

AudioCodes EMS Element Management System

Element Management System (EMS) Server Installation, Operation & Maintenance Manual

Version 5.8

Document #: LTRT- 94124



Notice

In this document, the Avaya G860 Media Gateway corresponds to the Mediant 5000. Note that some features and capabilities contained in this document are not supported by Avaya. Consult your authorized Avaya Sales or Partner resource to confirm the Avaya support features.

Table of Contents

1	Overview	11
2	EMS Server and Client Requirements.....	13
3	EMS Software Delivery – DVD	15
4	EMS Server Installation Requirements.....	17
	4.1 Hardware Requirements.....	17
	4.1.1 Testing Hardware Requirements on the Solaris Platform.....	17
	4.1.2 Testing Hardware Requirements on the Linux Platform.....	18
5	Installing the EMS Server on the Solaris Platform	21
	5.1 Installing the Solaris 10 OS from the AudioCodes DVD	21
	5.2 Installing the EMS Server on the Solaris Platform	22
6	Installing the EMS Server on the Linux Platform.....	25
	6.1 Installing Linux CentOS 5.3 from the AudioCodes DVD	25
	6.2 Installing the EMS Server on the Linux Platform.....	28
	6.2.1 Oracle Software Installation.....	33
7	Upgrading the EMS Server.....	35
	7.1 Major Version Upgrade.....	35
	7.2 Minor Version Upgrade.....	35
	7.2.1 Upgrading from the Installation DVD	35
	7.2.2 Upgrading from the Installation TAR file	40
8	EMS Server Machine Maintenance.....	43
	8.1 General Info and Logs Collection.....	47
	8.1.1 General Info	47
	8.1.2 Collecting Logs	49
	8.2 Networking.....	49
	8.2.1 Change Server's IP Address.....	49
	8.2.2 Configure Ethernet Interfaces.....	50
	8.2.2.1 Add Interface.....	52
	8.2.2.2 Remove Interface.....	53
	8.2.2.3 Modify Interface	54
	8.2.3 Configure Ethernet Redundancy on Solaris	55
	8.2.3.1 Add Redundant Interface	56
	8.2.3.2 Remove Ethernet Redundancy	58
	8.2.3.3 Modify Redundant Interface	59
	8.2.4 Configure Ethernet Redundancy on Linux.....	60
	8.2.4.1 Add Redundant Interface	60
	8.2.4.2 Remove Ethernet Redundancy	62
	8.2.4.3 Modify Redundant Interface	63
	8.2.5 Configuring the DNS Client.....	64
	8.2.6 Static Routes	65
	8.2.7 SNMP Agent.....	66
	8.2.7.1 SNMP Manager Configuration	66
	8.2.7.2 Configure NAT	66
	8.2.7.3 Sending System Alarms.....	67
	8.2.7.4 Stopping System Alarms.....	67

8.3	Security	68
8.3.1	Basic Hardening	68
8.3.1.1	Start Basic Hardening	69
8.3.1.2	Rollback	70
8.3.2	Advanced Hardening	72
8.3.3	SSL Tunneling Configuration	73
8.3.3.1	EMS Server-SSL Tunneling Configuration	73
8.3.3.2	EMS Client-SSL Tunneling Configuration	74
8.3.4	Changing DBA Password	75
8.3.5	OS Passwords Settings	76
8.3.6	Add EMS User	77
8.3.7	Start / Stop File Integrity Checker	77
8.4	Maintenance.....	77
8.4.1	Configure NTP	77
8.4.2	Change System Timezone	78
8.4.3	Change System Time and Date.....	79
8.4.4	Start /Stop the EMS Server	79
8.4.5	Web Server Configuration	79
8.4.6	Backup the EMS Server	81
8.4.7	Schedule Backup for the EMS Server	82
8.4.8	Restore the EMS Server.....	82
8.4.9	Reboot the EMS Server.....	82
9	Configuring the Firewall.....	83
10	Installing the EMS Client.....	87
10.1	Installing the EMS Client on a Client PC.....	87
10.2	Running the EMS on a Client PC	87
10.3	First-Time Login	87
10.4	Installing and Running the EMS Client on a Client PC using Java Web Start (JAWS):.....	88
11	Appendix A - Frequently Asked Questions (FAQs).....	89
11.1	“SC>” Prompt Displayed in User Console on Sun Solaris	89
11.2	JAWS not running	89
11.3	After installing JAWS - the EMS application icon is not displayed on the desktop	90
11.4	After Rebooting the Machine	91
11.5	Changes Not Updated in the Client.....	91
11.6	Removing the EMS Server Installation	91
12	Appendix B – Site Preparation Prior to Upgrade.....	93
13	Appendix C - Daylight Saving Time (DST).....	95
13.1	EMS Client.....	95
13.2	Windows.....	95
13.2.1	Java	96

13.3 Example of Installing Windows Patches on the EMS Client	96
13.4 Example of Installing the Java Patch for the EMS Client.....	98
14 Appendix D - OpenCA OCSP Daemon (OCSPD) v1.5.2	99
14.1 Overview.....	99
14.2 Installation.....	99
14.3 Viewing OCSPD Logs	99
14.4 Starting/Stopping OCSPD	100
14.5 Verifying OCSPD Installation	100
14.6 Configuring OCSPD	101
15 Appendix E - Security Certificates Signing Procedure.....	103
15.1 Overview.....	103
15.1.1 Mediant 3000 and MediaPack	103
15.2 Installing External CA Certificates on the EMS Server	104
15.3 Installing External CA Certificates on the EMS Client	107
15.3.1 Installing External CA Certificates on a Later EMS Client	109
15.4 Client – Server Communication Test	109
15.5 Certificate Integration on Web Browser Side (Northbound Interface).....	109
16 Appendix F – EMS Application Acceptance Tests	111
16.1 Introduction	111
16.2 Configuration.....	111
16.2.1 Client Installation	111
16.2.2 Server Installation	111
16.2.3 Add Auxiliary File	112
16.2.4 Add Media Gateway	112
16.2.5 Provisioning – M5K/ M8K	112
16.2.6 Provisioning – MP/ M1K/ M2K/ M3K.....	113
16.2.7 Entity Profile – M1K Digital/M2K/M3K/ M5K/M8K.....	113
16.2.8 Entity Profile – MP/M1K Analog.....	114
16.2.9 Create Master Profile.....	114
16.2.10 Remove & Add MG.....	114
16.2.11 Apply Master Profile.....	115
16.3 Faults	115
16.3.1 Alarm Receiver	115
16.3.2 Delete Alarms	115
16.3.3 Acknowledge Alarm	115
16.3.4 Forwarding Alarms.....	116
16.4 Security	116
16.4.1 Adding Operator	116
16.4.2 Non Repetitive Passwords.....	117
16.4.3 Removing Operator	117
16.4.4 Journal Activity.....	117
16.5 Utilities.....	118
16.5.1 Provisioning Parameter Search	118
16.5.2 MG Search.....	118
16.5.3 Online Help	119
16.5.4 Backup & Recovery	119

List of Figures

Figure 5-1: Finish system checks.....	22
Figure 5-2: Orahome and Oradata directories	23
Figure 5-3: EMS software directory.....	23
Figure 5-4: Oracle Software Installation.....	24
Figure 5-5: Installation Finish Screen.....	24
Figure 6-1: CentOS.-5 Welcome screen	25
Figure 6-2: General Linux Patching	28
Figure 6-3: Linux License Agreement	29
Figure 6-4: Linux JDK Software License Agreement.....	30
Figure 6-5: Linux Pre-installation Requirements Check	31
Figure 6-6: Linux Kernel Verification	31
Figure 6-7: Linux-ORACLE Variables Verification.....	32
Figure 6-8: Linux-EMS Variables Verification.....	33
Figure 6-9: Linux-Installing EMS Software.....	33
Figure 6-10: Linux-Oracle Software Installation	34
Figure 6-11: Linux-Installation Completed Successfully.....	34
Figure 8-1: ACEMS menu.....	43
Figure 8-2: EmsServerManager Menu (All SSH options – Solaris).....	44
Figure 8-3: EmsServerManager Menu (All options – Linux).....	45
Figure 8-4: General Info.....	48
Figure 8-5: Server IP Configuration Updates	49
Figure 8-6: User Configuration Updates	50
Figure 8-7: EMS Server: Triple Ethernet Interfaces	51
Figure 8-8: Physical Interface Configuration Menu (Solaris)	52
Figure 8-9: Modify Interface	54
Figure 8-10: Physical Ethernet Interfaces Redundancy	55
Figure 8-11: Ethernet Redundancy Configuration Menu	56
Figure 8-12: Add Redundant Interface.....	57
Figure 8-13: Ethernet Redundancy Interface to Disable	58
Figure 8-14: Modify Redundant Interface.....	59
Figure 8-15: Ethernet Redundancy Configuration Menu	60
Figure 8-16: Add Redundant Interface (Linux).....	61
Figure 8-17: Ethernet Redundancy Interface to Disable	62
Figure 8-18: Modify Redundant Interface (Linux).....	63
Figure 8-19: Configure DNS Client	64
Figure 8-20: Configure DNS Client	64
Figure 8-21: DNS Setup.....	64
Figure 8-22: Routing Table and Menu	65
Figure 8-23: Solaris SNMP Manager	67
Figure 8-24: Basic Hardening Menu	69
Figure 8-25: Prompts Referring to SNMP Services.....	69
Figure 8-26: Activating the EMS Hardening Feature.....	70
Figure 8-27: Basic Hardening, Rollback - Open all services	70
Figure 8-28: Rolling Back from Hardened Server -1	71
Figure 8-29: Rolling Back from Hardened Server -2	71
Figure 8-30: Rolling Back from Hardened Server -3	71
Figure 8-31: Activating the Advanced Hardening Feature.....	72
Figure 8-32: Rolling Back from Advanced Hardening	73
Figure 8-33: SSL Tunneling Configuration Manager.....	73
Figure 8-34: Changing the DB Password.....	75
Figure 8-35: Changing the DB Password.....	75
Figure 8-36: Changing Password General Settings	76
Figure 8-37: Changing User's Password and Properties	76
Figure 8-38: Start NTP.....	78
Figure 8-39: Change System Timezone	79
Figure 8-40: Change System Time and Date.....	79
Figure 8-41: Web Server Configuration	80

Figure 8-42: Scheduled Backup for the EMS Server.....	82
Figure 9-1: Firewall Configuration Schema.....	85
Figure 12-1: Save MGs Tree Command	93
Figure 13-1: Installing Windows OS Patches – PC Information	96
Figure 13-2: Installing Windows OS Patches – Selecting the Operating System	97
Figure 13-3: Installing Windows OS Patches – Download and Install	97
Figure 13-4: Java Installation’s Home Directory.....	98
Figure 13-5: Changing the Directory to ‘bin’	98
Figure 13-6: Installing the Patch	98

List of Tables

Table 2-1: EMS- Minimal Platform Requirements	13
Table 9-1: Firewall Configuration Rules	83
Table 9-2: OAM&P Flows: NOC ↔MG EMS.....	86
Table 9-3: OAM&P Flows: MG EMS→NOC.....	86

Notice

This IO&M Manual describes the installation, operation and maintenance of AudioCodes' EMS 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>.

© 2009 AudioCodes Inc. All rights reserved

This document is subject to change without notice.

Date Published: December-21-2009



Note: The EMS supports the following AudioCodes products:

- Mediant 600/1000/2000/3000/5000/8000 Media Gateways.
- IPmedia 2000/3000/5000/8000 Media Servers.
- MediaPack Media Gateways MP-500, MP-102 (FXS), MP-104 (FXS and FXO), MP-108 (FXS and FXO), MP-112 (FXS), MP-114 (FXS), MP-118 (FXS) and MP-124 (FXS), collectively referred to in this manual as MediaPacks.

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.

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 provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com

Document Conventions

- Courier - UNIX Commands
 - []** - **User-inserted input**
 - Times New Roman, bold, size 11** - User name, path or file name
- When x.y.z appears in this document as part of a software file name, 'x.y' indicates the major version and 'z' indicates the build number. For example, 5.6.14: '5.6' indicates the major version and '14' indicates the build number.

Related Documentation

Manual Name
Mediant 5000 / 8000/IPmedia 8000 Media Gateway Installation, Operation and Maintenance Manual
Mediant 5000 / 8000/IPmedia 8000 Media Gateway Release Notes
Mediant 3000 User's Manual
IPmedia 3000 Media Server User's Manual
Mediant 600 User's Manual
Mediant 2000 User's Manual
IPmedia 2000 Media Server User's Manual
MediaPack MGCP-MEGACO User's Manual
MediaPack User's Manual
MP-500 User's Manual
Element Management System (EMS) Server Installation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) Release Notes
Element Management System (EMS) Online Help
Mediant 5000 / 8000/IPmedia 8000 Media Gateway Programmer's User Manual
EMS Parameter Guide for the Mediant 5000 and Mediant 8000 Gateways/IPmedia 8000 Media Server
EMS Parameter Guide for the MP-500, Mediant 600 and Mediant 1000
EMS Parameter Guide for the Mediant 2000
EMS Parameter Guide for the Mediant/IPmedia 3000
EMS Parameter Guide for the MediaPack

1 Overview

The EMS provides customers with the capability to easily and rapidly provision, deploy and manage the following:

- Mediant 5000 / 8000 Media Gateways and IPmedia 5000/8000 Media Servers
- Mediant 600 / 1000 / 2000 / 3000 Media Gateways and IPmedia 3000 Media Servers
- MP-500 and MediaPack Media Gateways

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

The EMS comprises two infrastructure elements:

- EMS Server (running on Solaris or Linux operating systems)
- EMS Client (running on Microsoft™ Windows™ operating system), displaying the EMS GUI screens that provide the Customer access to system entities.

This EMS Installation & Maintenance Manual is intended for anyone responsible for installing and maintaining AudioCodes' EMS server and the server database.

Reader's Notes

2 EMS Server and Client Requirements

This section lists the platform and software required to run the EMS Standard Version.

Table 2-1: EMS- Minimal Platform Requirements

Resource	EMS Server		EMS Client
	Solaris OS	Linux OS	
Hardware	<ul style="list-style-type: none"> • Sun™ Fire™ V240 • Sun™ Fire™ V215 • Sun™ Netra™ T2000 	HP DL360 G6	
Operating System	Solaris™ 64-bit, version 10	Linux CentOS 64-bit, kernel version 5.3	Windows™ / 2000 / XP / 2003 / Vista
Memory	1 GB RAM	2 GB RAM	512 MB RAM
Disk space	73 GB	146 GB	300 MB
Processor	UltraSPARC IIIi 1-1.5 GHz	Intel Xeon E5504 (4M Cache, 2.00 GHz)	600 MHz Pentium III
Swap space	2 GB	4 GB	1 GB
DVD-ROM	Local		

- 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 / IPmedia 5000 / 8000 Online Software Upgrade
 - The working space requirements on the EMS server are as follows:
 - Solaris; Executable tcsh and X Server and Window Manager
 - Linux; Executable bash
 - The EMS server works with the JDK version 1.6 (JDK 1.6 for Solaris™, 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.

Reader's Notes

3 EMS Software Delivery – DVD

The following two DVDs are provided for each Operating System:

1. Operating System DVD for Solaris or Linux:

- Solaris 10 Installation for EMS server, Solaris 10 11/06 REV6
 - Linux (CentOS) 5.3 Installation for EMS server, Linux CentOS 5.3 REV3
- The EMS Operating System DVD is based on an image of the Operating system according to a specific machine, therefore when you order the EMS server DVD, you must specify on which machine type you are working. The following machines are currently supported:
- Sun Fire V215, V240 - Solaris 10 Installation for EMS server, Solaris 10 11/06 REV 6
 - Netra T2000 - Solaris 10 Installation for EMS server, Solaris 10 11/06 REV 6
 - HP DL360 G6 - Linux (CentOS) 5.3 Installation for EMS server, Linux CentOS 5.3 REV3

2. SW Installation and Documentation DVD for Solaris or Linux:

The DVD 'SW Installation & 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, and 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.
- EmsServerInstall – EMS server software, to be installed on the dedicated Solaris 10 or Linux 5.3 based EMS server machine.
- Oracle Database Installation for the Solaris or the Linux platform respectively.

Reader's Notes

4 EMS Server Installation Requirements

Before commencing the EMS server installation procedure, verify that your system meets the hardware, disk space, operating system and other requirements. This is necessary for the installation to succeed.

4.1 Hardware Requirements

- Operating System – the Solaris or Linux Operating Systems are supported. To determine the system OS, enter the following command:

```
uname
```

This command returns **SunOS** or **Linux**. Depending on the relevant Operating System, proceed to either Testing Hardware Requirements on Solaris OS or Testing Hardware Requirements on Linux OS.

4.1.1 Testing Hardware Requirements on the Solaris Platform

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

- **RAM** - A minimum of 1 GB is required
To determine the amount of random access memory installed on your system, enter the following command:

```
prtdiag | grep "Memory size"
```

- **Swap Space** - Disk space of 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:

```
df -h | grep -i swap | grep "tmp" | awk '{print $2}'
```

- **Disk Space** – A minimum of 73 GB (on the same disk or under RAID - Redundant Arrays of Independent Disks)
To determine the amount of disk space of your system, enter the following command:

```
iostat -En | grep "Size" | head -1
```

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

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

```
EMS-Server39:/ [root] => tcsh
EMS-Server39:/ [root] => uname
SunOS
EMS-Server39:/ [root] => prtdiag | grep "Memory size"
Memory size: 1GB
EMS-Server39:/ [root] => df -h | grep -i swap | grep "tmp" | awk '{print $2}'
4.1G
EMS-Server39:/ [root] => iostat -En | grep "Size" | head -1
Size: 73.40GB <73400057056 bytes>
EMS-Server39:/ [root] =>
```



Note: Use AudioCodes' DVD to install the Solaris 10 operating system (refer to Section 5 on Installing Solaris 10 from AudioCodes' DVD on page 21.

