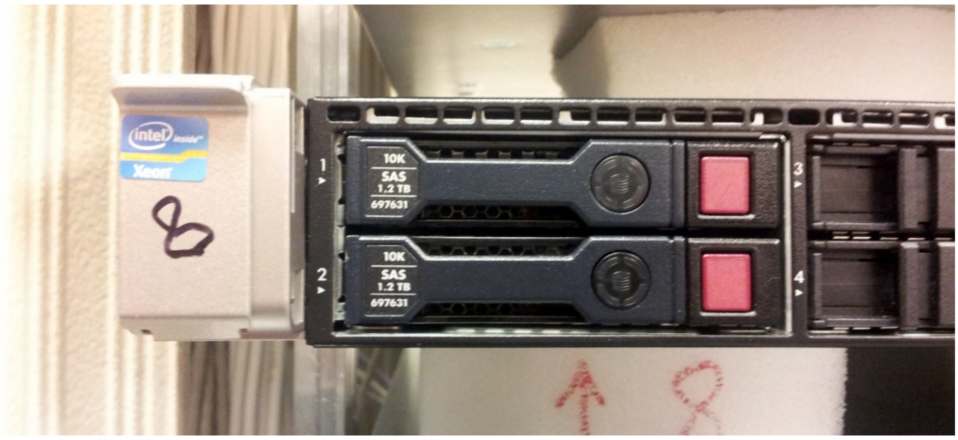
This procedure requires the following:

- ProLiant DL360p Gen8 server pre-installed in a compatible rack and connected to power.
- Two 1.2TB SAS disk drives
- A VGA display, USB keyboard, and USB mouse must be connected to the server back I/O panel.

C.2 Hardware Preparation

Make sure that two 1.2TB SAS disk drives are installed on slot 1 and 2 of the server. If required, refer to the *HP Service Manual*.

Figure C-1: Hardware Preparation



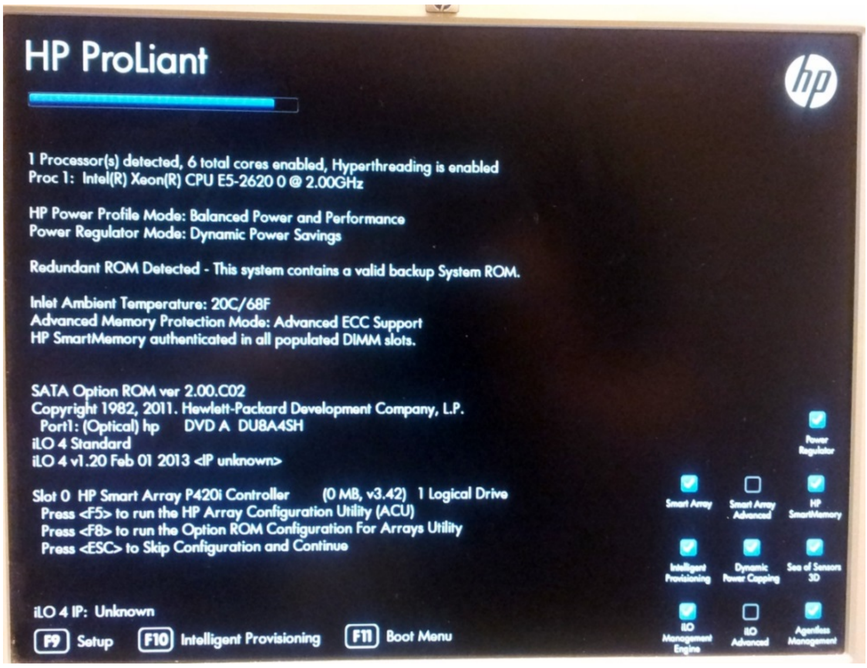
C.3 Configuring RAID-0

This procedure describes how to configure RAID-0 using the HP Array Configuration Utility (ACU).

➢ To configure RAID-0:

1. Power up the server. If the server is already powered up and running, use the 'reboot' command (from system console as user root) to reboot the server.
2. While the server is powering up, monitor the server and wait for the following screen:

Figure C-2: HP Array Configuration Utility (ACU)

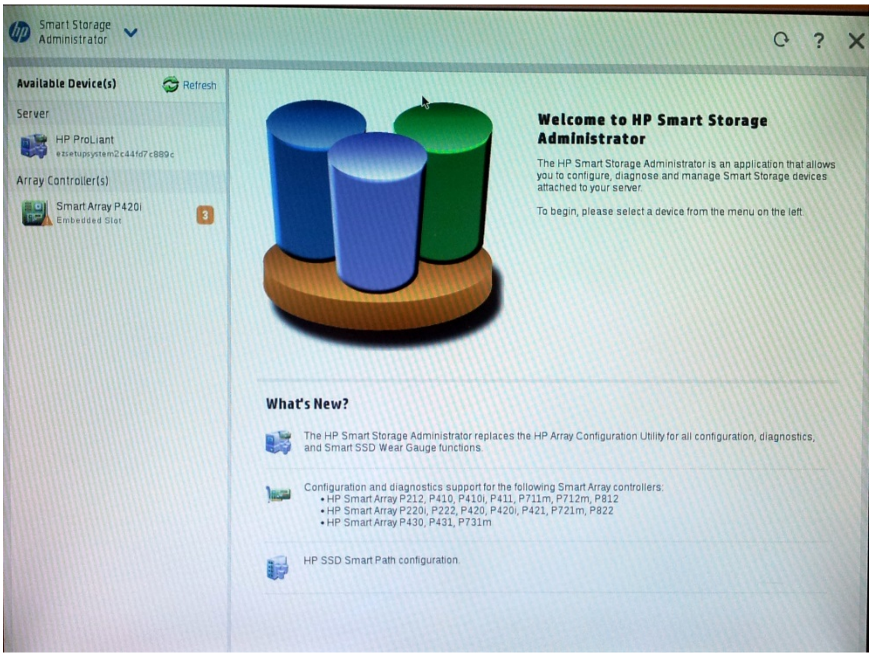


```
HP ProLiant

1 Processor(s) detected, 6 total cores enabled, Hyperthreading is enabled
Proc 1:  Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz

HP Power Profile Mode: Balanced Power and Performance
Power Regulator Mode: Dynamic Power Savings

Redundant ROM Detected - This system contains a valid backup System ROM.

Inlet Ambient Temperature: 20C/68F
Advanced Memory Protection Mode: Advanced ECC Support
HP SmartMemory authenticated in all populated DIMM slots.


SATA Option ROM ver 2.00.C02
Copyright 1982, 2011. Hewlett-Packard Development Company, L.P.
 Port1: (Optical) hp     DVD A  DU8A4SH
iLO 4 Standard
iLO 4 v1.20 Feb 01 2013 <IP unknown>

Slot 0  HP Smart Array P420i Controller      (0 MB, v3.42)  1 Logical Drive
 Press <F5> to run the HP Array Configuration Utility (ACU)
 Press <F8> to run the Option ROM Configuration For Arrays Utility
 Press <ESC> to Skip Configuration and Continue


iLO 4 IP:  Unknown
```

3. Press <**F5**> to run the HP Array Configuration Utility (ACU).
4. Wait for the ACU to finish loading.

When the ACU is ready, the following screen is displayed:

Figure C-3: RAID-Latest Firmware Versions



Welcome to HP Smart Storage Administrator

The HP Smart Storage Administrator is an application that allows you to configure, diagnose and manage Smart Storage devices attached to your server.

To begin, please select a device from the menu on the left.

The HP Smart Storage Administrator replaces the HP Array Configuration Utility for all configuration, diagnostics, and Smart SSD Wear Gauge functions.

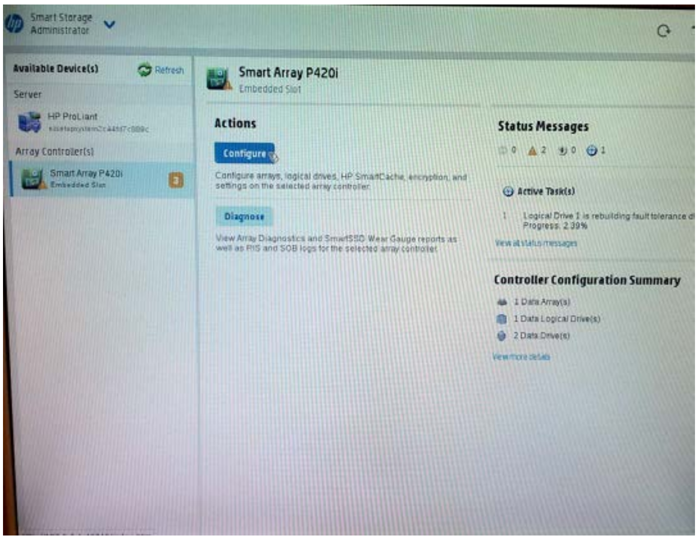
Configuration and diagnostics support for the following Smart Array controllers:

- HP Smart Array P212, P410, P410i, P411, P711m, P712m, P812
- HP Smart Array P220i, P222, P420, P420i, P421, P721m, P822
- HP Smart Array P430, P431, P731m

HP SSD Smart Path configuration.

5. In the left-hand pane, select **Smart Array P420i**; an Actions menu is displayed:

Figure C-4: Actions Menu



Configure arrays, logical drives, HP SmartCache, encryption, and settings on the selected array controller.

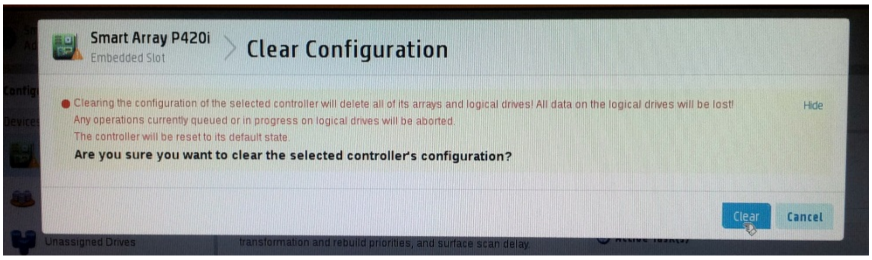
View Array Diagnostics and SmartSSD Wear Gauge reports as well as RIS and SOB logs for the selected array controller.

1 Logical Drive 1 is rebuilding fault tolerance d
Progress: 2.39%

1 Data Array(s)
1 Data Logical Drive(s)
2 Data Drive(s)

6. Click **Configure**, and then click **Clear Configuration** to clear any previous configuration; the following confirmation is displayed:

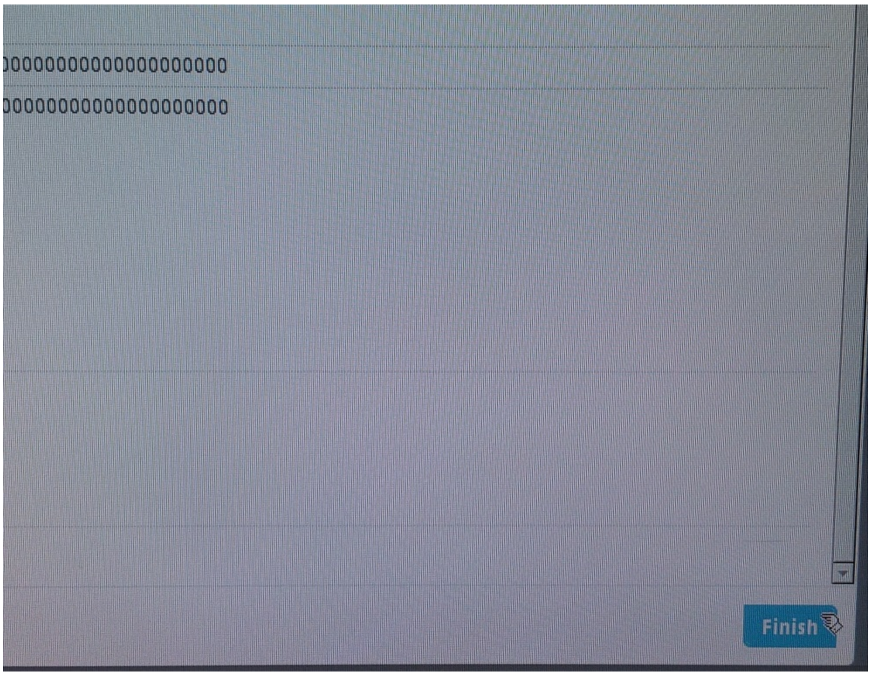
Figure C-5: Clear Configuration



● Clearing the configuration of the selected controller will delete all of its arrays and logical drives! All data on the logical drives will be lost!
Any operations currently queued or in progress on logical drives will be aborted.
The controller will be reset to its default state.
Are you sure you want to clear the selected controller's configuration?

