

# EMS for AudioCodes Media Gateways and Servers

EMS

Element Management System

## Installation, Operation and Maintenance Manual

### Element Management System (EMS) Server

Version 6.6





---

## Table of Contents

---

<b>1</b>	<b>Overview .....</b>	<b>19</b>
<hr/>		
<b>Part I: Pre-installation Information .....</b>		<b>21</b>
<b>2</b>	<b>Component Information.....</b>	<b>23</b>
	2.1.1 Managed Devices for All EMS Server Versions .....	23
	2.1.2 SEM Monitored Devices .....	23
	2.1.3 SEM Server Disk Requirements .....	24
<b>3</b>	<b>Hardware and Software Requirements.....</b>	<b>25</b>
	<b>3.1 EMS Server and Client Requirements .....</b>	<b>25</b>
	<b>3.2 EMS and SEM Bandwidth Requirements.....</b>	<b>27</b>
	3.2.1 EMS Bandwidth Requirements.....	27
	3.2.2 SEM Bandwidth Requirements.....	28
<b>4</b>	<b>EMS Software Deliverables .....</b>	<b>29</b>
	<b>4.1 Dedicated Hardware Installation – DVDs 1-4.....</b>	<b>29</b>
	<b>4.2 VMware vSphere Installation– DVD 5 .....</b>	<b>30</b>
<hr/>		
<b>Part II: EMS Server Installation.....</b>		<b>31</b>
<b>5</b>	<b>Testing Installation Requirements -Dedicated Hardware .....</b>	<b>33</b>
	<b>5.1 Hardware Requirements .....</b>	<b>33</b>
	5.1.1 Testing Hardware Requirements on the Solaris Platform.....	33
	5.1.2 Testing Hardware Requirements on the Linux Platform .....	35
<b>6</b>	<b>Installing the EMS Server on Dedicated Hardware.....</b>	<b>37</b>
	<b>6.1 Installing the EMS Server on the Solaris Platform .....</b>	<b>38</b>
	6.1.1 DVD1: Solaris 10 Rev 7 / Rev 8 Installation .....	38
	6.1.1.1 Accessing the OK Prompt.....	38
	6.1.1.2 Installing the Solaris 10 Operating System.....	40
	6.1.2 DVD2: Oracle DB Installation .....	42
	6.1.3 DVD3: EMS Server Application Installation .....	44
	<b>6.2 Installing the EMS Server on the Linux Platform.....</b>	<b>48</b>
	6.2.1 DVD1: Linux CentOS 5.3 and CentOS 5.9 .....	48
	6.2.2 DVD2: Oracle DB Installation .....	50
	6.2.3 DVD3: EMS Server Application Installation .....	52
	<b>6.3 EMS Server Users.....</b>	<b>55</b>
<b>7</b>	<b>Installing the EMS Server on the VMware Platform.....</b>	<b>57</b>
<hr/>		
<b>Part III: EMS Server Upgrade .....</b>		<b>67</b>