4.1.2 Testing Hardware Requirements on the Linux Platform

To ensure that your machine answers 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 73 GB (on the same disk or under RAID - Redundant Arrays of Independent Disks)

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.

```
[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' DVD to install the Linux Operating System.

Reader's Notes

5 Installing the EMS Server on the Solaris Platform

This section describes how to install the EMS server on the Solaris 10 platform.

5.1 Installing the Solaris 10 OS from the AudioCodes DVD

Note: the estimated time for this step is 30 minutes.

➤ To install the Solaris 10 OS from the AudioCodes DVD:

1. This section describes how to install the Solaris 10 Operating System from the AudioCodes DVD on an EMS server Solaris-based Machine. Insert the DVD labeled 'Solaris 10 for EMS' into the DVD ROM.
2. Connect the server via the serial port with a terminal application and login with **root** user.
3. Send a break in order to change into ok mode (Usually Alt+b).
4. Type: 'boot cdrom' and press **<Enter>**.
5. Wait for installation completion.
6. Reboot your machine if it doesn't reboot automatically.
7. Login as root user with *root* password.
8. Type: 'network-config' and press **<Enter>**.
9. The Current configuration will be shown. You will be prompt to change configuration, press **Y**.
10. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.
11. Confirm the changes by pressing **Y**.
12. You will be prompt to reboot, press **Y**.

5.2 Installing the EMS Server on the Solaris Platform

This section describes how to install the EMS server components on the Solaris 10 platform. Estimated installation time is 60 minutes.



Important: Don't install the EMS server on the Solaris platform via the RS-232 serial port.

➤ To install the EMS server:

1. Insert the DVD labeled 'SW Installation and Documentation' into the DVD ROM.
2. Log into the server as **acems** user with password *acems*.
3. Run the installation script **install** from its location:
Under EmsServerInstall:

```
> cd /cdrom/cdrom0/EmsServerInstall/
> ./install
```

4. You will be prompted for the user *root* password. Provide *root* password when required.
5. Press **Y** and **<Enter>** to accept License Agreement.
6. Provide **root** password and press **<Enter>**.
7. Accept the License Agreement by pressing '**y**' and **<Enter>**.
8. Press **<Enter>** to continue at the end of Java installation.
9. Accept the License Agreement by pressing '**y**' and **<Enter>**.
10. Press **<Enter>** to continue at the end of installation.
11. After System Checks have completed, press **<Enter>** to continue.

Figure 5-1: Finish system checks

```

----> SUNwils OK
----> SUNwi15cs OK
----> SUNwxfnt OK
Finish executing CheckPatches script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckJavaVersion script at Wed Nov 4 21:27:27 IST 2009
Java Version OK (java full version "1.6.0_06-b02")
Finish executing CheckJavaVersion script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckPhyMemory script at Wed Nov 4 21:27:27 IST 2009
Physical Memory OK (1024 M)
Finish executing CheckPhyMemory script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckTmpFileSystem script at Wed Nov 4 21:27:27 IST 2009
/tmp Size OK (3394M)
Finish executing CheckTmpFileSystem script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckGroup script at Wed Nov 4 21:27:27 IST 2009
Group Check OK (dba)
Finish executing CheckGroup script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckUser script at Wed Nov 4 21:27:27 IST 2009
User Check OK (acems)
Finish executing CheckUser script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckUmask script at Wed Nov 4 21:27:27 IST 2009
UMASK Check OK (0022)
Finish executing CheckUmask script at Wed Nov 4 21:27:27 IST 2009
Start executing CheckCurrentShellSettings script at Wed Nov 4 21:27:27 IST 2009
Shell File OK (.cshrc)
Finish executing CheckCurrentShellSettings script at Wed Nov 4 21:27:27 IST 2009
Press ENTER to continue...
    
```

12. When you prompted for Oracle installation directory press **<Enter>**.
13. When you prompted for Database directory press **<Enter>**.
14. Press **<Enter>** to continue.
15. Press **<Enter>** to continue after ORACLE Variables Verification.

Figure 5-2: Orahome and Oradata directories

```

Pre-Install Requirements Check
=====
ORACLE Variables Verification
=====
Start executing CheckOracleHomeVariables script at Wed Nov 4 21:28:20 IST 2009
ORACLE_BASE Exists?           OK (/ACEMS)
ORACLE_BASE User Ownership    OK (acems)
ORACLE_BASE Group Ownership   OK (dba)
Enter the path of the location in which you will be installing Oracle (ORACLE_HOME)
Default: /ACEMS/orahome
-->
Oracle Home Exist?            OK (/ACEMS/orahome NOT Exist and will be created)
Oracle Home User Ownership    OK (acems)
Oracle Home Group Ownership   OK (dba)
Oracle Home Free Space        OK (54858M)
Finish executing CheckOracleHomeVariables script at Wed Nov 4 21:28:25 IST 2009

Enter the path of the location in which you will be installing the Database
Default: /ACEMS/oradata
-->
DB Install Path Exist?        OK (/ACEMS/oradata NOT Exists and will be created)
Database User Ownership       OK (acems)
Database Group Ownership      OK (dba)
Database Free Space           OK (54858M)

Press ENTER to continue...

```

16. When you prompted for EMS Software directory press **<Enter>**.

Figure 5-3: EMS software directory

```

=====
All Checks Completed Successfully
=====

EMS Software Installation
=====
EMS Variables Verification
=====
Start executing StartEMSInstall script at Wed Nov 4 21:29:23 IST 2009

Enter the path of the location in which you will be installing AudioCodes EMS software
Default: /ACEMS
-->

```

17. Provide *root* password in order to run NTP Server and install Apache Server.
18. Press 'Y' and **<Enter>** when you prompted to install conflicting files.
19. Press **<Enter>** to begin Oracle Software Installation.
20. Provide *root* password.
21. Enter *root* password to run **root.sh** script.

Figure 5-4: Oracle Software Installation

```

Oracle Software Installation
=====
Press ENTER to continue...

Searching for Oracle Software Image File orahome.tar.gz
Searching for DB Backup File db-backup.tar.gz
Starting Oracle Installation. This may take 10-15 minutes.
Loading... (Press ^C to abort)
Start executing prepareInventory script at Thu Nov 5 11:25:11 IST 2009
Updating oraInventory file...
Please provide root Password:
Password:
starting oraInst.sh
Creating Oracle Inventory pointer file (/var/opt/oracle/oraInst.loc)
Creating the Oracle Inventory Directory (/ACEMS/./oraInventory)
Changing groupname of /ACEMS/./oraInventory to dba.
OK
Please Wait...
Finish executing prepareInventory script at Thu Nov 5 11:25:58 IST 2009
Copying ORACLE_HOME image files from CD...
Unzipping image file...
Untarring image file...
Registering Oracle Home...
Enter root password to run root.sh script:
Password: █
    
```

22. When you prompted for SYS password type 'sys' and then press <Enter>.
23. When prompted enter *root* password.
24. Wait for the installation to complete.
25. Reboot the server.

Figure 5-5: Installation Finish Screen

```

Please provide root Password: Password:
=====
Installation Completed Successfully
=====
Note: after successful installation, reboot is recommended,
to verify automatic startup.
=====
Finish executing Create_StartShutScripts_InEtcDir_AndChangeOratab script at Thu Nov 5 12:09:56 IST 2009
Remove Oracle demo directory: /ACEMS/orahome/xdm/Gemo/java
/ACEMS/orahome/xdm/demo/java: No such file or directory
Remove Oracle demo directory: /ACEMS/orahome/rdms/demo
Finish executing installprepFast script at Thu Nov 5 12:09:56 IST 2009
Formatting Log...
Formatting Log done.
The installation log file can be found in: /ACEMS/server_5.8.66/EmsInstall.log
=====*****=====*****
Backup schema_scripts and oracle hardening at:/ACEMS
/tmp/emsoldVersion.txt: No such file or directory
=====
Installation Completed, Oracle is Now Secured
=====
Remove /tmp/ems_path
Remove /tmp/EmsServerInstall
█
    
```


6 Installing the EMS Server on the Linux Platform

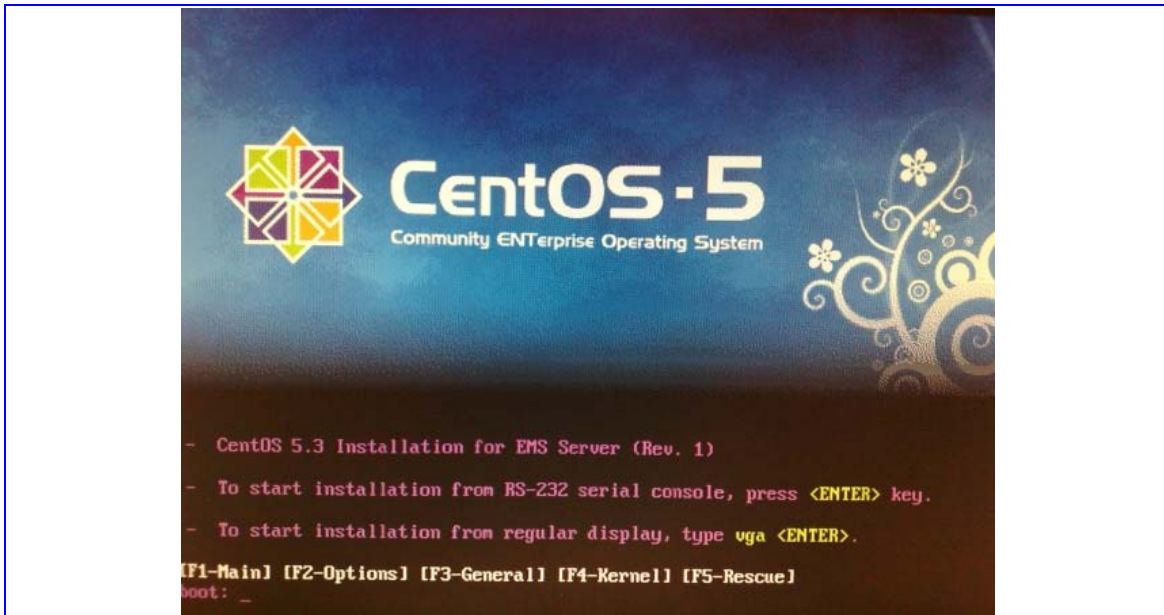
6.1 Installing Linux CentOS 5.3 from the AudioCodes DVD

This section describes how to install the Linux CentOS 5.3 (**AudioCodes EMS adapted version**) Operating System from the AudioCodes DVD on the EMS server Linux-based machine. The estimated completion time for the procedure described below is 20 minutes.

➤ To install the Linux CentOS 5.3:

1. Insert the DVD labeled 'Linux CentOS 5.3 for EMS' into the DVD ROM.
2. There are two methods to install CentOS 5.3:
 - Connect directly to server peripheral I/O devices: keyboard and display.
 - Connect the server via the serial port with a terminal application.
3. Turn the server on or reboot it.
4. Wait for the pre-installation menu to load:
 - The following installation menu is displayed when connected to a server keyboard and display. To start the installation process using this method, at the command prompt, type **vga** and press **Enter**.

Figure 6-1: CentOS.-5 Welcome screen



- The following installation menu is displayed when connected to the server via a serial port and terminal. To start the installation process using this method, press **Enter**.

```

Tera Term - COM1 VT
File Edit Setup Control Window Help
ISOLINUX 3.72 2008-09-25 Copyright (C) 1994-2008 H. Peter Anvin

- CentOS 5.3 Installation for EMS Server (Rev. 1)
- To start installation from RS-232 serial console, press <ENTER> key.
- To start installation from regular display, type vga <ENTER>.
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot:
    
```

The following steps are configured to run automatically.

5. Wait for the installation process to complete. When the installation process completes, you are prompted to reboot the server.



Important: Before performing the reboot, ensure you remove the installation DVD from the DVD ROM.

6. Reboot the server by pressing **Enter**.

```

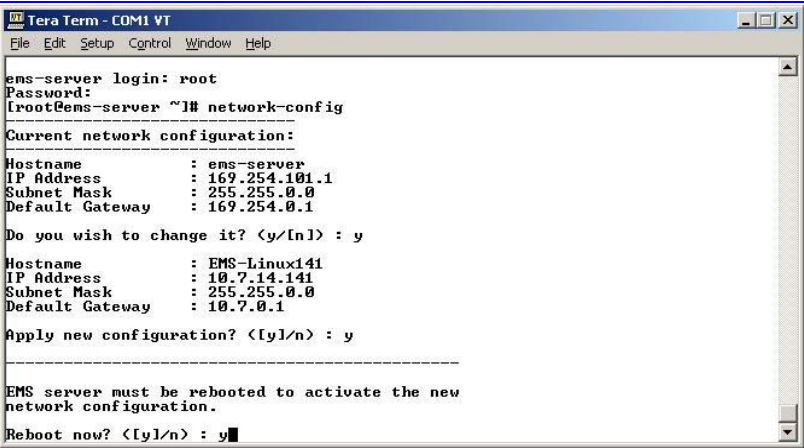
Tera Term - COM1 VT
File Edit Setup Control Window Help
Welcome to CentOS

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

<Enter> to reboot
    
```

7. After the reboot has completed, enter the system with user **root**, and password *root*.

8. Configure the server's network settings; type **network-config** and press **Enter**.



```
Tera Term - COM1 VT
File Edit Setup Control Window Help
ens-server login: root
Password:
[root@ens-server ~]# network-config
-----
Current network configuration:
-----
Hostname       : ens-server
IP Address     : 169.254.101.1
Subnet Mask    : 255.255.0.0
Default Gateway : 169.254.0.1

Do you wish to change it? <y/Inl> : y
-----
Hostname       : EMS-Linux141
IP Address     : 10.7.14.141
Subnet Mask    : 255.255.0.0
Default Gateway : 10.7.0.1

Apply new configuration? <[y]/n> : y
-----
EMS server must be rebooted to activate the new
network configuration.
Reboot now? <[y]/n> : y
```

9. To change the default configuration, type **y** and press **Enter**.
10. Define the server's Host name. Press **Enter**.
11. Define the server's IP address. Press **Enter**.
12. Define the server's Subnet Mask. Press **Enter**.
13. Define the server's Default Gateway. Press **Enter**.
14. To apply the new configuration, type **y** and press **Enter**.
15. To complete the network configuration changes, the server must be rebooted. Type **y** and press **Enter**.

6.2 Installing the EMS Server on the Linux Platform

This section describes how to install the EMS server on the Linux CentOS 5.3 (EMS adapted version) platform. Estimated installation time is 90 minutes.



Important: Don't install the EMS server on the Linux platform via the RS-232 serial port.

➤ **To install the EMS server on the Linux CentOS 5.3 (EMS adapted version), perform the following with 'acems' user:**

1. Connect the EMS server machine via the SSH client.
2. Insert the DVD labeled 'EMS Server for Linux' into the DVD ROM.
3. Run the EMS installation script by specifying the following command:

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

4. A few seconds after the start of the installation process, you are prompted to enter the *root* password to continue.

```
[acems@EMS-Linux141 ~]$ cd /misc/cd/EmsServerInstall/
[acems@EMS-Linux141 EmsServerInstall]$ ./install
```

5. *General Linux Patching*. The estimated running time for this step is 5 minutes. This step runs automatically.

Figure 6-2: General Linux Patching

```
Please provide root Password:
Password:
*****
Start General Linux Patching
Mon Aug 10 13:07:38 BST 2009
*****
29/29 - kernel-headers-2.6.18-128.1.14.el5.x86_64.rpm
Saving Primary metadata
Saving file lists metadata
Saving other metadata
CentOS-Base.repo.orig--> move to backup
CentOS-Media.repo.orig--> move to backup
>>> Install OS patches ...
>>> acpid.x86_64                               1.0.4-7.el5_3.1    ems-local    ...
>>> apr-util.x86_64                             1.2.7-7.el5_3.1    ems-local    ...
>>> curl.x86_64                                 7.15.5-2.1.el5_3.4 ems-local    ...
```

6. *Linux OS Hardening*. This step is performed for the purposes of compliance with DoD STIG. After the *General Linux Patching* step has completed, you will be prompted to change *acems* and *root* passwords.



Important: By default, the minimum acceptable OS user password length is 9 characters. Enter this password to continue the installation.

```
*****
Finishing General Linux Patching
Mon Aug 10 13:08:25 BST 2009
*****
>>> Harden Linux OS for DoD STIG compliancy ...
>> Please change user acems password
Changing password for user acems.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
>> Please change user root password
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

7. After the Linux OS Hardening step has completed, you will be prompted to press **Enter** to reboot the EMS server machine.

```
passwd: all authentication tokens updated successfully.
/root
Press ENTER to Reboot...\c
```

8. When the EMS server machine reboots, perform the following steps to continue the installation process:
 - Connect the server machine via the SSH client.
 - Run the EMS installation script by specifying the following with **acems** user:

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

9. *Software License Agreement.* Type **y** and press **Enter** to continue.

Figure 6-3: Linux License Agreement

```
[acems@EMS-Linux141 ~]$ cd /misc/cd/EmsServerInstall/
[acems@EMS-Linux141 EmsServerInstall]$ ./install
```

```
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
```

10. Copying *Install Scripts*. This estimated running time for this step is 2-3 minutes. This step runs automatically. When this step has completed, you will be prompted to enter the **root** password to continue.

```
Copying Install Scripts to /tmp/EmsServerInstall...

Applying Java 1.6.0_10 Patch
Please provide root Password:
Password: █
```

11. *Software License Agreement for Java JDK.* Read carefully through the agreement by pressing the Space button, type **y** and press **Enter** to continue.