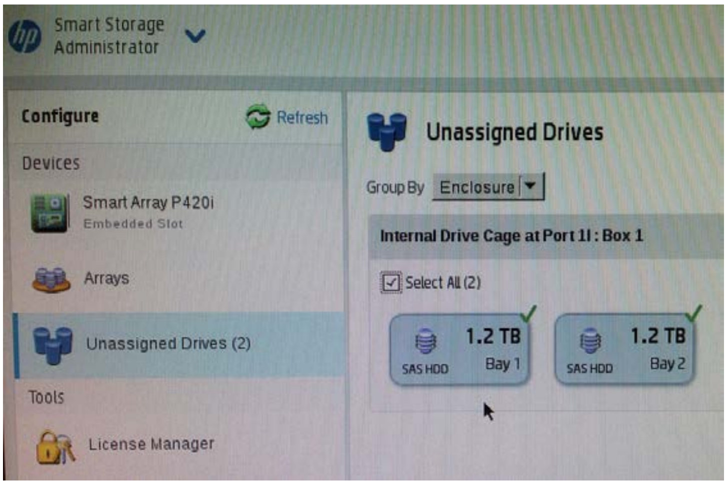
7. Click **Clear** to confirm; a summary display appears:

Figure C-6: Summary Screen



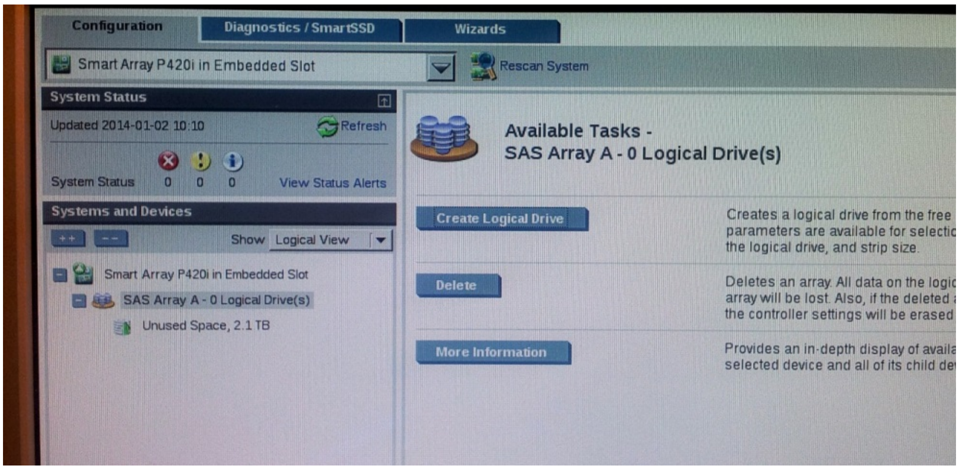
8. Click **Finish** to return to the main menu. The following screen is displayed:

Figure C-7: Main Screen



9. In the left-hand pane, select **Unassigned Drives (2)**; make sure that both the drives are selected, and then click **Create Array**.
10. Select **RAID 0** for RAID Level.
11. Select the 'Custom Size' check box, and then enter **2000 GiB**.
12. At the bottom of the screen, click **Create Logical Drive**; the following screen is displayed:

Figure C-8: Logical Drive



Updated 2014-01-02 10:10

System Status 0 0 0

Creates a logical drive from the free parameters are available for selectic the logical drive, and strip size.

Deletes an array. All data on the logic array will be lost. Also, if the deleted the controller settings will be erased

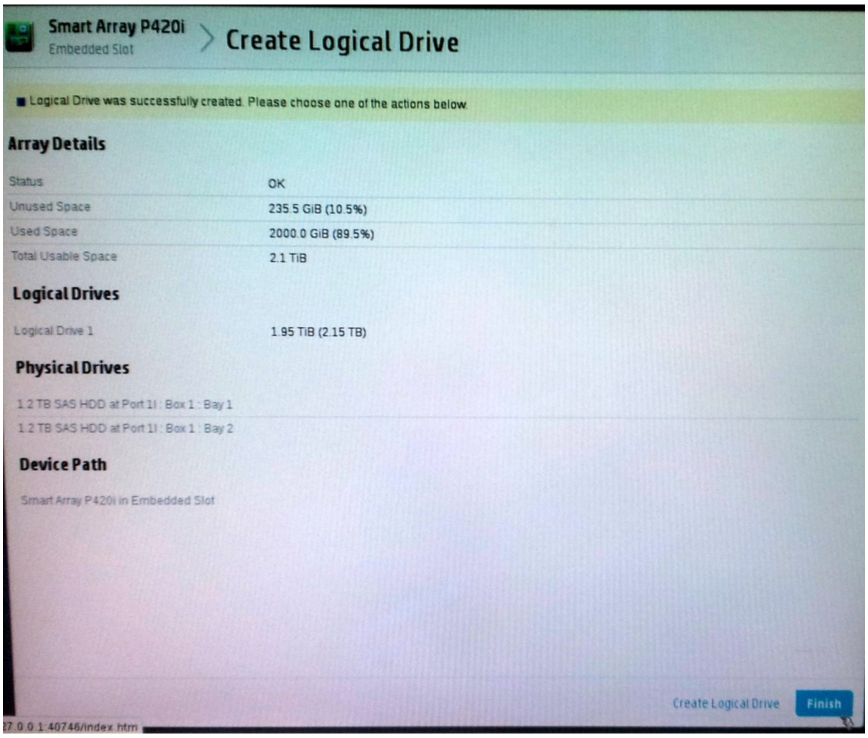
Provides an in-depth display of availa selected device and all of its child de

After the array is created, a logical drive should be created.

13. Click **Create Logical Drive**.

A summary screen is displayed:

Figure C-9: Summary Screen



Smart Array P420i
Embedded Slot

Create Logical Drive

Logical Drive was successfully created. Please choose one of the actions below.

Array Details

Status	OK
Unused Space	235.5 GiB (10.5%)
Used Space	2000.0 GiB (89.5%)
Total Usable Space	2.1 TiB

Logical Drives

Logical Drive 1	1.95 TiB (2.15 TB)

Physical Drives

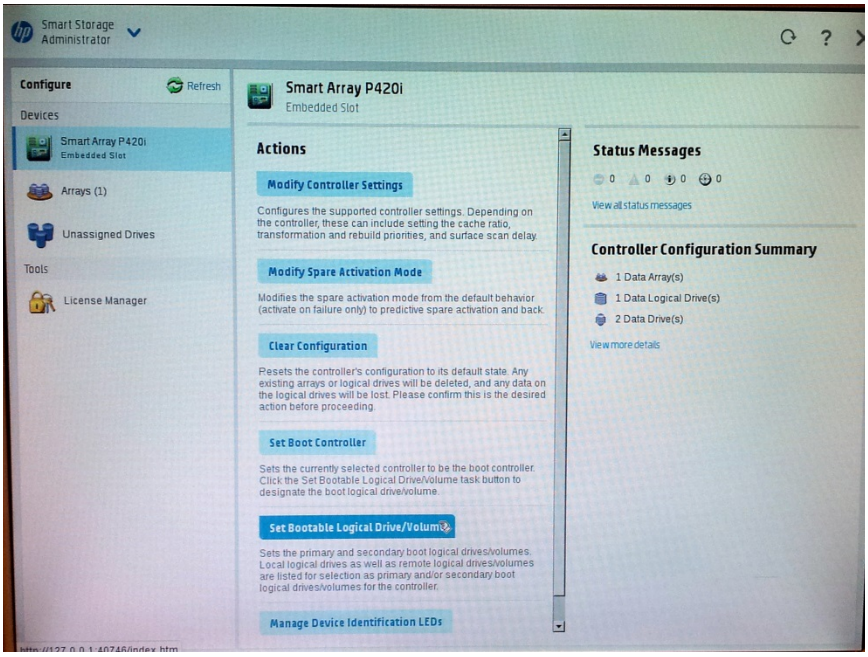
1.2 TB SAS HDD at Port 1I : Box 1 : Bay 1
1.2 TB SAS HDD at Port 1I : Box 1 : Bay 2

Device Path

Smart Array P420i in Embedded Slot

14. Click **Finish**.

Figure C-10: Set Bootable Logical Drive/Volume



Actions

Modify Controller Settings

Configures the supported controller settings. Depending on the controller, these can include setting the cache ratio, transformation and rebuild priorities, and surface scan delay.

Modify Spare Activation Mode

Modifies the spare activation mode from the default behavior (activate on failure only) to predictive spare activation and back.

Clear Configuration

Resets the controller's configuration to its default state. Any existing arrays or logical drives will be deleted, and any data on the logical drives will be lost. Please confirm this is the desired action before proceeding.

Set Boot Controller

Sets the currently selected controller to be the boot controller. Click the Set Bootable Logical Drive/Volume task button to designate the boot logical drive/volume.

Set Bootable Logical Drive/Volume

Sets the primary and secondary boot logical drives/volumes. Local logical drives as well as remote logical drives/volumes are listed for selection as primary and/or secondary boot logical drives/volumes for the controller.

Manage Device Identification LEDs

Status Messages

0 0 0 0

View all status messages

Controller Configuration Summary

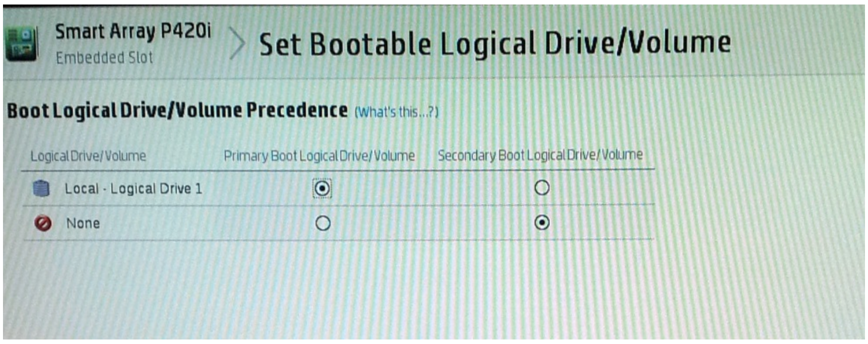
1 Data Array(s)
1 Data Logical Drive(s)
2 Data Drive(s)

View more details

The new logical volume needs to be set as a bootable volume.

15. In the left-hand pane, select **Smart Array P420i**, and then click **Set Bootable Logical Drive/Volume**; the following screen is displayed:

Figure C-11: Set Bootable Logical Drive/Volume



Boot Logical Drive/Volume Precedence (What's this...?)

Logical Drive/Volume	Primary Boot Logical Drive/Volume	Secondary Boot Logical Drive/Volume
Local - Logical Drive 1	◉	○
None	○	◉

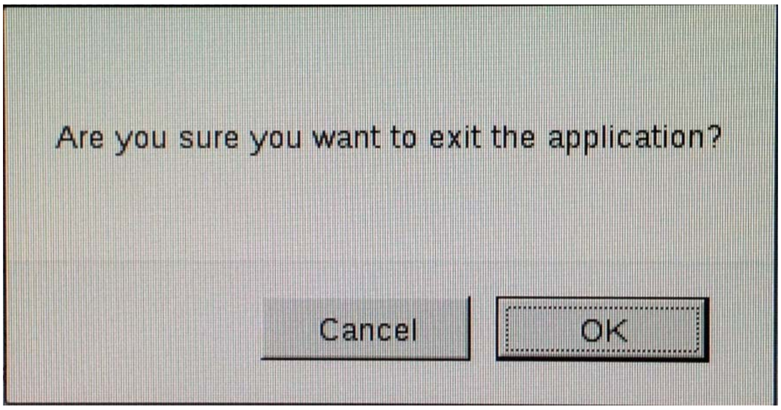
16. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.

A summary window is displayed.

17. Click **Finish**.

18. Exit the ACU by clicking the **X** sign on the top right-hand side of the screen, and then confirm the following dialog:

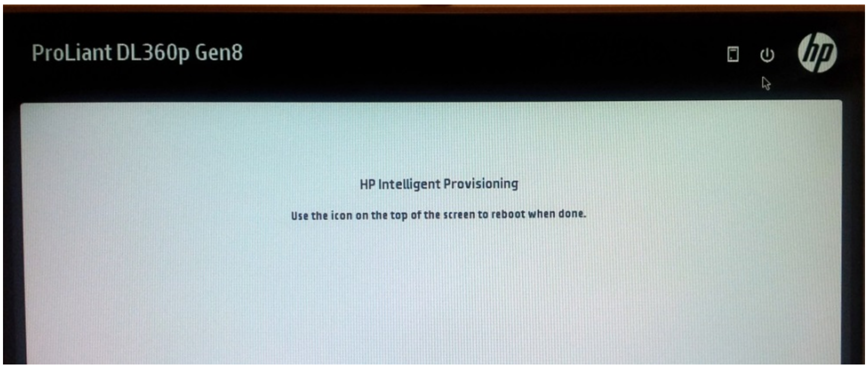
Figure C-12: Exit Application



Are you sure you want to exit the application?

