AudioCodes One Voice Operations Center

Element Management System &
Session Experience Manager

Installation, Operation and Maintenance Manual

Version 6.8

AudioCodes

Table of Contents

List of Figures

List of Tables

Notice

This IO&M Manual describes the installation, operation and maintenance of AudioCodes' EMS server and Session Experience Manager (SEM) server.

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.

Date Published: June-30-2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

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 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) OAMP Integration Guide
Element Management System (EMS) User's Manual
SEM User's Manual
Element Management System (EMS) Online Help
Mediant 5000 / 8000 Media Gateway Installation, Operation and Maintenance Manual
Mediant 5000 / 8000 Media Gateway Release Notes
Mediant 500 E-SBC and Mediant 800 Gateway and E-SBC OAMP Guide
Mediant 1000B Gateway and E-SBC OAMP Guide
Mediant 2600-4000-9000-SW SBC Series OAMP Guide
Mediant 3000 with TP-6310 OAMP Guide
Mediant 3000 with TP-8410 OAMP Guide
Mediant MSBR Series OAMP 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 Component Information

The EMS comprises the following components:

- EMS server (running on the Linux operating system on dedicated Hardware or VMware vSphere). The EMS server serves both the EMS and SEM applications.
- EMS client (running on Microsoft™ Windows™ operating system), displaying the EMS GUI screens that provide the customer access to system entities. For the EMS client running on Java Web Start, NIBF and SEM application, the following browsers are supported:
  - Internet Explorer – version 8 and higher
  - Google Chrome – version 19.0 and higher
  - Mozilla Firefox – version 12.0 and higher

2.1 Managed VoIP Equipment

The following products (and product versions) can be managed by this EMS / SEM release (**bold** font indicates new products / versions):

- *Mediant 8000 Media Gateway: versions 6.6, 6.2
- *Mediant 5000 Media Gateway: versions 6.6, 6.2
- Mediant 4000 E-SBC: versions **6.8**, 6.6
- Mediant 2600 E-SBC: versions **6.8**, 6.6
- **Mediant SE SBC: version 6.8**
- **Mediant VE SBC: version 6.8**
- Mediant 3000 Media Gateways: versions **6.8**, 6.6, 6.4
- Mediant 2000 Media Gateways: versions 6.6, 6.4
- *Mediant 1000 Gateway: versions 6.6 and 6.4
- Mediant 1000B Gateway and E-SBC and Mediant 1000B MSBR: versions **6.8**, 6.6, 6.4
- Mediant 800B Gateway and E-SBC and Mediant 800B MSBR: versions **6.8**, 6.6, 6.4
- *Mediant 600: versions 6.6, 6.4
- **Mediant 500 E-SBC and Mediant 500 MSBR: versions 6.8**
- MediaPack 11x Media Gateways: versions 6.6
- *Mediant 800 SBA, *Mediant 1000 SBA and *Mediant 2000 SBA devices with SBA version **1.1.13.0** and above and gateway versions 6.6 and **6.8**

Note:

- * Refers to products that are not supported by the SEM.
- All version 6.8 VoIP equipment works with the SIP control protocol.

2.2 SEM Server Disk Requirements

The SEM database resides on the EMS Server machine. The chosen disk storage type depends on the size of the database load (the number of simultaneous calls monitored by the SEM).

The three configurations shown in the table below are supported:

Table 2-1: SEM Server Disk Requirements

Size	Maximum detailed Storage Size	Maximum statistics Storage Size
Virtual EMS, low profile	8 million calls	15 million calls
Virtual EMS, high profile	80 million calls	150 million calls
Dedicated EMS Hardware	80 million calls	150 million calls

3 Hardware and Software Requirements

This section describes the hardware and software requirements 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 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 DL360 G6	HP ProLiant DL360p Gen8	_	_	Monitor resolution: 1152*864 or higher
Operating System	Linux CentOS 64-bit, kernel version 5.9, Rev6	Linux CentOS 64-bit, kernel version 5.9, Rev6	Linux CentOS 64-bit, kernel version 5.9 Rev6,	Linux CentOS 64-bit, kernel version 5.9 Rev6,	Windows™ 2000 / XP/ Vista/Windows 7/ Windows 8/Windows 8.1
Memory	2 GB RAM	32 GB RAM	4 GB RAM	32 GB RAM	512 MB RAM
Disk space	146 GB	Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0	170 GB	1200 GB	300 MB
Processor	Intel Xeon E5504 (4M Cache, 2.00 GHz)	CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each)	1 core not less than 2 GHz	6 cores not less than 2 GHz	600 MHz Pentium III or higher
DVD-ROM	Local		_	_	_

- The working space requirements on the EMS server are as follows:
  - Linux: Executable bash
- The EMS server works with the JDK version 1.6 (JDK 1.6 for Linux™). The EMS client works with the JDK version 1.6 for Windows™.

  All of the above mentioned components are automatically installed in the current version of the EMS server and EMS client.

3.2 EMS and SEM Bandwidth Requirements

This section describes the bandwidth requirements of the EMS and the SEM.

3.2.1 EMS Bandwidth Requirements

The bandwidth requirement is for EMS/SEM Server <-> Device communication. The network bandwidth requirements per media gateway are as follows:

- 500 Kb/sec for faults, performance monitoring, provisioning and maintenance actions.
- 20 Mb/sec for Mediant 5000 / Mediant 8000 Online Software Upgrade

3.2.2 SEM Bandwidth Requirements

The following table describes the 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	Gateway Sessions	Required Kbits/sec
MP-118	_	_	8	15 Kbits/sec
MP-124	_	_	24	45 Kbits/sec
Mediant 800 Mediant 850	60	135 Kbits/sec	60	110 Kbits/sec
Mediant 1000	150	330 Kbits / sec	120	220 Kbits/sec
Mediant 2000	_	_	480	880 Kbits/sec
Mediant 2600	600	1.3 Mbit/sec	_	_
Mediant 3000	1024	2.2 Mbit/sec	2048	3.6 Mbit/sec
Mediant 4000	4,000	8.6 Mbit/sec	_	_

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, REV5

    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 REV6.
- **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 27).

5.1.1 Testing Hardware Requirements on the Linux Platform

To ensure that your machine meets the minimal hardware requirements for the EMS application, run the following commands in the **tcsh**.

- **RAM** - A minimum of 2 GB is required

  To determine the amount of random access memory installed on your system, enter the following command:

  ```
  more /proc/meminfo | grep MemTotal
  ```

- **Swap Space** - Disk space twice the system's physical memory, or 2 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 146 GB for the EMS Dedicated. Hardware version (on the same disk or under RAID - Redundant Arrays of Independent Disks) and up to 120 GB for the VMware version (for more information, see Section 3 on page 21).

  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)

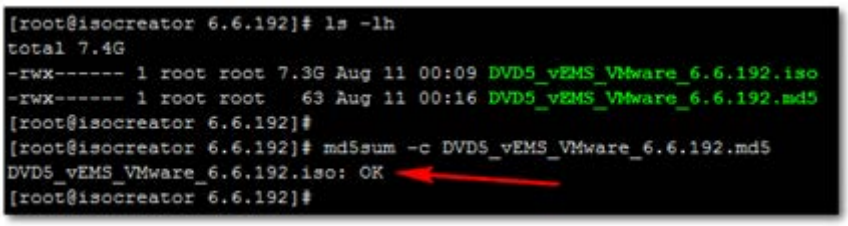
6.1.2 Linux

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



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 H on page 215).

➢ **To perform DVD1 installation:**

1. Insert the **DVD1-Linux for EMS Rev 6** (CentOS 5.9) into the DVD ROM.
2. Connect the EMS server via the serial port with a terminal application and login with 'root' user.
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 via the RS-232 console or via 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

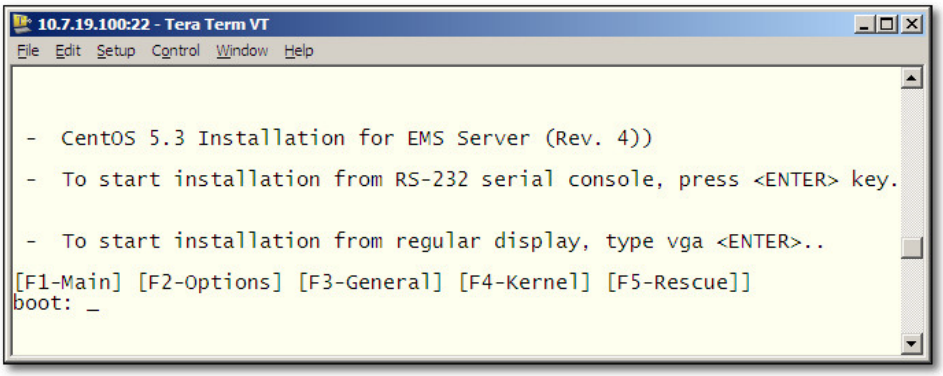
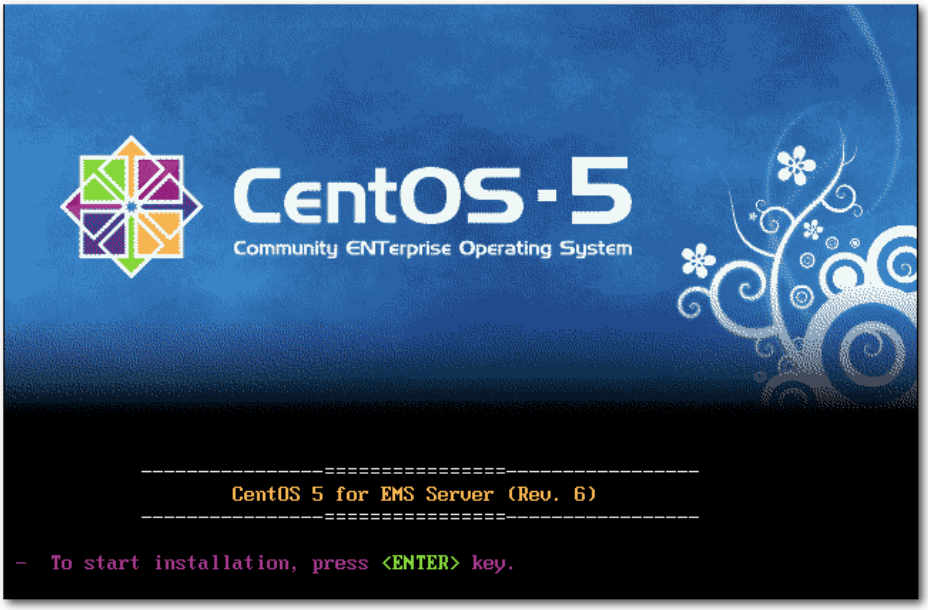


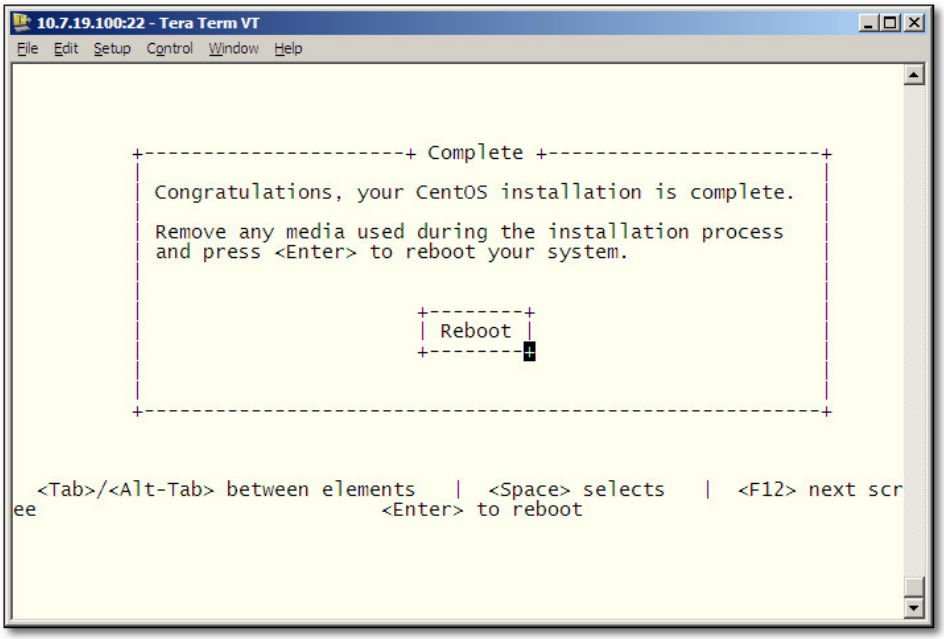
Figure 6-3: CentOS 5



6. Wait for the installation to complete.
7. Reboot your machine by pressing Enter.

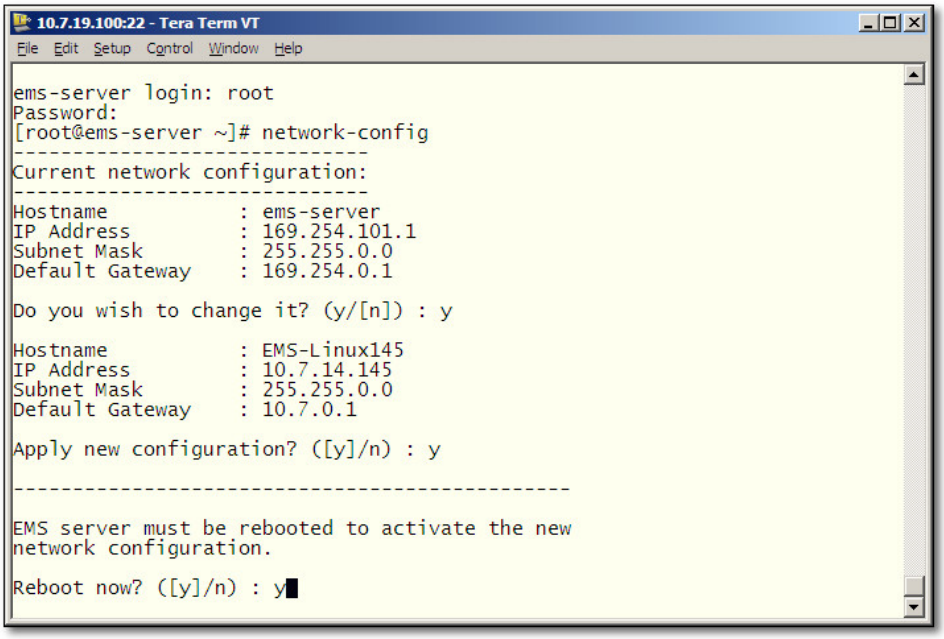
Note: Do not forget to remove the Linux installation DVD from the DVD-ROM before rebooting your machine.

Figure 6-4: Linux CentOS Installation Complete



8. Login as 'root' user with *root* password.
9. Type **network-config**, and then press Enter; the current configuration is displayed:

Figure 6-5: Linux CentOS Network Configuration



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 by entering **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 provide *acems* password.
3. Switch to 'root' user and provide *root* password:

```
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 *acems* password.
3. Switch to 'root' user and provide *root* password:

```
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 (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