<b>8</b>	<b>Upgrading the EMS Server on Dedicated Hardware .....</b>	<b>69</b>
8.1	Upgrading the EMS Server on the Solaris Platform .....	70
8.2	Upgrading the EMS Server on the Linux Platform.....	74
8.3	Upgrading from the Installation TAR file.....	77
<b>9</b>	<b>Upgrading the EMS Server on the VMware Platform .....</b>	<b>79</b>
<hr/>		
<b>Part IV: EMS Server Machine Maintenance .....</b>		<b>81</b>
<b>10</b>	<b>EMS Server Manager.....</b>	<b>83</b>
10.1	General Info and Logs Collection .....	88
10.1.1	General Info.....	88
10.1.2	Collecting Logs .....	91
10.2	Networking.....	92
10.2.1	Change Server's IP Address.....	92
10.2.2	Add SNMP Manager.....	94
10.2.3	Configure Ethernet Interfaces.....	95
10.2.3.1	EMS Client Login on all EMS server Network Interfaces .....	95
10.2.3.2	Add Interface .....	97
10.2.3.3	Remove Interface .....	98
10.2.3.4	Modify Interface .....	99
10.2.4	Configure Ethernet Redundancy on Solaris .....	100
10.2.4.1	Add Redundant Interface.....	102
10.2.4.2	Remove Ethernet Redundancy .....	103
10.2.4.3	Modify Redundant Interface .....	104
10.2.5	Configure Ethernet Redundancy on Linux.....	105
10.2.5.1	Add Redundant Interface.....	106
10.2.5.2	Remove Ethernet Redundancy .....	107
10.2.5.3	Modify Redundant Interface .....	108
10.2.6	Configure the DNS Client .....	109
10.2.7	Static Routes .....	111
10.2.8	SNMP Agent.....	113
10.2.8.1	SNMP Manager Configuration.....	114
10.2.8.2	Sending System Alarms .....	114
10.2.8.3	Stopping System Alarms .....	114
10.2.9	Configure NAT .....	115
10.2.10	Configure Server SNMPv3 Engine ID.....	116
10.3	Security .....	118
10.3.1	Basic Hardening .....	119
10.3.1.1	Start Basic Hardening.....	121
10.3.1.2	Rollback.....	122
10.3.2	Advanced Hardening .....	124
10.3.3	SSL Tunneling Configuration .....	125
10.3.3.1	EMS Client-SSL Tunneling Configuration .....	126
10.3.4	Strict PKI Configuration .....	127
10.3.5	SSH Server Configuration Manager .....	128
10.3.5.1	Configure SSH Log Level .....	129
10.3.5.2	Configure SSH Banner .....	130
10.3.5.3	Configure SSH on Ethernet Interfaces .....	132
10.3.5.4	Disable SSH Password Authentication.....	136
10.3.5.5	Enable SSH IgnoreUserKnownHosts Parameter .....	138
10.3.5.6	Configure SSH Allowed Hosts.....	139



10.3.6	Changing DBA Password .....	149
10.3.7	OS Passwords Settings .....	150
10.3.7.1	General Password Settings .....	151
10.3.7.2	Operating System Users Security Extensions .....	153
10.3.8	Add EMS User .....	155
10.3.9	Start / Stop File Integrity Checker .....	156
10.3.10	Network Options .....	156
10.3.11	Start/Stop Software Integrity Checker (AIDE) and Pre-linking .....	158
10.3.12	Enable/Disable USB Storage .....	159
10.3.13	Auditd Options .....	160
<b>10.4</b>	<b>Maintenance .....</b>	<b>161</b>
10.4.1	Configure NTP .....	162
10.4.2	Change System Timezone .....	163
10.4.3	Change System Time and Date .....	165
10.4.4	Start /Stop the EMS Server .....	166
10.4.5	Web Server Configuration .....	166
10.4.5.1	Changing the JAWS Login Interface .....	168
10.4.6	Backup the EMS Server .....	169
10.4.7	Schedule Backup for the EMS Server .....	171
10.4.7.1	Schedule New Backup .....	172
10.4.7.2	View Scheduled Backups .....	173
10.4.7.3	Remove Scheduled Backup .....	174
10.4.7.4	Set Number of Scheduled Backups to Save .....	175
10.4.8	Restore the EMS Server .....	176
10.4.9	Reboot the EMS Server .....	178
10.4.10	HA (High Availability) Configuration .....	179
10.4.10.1	HA Overview .....	179
10.4.10.2	EMS HA Pre-requisites .....	181
10.4.10.3	EMS HA Data Synchronization .....	182
10.4.10.4	EMS HA Configuration .....	183
10.4.10.5	EMS Server Manual Switchover .....	191
10.4.10.6	EMS HA Uninstall .....	192
10.4.10.7	EMS HA – General Information .....	194
10.4.11	Syslog Configuration .....	199
10.4.12	Board Syslog Logging Configuration .....	201
10.4.13	TP Debug Recording Configuration .....	202

---

## **Part V: Configuring the Firewall and Installing the EMS Client .....**

<b>11</b>	<b>Configuring the Firewall .....</b>	<b>207</b>
<b>12</b>	<b>Installing the EMS Client .....</b>	<b>211</b>
12.1	Installing the EMS Client on a Client PC or Laptop .....	211
12.2	Running the EMS on a Client PC or Laptop .....	212
12.3	Initial Login .....	213
12.4	Installing and Running the EMS Client on a Client PC using Java Web Start (JAWS) .....	214