19. Click **Exit ACU** at the bottom left-hand corner of the screen; the following screen is displayed:

Figure C-13: Power Button



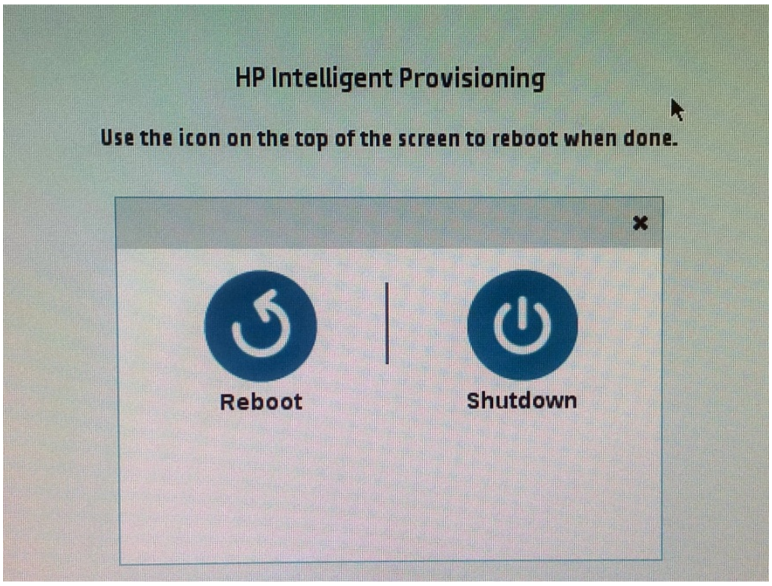
HP Intelligent Provisioning

Use the icon on the top of the screen to reboot when done.

20. Click the **Power** icon in the upper right-hand corner of the screen.

    The following screen is displayed:

Figure C-14: Reboot Button



HP Intelligent Provisioning

Use the icon on the top of the screen to reboot when done.

21. Click **Reboot** to reboot the server.

    The Disk Array configuration is now complete.

22. Install the EMS server installation (see Section 6.2 on page 37).

D Managing Clusters

This appendix describes how to manually migrate or move EMS VMs to another cluster node.

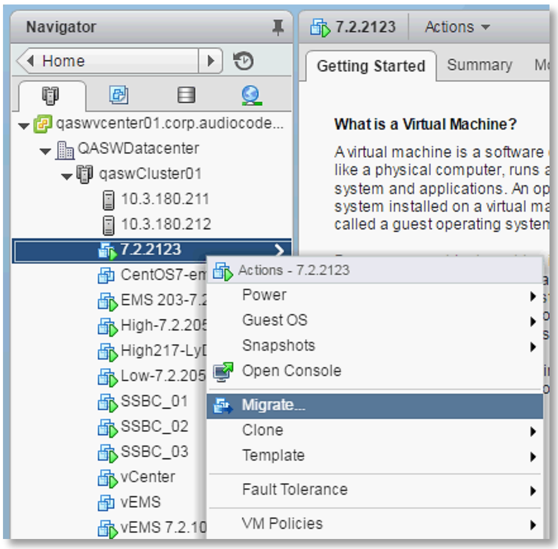
D.1 Migrating EMS Virtual Machines in a VMware Cluster

This section describes how to migrate your EMS Virtual Machine from one ESXi host to another.

➢ To migrate your EMS VM:

1. Select the EMS VM that you wish to migrate and then choose the **Migrate** option:

Figure D-1: Migration

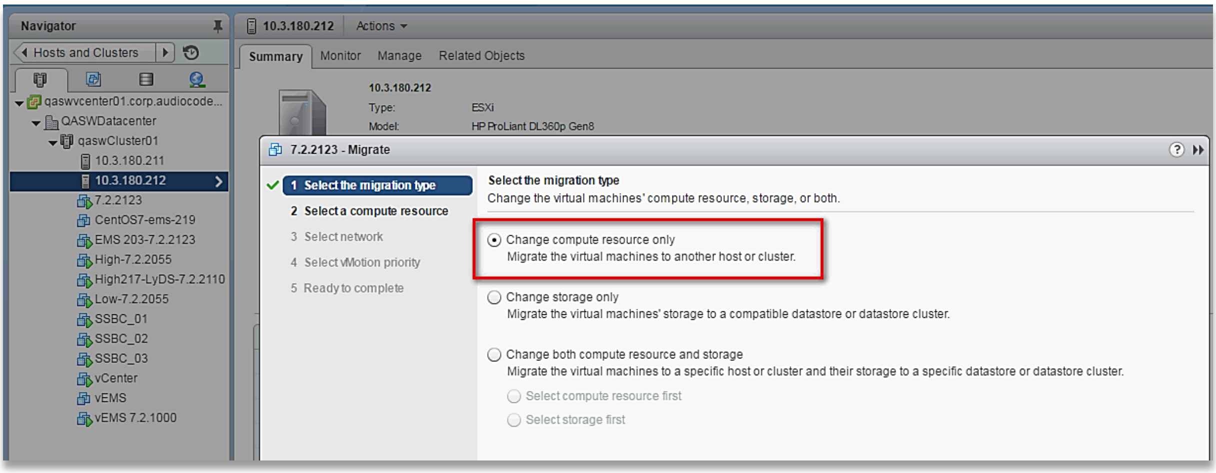


What is a Virtual Machine?

A virtual machine is a software like a physical computer, runs a system and applications. An op system installed on a virtual ma called a guest operating system

3. Change a cluster host for migration:

Figure D-2: Change Host



10.3.180.212

Type: ESXi

Model: HP ProLiant DL360p Gen8

Select the migration type

Change the virtual machines' compute resource, storage, or both.

● Change compute resource only
Migrate the virtual machines to another host or cluster.

○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

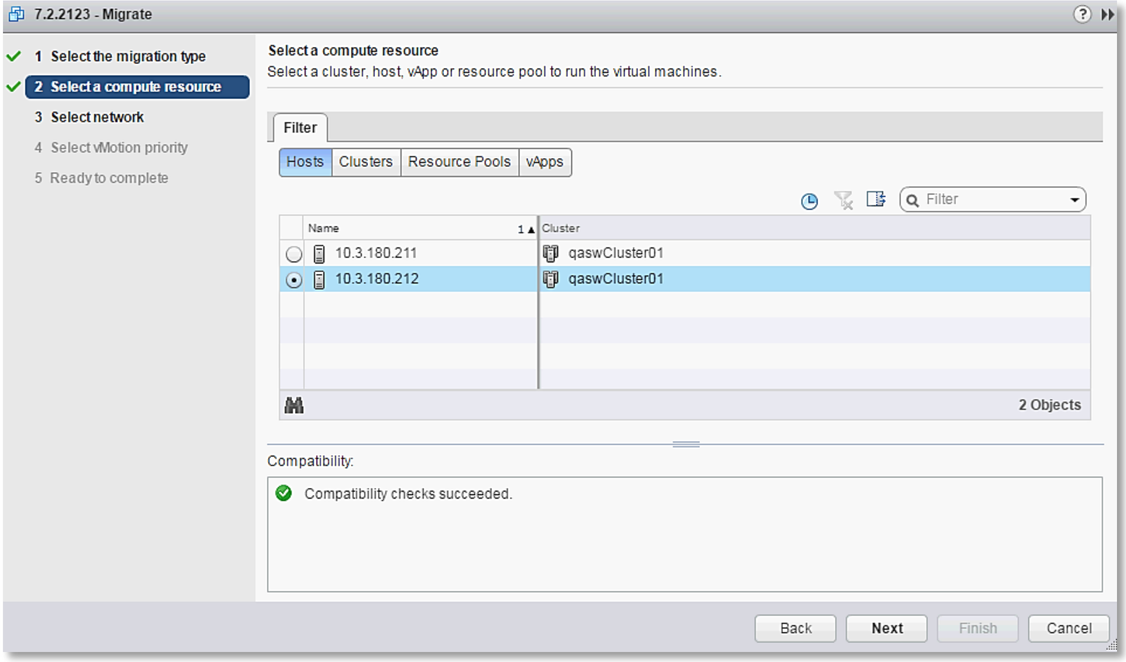
○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Select compute resource first

○ Select storage first

4. Choose the target host for migration:

Figure D-3: Target Host for Migration



7.2.2123 - Migrate

1 Select the migration type
2 Select a compute resource
3 Select network
4 Select vMotion priority
5 Ready to complete

Select a compute resource
Select a cluster, host, vApp or resource pool to run the virtual machines.

Filter

Hosts | Clusters | Resource Pools | vApps

	Name	Cluster
○	10.3.180.211	qaswCluster01
●	10.3.180.212	qaswCluster01

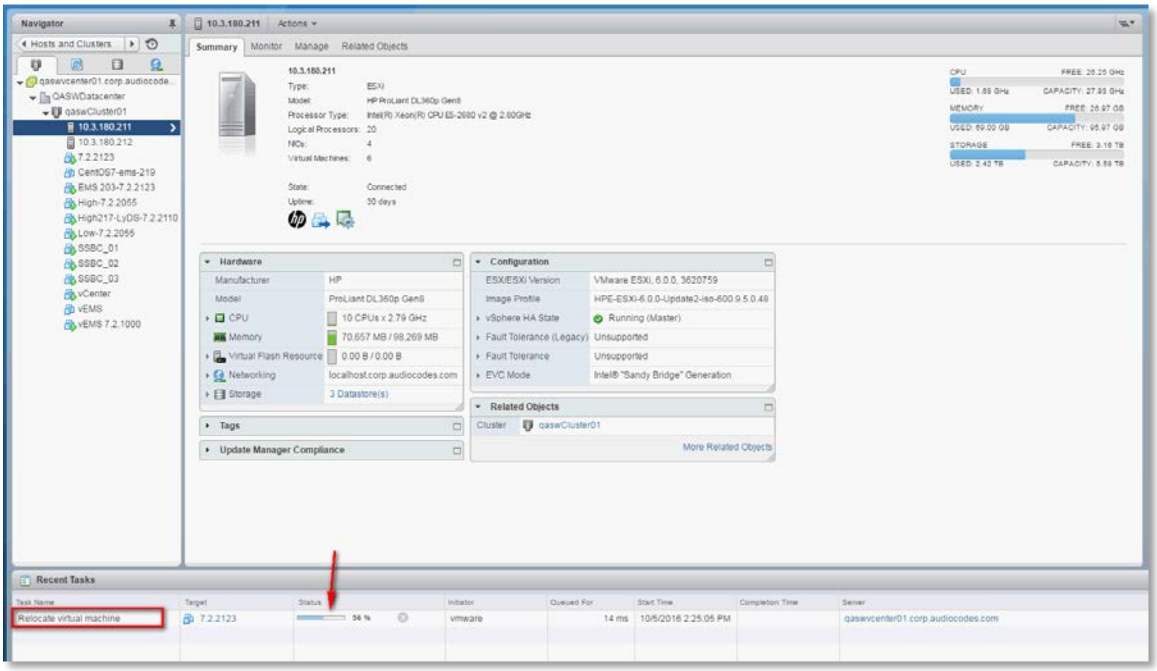
2 Objects

Compatibility:

Compatibility checks succeeded.

The migration process commences:

Figure D-4: Migration Process Started



10.3.180.211
Type: ESXi
Model: HP ProLiant DL360p Gen8
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 20
NICs: 4
Virtual Machines: 6

State: Connected
Uptime: 30 days

CPU FREE: 26.25 GHz
USED: 1.68 GHz CAPACITY: 27.93 GHz
MEMORY FREE: 26.97 GB
USED: 69.00 GB CAPACITY: 95.97 GB
STORAGE FREE: 3.16 TB
USED: 2.42 TB CAPACITY: 5.58 TB

Hardware	
Manufacturer	HP
Model	ProLiant DL360p Gen8
CPU	10 CPUs x 2.79 GHz
Memory	70,657 MB / 98,269 MB
Virtual Flash Resource	0.00 B / 0.00 B
Networking	localhost.corp.audiocodes.com
Storage	3 Datastore(s)

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

Related Objects	
Cluster	qaswCluster01

Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Relocate virtual machine	7.2.2123	56 %	vmware	14 ms	10/5/2016 2:25:05 PM		qaswvcenter01.corp.audiocodes.com

After the migration has completed, the EMS application will run seamlessly on the VM on the new cluster’s host.