Figure 6-4: Linux JDK Software License Agreement

```
FOR INQUIRIES PLEASE CONTACT: SUN MICROSYSTEMS, INC.,
Network Circle, Santa Clara, California 95054, U.S.A.

Do you agree to the above license terms? [yes or no]
y█

Please provide root Password:
Password:
Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA SE DEVELOPMENT KIT (JDK), VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE
SOFTWARE IDENTIFIED BELOW TO YOU ONLY FROM THE CONDITION
```

12. *Java JDK Installation.* The estimated running time for this step is a few seconds. This step runs automatically. When this step has completed, you will be prompted to press **Enter** to continue.

```
Do you agree to the above license terms? [yes or no]
y
Unpacking...
Checksumming...
Extracting...
UnZipSFX 5.50 of 17 February 2002, by Info-ZIP (Zip-Bugs@lists.wku.edu).
  inflating: jdk-6u10-linux-amd64.rpm
  inflating: sun-javadb-common-10.4.1-3.1.i386.rpm
  inflating: sun-javadb-core-10.4.1-3.1.i386.rpm
  inflating: sun-javadb-client-10.4.1-3.1.i386.rpm
  inflating: sun-javadb-demo-10.4.1-3.1.i386.rpm
  inflating: sun-javadb-docs-10.4.1-3.1.i386.rpm
  inflating: sun-javadb-javadoc-10.4.1-3.1.i386.rpm
Preparing...
 1:jdk
Unpacking JAR files...
  rt.jar...
  jsse.jar...

For more information on how Java registration works and
how it is managed and used, see:
http://java.sun.com/javase/registration/JDKRegistrationPrivacy.html

Press Enter to continue.....
█
```

13. *Pre-Install Requirements Check.* This estimated running time for this step is a few seconds. This step runs automatically. When this step has completed, you will be prompted to enter the *root* password to continue.

Figure 6-5: Linux Pre-installation Requirements Check

```

Pre-Install Requirements Check
=====
SYSTEM CHECKS
=====
Start executing GetPhysicalMemory script at Mon Aug 10 17:34:46 BST 2009
Finish executing GetPhysicalMemory script at Mon Aug 10 17:34:46 BST 2009
Start executing GetSwap script at Mon Aug 10 17:34:46 BST 2009
Finish executing GetSwap script at Mon Aug 10 17:34:46 BST 2009
Start executing GetTemp script at Mon Aug 10 17:34:46 BST 2009
Finish executing GetTemp script at Mon Aug 10 17:34:46 BST 2009
Start executing CheckTcpIpDefinitions script at Mon Aug 10 17:34:46 BST 2009
Tcp/Ip Def.      OK (10.7.14.141)
Finish executing CheckTcpIpDefinitions script at Mon Aug 10 17:34:46 BST 2009
Start executing CheckOSVersion script at Mon Aug 10 17:34:46 BST 2009
OS Platform      OK (Linux)
Redhat Release   OK
Finish executing CheckOSVersion script at Mon Aug 10 17:34:46 BST 2009
Start executing CheckPatches script at Mon Aug 10 17:34:46 BST 2009
Patch  ---->  compat-libstdc++-33-x86_64      OK
          ---->  compat-libstdc++-33-i386      OK
          ---->  elfutils-libelf-devel-x86_64    OK
          ---->  libgomp-x86_64              OK
          ---->  gcc-x86_64                OK
          ---->  libstdc++-devel-x86_64        OK
Start executing CheckCurrentShellSettings script at Mon Aug 10 17:35:00 BST 2009
Shell File      OK (.bash profile)
Finish executing CheckCurrentShellSettings script at Mon Aug 10 17:35:00 BST 2009
Enter root password to check Kernel parameters and disable antivirus:
Password: █

```

14. *Linux Kernel Verification.* This estimated running time for this step is a few seconds. This step runs automatically. When this step has completed, you will be prompted to press **Enter** to continue.

Figure 6-6: Linux Kernel Verification

```

Start executing GetKernelParam script at Mon Aug 10 17:37:45 BST 2009
Linux Kernel Verification
=====
Checking required Kernel parameters for minimum values needed

Preparing a Kernel Parameters report. Please wait...
Finish executing GetKernelParam script at Mon Aug 10 17:37:46 BST 2009
Checking SEMMSL:      OK
Checking SEMMNS:     OK
Checking SEMOPM:     OK
Checking SEMMNI:     OK
Checking SHMALL:     OK
Checking SHMMNI:     OK
Checking FILE_MAX:   OK
Checking IP_LOCAL_PORT_RANGE (min):  OK
Checking IP_LOCAL_PORT_RANGE (max):  OK
Checking RMEM_DEFAULT: OK
Checking RMEM_MAX:   OK
Checking WMEM_DEFAULT: OK
Checking WMEM_MAX:   OK

All kernel parameters were set correctly
Finish executing CheckKernelParam script at Mon Aug 10 17:37:46 BST 2009

Press ENTER to continue... █

```

15. *ORACLE Variables Verification.* This estimated running time for this step is a few seconds. This step runs automatically. When this step has completed, you will be prompted to enter several parameters in reference to the Oracle DB installation:

- The path of the location in which you will be installing the Oracle Application. If you *don't* wish to change the default location, press **Enter**.

Figure 6-7: Linux-ORACLE Variables Verification

```

Pre-Install Requirements Check
-----
ORACLE Variables Verification
-----
Start executing CheckOracleHomeVariables script at Mon Aug 10 17:40:30 BST 2009
ORACLE_BASE Exists?      OK (/ACEMS/oracle did not Exist and was created)
ORACLE_BASE User Ownership  OK (acems)
ORACLE_BASE Group Ownership OK (dba)
Enter the path of the location in which you will be installing Oracle (ORACLE_HOME)
Default: /ACEMS/oracle/orahome
-->
    
```

- The path of the location where you wish to install the Oracle Database. If you *don't* wish to change the default location, press **Enter**.

```

Oracle Home Exist?      OK (/ACEMS/oracle/orahome NOT Exist and will be created)
Oracle Home User Ownership  OK (acems)
Oracle Home Group Ownership OK (dba)
Oracle Home Free Space     OK (31304M)
Finish executing CheckOracleHomeVariables script at Mon Aug 10 17:44:30 BST 2009

Enter the path of the location in which you will be installing the Database
Default: /ACEMS/oracle/oradata
-->
    
```

- The last two steps of the Oracle pre-install settings display a summary of all parameters to be configured during the installation. Press **Enter** twice to start the installation process.

```

DB Install Path Exist?      OK (/ACEMS/oracle/oradata NOT Exists and will be created)
Database User Ownership     OK (acems)
Database Group Ownership    OK (dba)
Database Free Space         OK (31304M)

Press ENTER to continue...
    
```

```

ORACLE Variables Verification
-----
Checking for the following environment variables in your .bash profile file

Variable      Value Required      Value Presently Defined
-----
PATH          /ACEMS/oracle/orahome/bin      Defined correctly
ORACLE_SID    dbems                    dbems
NLS_LANG      AMERICAN_AMERICA.UTF8        AMERICAN_AMERICA.UTF8
DISPLAY      :
-----
Info: All Oracle Variables are defined OK
Press ENTER to continue...
    
```

16. *EMS Variables Verification.* This estimated running time for this step is a few seconds. This step runs automatically. When this step has completed, you will be prompted to provide the path of the location where you wish to install the AudioCodes EMS software. If you *don't* wish to change the default location, press **Enter**.

Figure 6-8: Linux-EMS Variables Verification

```

=====
All Checks Completed Successfully
=====

EMS Software Installation

EMS Variables Verification
=====
Start executing StartEMSInstall script at Mon Aug 10 17:59:53 BST 2009

Enter the path of the location in which you will be installing AudioCodes EMS software
Default: /ACEMS
--> █

```

17. *Copying of EMS Software files.* The estimated running time for this step is 2-3 minutes. This step runs automatically. When this step has completed, you will be prompted to enter the *root* password to continue.

```

Copy EMS Software files...

chtext: change 'CUR_LOCATION' to '/ACEMS/server_5.8.55'
chtext: /ACEMS/server_5.8.55/watchDog_unix
chtext: change 'CUR_LOCATION' to '/ACEMS/server_5.8.55'
chtext: /ACEMS/server_5.8.55/runServer_unix

EMS files copied OK

In order to run NTP Server and install Apache Server,
root permissions are required.
Please provide root Password:
Password: █

```

18. *Installing the EMS Server Software.* This estimated running time for this step is 2-3 minutes. This step runs automatically. When this step has completed, a message is displayed informing you of the commencement of the Oracle Software Installation step. Press **Enter** to continue.

Figure 6-9: Linux-Installing EMS Software

```

NTP Server OK
Apache Server OK

Finish executing StartEMSInstall script at Mon Aug 10 18:07:43 BST 2009

Oracle Software Installation
=====
Press ENTER to continue... █

```

6.2.1 Oracle Software Installation

➤ To install the Oracle Software on the Linux platform:

1. Immediately after starting the Oracle Software Installation step, the ORACLE image will be copied from the installation DVD. At the end of the process you will be prompted for *root* user's password. Enter *root* and then press **ENTER**.

Figure 6-10: Linux-Oracle Software Installation

```

Oracle Software Installation
=====
Press ENTER to continue...

Searching for Oracle Software Image File orahome.tar.gz
Searching for DB Backup File db-backup.tar.gz
Starting Oracle Installation. This may take 10-15 minutes.
Loading... (Press ^C to abort)
Start executing prepareInventory script at Wed Nov 11 14:17:37 GMT 2009
OK
Please Wait...
Finish executing prepareInventory script at Wed Nov 11 14:17:37 GMT 2009
Copying ORACLE_HOME image files from CD...
Unzipping image file...
Untarring image file...
Registering Oracle Home...
Enter root password to run root.sh script:
Password:
    
```

2. Continuation of step *Oracle Software Installation*. When this step has completed, you will be prompted to enter *root* password in order to run **root.sh** script. Enter *root* password and then press **ENTER**.
3. After entering the *root* password, the installation continues restoring ORACLE from the DVD. At the end of this step, you will be prompted to enter **sys** user's password. Type **sys** and then press **ENTER**.
4. At the end of this step you will be prompted to enter *root* password in order to complete the installation. Enter *root* password and then press **ENTER**.

Figure 6-11: Linux-Installation Completed Successfully

```

Please provide root Password:
=====
Installation Completed Successfully

Note: after successful installation, reboot is recommended,
to verify automatic startup.
=====
Finish executing Create_StartShutScripts_InEtcDir_AndChangeOratab script at Wed Nov 11 14:50:55 GMT 2009
Finish executing installprepFast script at Wed Nov 11 14:50:55 GMT 2009

Formatting Log...
Formatting Log done.
The installation log file can be found in: /ACEMS/server_5.8.66//EmsInstall.log

=====*=====*=====*=====*=====
Installation Completed, Oracle is Now Secured
=====
Remove /tmp/ems_path
Remove /tmp/EmsServerInstall
    
```

5. When the installation process has completed, reboot the EMS server machine by specifying the following commands:

```

su - root
**** //Provide root password.
reboot
    
```

7 Upgrading the EMS Server

**Important:**

Before you start the upgrade process, back up the current database and save the DMP file on a separate hardware device (refer to Backup the EMS Server on page 81).

7.1 Major Version Upgrade

Due to the significant modification of the Database, the major version upgrade is not supported. All customers with the Solaris server installed with one of the previous versions, should perform disk format, re-install Solaris and then follow the Installation Guide.

For the Linux OS, a major version upgrade is not applicable as this is the first version when this Operating System is supported.

Prior to starting the version 5.8 Installation process, refer to the site preparation procedure in Appendix B – Site Preparation Prior to Upgrade.

7.2 Minor Version Upgrade

A minor version upgrade of the EMS is from 5.8 version only. You can perform the minor version upgrade using one of the following methods:

- Upgrade from the AudioCodes supplied DVD
- Upgrade from the AudioCodes supplied TAR file

7.2.1 Upgrading from the Installation DVD

This section describes how to upgrade from the AudioCodes supplied installation DVD.

➤ **To upgrade the EMS server from the installation DVD, take the following steps:**

1. Login to the EMS server as **acems** user with password 'acems'.

```
EMS-Server:/ [root] => su - acems
Password: *****
```

2. Insert the DVD with the EMS installation kit into the server DVD-reader and specify the following commands to verify device availability.

```
> cd /cdrom/cdrom0/EmsServerInstall/
> ls -lt
```

```

>
>
> cd /cdrom/cdrom0/EmsServerInstall/
> ls -lt
total 492
drwxr-xr-x  2 root    other    16384 May 31 13:57 SolarisSecurity
drwxr-xr-x  2 root    root      2048 May 31 13:53 Java
-rwxr-xr-x  1 root    other      49 May 27 18:10 start_agent
-rwxr-xr-x  1 root    other    3110 May 27 18:10 StartDbca
-rwxr-xr-x  1 root    other    8696 May 27 18:10 StartEMSInstall
-rwxr-xr-x  1 root    other      47 May 27 18:10 start_listener
-rwxr-xr-x  1 root    other     323 May 27 18:10 StartNetca
-rwxr-xr-x  1 root    other   2383 May 27 18:10 StartOPatchApply
-rwxr-xr-x  1 root    other   2538 May 27 18:10 StartOPatchInstall
-rwxr-xr-x  1 root    other     447 May 27 18:10 StartOracleInstall
-rwxr-xr-x  1 root    other   2231 May 27 18:10 StartPatchInstaller
-rwxr-xr-x  1 root    other   2310 May 27 18:10 StartRunInstaller
-rwxr-xr-x  1 root    other   1457 May 27 18:10 StartSchemaScripts
-rwxr-xr-x  1 root    other     508 May 27 18:10 test
-rwxr-xr-x  1 root    other   1896 May 27 18:10 values.install
-rwxr-xr-x  1 root    other   3739 May 27 18:10 versionUpgradeMap.txt
drwxr-xr-x  5 root    other    2048 May 27 18:10 OPatch
drwxr-xr-x  2 root    other    6144 May 27 18:10 oracle_hardening
-rwxr-xr-x  1 root    other    5434 May 27 18:10 oracleUpgrade 3 2
    
```

3. Run the script **install** from its location (under EmsServerInstall - not with a full path).

```

> cd /cdrom/cdrom0/EmsServerInstall/
> ./install
    
```

The installation script automatically stops the EMS server.

```

>
> cd /cdrom/cdrom0/EmsServerInstall/
> ./install
Stopping The EMS Server
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
"PRODUCT"). THE PRODUCT CONTAINS PROPRIETARY TECHNOLOGY
(PROTECTED BY, AMONGST OTHER THINGS, PATENT AND COPYRIGHT
LAWS), AND IS LICENSED (NOT SOLD). BY OPENING THE PACKAGE
CONTAINING THE PRODUCT OR INSTALLING THE PROGRAM, YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS SOFTWARE EVALUATION
AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF
    
```

- Enter **Y** to confirm the Software License Agreement and press **Enter** to continue the installation process.

```

terms of this License Agreement shall remain in full force and effect.

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

```

- Enter the *root* password to stop the EMS server and press **Enter** to continue.

```

Copying Install Scripts to /tmp/EmsServerInstall...

Stopping the server, please provide root's password
Password:

```

- The 'Pre-install requirements check' is run automatically. At the end of this process, you will be prompted to press **Enter** to continue.

```

EMS SW IS DOWN
Start executing CheckCurrentShellSettings script at Mon Jun 1 12:03:43 IDT 2009
Shell File (.cshrc)
Finish executing CheckCurrentShellSettings script at Mon Jun 1 12:03:43 IDT 2009
Checking for the following environment variables in your .cshrc file

Variable      Value Required      Value Presently Defined
-----
PATH          /ACEMS/orahome/bin  Defined correctly
ORACLE_SID    dbems               dbems
NLS_LANG      AMERICAN_AMERICA.UTF8 AMERICAN_AMERICA.UTF8
DISPLAY       :                   10.6.1.9:1.0
-----
Info: All Oracle Variables are defined
Press ENTER to continue...

```

- Enter the path of the location where you wish to install the AudioCodes EMS software.
Default: /ACEMS (recommended). If you wish to use the default path, press **Enter** to continue.

```

=====
All Checks Completed Successfully
=====

                                EMS Software Upgrade
                                =====

EMS Upgrade Verification

                                EMS Software Installation
                                =====

EMS Variables Verification

Start executing StartEMSInstall script at Mon Jun 1 12:07:38 IDT 2009
Enter the path of the location in which you will be installing AudioCodes EMS software
Default: /ACEMS
--> █
    
```

8. The EMS software files are copied to the location '/tmp/EmsServerInstall'. At the end of this process, you will be prompted to provide the *root* password. Enter 'root' and press **Enter** to continue.

```

chtext: /tmp/EmsServerInstall/CheckNTPatches
chtext: change 'INSTALL_BASE' to '/tmp/EmsServerInstall'
chtext: /tmp/EmsServerInstall/CheckNSS
chtext: change 'EMS_LOCATION' to '/ACEMS/server_5.8.44'
chtext: /tmp/EmsServerInstall/CheckNSS
Copy EMS Server configuration ...

EMS files copied      OK

In order to run NTP Server and install Apache Server,
root permissions are required.
Please provide root Password:
Password: █
    
```

9. The following screen appears as a notification of a successful installation process:

```

=====
deleting library /ACEMS/schema_scripts
deleting library /ACEMS/oracle_hardening
Backup schema_scripts and oracle_hardening at:/ACEMS

=====
Installation Completed, Oracle is Now Secured
=====

Remove /tmp/ems_path
Remove /tmp/EmsServerInstall
>
<
    
```

10. Specify the following commands to reboot the EMS server in order to complete the installation process:
 - Switch user to **root**, enter password *root*.
 - Enter **reboot** command and press **Enter**.

```
-> su -  
Password: *****  
EMS-Server:/ [root] => reboot
```

```
>  
> su -  
Password:  
Sun Microsystems Inc. SunOS 5.10 Generic January 2005  
# tcsh  
EMS-Server21:/ [root] => reboot
```

11. When the server loads back after the reboot, verify that all relevant processes are 'Up'. You can perform this check using the 'Ems Server Manager' tool **General Info** option (see General Info on page 47).

```
EMS Watchdog is UP  
EMS Server Process is UP  
EMS Security Status: Not Secured  
Apache Server Status: Up  
Apache Version:  
Server version: Apache/2.2.6 (Unix)  
Server built: Nov 29 2007 04:35:15  
  
Oracle Server Processes Status:  
DB Processes are UP  
Oracle listener is UP  
# of DB Connections: 50
```

7.2.2 Upgrading from the Installation TAR file

This section describes how to upgrade from the AudioCodes supplied installation TAR file.