---

## **Part VI: Appendices .....**

<b>A</b>	<b>Frequently Asked Questions (FAQs)</b> .....	<b>217</b>
A.1	SC> Prompt Displayed in User Console on Sun Solaris.....	217
A.2	After installing JAWS - the EMS application icon is not displayed on the desktop.....	217
A.3	After Rebooting the Machine.....	218
A.4	Changes Not Updated in the Client.....	219
A.5	Removing the EMS Server Installation.....	219
<b>B</b>	<b>Site Preparation</b> .....	<b>221</b>
<b>C</b>	<b>Daylight Saving Time (DST)</b> .....	<b>223</b>
C.1	EMS Client.....	224
C.2	Windows.....	224
C.2.1	Java.....	224
C.3	Example of Installing Windows Patches on the EMS Client.....	225
<b>D</b>	<b>OpenCA OCSP Daemon (OCSPD) v1.5.2</b> .....	<b>227</b>
D.1	Overview.....	227
D.2	Installation.....	227
D.3	Viewing OCSPD Logs.....	227
D.4	Starting/Stopping OCSPD.....	228
D.5	Verifying OCSPD Installation.....	228
D.6	Configuring OCSPD.....	229
<b>E</b>	<b>Working with HTTPS</b> .....	<b>231</b>
E.1	Working with HTTPS on CPE Media Gateways.....	231
E.2	Working with HTTPS for JAWS and NBIF.....	233
<b>F</b>	<b>External Security Certificates-Signing Procedure</b> .....	<b>235</b>
F.1	Overview.....	235
F.2	Installing External CA Certificates on the EMS Server.....	235
F.3	Installing External CA Certificates on the EMS Client.....	237
F.4	Installing External CA Certificates on the JAWS EMS Client.....	239
F.5	Installing External CA Certificates on a Later EMS Client or JAWS Client.....	241
F.6	Client – Server Communication Test.....	241
F.7	Certificate Integration on Web Browser Side (Northbound Interface).....	241
<b>G</b>	<b>EMS Client and Server Certificates Extensions and DoD PKI</b> .....	<b>243</b>
G.1	DoD PKI Validation Extensions.....	243
G.1.1	The CA Trust Chain.....	243
G.1.2	DoD PKI Strict Validations.....	244
G.1.3	Debugging.....	245
G.2	DoD PKI and Certificate Management Extension.....	245
G.2.1	SSL Handshake Process.....	245
G.2.2	NSS Database Parameters.....	245
G.2.3	HTTPS Client.....	246

---

G.2.4	DoD PKI Strict Validations .....	246
G.2.5	Debugging .....	247
<b>H</b>	<b>RAID 1 Configuration in Oracle/Sun Netra T5220 .....</b>	<b>249</b>
<b>I</b>	<b>EMS Application Acceptance Tests.....</b>	<b>255</b>
<b>I.1</b>	<b>Introduction.....</b>	<b>255</b>
<b>I.2</b>	<b>Configuration .....</b>	<b>255</b>
I.2.1	Client Installation .....	255
I.2.2	Server Installation .....	256
I.2.3	Add Auxiliary File .....	256
I.2.4	Add Media Gateway .....	256
I.2.5	Provisioning – Mediant 5000/ Mediant 8000.....	257
I.2.6	Provisioning – CPE Devices .....	257
I.2.7	Entity Profile – Digital CPE Devices .....	258
I.2.8	Entity Profile – Analog CPE Devices .....	259
<b>I.3</b>	<b>Faults.....</b>	<b>260</b>
I.3.1	Alarm Receiver .....	260
I.3.2	Delete Alarms .....	260
I.3.3	Acknowledge Alarm .....	260
I.3.4	Forwarding Alarms.....	261
<b>I.4</b>	<b>Security .....</b>	<b>262</b>
I.4.1	Users List.....	262
I.4.2	Non Repetitive Passwords.....	262
I.4.3	Removing Operator .....	262
I.4.4	Journal Activity.....	263
<b>I.5</b>	<b>Utilities .....</b>	<b>264</b>
I.5.1	Configuration Parameter Search .....	264
I.5.1.1	Basic Search.....	264
I.5.1.2	Advanced MG Search.....	265
I.5.2	MG Search.....	266
I.5.3	Online Help .....	267
I.5.4	Backup and Recovery.....	267