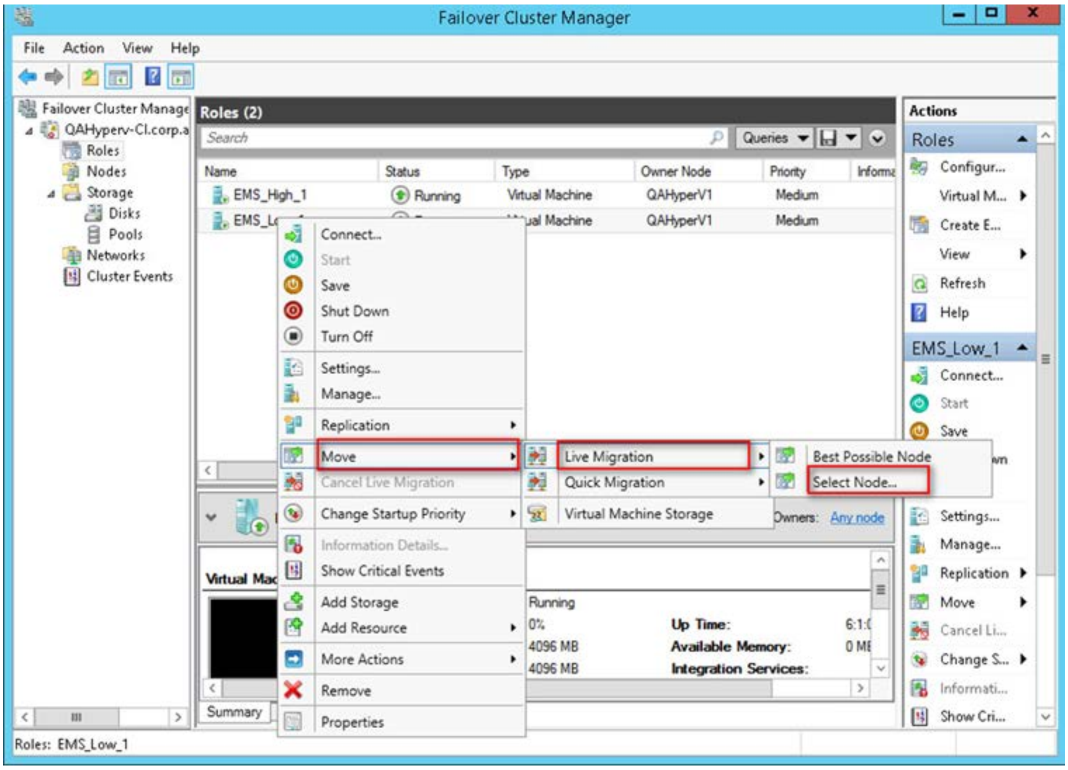
D.2 Moving EMS VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

➢ To move a Virtual Machine to another node of the cluster:

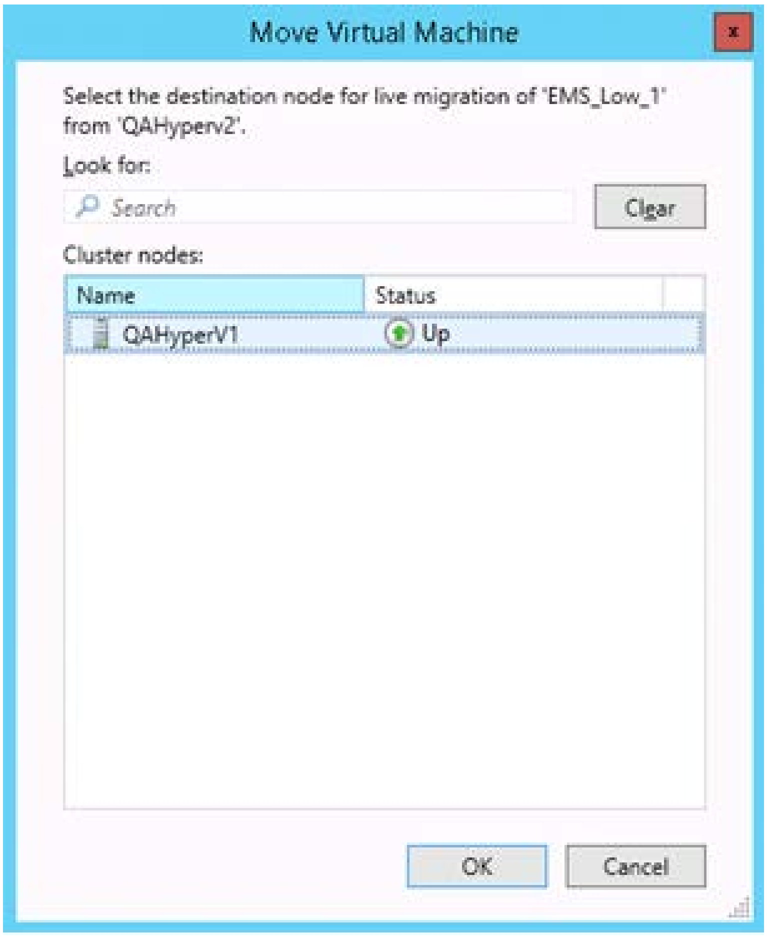
1. Select the Virtual Machine, right-click and from the menu, choose **Move** > **Live Migration > Select Node**.

Figure D-5: Hyper-V Live Migration



The following screen is displayed:

Figure D-6: Move Virtual Machine



Select the destination node for live migration of 'EMS_Low_1' from 'QAHyperv2'.

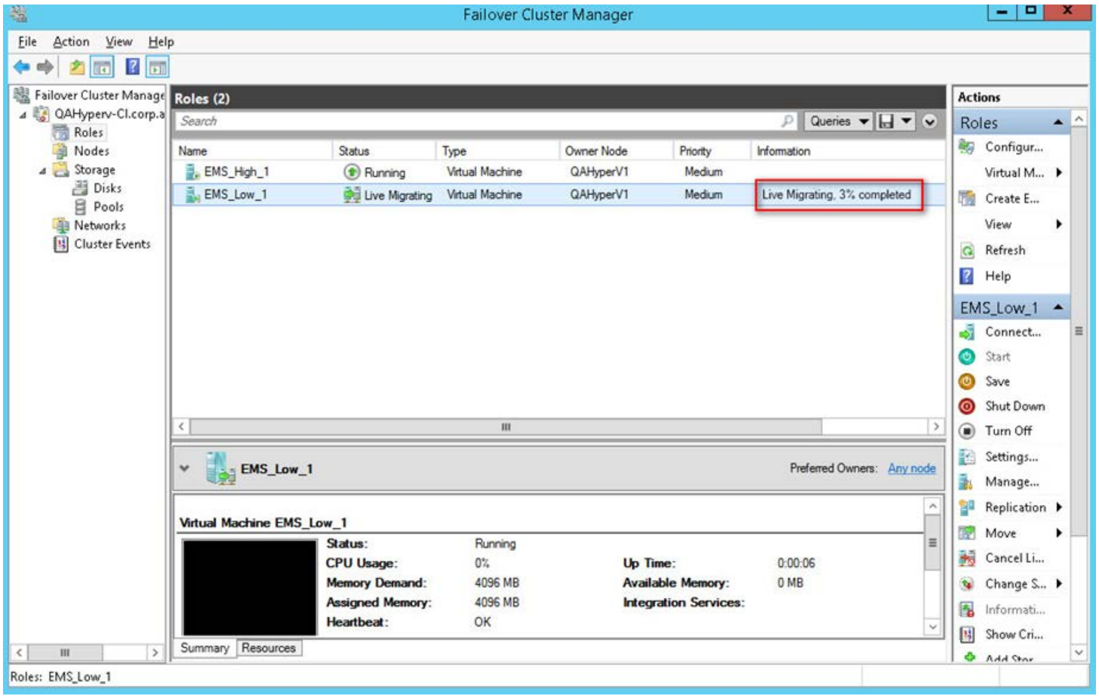
Look for:

Name	Status
QAHyperV1	Up

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

The migration process starts.

Figure D-7: Hyper-V Migration Process Started



Name	Status	Type	Owner Node	Priority	Information
EMS_High_1	Running	Virtual Machine	QAHyperV1	Medium	
EMS_Low_1	Live Migrating	Virtual Machine	QAHyperV1	Medium	Live Migrating, 3% completed

EMS_Low_1 Preferred Owners: Any node

Virtual Machine EMS_Low_1

Status:	Running		
CPU Usage:	0%	**Up Time:**	0:00:06
Memory Demand:	4096 MB	**Available Memory:**	0 MB
Assigned Memory:	4096 MB	**Integration Services:**	
Heartbeat:	OK		

After the migration has completed, the EMS application will run seamlessly on the VM on the new cluster’s node.

This page is intentionally left blank.

E Custom X.509 Certificates- Supplementary Procedures

The procedures in this appendix describe supplementary procedures for completing the setup of X.509 Custom certificates.

Note:

- For more information on the implementation of custom certificates, refer to the OVOC Security Guidelines document.
- If you wish to configure the JAWS page to use HTTPS (see Section 19.10.3).

This appendix describes the following procedures:

- Load KeyStore File to PC Client (see below)
- Cleanup Temporary Files on EMS Server (see Section E.2)
- Cleanup Java Web Start Client Files (see Section E.3)
- Update the Java Security Level on PC (see Section E.4)
- Download certificates to the AudioCodes device (see Section E.5).

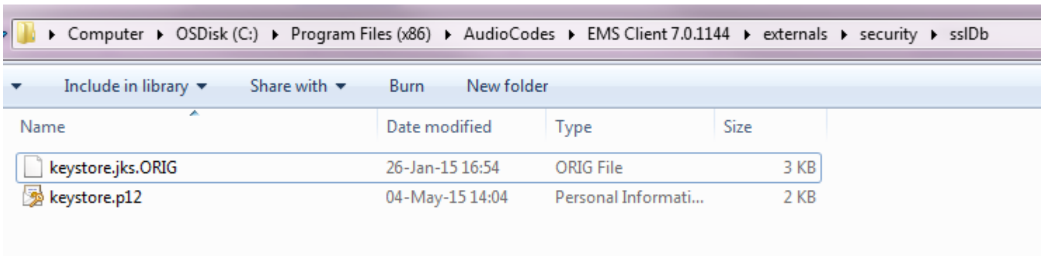
E.1 Load KeyStore File to PC Client

If you are connecting to the EMS from your PC client, you need to manually copy the KeyStore.jks file to the EMS client installation directory on your PC.

➢ To load the certificate file to the PC client:

1. Transfer the file /home/acems/client_certs/KeyStore.jks from the EMS server to the PC that runs the EMS client.
1. On the PC that runs EMS client, close EMS client application.
2. Navigate to: C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\security\sslDb.
3. Rename the existing KeyStore.jks file to KeyStore.jks.ORIG.

Figure E-8: Java KeyStore


Computer ▸ OSDisk (C:) ▸ Program Files (x86) ▸ AudioCodes ▸ EMS Client 7.0.1144 ▸ externals ▸ security ▸ sslDb
Include in library ▾
Share with ▾
Burn
New folder

Name	Date modified	Type	Size
keystore.jks.ORIG	26-Jan-15 16:54	ORIG File	3 KB
keystore.p12	04-May-15 14:04	Personal Informati...	2 KB

Note: If you have performed an EMS upgrade, copy the KeyStore file generated in this step to the new EMS client.

4. Copy the generated java KeyStore file 'KeyStore.jks' to the following directory:

   `C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\security\sslDb`

5. If you defined a custom (non-default) password, open the file `C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\configurationProperties\sslConfig.properties`

   and update the following line with the new password:

```
sslPassword=password
```

E.2 Cleanup Temporary Files on EMS Server

It is highly recommended to cleanup temporary files on the EMS server after certificates have been successfully installed. This is necessary to prevent access to security-sensitive material (certificates and private keys) by malicious users.

➢ **To delete temporary certificate files:**

1. Login to the EMS server as user *root.*
2. Remove the temporary directories:

```
rm -rf /home/acems/server_certs
rm -rf /home/acems/client_certs
```

E.3 Cleanup Java Web Start Client Files

This step describes how to update the Java Web Start Client Certificates.

Note: Apply this procedure if you are connecting to the EMS server using Java Web Start (i.e., https://EMS-IP/jaws). Skip this procedure when installing the EMS client using the AudioCodes-supplied Installation DVD.

➢ **Do the following:**

1. Before connecting with JAWS:
   - JAWS for Chrome:

     Delete directory C:\Users\<pc user>\Downloads\JavaWebStart
   - JAWS for IE:

     Delete directory C:\Users\<pc user>\AppData\Local\Temp\JavaWebStart.