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

```
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 as 'acems' user, switch to 'root' user and verify that the Date and Time are set correctly (see Section 10.7 on page 101 to set the date and time).
11. Verify that the EMS server is up and running (see Section 10.5 on page 81) 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/ Telnet/FTP 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 41).
- Installing the EMS server on Microsoft Hyper-V platform (see Section 7.2 on page 48).

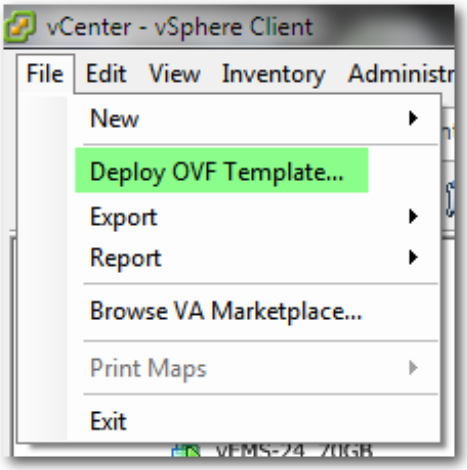
7.1 Installing the EMS Server on the VMware Platform

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 on page 27) and depends largely on the hardware machine where the VMware vSphere platform is installed.

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

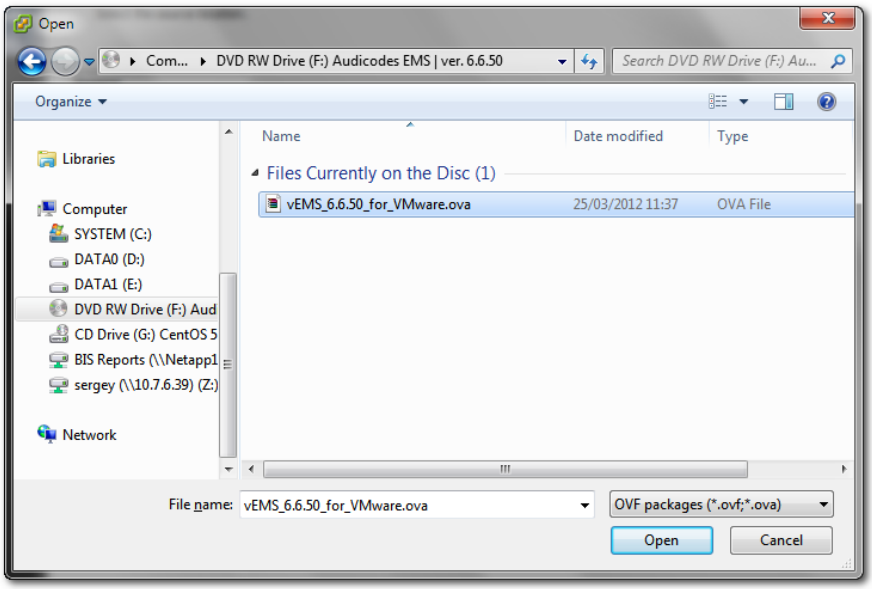
1. Insert the vEMS installation DVD (DVD5) into the disk reader on the PC where the installed vSphere client is installed.

Figure 7-1: Deploy OVF Template Option



2. On the vSphere client, from the menu, choose **File > Deploy OVF Template**.

Figure 7-2: Open OVA Package



3. Select the vEMS virtual appliance file with extension OVA from the inserted DVD disk, and then click **Next**.

Figure 7-3: OVF Template Source Screen

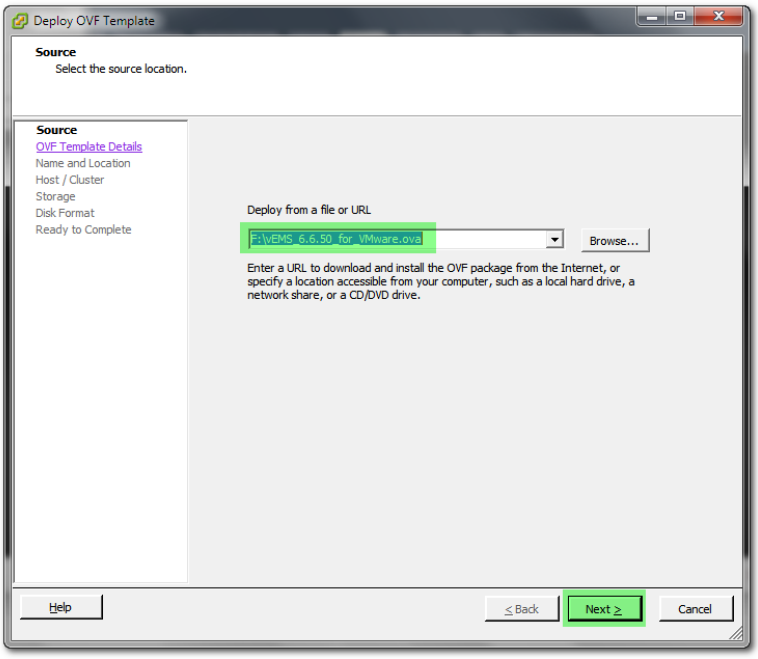
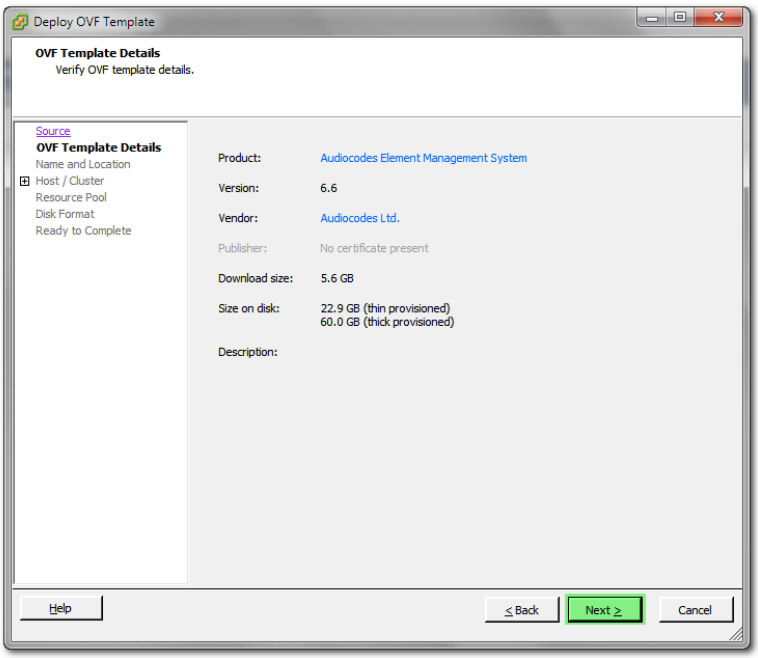
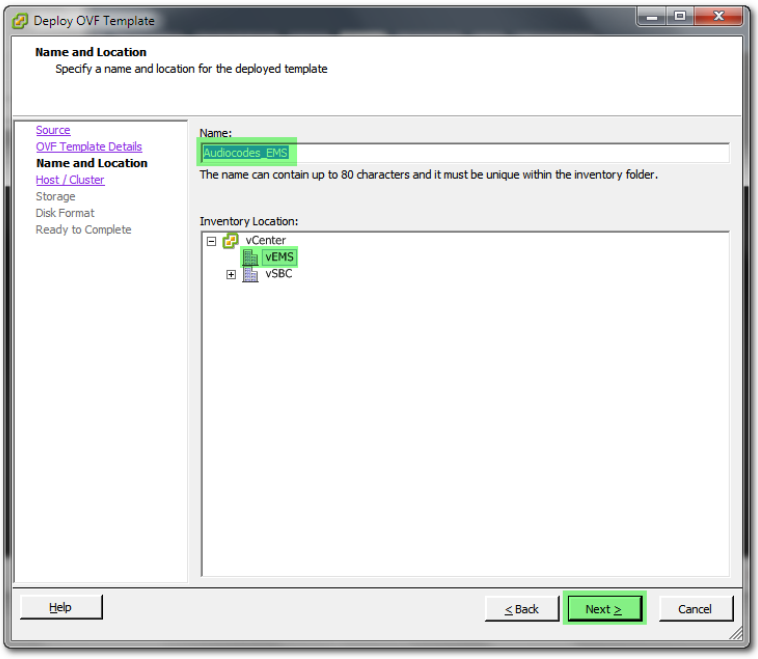


Figure 7-4: OVF Template Details Screen



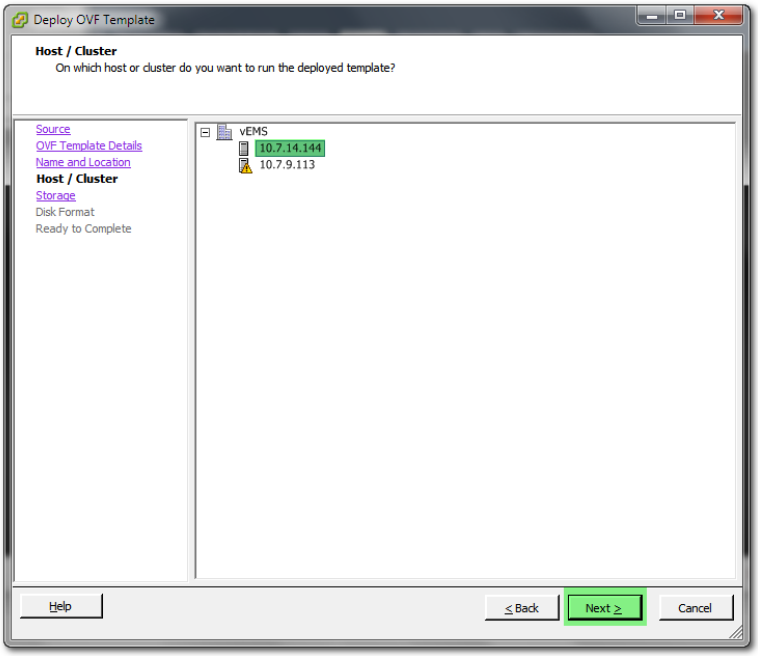
4. In the OVF Template Details screen, click **Next**.

Figure 7-5: Virtual Machine Name and Location Screen



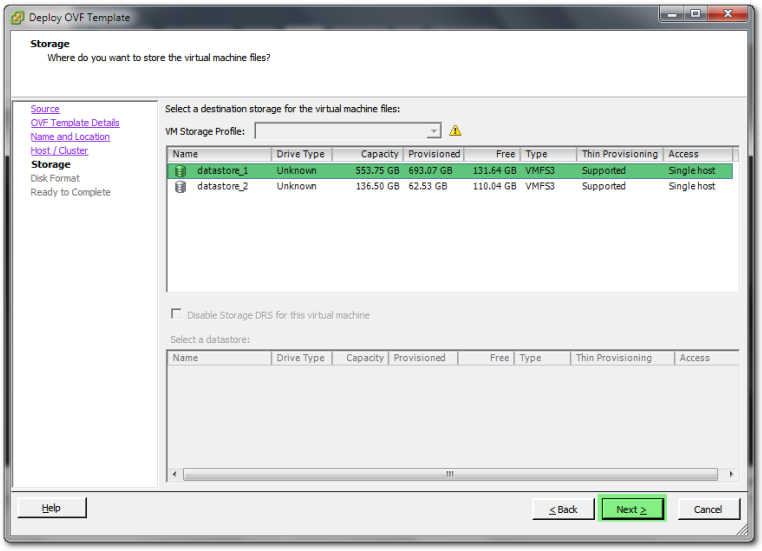
5. In the Name and Location screen, enter the desired virtual machine name and choose the inventory location (the data center to locate the machine), and then click **Next**.

Figure 7-6: Host / Cluster Screen



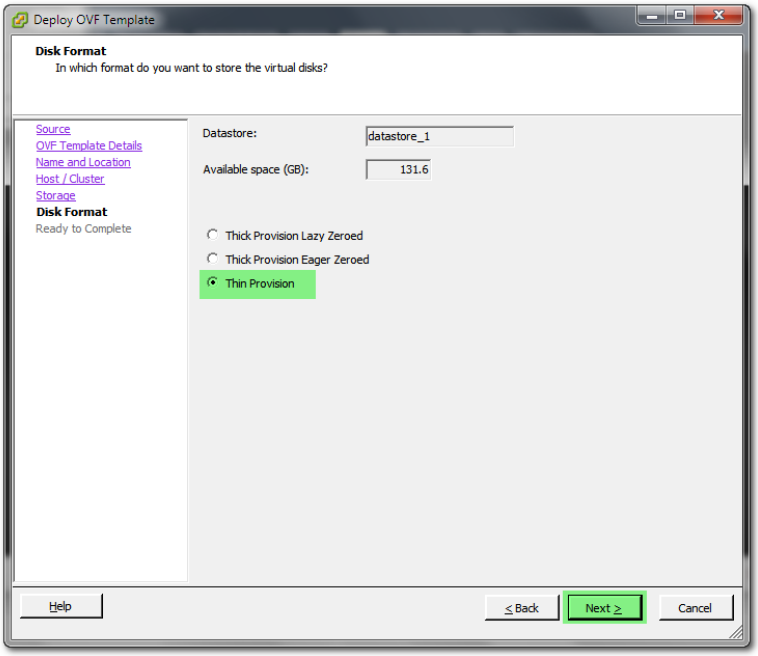
6. In the Host / Cluster screen, select the server to locate the virtual machine, and then click **Next.**

Figure 7-7: Destination Storage Screen



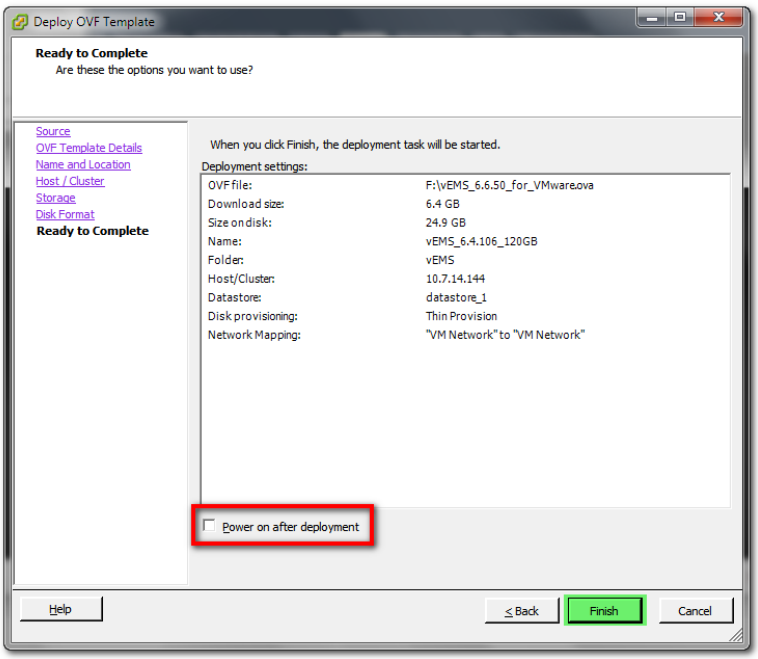
7. In the Storage screen, select the data store where you'd like to locate your machine, and then click **Next**.

Figure 7-8: Disk Format Screen



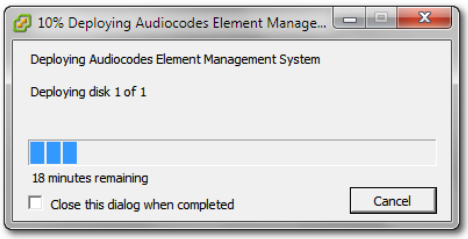
8. In the Disk Format screen, choose the desired provisioning option ('Thin Provisioning' is recommended), and then click **Next**.

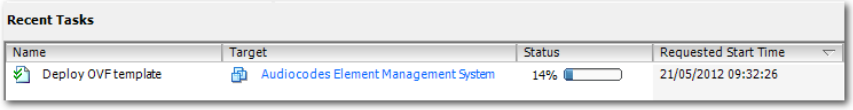
Figure 7-9: Ready to Complete Screen

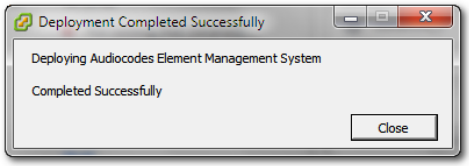


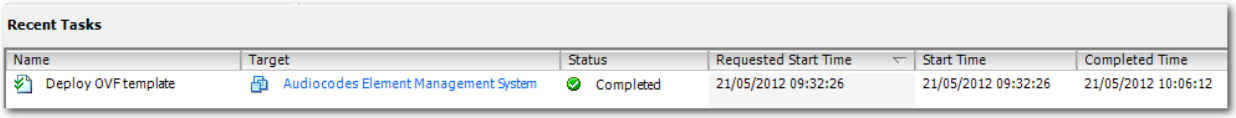
9. In the Ready to Complete screen, leave the option `Power on after deployment` unchecked, and then click **Finish**.

Figure 7-10: Deployment Progress Screen









10. Wait until deployment process has completed. This process may take approximately half an hour.
11. Before powering up the machine, go to the virtual machine **Edit Settings** option.

Figure 7-11: Edit Settings option

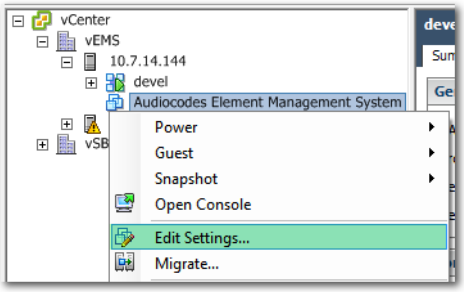
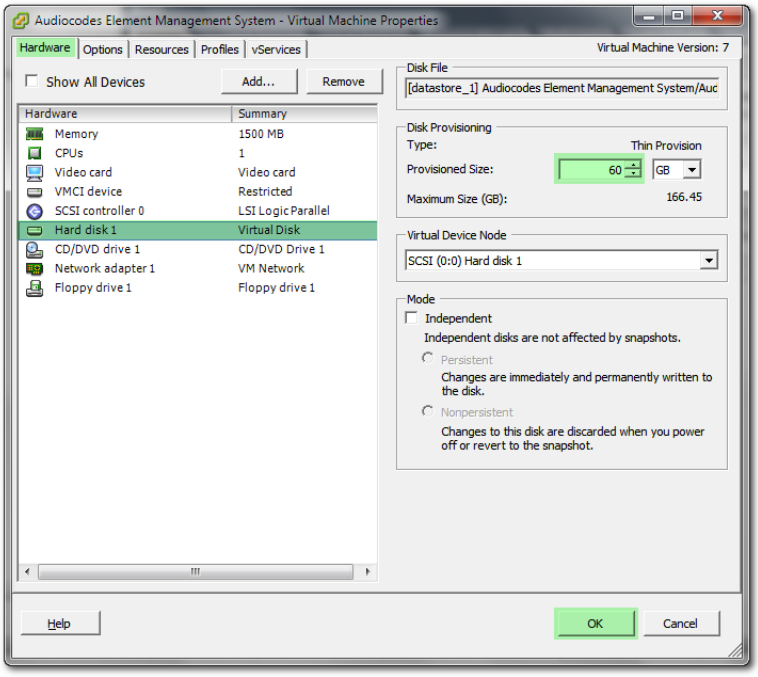


Figure 7-12: Hard Disk Settings

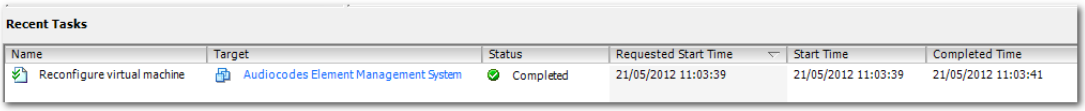


12. In the **Hardware** tab, select the **Hard disk** item, and then set the ˋProvisioned Sizeˋ parameter accordingly to the desired EMS server VMware Disk Space allocation (see Section 3 on page 21), and then click **OK**.

Note: Once the hard disk space allocation has been increased, it cannot be reduced to a lower amount.

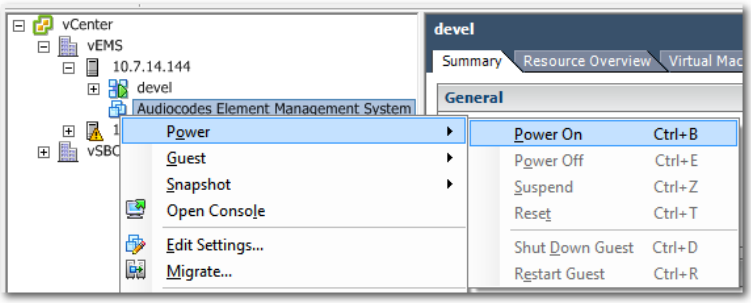
13. **Wait** until the machine reconfiguration process has completed.

Figure 7-13: Recent Tasks



14. 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 Section 3 on page 21).

Figure 7-14: Power On



15. Wait until the boot process is complete, and then connect the running server via the vSphere client console.
16. Login to the server as 'acems' user and enter *acems* password.
17. Switch user to 'root' and enter password *root*.
18. Proceed to the network configuration using the Ems Server Manager. To run the manager type ‘EmsServerManager’, and then press Enter.
19. Set the EMS server network IP address by following the steps in 10.6.1
20. Perform configuration actions as required using the EMS Server Manager (see Section 10 on page 73).

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.

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

- Install the Virtual Machine (VM) (see Section 7.2.1 on page 49).
- Configure the deployed VM (see Section 7.2.2 on page 53 and Section 7.2.3 on page 55).
- Change the default IP address to suite your IP addressing scheme (see Section 7.2.4).

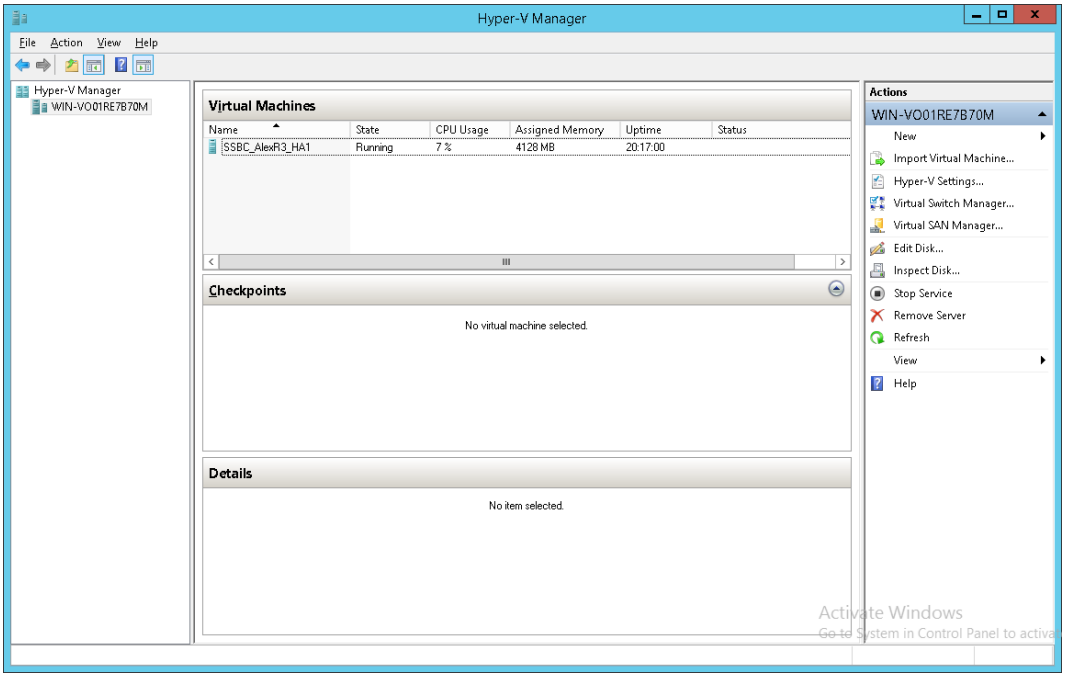
7.2.1 Installing the Virtual Machine

The EMS server is distributed as a VM image (see Section 4.2 on page 24).

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

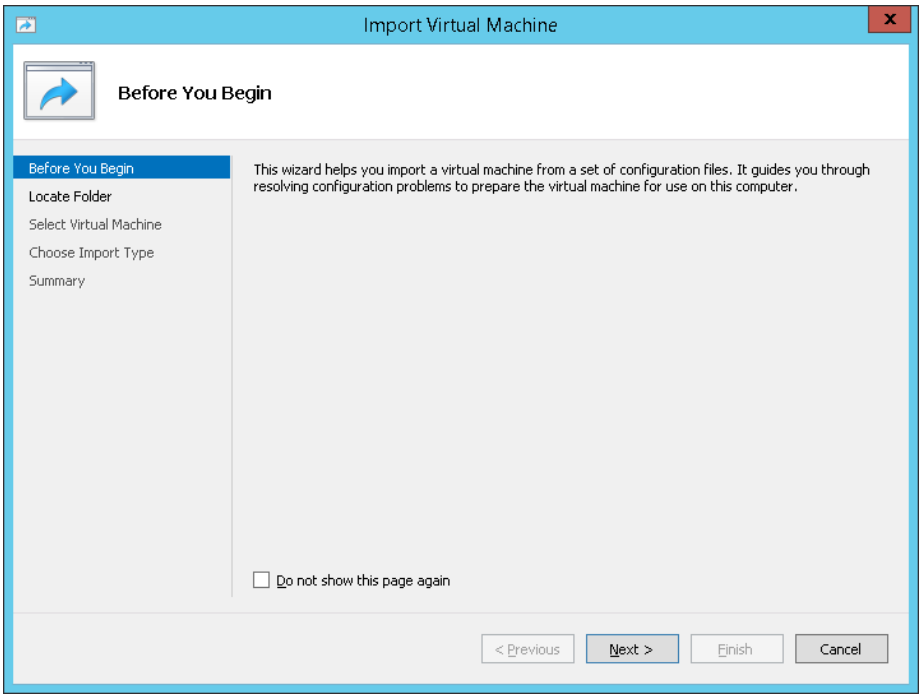
1. Extract the zip file containing the EMS server installation received from AudioCodes to a local directory on the Hyper-V server.
2. Open Hyper-V Manager by clicking **Start** > **Administrative Tools** > **Hyper-V Manager**; the following screen opens:

Figure 7-15: Installing the EMS server on Hyper-V – Hyper-V Manager



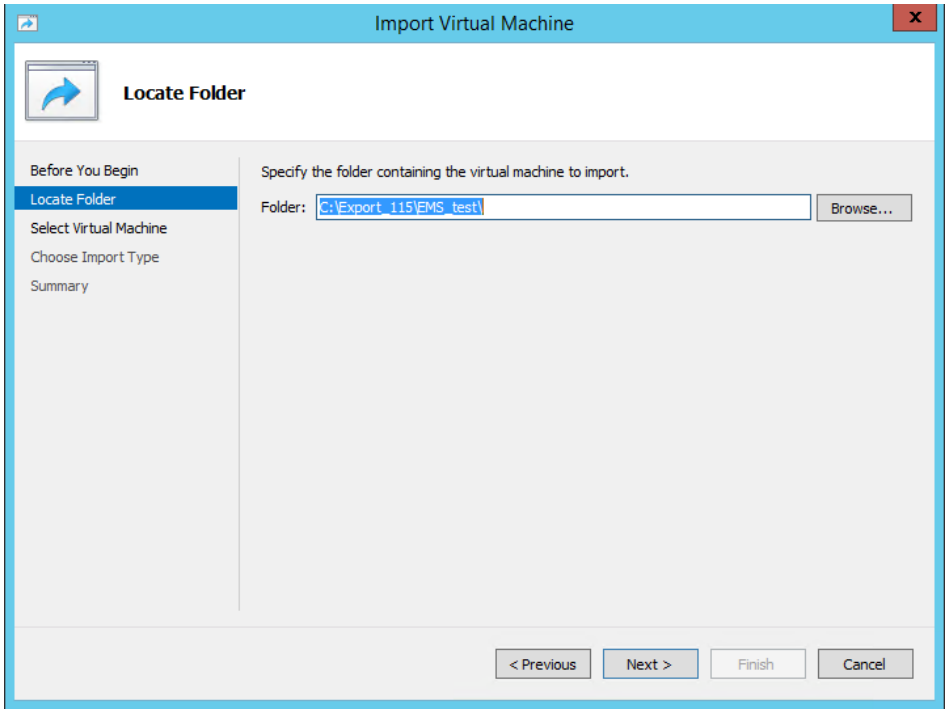
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

Figure 7-16: Installing EMS server on Hyper-V – Import Virtual Machine Wizard



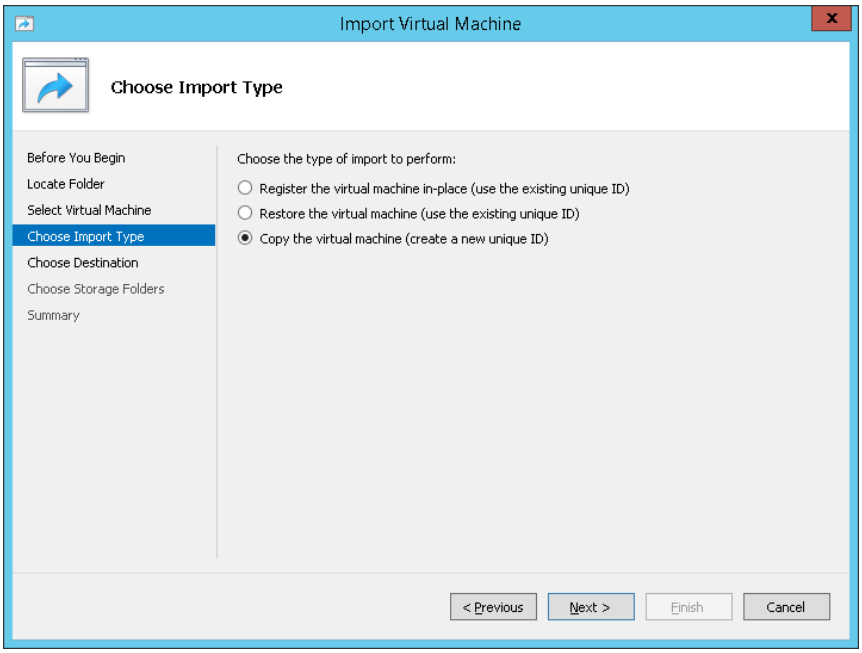
4. Click **Next**; the Locate Folder screen opens:

Figure 7-17: Installing EMS server on Hyper-V – Locate Folder



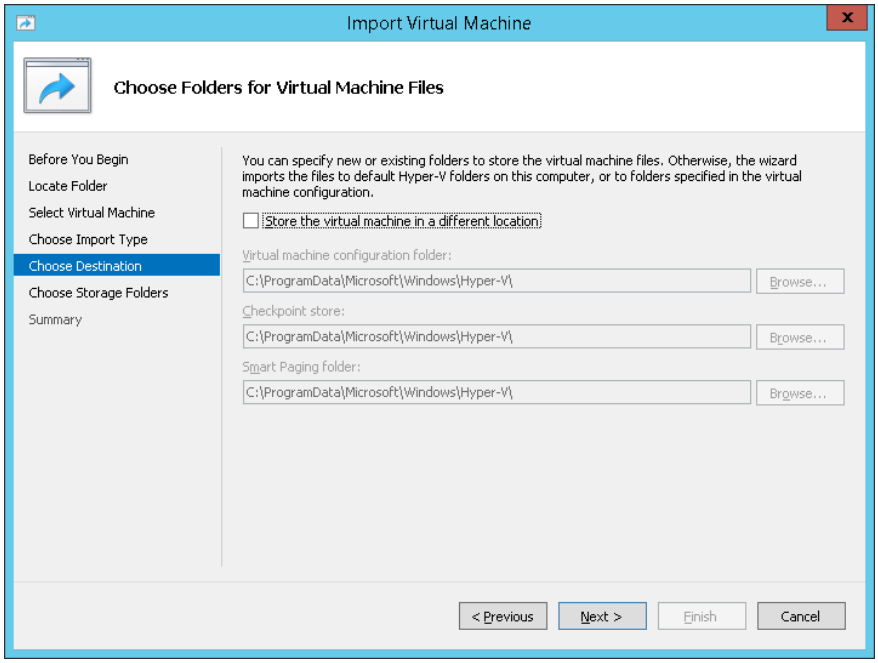
5. Enter the location of the VM installation folder which was previously extracted from the zip file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

Figure 7-18: Installing EMS server on Hyper-V – Choose Import Type



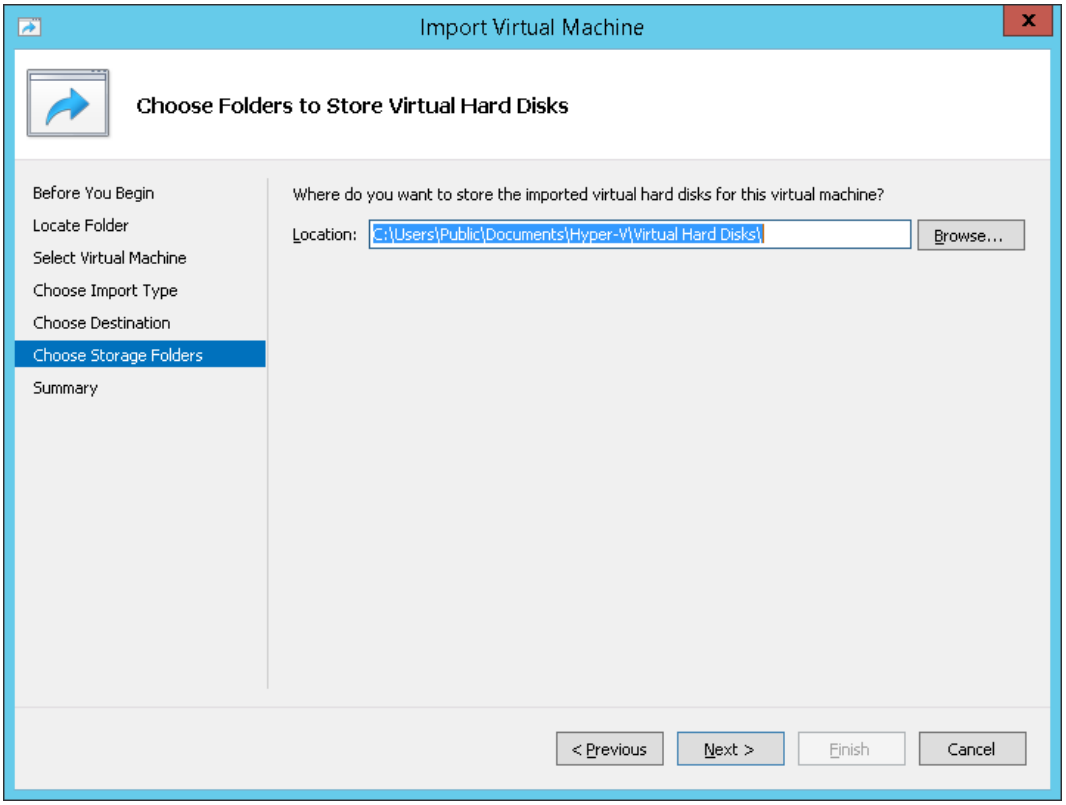
7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

Figure 7-19: Installing EMS server on Hyper-V – Choose Destination



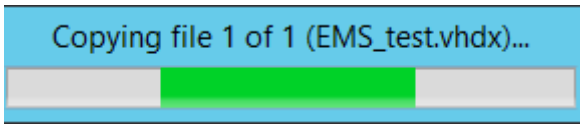
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

Figure 7-20: Installing EMS server on Hyper-V – Choose Storage Folders



9. Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.
10. Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

Figure 7-21: File Copy Progress Bar



This step may take approximately 30 minutes to complete.

11. Proceed to Section 7.2.2 on page 53.

7.2.2 Configuring the Virtual Machine to run the EMS server

This section shows how to configure the Virtual Machine to run the EMS server.

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 Section 3 on page 21.

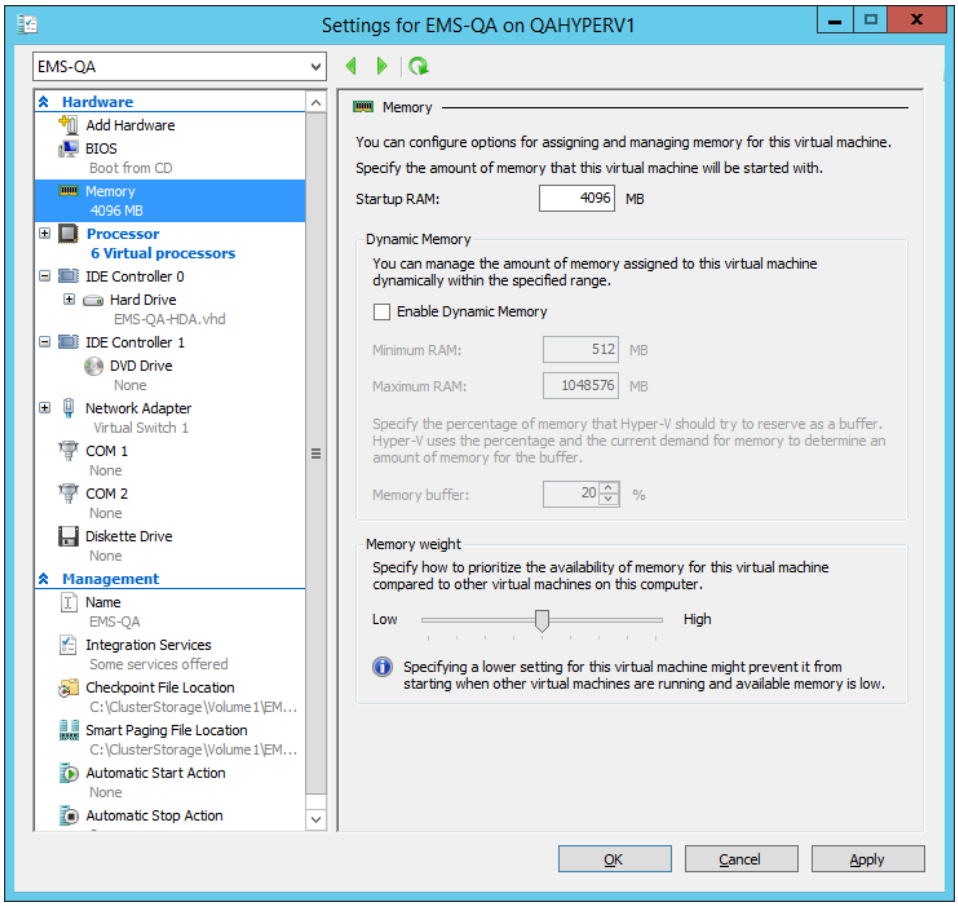
Table 7-1: Virtual Machine Configuration

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

➢ To configure the VM for EMS server:

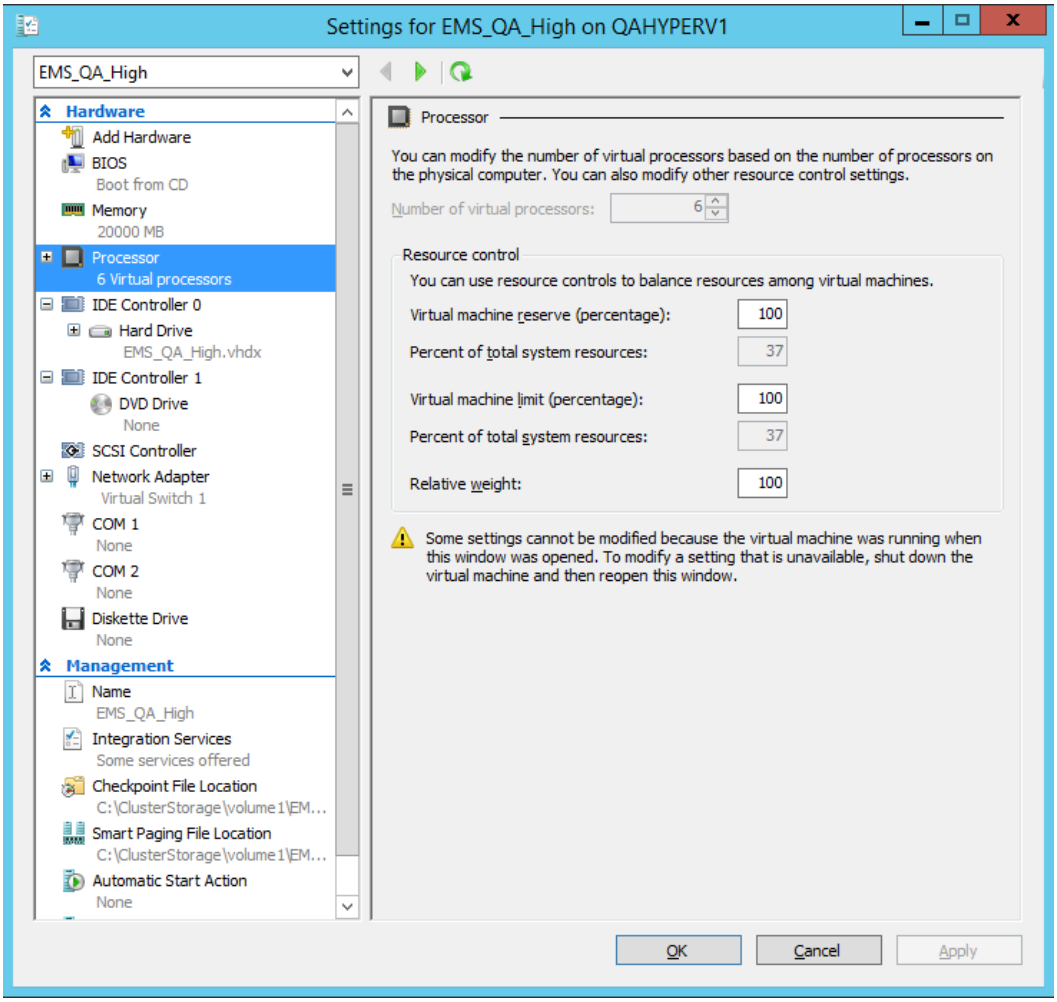
1. Locate the new EMS server VM in the tree in the Hyper-V Manager, right-click it, and then select **Settings**; the Virtual Machine Settings screen opens:

Figure 7-22: Adjusting VM for EMS server – Settings - Memory



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

Figure 7-23: Adjusting VM for EMS server - Settings - Processor



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

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

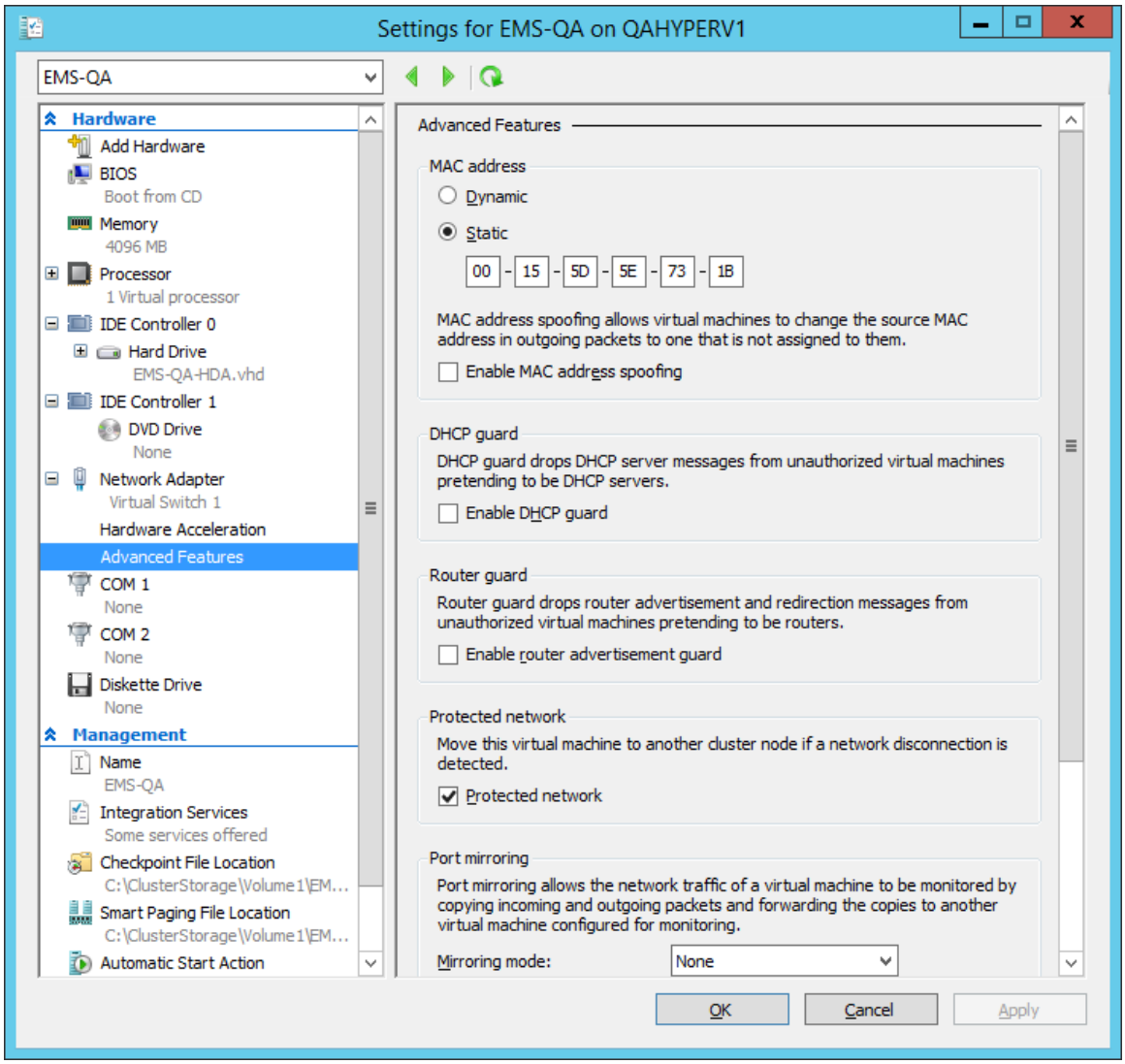
By default, the MAC addresses of the EMS server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license for features such as 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 10.5.4 on page 85).
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 7-24: Advanced Features - Network Adapter – Static MAC Address



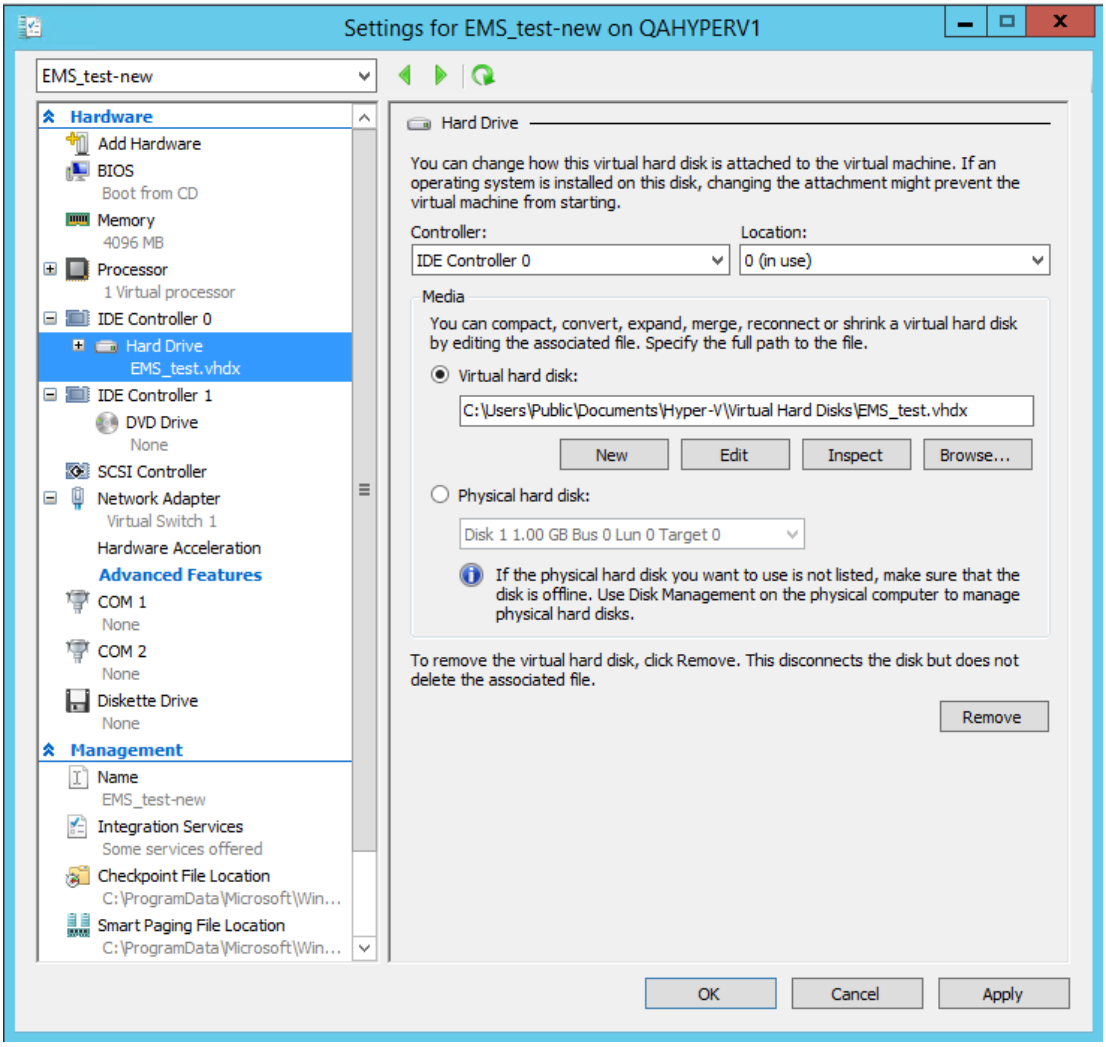
7.2.4 Expanding Disk Capacity

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:**

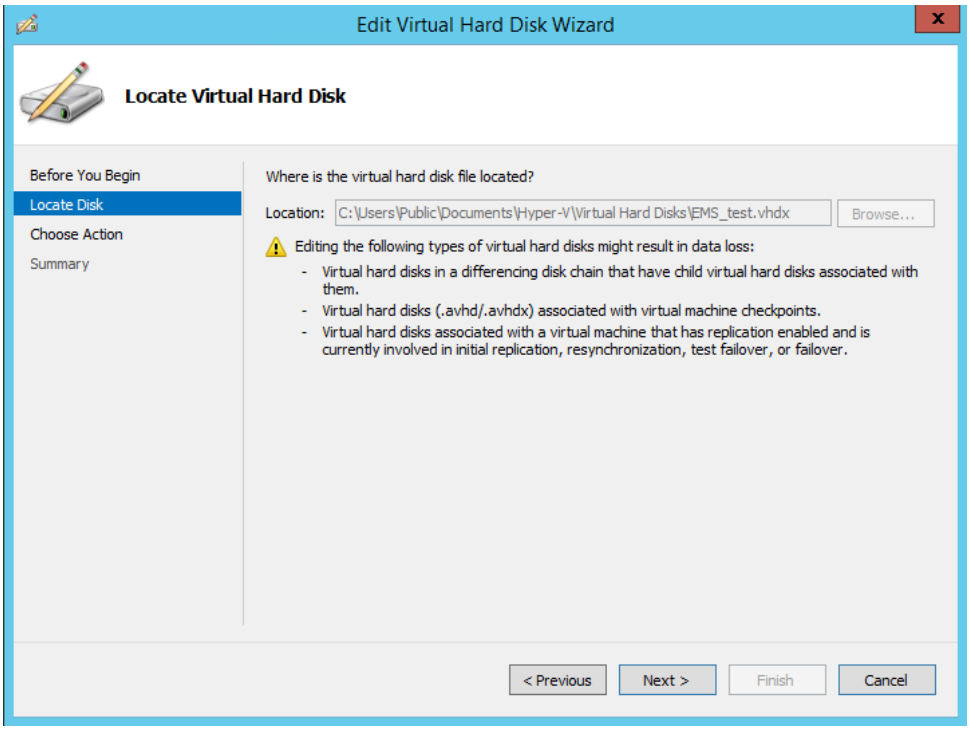
1. Make sure that the target EMS server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

Figure 7-25: Expanding Disk Capacity



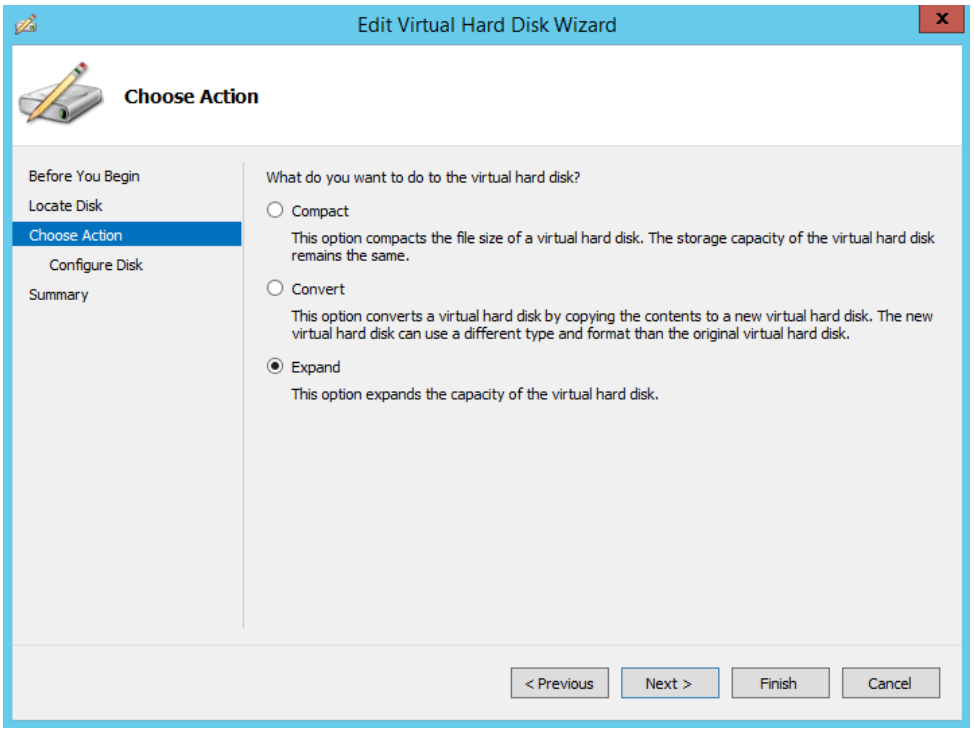
The Edit Virtual Disk Wizard is displayed as shown below.

Figure 7-26: Edit Virtual Hard Disk Wizard



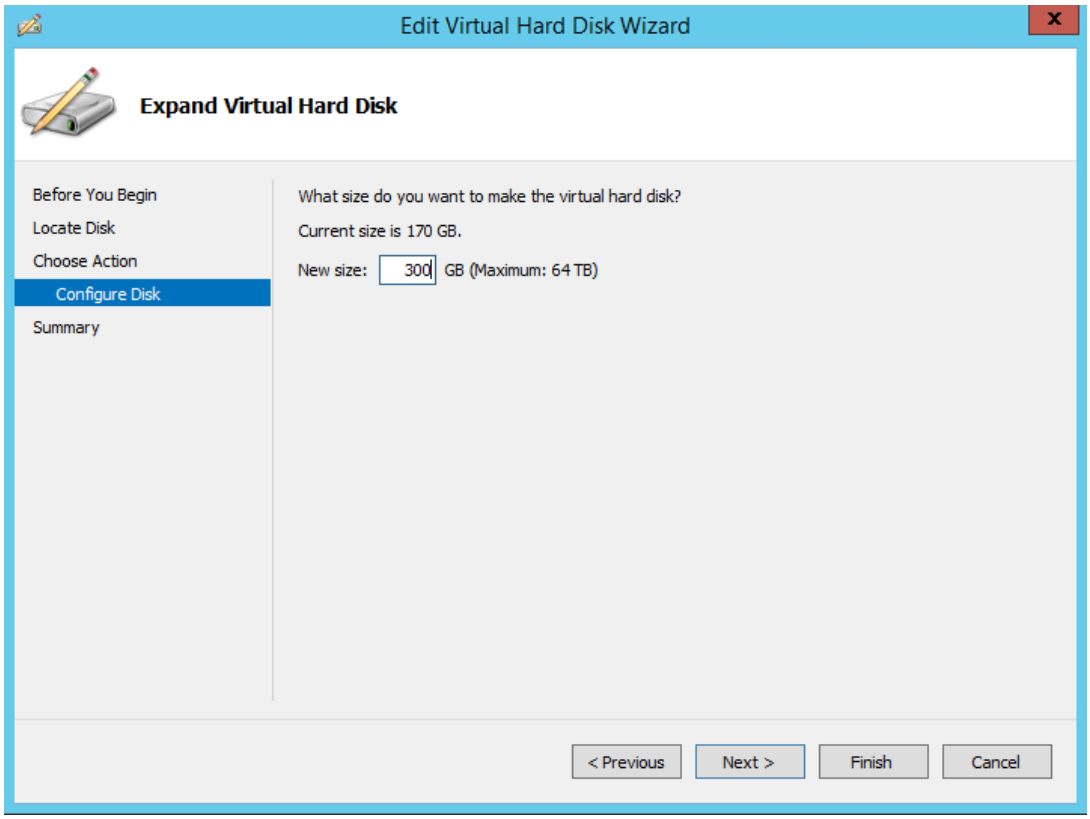
3. Click **Next**; the Choose Action screen is displayed:

Figure 7-27: Edit Virtual Hard Disk Wizard-Choose Action



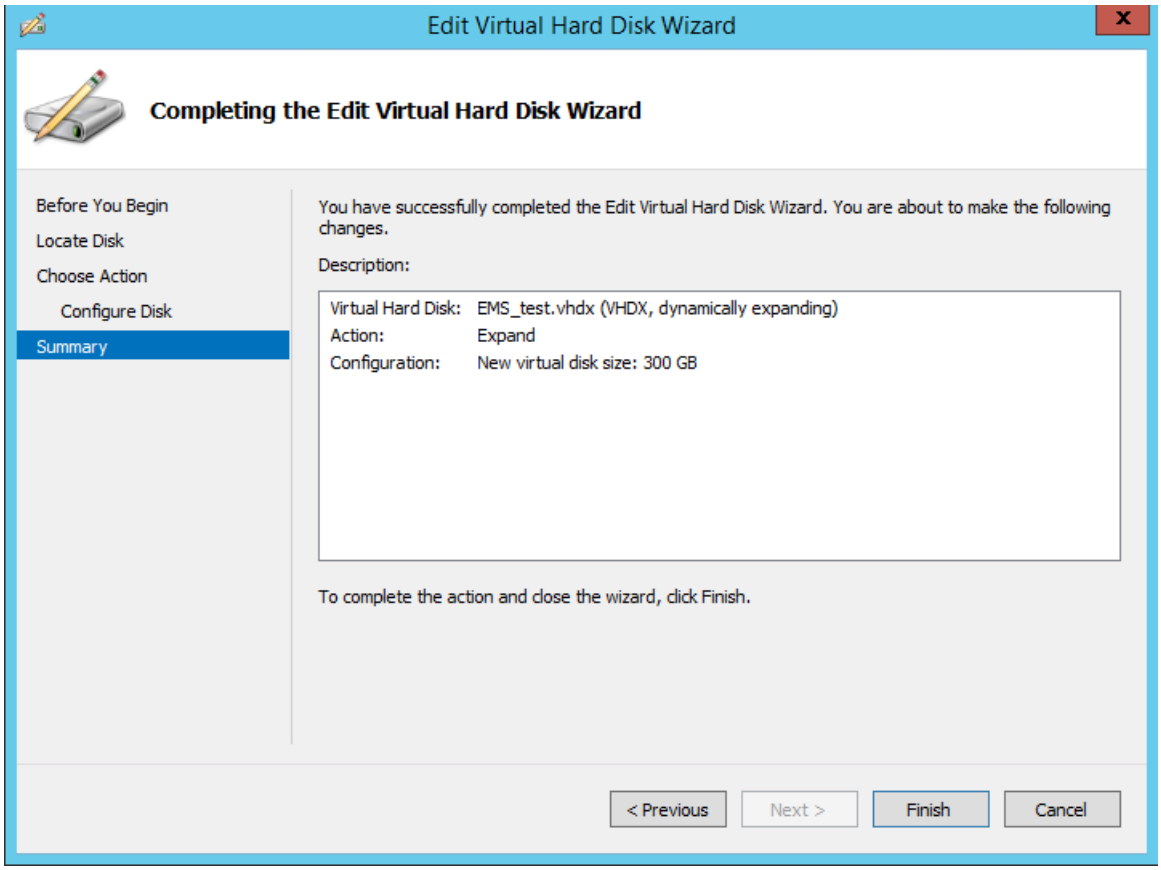
4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

Figure 7-28: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk



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

Figure 7-29: Edit Virtual Hard Disk Wizard-Completion



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

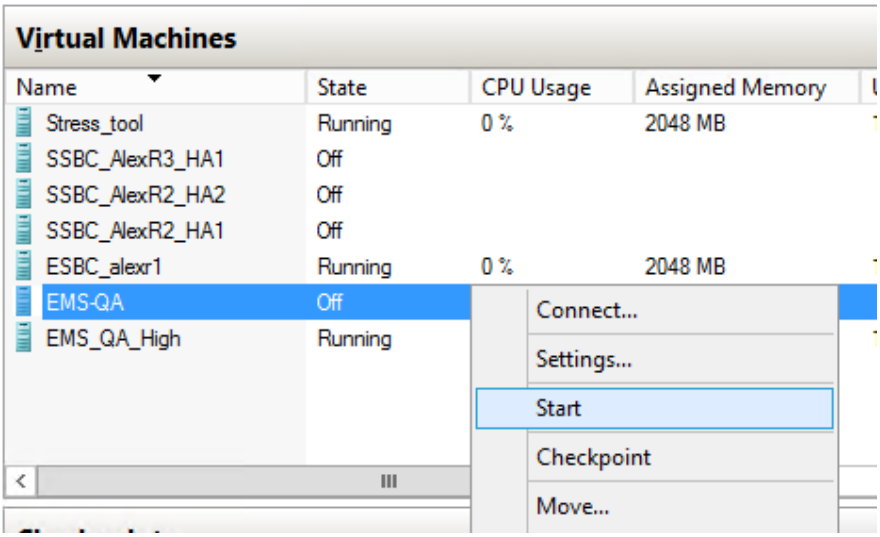
7.2.5 Assigning EMS Server IP Address to Network

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:**

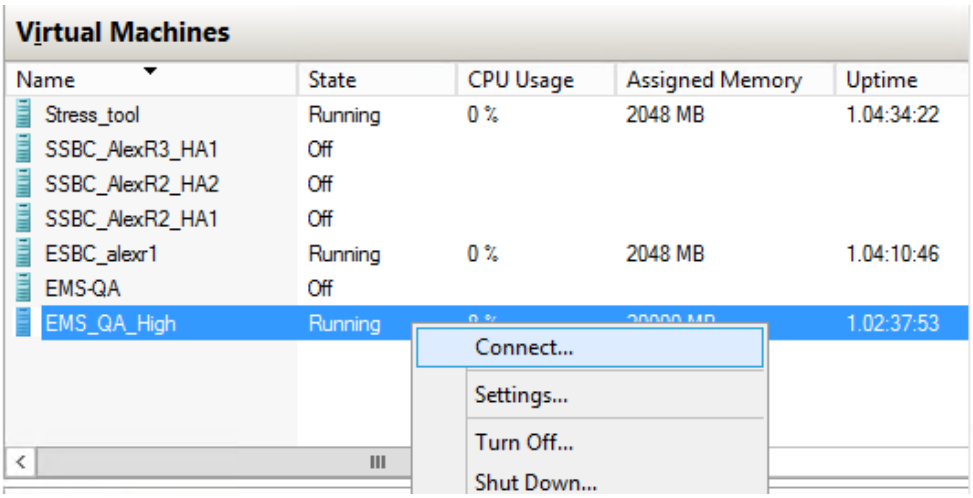
1. Start the EMS server virtual machine, on the Hyper-V tree, right-click the EMS server, and then in the drop-down menu, choose **Start**.

Figure 7-30: Power On Virtual Machine



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**.

Connect to EMS Server Console



3. When the EMS server completes the start-up process, connect to the EMS server as 'acems' with password *acems*.

4. Switch user to 'root', and then enter password *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 10.6.1).
7. Perform other configuration actions as required using the EMS Server Manager (see Section 10 on page 73).

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 hardware.

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 Section B on page 167.

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 6.8 as described in Section 6 on page 29.

8.1 Upgrading the EMS Server

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 6.6, only DVD3 is required. Verify in the EMS Manager 'General Info' screen that you have installed the latest Linux revision (OS Revision **Rev4**), see Section 10.3 on page 77. If you have an older OS revision, a clean installation must be performed using all three DVDs (see Section 6.2 on page 31).

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 provide *acems* password.
3. Switch to 'root' user and provide *root* password:

```
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 (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

Figure 8-2: EMS Server Upgrade (Linux) – License Agreement

```
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
```

This page is intentionally left blank

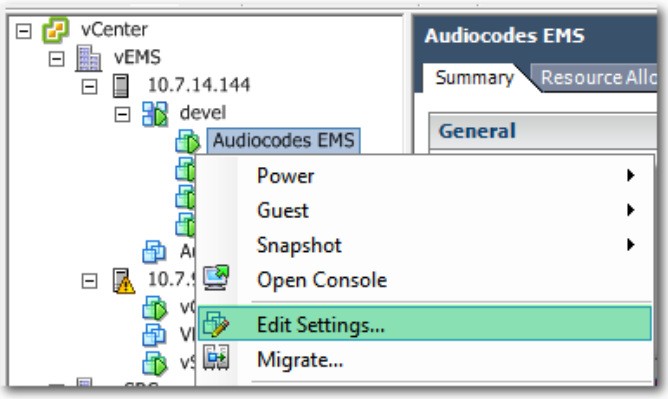
9 Upgrading the EMS Server on the VMware Platform

This section describes how to upgrade the EMS server on the VMware platform.

➢ To upgrade the EMS server on the VMware platform:

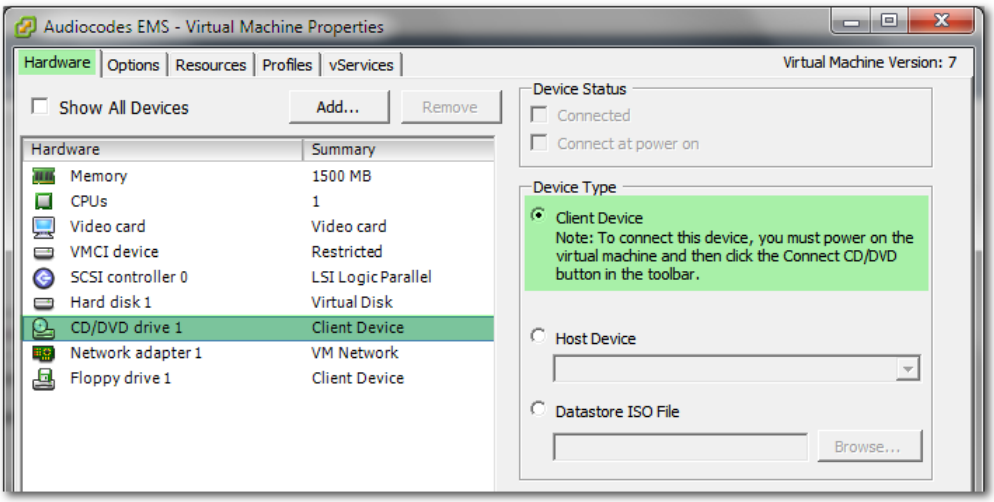
1. Insert the **DVD3-EMS Server Application Installation** into the disk reader on the PC with the installed vSphere client.
2. In the vCenter navigation tree, right-click the AudioCodes EMS node and choose the **Edit Settings** option.

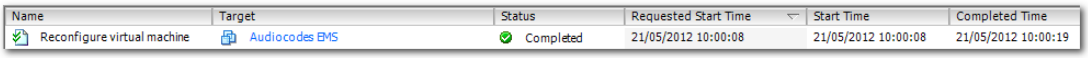
Figure 9-1: Edit Settings Option



3. In the **Hardware** tab, select the CD/DVD drive item, mark the Client Device option and wait until the machine reconfiguration has completed.

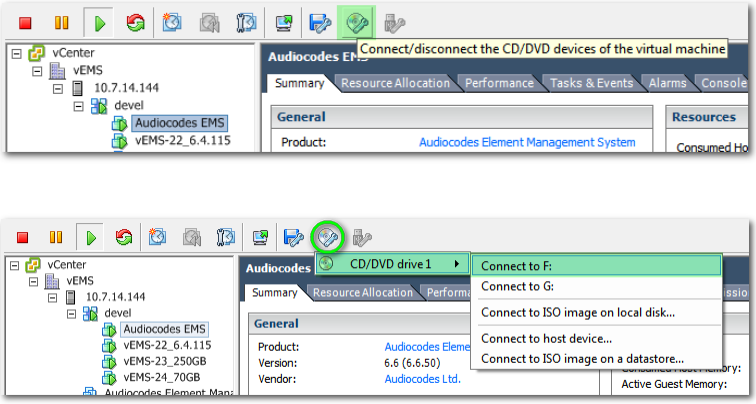
Figure 9-2: Hardware Tab





4. In the toolbar, click the **Connect/disconnect the CD/DVD devices of the virtual machine** option, and then in drop-down menu, choose your DVD-reader device.

Figure 9-3: Connect/disconnect Button



5. Connect to the vEMS server via SSH and switch user to *root*.

```
su -
```

```
[acems@ems-server ~]$
[acems@ems-server ~]$ su -
Password:
[root@ems-server ~]#
```

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.

6. Change directory to '/misc/cd/EmsServerInstall' and run the install script.

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

Figure 9-4: 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
```

7. Perform steps 6 to 10 in Section on page 65.

Part IV

EMS Server Machine Maintenance

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

10 EMS Server Manager

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 via 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**.

10.1 Getting Started with EMS Server Manager

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

10.1.1 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. Connect to the EMS server as 'acems' using Secure Shell (SSH); switch user to root (su - root), and then enter the *root* password.
2. Type the following command:

```
# EmsServerManager
```

The EMS Server Manager menu is displayed:

Figure 10-1: EMS Server Manager Menu

```
                EMS Server 6.8.155 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 Section 10.2 on page 76)
- **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 Section 10.3 on page 77.
- **Collect Logs** – Collates all important logs into a single compressed file (see Section 10.4 on page 79):
  - General Info
  - Collect Logs
- **Application Maintenance** – Manages system maintenance actions (see Section 10.5 on page 81):
  - SNMP Agent
  - Start / Stop the Application
  - Upgrade Application

- Web Servers
- Schedule Automation Backup
- Backup
- Restore
- SEM License Configuration
- Shutdown the EMS server machine
- Reboot the EMS server machine

- **Network Configuration** – Provides all basic, advanced network management and interface updates (see Section 10.6 on page 86):
  - Server's IP Address (Reboot is performed)
  - Ethernet Interfaces (Reboot is performed)
  - Ethernet Redundancy (Reboot is performed)
  - DNS Client
  - NAT
  - Static Routes
  - SNMP Agent
  - SNMPv3 Engine ID
- **Date & Time** – Configures time and date settings (see Section 10.7 on page 101):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (see Section 10.8 on page 105):
  - EMS user
  - SSH Configuration
  - DBA Password (EMS Server will be shut down)
  - OS Passwords Settings
  - File Integrity Checker
  - Software Integrity Checker (AIDE) and Prelinking
- **Diagnostics** – Manages system debugging and troubleshooting (see Section 10.8 on page 105):
  - Syslog Configuration
  - Board Syslog Logging Configuration
  - TP Debug Recording Configuration

10.1.2 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".

10.2 Status

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 10-2: Application Status

10.3 General Information

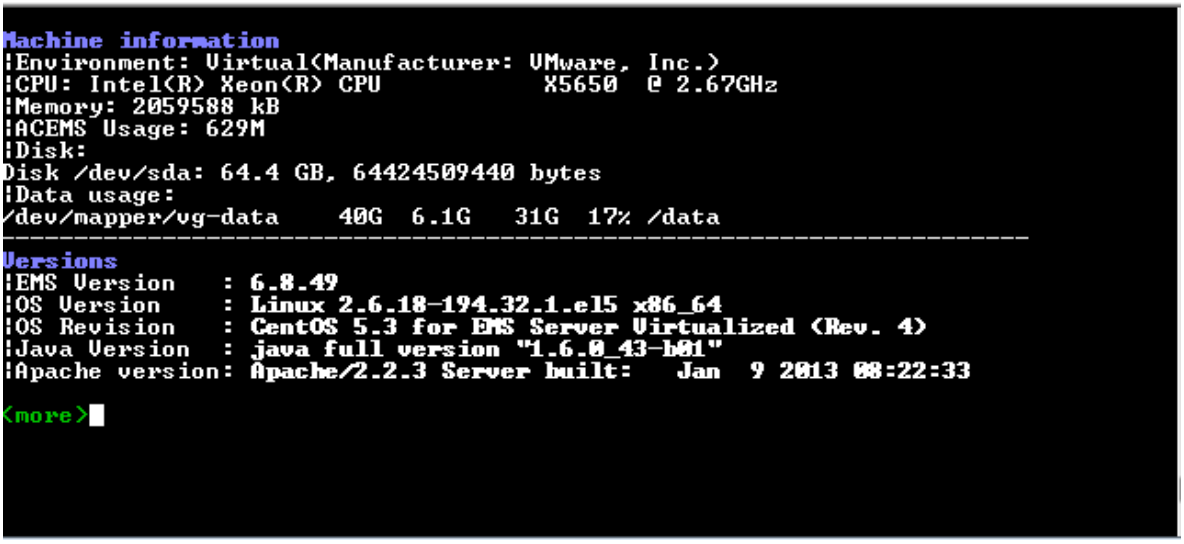
This section describes the General Information and Logs collection options. The General Information option provides detailed information about the EMS server configuration and current status variables. The following information is provided:

- 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 10-3: General Information



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

Figure 10-4: 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...
```

10.4 Collect 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 10-5: 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 10-6: 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
```

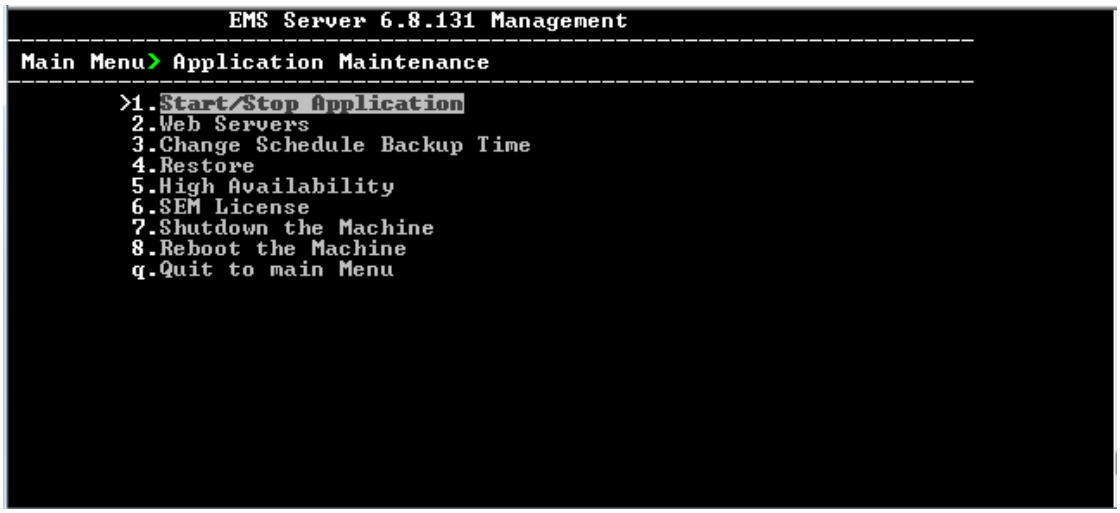
10.5 Application Maintenance

This section describes the application maintenance.