---

## List of Figures

---

Figure 5-1: Solaris Testing Requirements .....	34
Figure 5-2: Linux Testing Requirements .....	35
Figure 6-1: Sun Server Power Button .....	39
Figure 6-2: Installing Solaris 10-Current Configuration .....	40
Figure 6-3: Oracle DB Installation-Solaris .....	42
Figure 6-4: Oracle DB Installation-Solaris-License Agreement.....	42
Figure 6-5: SYS Password Prompt .....	43
Figure 6-6: Complete Oracle DB Installation (Solaris) .....	43
Figure 6-7: EMS Server Application Installation (Solaris) .....	44
Figure 6-8: EMS Server Installation (Solaris) - License Agreement.....	44
Figure 6-9: EMS Server Installation (Solaris) - Patches Installation .....	45
Figure 6-10: EMS Server Installation (Solaris) – Java License Agreement .....	45
Figure 6-11: EMS Server Installation (Solaris) – Java Installation (cont).....	45
Figure 6-12: EMS Server Installation (Solaris) – Java License Agreement .....	46
Figure 6-13: EMS Server Installation (Solaris) Java Installation (cont).....	46
Figure 6-14: EMS Server Installation (Solaris) Java Installation Complete .....	46
Figure 6-15: Linux CentOS Installation .....	48
Figure 6-16: Linux CentOS Installation Complete .....	49
Figure 6-17: Linux CentOS Network Configuration.....	49
Figure 6-18: Oracle DB Installation (Linux) .....	50
Figure 6-19: Oracle DB Installation - License Agreement (Linux).....	51
Figure 6-20: Oracle DB Installation (Linux) (cont).....	51
Figure 6-21: Oracle DB Installation (Linux) (cont).....	51
Figure 6-22: EMS Server Application Installation (Linux).....	52
Figure 6-23: EMS Server Application Installation (Linux) – License Agreement .....	53
Figure 6-24: EMS Server Application Installation (Linux) (cont) .....	53
Figure 6-25: EMS Server Application Installation (Linux) - Java Installation .....	54
Figure 6-26: EMS Server Application Installation (Linux) – Oracle CPU Patch .....	54
Figure 7-1: Deploy OVF Template Option.....	57
Figure 7-2: Open OVA Package.....	57
Figure 7-3: OVF Template Source Screen.....	58
Figure 7-4: OVF Template Details Screen .....	58
Figure 7-5: Virtual Machine Name and Location Screen .....	59
Figure 7-6: Host / Cluster Screen .....	59
Figure 7-7: Destination Storage Screen .....	60
Figure 7-8: Disk Format Screen .....	60
Figure 7-9: Ready to Complete Screen.....	61
Figure 7-10: Deployment Progress Screen .....	61
Figure 7-11: Edit Settings option .....	62
Figure 7-12: Hard Disk Settings .....	62
Figure 7-13: Power On .....	63
Figure 7-14: vSphere Client Console .....	63
Figure 7-15: EMS Server Manager Prompt.....	64
Figure 7-16: Element Management System Menu Option .....	64