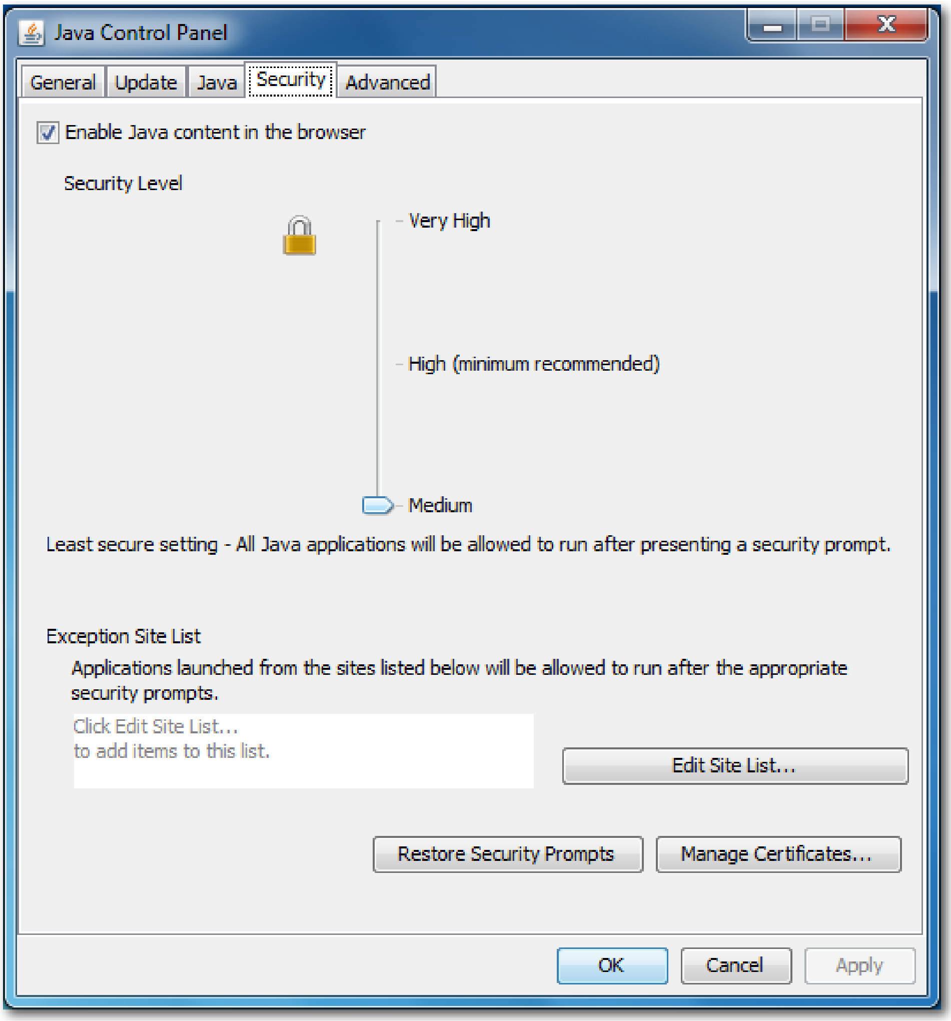
E.4 Update the Java Security Level on PC

For Java Versions 7 or 8 on your PC, you need to update the Java security level on your PC for your EMS client to function correctly.

Note: This procedure is relevant for both HTTP and HTTPS connections.

- **Java Version 7:**
  1. Open the Java Control Panel (**Start** > **Program Files** > **Control Panel** > **Java**).
  2. Click the **Security** tab, and then set the 'Security Level' to **Medium**.

Figure E-9: Java Control Panel (Version 7.2)



Java Control Panel

General | Update | Java | Security | Advanced

☑ Enable Java content in the browser

Security Level

Least secure setting - All Java applications will be allowed to run after presenting a security prompt.

Exception Site List

Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

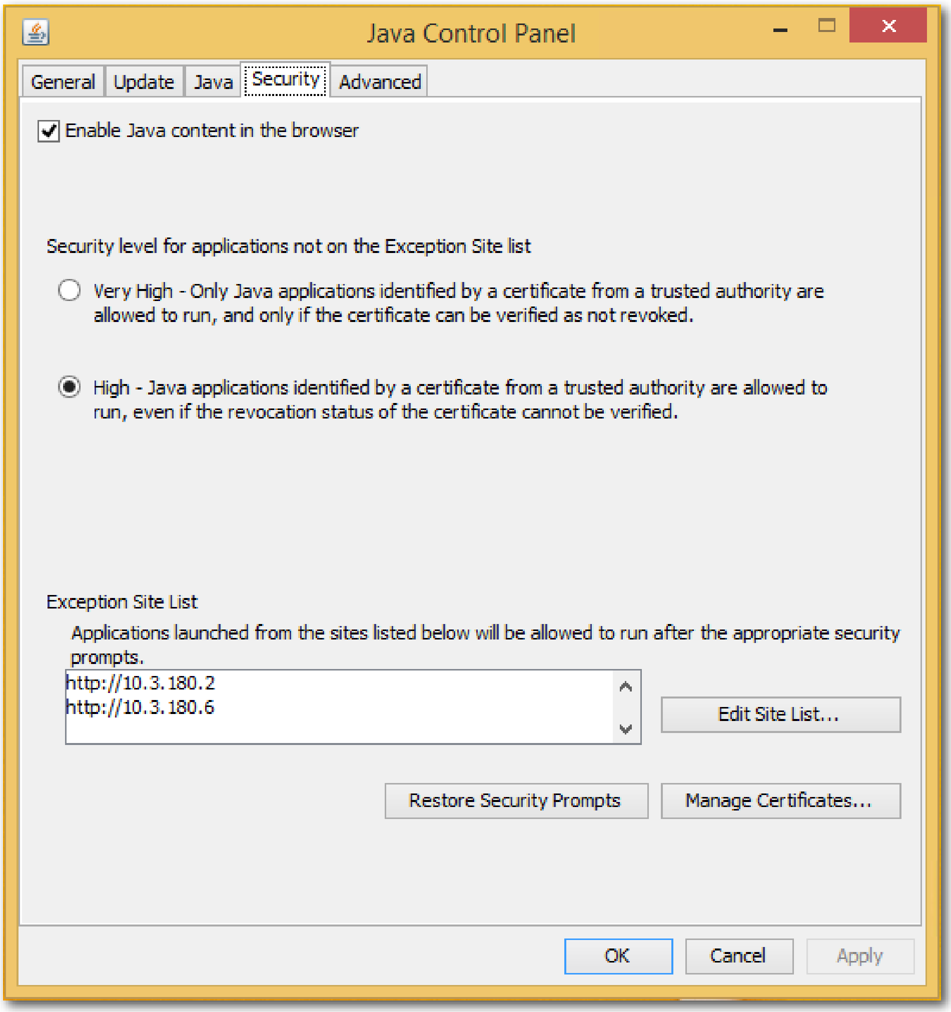
Click Edit Site List...
to add items to this list.

3. Click **OK**.

- **Java Version 8:**

1. Open the Java Control Panel (**Start** > **Program Files** > **Control Panel** > **Java**).
2. Click the **Security** tab and set the Security Level to **High**.

Figure E-10: Java Control Panel (Version 8.0)



☑ Enable Java content in the browser

Security level for applications not on the Exception Site list

○ Very High - Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.

● High - Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.

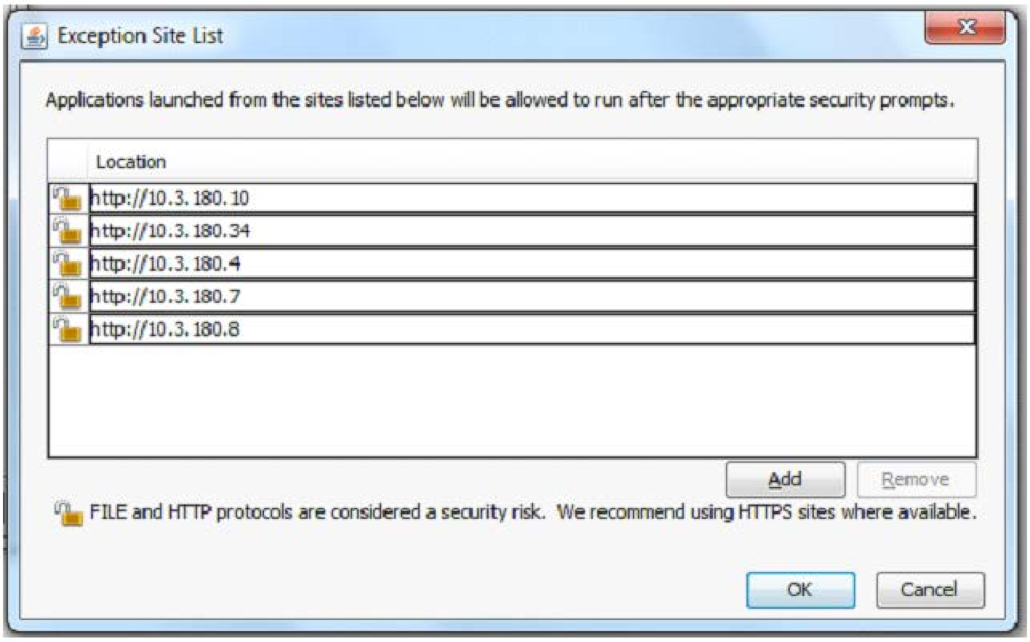
Exception Site List

Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

http://10.3.180.2
http://10.3.180.6

3. Click **Edit Site List…**, and then click **Add**.

Figure E-11: Exception Site List



Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

Location
http://10.3.180.10
http://10.3.180.34
http://10.3.180.4
http://10.3.180.7
http://10.3.180.8

FILE and HTTP protocols are considered a security risk. We recommend using HTTPS sites where available.

4. Enter the server IP address in *http://<server IP>* format.
5. Click **OK** to close the Exception Site List window.
6. Click **OK** to close the Java Control Panel.

E.5 Installing Custom Certificates on AudioCodes Devices

This section describes how to install Custom certificates on AudioCodes devices. These certificates will be used to secure the connection between the device and EMS / SEM server.

This procedure is performed using the device's embedded Web server. This section describes how to install certificates for the following devices:

- Enterprise gateways and SBC devices (see Section E.5.1).
- MP-1xx devices (see Section E.5.3 on page 253).

Note: When you wish to secure the connection with the device over HTTPS, the certificate loaded to the device must be signed by the same CA as the certificate loaded to the OVOC server.

E.5.1 Single-Sign On to the AudioCodes Device

The Single-Sign On mechanism is used to enable automatic login to the devices embedded Web server tool from the device's status screen in the EMS. When this connection is secured over HTTPS and you wish to replace the certificate, then it can be loaded using the "Certificate File" option in the EMS Software Manager (refer to the *EMS User's Manual*).

When this mechanism is used, the certificate loaded to the EMS must be signed by the same root CA used by the AudioCodes device. In this scenario, the EMS authenticates the device before establishing the connection.

E.5.2 Enterprise Gateways and SBC Devices

This section describes how to install custom certificates on Enterprise gateways and SBC devices.

The device uses TLS Context #0 to communicate with the EMS / SEM server. Therefore, the configuration described below should be performed for **TLS Context #0**.

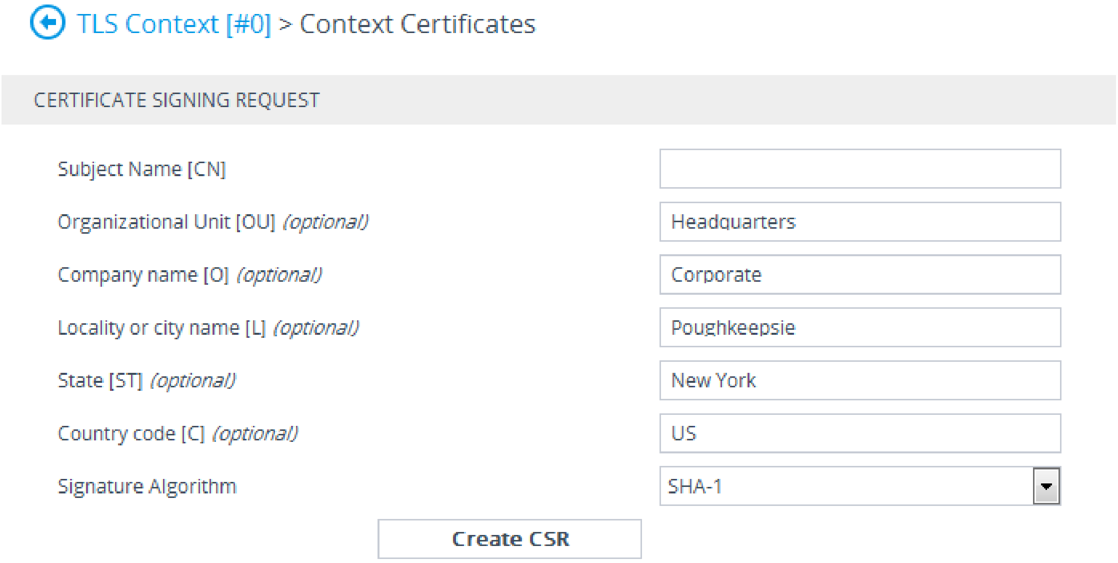
E.5.2.1 Step 1: Generate a Certificate Signing Request (CSR)