➢ **To configure application maintenance:**

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

Figure 10-7: Application Maintenance



This menu includes the following options:

- Start/Stop Application (see Section 10.5.1 on page 82).
- Web Servers (see Section 10.5.2 on page 83).
- High Availability (see Chapter 11 on page 133).
- SEM License (see Section 10.5.3 on page 84).
- Shutdown the Machine (see Section 10.5.4 on page 85).
- Reboot the Machine (see Section 10.5.5 on page 85).

10.5.1 Start /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 10-8: Start/ Stop EMS Server

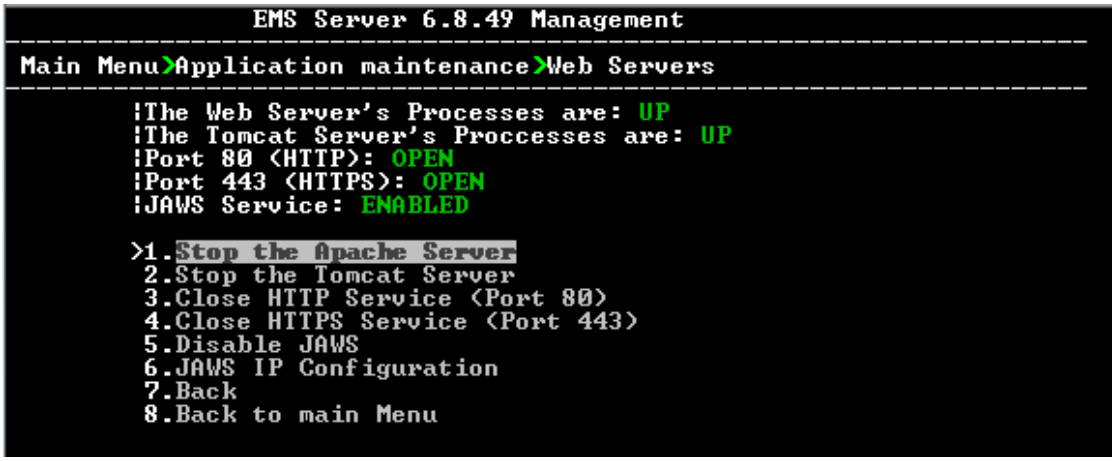
```
                EMS Server 6.8.49 Management
-------------------------------------------------------------------
 Main Menu>Application maintenance
-------------------------------------------------------------------
EMS Server is started. Stop EMS Server?
        >1.Yes
         2.No
```

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

10.5.2 Web Servers

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

Figure 10-9: – Web Servers



➢ **To stop the Apache server:**

- In the Web Servers menu, choose option **1**, and then press Enter.

➢ **To stop the Tomcat server:**

- In the Web Servers menu, choose option **2**, and then press Enter.

➢ **To close HTTP Service (Port 80):**

- In the Web Servers menu, choose option **3**, and then press Enter.

➢ **To close HTTP Service (Port 443):**

- In the Web Servers menu, choose option **4**, and then press Enter.

➢ **To disable JAWS:**

- In the Web Servers menu, choose option **5**, and then press Enter.

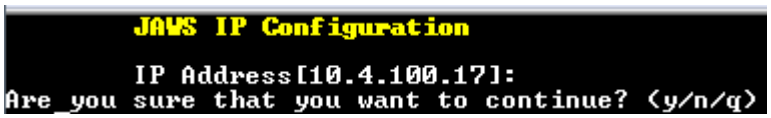
10.5.2.1 JAWS IP Configuration

By default, logging into the EMS server using JAWS can only be performed via 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 10-10: JAWS IP Configuration



10.5.3 SEM License

You can view the details of the existing SEM Server License or upload a new license.

➢ **To configure the SEM license configuration:**

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

Figure 10-11: SEM License Configuration Manager

2. To load a new SEM Server License, choose option **1**.
3. Enter the SEM License File path and name.
4. Restart the EMS server.

10.5.4 Shutdown the EMS Server Machine

This section describes how to shutdown the EMS Server machine.

➢ **To shutdown 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.

10.5.5 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.

10.6 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 10-12: Network Configuration

```
                EMS Server 6.8.49 Management
-----------------------------------------------------------------------
Main Menu> Network Configuration
-----------------------------------------------------------------------
        >1.Server IP Address      (Reboot is performed)
         2.Ethernet Interfaces    (Reboot is performed)
         3.Ethernet Redundancy    (Reboot is performed)
         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's IP Address (see Section 10.6.1 on page 87).
- Ethernet Interfaces (see Section 10.6.2 on page 88).
- Ethernet Redundancy (see Section 10.6.3 on page 92).
- DNS Client (see Section 10.6.4 on page 97).
- NAT (see Section 10.6.5 on page 98).
- Static Routes (see Section 10.6.6 on page 99).
- SNMP Agent (see Section 10.6.7 on page 100).
- SNMPv3 Engine ID (see Section 10.6.8 on page 100).

10.6.1 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 10-13: 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 10-14: 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.

10.6.2 Ethernet Interfaces

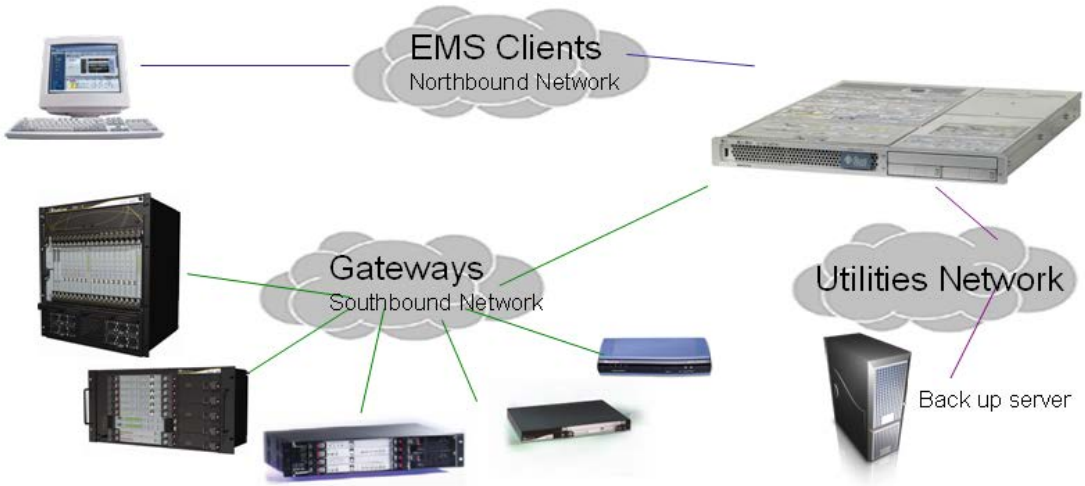
This section describes how to configure ethernet interfaces.

10.6.2.1 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 10-15: 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 10.6.6 on page 99.

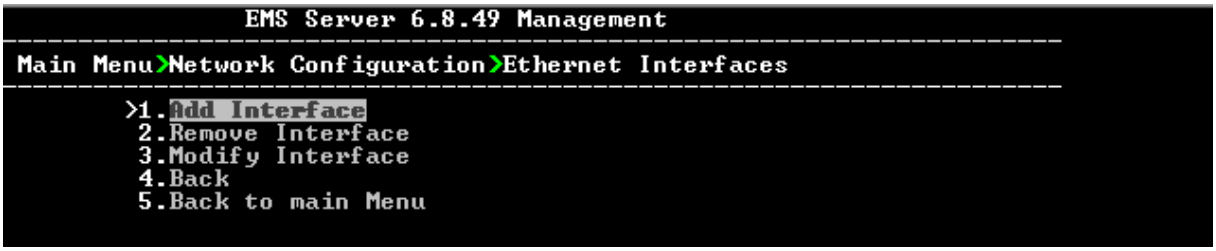
To ensure that the network configuration is performed successfully, test that the EMS is successfully connected to each one of the gateways by running the following basic tests:

- 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 10-16: EMS Server Manager – Configure Ethernet Interfaces



2. Choose from one of the following options:
   - **Add Interface** – Adds a new interface to the EMS server (see Section 10.6.2.2 on page 90).
   - **Remove Interface** – Removes an existing interface from the EMS server (see Section 10.6.2.3 on page 91).
   - **Modify Interface** – Modifies an existing interface from the EMS server (see Section 3 on page 91).

10.6.2.2 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 10-9: 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)
```

10.6.2.3 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.

10.6.2.4 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.

10.6.3 Ethernet Redundancy

This section describes how to configure Ethernet Redundancy.

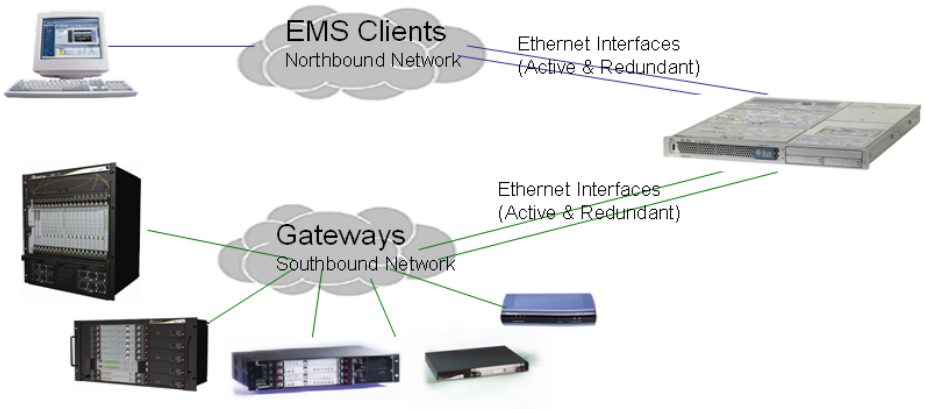
Physical Ethernet Interfaces Redundancy provides failover when you have multiple network interface cards that are connected to the same IP link.

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.

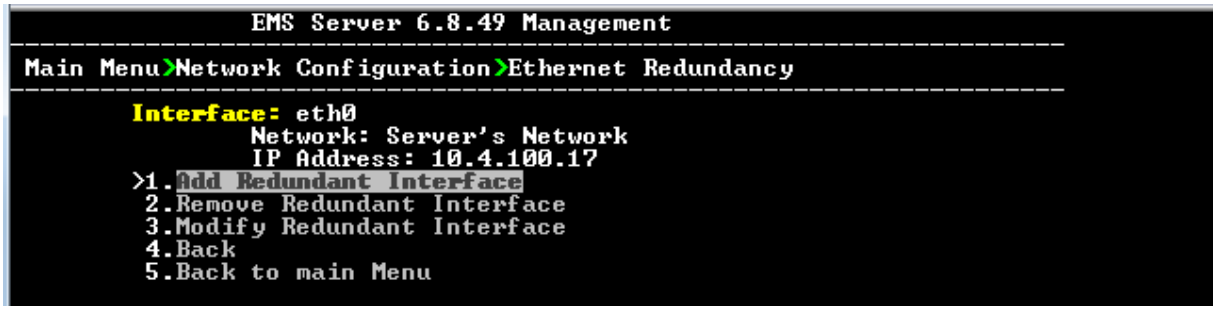
Figure 10-17: Physical Ethernet Interfaces Redundancy



➢ **To configure Ethernet Redundancy:**

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

Figure 10-18: Ethernet Redundancy Configuration



2. This menu includes the following options:
   - Add Redundant Interface (see Section 10.6.3.1 on page 93.
   - Remove Redundant Interface (see Section 10.6.3.2 on page 95).
   - Modify Redundant Interface (see Section 10.6.3.3 on page 96).

10.6.3.1 Add Redundant Interface

Remove a redundant interface under the following circumstances:

- You have configured an Ethernet interface (see Section 10.6.2 on page 88).
- 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 10-19: 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)
```

10.6.3.2 Remove Ethernet Redundancy

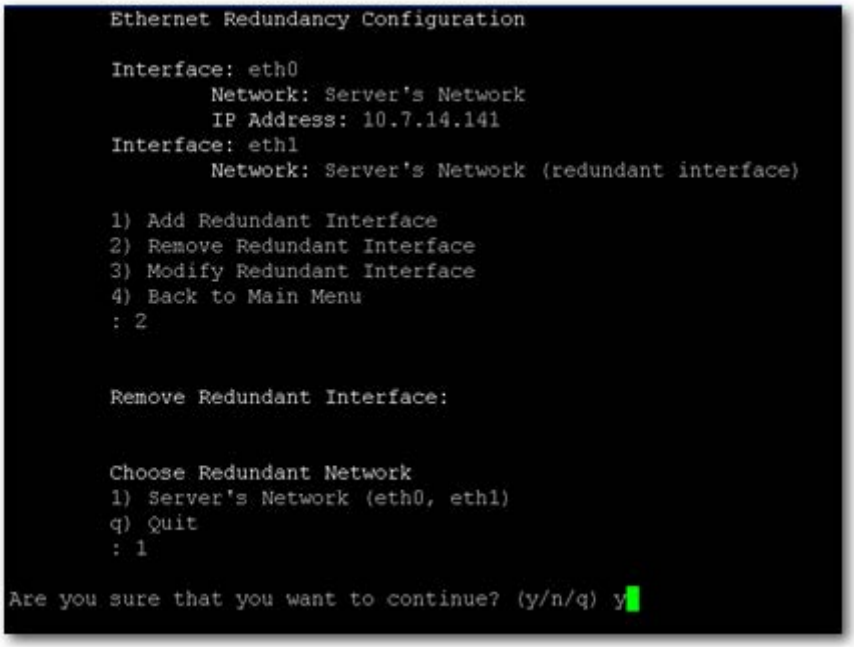
This section describes how to remove an ethernet redundancy interface.

➢ **To remove the Ethernet Redundancy interface:**

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

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

Figure 10-20: Ethernet Redundancy Interface to Disable



10.6.3.3 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 10-21: 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
```

10.6.4 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 10-22: 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.

10.6.5 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.

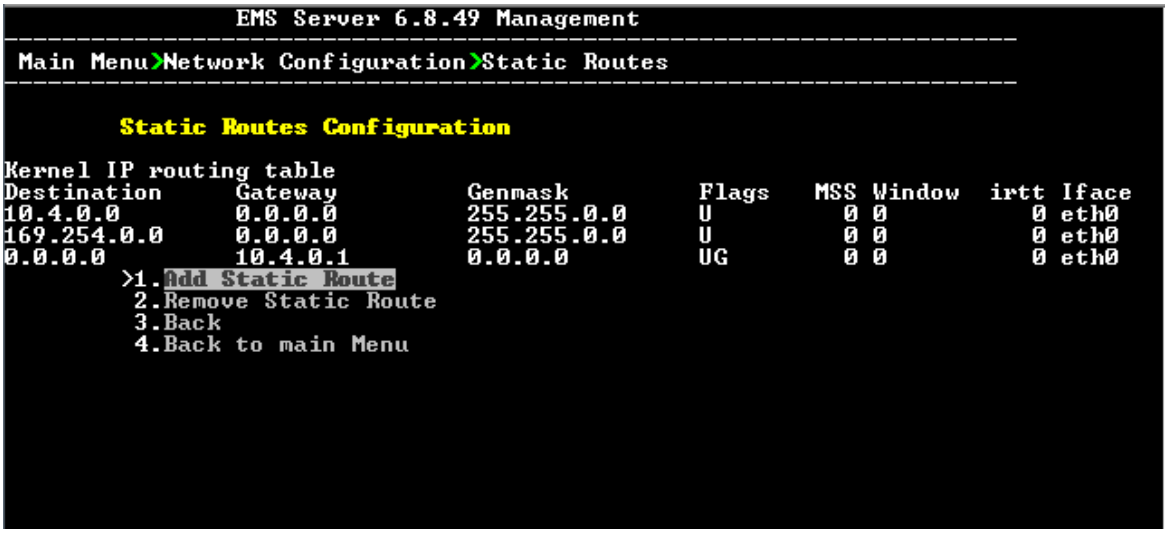
10.6.6 Static Routes

This option enables you to add or remove static route rules. Static routes are usually only used in conjunction with a **/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 10-23: Routing Table and Menu



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

➢ To add a static route:

1. From the Static Routes menu, choose option **1**.
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.

10.6.7 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.

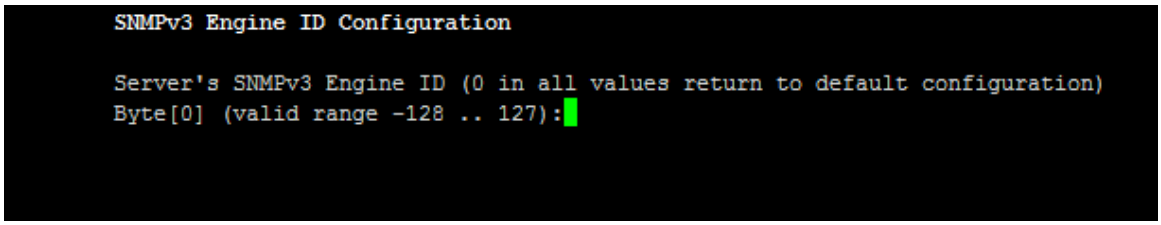
10.6.8 Server SNMPv3 Engine ID

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 10-24: EMS Server Manager – Configure SNMPv3 Engine ID



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

Figure 10-25: 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)
```

10.7 Date and Time Settings

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

➢ **To change system time and date:**

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

Figure 10-26: EMS Server Manger - Change System Time & Date

```
                EMS Server 6.8.49 Management
-------------------------------------------------------------------------
 Main Menu>Date & Time
-------------------------------------------------------------------------
        >1.NTP
         2.Timezone Settings     <Reboot is performed>
         3.Date & Time Settings
         4.Back to main menu
```

This menu includes the following options:

- NTP (see Section 10.7.1 on page 102)
- Timezone Settings (see Section 10.7.2 on page 103)
- Date & Time Settings (see Section 10.7.3 on page 103)

10.7.1 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 synchronize its clock with other devices in the IP network. These devices can be any device containing an NTP server or client, such as the Mediant 5000 or Mediant 8000 Media Gateways.

Alternatively you can configure the NTP server to allow other devices 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.

➢ **To configure NTP:**

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

Figure 10-27: EMS Server Manager - Configure NTP

```
                EMS Server 6.8.49 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
==============================================================================
*LOCAL(0)        .LOCL.          13 1   53   64  377    0.000    0.000   0.001
        >1.Configure NTP
         2.Stop NTP
         3.Restrict access to NTP clients
         4.Back
         5.Back 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.

10.7.1.1 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.

10.7.1.2 Allow and Restrict Access to NTP Clients

This section describes how to allow access to NTP clients.

➢ **To allow access to NTP clients:**

1. From the NTP menu, choose option **3**, and then press Enter; the following is displayed:

Figure 10-28: Allow Access to NTP Clients

```
                EMS Server 6.8.49 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
==========================================================================
*LOCAL(0)        .LOCL.          13 l   31   64  377    0.000    0.000   0.001
        >1.Configure NTP
         2.Stop NTP
         3.Restrict access to NTP clients
         4.Back
         5.Back to main Menu
```

2. Type **3** to either allow or restrict access to NTP clients; the screen is updated accordingly.

10.7.2 Timezone Settings

This option enables you to change the timezone of the EMS server. For more information, go to '/usr/share/lib/zoneinfo/src/README'.

➢ **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 automatically reboots for the changes to take effect.

10.7.3 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 10-29: 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.

10.8 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:**

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

Figure 10-30: Security Settings

```
                EMS Server 6.8.155 Management
-----------------------------------------------------------------------
 Main Menu> Security
-----------------------------------------------------------------------
        >1.Add EMS User
         2.SSH
         3.DB Password  (Reboot is performed)
         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  (Reboot is performed)
         q.Quit to main Menu
```

This menu includes the following options:

- Add EMS User (see Section 10.8.1 on page 106).
- SSH Server Configuration Manager (see Section 10.8.2 on page 100.
- Changing DBA Password (see Section 10.8.3 on page 120).
- OS Password Settings (see Section 10.8.4 on page 120.
- Start / Stop File Integrity Checker (see Section 10.8.5 on page 124.
- Software Integrity Checker (AIDE) and Prelinking (see Section 10.8.6 on page 124).
- USB Storage (see Section 10.8.7 on page 125).
- Network options (see Section 10.8.8 on page 126).
- Audit Agent Options (see Section 10.8.9 on page 126).

10.8.1 Add EMS User

This option enables you to add a new 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.

10.8.2 SSH Server Configuration Manager

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 10-31: SSH Configuration

```
                EMS Server 6.8.155 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 10.8.2.1 on page 108).
- Configure SSH Banner (see Section 10.8.2.2 on page 109).
- Configure SSH on Ethernet Interfaces (see Section 10.8.2.3 on page 110).
- Disable SSH Password Authentication (see Section 10.8.2.4 on page 113.
- Enable SSH IgnoreUserKnownHosts Parameter (see Section 10.8.2.5 on page 114).
- Configure SSH Allowed Hosts (see Section 10.8.2.6 on page 115).

10.8.2.1 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 10-32: SSH Log Level Manager

```
                EMS Server 6.8.155 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.

10.8.2.2 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 10-33: SSH Banner Manager

```
                EMS Server 6.8.155 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.

10.8.2.3 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:**

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

Figure 10-34: Configure SSH on Ethernet Interfaces

```
                EMS Server 6.8.155 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                 | 10.3.180.8      | G8-EMS-8
        >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 10.8.2.3.1 on page 111.
- Add SSH to Ethernet Interface (see Section 10.8.2.3.2 on page 112).
- Remove SSH from Ethernet Interface (see Section 10.8.2.3.3 on page 112).

10.8.2.3.1 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.

Figure 10-35: SSH Listener Status - ALL

```
                EMS Server 6.8.49 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                 ¦ 10.4.100.17     ¦ global-logic-2
        >1.Add SSH to All Ethernet Interfaces
         2.Add SSH to Ethernet Interface
         3.Remove SSH from Ethernet Interface
         4.Back
         5.Back to main Menu
```

10.8.2.3.2 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.

10.8.2.3.3 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.

10.8.2.4 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 10-36: 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.

10.8.2.5 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 10-37: 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.

10.8.2.6 SSH Allowed Hosts

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

➢ **To Configure SSH Allowed Hosts:**

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

Figure 10-38: Configure SSH Allowed Hosts

```
                EMS Server 6.8.155 Management
-----------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----------------------------------------------------------------------
        Current Allowed Hosts/Subnets:

        Subnet Masks:
         10.3.0.0/255.255.0.0

        IP Addresses:
         10.3.180.74

        >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
```

This menu includes the following options:

- Allow ALL Hosts (see Section 10.8.2.6.1 on page 116).
- Deny ALL Hosts (see Section 10.8.2.6.2 on page 116).
- Add Host/Subnet to Allowed Hosts (see Section 10.8.2.6.3 on page 117).
- Remove Host/Subnet from Allowed Hosts (see Section 10.8.2.6.4 on page 119).

10.8.2.6.1 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.

10.8.2.6.2 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 via SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM connection.

10.8.2.6.3 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 via 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 10-39: Add Host/Subnet to Allowed Hosts

```
                EMS Server 6.8.155 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 10-40: Add Host/Subnet to Allowed Hosts-Configured Host

```
                EMS Server 6.8.155 Management
-----------------------------------------------------------------------------
 Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----------------------------------------------------------------------------
        Current Allowed Hosts/Subnets:

        Subnet Masks:
         10.3.0.0/255.255.0.0

        IP Addresses:
         10.3.180.74

         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
```

10.8.2.6.4 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 via 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 via SSH. Therefore, prior to disabling SSH access, ensure that alternative connection methods have been provisioned, for example, serial management connection or KVM connection.

10.8.3 DBA Password

This option enables you to change the DBA password. The EMS server shuts down automatically before changing the DBA password.

➢ **To change the DBA 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 10-41: EMS Server Manager – Change DBA 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 DBA password.
- Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the EMS Database without them.

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

10.8.4 OS Passwords Settings

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.

   Proceed to one of the following procedures:

   - General Password Settings (see Section 10.8.4.1 on page 121.
   - Operating System User Security Extensions (see Section 10.8.4.2 on page 122).

10.8.4.1 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
```

5. 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
```

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

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

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

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

8. 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
```

Note: User **NBIF** is created password less for SSH Login. When you provide a new password for **NBIF** user, a normal login is allowed. When changing passwords, retain these passwords for future access.

10.8.4.2 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 10-42).

➢ **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 place limitations, 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 10-42: 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 10-43: 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 via 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 via SSH other than with the *acems* user.

10.8.5 Start / Stop 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 via 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.

10.8.6 Start/Stop 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 10-44: 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.

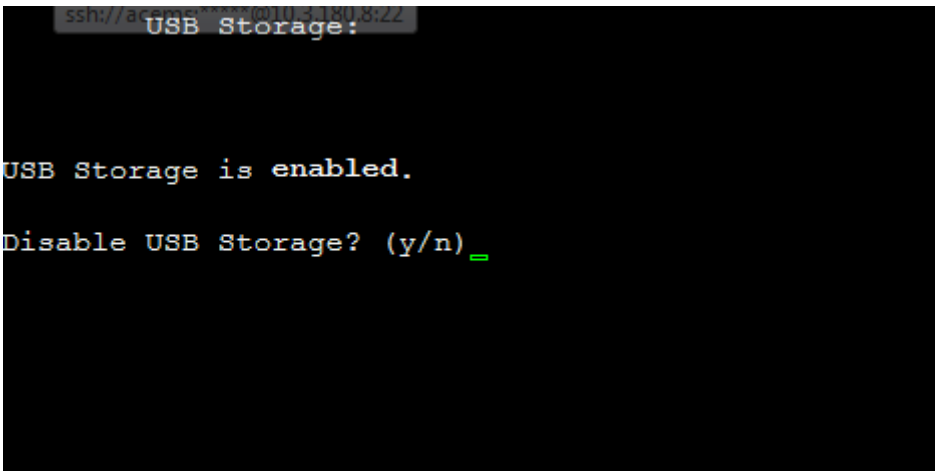
10.8.7 USB Storage

This menu option allows to enable or disable 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 10-45: USB Storage



2. Enable or disable USB storage as required.

10.8.8 Network Options

This menu option provides several items to enhance network security.