➤ **To upgrade from the Installation TAR file, take the following steps:**

1. Log into the EMS server as **acems** user with password *acems*:

```
EMS-Server:/ [root] => su - acems
Password: *****
```

2. Copy the installation TAR file (**emsServerDeploy_5.8.xx.tar**) into the /ACEMS folder.
3. If the previous installation or upgrade was performed from the installation TAR file, then remove the folder /ACEMS/EmsServerInstall by specifying the following command:

```
> cd /ACEMS
> rm -Rf EmsServerInstall
```

4. Open the installation TAR file by specifying the following command:

```
> tar -xvf emsServerDeploy_5.8.xx.tar
```

5. When the installation TAR file has opened successfully, the new folder /ACEMS/EmsServerInstall must appear at the command prompt.
6. Remove the installation TAR file by specifying the following command:

```
> cd /ACEMS
> rm emsServerDeploy_5.8.xx.tar
```


7. If the new minor EMS version requires a Java SDK version upgrade (see the relevant notification in the Version Description Document (VDD)), then perform the following:
 - Into folder /ACEMS/EmsServerInstall, create the folder **Java** by specifying the following command:

```
> cd /ACEMS/EmsServerInstall
> mkdir Java
```

- Copy the relevant Java files kit (previously downloaded from FTP) to the newly created folder.

```
> cd /ACEMS/EmsServerInstall/Java/
> ls -lt
total 201076
-rw-r--r--  1 acems  dba      257580 May 31 10:29 tzupdater.jar
-rw-r--r--  1 acems  dba        378 May 31 10:29 StartJavaUpgrade.sh
-rw-r--r--  1 acems  dba    15951256 May 31 10:29 jre-6u6-windows-i586-p-s.exe
-rw-r--r--  1 acems  dba    11273070 May 31 10:29 jdk-6u6-solaris-sparcv9.sh
-rw-r--r--  1 acems  dba    75369884 May 31 10:29 jdk-6u6-solaris-sparc.sh
-rw-r--r--  1 acems  dba      1017 May 31 10:29 JavaInstaller.pl
>
```

8. Proceed to step 3 (Run the installation script) in procedure Upgrading from the Installation DVD above. This part is identical for both upgrade methods.

Reader's Notes

8 EMS Server Machine Maintenance

The EMS server Management utility is used to perform actions on the EMS server such as basic and advanced configuration, System activation/deactivation and System maintenance and debugging.



Important:

All available actions in the EMS Server Management utility must be performed using this utility and not directly from a Solaris or Linux OS shell. If you have previously performed the available EMS Server Management utility actions directly from Solaris or Linux OS shells, then you cannot use this utility.

To exit EMS Server Manager to Solaris or Linux OS shell level press **99**.

The EMS Server Management menu opens automatically when you login to EMS server via telnet. If it does not open automatically, run the following command:

```
# EmsServerManager
```

The Management menu options different according to the user OS, permissions and telnet connection types as described below:

User **acems** : For **acems** user, the menu will be displayed as in Figure 8-1 (regardless of the telnet connection type (secured shell (SSH) or non secured)).

Figure 8-1: ACEMS menu

```

EMS Server 5.8.63 Management

1 ) General Info
2 ) Collect Logs

Maintenance:
3 ) Backup the EMS Server
4 ) Schedule Backup for the EMS Server

Additional Tasks:
5 ) Additional Management Tasks (Root password is required)

e ) Exit to OS terminal
q ) Quit
: █

```

User **root**: Connect to the server as **acems**, using Secure Shell (ssh); switch user to root (su root) and enter the *root* password (run 'su' without hyphen ("-")).

The root menu differs according to the telnet connection types. If you have connected to the EMS server using secured shell (SSH), the full menu is displayed with hardening options added such as Basic Hardening, Advanced Hardening and Oracle Hardening.

Figure 8-2: EmsServerManager Menu (All SSH options – Solaris)

```

    EMS Server 5.8.63 Management

    1 ) General Info
    2 ) Collect Logs

    Networking:
    3 ) Change Server's IP Address    (Reboot is performed)
    4 ) Configure Ethernet Interfaces (Reboot is performed)
    5 ) Configure Ethernet Redundancy (Reboot is performed)
    6 ) Configure DNS Client
    7 ) Configure Static Routes
    8 ) Configure SNMP Agent
    9 ) Configure NAT

    Security:
    10 ) Basic Hardening    (Reboot is performed)
    11 ) Advanced Hardening (Reboot is performed)
    12 ) SSL Tunneling Configuration
    13 ) Change DBA Password (EMS Server will be shut down)
    14 ) OS Passwords Settings
    15 ) Add EMS User
    16 ) Start/Stop File Integrity Checker

    Maintenance:
    17 ) Configure NTP
    18 ) Change System Timezone (Reboot is performed)
    19 ) Change System Time & Date
    20 ) Start/Stop EMS Server
    21 ) Web Server Configuration
    22 ) Enable/Disable Jumpstart Services
    23 ) Backup the EMS Server
    24 ) Schedule Backup for the EMS Server
    25 ) Restore the EMS Server
    26 ) Reboot the EMS Server

    q ) Quit
    : █
    
```

Figure 8-3: EmsServerManager Menu (All options – Linux)

```

EMS Server 5.8.63 Management

1 ) General Info
2 ) Collect Logs

Networking:
3 ) Change Server's IP Address    (Reboot is performed)
4 ) Configure Ethernet Interfaces (Reboot is performed)
5 ) Configure Ethernet Redundancy (Reboot is performed)
6 ) Configure DNS Client
7 ) Configure Static Routes
8 ) Configure SNMP Agent
9 ) Configure NAT

Security:
10 ) Change DBA Password    (EMS Server will be shut down)
11 ) OS Passwords Settings
12 ) Add EMS User
13 ) Start/Stop File Integrity Checker

Maintenance:
14 ) Configure NTP
15 ) Change System Timezone
16 ) Change System Time & Date
17 ) Start/Stop EMS Server
18 ) Web Server Configuration
19 ) Backup the EMS Server
20 ) Schedule Backup for the EMS Server
21 ) Restore the EMS Server
22 ) Reboot the EMS Server
23 ) HA Configuration

q ) Quit
: █

```

**Important:**

1. Whenever prompted to enter **Host Name** please provide only letters. Numbers and hyphen spaces are not allowed in Host Names.
2. Ensure IP addresses contain all correct digits.
3. For Menu options where reboot is required, the server will reboot itself automatically after changes confirmation.
4. 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** will cancel the changes and return you to the initial prompt for the selected menu option, **Quit** returns to the previous menu.

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

- [General Info and Logs collection](#) – These options provide the general EMS server current information from the Solaris operating system, including EMS Version, EMS Server Process Status, Oracle Server Status, Apache Server Status, Java Version, Memory size and Time Zone. Also the log collector collates all important logs into a single compressed file.
 - General Info
 - Collect Logs
- [Networking](#) – These options provide all basic, advanced network management and interface changes.

Networking menu:

 - Change Server's IP Address (Reboot is performed)
 - Configure Ethernet Interfaces (Reboot is performed)
 - Configure Ethernet Redundancy (Reboot is performed)
 - Configure DNS Client
 - Configure Static Routes
 - Configure SNMP Agent
 - Configure NAT
- [Security](#) – These options manage all the relevant security configurations.

Security full menu:

 - Basic Hardening (only with SSH connection, reboot is performed).
 - Advanced Hardening (only with SSH connection, reboot is performed).
 - SSL Tunneling Configuration (only with SSH connection)
 - Change DBA Password (EMS Server will be shut down)
 - OS Passwords Settings
 - Add EMS User
 - Start/Stop File integrity checker
- [Maintenance](#) – These options manage all System Maintenance actions.

Maintenance menu:

 - Configure NTP
 - Change System Timezone (Reboot is performed)
 - Change System Time & Date
 - Start / Stop the EMS Server
 - Web Server Configuration
 - Backup the EMS Server
 - Schedule Backup for the EMS Server
 - Restore the EMS Server
 - Reboot the EMS Server
 - HA Configuration
 - Quit

8.1 General Info and Logs Collection

This section describes the General Information and Logs collection options.

8.1.1 General Info

The **General Info** provides detailed information about the EMS server configuration and current status variables. The following information is provided:

- Components Versions: EMS, Solaris, Java, Apache
- Components Statuses: EMS Server process and security, Watchdog, Apache, Oracle, SNMP Agent.
- Memory Size and Disk Usage
- Network Configuration
- Time Zone & NTP configuration
- User logged in & Session type

➤ **To view General Info:**

- In the EMS Server Management menu, choose option **General Info**; the **General Information** screen is displayed.

Figure 8-4: General Info

```

                                General Info
EMS Version: 5.8.63
OS Version: SunOS 5.10 SUNW,Sun-Fire-V210
Java Version: java full version "1.6.0_06-b02"
Memory Size: 2GB
ACEMS Disk Usage:
/dev/dsk/clt0d0s3          54G    20G    34G    37%    /ACEMS
Swap Spaces:
swap          3.9G    1.1M    3.9G    1%    /etc/svc/volatile
swap          4.0G    8.0M    3.9G    1%    /tmp
swap          3.9G    48K    3.9G    1%    /var/run

EMS Watchdog Status: Up
EMS Server Process Status: Up
EMS Security Status: Not Secured

Apache Server Status: Down
Apache Version:
Server version: Apache/2.2.6 (Unix)
Server built:   Nov 29 2007 04:35:15

Oracle Server Processes Status:
DB Processes Status: Up
Oracle Listner Status: Up
Number of DB Connections:      9

SNMP Agent Status: Up
NTP Daemon Status: Down
Time: [03/11/2009 14:14:13]
Time Zone: Cuba

Network Configuration:
Server's Network:
    Interface      : bge0
    Host Name      : EMS-Server14
    IP Address     : 10.7.6.14
    Subnet Mask    : 255.255.0.0
    Network Address : 10.7.0.0
Network 1 (MG's Network):
    Not configured
Network 2:
    Not configured
Network 3:
    Not configured

Ethernet Redundancy Configuration:
    
```


8.1.2 Collecting Logs

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

The following log files are collected:

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

➤ To collect Logs:

- In the EMS Server Management menu, choose option **Collect Logs**.
A message is displayed on the screen informing you that a Diagnostic **tar** file has been created and the location of the **tar** file.

8.2 Networking

8.2.1 Change Server's IP Address

This option enables you to update the EMS server's IP address.



Note: When the operation is finished, the server will reboot itself for the changes to take effect.

➤ To change Server's IP Address:

1. In the EMS Server Management menu, choose option **Change Server's IP address**.
The current IP configuration of the EMS server is displayed. The information includes Server Host Name, and IP information. The user is prompted to enter relevant network configuration parameters.

Figure 8-5: Server IP Configuration Updates

```
IP Address [10.7.14.146]: 10.7.9.211
Subnet Mask [255.255.0.0]: 255.255.0.0
Default Gateway [10.7.0.1]: 10.7.0.1
```

2. Once you have updated the IP configuration, you will be asked to confirm the changes.
Upon confirmation, the server will reboot itself for changes to take effect.

Figure 8-6: User Configuration Updates

```

New EMS Server IP Configuration (Server Network):
  IP: 10.7.9.211
  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) █
  
```

8.2.2 Configure Ethernet Interfaces

The EMS server supports up to four Ethernet Interfaces, which can be configured to support up to four different networks:

- EMS Client-Server Network
- Network 1 (Media Gateways Network only)
- Network 2
- Network 3

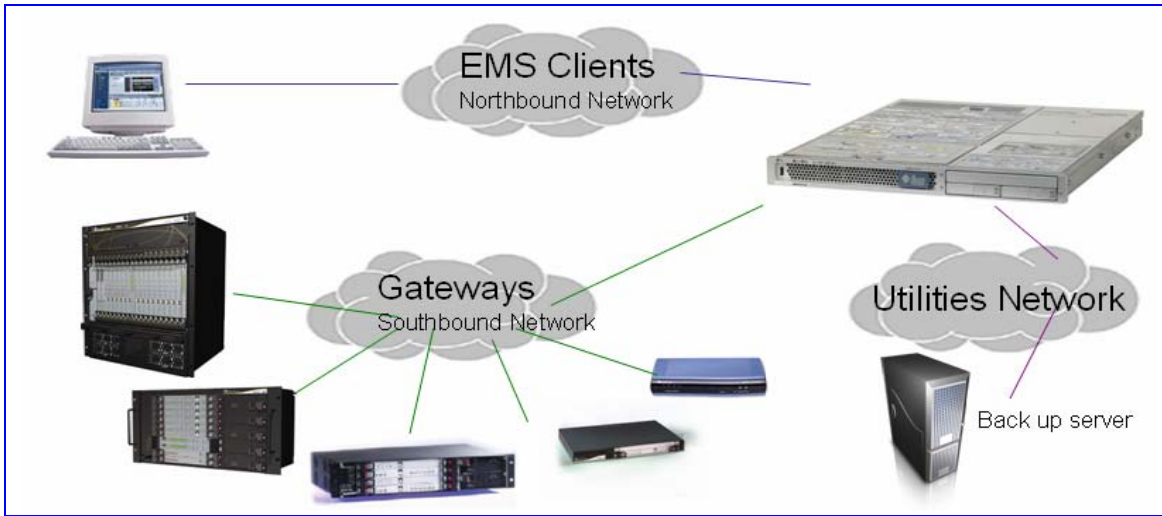
The different interfaces could be used for various purposes, including: separation between EMS Clients and MGW networks, Backup, Maintenance utilities or for Ethernet redundancy purposes.

This option enables you to Add, Remove or Modify these server interfaces.



Note: When this operation has completed, the server will reboot itself for the changes to take effect.

Figure 8-7: 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 Static Routes.

In order 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 change Physical Interface Configuration:

1. In the EMS Server Management menu, choose option **Configure Ethernet Interfaces**.



Note: Don't use the '#' sign in hostnames on the Solaris platform.

Figure 8-8: Physical Interface Configuration Menu (Solaris)

```

Ethernet Interface Configuration

Interface: bge0
        Network: Server's Network
        IP Address: 10.7.6.14
Interface: bge1
        Not configured
Interface: bge2
        Not configured
Interface: bge3
        Not configured

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

2. Choose from one of the following options:
 - **Add Interface** – Adds a new interface to the EMS Server.
 - **Remove Interface** - Removes existing interface from the EMS Server
 - **Modify Interface** - Modifies a existing interface from the EMS Server

8.2.2.1 Add Interface

➤ To Add a New Interface:

1. Choose **Option 1 - Add Interface**.
A list of currently available interfaces (not yet configured) are displayed.
2. Choose an interface (in 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. Confirm the changes; the server will reboot itself for the changes to take effect.

Figure 8-9: Add Interface Parameters

```
Add Interface:

Choose Interface:
  1) bge1
  2) bge2
  3) bge3
  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 : 10.7.9.211
Hostname   : GW
Subnet Mask : 255.255.0.0

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

8.2.2.2 Remove Interface

➤ To remove an existing interface:

1. Choose option **2**.
2. Choose the interface to remove.
A list of currently configured interfaces are displayed.
3. Confirm the changes; the server will reboot itself for the changes to take effect.