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

➢ **To generate certificate signing request:**

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

Figure E-12: Context Certificates



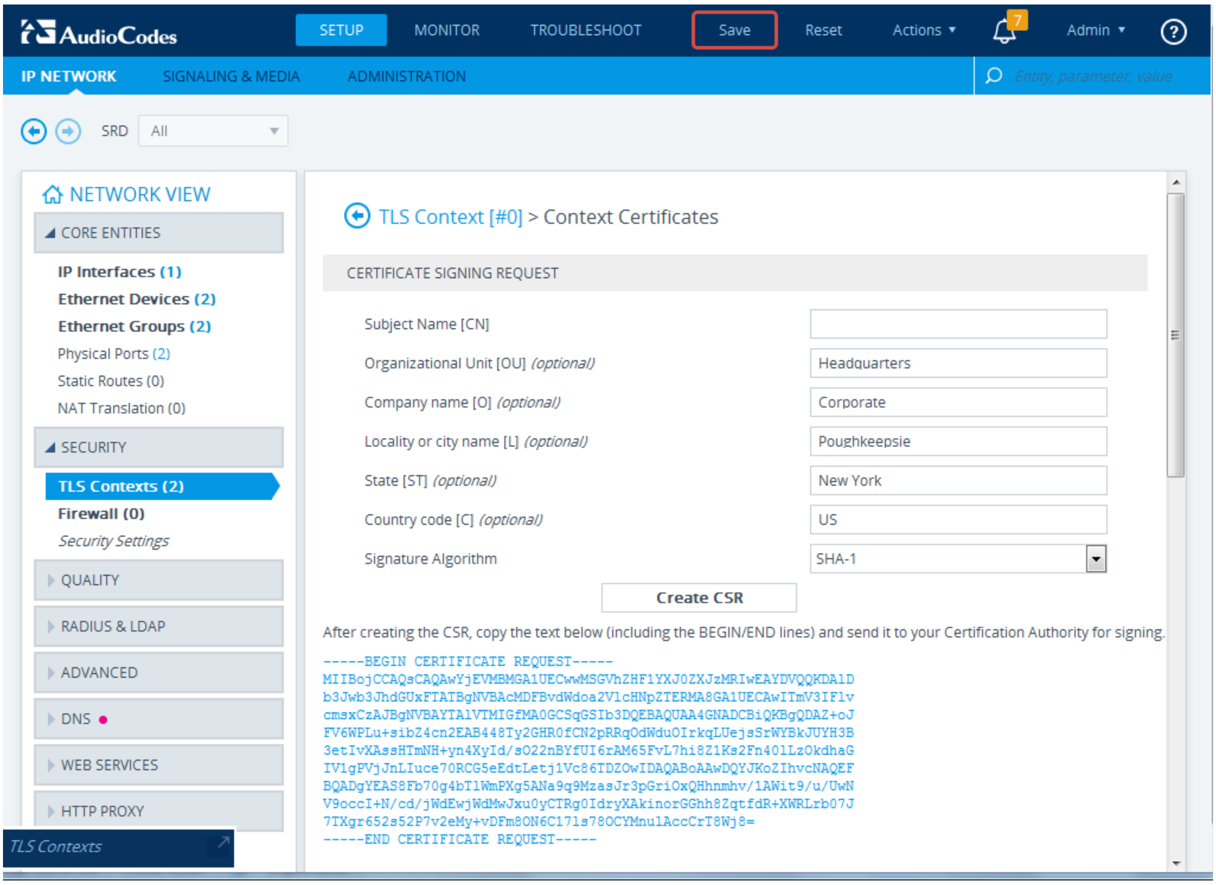
TLS Context [#0] > Context Certificates

CERTIFICATE SIGNING REQUEST

Subject Name [CN]	
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US
Signature Algorithm	SHA-1

3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the device’s DNS name, if such exists, or device’s IP address
   b. Fill in the rest of the request fields according to your security provider's instructions.
   c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure E-13: Certificate Signing Request Group



Subject Name [CN]	
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US
Signature Algorithm	SHA-1

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBojCCAQsCAQAwYjEVMBMGA1UECwwMSGVhZHF1YXJ0ZXJzMRIwEAYDVQQKDA1D
b3Jwb3JhdGUxFTATBgNVBAcMDFBvdWdoa2VlcHNpZTERMA8GA1UECAwITmV3IFlv
cmsxCzAJBgNVBAYTAlVTMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDAZ+oJ
FV6WPLu+sibZ4cn2EAB448Ty2GHR0fCN2pRRqOdWduOIrkqLUejsSrWYBkJUYH3B
3etIvXAssHTmNH+yn4XyId/sO22nBYfUI6rAM65FvL7hi8Z1Ks2Fn40lLzOkdhaG
IV1gPVjJnLIuce70RCG5eEdtLetj1Vc86TDZOwIDAQABoAAwDQYJKoZIhvcNAQEF
BQADgYEAS8Fb70g4bTlWmPXg5ANa9q9MzasJr3pGriOxQHhnmhv/1AWit9/u/UwN
V9occI+N/cd/jWdEwjWdMwJxu0yCTRg0IdryXAkinorGGhh8ZqtfdR+XWRLrb07J
7TXgr652s52P7v2eMy+vDFm8ON6C17ls78OCYMnulAccCrT8Wj8=
-----END CERTIFICATE REQUEST-----
```

4. Copy the text and send it to the certificate authority (CA) to sign this request.

E.5.2.2 Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to "device.crt"
- Root certificate – rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) – rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0MFowKjET
...
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0
L6V8lzUYOfHrEiq/6g==
-----END CERTIFICATE-----
```

Notes:

- The above files are required in the following steps. Make sure that you obtain these files before proceeding and save them to the desired location.
- Use the exact filenames as mentioned above.

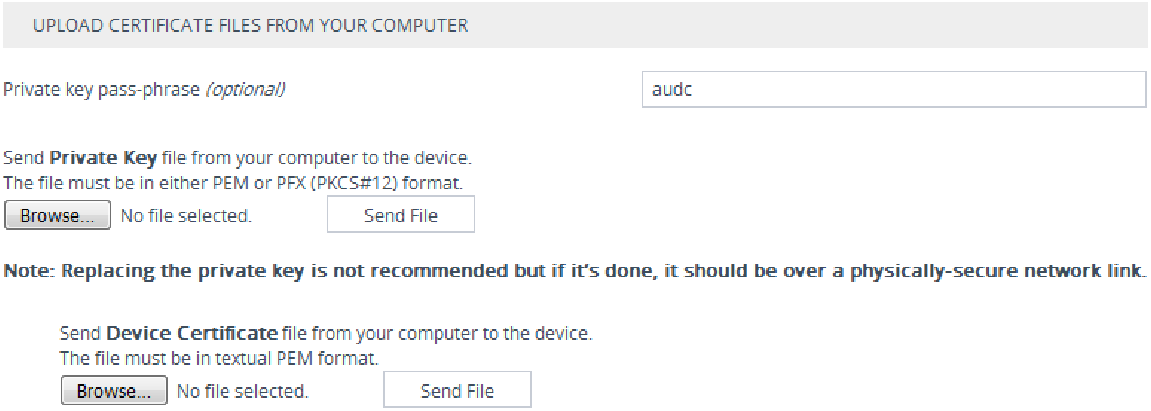
E.5.2.3 Step 3: Update Device with New Certificate

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

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

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Certificate** button, located below the table; the Context Certificates page appears.
3. Under the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.

Figure E-14: Upload Certificate Files from your Computer Group



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)* audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

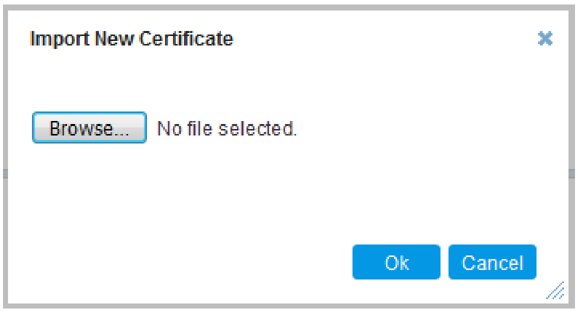
E.5.2.4 Step 4: Update Device’s Trusted Certificate Store

This step describes how to update the device's Trusted Certificate Store.

➢ **To update device’s trusted certificate store:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Trusted Root Certificates** button, located below the table; the Trusted Certificates page appears.
3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

Figure E-15: Importing Certificate into Trusted Certificates Store



Import New Certificate

No file selected.

4. If you received intermediary CA certificates – ca1.crt, ca2.crt, etc. – import them in a similar way.

E.5.2.5 Step 5: Configure HTTPS Parameters on the Device

This section describes how to configure HTTPS related parameters on the device.

Note:

- You can optionally pre-stage the device with a pre-loaded ini file including this configuration (for more information, contact your AudioCodes representative).
- If you have enabled the Interoperability Automatic Provisioning feature, ensure that your template file is also configured as described in this procedure to maintain an active HTTPS connection after the template file has been loaded to the device.
- When you setup an HTTPS connection on the device, you must also enable HTTPS ("Enable HTTPS Connection") when adding the device to the EMS (refer to the *EMS User's manual*).

➢ **To configure HTTPS parameters on the device:**

1. Create a new text file using a text-based editor (e.g., Notepad).
2. Include the following ini file parameters for server-side authentication:
   - For Media Gateway and SBC devices:

```
AUPDVerifyCertificates=1
```

   - For MP-1xx devices:
     - ♦ The ini file should include the following two lines:

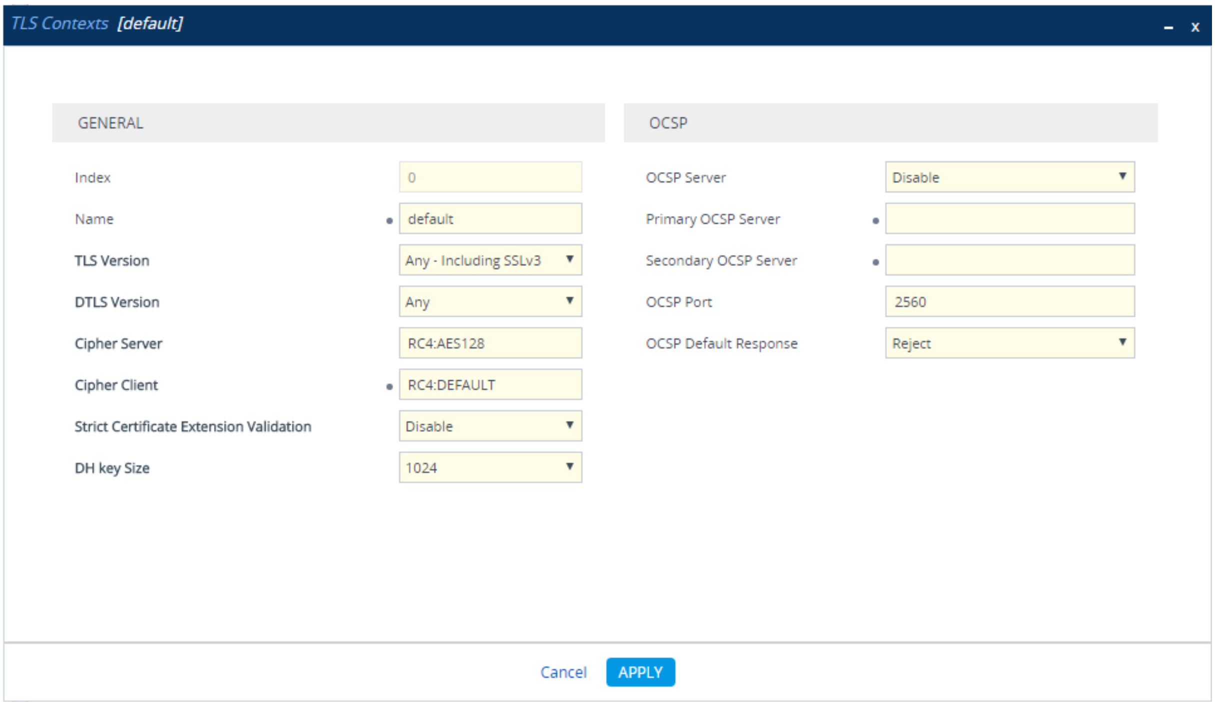
```
AUPDVerifyCertificates=1
ServerRespondTimeout=10000
```

     - ♦ When working with SEM TLS (see Section 19.10.5), add the following parameter.

```
QOEENABLETLS=1
```

3. Save and close the file.
4. Load the generated file as “Incremental INI file” (**Maintenance** menu > **Software Update** > **Load Auxiliary Files** > **INI** file (incremental).
5. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
6. In the table, select the **TLS Context #0**, and then click **Edit** button. The following screen is displayed:

Figure E-16: TLS Contexts: Edit Record



TLS Contexts [default]

GENERAL

Index	0
Name	default
TLS Version	Any - Including SSLv3
DTLS Version	Any
Cipher Server	RC4:AES128
Cipher Client	RC4:DEFAULT
Strict Certificate Extension Validation	Disable
DH key Size	1024

OCSP

OCSP Server	Disable
Primary OCSP Server	
Secondary OCSP Server	
OCSP Port	2560
OCSP Default Response	Reject

7. Set 'TLS Version' to **1** (TLS 1.0 only).
8. Set 'HTTPS Cipher Server' to **ALL**.
9. Set 'HTTPS Cipher Client' to **ALL**.