➢ **To enable network options:**

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

Figure 10-46: Network Options

```
                EMS Server 6.8.155 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.

10.8.9 Auditd Options

Using the Auditd option, you can change the auditd tool settings to comply with STIG recommendations.

➢ **To set Auditd options according to STIG:**

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

Figure 10-47: 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.

10.9 Diagnostics

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

➢ **To run EMS Server diagnostics:**

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

Figure 10-48: Diagnostics

```
                EMS Server 6.8.49 Management
-------------------------------------------------------------------
 Main Menu> Diagnostics
-------------------------------------------------------------------
        >1.Server Syslog
         2.Devices Syslog
         3.Devices Debug
         q.Quit to main Menu
```

This menu includes the following options:

- Syslog Configuration (see Section 10.9.1 on page 129).
- Board Syslog Logging Configuration (see Section 10.9.2 on page 129).
- TP Debug Recording Configuration (see Section 10.9.3 on page 130).

10.9.1 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 10-49: 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 10-50: 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.

10.9.2 Board Syslog Logging 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 *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:

'/opt/ACEMS/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**.

10.9.3 TP Debug Recording 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 via 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:

'/opt/ACEMS/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 TP Debug Recording:**

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 V

HA (High Availability)

This section describes the EMS HA Configuration options.

11 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.

Note: The SEM is currently not supported in this setup.

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.

Note: Any server configuration actions, performed via the EMS Server Manager, prior and after the HA configuration, should be manually updated on both EMS server machines, because these actions are not automatically replicated by the HA application processing.

11.1 EMS HA Pre-requisites

Before implementing an EMS HA configuration, ensure that both EMS servers have an identical configuration, noting the following:

- Both servers have identical hardware. See EMS Server and Client Requirements section for supported machines (see Section 3 on page 21).
- An identical Linux OS is installed on both servers.
- An identical EMS version is installed 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 shutdown 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 63GB on HP DL360 G6 servers and 900GB on HP DL360p G8 servers. A network speed of at least 80 Mbps is required to complete the initial sync process in up to 2 hours on G6 servers and 4 hours on G8 servers.

    Assuming a slower network, the process will take longer. For example, on G6 servers:
    - 20 Mbps -> 7 hours
    - 10 Mbps -> 14 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.

11.2 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
- 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.

11.3 EMS Server Manager

This section describes specific details in reference to the maintenance procedures on the EMS Server Manager

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 EMS Server

The following menu items are not displayed on the secondary server:

- Start/Stop EMS Server
- Backup the EMS Server
- Schedule Backup for the EMS Server
- Restore the EMS Server

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 will be hidden after exiting the EMS Server Manager and running it again.

11.4 EMS Client

Once the switchover has successfully completed, the EMS client relogins to the active server and a "Server Startup" alarm is displayed.

11.5 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 only then the primary server.

- To uninstall HA, see Section 12.6 on page 148.
- To upgrade the EMS server, see Section 8.1 on page 65.

11.6 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 12.6 on page 148.

12 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 12-1: EMS Server Manager - HA Configuration

This menu includes the following options:

- Primary Server Installation in Global IP Model (see Section 12.1 on page 138.
- Primary Server Installation in in Geo HA model. see Section 12.2 on page 140.
- Secondary Server Installation (see Section 12.3 on page 140.
- HA Status (see Section 12.4 on page 144).

12.1 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.

➢ **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 12-2: 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 12.2.1 on page 142).

Figure 12-3: 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 12-4: 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 12-5: 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'.

12.2 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 12-6: 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:
   - '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 12.2.1 on page 142).

Figure 12-7: 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 12-8: 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 12-9: 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'.

12.2.1 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, therefore 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.

12.3 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 12-10: 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 12-11: 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.

12.4 HA Status

The 'HA status' displays both servers' High Availability parameters.

➢ **To verify the EMS HA status:**

1. In the High Availability menu, choose option **3** (**HA Status**), and then press Enter; the following is displayed:

Figure 12-12: EMS HA Status

```
        High Availability Status

HA Heartbeat Service Status      [  Heartbeat Not Installed  ]
HA DRBD Service Status           [  DRBD Not Installed  ]

HA EMS Status                    [ Unknown - Not Primary Server  ]

Press "s" - status view, "a" - advanced status view or any other key to continue
...
```

The following status view is displayed (Example only):

Figure 12-13: 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.

12.4.1 Advanced Status View

This section describes the advanced status view.

➢ **To view the advanced status:**

1. In the High Availability Status screen, press **a**; the following is displayed:

Figure 12-14: 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).

12.5 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 12-15: Manual Switchover

```
                EMS Server 6.8.49 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 12-16: 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 12-17: 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!!  ]
```

12.6 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

➢ **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 12-18: 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 10.5.1 on page 82).

This page is intentionally left blank

Part VI

Configuring the Firewall and Installing the EMS Client

This part describes how to configure the EMS firewall and install the EMS client.

13 Configuring the Firewall

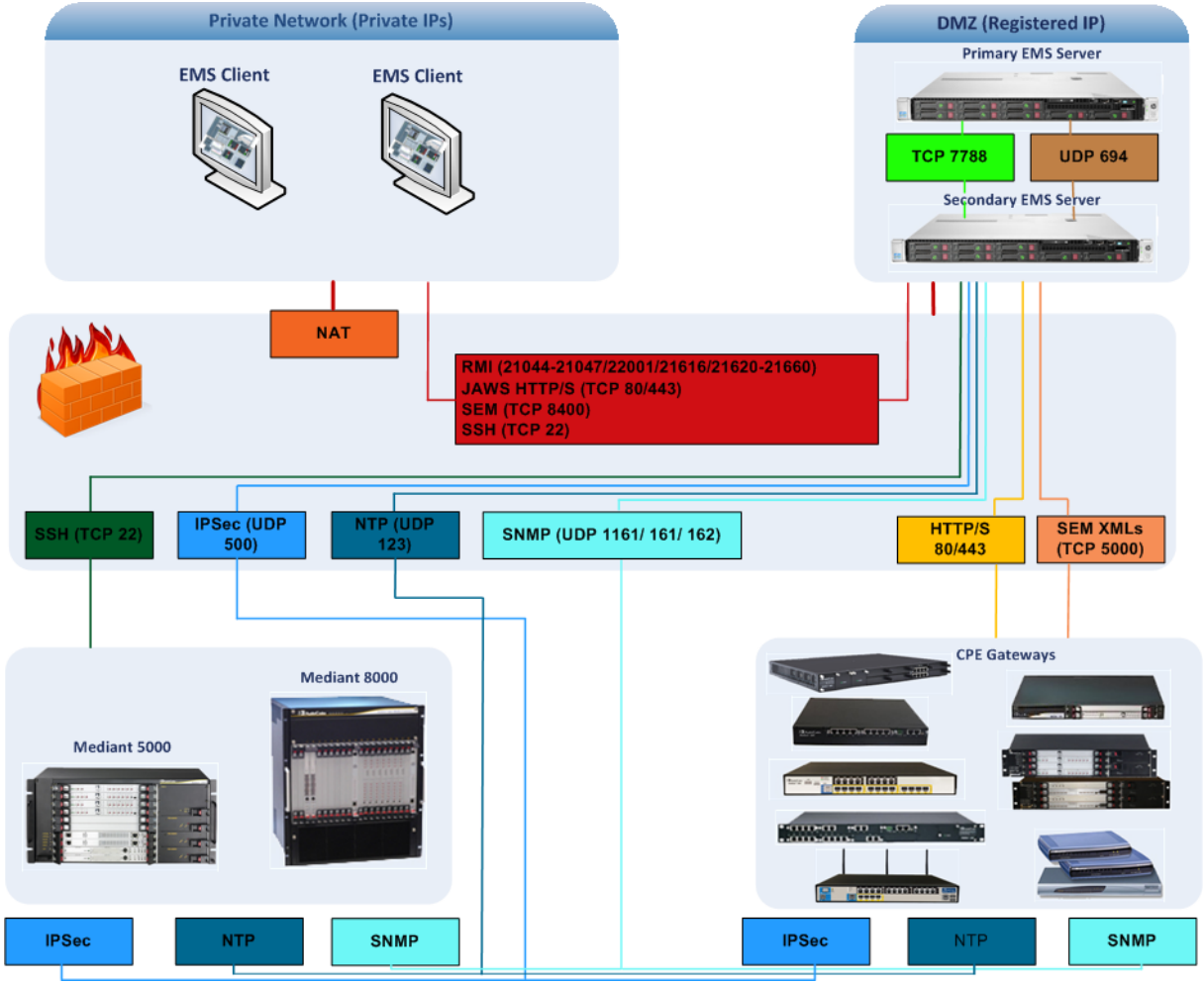
To enable EMS Client ↔ EMS Server ↔ Managed Gateways communication according to Figure 13-1, define the rules specified in the Firewall Configuration Rules table below:

Table 13-1: Firewall Configuration Rules

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
EMS Client ↔ EMS Server	TCP	22001, 21044-21047, 21616 and 21620-21660	RMI communication. Initiator: EMS Client	EMS Server side / Bi-Directional
	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	EMS Server side / Bi-Directional
	TCP	443	HTTPS for JAWS and NBIF. Initiator: Client PC	
EMS server ↔ All Media Gateways	UDP	1161	SNMP communication. Initiator: EMS Server	EMS Server side / Bi-Directional
	UDP	162	SNMP Traps. Initiator: MG	EMS Server side / Receive only.
	UDP	161	SNMP communication. Initiator: EMS Server	MG side / Bi-Directional
	UDP	123	NTP synchronization. Initiator: MG (and EMS Server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-Directional
	UDP	500	IPSec communication. Initiator: Both sides	Both sides / Bi-Directional

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
EMS Server ↔ All Media Gateways except M5K & M8K	TCP	80	HTTP connection for files transfer. Initiator: EMS Server	EMS Server side / Bi-Directional
	TCP	443	HTTPS connection for files transfer. Initiator: EMS Server	
EMS Server ↔ Mediant 5000/8000 Media Gateways	TCP	22	SSH communication for files transfer. Note, ports should be open for both Global IP and SC private IP Addresses. Initiator: EMS Server	Mediant 5000/Mediant 8000 side / Bi-Directional
Media Gateways ↔ SEM server	TCP	5000	XML based SEM communication. Initiator: MG	EMS Server side / Bi-Directional
SEM client ↔ Tomcat server	TCP	8400	SEM connection between the user's browser and Tomcat server. Initiator: Client's PC.	EMS Server side / Bi-Directional
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	

Figure 13-1: Firewall Configuration Schema



Note: The above figure displays images of example CPE gateways. For the full list of supported products, see Section 2.1 on page 19.

- NOC ↔ EMS (Server) ports

Table 13-2: OAM&P Flows: NOC ↔MG EMS

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
NOC/OSS	MG EMS	SFTP	1024 - 65535	20
		FTP	1024 - 65535	21
		SSH	1024 - 65535	22
		Telnet	1024 - 65535	23
		NTP	123	123
		IPSec	N/A	500
		HTTP/HTTPS	N/A	80,443

Table 13-3: OAM&P Flows: MG EMS→NOC

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
MG EMS	NOC/OSS	NTP	123	123
		SNMP Trap	1024 – 65535	162
		IPSec	500	N/A

14 Installing the EMS Client

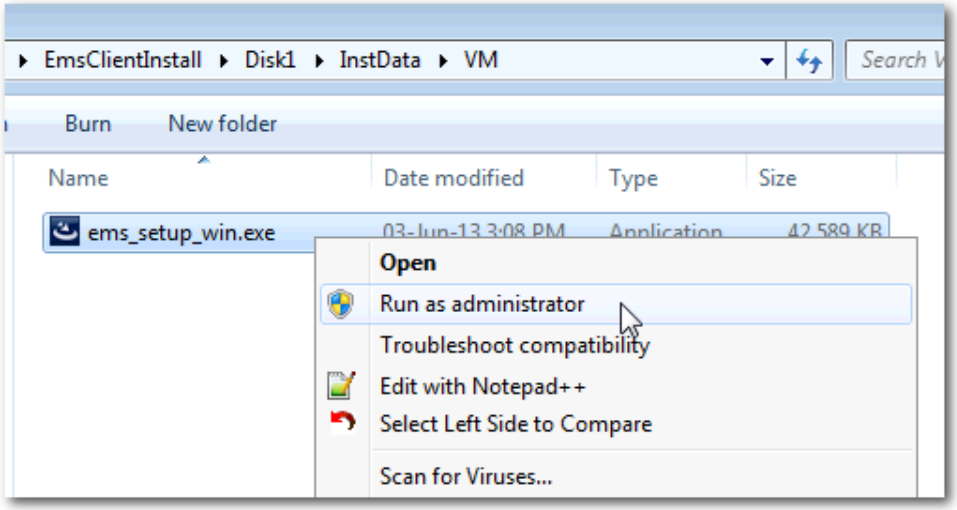
This section describes how to install the EMS Client on a PC or Laptop.

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.

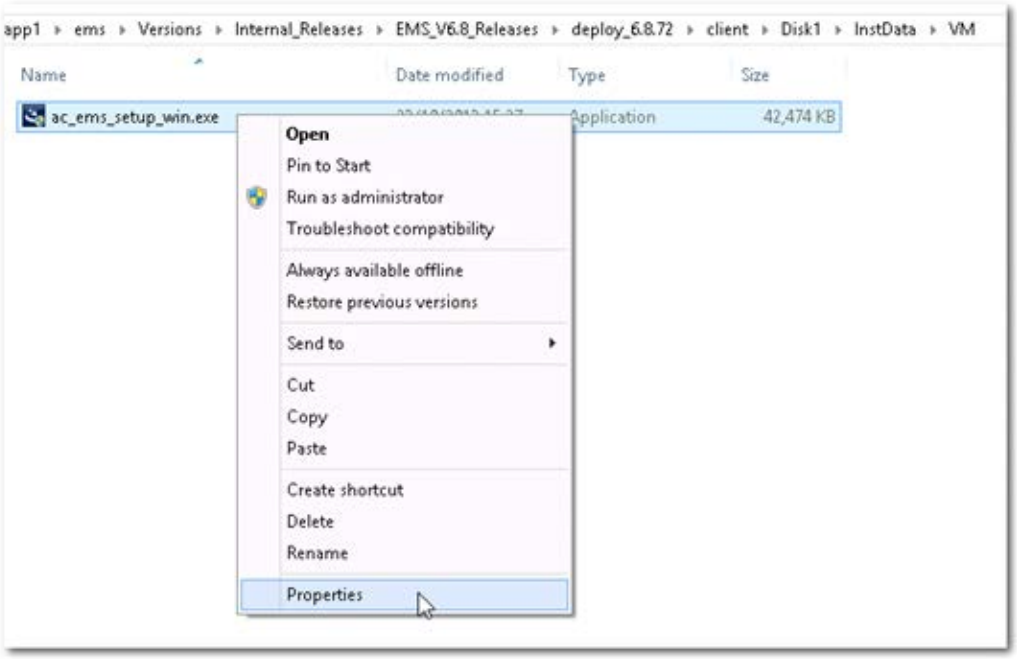
Figure 14-1: EMS Client Installation-Run as Administrator



Upon the completion of the installation process, the EMS client icon is added to the desktop.

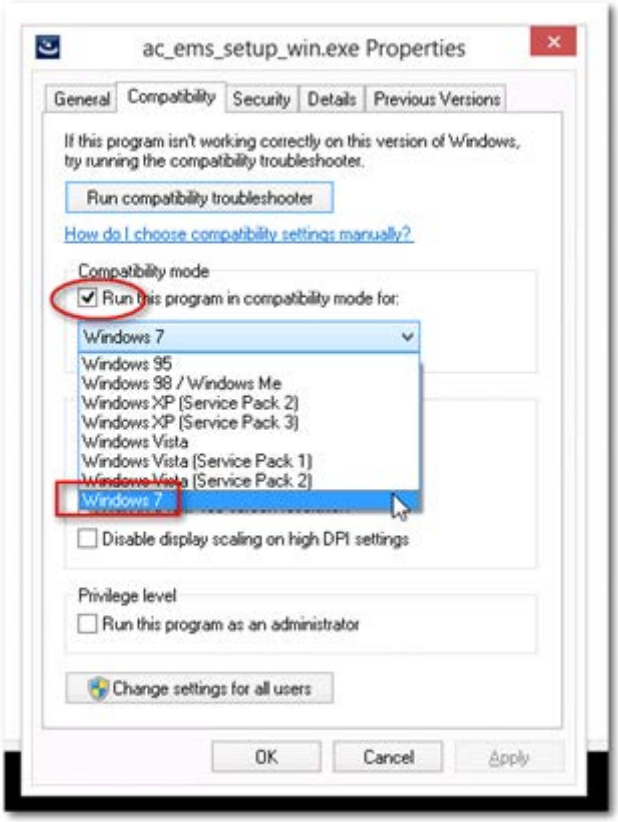
- On **Windows 8**:
  a. Right-click the installation exe file, and then choose **Properties**; the Properties window is displayed:

Figure 14-2: 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 14-3: EMS Client Installation File-Compatibility Tab



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**.

14.1 Running the EMS Client on a PC or Laptop

This section describes how to run the EMS client on a PC or Laptop

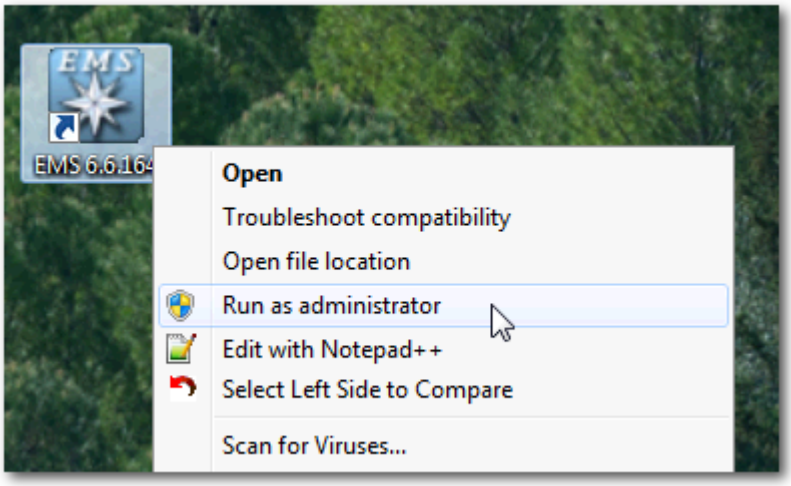
➢ **To run the EMS on Windows XP or older:**

- 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 14-4: Running EMS Client-Run as Administrator



14.2 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.

14.3 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 via 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 VII

Appendices

This part describes additional EMS server procedures.

A Frequently Asked Questions (FAQs)

This appendix describes the Frequently Asked Questions (FAQs) for troubleshooting EMS server and EMS client installation, operations and maintenance issues.

A.1 After installing JAWS - the EMS application icon is not displayed on the desktop

Q: After installing Jaws, the EMS application icon is not created on the desktop.

A: You must update the Java properties and reinstall the EMS application.

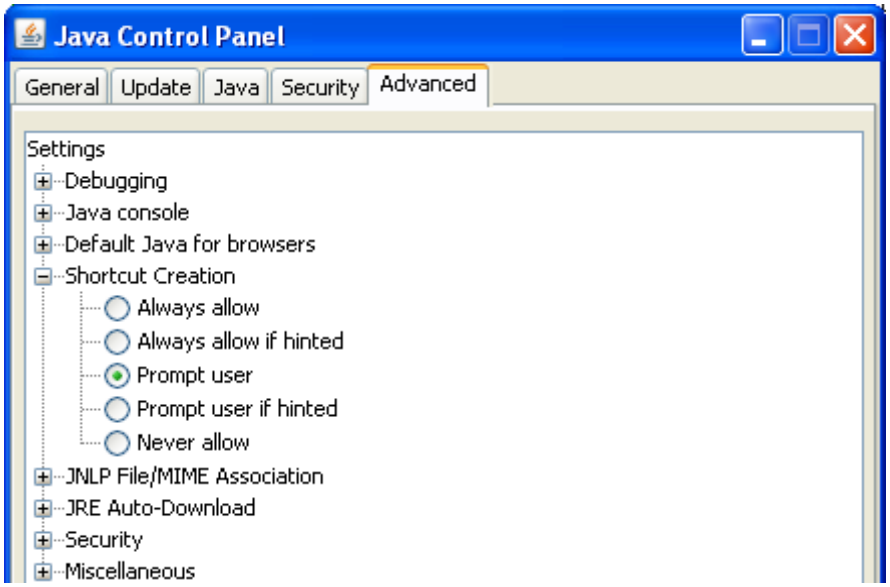
➢ **To display the EMS icon, do the following:**

1. Go to **Start>Settings>Control Panel> Add Remove Programs**.
2. Choose **EMS Application,** and then press **Remove**.

Figure A-1: EMS Client Removal

3. After removing the EMS application, go to Start>Settings>Control Panel
4. Double-click the Java Icon  .
5. Choose the **Advanced** tab.

Figure A-2: Java Control Panel



6. Choose Shortcut Creation in the Settings dialog.

7. Select the **Always allow** box to always create an icon on desktop or Prompt user to ask before icon creation.
8. Install client using Jaws. For more information, see Section 14.3 on page 161.
9. After the installation has completed, the new Icon is created on your desktop:

A.2 After Rebooting the Machine

Q: The database doesn't start automatically after the machine is rebooted.

A: Perform the procedure below:

➢ **To check the reason why the database does not starting automatically:**

1. Verify the syntax in 'var/opt/oracle/oratab'; the file should end with an empty line.
2. Verify whether the symbolic link ‘S90dbstart’ under /etc/rc2.d is not broken.
3. Verify whether all scripts have execute permissions for **acems** user.
4. Verify whether the default shell for **acems** user is ‘tcsh’.

A.3 Changes Not Updated in the Client

Q: After a successful installation, the multiple GWs add operations - as well as changes made by other clients - are not updated in the client.

A: Check the configuration of the date on the EMS server machine. This problem occurs when the daylight-saving configuration is defined incorrectly.

➢ **To redefine the clock in the EMS application:**

1. Change clock in the EMS server (using the command **date**).
2. Reboot the EMS server machine (verify that the EMS server application is up and running).
3. Change the clock in the EMS client machine.
4. Reboot the EMS client machine.
5. Open the EMS client application and connect to the EMS server.
6. Verify correct clock settings by opening the ‘User Journal’ and checking your last login time.

A.4 Removing the EMS Server Installation

Q: How do I remove the EMS server installation?

A: See Section 12.6 on page 148.

B Site Preparation

This appendix describes the procedures for backing up the EMS server.

Note: It is highly recommended to perform a complete backup the EMS Server prior to performing an installation or upgrade, according to the procedures described below.

1. 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 6.2 version, and decides to roll back to the previous version.
2. 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.
4. 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, IPSec pre-shared key and (Mediant 5000 / 8000) *root* password. This information will be required during the Media gateway'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 B-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

C Daylight Saving Time (DST)

This appendix explains how to apply Daylight Saving Time (DST) changes for Australia (2006), USA (2007), Canada (2007) and other countries, after the EMS application is installed.

Many countries around the world over the past two years have implemented legislation to change their Daylight Savings Time (DST) dates and time zone definitions.

The following major changes are implemented:

- tz2005o - Australia, USA
- tz2006a - Canada (Quebec, Ontario, Nova Scotia, Nunavut, Saskatchewan, Manitoba, New Brunswick and Prince Edward Island)
- tz2006n - Canada (the other provinces)
- tz2006p - Western Australia
- tz2007a - Bahamas

Customers who maintain local time on their AudioCodes products and reside in Australia or North America must update AudioCodes' software to support the new DST settings.

- **EMS Server**

The local time of the EMS server is used to calculate the time of the Performance Measurements (PMs) and EMS Journal events, displayed in the EMS GUI. Users who configured a local time zone on an EMS server which is subject to new DST settings are affected.

New DST settings are fully supported starting v5.6.

Patches are applied automatically for the EMS server, as it is installed.

- **EMS Client**

The local time of the EMS client is used to calculate the time of the SNMP alarms displayed in the EMS GUI. Users who configured a local time zone on an EMS client that is subject to new DST settings are affected.

AudioCodes does not provide an operating system that is used on the computers that run EMS client software. Customers should therefore consult the vendor of the specific operating system that is used. For Windows XP, see the page in URL: http://support.microsoft.com/DST2007.

After applying the OS-specific patches, patch the Java installation on the EMS client as well. Detailed instructions are provided in this section.

C.1 EMS Client

To apply new DST settings to the EMS client, update the Windows operating system (see Section C.3 on page 171).

C.2 Windows

Install Windows OS patches as specified in the following URL:

http://support.microsoft.com/DST2007.

C.2.1 Java

➢ **Do the following:**

1. Open the EMS client and open menu option Help>About. Determine the home directory of the Java installation that the EMS client uses.
2. Copy the JAVA patch file 'tzupdater.jar' from the EMS software CD/DVD in the folder '\Documentation\Patches' and place it in directory 'bin' under the Java home directory, whose path can be determined according to step 1.
3. Open the Command Line window and change the directory to **bin** under the Java home directory, whose path can be determined according to the instruction in step 1. For example:

```
cd C:\j2sdk1.4.2\bin
```

4. Install the patch by running the following command:

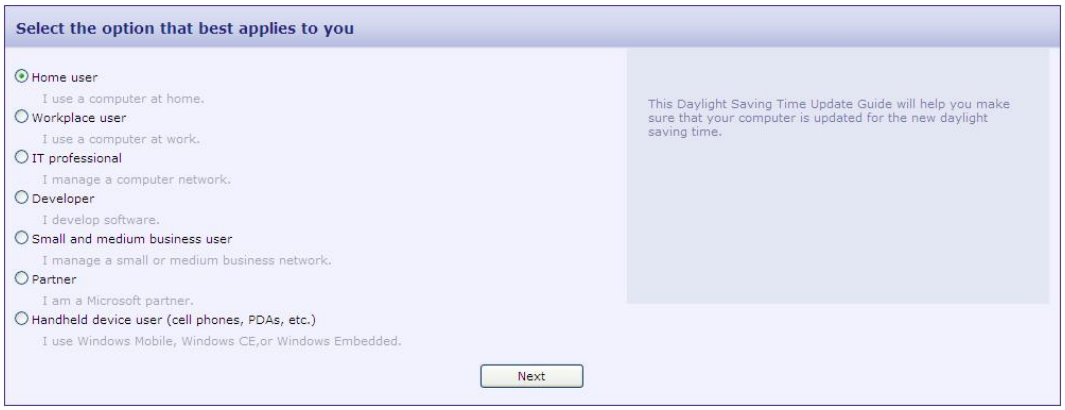
```
java –jar tzupdater.jar –f –bc -v
```

C.3 Example of Installing Windows Patches on the EMS Client

➢ **Do the following:**

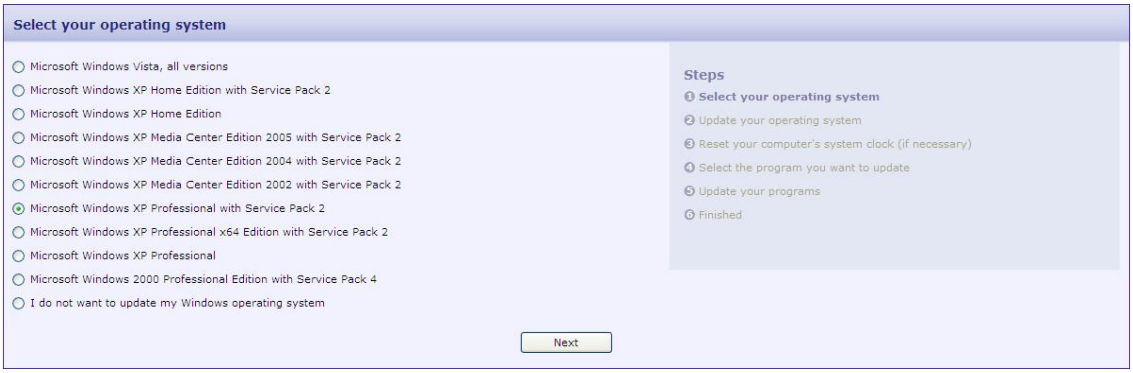
1. Install the Windows operating system patches as specified in URL: http://support.microsoft.com/DST2007.
2. In the Microsoft page, define the relevant data (see below).

Figure C-1: Installing Windows OS Patches – PC Information



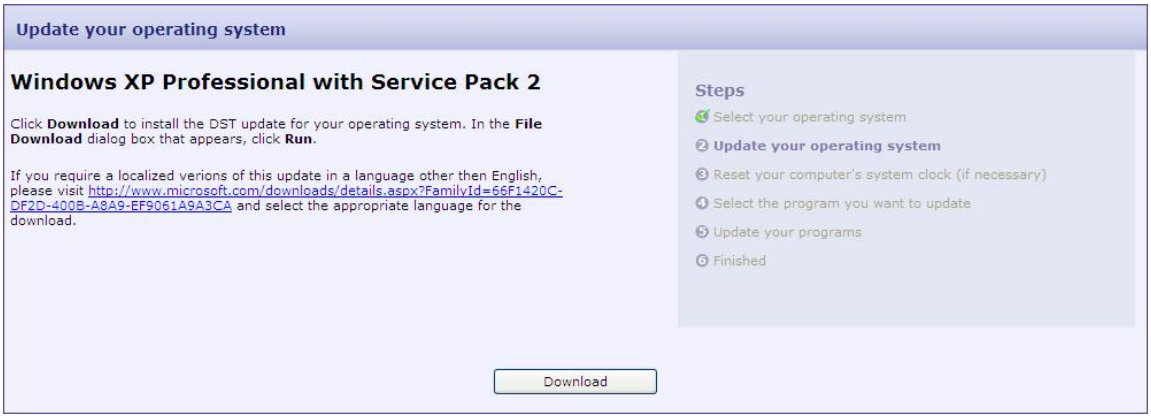
3. Select your operating system information.

Figure C-2: Installing Windows OS Patches – Selecting the Operating System



4. Download and install the patch.

Figure C-3: Installing Windows OS Patches – Download and Install



5. Continue the installation according to Microsoft's instructions.

D Working with HTTPS

This appendix describes the actions required to work with HTTPS and certificates.

D.1 Working with HTTPS on CPE Media Gateways

If you are using the “AudioCodes-issued” certificates in the EMS client and EMS server installations, perform the procedure described in this section to activate the HTTPS connection between the EMS server and the media gateway.

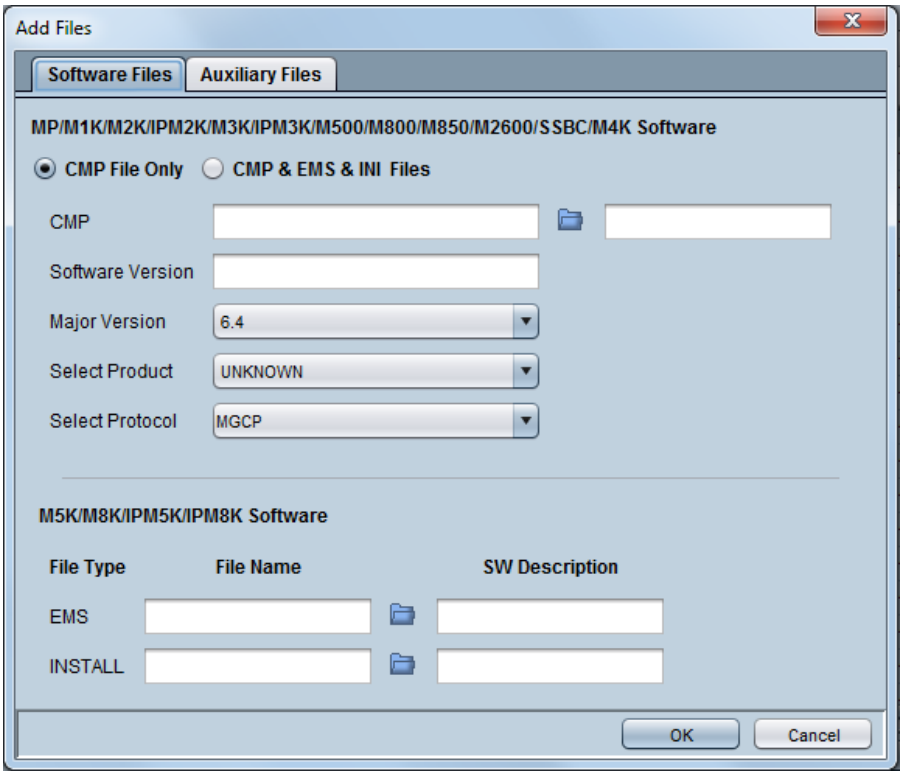
Note: If you wish to work with HTTPS and external certificates that are signed by an external trusted CA, perform the procedure described in Section E 0on page 186.

When working in *secure mode* ('HTTPS Enabled'), the ”appropriate” gateway certificate (the certificate that is signed by the same CA as the EMS server certificate) **must** be added to the EMS Software Manager. In addition, the CA certificate must also be loaded on the media gateway devices.

➢ **To set up an HTTPS connection with the media gateway:**

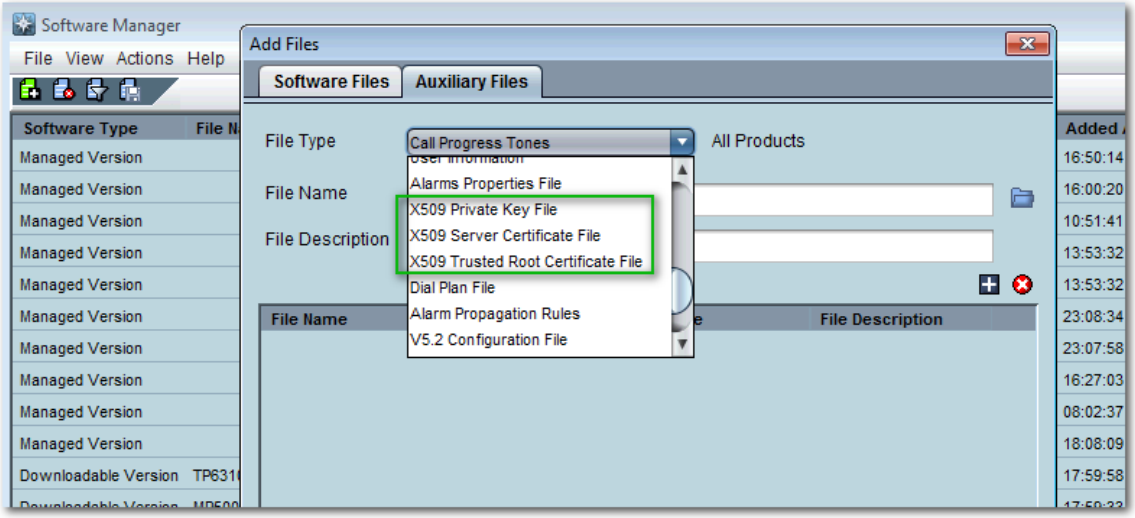
1. Install and login to the EMS client.
2. Open the EMS Software Manager (In the Main Menu, **Software Manager** (**Tools** > **Software Manager**); the following is displayed:

Figure D-1: EMS Software Manager



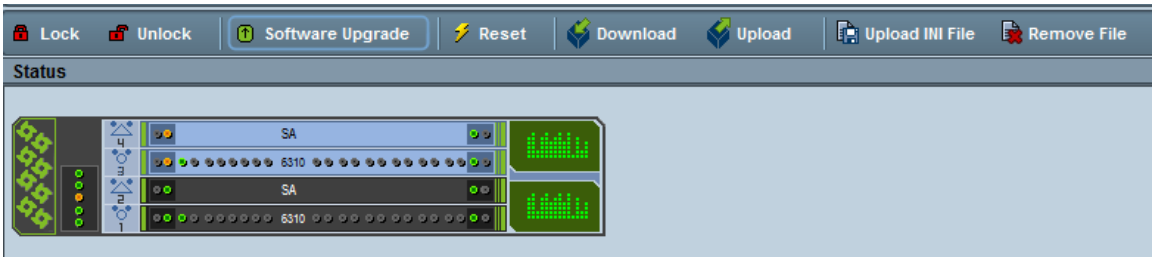
3. In the Actions bar, click the Add button ; and then select the **Auxiliary Files** tab.

Figure D-2: X509 Files-Software Manager



4. From the File Name drop-down list, select **X509 Private Key File**.
5. In the File Name Field, click the **browse** button, browse to the EMS client folder path externals\security\clientNssDb\boardCertFiles, select the file **board_cert.pem**, and then click **OK**.
6. From the 'File Type' drop-down list, select **X509 Server Certificate File**.
7. In the File Name Field, click the **browse** button, browse to the EMS client folder path externals\security\clientNssDb\boardCertFiles, select the file **root.pem**, and then click **OK**.
8. From the File Name drop-down list, select **X509 Trusted Root Certificate File**.
9. In the File Name Field, click the **browse** button, browse to the EMS client folder path externals\security\clientNssDb\boardCertFiles, select the file **board_pkey.pem**, and then click **OK**.
10. Download these files to the media gateway to which you wish to configure. Download the files as Server Certificate, Trusted Root Certificate Store and Private Key respectively, using the 'Software Upgrade' option.

Figure D-3: Software Upgrade

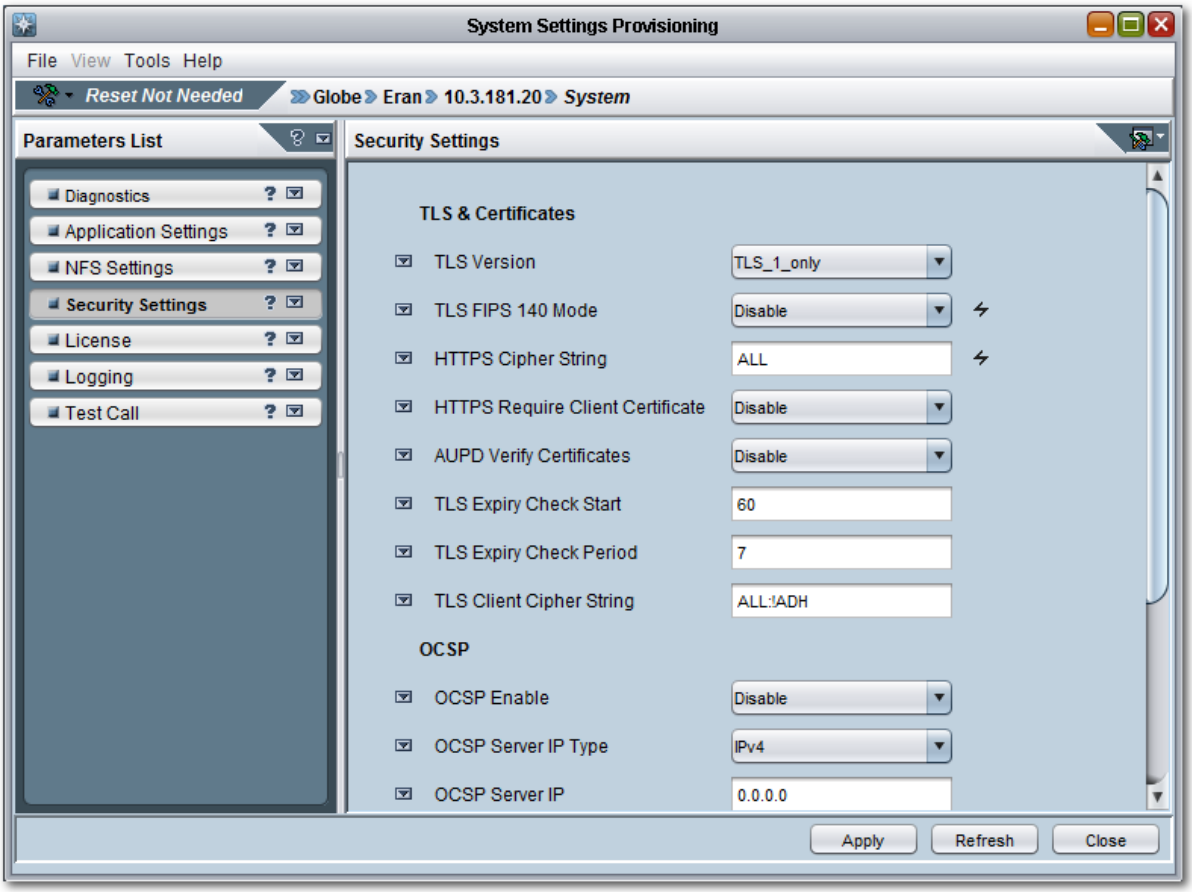


Note:

- This action is performed while the connection between the EMS and the gateway is still 'HTTP'.
- It is recommended to perform this action in a private internal network.

11. In the Navigation pane, select **System**, and then in the Configuration pane, select **System Settings** frame; the System Settings frame is displayed.
12. Select the **Security Settings** Tab.

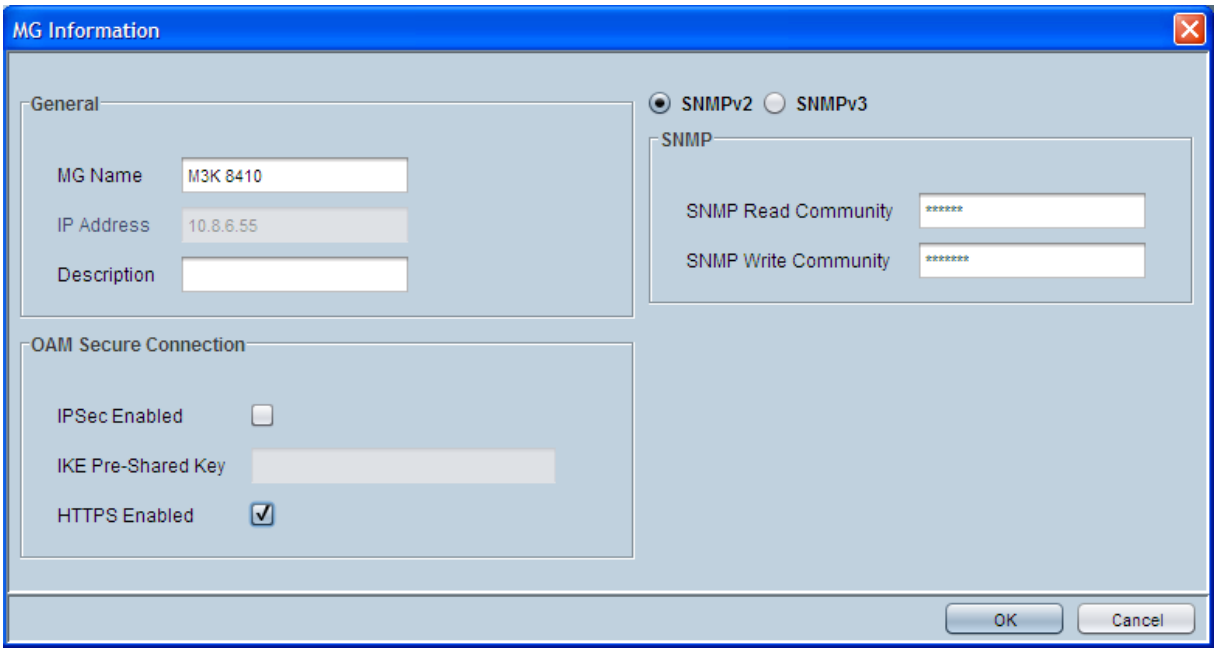
Figure D-4: System Settings Provisioning



13. Set 'TLS Version' to **TLS 1.0 only**.
14. Set 'HTTPS Cipher String' to **ALL**.
15. Reset the Media Gateway.

16. In the MG Tree, right-click the Media Gateway, and then select **Details**; the MG Information screen is displayed:

Figure D-5: MG Information



17. Select the 'HTTPS Enabled' check box .
18. Perform the desired HTTPS secure action (using the EMS 'Software Upgrade' button option as shown in Figure).

D.2 Importing HTTPS Certificates

When you wish to access NBIF (Northbound Interface) data or when you wish to run the EMS client using JAWS with HTTPS enabled, then you must import the 'clientcert.crt' file from the EMS client directory or from an external pkcs12 source to your web browser. This file includes the certificate for securing the connection between your EMS client and a web browser.

Note:

- For a list of the supported Web browsers, see Section 2 on page 19.
- The certificate file shown in this example is for an AudioCodes certificate file; however, this procedure also applies for any other external pkcs12 file that you wish to import.

Proceed to one of the following sections:

- Importing Certificate to a Mozilla Firefox browser (see Section D.2.1)
- Importing Certificates to a Google Chrome and IE Browser (see Section D.2.2).

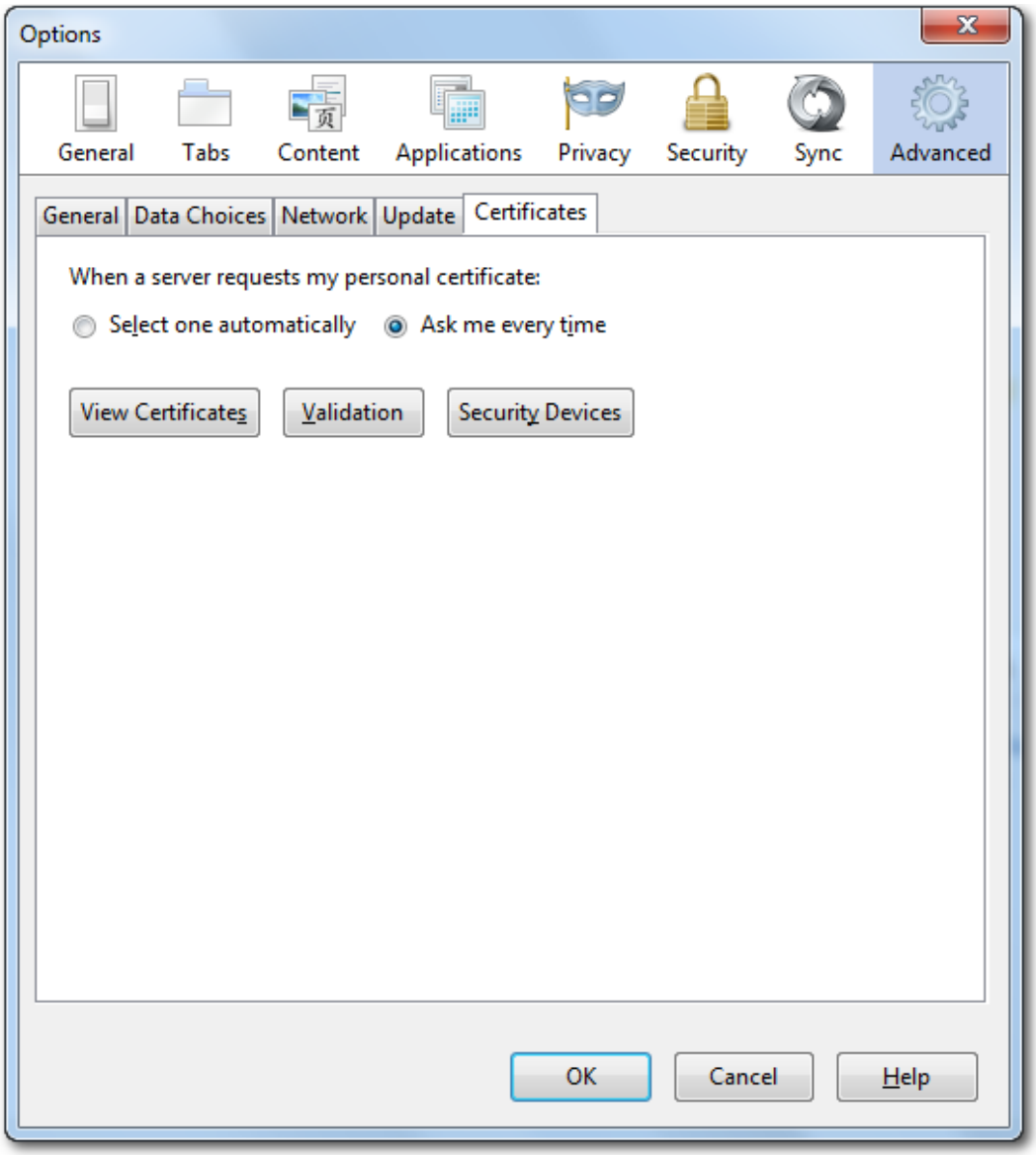
D.2.1 Importing Certificate to a Mozilla FireFox Browser

This section describes how to import a certificate file to a Mozilla Firefox browser.

➢ **To import a certificate file to a Mozilla Firefox browser:**

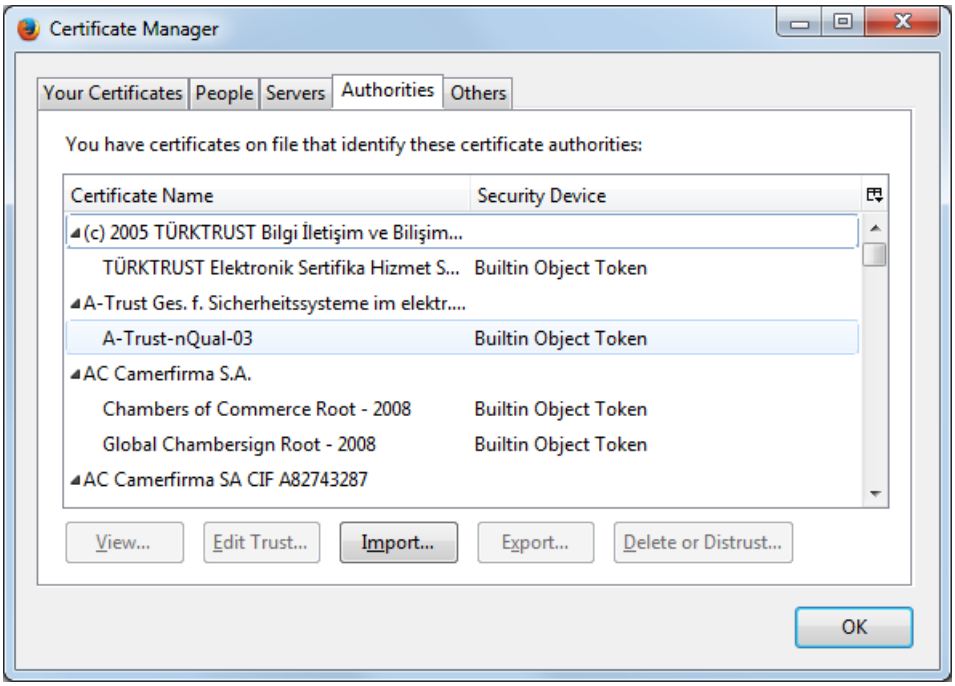
1. Click the **Menu** button, then the **Options** button, then the **Advanced** button, and then click the **Certificates** tab; the View Certificates screen is displayed.

Figure D-6: View Certificates



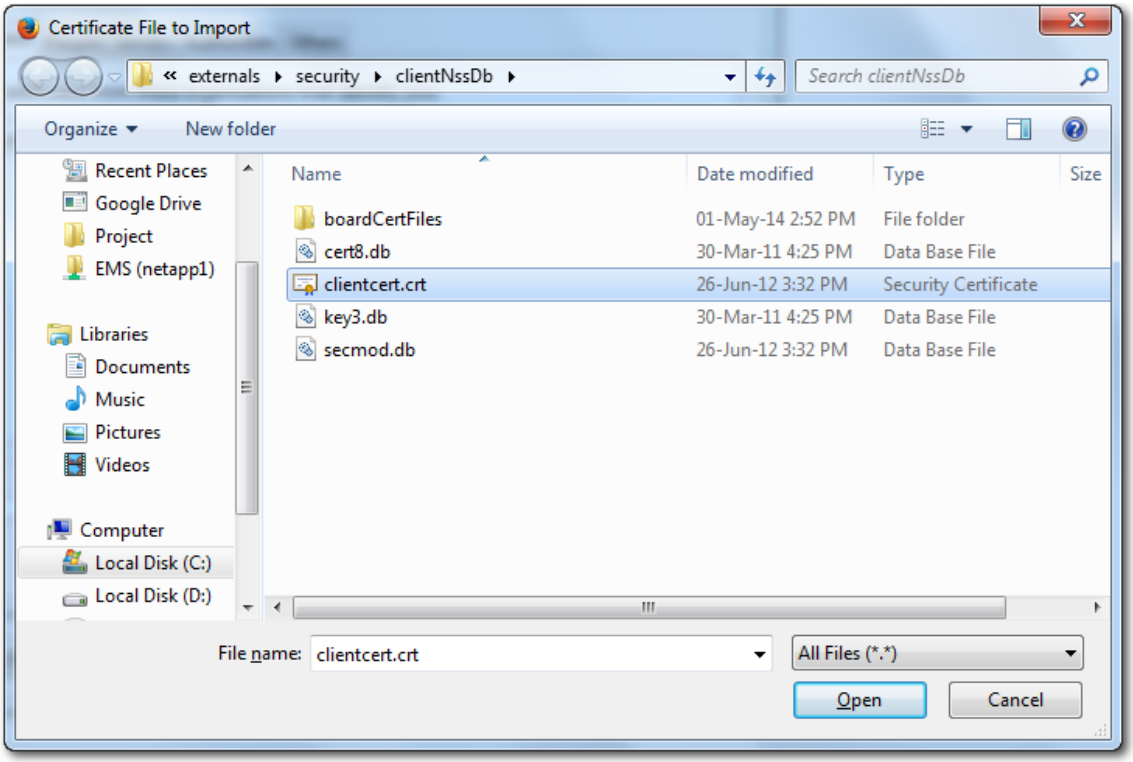
2. Click the **View Certificates** button; the following screen is displayed:

Figure D-7: Certificate Manager



3. Click the **Import** button; the following screen is displayed:

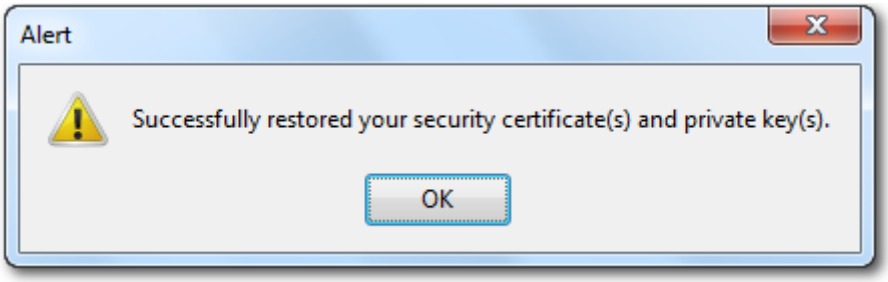
Figure D-8: Certificate File to Import



4. Do one of the following:
   - Browse to the “clientcert.crt” file in the EMS Client directory i.e.:C:\Program Files\AudioCodes\EMS Client 6.8.174\externals\security\clientNssDb \clientcert.crt
   - Browse to the saved location of the external pkcs12 file.
5. Select the “clientcert.crt” file, and then enter the password:
   - For AudioCodes file, enter string “passfile”.
   - For external pkcs12 file, enter the required string.

   The following confirmation screen is displayed:

Figure D-9: Security Certificate Restored



6. Click **OK** twice.

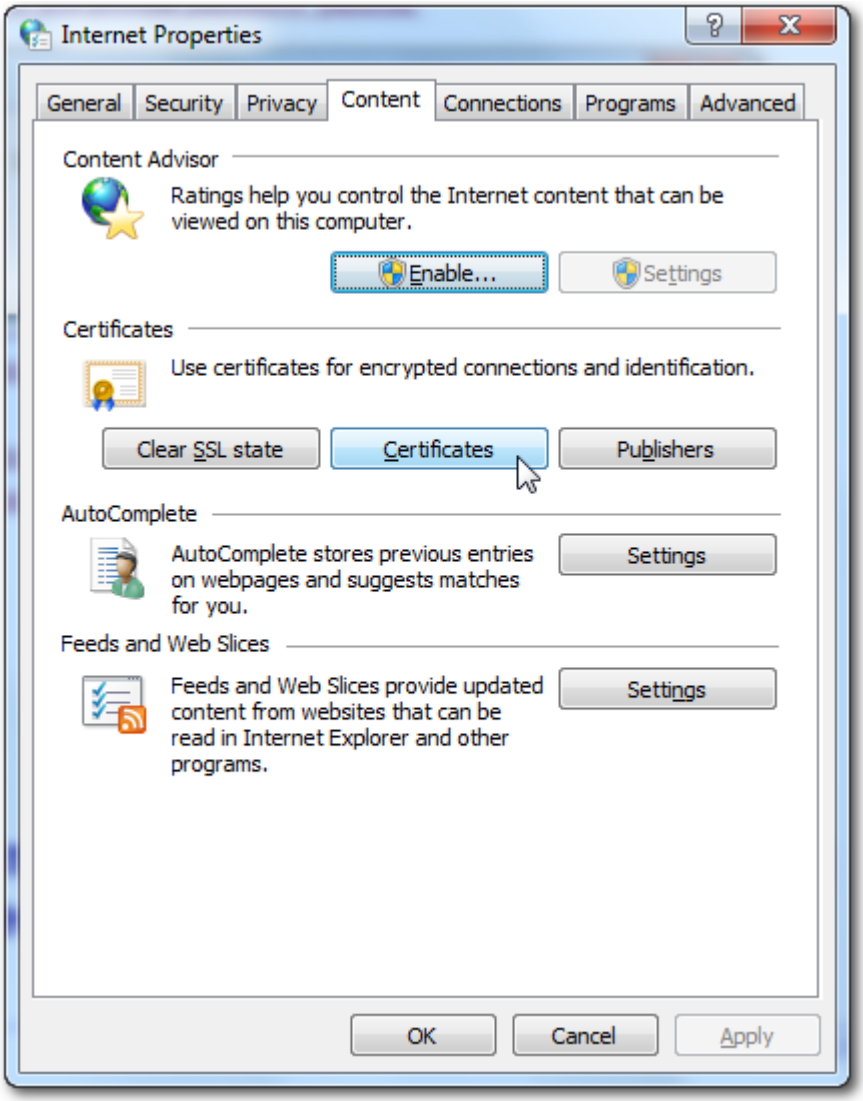
D.2.2 Importing a Certificate to a Google Chrome and IE Browser

This section describes how to import a certificate to a Google Chrome and IE Browser.

➢ **To import a certificate to a Google Chrome and IE browser:**

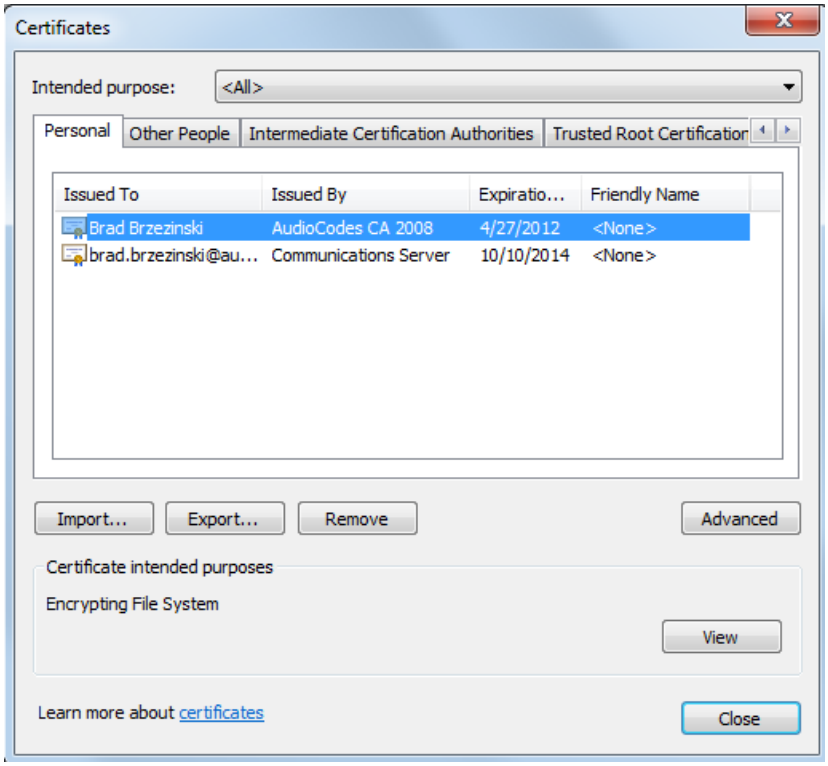
1. Click the **Tools** button, from the drop-down menu, choose **Internet Options**, and then select the **Content** tab; the following screen is displayed:

Figure D-10: Internet Properties



2. Click the **Certificates** button.

Figure D-11: Certificates

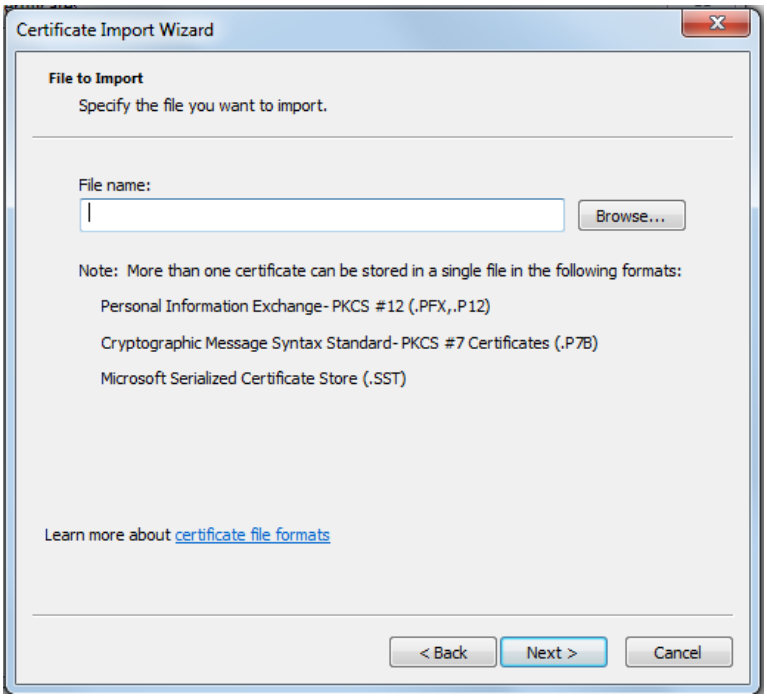


3. Click the **Import** button; the Certificate Import Wizard opens.

Figure D-12: Welcome to Certificate Import Wizard

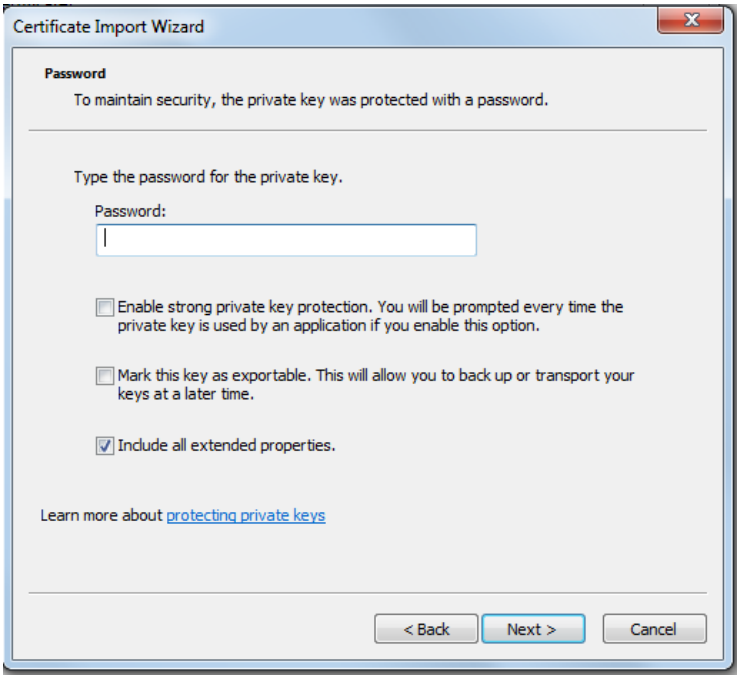
4. Click **Next**; the File Import screen is displayed:

Figure D-13: Browse to Certificate File



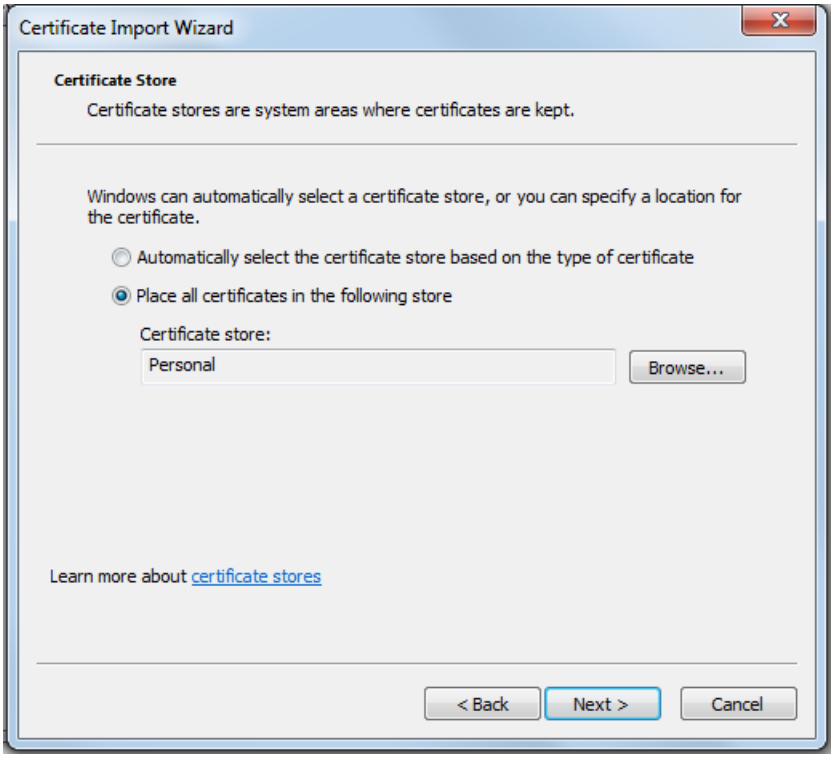
5. Do one of the following:
   - Browse to the “clientcert.crt” file in the EMS Client directory i.e. :C:\Program Files\AudioCodes\EMS Client 6.8.174\externals\security\clientNssDb \clientcert.crt
   - Browse to the saved location of the external pkcs12 file.
6. Click **Next**; the Password screen is displayed.

Figure D-14: Certificate Password



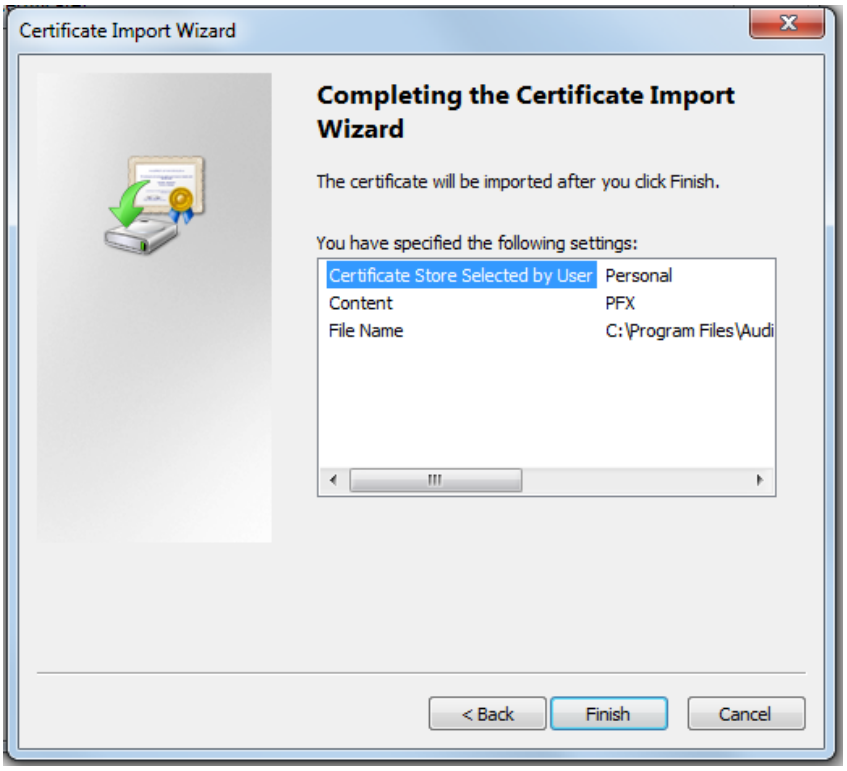
7. Enter the password string:
   - For AudioCodes file, enter string “passfile”.
   - For external pkcs12 file, enter the required string.
8. Click **Next**; the Certificate Store screen is displayed:

Figure D-15: Certificate Store



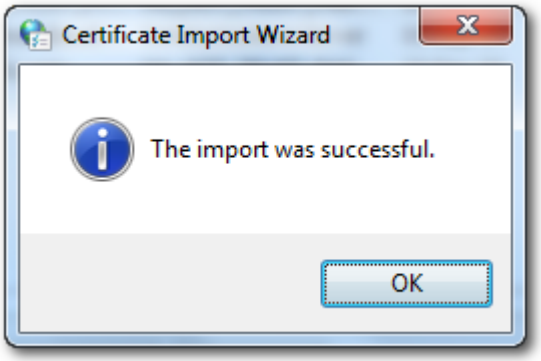
9. Choose the appropriate action, and then click **Next**; the Certificate Configuration parameters are displayed.

Figure D-16: Certificate Import Wizard Complete



10. Click **Finish**; the following confirmation is displayed:

Figure D-17: Certificate Import Wizard Confirmation



11. Click **OK**.

This page is intentionally left blank

E External Security Certificates-Signing Procedure

This appendix describes the External Security Certificates Signing Procedure.

E.1 Overview

The EMS client and EMS server are by default configured with “AudioCodes-issued” certificates. This section explains how to replace these “AudioCodes-issued” certificates with certificates issued by an “external CA” (e.g. DoD CA). To maintain an active connection between the EMS server and EMS client, these certificates must be simultaneously replaced on both the EMS server and EMS client.

E.2 Installing External CA Certificates on the EMS Server

On the EMS server, external CA certificates must be saved in a single location. In the procedures described in this section, customers must perform the following actions:

- Create a certificate request
- Transfer the CSR to the Certificate Authority (CA) for signing
- Import the signed certificate to the EMS server certificates database.

Note: If you have previously installed external certificates, and then upgraded the EMS server, you do not need to reinstall these external CA certificates.

➢ **To install external CA Certificates on the EMS server:**

1. Login to the EMS server machine as 'root' user.
2. Stop the EMS server (use the EMS Manager options).
3. Stop the Apache web server (use the EMS Manager options).
4. Move the old/default Certificates database to a temporary folder and create a temporary noise file for key generation.