Figure 8-9: Remove Interface

```
Ethernet Interface Configuration

Interface: bge0
  Network: Server's Network
  IP Address: 10.7.19.40
Interface: bge1
  Network: Network 1 (MG's Network)
  IP Address: 10.7.9.211
Interface: bge2
  Not configured
Interface: bge3
  Not configured

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

Remove Interface:

Choose Interface:
  1) bge1
  q) Quit
  : 1

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

8.2.2.3 Modify Interface

➤ **To modify an existing interface:**

1. Choose option **3**.
2. Choose the interface to modify.
A list of currently configured interfaces are displayed.
3. Change the interface parameters.
4. Confirm the changes; the server will reboot itself for changes to take effect.

Figure 8-9: Modify Interface

```

Ethernet Interface Configuration

Interface: bge0
    Network: Server's Network
    IP Address: 10.7.19.40
Interface: bge1
    Network: Network 1 (MG's Network)
    IP Address: 10.7.9.211
Interface: bge2
    Not configured
Interface: bge3
    Not configured

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

Modify Interface:

Choose Interface:
    1) bge1
    q) Quit
: 1

Interface Configuration:

    IP Address: [10.7.9.211]: 10.7.9.212
    Host Name [MG]: MG
    Subnet Mask: [255.255.0.0]: 255.255.0.0

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

8.2.3 Configure Ethernet Redundancy on Solaris

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

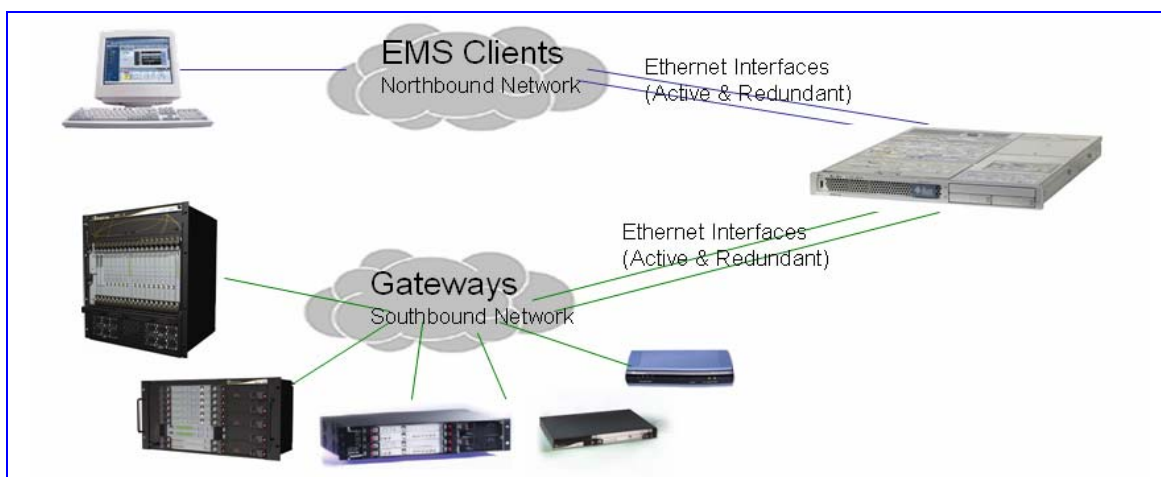
The EMS server supports up to 4 Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them (for example, EMS Clients (northbound) and Gateways (southbound)).

This option enables you to configure Ethernet ports redundancy.



Note: When the operation is finished, the server will reboot itself for the changes to take effect.

Figure 8-10: Physical Ethernet Interfaces Redundancy



➤ **To configure Ethernet Redundancy:**

1. In the EMS Server Management menu, choose option **Configure Ethernet Redundancy**.

Figure 8-11: Ethernet Redundancy Configuration Menu

```

Ethernet Redundancy Configuration

Interface: bge0
    Network: Server's Network
    IP Address: 10.7.19.40
Interface: bge1
    Not configured
Interface: bge2
    Not configured
Interface: bge3
    Not configured

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

2. Choose from one of the following options:
 - Add Redundant Interface
 - Remove Redundant Interface
 - Modify Redundant Interface

8.2.3.1 Add Redundant Interface

Use this option under the following circumstances:

- When you have configured an interface (see Configure Ethernet Interfaces on page 50).
- When your default router can respond to a ping command due to a heartbeat procedure between interfaces and the default router (in order to verify activity).

➤ **To add redundant interface:**

1. Choose **Option 1: Add Redundant Interface**.
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. Enter Private IP address and Host Name for both the Active and Standby interfaces. It is mandatory that both Private IP addresses and Global IP address reside in the same subnet. Don't use the '#' sign in hostnames.

5. Confirm the changes; the server will reboot itself for changes to take effect.

Figure 8-12: Add Redundant Interface

```
Add Redundant Interface:

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

Choose Redundant Interface:
 1) bge1
 2) bge2
 3) bge3
 q) Quit
 : 1

Ethernet Redundancy Settings:

Active Interface - Host Name : MG1
Active Interface - IP Address : 10.7.9.211
Standby Interface - Host Name : MG2
Standby Interface - IP Address : 10.7.9.212

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

8.2.3.2 Remove Ethernet Redundancy

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

1. Choose option 2 - **Remove Redundant Interface**.
2. Choose the Ethernet Redundancy Interface to remove.
3. Current network type Ethernet Redundancy configuration is displayed.
4. Enter **Y** to confirm the changes. The server will reboot itself for changes to take effect.

Figure 8-13: Ethernet Redundancy Interface to Disable

```

Ethernet Redundancy Configuration

Interface: bge0
    Network: Server's Network
    IP Address: 10.7.19.40
Interface: bge1
    Network: Server's Network (redundant interface)
Interface: bge2
    Not configured
Interface: bge3
    Not configured

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

Remove Redundant Interface:

Choose Redundant Network
    1) Server's Network (bge0, bge1)
    q) Quit
    : 1

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

8.2.3.3 Modify Redundant Interface

➤ **To modify redundant interface and change redundancy settings:**

1. Choose option 3 - **Modify Redundant Interface**.
2. Choose the Ethernet Redundancy Interface to modify.
3. Change the redundancy settings.
4. Enter **Y** to confirm the changes. The server will reboot itself for changes to take effect.

Figure 8-14: Modify Redundant Interface

```
Ethernet Redundancy Configuration

Interface: bge0
  Network: Server's Network
  IP Address: 10.7.19.40
Interface: bge1
  Network: Server's Network (redundant interface)
Interface: bge2
  Not configured
Interface: bge3
  Not configured

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 (bge0, bge1)
q) Quit
: 1

Ethernet Redundancy Settings:

Active Interface - Host Name [MG1]: 1
Active Interface - IP Address [10.7.9.211]: 10.7.9.211
Standby Interface - Host Name [MG2]: 2
Standby Interface - IP Address [10.7.9.212]: 10.7.9.212

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

8.2.4 Configure Ethernet Redundancy on Linux

➤ To configure Ethernet Redundancy:

1. In the EMS Server Management menu, choose option **Configure Ethernet Redundancy**.

Figure 8-15: Ethernet Redundancy Configuration Menu

```

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
: █
    
```

2. Choose from one of the following options:
 - Add Redundant Interface
 - Remove Redundant Interface
 - Modify Redundant Interface

8.2.4.1 Add Redundant Interface

Use this option under the following circumstances:

- When you have configured an Ethernet interface (see Configure Ethernet Interfaces on page 50).
- When your default router can respond to a 'ping' command, due to a heartbeat procedure between interfaces and the default router (in order to verify activity).

➤ To add redundant interface:

1. Choose **Option 1: Add Redundant Interface**.
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. Confirm the changes; the server will reboot itself for changes to take effect.

Figure 8-16: 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) █
```

8.2.4.2 Remove Ethernet Redundancy

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

1. Choose option 2 - **Remove Redundant Interface**.
2. Choose the Ethernet Redundancy Interface to remove.
The Current network type Ethernet Redundancy configuration is displayed.
3. Enter **Y** to confirm the changes. The server will reboot itself for changes to take effect.

Figure 8-17: Ethernet Redundancy Interface to Disable

```

Ethernet Redundancy Configuration

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

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

Remove Redundant Interface:

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

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

8.2.4.3 Modify Redundant Interface

➤ **To modify redundant interface and change redundancy settings:**

1. Choose option 3 - **Modify Redundant Interface**.
2. Choose the Ethernet Redundancy Interface to modify.
3. Change the redundancy settings.
4. Enter **Y** to confirm the changes. The server will reboot itself for changes to take effect.

Figure 8-18: 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
```

8.2.5 Configuring the 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 will refer 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 **Configure DNS** option is displayed. If already configured, the **Modify DNS** option is displayed.

➤ To Configure the DNS Client:

1. In the EMS Server Management menu, choose option **Configure DNS Client**.
2. In the **DNS Configuration** menu, choose option 1.

Figure 8-19: Configure DNS Client

```

DNS Configuration:
1) Configure DNS
2) Back to Main Menu
: █
    
```

3. You are prompted to specify the location domain. Enter **Y** to specify the local domain name.
4. You are prompted to specify the search list. Enter **Y** to specify a list of domains (use a comma delimiter to separate search entries in the list).
5. Specify DNS IP addresses **1, 2** and **3**.

Figure 8-20: Configure DNS Client

```

Do you want to specify the local domain name ? (y/n)y
Local Domain Name: domain.example.com
Do you want to specify a search list ? (y/n)y
Search List (use "," between domains names): dm1.example.com,d2.example.com
DNS IP Address 1: 10.1.1.10
DNS IP Address 2: 10.1.1.11
DNS IP Address 3: 10.1.1.12
    
```

Figure 8-21: DNS Setup

```

New DNS Configuration:
Domain Name: domain.example.com
Search List: dm1.example.com,d2.example.com
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) █
    
```


8.2.6 Static Routes

Static routes are usually only used in conjunction with a `/etc/defaultrouter`. You may require static routes when there are networks that you did not wish to go through your default Gateway/Router. In this case, you will probably want to make the routes permanent by adding the static routes rules.

This option enables you to add or remove static route rules.

➤ To configure Static Routes:

1. In the EMS Server Management menu, choose option **Static Routes**. The Static Routes menu and all current static rules are displayed.

Figure 8-22: Routing Table and Menu

```

Static Routes Configuration

Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
10.7.0.0         0.0.0.0        255.255.0.0    U       0 0        0 bond0
169.254.0.0     0.0.0.0        255.255.0.0    U       0 0        0 bond0
0.0.0.0         10.7.0.1       0.0.0.0        UG      0 0        0 bond0

1) Add Static Route
2) Remove Static Route
3) Back to Main Menu
: █

```

2. In 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. Choose option **1 Add a Static Route**.
2. Enter the Destination Network Address.
3. Enter the router's IP address.
4. Enter **Y** to confirm these changes.

Figure 7-2-18: Static Route Changes

```

1) Add Static Route
2) Remove Static Route
3) Back to Main Menu
: 1
Destination Network Address : 10.17.0.0
Network Mask : 255.255.0.0
Router IP Address : 10.17.0.1

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

```

➤ **To remove a Static Route:**

1. Choose option **2 Remove a Static Route**.
2. Enter the Destination Network Address for the static route you wish to remove.
3. Enter the router's IP address.
4. Enter **Y** to confirm these changes.

8.2.7 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 determine whether or not to forward system alarms from the EMS server to the NMS.

➤ **To configure SNMP Agent:**

1. In the EMS Server Management menu, choose option **Configure SNMP Agent**. The SNMP Manager screen is displayed with the Process ID information.
2. Choose one of the following options:
 - **SNMP Manager Configuration:** Configure the OS SNMP Agent to send system alarms to the NMS IP address.
 - **Start Sending Alarms:** Starts forwarding system alarms from the EMS to the NMS.
 - **Stop Sending Alarms:** Stops forwarding system alarms from the EMS to the NMS.

8.2.7.1 SNMP Manager Configuration

➤ **To configure the SNMP Manager:**

1. Choose option **1 SNMP Manager Configuration**.
2. Enter the **NMS IP address**.
3. Enter the **Community string**.

8.2.7.2 Configure 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. Enter the NAT IP address.
2. Press 'Y' to confirm the changes.

➤ **To remove NAT configuration:**

1. Enter the value -1.
2. Press 'Y' to confirm the changes.

Figure 8-23: Solaris SNMP Manager

```
SNMP Agent Configuration

SNMP Agent Status: Up

1) Configure SNMP Agent
2) Stop SNMP Agent
3) Back to Main Menu
: 1

Configure SNMP Agent

NMS IP [10.22.13.126]: 10.22.13.126
Community string : public

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

8.2.7.3 Sending System Alarms

➤ **To start sending system alarms to the NMS:**

- Choose option 2 Start Sending Alarms (when the SNMP Agent status is Down)

8.2.7.4 Stopping System Alarms

➤ **To stop sending system alarms sending to the NMS:**

- Choose option 2 Stop Sending Alarms (when the SNMP Agent status is Up)

8.3 Security

The EMS Management security options enable you to perform security actions such as hardening Solaris 10-**Basic** and **Advanced** security performance, Oracle hardening and users administration.

8.3.1 Basic Hardening



Note: This option is not supported on Linux Operating System.

The purpose of basic hardening is to protect the EMS server from unauthorized access and hostile attack. The Basic Hardening uses JumpStart Architecture and the Security Scripts (JASS) toolkit to harden and audit Solaris Operating Systems services. The script disables all Solaris services except those services used by the EMS. For a list of services used by the EMS, refer to the section Configuring the Firewall on page 83.

After running the Basic Hardening script, the EMS server is qualified to use in the Internet.



Notes:

1. This option is only available when using secured shell (ssh).
2. When the operation is finished, the server will reboot itself for the changes to take effect.
3. During this procedure, do not press Ctrl+C.

The EMS server utilizes the Apache Web server for the purpose of software upgrades and regional files loading to media gateways (MediaPack / Mediant 1000 / Mediant 2000 / Mediant 3000), as well as for running Java web start (JAWS). The Apache Web server uses the HTTP and HTTPS ports for the above operations. When Basic Hardening is performed, the HTTP port is closed.

The rollback procedure can be performed after configuring basic hardening to open all services. The rollback procedure restores the EMS server to the state prior to when the basic hardening was performed.

➤ To configure basic hardening:

1. In the EMS Server Management menu, choose option **Basic Hardening**. The Hardening menu is displayed.
2. Choose one of the following options:
 - **Option 1: Start Hardening (Close all services)**
Choose this option to close all services.
 - **Option 2: Rollback (Open all services)**
Choose this option to open all services.

8.3.1.1 Start Basic Hardening

➤ **To start basic hardening:**

1. Choose option 1 **Start Hardening**.

Figure 8-24: Basic Hardening Menu

```
Reboot is required at the end of the script.

1. Start Hardening - Close all services
2. Rollback - Open all services
3. Quit
choose: █
```

The following prompt is displayed:

Figure 8-25: Prompts Referring to SNMP Services

```
Installation of <SUNWjass> was successful.
application SUNWjass Solaris Security Toolkit 4.2.0

Do you want to enable SNMP services (y/n)?
y
>> backup default values
The Apache server stopped.
Starting the Apache server.
[NOTE] The following prompt can be disabled by setting JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured, it
is both possible and likely that by default all remote shell and file transfer
access to this system will be disabled upon reboot effectively locking out any
user without console access to the system.

Are you sure that you want to continue? (yes/no): [no]
yes █
```

2. You are prompted if you want to continue?
 - Enter **Y** to run the JASS package.
3. Wait a few minutes.
4. Choose a new password for the **acems** user and for user **root**. It is recommended to change the default password.



Note: Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the server without them.

Figure 8-26: Activating the EMS Hardening Feature

```

=====
>> Please change user acems password
New Password:
Re-enter new Password:
passwd: password successfully changed for acems
>> Please change user root password
New Password:
Re-enter new Password:
passwd: password successfully changed for root
*****
**      Please Reboot the server      **
*****

Press Enter to continue.
█
    
```

When the operation has finished, the server will reboot itself for changes to take effect.

8.3.1.2 Rollback

➤ **To perform a rollback**

1. Choose Option **2 Rollback-Open All services**.



Note: If the server is in an advanced hardened status (i.e., the script *emsAdvancedHarden.pl* has already been run on this server), refer to Advanced Hardening- Rolling Back from Advanced Hardening.

Figure 8-27: Basic Hardening, Rollback - Open all services

```

Reboot is required at the end of the script.

1. Start Hardening - Close all services
2. Rollback - Open all services
3. Quit
choose: █
    
```

2. Choose 1 to roll back the last hardened package.

Figure 8-28: Rolling Back from Hardened Server -1

```
Please select a Solaris Security Toolkit run to restore through:
1. August 16, 2007 at 12:34:35 (/var/opt/SUNWjass/run/20070816123435)
Choice ('q' to exit)? 1
```

3. Choose 5 ALWAYS Keep.

Figure 8-29: Rolling Back from Hardened Server -2

```
Select your course of action:
1. Backup - Save the current file, BEFORE restoring original.
2. Keep - Keep the current file, making NO changes.
3. Force - Ignore manual changes, and OVERWRITE current file.

NOTE: The following additional options are applied to this and ALL subsequent files:
4. ALWAYS Backup.
5. ALWAYS Keep.
6. ALWAYS Force.

Enter 1, 2, 3, 4, 5, or 6:

```

4. Enter Y to remove the package.

Figure 8-30: Rolling Back from Hardened Server -3

```
The following package is currently installed:
SUNWjass Solaris Security Toolkit 4.2.0
(Solaris) 4.2.0

Do you want to remove this package? [y,n,?,q]
```

5. Restore the default passwords.
6. When finished, the server will reboot itself for changes to take affect.

8.3.2 Advanced Hardening



Note: Before performing Advanced Hardening, you must perform Basic Hardening (See section Basic Hardening above). This option is not supported on the Linux Operating System.

This option enables you to harden the Solaris 10 for enhanced security performance. The Advanced Hardening script removes OS packages which are not required by the system and are security vulnerable. It change file permissions/groups for several files in the system (Operating system and EMS application files) and removes the snoop utility from the system.

Also the Advanced Hardening script adds password and login restrictions such as password aging limitations about password characters.

The security script is supplemented to comply with special US DoD (Department of Defense) requirements as described in the "[Security Technical Implementation Guides \(STIG\)](#)".

The security script is supplemented to comply with special US DoD requirements.



Notes:

1. This option is only available when using secured shell (ssh).
2. When the operation is finished, the server will reboot itself for the changes to take effect.
3. Before implementing Advanced Hardening, please contact your AudioCodes FAE.
4. During this procedure, do not press Ctrl+C.

➤ **To configure advanced hardening:**

1. In the EMS Server Management menu, choose option **Advanced Hardening**.
2. Choose one of the following options:
 - **Option 1:** Enter 1 to start additional hardening of the system.

Figure 8-31: Activating the Advanced Hardening Feature

```
1. Start additional hardening of the system
2. Rollback to a non-secured system
3. Quit
choose: █
```

The EMS server is now in Advanced Hardening mode.

- **Option 2:** Enter 2 to Rollback to a non-secured system.

Figure 8-32: Rolling Back from Advanced Hardening

```

1. Start additional hardening of the system
2. Rollback to a non-secured system
3. Quit
choose: █

```

The EMS server is hardened. The EMS server is rolled back to its previous status of hardened state.