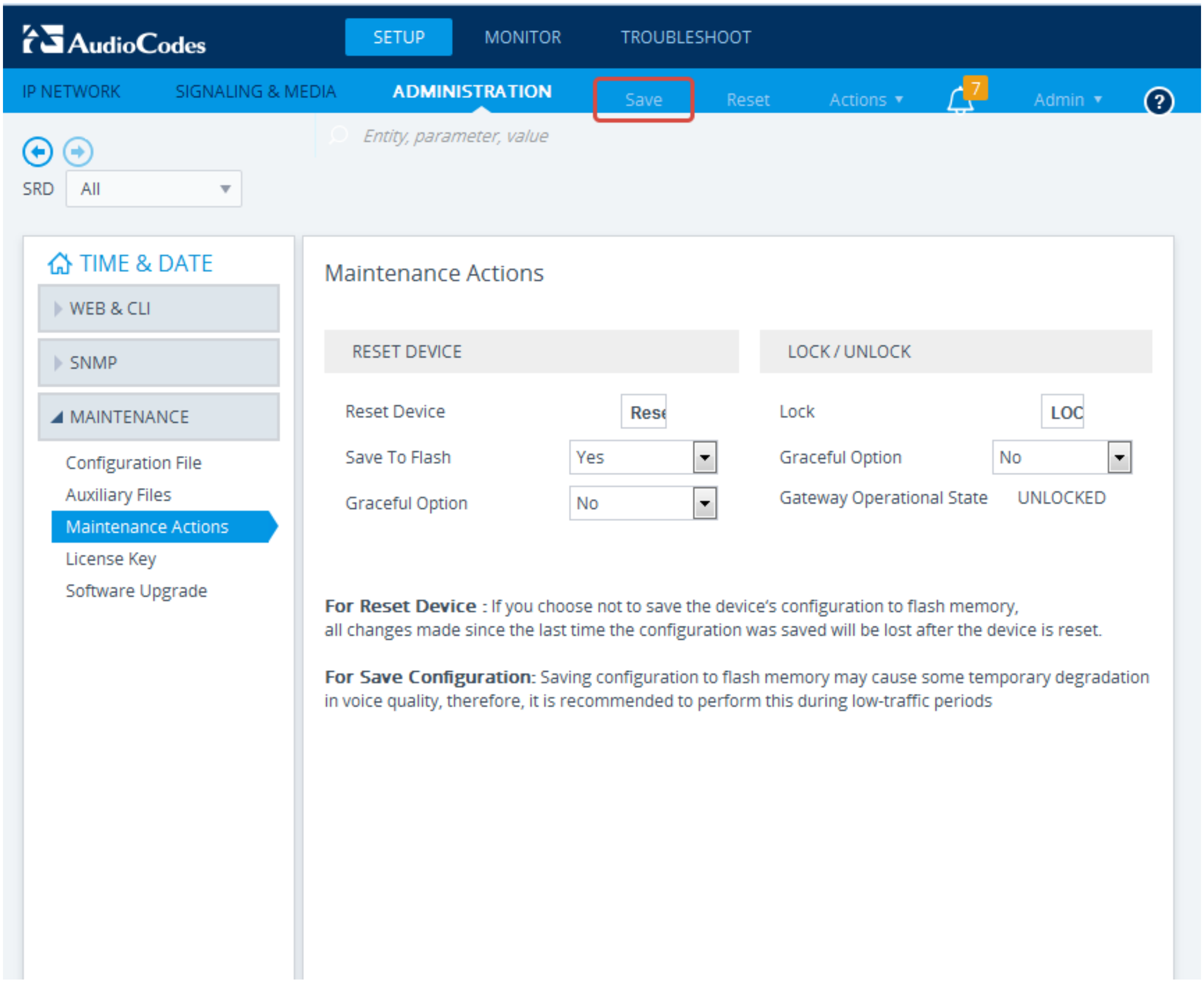
E.5.2.6 Step 6: Reset Device to Apply the New Configuration

This step describes how to reset the device to apply the new configuration.

➢ **To reset the device:**

1. In the top-level menu, click **Device Actions > Reset.** The following screen is displayed.

Figure E-17: Device Reset



Maintenance Actions

RESET DEVICE

Reset Device	Rese
Save To Flash	Yes
Graceful Option	No

LOCK / UNLOCK

Lock	LOC
Graceful Option	No
Gateway Operational State	UNLOCKED

For Reset Device : If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods

2. From the Burn to FLASH drop-down list, select **Yes**, and then click **Reset** button.

   The device will save the new configuration to non-volatile memory and reset itself.

E.5.3 MP-1xx Devices

This section describes how to install Custom certificates on the MP 1xx devices.

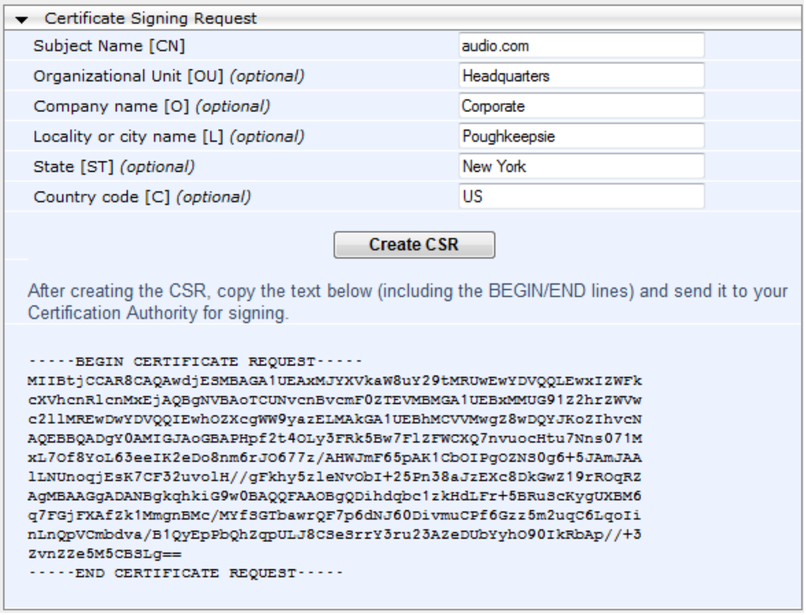
E.5.3.1 Step 1: Generate a Certificate Signing Request (CSR)

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

➢ **To generate a CSR:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to **HTTP and HTTPS** (refer to the *MP-11x and MP-124 User's Manual*). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
3. Login to the MP-1xx Web server.
4. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
5. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the DNS name.
   b. Fill in the rest of the request fields according to your security provider's instructions.
   c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure E-18: Certificate Signing Request Group



Subject Name [CN]	audio.com
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwdjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLEwxIZWFk
cXVhcnRlcnMxEjAQBgNVBAoTCUNvcnBvcmF0ZTEVMBMGA1UEBxMMUG91Z2hrZWVw
c2llMREwDwYDVQQIEwhOZXcgWW9yazELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPHpf2t4OLy3FRk5Bw7FlZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CbOIPgOZNS0g6+5JAmJAA
lLNUnoqjEsK7CF32uvolH//gFkhy5zleNvObI+25Pn38aJzEXc8DkGwZ19rROqRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbc1zkHdLFr+5BRuScKygUXBM6
q7FGjFXAfZk1MmgnBMc/MYfSGTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LqoIi
nLnQpVCmbdva/B1QyEpPbQhZqpULJ8CSeSrrY3ru23AZeDUbYyhO90IkRbAp//+3
ZvnZZe5M5CBSLg==
-----END CERTIFICATE REQUEST-----
```

6. Copy the text and send it to the certificate authority (CA) to sign this request.

E.5.3.2 Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to “device.crt”
- Root certificate – rename this file to “root.crt”
- Intermediate CA certificates (if such files exist) – rename these files to “ca1.crt”, “ca2.crt” etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEw
JGUjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBT
ZXJ2ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1
UEBhMCRlIxEzARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9z
dGUgU2VydmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4Mz
iR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWUL
f7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMyb
FkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJ
uZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```

Notes:

- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above.

E.5.3.3 Step 3: Update Device with New Certificate

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

➢ To update the device with the new certificate:

1. In the Certificates page, scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.
2. After the certificate successfully loads to the device, save the configuration with a device reset (see Section E.5.3.6 below).

E.5.3.4 Step 4: Update Device’s Trusted Certificate Store

For the device to trust a whole chain of certificates you need to combine the contents of the root.crt and ca.crt certificates into a single text file (using a text editor).

➢ To update the device with the new certificate:

1. Open the root.crt file (using a text-based editor, e.g., Notepad).
2. Open the ca.crt file (using a text-based editor, e.g., Notepad).
3. Copy the content of the ca.crt file and paste it into the root.crt file above the existing content.

Below is an example of two certificate files combined (the file "ca2.crt" and the "root.crt") where the ca2.crt file contents are pasted above the root.crt file contents:

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNfQ0EyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggwnlQiUYhOK
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/
0fmXKHWlPIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4yk
ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu
5B6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI
hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM
BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvrTBJBgNV
HSMEQjBAgBThf6GbMQbO5b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM
MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcg
TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+
CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhlCq
hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO
RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V
XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBlO+np/O8F+P551uH0iOYA6Cc
Cj6oHGLq8RIndA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhnUQrS
667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+7/q
ebESJyW8pTLTszGQns2E214+U18sKHItpUZvs1dVUIX6xQiSYFDG1CDIPR5/70pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOIp6LR72Ta9HMJFJ4gyxJPUQA
jV3Led2Y4JObvBTNlka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPUf1wRjDWgl4G
BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9lXI/HQkKRSTf8CAwEAAaN6MHgw
DAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAIYwSQYD
VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBAoTA0FD
TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggEBAHqkg4F6
wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFCz1q4QVpQNYAwdBdEAKENznZttoP3aPZE
3EOx1C8Mw2wU4pOxD7B6pH0XO+oJ4LrxLB3SAJd5hW495X1RDF99BBA9eGUZ2nXJ
9pin4PWbnfc8eppq8Tpl8jJMW0Zl3prfPt012q93iEalkDEZX+wxkHGZEqS4ayBn
```

```
8bU3NHt5qh0Egpai8hB/nth1xnA1m841wxCbJW86AMRs2NznROyG695InAYaNlIo
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2k9STOpN
itSUgGYwEagnsMU=
-----END CERTIFICATE-----
```

Notes: The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

4. Save the combined content to a file named "chain.pem" and close the file.
5. Open the Certificates page and upload chain.pem file using the 'Trusted Root Certificate Store' field.

E.5.3.5 Step 5: Configure HTTPS Parameters on Device

- Configure HTTPS Parameters on the device (see Section E.5.2.5 above).

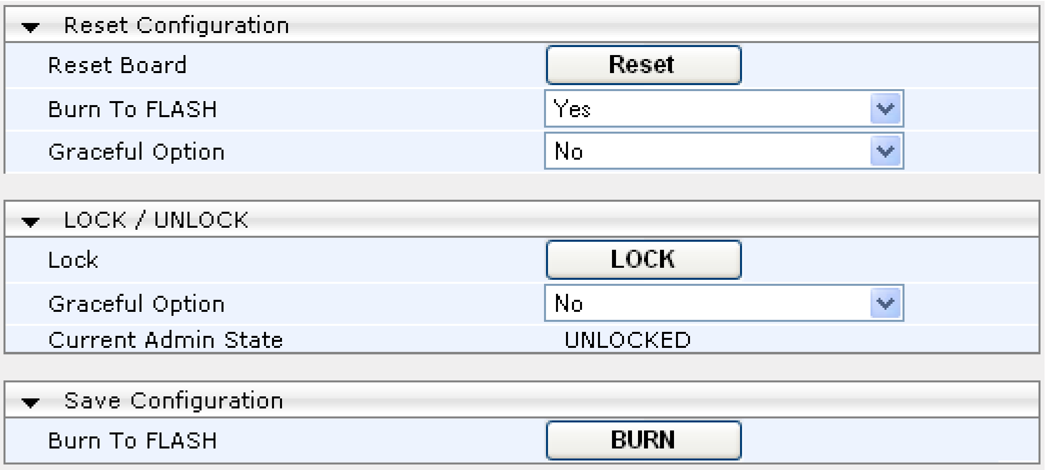
E.5.3.6 Step 6: Reset Device to Apply the New Configuration

This section describes how to apply the new configuration.