```
mv /opt/nss/fipsdb /opt/nss/fipsdb_old
( ps -elf ; date ; netstat -a ) > /tmp/noise
```

5. Create a new empty Certificates database and corresponding password files.

```
mkdir /opt/nss/fipsdb
chmod 755 /opt/nss/fipsdb

echo fips140-2 > /tmp/pwdfile.txt

/opt/nss/nss-3.12.6-with-nspr-4.8.4/bin/certutil -N -d
/opt/nss/fipsdb -f /tmp/pwdfile.txt

chmod 644 /opt/nss/fipsdb/*.db
chown emsadmin:dba /opt/nss/fipsdb/*.db
```

6. Create a certificate request file (CSR) to transfer to the external CA for signing.

```
/opt/nss/nss-3.12.6-with-nspr-4.8.4/bin/certutil -R -d
/opt/nss/fipsdb -s "CN=EMS Server, O=AudioCodes, C=US" -a -
o /tmp/server.csr -g 1024 -f /tmp/pwdfile.txt -z /tmp/noise
-1 -6
enter the following options after the previous
command:0,2,9,n,1,0,9,n
```

7. Transfer the CSR to the external CA for signing and receive them back.

```
Transfer the generated CSR - /tmp/ server.csr (via SFTP or
SCP) and pass it to the Certificate Authority.
You should receive back 2 files: your signed certificate
(let's call it server.pem) and certificate of trusted
authority (let's call it cacert.pem).
Now transfer these 2 files back to the EMS server under
/tmp directory and use the following commands to import the
files into the EMS server's NSS:
```

8. Import the Signed Certificates and the CA Certificate into the Certificates Database.

```
/opt/nss/nss-3.12.6-with-nspr-4.8.4/bin/certutil -A -d
/opt/nss/fipsdb -n servercert -t u,u,u -a -i
/tmp/server.pem -f /tmp/pwdfile.txt

/opt/nss/nss-3.12.6-with-nspr-4.8.4/bin/certutil -A -d
/opt/nss/fipsdb -n cacert -t CTu,CTu,CTu -a -i
/tmp/cacert.pem -f /tmp/pwdfile.txt

echo "\n" | /opt/nss/nss-3.12.6-with-nspr-4.8.4/bin/modutil
-fips true -dbdir /opt/nss/fipsdb
```

9. Cleanup temporary files.

```
rm /tmp/pwdfile.txt /tmp/noise /tmp/server.pem
/tmp/cacert.pem /tmp/server.csr
```

10. Restart the Apache web server using the EMS Manager.
11. Restart the EMS server using the EMS Manager.

E.3 Installing External CA Certificates on the EMS Client

For each new EMS client version, the location of the NSS database is updated relative to the EMS client's path. For example, in version 6.6.31, it is located under the path "C:\Program Files\AudioCodes\EMS Client 6.6.31\externals\security\clientNssDb".

In the procedure below, <version> refers to the EMS client version number.

➢ **To install external CA Certificates on the EMS client:**

1. Stop the EMS client (if it is running).
2. Extract attached lib_old_nss.zip to C:\.
3. Move the old Certificate Database to a temporary folder and save the temporary noise file for key generation.

```
rename "C:\Program Files\AudioCodes\EMS Client
<version>\externals\security\clientNssDb" "clientNssDb_old"
```

```
echo
121212121212121212121212121212121212121212121212121212121212121
21212> C:\noise.txt
```

4. Create a new empty Certificate Database and corresponding password file.

```
echo fips140-2> C:\pwdfile.txt
mkdir "C:\Program Files\AudioCodes\EMS Client
6.2.35\externals\security\clientNssDb"
"C:\lib_old_nss\certutil.exe" -N -d "C:\Program
Files\AudioCodes\EMS Client
<version>\externals\security\clientNssDb" -f
"C:\pwdfile.txt"
```

5. Create a certificate request file (CSR) to transfer to the external CA for signing.

```
"C:\lib_old_nss\certutil.exe" -R -d "C:\Program
Files\AudioCodes\EMS Client
<version>\externals\security\clientNssDb" -s "CN=EMS
Client,O=AudioCodes" -a -o "C:\client.csr" -m 708 -f
"C:\pwdfile.txt" -z "C:\noise.txt" -1 -6
enter the following options after the previous
command:0,2,9,n,1,9,n
```

6. Transfer the generated CSR - "C:\client.csr" from the EMS client PC to the trusted CA.
7. Sign the CSR on the trusted CA machine.
8. Receive back two files from the trusted CA: your signed certificate (**client.pm**) and the certificate of the trusted CA (**cacent.pem**) and then save these files to the EMS client ("C:\" directory).

9. Import the Signed Certificate and CA Certificate into the EMS client's NSS database (Certificate Database).

```
"C:\lib_old_nss\certutil.exe" -A -d "C:\Program
Files\AudioCodes\EMS Client
6.2.35\externals\security\clientNssDb" -n clientcert -t
u,u,u -a -i "C:\client.pem" -f "C:\pwdfile.txt"
```

```
"C:\lib_old_nss\certutil.exe" -A -d "C:\Program
Files\AudioCodes\EMS Client
6.2.35\externals\security\clientNssDb" -n cacert -t
CT,CT,CT -a -i "C:\cacert.pem" -f "C:\pwdfile.txt"
```

```
"C:\lib_old_nss\modutil.exe" -fips true -dbdir "C:\Program
Files\AudioCodes\EMS Client
6.2.35\externals\security\clientNssDb"
```

10. Remove the temporary files (C:\pwdfile.txt, C:\noise.txt, C:\client.pem, C:\cacert.pem, and C:\client.csr).

11. Restart the EMS client.

E.4 Installing External CA Certificates on the JAWS EMS Client

For each new EMS client version, the location of the NSS database is updated relative to the EMS client's path. For example, in version 6.6.31, it is located under the path "C:\Program Files\AudioCodes\EMS Client 6.6.31\externals\security\clientNssDb". Before performing this procedure, change the "EMS Client 6.6.31" pattern to your actual EMS Client folder.

In cases where Mozilla FireFox is used, replace 'C:\Documents and Settings\%username%\Desktop' with 'C:\Program Files\Mozilla Firefox'

In cases where Maxthon2 is used, replace 'C:\Documents and Settings\%username%\Desktop" with "C:\Program Files\Maxthon2'

➢ **To install external CA Certificates on the EMS client:**

1. Stop the JAWS EMS client (if it is running).
2. Extract attached lib_old_nss.zip to C:\
3. Move the old Certificate Database to temporary folder and save the temporary noise file for key generation.

```
rename "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb" "clientNssDb_old"
```

```
echo
1212121212121212121212121212121212121212121212121212121212121
21212> C:\noise.txt
```

4. Create a new empty Certificate Database and corresponding password file for it.

```
echo fips140-2> C:\pwdfile.txt
mkdir "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb"
"C:\lib_old_nss\certutil.exe" -N -d "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb" -f "C:\pwdfile.txt"
```

5. Create a certificate request file (CSR) to be transferred to the external CA for signing.

```
"C:\lib_old_nss\certutil.exe" -R -d "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb" -s "CN=EMS Client,O=AudioCodes" -a -o
"C:\client.csr" -m 708 -f "C:\pwdfile.txt" -z
"C:\noise.txt" -1 -6
enter the following options after the previous
command:0,2,9,n,1,9,n
```

6. Transfer the generated CSR - "C:\client.csr" from the EMS client PC to the trusted CA.
7. Sign the CSR on the trusted CA machine.
8. Receive back two files from the trusted CA: your signed certificate (**client.pm**) and the certificate of the trusted CA (**cacent.pem**) and then save these files to the EMS client ("C:\" directory.
9. Import the Signed Certificate and CA Certificate into the EMS client's NSS database (Certificate Database).

```
"C:\lib_old_nss\certutil.exe" -A -d "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb" -n clientcert -t u,u,u -a -i "C:\client.pem"
-f "C:\pwdfile.txt"
```

```
"C:\lib_old_nss\certutil.exe" -A -d "C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb" -n cacert -t CT,CT,CT -a -i "C:\cacert.pem" -
f "C:\pwdfile.txt"
```