To roll back to the server default status, refer to Section [7.3.1 Basic Hardening](#).

8.3.3 SSL Tunneling Configuration



Note: This option is not supported on the Linux Operating System.

SSH over SSL tunneling access for server operation and maintenance provides FIPS-140.2 compliance for SSH access to the EMS server machine. To connect the EMS server using SSL tunneling, you must configure both the EMS server and the EMS client to support this feature.

8.3.3.1 EMS Server-SSL Tunneling Configuration

➤ To configure the EMS server for SSL Tunneling:

1. In the EMS Server Manager Security menu, choose option 12. **SSL Tunneling Configuration**.

The current SSL Tunneling Status is displayed. In addition, the SSH port status is displayed as (open / close).

Figure 8-33: SSL Tunneling Configuration Manager

```

SSL Tunneling Configuration Manager:
SSL Tunneling Status: Disable
SSL Tunneling Processes Status: Down
Port 22 (SSH): Open

1) Stop SSL Tunneling
2) Start SSL Tunneling
3) Close SSH Service (Port 22)
4) Back to Main Menu
: █

```

➤ **To Enable SSL Tunneling:**

1. Select (2) **Start SSL Tunneling**. Ensure that the SSL Tunneling Status is changed to **Enabled** and the **SSL Tunneling Processes Status** is changed to **Up**.
2. Connect the EMS client to the EMS server via the SSL Tunneling application (see section 'EMS Client-SSL Tunneling Configuration' below).
3. Ensure that the SSL connection between the EMS client and the EMS server is successful by running basic actions such as **EMS Server Manager -> General Info**.
Select (3) Close SSH Service to make SSL Tunneling the only possible communication option between the EMS client and the EMS server.

➤ **To Disable SSL Tunneling:**

1. Select (3) Open SSH Service. Connect EMS Server via SSH.
2. Select (1) Stop SSL Tunneling.

8.3.3.2 EMS Client-SSL Tunneling Configuration

➤ **To connect to the EMS server:**

1. Run the SSL Tunneling Client application (this application is part of the EMS client Installation in the Client install folder) and provide the appropriate EMS server IP address.
2. Using a communication application (i.e Putty), enter the local host IP (127.0.0.1) and port 10022 details.

The SSL client listens to this port, and all packets received on this port from the local host are rerouted to the provisioned EMS server IP address through the SSL Tunnel.

8.3.4 Changing DBA Password

This option enables you to change the DBA password. The EMS server will shutdown automatically before changing the DBA Password.

➤ **To change the DBA Password:**

1. In the EMS Server Management menu, choose option **Change DB Password**.

Figure 8-34: Changing the DB Password

```

-----
*****
Oracle Change password Script start
*****
-----
User name:
EMSADMIN
Current Password:
█

```



Note: Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the EMS Database without them.

2. After validation, check that the password was changed successfully.

Figure 8-35: Changing the DB Password

```

----- Validation check -----
*****1*****
DB output ok !
-----
*****
Oracle Change password Completed successfully
*****
-----
Press Enter to continue.
█

```

8.3.5 OS Passwords Settings

This option enables you to change the OS general password settings (like Minimum Acceptable Password Length, Enable User Block on Failed Login, Maximum Login Retries, and Failed Login Locking Timeout). It also lets you change settings for a specific user (like User's Password, Password Validity Max Period, Password Update Min Period, and Password Warning Max Period).

➤ **To change OS passwords:**

1. In the EMS Server Management menu, choose option **Change OS Passwords**.
2. Follow the instructions as shown in the figures below.

Figure 8-36: Changing Password General Settings

```

OS Passwords Settings

Do you want to change general password settings? (y/n) y
Minimum Acceptable Password Length [10]: 10
Enable User Block on Failed Login (y/n) [y]: y
Maximum Login Retries [3]: 3
Failed Login Locking Timeout [900
]: 900

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

Changing general password settings...
Done.
    
```

Figure 8-37: Changing User's Password and Properties

```

Do you want to change password for specific user? (y/n) y
Enter User: acems

Do you want to change its password ? (y/n) y
Changing password for user acems.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

Do you want to change its password properties? (y/n) y
Password Validity Max Period (days) : 100
Password Update Min Period (days) : 0
Password Warning Max Period (days) : 10

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



Note: User **NBIF** is created passwordless 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.

8.3.6 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 be used for 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. In the EMS Server Management menu, choose option **Add EMS User**.



Note: Note and retain these passwords for future access.

2. Enter the name of the user you wish to add.
3. Enter a password for the user.
A confirmation message is displayed.

8.3.7 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.

In the EMS Server Management menu, choose option **Start / Stop File Integrity checker**.

8.4 Maintenance

8.4.1 Configure 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:**

- In the EMS Server Management menu, choose option **Configure NTP**. The **Configure NTP** menu is displayed.
1. Choose **1** to configure NTP.
 2. At the prompt, do one of the following:
 - Enter **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).
 - Enter **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 is started and the NTP status information is displayed on the screen.

➤ **To start NTP services:**

1. Choose **2** and then one of the following options:
 - **Start NTP** (If NTP Service is off).
 - **Stop NTP** (If NTP Service is on).

Figure 8-38: Start NTP

```

Current NTP status:

ntpq: read: Connection refused

NTP Configuration menu:

    1 ) Configure NTP
    2 ) Start NTP
    3 ) Back to Main Menu
Choose: 1
Do you want the EMS to act as an NTP client? [y/n]: y
Enter NTP server 1 IP []: █
    
```

The NTP Daemon process is started and configuration data is displayed.

8.4.2 Change System Timezone

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. In the EMS Server Management menu, choose option **Change System Time Zone**.
2. Enter the required Time Zone.



Note: In Solaris when the operation has completed, the server will reboot itself for the changes to take effect.

Figure 8-39: Change System Timezone

```

Current EMS Server's Time Zone is : Israel

Enter the new timezone name (e.g. "US/Eastern")
or type ? for interactive timezone selection.
: GMT

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

```

3. Enter **Y** to confirm the changes; the server automatically reboots itself for changes to take effect.

8.4.3 Change System Time and Date

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

➤ To change system time and date:

1. In the EMS Server Management menu, choose option **Change System Time and Date**.
2. Enter the new time in the following order:
mmddHHMMyyyy.SS : month(08),day(16),Hour(16),Minute(08),year(2007),"."
Second
See the following example :

Figure 8-40: Change System Time and Date

```

Server's Time Is: [16/08/1970 16:21:35]
New Time (mmddHHMMyyyy.SS) []: 081616342007.00
Are you sure that you want to continue ? (y/n/q) y
Thu Aug 16 16:34:00 IDT 2007
Press Enter to continue
█

```

8.4.4 Start /Stop the EMS Server

- In the EMS Server Management menu, choose option **Start / Stop the EMS Server**.

8.4.5 Web Server Configuration

This option enables you to Start and Stop the Apache server and to Open and Close HTTP/HTTPS Services.

- In the EMS Server Management menu, choose option **Web Server Configuration**.

Figure 8-41: Web Server Configuration

```
Web Server Configuration Manager:
The Web Server's Processes are: UP
The Web Server's Watchdog is: UP
Port 80 (HTTP): Open
Port 443 (HTTPS): Open
JAWS Service: Enabled

1 ) Stop the Apache Server
2 ) Close HTTP Service (Port 80)
3 ) Close HTTPS Service (Port 443)
4 ) Disable JAWS
5 ) Back to Main Menu
Choose: █
```

➤ **To stop the Apache server:**

- In the Web Server Configuration menu, choose option **1 - Stop the Apache Server**.

➤ **To start the Apache server:**

- In the Web Server Configuration menu, choose option **1 - Start the Apache Server**.

➤ **To open/close HTTP service (port 80):**

- In the Web Server Configuration menu, choose option **2 - Open/Close HTTP Service (Port 80)**.

➤ **To open/close HTTPS service (port 443):**

- In the Web Server Configuration menu, choose option **3 - Open/Close HTTPS Service (Port 443)**.

➤ **To disable JAWS:**

- In the Web Server Configuration menu, choose option **4 - Disable JAWS**.

8.4.6 Backup the EMS Server

AudioCodes provides a simple mechanism for data backup in the form of a script that uses Oracle import and export tools.

It is highly recommended to back up the EMS data manually, especially after an extensive configuration process in order to safeguard against a malfunction.

The backup generates two files: **EMSexport.dmp** which contains server database information and **emsServerBackup.tar**, which contains all version directories. All the server files and the database are backed up to one of these files. These files are located under /ACEMS/NBIF/emsBackup folder.

All EMS Server Manager configurations (e.g Network, Interface redundancy and Security) are not backed up.

The created backup file can be restored only on the exactly the same software version from which it was made.



Note: Configuration performed via the EMS Server Manager (Network, Interface redundancy, Security) is not backed up. **Before running this option, please verify the following:**

1. All EMS server configurations performed via the EMS Server Manager should be performed prior to the Backup such as Security and Networking.
2. The Destination server should be at the same security level (hardening) as the source server.
3. The backup files can later be restored only for the same EMS version.

➤ To backup the EMS Server:

1. In the EMS Server Management menu, choose option **Backup the EMS Server**. Backup data is displayed. A confirmation message is displayed at the end of the backup.

8.4.7 Schedule Backup for the EMS Server

This option enables you to schedule backup to automatically run periodically.

➤ To schedule backup of the EMS Server:

1. In the EMS Server Management menu, choose option **Schedule Backup for the EMS Server**.

Figure 8-42: Scheduled Backup for the EMS Server

```
The data will be exported once a week, to a file named EMSexport.dmp
you should backup this file to another machine.
choose a day of the week to perform backup (0-6)
0-Sunday, 1-Monday, 2-Tuesday, 3-Wednesday, 4-Thursday, 5-Friday, 6-Saturday:
█
```

2. Choose the day of the week for the EMS to perform backup.
3. Choose an hour to perform backup (0-23) and press **Enter**.
A confirmation message is displayed.

8.4.8 Restore the EMS Server

This option enables you to import backup data.

The restore can be made only from the backup file created on the exactly same software version.



Note: Before running this option, please verify the following:

1. The EMS server configuration should be performed prior to the restore procedure, for example Security and Networking.
2. The EMS Server security level should be the same level as the pre-restored server (Hardening level).
3. The Restore action can be performed only with a backup file which was previously saved in the same EMS version.

➤ To restore the EMS Server:

1. In the EMS Server Management Menu, choose option **Restore the EMS Server**.
2. Copy the backup files **EMSexport.dmp** and **emsServerBackup.tar** to the directory **/ACEMS/NBIF/emsBackup**.
3. Enter **root** password.

8.4.9 Reboot the EMS Server

➤ To reboot the EMS Server:

- In the EMS Server Management menu, choose option **Reboot the EMS Server**.

9 Configuring the Firewall

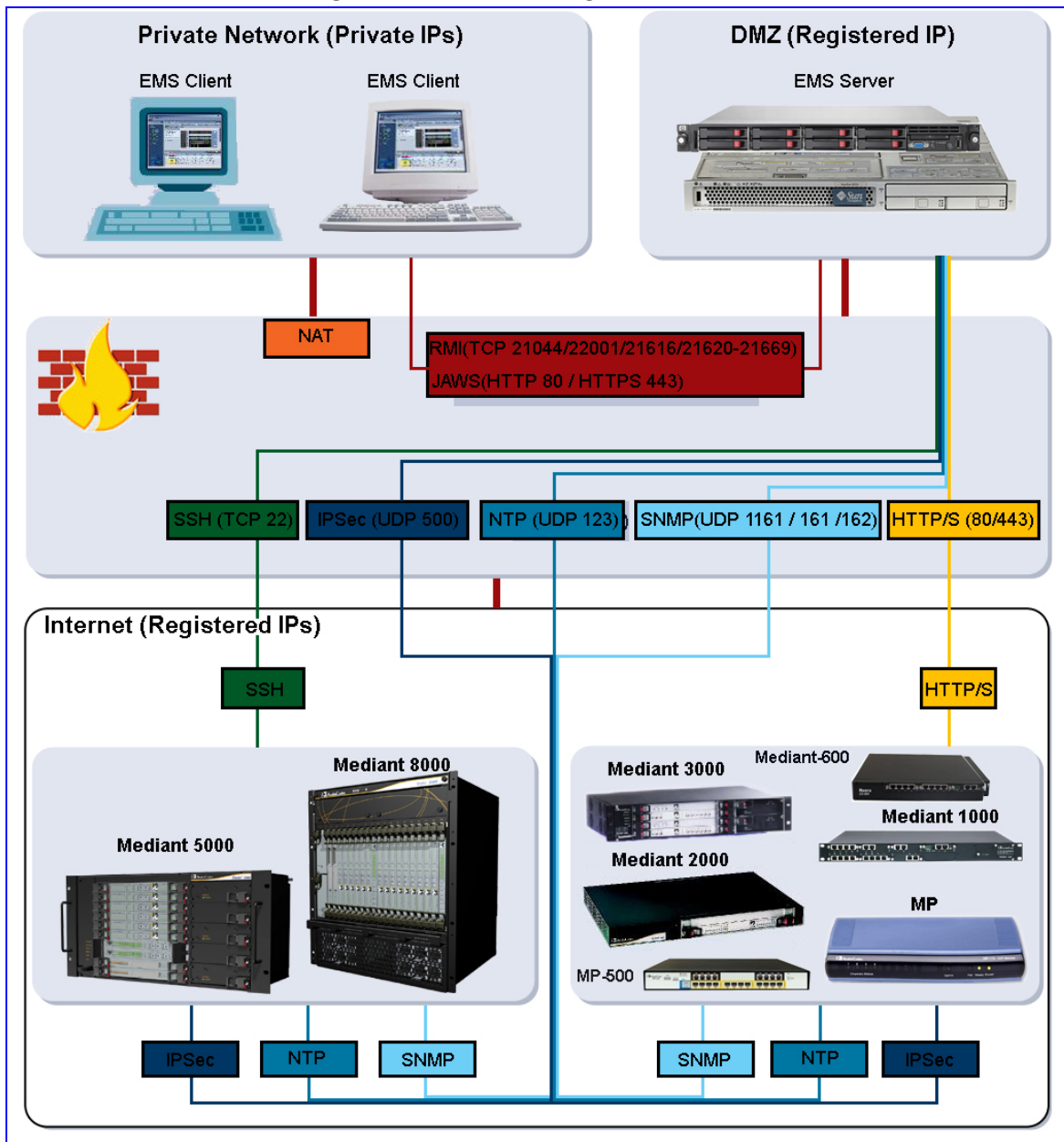
To enable EMS Client ↔ EMS Server ↔ Managed Gateways communication according to Figure 8-1, define the rules specified in the Firewall Configuration Rules table below:

Table 9-1: Firewall Configuration Rules

Connection	Port Type	Port Number	Purpose
EMS Client ↔ EMS Server	TCP	22001, 21044, 21616 and 21620-21660	RMI communication
	HTTP	80 or 443	JAWS application.
EMS server ↔ All managed media gateways	UDP	1161 and 162	On the EMS server side for SNMP communication.
	UDP	161	For all media gateways for SNMP communication
	UDP	123	On the EMS server side for NTP synchronization
	UDP	500	On the EMS server and MGs for IPSec communication
EMS Server ↔ Managed Mediant 600/1000/2000/3000 Media Gateways, IPmedia 3000 Media Servers, and/or MediaPacks	HTTP	80	Web-based connection between the EMS server and the listed Media Gateways (HTTPS-secure mode).
	HTTPS	443	

Connection	Port Type	Port Number	Purpose
EMS Server ↔ Managed Mediant 5000/8000 Media Gateways	TCP	22	TCP based connection between the EMS server and the listed Media Gateways SCP and SSH communications. Note, ports should be open for both Global and SC private IP Addresses.

Figure 9-1: Firewall Configuration Schema



- NOC ↔ EMS (Server) ports

Table 9-2: 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 9-3: 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

10 Installing the EMS Client

10.1 Installing the EMS Client on a Client PC

1. Insert AudioCodes' EMS installation disk.
2. Double-click the EMS Client Installation file (PC)/ac_ems_setup_win32.exe and follow the installation instructions.
3. As a result 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**.

10.2 Running the EMS on a Client PC

➤ **To run the EMS on a client PC:**

- Double-click the EMS Client icon on your desktop or run Start>Programs>EMS Client.

10.3 First-Time Login

1. Log in as user 'acladmin' with password 'pass_1234' or 'pass_12345'.

Note that first-time access defaults are case sensitive. After you login to the EMS for the first-time, you will be 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.

10.4 Installing and Running the EMS Client on a Client 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 client PC using JAWS:

1. Open Internet Explorer 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:

1. Specify the path `http://<server_ip>/jaws`.

An 'EMS Login Screen' is opened.

For example: `http://10.7.6.18/jaws/`

- `http://<server_ip>/jaws/?username=<user_name>&password=<password>`.

For example: `http://10.7.6.18/jaws/?username=acladmin&password=pass_12345`

- `http://<server_ip>/jaws/?username=<user_name>&password=<password>&showtree=<false>&showalarmbrowser=<false>&nodeip=<node ip>` where each one of the supported arguments can be provided in any order. Upon client opening, User can change initial settings of his view by editing 'View' menu items.

Supported arguments are:

- **username** - should include the username
- **password** - should include clear text password
- (optional) **nodeip** - when requested the EMS client will be opened to the requested node status screen. Default - globe view on the status screen.
- (optional) **showtree** - two values supported: true/false. Default value is true.
- (optional) **showalarmbrowser** - two values supported: true/false. Default value is true.
- For example:
`http://10.7.6.18/jaws/?username=acladmin&password=pass_12345&challenge=nomatter&showtree=false&showalarmbrowser=false&nodeip=10.7.5.201`

11 Appendix A - Frequently Asked Questions (FAQs)

11.1 “SC>” Prompt Displayed in User Console on Sun Solaris

Q: SC> Prompt is displayed in the user console and it is not possible to open the Solaris OS shell.

A: The sc> prompt is shown when you connect to the Sun Solaris Server via the serial port and the Sun Server power is off.

In order to return the Solaris OS shell, press the Power button for 2 seconds to power on the system.



11.2 JAWS not running

Q: Java Web Start is not running.

A: Upgrade Java Web Start version as described below.

➤ **To run the Java Upgrade script, do the following:**

1. Insert the DVD labeled 'SW installation and Documentation' into the DVD ROM.
2. Log the server in as **root** user with password *root*.
3. Run the installation script **Javalnstaller.pl** from the following location:
Under **Documentation\Java_1.6_version** (it's important to run it from its location and not with a full path)