➢ **To save the changes and reset the device:**

1. Do one of the following:
   - On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
   - On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

Figure E-19: Maintenance Actions Page



▼ Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

▼ LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Current Admin State	UNLOCKED

▼ Save Configuration

Burn To FLASH	BURN

2. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
3. Click **OK** to confirm device reset; when the device begins to reset, a notification message is displayed.

This page is intentionally left blank.

F Transferring Files

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

Note: .FTP by default is disabled in the EMS server.

➢ To transfer files to and from the EMS server:

1. Open your SFTP/SCP application, such as WinSCP or FileZilla.
2. Login with the acems/acems credential (all files transferred to the EMS 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 EMS server host machine.

This page is intentionally left blank.

G Verifying and Converting Certificates

This appendix describes how to verify that certificates are in PEM format and describes how to convert them from DER to PEM if necessary.

➢ To verify and convert certificates:

1. Login to the EMS server as user *root.*
2. Transfer the generated certificate to the EMS server.
3. Execute the following command on the same directory that you transfer the certificate to verify that the certificate file is in PEM format:

```
Openssl x509 –in certfilename.crt –text -noout
```

4. Do one of the following:
   a. If the certificate is displayed in text format, then this implies that the file is in PEM format, and therefore you can skip the steps below.
   b. If you receive an error similar to the one displayed below, this implies that you are trying to view a DER encoded certificate and therefore need to convert it to the PEM format.

```
unable to load certificate
12626:error:0906D06C:PEM routines:PEM_read_bio:no start
line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
```

5. Convert the DER certificate to PEM format:

```
openssl x509 -inform der -in certfilename.crt -out
certfilename.crt
```

This page is intentionally left blank.

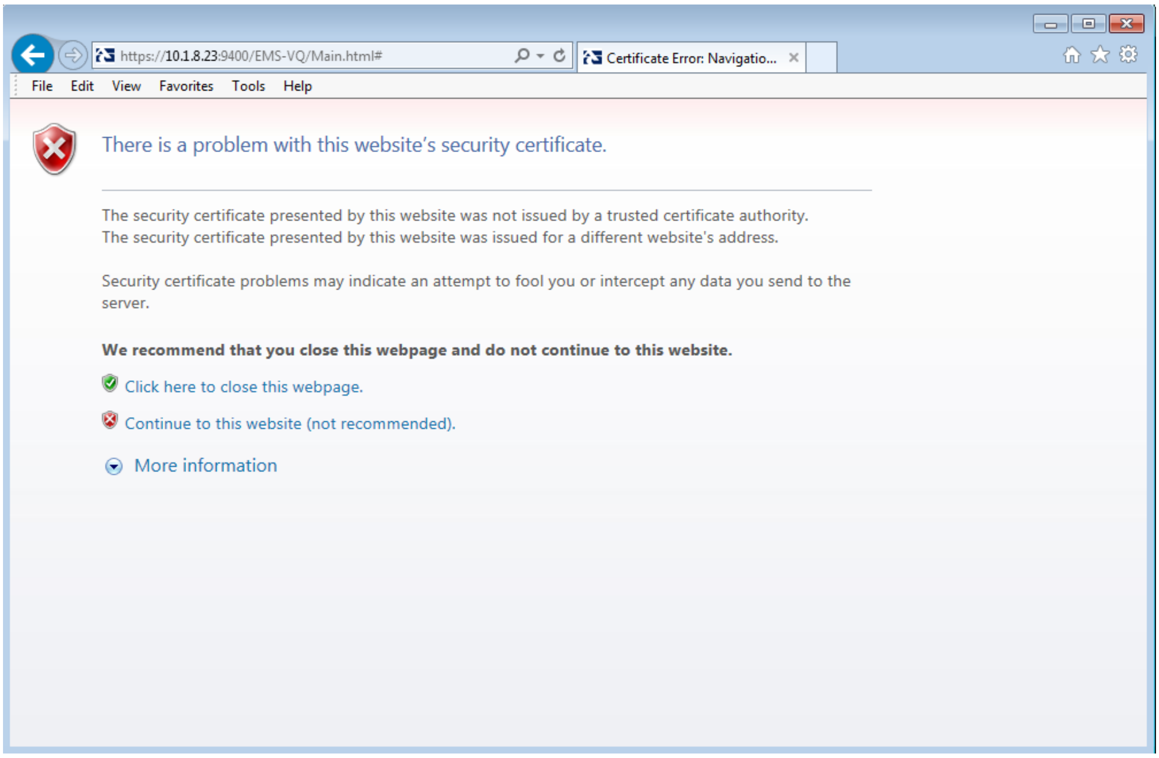
H Self-Signed Certificates

When using self-signed certificates, use the following instructions for recognizing the secure connection with the EMS server from your IP Phone Manager and SEM Web client browsers.

H.1 Internet Explorer

When the following screen is displayed, select the “Continue to website (not recommended)” option.

Figure H-1: Continue to Website



https://10.1.8.23:9400/EMS-VQ/Main.html#
Certificate Error: Navigatio...
File
Edit
View
Favorites
Tools
Help

There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

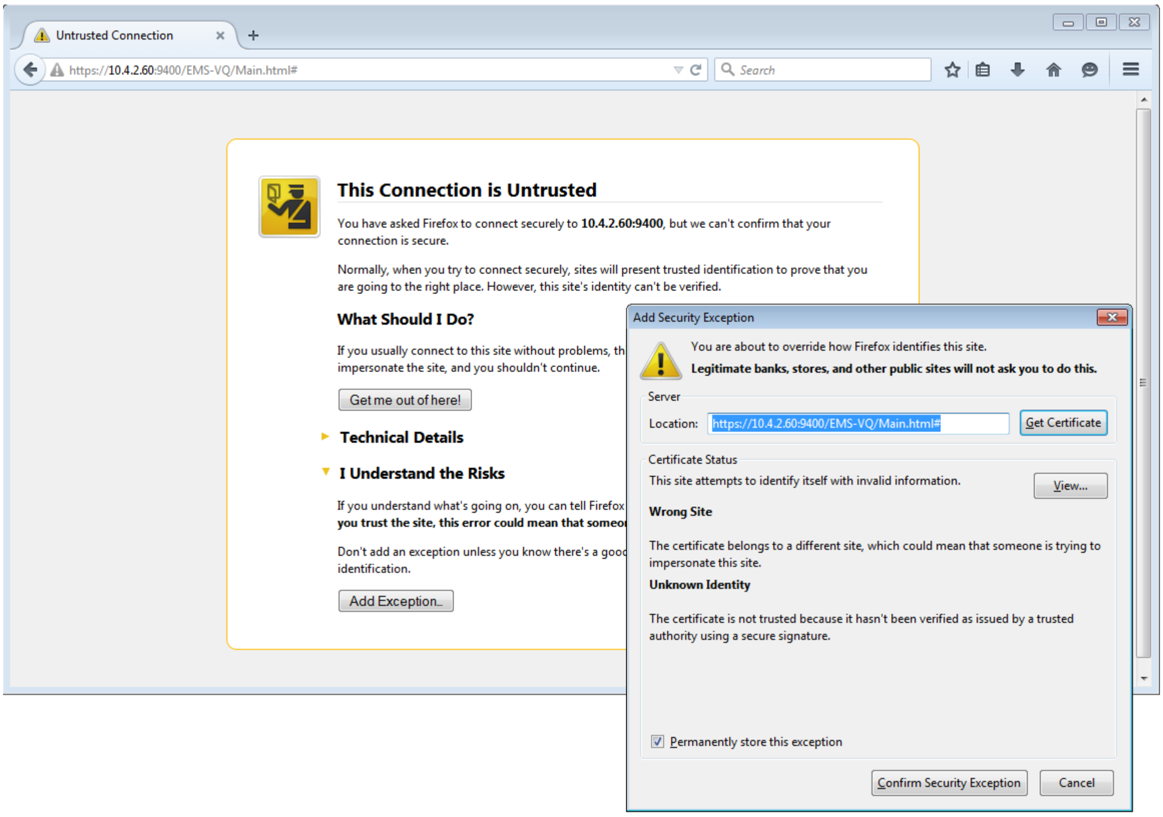
More information

H.2 Using Mozilla Firefox

Do the following:

1. When the following screen is displayed, click the “I Understand the Risks” option.
2. Click the **Add Exception** button, and then click the **Confirm Security Exception** button.

Figure H-2: Mozilla Firefox Settings



This Connection is Untrusted

You have asked Firefox to connect securely to **10.4.2.60:9400**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, th
impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox
you trust the site, this error could mean that someo

Don't add an exception unless you know there's a good
identification.

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.4.2.60:9400/EMS-VQ/Main.html#

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

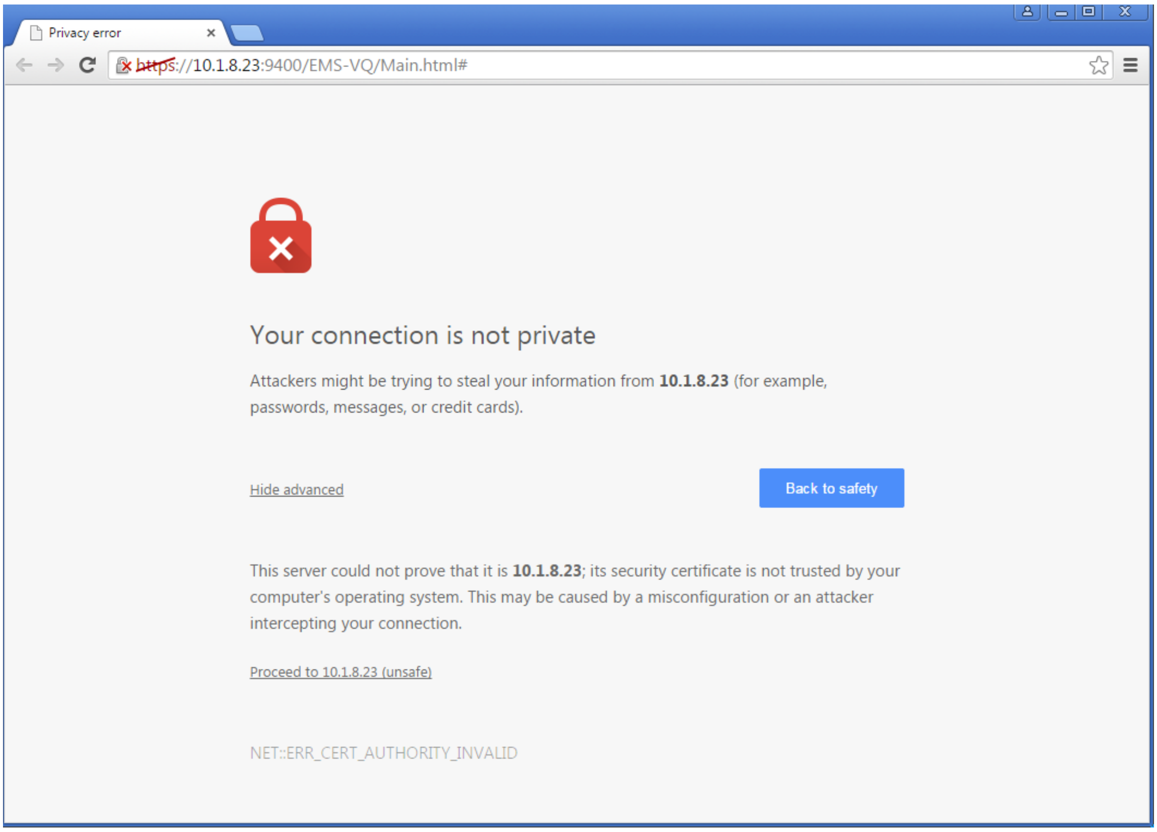
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

H.3 Chrome

When the following screen is displayed, click **Advanced** and then click the “Proceed to <Server IP> (unsafe)” link.

Figure H-3: Chrome Browser Settings



Privacy error
~~https~~://10.1.8.23:9400/EMS-VQ/Main.html#

Your connection is not private

Attackers might be trying to steal your information from **10.1.8.23** (for example, passwords, messages, or credit cards).

Hide advanced
Back to safety

This server could not prove that it is **10.1.8.23**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.1.8.23 (unsafe)

NET::ERR_CERT_AUTHORITY_INVALID

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: www.audiocodes.com/contact
Website: www.audiocodes.com