```
"C:\lib_old_nss\modutil.exe" -fips true -dbdir
"C:\Documents and
Settings\%username%\Desktop\JavaWebStart\externals\security
\clientNssDb"
```

10. Remove the temporary files (C:\pwdfile.txt, C:\noise.txt, C:\client.pem, C:\cacert.pem, and C:\client.csr).
11. Restart the JAWS EMS client.

E.5 Installing External CA Certificates on a Later EMS Client or JAWS Client

If you now replace the “AudioCodes-issued” certificates with external CA certificates and in future upgrade the EMS client, you do not need to repeat the procedure described above. Instead, you need only to overwrite the newly deployed **clientNssDb** with the NSS files from the previous EMS client version. Therefore, ensure that you maintain a *backup* of the **clientNssDb** files (**cert8.db**, **key3.db**, **secmod.db**) from the previous EMS client version. In addition, the new external CA certificates that are installed on the EMS client must match the external CA certificates that are installed on the EMS server.

Note that this procedure is relevant for certificate installation on both the EMS client and the JAWS client.

E.6 Client – Server Communication Test

- Verify the Client – Server communication.

  Ensure that the basic operations such as User Login, Gateway definition and Auxiliary File download to the gateway are working correctly.

E.7 Certificate Integration on Web Browser Side (Northbound Interface)

For the EMS client to operate with a web-based NMS system and to communicate with the EMS server via HTTPS, you require the appropriate certificate for the client side that is signed by the same external CA authority as the other external CA certificates obtained in the above procedures. Under these circumstances, the certificate should be in PKCS12 format and be loaded to the browser.

For the procedure for loading these certificates to a web browser, see Section D on page 173.

This page is intentionally left blank

F EMS Certificates Extensions for DoD PKI

This appendix describes the EMS client and server certificates extensions for DoD PKI.

The US Department of Defense includes a list of strict adherence requirements for the implementation of Client-Server PKI. To address these requirements, the following is implemented on the EMS server and client. In addition, the certificate management process on both the EMS server and client has been enhanced (persistence and usage):

- **DoD PKI Validation Extensions**

  This section describes the Validation extensions that are implemented on the EMS server and client for addressing the DoD PKI requirements. For example, certificate approval during SSL handshake information logging. By default, DoD PKI validations are disabled.

  See Section F.1 on page 195

- **DoD PKI and Certificate Management Extension**

  This section describes how a single NSS database and ESM server certificate implementation affects the SSL handshake process and the structure and configuration of the NSS database.

  See Section F.2 on page 197

F.1 DoD PKI Validation Extensions

The EMS server and client addresses the DoD PKI requirements that are described in this section.

F.1.1 The CA Trust Chain

The following actions must be performed to ensure that the EMS operates properly with the 'CA trust chain':

- Generate 'root CA' certificate (self-signed)
- Generate 'intermediate CA 1' certificate (signed by 'root CA')
- Generate 'intermediate CA 2' certificate (signed by 'root CA')
- Generate the 'EMS client' certificate (signed by 'intermediate CA 1')
- Generate the 'EMS server' certificate (signed by 'intermediate CA 2')
- On the 'EMS client', save the 'Trust store' certificates of 'root CA' and 'intermediate CA 1'
- On the 'EMS server', save the 'Trust store' certificates of 'root CA' and 'intermediate CA 2'
- Verify that the TLS connection (RMI) between the EMS client and the EMS server works properly.

F.1.2 DoD PKI Strict Validations

Additional DoD PKI strict validations can be applied to the EMS server, client or watchdog processes as described below. These validations are applied to end-entity and CA certificates.

The parameter 'RequireStrictCert', configured in the EMS properties file determines whether additional strict certification PKI validations are applied:

- Name: RequireStrictCert (or any other desired name); Type: integer; Range: 0-1 (0=disable, 1=enable); Default: 0

Note that CA certificates are not only stored in the NSS DB trust store, but may also be displayed by the remote SSL/TLS party as part of the connection negotiation (certificates of the intermediate CAs for the complete trust chain must be displayed together with the end-party certificate).

The certificate validation extensions described below are relevant for a PKI implementation using the following APIs:

- RMI over SSL
- HTTPS (Apache)
- SSH over SSL

When requireStrictCert is set to ‘1’, the following certificate validation extensions are performed:

- Verifies that all end-entity and CA certificates (not root certificates) have keyUsage (-1) extension
- CA certificates with the keyCertSign set to '0' are rejected
- Verifies that all CA certificates have the basicConstraints extension
- Verifies that all CA certificates have cA bit in basicConstraints extension set to 1.
- Verifies that all end-entity certificates with keyCertSign set to '1' also have the basicConstraints extension. End-entity certificate with keyCertSign set to '0' and without basicConstraints extension are allowed.
- Verifies that certificate chains in violation of a pathLenConstraint set in one of the CA certificates are rejected.
- Verifies that the End-entity certificates used for the TLS client connections include the digitalSignature bit set.
- Verifies that the End-entity certificates used for the TLS server connections, include either the digitalSignature or the keyEncipherment bits set
- Verifies that all certificates have non-empty CN (common name) in the 'Subject' field.

F.1.3 Debugging

- When a certificate is rejected – a log specifying the reason for the rejection is generated.
- Generation of a complete trace of a TLS certificate exchange (including dumping of all certificates received, success/failure status and reasons).

F.2 DoD PKI and Certificate Management Extension

A **single** NSS database with a **single** server certificate is used by the EMS server, Apache and Watchdog processes.

This section describes how this implementation affects the SSL handshake process and the structure and configuration of the NSS database.

F.2.1 SSL Handshake Process

The NSS validation process for the EMS client and EMS server certificates during the SSL handshake is described as follows:

- The only NSS database on the EMS server side is located at /opt/nss/fipsdb and contains a single server certificate.
- During the EMS server upgrade, the single NSS database is not replaced by the new version.
- The only NSS database on the client side is located at the usual location: (externals/security/clientNssDb)

F.2.2 NSS Database Parameters

The NSS database parameters described in this section can be configured for all EMS server processes from the same location (externals/configurationProperties directory):

- **certNickname** – The nickname of the server/ client/ watchdog in the NSS database. This parameter can be configured at the following locations:

  'externals/configurationProperties/serverNssConfig.properties'
  (default – servercert)
  'externals/configurationProperties/watchdog.propeties'
  (default – servercert)
  'externals\configurationProperties\ clientNssConfig.properties'
  (default – clientcert)
- **unixNssDbPath** – The absolute path of the single NSS database on the EMS server side. This parameter can be configured at the following location:
  'externals/configurationProperties/serverNssConfig.properties'
  (default –/opt/nss/fipsdb)
- **nssDbPath**– The relative path of the single NSS database on the client side. The parameter can be configured at the following location:
  'externals/configurationProperties/clientNssConfig.properties'
  (default – externals\\security\\clientNssDb)

- **nssDbPassword** – The password of the NSS database. The parameter can be configured at the following location:
  'externals/configurationProperties/serverNssConfig.properties'
  (default – fips140-2)
  'externals\configurationProperties\clientNssConfig.properties'
  (default – fips140-2)
- **The configuration file** – 'externals/configurationProperties/serverNssConfig.properties' has permissions of 600 of user 'root', due to sensitive NSS database password information.

F.2.3 HTTPS Client

The pkcs12 file 'clientcert.crt' for the HTTPS client is located in the EMS client folder at the 'nssDbPath' at the following location:

'Externals\configurationProperties\clientNssConfig.properties'

The password of this file is 'passfile'. The 'clientcert.crt' file is the "default" configuration file that uses self-signed certificates (supplied by AudioCodes) for the 'DoD configuration'. If you are using external certificates, then these should be provided by the DoD.

For the procedure for loading these certificates to a web browser, see Section D on page 173.

F.2.4 DoD PKI Strict Validations

Additional DoD PKI strict validations can be applied to the EMS server, client, WatchDog, Apache and SSH over SSL processes. These validations are applied to end-entity and CA certificates.

The parameter 'requireStrictCert' determines whether additional DoD PKI validations are implemented. By default, 'requireStrictCert' is disabled ('0'). When set to '1', additional DoD PKI validations are applied on the EMS server, client, WatchDog, Apache and SSH over SSL processes.

For EMS server, WatchDog and SSH over SSL server side processes, the parameter 'requireStrictCert' is added to the following file:

- 'externals/configurationProperties/serverNssConfig.properties'

For EMS client and SSH over SSL client side processes, the parameter 'requireStrictCert' is added to the following file:

- 'externals/configurationProperties/clientNssConfig.properties'

For Apache process on server side, the parameter 'NSSRequireStrictCert' is added to the following file:

- '/usr/local/apache/conf/nss.conf'

The entire list of strict certification validations are described in Section F.1.2 on page 196.

The option EmsServerManager – 'Strict PKI Configuration' under the 'Security' sub menu displays the status of the 'requireStrictCert' parameter and allows you to enable or disable this feature.

Note: This feature can only be enabled or disabled via the EMS Server Manager for the server side. For the client side, this action should be performed manually by the user – directly in the mentioned file ('externals/configurationProperties/clientNssConfig.properties'). Regardless, after a modification on either the server or the client, the relevant applications should be restarted to activate the modification.

F.2.5 Debugging

- On both the EMS client and server side, a logger (with cycle=3) in the Logs folder 'sslLog.txt' is generated. This log file contains all SSL handshake and certificates information, including failure reasons and success details.
- SSL Tunneling uses its own log file: 'sslTunnelingLog.txt'.
- In case of certificate approval failure by the NSS, or any error during the approval stage, a new Event is generated (‘Source’ of event: X509 Certificate)
- When 'Strict PKI' is enabled, the directive LogLevel (in '/usr/local/apache2/conf/nss.conf') is changed to 'info' (instead of 'warn').

  The directive log level 'NSSRequireStrictCert' (disabled by default) is added in the following location:

  ' /usr/local/apache2/conf/nss.conf'

  This directive indicates whether ‘Strict PKI’ is enabled.
- In the case of Java Web Start, the NSS database is located at the same path as the regular EMS client:

  'externals\security\clientNssDb'

  As a relative path to its home directory (depending on the browser type).

  In addition, the file
  'externals\configurationProperties\clientNssConfig.properties'
  is located under the same relative path, and is configurable after the initial launch of the same version.

  All the information in reference to certificates, SSL handshake, successes and failures are displayed in the JAWS console and not in the 'sslLog.txt' file, as in the case for a regular EMS client.

This page is intentionally left blank

G EMS Application Acceptance Tests

This appendix describes the EMS Application Acceptance tests.

G.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.

G.2 Configuration

This section describes the EMS application configuration acceptance tests.

G.2.1 Client Installation

Table G-1: Acceptance Test – Client Installation

Step Name	Description	Expected Result
Install	Install the client software	Verify that all the instructions are clear.

G.2.2 Server Installation

Table G-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.

G.2.3 Add Auxiliary File

Table G-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.

G.2.4 Add Media Gateway

Table G-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.

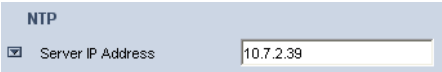
G.2.5 Provisioning – Mediant 5000/ Mediant 8000

Table G-5: Acceptance Test – Provisioning: Mediant 5000/ Mediant 8000

Step Name	Description	Expected Result
Configure the MG	Configure the MG with at least one board and unlock it	MG & Board status is unlocked.
Go to trunk level	Drill down to trunk level Board right click >> Status >> DS1 trunks	Trunks table is displayed according to the board type.
Trunk Properties	Open trunk#1 properties	The frame provisioning opens and all the parameters are available.
Set parameter "Trunk Name"	Set the parameter "Trunk Name" to TrunkNameTest 	The new value is set on the media gateway. 
Restore parameter value	Set the parameter back to the original trunk name.	The old value was restored.

G.2.6 Provisioning – CPE Devices

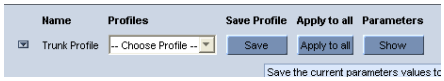
Table G-6: Acceptance Test – Provisioning: CPE Devices

Step Name	Description	Expected Result
Go to network frame	Click the network button.	Network configuration is displayed.
RTP Settings tab	Click the Application tab	Applications settings are displayed.
Set parameter "NTP Server IP Address"	Set the parameter to your PC IP address. 	The new value is set on the media gateway. 
Restore parameter value	Restore the parameter to your NTP Server IP address.	The original value was restored.

Note: CPE devices include the following products: MediaPack; Mediant 600; Mediant 800 MSBR; Mediant 800 Gateway and E-SBC, Mediant 1000 MSBR; Mediant 1000 Gateway and E-SBC; Mediant 1000, Mediant 2000, Mediant 2600 E-SBC, Mediant 3000, Mediant 4000 SBC, Mediant 9000 SBC, Mediant SE and Mediant VE products.

G.2.7 Entity Profile – Digital CPE Devices

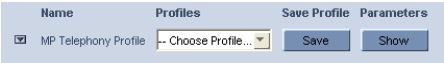
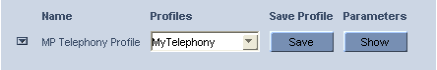
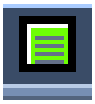
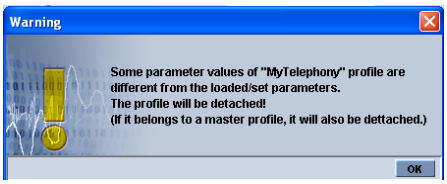
Table G-7: Acceptance Test – Entity Profile: Digital CPE Devices

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. 	The new profile appears in the profiles list. 
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 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; Mediant 1000, Mediant 2000 and Mediant 3000.

G.2.8 Entity Profile – Analog CPE Devices

Table G-8: 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 	The new profile is displayed in the profiles list. 
Expose profile parameters	Press on the “show profile parameters” button 	All profiles parameters are marked with the profile name. 
Detach profile	Change one of the profile parameters, and then press **Apply**.	A detach profile pop up message is displayed. 

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.

G.3 Faults

G.3.1 Alarm Receiver

Figure G-1: Alarm Receiver

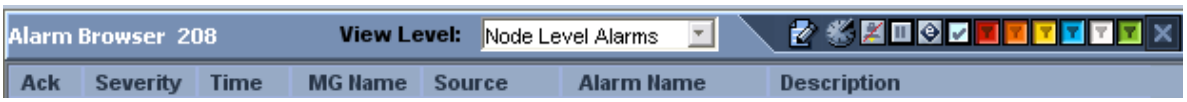


Table G-9: Acceptance Test – Alarm Receiver

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.

G.3.2 Delete Alarms

Table G-10: 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.

G.3.3 Acknowledge Alarm

Table G-11: Acceptance Test – Acknowledge Alarm

Step Name	Description	Expected Result
Check Box	Click on the Acknowledge check box	The alarm is marked as acknowledge.

G.3.4 Forwarding Alarms

Figure G-2: Destination Rule Configuration

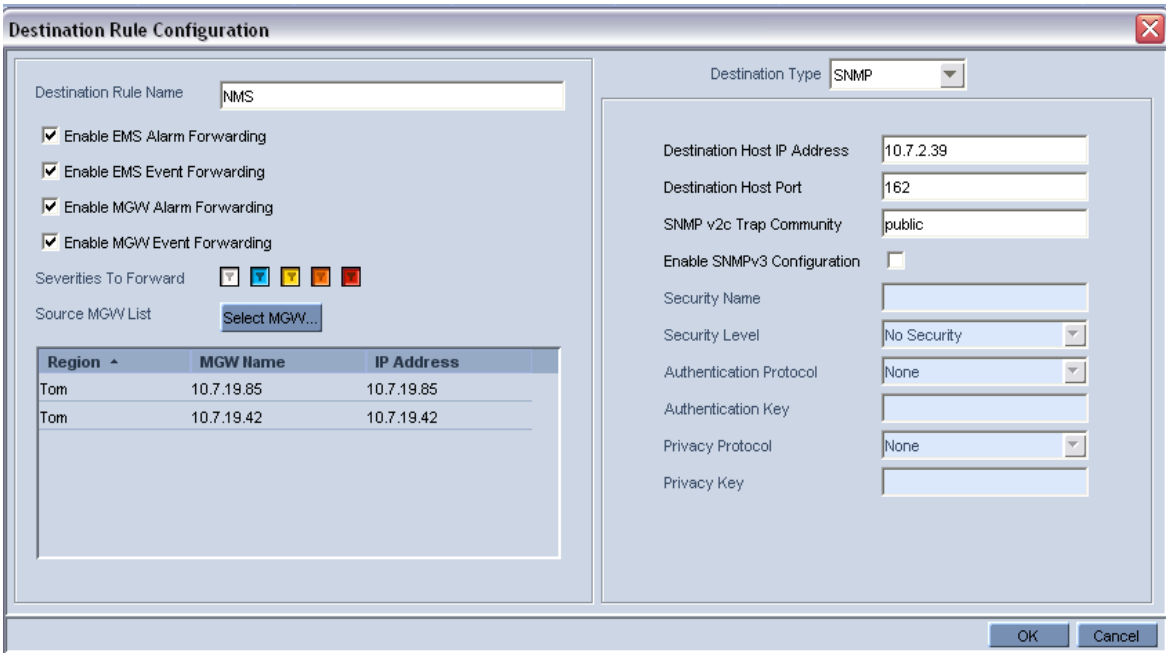


Table G-12: Acceptance Test – Forwarding Alarms

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.

G.4 Security

This section describes the EMS application security tests.

G.4.1 Users List

Figure G-3: Users List

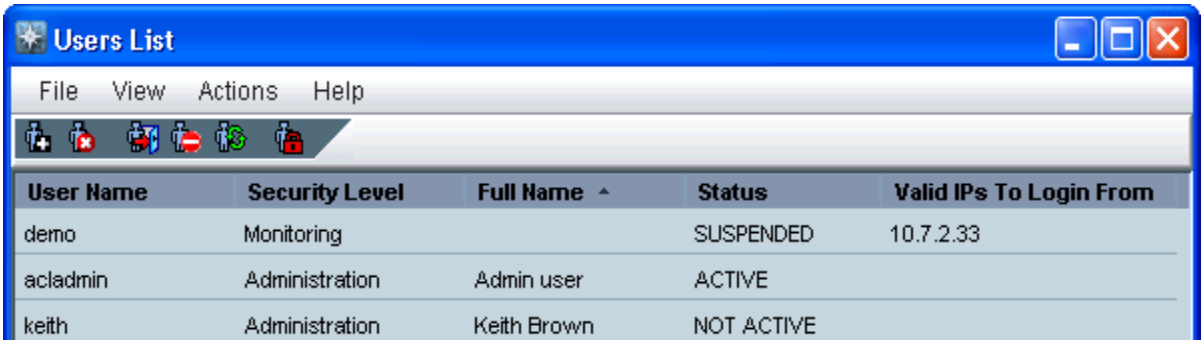


Table G-13: Acceptance Test – Add an Operator

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.

G.4.2 Non Repetitive Passwords

Table G-14: 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."

G.4.3 Removing Operator

Table G-15: 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.

G.4.4 Journal Activity

Figure G-4: Actions Journal

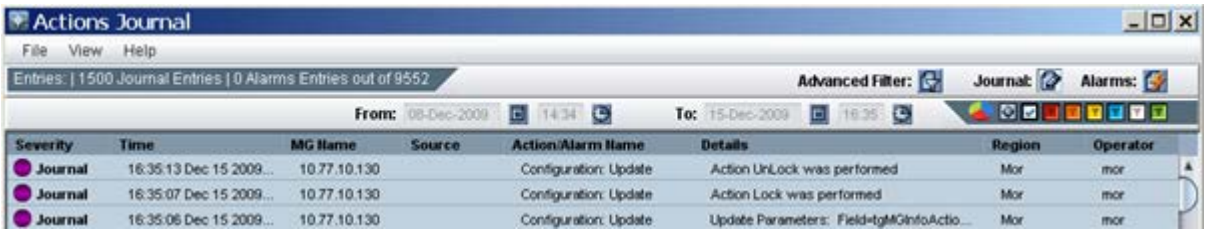


Table G-16: Acceptance Test – Journal Activity

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.

G.5 Utilities

This section describes the EMS application utilities acceptance tests.

G.5.1 Configuration Parameter Search

G.5.1.1 Basic Search

Figure G-5: Configuration Parameter Search drop-down list box

Table G-17: Acceptance Test – Configuration Parameter: Basic Search

Step Name	Description	Expected Result
Search Box	In the toolbar, enter a search string in the parameter search box and then click the button. The configuration parameter basic search option is context-sensitive; therefore you must connect to a media gateway to enable this feature.	Displays a dialog with a list of results according to selected criteria.

G.5.1.2 Advanced MG Search

Figure G-6: Configuration Parameter: Advanced Search

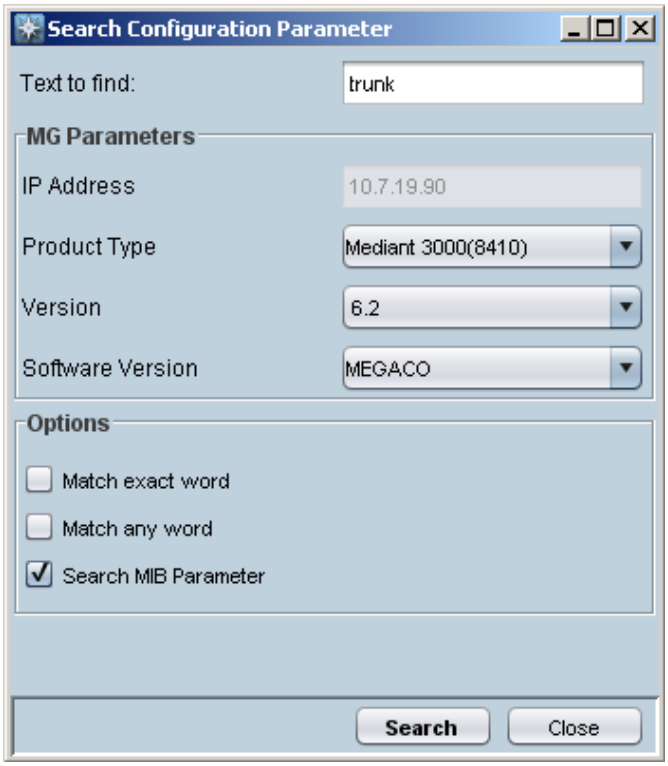


Table G-18: Acceptance Test – Configuration Parameter: Advanced Search

Step Name	Description	Expected Result
Open Advanced Search Configuration Parameter screen	Open the Advanced search dialog by clicking  in the Toolbar or by choosing Tools >> Search Configuration Parameter in the EMS Main menu.	The Advanced Search Configuration dialog opens.
IP	Search /MG/Unknown machine by IP address	Displays a dialog with a list of results according to selected criteria.
Product Type	Search according to product type	Displays a dialog with a list of results according to selected criteria.
Version	Search according to the product version	Displays a dialog with a list of results according to selected criteria.
Software Version	Search according to the software version	Displays a dialog with a list of results according to selected criteria.
Advanced search Options	Match exact word, any word or search for a MIB parameter.	Displays a dialog with a list of results according to selected criteria.

When you double-click on a specific retrieved entry, the navigation path to the parameter's provisioning frame is displayed in the lower pane of the Search result dialog. You then have the option to open the provisioning frame that is related to the search result entry.

G.5.2 MG Search

Figure G-7: Media Gateway Search

Table G-19: 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.

G.5.3 Online Help

Table G-20: 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.

G.5.4 Backup and Recovery

Table G-21: 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.

This page is intentionally left blank

H 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 prior data residing on the designated disk drives.

H.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.

H.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*.

H-1: Hardware Preparation

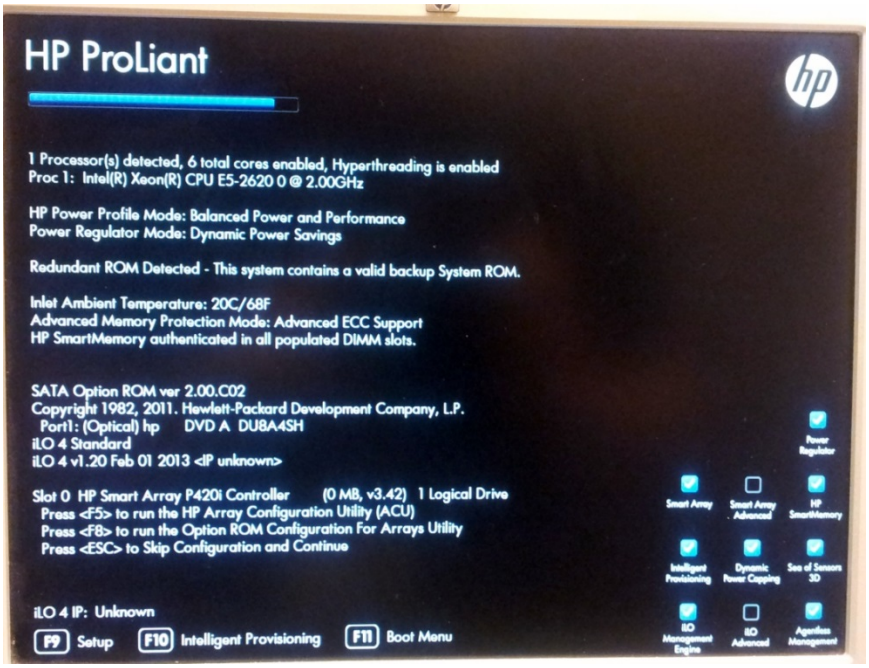
H.3 Configuring RAID-0

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:

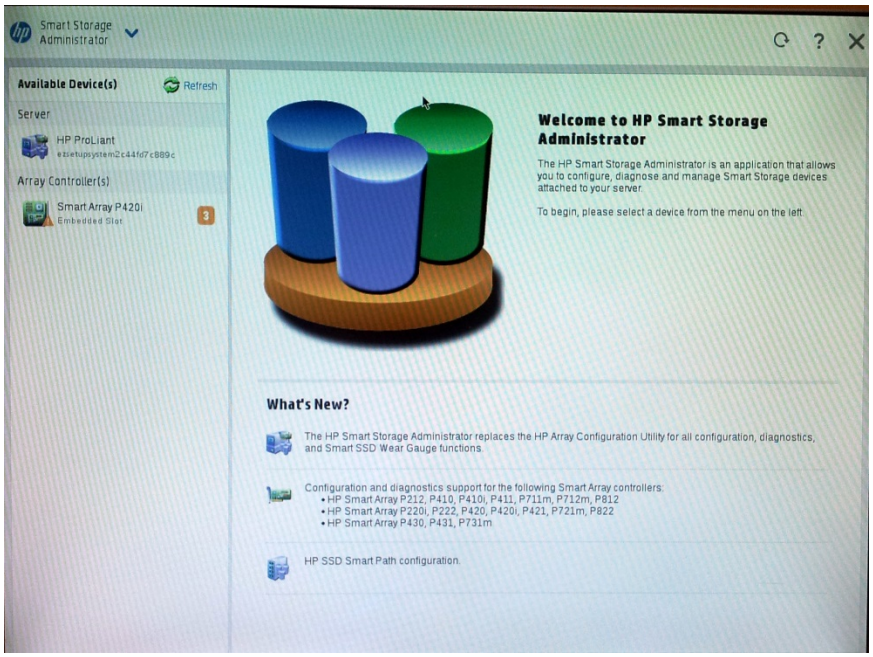
H-2: HP Array Configuration Utility (ACU)



3. Press <**F5**> to run the HP Array Configuration Utility (ACU).
4. Wait for the ACU to finish loading.

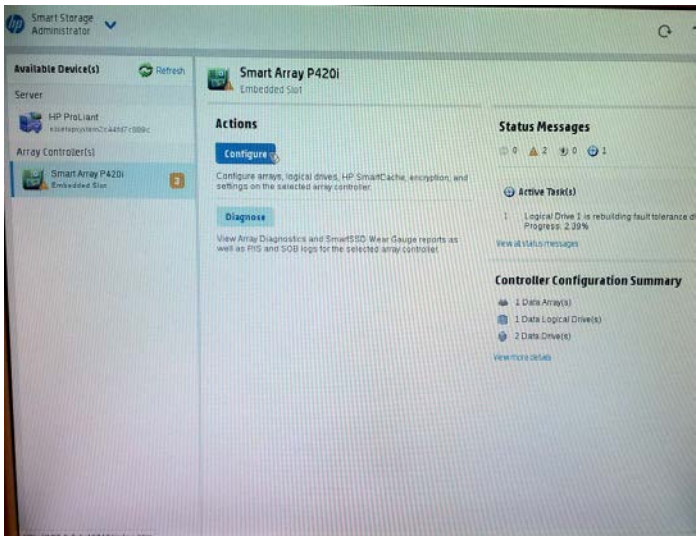
When the ACU is ready, the following screen is displayed:

H-3: RAID-Latest Firmware Versions



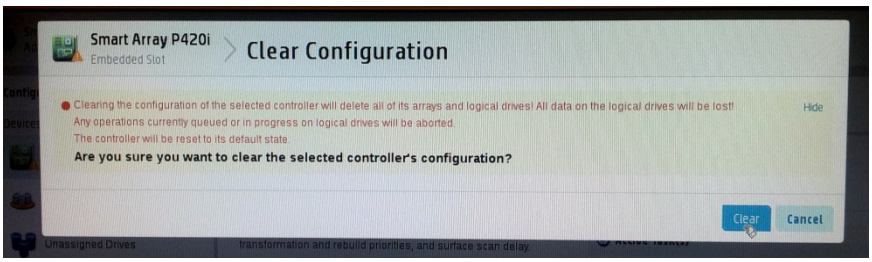
5. In the left-hand pane, select **Smart Array P420i**; an Actions menu is displayed:

H-4: Actions Menu



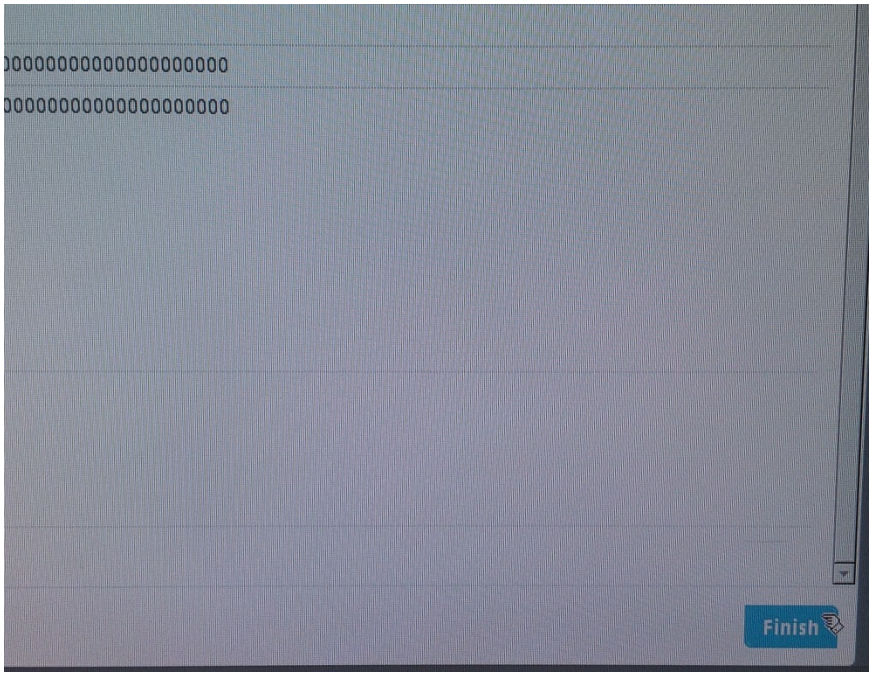
6. Click **Configure**, and then click **Clear Configuration** to clear any previous configuration; the following confirmation is displayed:

H-5: Clear Configuration



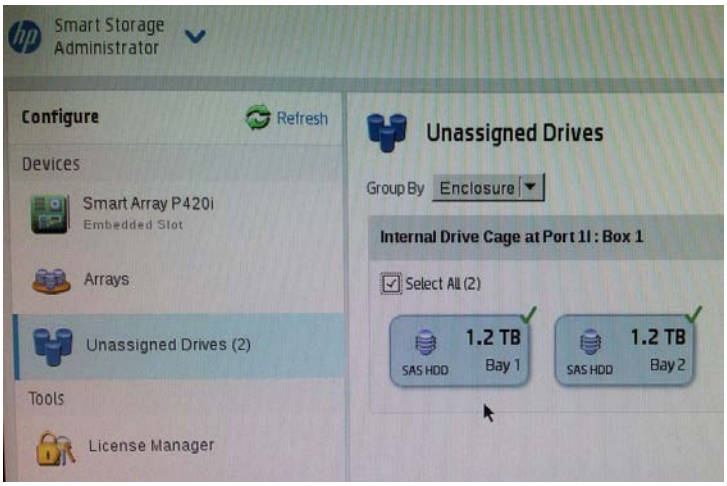
7. Click **Clear** to confirm; a summary display appears:

H-6: Summary Screen



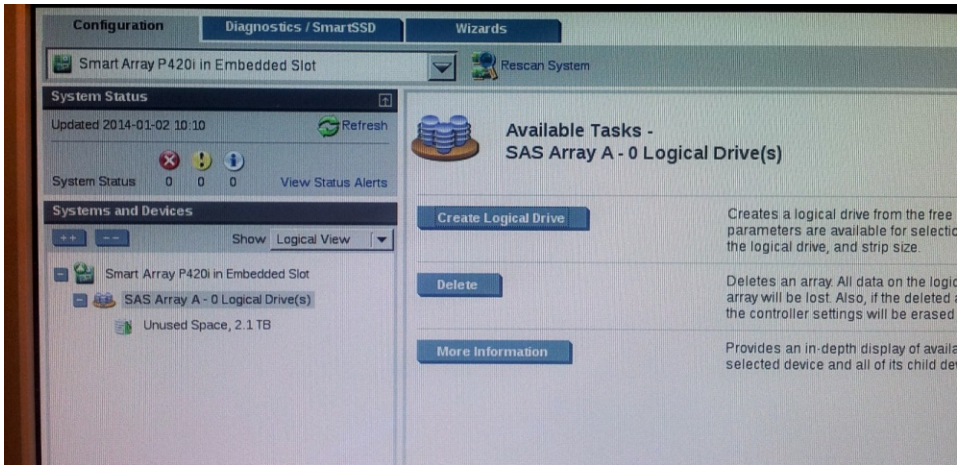
8. Click **Finish** to return to the main menu. The following screen is displayed:

H-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:

H-8: Logical Drive

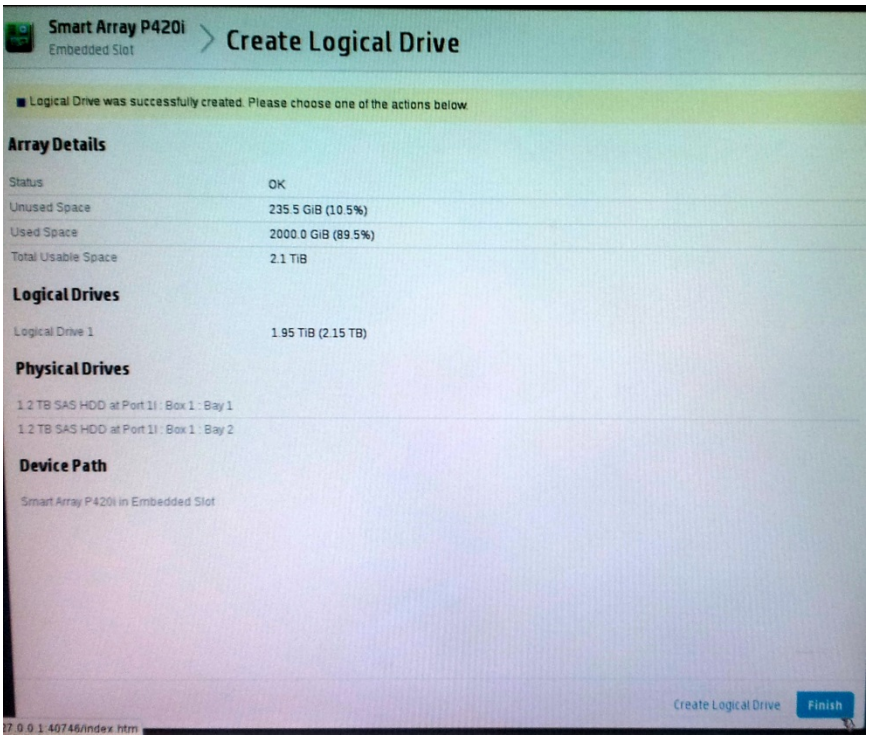


After the array is created, a logical drive should be created.

13. Click **Create Logical Drive**.

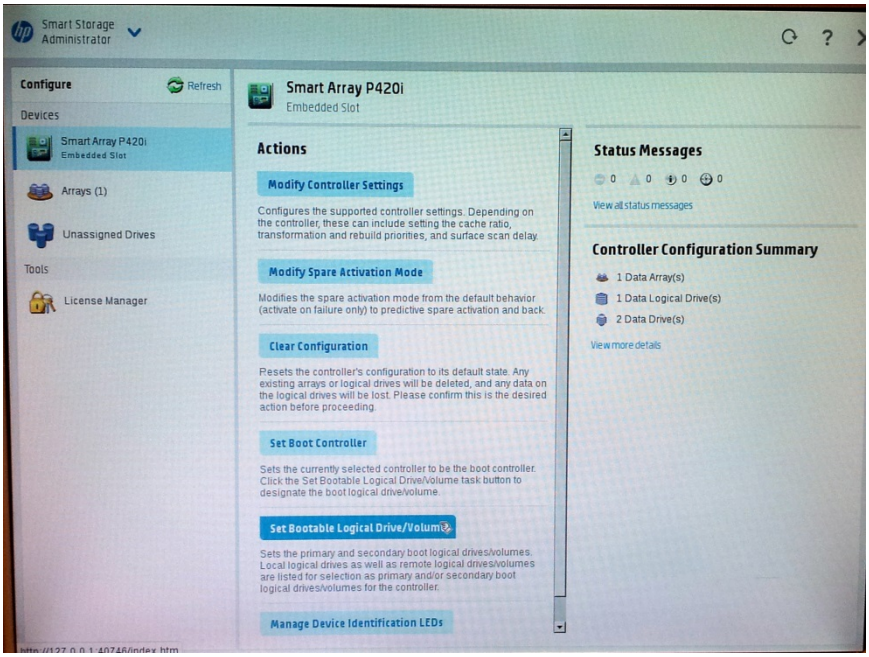
A summary screen is displayed:

H-9: Summary Screen



14. Click **Finish**.

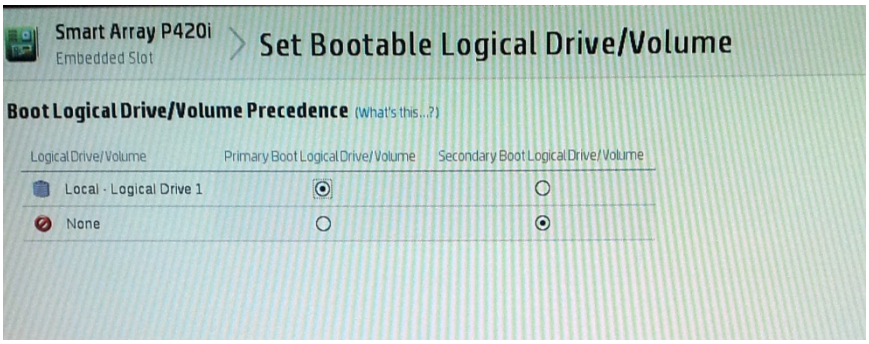
H-10: Set Bootable Logical Drive/Volume



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:

H-11: Set Bootable Logical Drive/Volume



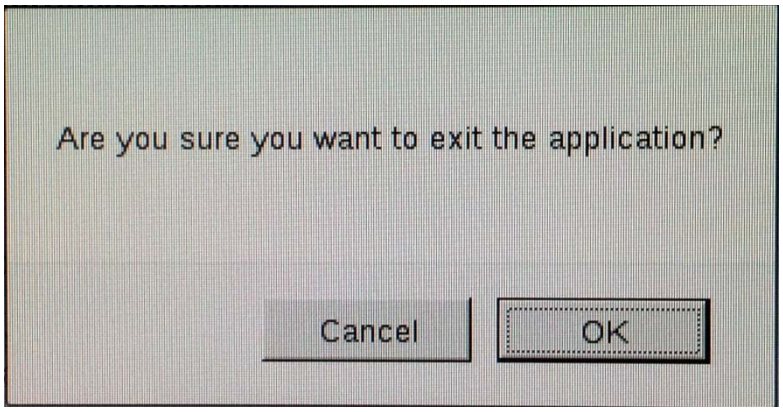
16. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.

    A summary window is displayed.

17. Click **Finish**.

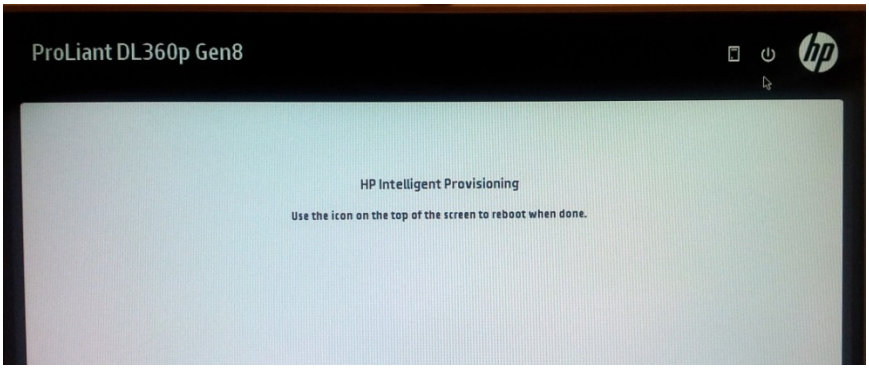
18. Exit the ACU by clicking the **X** sign on the top right-hand side of the screen, and then confirm the following dialog:

H-12: Exit Application



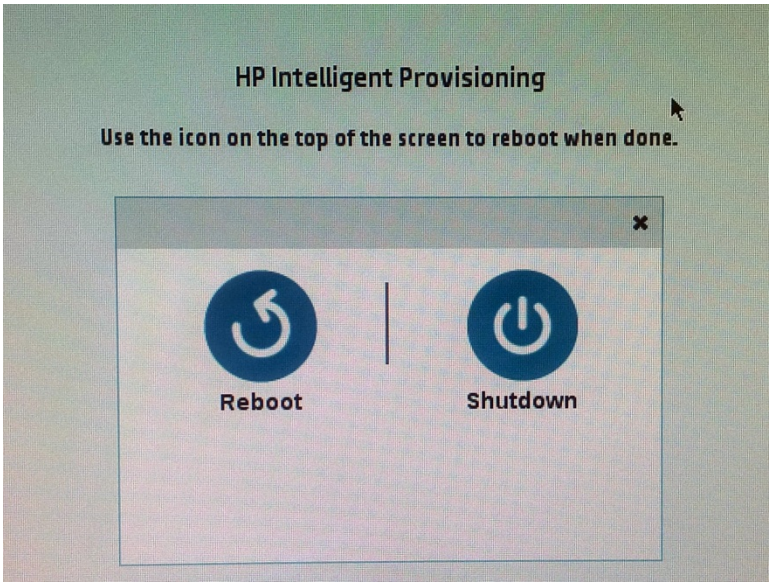
19. Click **Exit ACU** at the bottom left-hand corner of the screen; the following screen is displayed:

H-13: Power Button



20. Click the **Power** icon in the upper right-hand corner of the screen.
    The following screen is displayed:

H-14: Reboot Button



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 31).

This page is intentionally left blank

AudioCodes One Voice Operations Center

Element Management System &
Session Experience Manager

Installation, Operation and Maintenance Manual

www.audiocodes.com