Figure 7-17: EMS Server Network Configuration Details .....	65
Figure 7-18: SSH Client Login .....	65
Figure 7-19: EMS Server Manager - Main Menu .....	66
Figure 8-1: EMS Server Upgrade (Solaris) .....	70
Figure 8-2: EMS Server Upgrade (Solaris)- License Agreement .....	71
Figure 8-3: EMS Server Upgrade (Solaris) – Patch Installation .....	71
Figure 8-4: EMS Server Upgrade (Solaris) - License Agreement (Java) .....	72
Figure 8-5: EMS Server Upgrade (Solaris) - License Agreement (Java) (cont) .....	72
Figure 8-6: EMS Server Upgrade (Solaris) - License Agreement (Java) (cont) .....	73
Figure 8-7: EMS Server Upgrade (Java) (cont) .....	73
Figure 8-8: EMS Server Upgrade (Solaris) Complete .....	73
Figure 8-9: EMS Server Upgrade (Linux) .....	74
Figure 8-10: EMS Server Upgrade (Linux) – License Agreement .....	75
Figure 8-11: EMS Server Application Upgrade (Linux) - Java Installation .....	75
Figure 8-12: EMS Server Upgrade (Linux) Complete .....	76
Figure 8-13: EMS Server Upgrade from TAR File .....	77
Figure 9-1: Edit Settings Option .....	79
Figure 9-2: Hardware Tab .....	79
Figure 9-3: Connect/disconnect Button .....	80
Figure 9-4: EMS Server Installation Script .....	80
Figure 10-1: EMS Server Manager Menu (All options with SSH connection on Solaris) .....	84
Figure 10-2: Ems Server Manager Menu (Linux) .....	85
Figure 10-3: EMS Server Manager – General Info .....	89
Figure 10-4: General Info Display .....	89
Figure 10-5: General Info Display (cont) .....	90
Figure 10-6: EMS Server Manager – Collect Logs .....	91
Figure 10-7: EMS Server Manager – Change Server's IP Address .....	92
Figure 10-8: Server IP Configuration Updates .....	93
Figure 10-9: User Configuration Updates .....	93
Figure 10-10: IP Configuration Complete .....	93
Figure 10-11: EMS Server Manager – Change Additional SNMP Manager's IP Address .....	94
Figure 10-12: Additional Manager's Configuration .....	94
Figure 10-13: EMS Server: Triple Ethernet Interfaces .....	95
Figure 10-14: EMS Server Manager – Configure Ethernet Interfaces .....	96
Figure 10-15: Physical Interface Configuration Menu .....	96
Figure 10-16: Modify Interface .....	99
Figure 10-17: Physical Ethernet Interfaces Redundancy .....	100
Figure 10-18: EMS Server Manager – Configure Ethernet Redundancy .....	101
Figure 10-19: Ethernet Redundancy Configuration Menu .....	101
Figure 10-20: Add Redundant Interface .....	102
Figure 10-21: Ethernet Redundancy Interface to Disable .....	103
Figure 10-22: Modify Redundant Interface .....	104
Figure 10-23: EMS Server Manager Ethernet Redundancy Configuration .....	105
Figure 10-24: Add Redundant Interface (Linux) .....	106
Figure 10-25: Ethernet Redundancy Interface to Disable .....	107
Figure 10-26: Modify Redundant Interface (Linux) .....	108

Figure 10-27: EMS Server Manager – Configure DNS Client.....	109
Figure 10-28: DNS Client Sub-menu.....	109
Figure 10-29: Configure DNS Client – Specify Domain Name/Search List .....	110
Figure 10-30: DNS Setup .....	110
Figure 10-31: EMS Server Manager – Static Routes .....	111
Figure 10-32: Routing Table and Menu.....	111
Figure 10-33: Static Route Changes .....	112
Figure 10-34: EMS Server Manager – Configure SNMP Agent.....	113
Figure 10-35: Solaris SNMP Manager .....	114
Figure 10-36: EMS Server Manager – Configure NAT .....	115
Figure 10-37: EMS Server Manager – Configure SNMPv3 Engine ID .....	116
Figure 10-38: EMS Server Manager – SNMPv3 Engine ID Configuration (cont) .....	116
Figure 10-39: SNMPv3 Engine ID Configuration – Complete Configuration .....	117
Figure 10-40: Basic Hardening Menu.....	120
Figure 10-41: Prompts Referring to SNMP Services .....	121
Figure 10-42: Activating the EMS Hardening Feature .....	122
Figure 10-43: Basic Hardening, Rollback - Open all Services .....	122
Figure 10-44: Rolling Back from Hardened Server - 1 .....	123
Figure 10-45: Rolling Back from Hardened Server - 2 .....	123
Figure 10-46: Rolling Back from Hardened Server - 3 .....	123
Figure 10-47: Activating the Advanced Hardening Feature .....	124
Figure 10-48: Rolling Back from Advanced Hardening .....	125
Figure 10-49: SSL Tunneling Configuration Manager.....	125
Figure 10-50: EMS Server Manager – Strict PKI Configuration.....	127
Figure 10-51: EMS Server Manager – Strict PKI Configuration (cont) .....	127
Figure 10-52: EMS Server Manager – SSH Configuration .....	128
Figure 10-53: SSH Configuration (cont).....	128
Figure 10-54: SSH Log Level Manager.....	129
Figure 10-55: SSH Log Level Manager Options .....	129
Figure 10-56: SSH Log Current Level .....	130
Figure 10-57: Configure SSH Banner .....	130
Figure 10-58: SSH Banner Manager.....	130
Figure 10-59: SSH Banner Manager State .....	130
Figure 10-60: SSH Banner Manager Configuration Complete.....	131
Figure 10-61: Configure SSH on Ethernet Interfaces .....	132
Figure 10-62: Configure SSH on Ethernet Interfaces (cont) .....	132
Figure 10-63: Ethernet Interfaces – SSH Manager.....	133
Figure 10-64: SSH Listener Status - ALL.....	133
Figure 10-65: Configurable Ethernet Interfaces .....	134
Figure 10-66: SSH Listener Status - YES .....	134
Figure 10-67: Removing Ethernet Interface .....	134
Figure 10-68: SSH Listener Status - NO .....	135
Figure 10-69: Configurable Ethernet Interfaces .....	135
Figure 10-70: Disable SSH Password Authentication.....	136
Figure 10-71: Disable SSH Password Authentication - Confirm.....	136
Figure 10-72: Enable SSH Password Authentication.....	137