```
> cd /cdrom/cdrom0/Documentation\Java_1.6_version ***<<<version
> ./JavaInstaller.pl
```



Note: If an error “Permission denied is displayed.” at the beginning of the Javalnstaller.pl script please run it as follows:
>/bin/sh StartJavaUpgrade.sh

4. Read the License Agreement and then select **yes** to continue the installation.
5. When the script is finished, done is displayed.

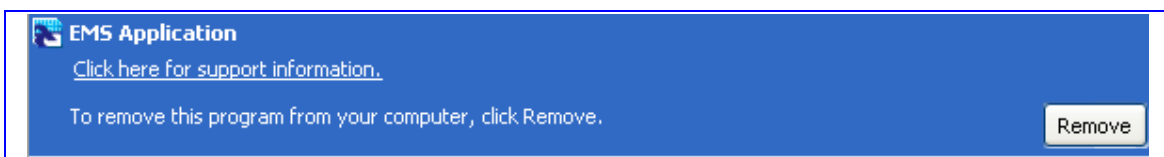
11.3 After installing JAWS - the EMS application icon is not displayed on the desktop


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

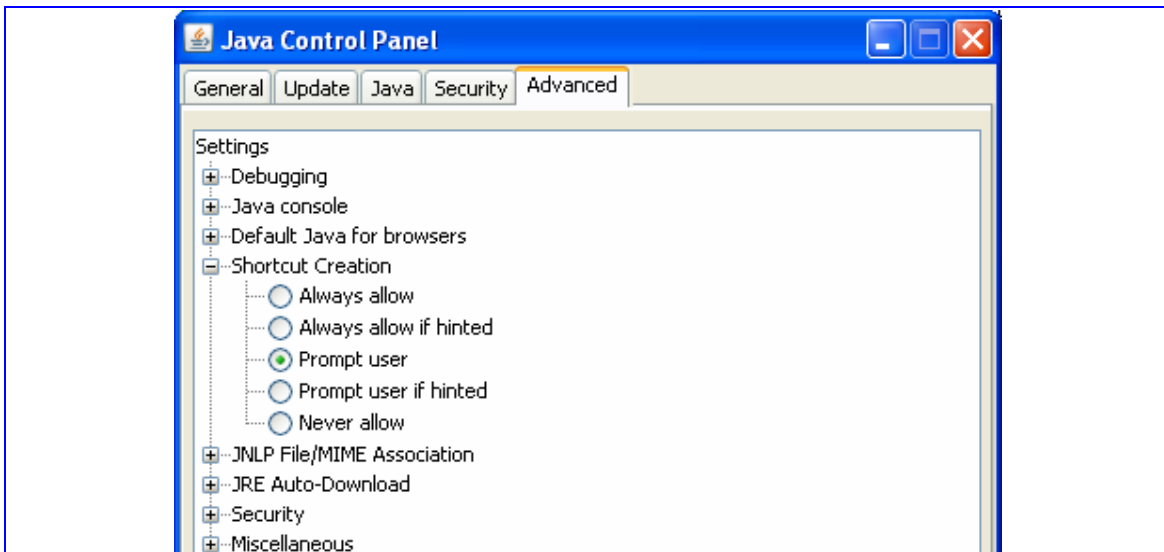
A: You must update the Java properties and reinstall the EMS application.

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

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



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



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 Installing and Running the EMS Client on a Client PC using Java Web Start (JAWS):
9. After the installation has completed, the new Icon is created on your desktop:



11.4 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 for the database not starting automatically:**

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

11.5 Changes Not Updated in the Client

- Q:** After a successful installation, the multiple GWs add operation - as well as changes made by other clients - are not updated in the client.
- A:** Check the configuration of the date on the 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.

11.6 Removing the EMS Server Installation

- Q:** How do I remove the EMS server installation?
- A:** Refer to Installing Solaris 10 from AudioCodes' DVD on page 21.

Reader's Notes

12 Appendix B – Site Preparation Prior to Upgrade

This procedure is only applicable to Solaris-based customers who have a lower version installed. Since version 5.8 requires a clean installation, specific data should be backed up in a separate location, prior to formatting the EMS server machine.

1. EMS server data backup should be performed prior to machine formatting. For more information, see Backup the EMS Server on page 81. Backup Files should be transferred to another machine prior to the EMS server installation. Note, that these backup files cannot be used for the 5.8 version. They should be kept in case the user fails to install the 5.8 version, and decides to rollback 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. Use Security -> User's List menu.
3. EMS Tree: the user can export the GWs 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 user 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 GW removal and adding and to ensure that the EMS <-> GW connection has been established.

Figure 12-1: 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 Chi
2	10.7.19.88	10.7.19.88	gena		MEDIANT 8000	5.8.57	Connectec	Unlocked	Enabled	No Misma	2009-11
3	10.7.5.220	10.7.5.220	Roye		UNKNOWN MP114 FXS/FXO	5.90A.006	Connected			No Misma	2009-11
4	10.7.5.221	10.7.5.221	Roye		UNKNOWN	5.50.020	Connected			No Misma	2009-11
5	10.7.5.217	10.7.5.217	Roye		MP112	5.80A.020	Not Connected			No Misma	2009-11
6	10.7.5.214	10.7.5.214	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-11
7	10.7.5.211	10.7.5.211	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-11
8	10.7.5.222	10.7.5.222	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-11
9	10.7.5.215	10.7.5.215	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-11

Reader's Notes

13 Appendix C - Daylight Saving Time (DST)

This section 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.

v5.6 fully supports new DST settings.

Patches are applied automatically for the EMS Standard 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, refer to 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.

13.1 EMS Client

To apply new DST settings to EMS client, update both the Windows operating system and the Java version (refer to Section 16.1.1 and Section 16.1.2).

13.2 Windows

Install Windows OS patches as specified in the following URL:

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

13.2.1 Java

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:

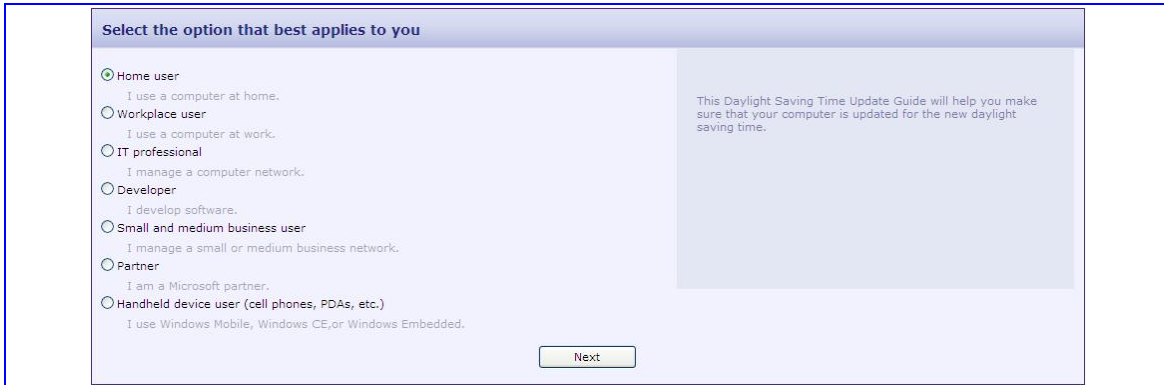
```
java -jar tzupdater.jar -f -bc -v
```

Refer to Section 16.3 on page 98 for an example of installing the Java patch for the EMS client.

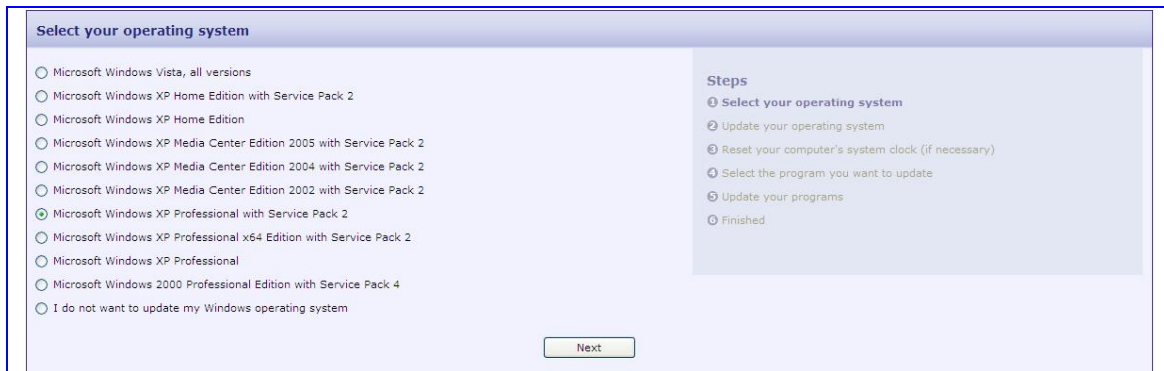
13.3 Example of Installing Windows Patches on the EMS Client

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 (refer to Figure 16-1).

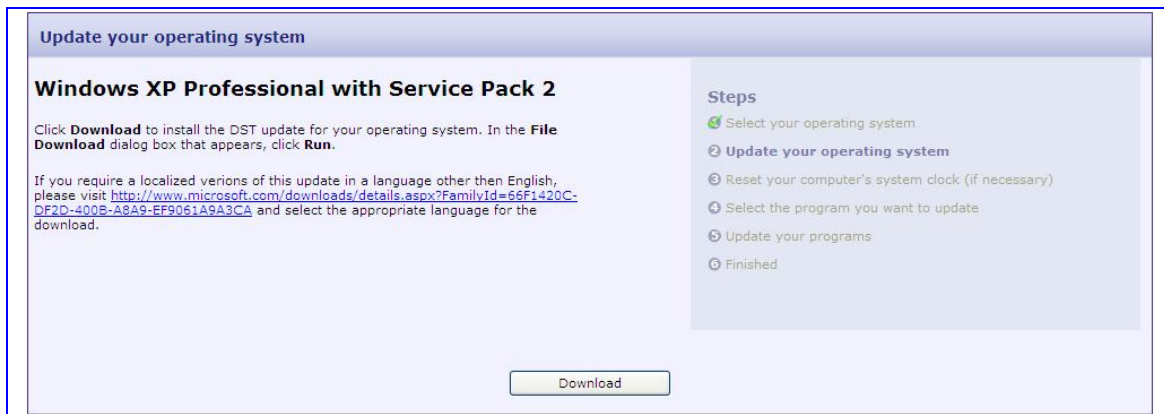
Figure 13-1: Installing Windows OS Patches – PC Information



3. Select your operating system information.

Figure 13-2: Installing Windows OS Patches – Selecting the Operating System

4. Download and install the patch.

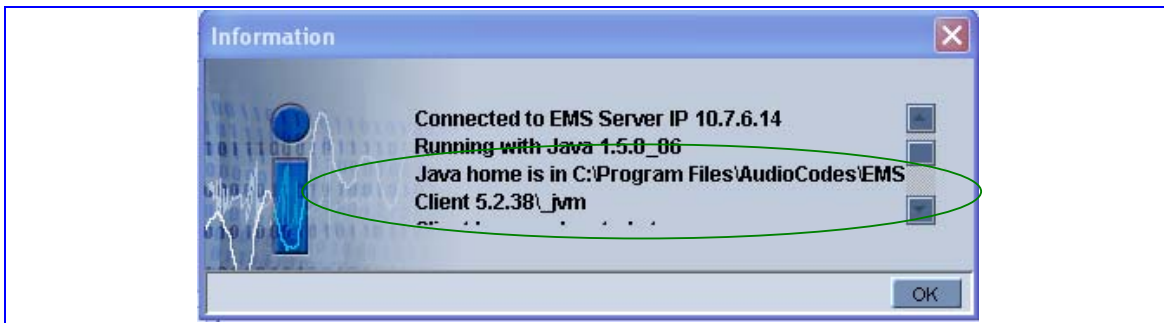
Figure 13-3: Installing Windows OS Patches – Download and Install

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

13.4 Example of Installing the Java Patch for the EMS Client

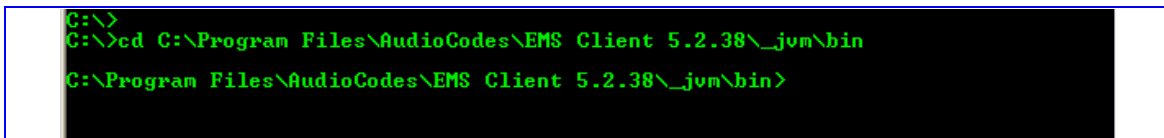
1. Open the EMS client.
2. Open the menu option Help>About to determine the home directory of the Java installation that the EMS client uses (refer to Figure 16-4).

Figure 13-4: Java Installation’s Home Directory



3. Copy the Java patch file **tzupdater.jar** from the EMS software CD/DVD in the folder \Documentation\Patches and place it in the directory **bin** under the Java home directory, whose path can be determined according to the instruction in step 2 (preceding).
4. 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 2 (preceding) (refer to Figure 16-5).

Figure 13-5: Changing the Directory to ‘bin’



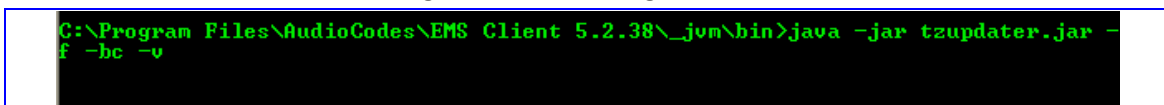
5. Install the patch (refer to Figure 16-6) by running command:

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



Note: It’s important to manually input the command into the Command Line window and not to copy it.

Figure 13-6: Installing the Patch



14 Appendix D - OpenCA OCSP Daemon (OCSPD) v1.5.2

14.1 Overview

OpenCA OCSP Daemon (OCSPD) is an RFC2560 compliant OCSP responder. It can be used to verify the statuses of MEGACO/SIP device certificates via OCSP on-line protocol. The OCSP Responder Server verifies in the CA Certificate Revocation List (CRL) whether the certificates installed on these devices are genuine and valid.

The following functionality is provided by OpenCA OCSPD:

- CRL retrieval via HTTP, HTTPS and LDAP protocols
- Support for multiple CAs (one CRL per CA)
- Periodic reload of the CRL file

14.2 Installation

OpenCA OCSPD package may be installed on any SPARC machine with Solaris 9 or 10 OS.

➤ **To install OpenCA OCSPD, take the following steps:**

1. Copy `ocspd.1.5.2-sparc-local.gz` installation package to the `/tmp` directory
2. Uncompress installation package:

```
gzip -d /tmp/ocspd.1.5.2-sparc-local.gz
```

3. Install OCSPD package:

```
pkgadd -d /tmp/ocspd.1.5.2-sparc-local
```

14.3 Viewing OCSPD Logs

OCSPD produces its operational and debugging logs via SYSLOG interface; all messages are associated with the daemon facility. During OCSPD installation SYSLOG server is automatically configured to store these logs in `/var/log/daemon` file.

Use standard UNIX tools to view OCSPD logs, e.g.:

```
tail -f /var/log/daemon
```

14.4 Starting/Stopping OCSPD

OCSPD is automatically started after reboot (via `/etc/rc2.d/S90ocspd` script). In addition to that, you may use the following commands to start/stop OCSPD (e.g. upon configuration change):

- To start OCSPD, use `/etc/init.d/ocspd-control start`
- To start OCSPD in debug mode, use `/etc/init.d/ocspd-control start-debug`
- To stop OCSPD, use `/etc/init.d/ocspd-control stop`
- To view status of OCSPD (running/stopped), use `/etc/init.d/ocspd-control status`

14.5 Verifying OCSPD Installation

OCSPD is installed in a “demo configuration” mode, with a self-signed certificate and a demoCA. This configuration is intended for demonstration purposes only. For real deployments, you must modify the OCSPD configuration as described in the following section.

In the “demo configuration” mode a sample local CA – demoCA – is installed in `/usr/local/etc/ocspd/demoCA` directory. Three certificates are created at installation time:

- `ca_cert.pem` – certificate of the demoCA itself
- `test1_cert.pem` – certificate of the 1st client (not revoked)
- `test2_cert.pem` – certificate of the 2nd client (revoked)

To verify OCSPD installation, run the following commands in the “demo configuration” and check the produced output:

```
cd /usr/local/etc/ocspd/demoCA/
```

```
/usr/local/ssl/bin/openssl ocspl -issuer ca cert.pem -cert
test1_cert.pem -noverify -url http://127.0.0.1:2560
test1_cert.pem: good
    This Update: Oct 29 14:36:03 2007 GMT
    Next Update: Oct 29 15:12:33 2007 GMT
/usr/local/ssl/bin/openssl ocspl -issuer ca cert.pem -cert
test2_cert.pem -noverify -url http://127.0.0.1:2560
test2_cert.pem: revoked
    This Update: Oct 29 14:36:03 2007 GMT
    Next Update: Oct 29 15:12:21 2007 GMT
    Revocation Time: Oct 29 14:36:03 2007 GMT
```

14.6 Configuring OCSPD

OCSPD configuration is stored in `/usr/local/etc/ocspd/ocspd.conf` file. Edit this file after OCSPD package installation and configure location of CRL and CA Certificates.

The `ocspd.conf` file has extensive comments and therefore is self-explainable. Nevertheless we provide a few recipes below for the most typical configurations.

For a simple configuration, where only one CA is supported, and CRL and CA certificate are retrieved via HTTP protocol, perform the following changes in `ocspd.conf` file:

1. Choose the correct database configuration section by un-commenting the “`dbms = dbms_http`” and commenting out “`dbms = dbms_file`” line.
2. In the `[dbms_http]` section, make sure that the 1st line – “`0.ca = @http_ca_1`” is un-commented.
3. In the `[http_ca_1]` section, change `crl_url` and `ca_url` parameters to point to the correct URLs where Certificates Revocation List (CRL) and CA Certificates are published. Use the following syntax when specifying URL:

Error! Hyperlink reference not valid.

For a configuration where two CAs are supported, and CRL and CA certificate are retrieved via the HTTPS protocol, perform the following changes in `ocspd.conf` file:

4. Choose the correct database configuration section by removing comments for the “`dbms = dbms_http`” line and commenting out “`dbms = dbms_file`” line??.
5. In the `[dbms_http]` section, ensure that comments are removed for the 1st – “`0.ca = @http_ca_1`” and the 2nd – “`1.ca = @http_ca_2`” lines.
6. In the `[http_ca_1]` section, change the `crl_url` and `ca_url` parameters to point to the correct URLs, where Certificates Revocation List (CRL) and CA Certificates are published by the 1st CA. Use the following syntax when specifying URL:

Error! Hyperlink reference not valid.

7. In the `[http_ca_2]` section, change `crl_url` and `ca_url` parameters to point to the correct URLs, where Certificates Revocation List (CRL) and CA Certificates are published by the 2nd CA.

In addition to the above-described configuration, it is recommended to generate a valid certificate for the OCSP Responder signed by a genuine CA, instead of the self-signed certificate created during the OCSPD package installation. To do so, take the following steps:

8. Generate Certificate Signing Request (CSR) via the following commands:

```
cd /usr/local/etc/ocspd/private
/usr/local/ssl/bin/openssl req -new -key ocspd key.pem -out
/tmp/ocspd.csr
```

9. Submit the generated CSR file – `/tmp/ocspd.csr` – to the CA. In response, you will receive a certificate file signed by this CA.
10. Place the certificate signed by the CA, together with the certificate of the CA itself, into the `/usr/local/etc/ocspd/certs` directory.

11. Update the **ocspd_certificate** and **ca_certificate** parameters in the **ocspd.conf** file to point to the new certificate files.
 - To activate new configuration, restart the OCSP Responder via the following command:

```
/etc/init.d/ocspd-control restart
```

15 Appendix E - Security Certificates Signing Procedure

15.1 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.



Note: The procedures described in this section are relevant for customers who have installed EMS server version 5.8.55 or higher.

15.1.1 Mediant 3000 and MediaPack

For the Mediant 3000 and the MediaPack, when working in *secure mode* (*HTTPS* enabled), the “AudioCodes-issued” certificates **must** be replaced with the external CA certificates (as described in this section). In addition, the external CA certificates must also be loaded on the Mediant 3000 and MediaPack devices (for more information, see section “Server Certificate Replacement” in the MP-11x and MP-124 SIP User’s Manual and in the Mediant 3000, TP-8410 and TP-6310 SIP User’s Manual).



Note: When working in *secure mode* (*HTTPS* enabled), failure to replace the “AudioCodes-issued” certificates with the external CA certificates will result in a failure of the software upgrade and will prevent the files upload features from functioning.

15.2 Installing External CA Certificates on the EMS Server

On the EMS Server, external CA certificates must be installed separately on the Apache Web Server, the RMI Server and the Watchdog applications. 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 data base.



Note: In future versions, to upgrade the external CA certificates, it will not be necessary to repeat the procedures described in this section. Instead, the EMS Server upgrade script will provide an option to automatically upgrade the NSS databases with the external CA certificates from a previous version.

➤ 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. Remove the old/default Certificates Database and create a temporary noise file for key generation.

```
rm -Rf /opt/nss/fipsdb
rm -Rf /ACEMS/server 5.6.96/externals/security/serverNssDb
rm -Rf
/ACEMS/server_5.6.96/externals/security/watchDogNssDb

( ps -elf ; date ; netstat -a ) > /tmp/noise
```

4. Create a new empty Certificates Database and corresponding password files.

```
mkdir -p /opt/nss/fipsdb
chmod -R o+r /opt/nss/fipsdb
mkdir -p
/ACEMS/server_5.6.96/externals/security/serverNssDb
mkdir -p
/ACEMS/server_5.6.96/externals/security/watchDogNssDb

echo httpptest > /tmp/apachePwdFile.txt
echo fips140-2 > /tmp/rmiPwdFile.txt

/opt/nss/nss-3.11.4/bin/certutil -N -d /opt/nss/fipsdb -f
/tmp/apachePwdFile.txt
/opt/nss/nss-3.11.4/bin/certutil -N -d
/ACEMS/server 5.6.96/externals/security/serverNssDb -f
/tmp/rmiPwdFile.txt
/opt/nss/nss-3.11.4/bin/certutil -N -d
/ACEMS/server_5.6.96/externals/security/watchDogNssDb
-f /tmp/rmiPwdFile.txt
```


5. Create certificate requests files (CSRs) to transfer to the external CA for signing.

```
/opt/nss/nss-3.11.4/bin/certutil -R -d /opt/nss/fipsdb -s
"CN=EMS Server (Apache), O=AudioCodes, C=US" -a -o
/tmp/apachereq.csr -g 1024 -f /tmp/apachePwdFile.txt -z
/tmp/noise
```

```
/opt/nss/nss-3.11.4/bin/certutil -R -d
/ACEMS/server 5.6.96/externals/security/serverNssDb -s
"CN=EMS Server, O=AudioCodes" -a -o /tmp/serverreq.csr -f
/tmp/rmiPwdFile.txt -z /tmp/noise
```

```
/opt/nss/nss-3.11.4/bin/certutil -R -d
/ACEMS/server 5.6.96/externals/security/watchDogNssDb -s
"CN=EMS Client,O=AudioCodes" -a -o /tmp/watchdogreq.csr -f
/tmp/rmiPwdFile.txt -z /tmp/noise
```

6. Transfer the CSRs to the external CA for signing and receive them back.

Transfer the generated CSRs - /tmp/apachereq.csr, /tmp/serverreq.csr, /tmp/watchdogreq.csr - from the EMS server to your PC (via SFTP or SCP) and pass it to the Certificate Authority.

You should receive back 4 files: your signed certificates (let's call them apachecert.pem, servercert.pem, watchdogcert.pem) and certificate of trusted authority (let's call it ca.pem).

Now transfer these 4 files back to the EMS server under /tmp directory and use the following commands to import the files into the EMS server's NSS databases of both server and watchdog:

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

```
/opt/nss/nss-3.11.4/bin/modutil -fips false -dbdir
/opt/nss/fipsdb
/opt/nss/nss-3.11.4/bin/modutil -fips false -dbdir
/ACEMS/server_5.6.96/externals/security/serverNssDb
/opt/nss/nss-3.11.4/bin/modutil -fips false -dbdir
/ACEMS/server_5.6.96/externals/security/watchDogNssDb
```

```
/opt/nss/nss-3.11.4/bin/certutil -A -d /opt/nss/fipsdb -n
Server-Cert -t u,u,u -a -i /tmp/apachecert.pem -f
/tmp/apachePwdFile.txt
```

```
/opt/nss/nss-3.11.4/bin/certutil -A -d
/ACEMS/server 5.6.96/externals/security/serverNssDb -n
servercert -t u,u,u -a -i /tmp/servercert.pem -f
/tmp/rmiPwdFile.txt
```

```
/opt/nss/nss-3.11.4/bin/certutil -A -d
/ACEMS/server 5.6.96/externals/security/watchDogNssDb -n
clientcert -t u,u,u -a -i /tmp/watchdogcert.pem -f
/tmp/rmiPwdFile.txt
```

```
/opt/nss/nss-3.11.4/bin/certutil -A -d /opt/nss/fipsdb -n
ca -t CTu,CTu,CTu -a -i /tmp/ca.pem -f
/tmp/apachePwdFile.txt
```

```

/opt/nss/nss-3.11.4/bin/certutil -A -d
/ACEMS/server 5.6.96/externals/security/serverNssDb -n
cacert -t CT,CT,CT -a -i /tmp/ca.pem -f /tmp/rmiPwdFile.txt
/opt/nss/nss-3.11.4/bin/certutil -A -d
/ACEMS/server 5.6.96/externals/security/watchDogNssDb -n
cacert -t CT,CT,CT -a -i /tmp/ca.pem -f /tmp/rmiPwdFile.txt
    
```

```

/opt/nss/nss-3.11.4/bin/modutil -fips true -dbdir
/opt/nss/fipsdb

/opt/nss/nss-3.11.4/bin/modutil -fips true -dbdir
/ACEMS/server_5.6.96/externals/security/serverNssDb
/opt/nss/nss-3.11.4/bin/modutil -fips true -dbdir
/ACEMS/server_5.6.96/externals/security/watchDogNssDb
    
```

8. Cleanup temporary files.

```

rm /tmp/apachePwdFile.txt /tmp/rmiPwdFile.txt /tmp/noise
/tmp/apachecert.pem /tmp/servercert.pem
/tmp/watchdogcert.pem /tmp/ca.pem /tmp/apachereq.csr
/tmp/serverreq.csr /tmp/watchdogreq.csr
    
```

9. Restart the Apache Web Server.

```

/usr/local/apache2/bin/apachectl stop
echo "httpstest" | /usr/local/apache2/bin/apachectl start
    
```

10. Restart the EMS server using the EMS Manager.

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

```
"C:\Program Files\AudioCodes\EMS Client
5.6.96\lib\modutil.exe" -fips false -dbdir "C:\Program
Files\AudioCodes\EMS Client
5.6.96\externals\security\clientNssDb"
```

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

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

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

7. Remove the temporary files (C:\pwdfile.txt, C:\noise, C:\clientcert.pem, C:\ca.pem, and C:\clientreq.csr).
8. Restart the EMS client.

15.3.1 Installing External CA Certificates on a Later EMS 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.

15.4 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.

15.5 Certificate Integration on Web Browser Side (Northbound Interface)

For the client PC to operate with a web browser and / or NMS system and communicate with the EMS server via HTTPS, it should obtain 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.

Reader's Notes

16 Appendix F – EMS Application Acceptance Tests

16.1 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 in order 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.

16.2 Configuration

16.2.1 Client Installation

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

16.2.2 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 Server with the EMS client	The connection should succeed.



16.2.3 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.



16.2.4 Add Media Gateway

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.



16.2.5 Provisioning – M5K/ M8K

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.





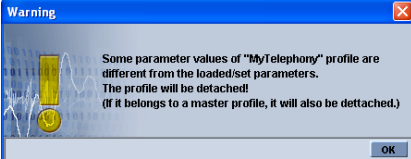
16.2.6 Provisioning – MP/ M1K/ M2K/ M3K

Step Name	Description	Expected Result
Go to network frame	Click on the network button.	Network configuration is displayed.
RTP Settings tab	Press on the application tab	Applications setting is 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	Set the parameter back to your NTP Server IP address.	The old value was restored.

16.2.7 Entity Profile – M1K Digital/M2K/M3K/ M5K/M8K

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 succeed 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.

16.2.8 Entity Profile – MP/M1K Analog

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 press Apply .	A detach profile pop up message is displayed. 

16.2.9 Create Master Profile

Step Name	Description	Expected Result
Go to Board/ MG level	Drill to board/ MG level	Board/ Media Gateway status is displayed.
Create master profile	Right click >> Create Master profile	Profile name pop up appears.
Attach Profile	Choose name	A new profile was attached to the Media Gateway.

16.2.10 Remove & Add MG

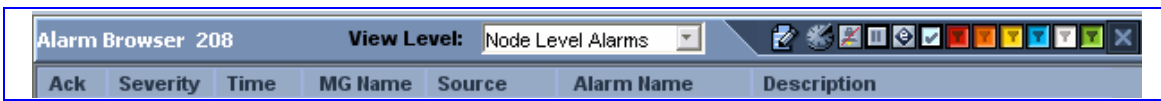
Step Name	Description	Expected Result
Remove MG	Remove the MG from the EMS	The Media Gateway was removed from the GUI.
Add MG	Add MG to the EMS	The Media Gateway is displayed in the EMS GUI.

16.2.11 Apply Master Profile

Step Name	Description	Expected Result
Go to Board/ MG level	Drill to board/ MG level	Board/ Media Gateway status appears
Apply Master Profile	Right Click >> Apply Master Profile	The Master profile that you created is attached to the board/ Media Gateway.

16.3 Faults

16.3.1 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.

16.3.2 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 is empty.

16.3.3 Acknowledge Alarm

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

16.3.4 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.

16.4 Security

16.4.1 Adding Operator

Step Name	Description	Expected Result
Add	Add a new operator and press the OK key in the screen.	Verify the new operator was added to the operators table frame.

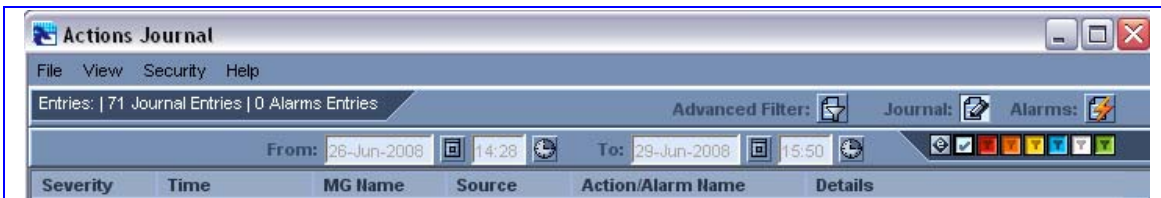
16.4.2 Non Repetitive Passwords

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."

16.4.3 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.

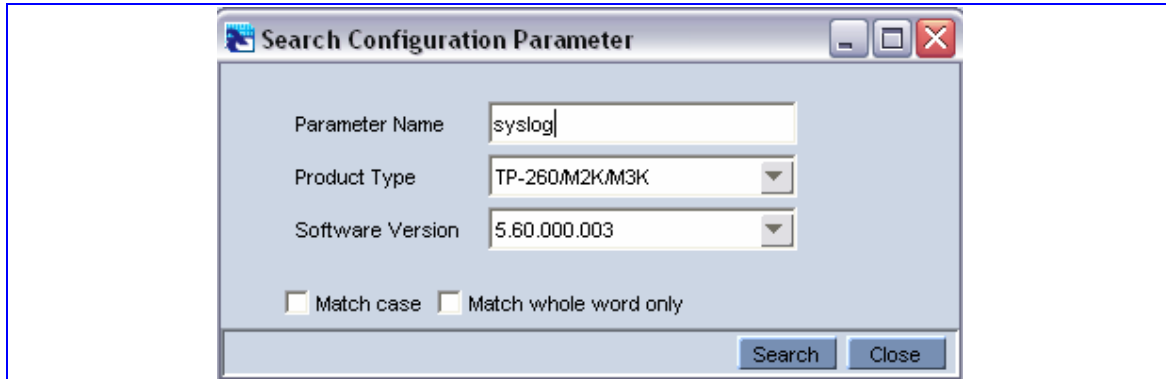
16.4.4 Journal Activity



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.

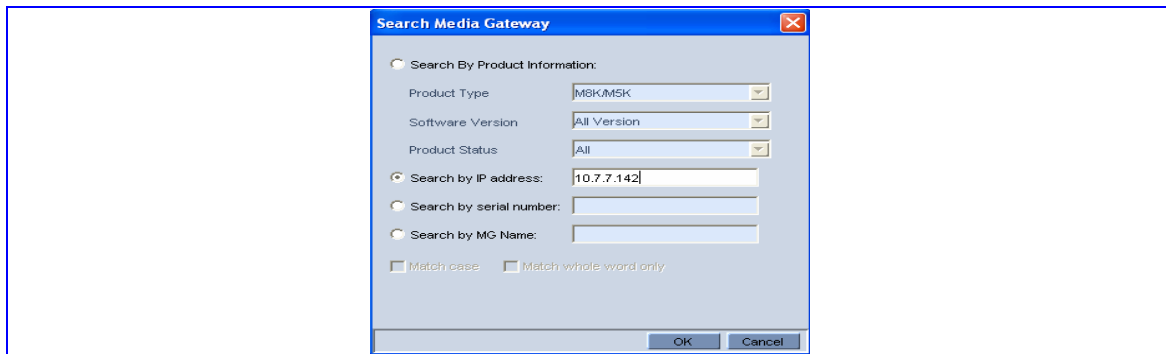
16.5 Utilities

16.5.1 Provisioning Parameter Search



Step Name	Description	Expected Result
Search Box	Open the search parameter tool Tools >> Search configuration	Search parameter tool opens.
Parameter syslog	Search the parameter syslog	A list of all relevant parameters with the search string opens.

16.5.2 MG Search



Step Name	Description	Expected Result
Search Box	Open search MG tool Tools >> Search MG	Search MG tool opens.
IP	Search /MG/Unknown machine by IP address	Show the MG status screen.

16.5.3 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.

16.5.4 Backup & 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.

EMS for AudioCodes' Media Gateways and Servers

AudioCodes EMS Element Management System

**Element Management System (EMS) Server
Installation, Operation and Maintenance Manual**

Version 5.8

Document #: LTRT- 94124