---

Figure 10-73: Enable SSH Password Authentication -Confirm.....	137
Figure 10-74: Enable SSH IgnoreUserKnowHosts Parameter .....	138
Figure 10-75: SSH IgnoreUserKnowHosts Parameter - Confirm.....	138
Figure 10-76: SSH IgnoreUserKnowHosts Parameter - YES .....	138
Figure 10-77: SSH Allowed Hosts.....	139
Figure 10-78: Allow ALL Hosts.....	140
Figure 10-79: Allow ALL Hosts - Confirm.....	140
Figure 10-80: Allow ALL Hosts – Display Configuration .....	140
Figure 10-81: Deny ALL Hosts .....	141
Figure 10-82: Deny ALL Hosts - Confirm .....	141
Figure 10-83: Deny ALL Hosts – Display Configuration.....	141
Figure 10-84: Add Host /Subnet to Allowed Hosts.....	142
Figure 10-85: Add Host to Allowed List.....	142
Figure 10-86: Insert IP Address .....	142
Figure 10-87: Insert IP Address-Confirm.....	142
Figure 10-88: SSH Allow/Deny Host Manager – Display Configuration .....	143
Figure 10-89: Remove from Allowed List .....	143
Figure 10-90: Current IP Addresses Allowed List.....	143
Figure 10-91: IP Address Allowed List – Removed IP Address.....	144
Figure 10-92: SSH NOT Allowed for ALL Hosts - Display Configuration.....	144
Figure 10-93: Add Subnet .....	144
Figure 10-94: Add Subnet-Confirm .....	145
Figure 10-95: SSH Allow/Deny Host Manager - Display Configuration .....	145
Figure 10-96: Remove Host/Subnet Mask.....	146
Figure 10-97: Remove Host/Subnet Mask - Confirm .....	146
Figure 10-98: Remove Host/Subnet Mask - Display Configuration .....	146
Figure 10-99: Add Host to Allowed List.....	147
Figure 10-100: Add Host to Allowed List - Confirm .....	147
Figure 10-101: SSH Allow/Deny Host Manager - Display Configuration .....	147
Figure 10-102: Remove Host/Subnet from Allowed Hosts.....	148
Figure 10-103: Remove Host/Subnet from Allowed Hosts - Hosts List .....	148
Figure 10-104: Remove Host/Subnet from Allowed Hosts - Display Configuration.....	148
Figure 10-105: EMS Server Manager – Change DBA Password .....	149
Figure 10-106: Changing the DB Password Sub-menu .....	149
Figure 10-107: Changing the DB Password – Confirmation Display .....	150
Figure 10-108: EMS Server Manager – OS Password Settings .....	150
Figure 10-109: Changing OS Password General Settings.....	152
Figure 10-110: Changing User’s Password and Properties.....	152
Figure 10-111: OS Passwords Settings with Security Extensions.....	154
Figure 10-112: Maximum Active SSH Sessions.....	154
Figure 10-113: EMS Server Manager – Add EMS User .....	155
Figure 10-114: EMS Server Manager – Start/Stop File Integrity Checker .....	156
Figure 10-115: EMS Server Manager – Network Options.....	156
Figure 10-116: Network Options Sub-menu.....	157
Figure 10-117: Software Integrity Checker (AIDE) and Pre-linking.....	158
Figure 10-118: Enable/Disable USB .....	159

Figure 10-119: USB Storage .....	159
Figure 10-120: Auditd Options .....	160
Figure 10-121: Auditd Options Prompt.....	160
Figure 10-122: EMS Server Manager - Configure NTP .....	162
Figure 10-123: Start NTP .....	163
Figure 10-124: EMS Server Manager - Change System Timezone.....	163
Figure 10-125: Change System Time Zone – Enter New Time Zone.....	164
Figure 10-126: EMS Server Manger - Change System Time & Date .....	165
Figure 10-127: Change System Time and Date Prompt.....	165
Figure 10-128: EMS Server Manager – Start/ Stop EMS Server.....	166
Figure 10-129: EMS Server Manager – Web Server Configuration.....	166
Figure 10-130: Web Server Configuration Sub-menu.....	167
Figure 10-131: JAWS IP Configuration .....	168
Figure 10-132: EMS Server Manager – Backup the EMS Server.....	170
Figure 10-133: EMS Server Manager – Scheduled Backup for the EMS Server .....	171
Figure 10-134: Schedule New Backup.....	172
Figure 10-135: View Scheduled Backups .....	173
Figure 10-136: Schedule Backup Time .....	173
Figure 10-137: Remove Scheduled Backup.....	174
Figure 10-138: List of Scheduled Backups.....	174
Figure 10-139: Scheduled Backups List.....	174
Figure 10-140: Set Number of Scheduled Backups to Save.....	175
Figure 10-141: Number of Backups to Store.....	175
Figure 10-142: EmsBackup File .....	175
Figure 10-143: EMS Server Manager – Restore the EMS Server .....	176
Figure 10-144: Saved Backups Sub-menu .....	176
Figure 10-145: Restore Process-Confirmation.....	177
Figure 10-146: EMS Server Manual Restart .....	177
Figure 10-147: EMS Server Manager – Reboot the EMS Server .....	178
Figure 10-148: EMS Server Manager - HA Configuration.....	183
Figure 10-149: High Availability sub-menu.....	183
Figure 10-150: Primary HA Server Menu .....	184
Figure 10-151: Primary HA Server Sub-menu .....	184
Figure 10-152: HA Configuration Display.....	184
Figure 10-153: HA Server Configured as Primary Server - Confirmation .....	185
Figure 10-154: Primary HA Server Menu .....	186
Figure 10-155: Primary HA Server Sub-menu .....	186
Figure 10-156: HA Configuration Display.....	186
Figure 10-157: HA Server Configured as Primary Server - Confirmation .....	187
Figure 10-158: Secondary HA Server Menu .....	189
Figure 10-159: Primary HA Server IP.....	189
Figure 10-160: Secondary HA Server Configuration.....	190
Figure 10-161: Manual Switchover.....	191
Figure 10-162: Switchover Status .....	191
Figure 10-163: Status after Switchover .....	192
Figure 10-164: Uninstall EMS HA .....	192



---

Figure 10-165: Uninstall EMS HA Status Display .....	193
Figure 10-166: EMS HA Status .....	195
Figure 10-167: EMS HA Status - Example Display .....	195
Figure 10-168: Advanced Status View .....	197
Figure 10-169: Syslog Configuration .....	199
Figure 10-170: Forward Messages to an External Server .....	200
Figure 10-171: Board Syslog Logging Configuration .....	201
Figure 10-172: Board Syslog Logging Configuration .....	203
Figure 11-1: Firewall Configuration Schema .....	209
Figure 12-1: EMS Client Installation-Run as Administrator .....	211
Figure 12-2: Running EMS Client-Run as Administrator .....	212
Figure A-1: Sun Solaris Server Power Button .....	217
Figure A-2: EMS Client Removal .....	217
Figure A-3: Java Control Panel .....	218
Figure B-1: Save MGs Tree Command .....	221
Figure C-1: Installing Windows OS Patches – PC Information .....	225
Figure C-2: Installing Windows OS Patches – Selecting the Operating System .....	225
Figure C-3: Installing Windows OS Patches – Download and Install .....	226
Figure E-1: X509 Files-Software Manager .....	231
Figure E-2: System Settings .....	232
Figure E-3: MG Information .....	233
Figure H-1: Sun Server Power Button .....	250
Figure I-1: Alarm Receiver .....	260
Figure I-2: Destination Rule Configuration .....	261
Figure I-3: Users List .....	262
Figure I-4: Actions Journal .....	263
Figure I-5: Configuration Parameter Search drop-down list box .....	264
Figure I-6: Configuration Parameter: Advanced Search .....	265
Figure I-7: Media Gateway Search .....	266

---

## List of Tables

---

Table 2-1: SEM Virtual Environment Server Disk Requirements.....	24
Table 3-1: EMS- Minimal Platform Requirements.....	25
Table 3-2: SEM Bandwidth Requirements.....	28
Table 11-1: Firewall Configuration Rules.....	207
Table 11-2: OAM&P Flows: NOC ↔MG EMS.....	210
Table 11-3: OAM&P Flows: MG EMS→NOC.....	210
Table I-1: Acceptance Test – Client Installation.....	255
Table I-2: Acceptance Test – Server Installation.....	256
Table I-3: Acceptance Test – Add Auxiliary File.....	256
Table I-4: Acceptance Test – Add MG.....	256
Table I-5: Acceptance Test – Provisioning: Mediant 5000/ Mediant 8000.....	257
Table I-6: Acceptance Test – Provisioning: CPE Devices.....	257
Table I-7: Acceptance Test – Entity Profile: Digital CPE Devices.....	258
Table I-8: Acceptance Test – Analog CPE Devices.....	259
Table I-9: Acceptance Test – Alarm Receiver.....	260
Table I-10: Acceptance Test – Delete Alarms.....	260
Table I-11: Acceptance Test – Acknowledge Alarm.....	260
Table I-12: Acceptance Test – Forwarding Alarms.....	261
Table I-13: Acceptance Test – Add an Operator.....	262
Table I-14: Acceptance Test – Non Repetitive Passwords.....	262
Table I-15: Acceptance Test – Removing Operator.....	262
Table I-16: Acceptance Test – Journal Activity.....	263
Table I-17: Acceptance Test – Configuration Parameter: Basic Search.....	264
Table I-18: Acceptance Test – Configuration Parameter: Advanced Search.....	265
Table I-19: Acceptance Test – MG Search.....	266
Table I-20: Acceptance Test – Online Help.....	267
Table I-21: Acceptance Test – Backup and Recovery.....	267

## 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>.

© 2013 AudioCodes Inc. All rights reserved

This document is subject to change without notice.

Date Published: July-17-2013



**Note:** The Element Management System supports the following products:

1. Mediant 8000 Media Gateway and E-SBC
2. Mediant 5000 Media Gateway and E-SBC
3. Mediant 4000 E-SBC
4. Mediant 3000
5. Mediant 2600 E-SBC
6. Mediant 2000
7. Mediant 1000
8. Mediant 1000 Gateway and E-SBC
9. Mediant 1000 MSBG
10. Mediant 850 MSBG
11. Mediant 800 MSBG
12. Mediant 800 Gateway and E-SBC
13. Mediant 600 Media Gateway
14. MediaPack Media Gateways MP-112 (FXS), MP-114 (FXS and FXO), MP-118 (FXS and FXO), MP-124 (FXS).

## Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI<sup>2</sup>, CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

## WEEE EU Directive

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

## Customer Support

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

## Document Conventions

Courier - UNIX Commands  
**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 600 and 1000 SIP User’s Manual
Mediant 800 Gateway and E-SBC SIP User’s Manual
Mediant 800 MSBR SIP User’s Manual
Mediant 850 MSBR SIP User’s Manual
Mediant 1000 Gateway and E-SBC User’s Manual
Mediant 1000B MSBR User’s Manual
Mediant 2000 SIP User’s Manual
Mediant 2600 E-SBC User’s Manual
Mediant 3000 SIP User’s Manual
MGCP-MEGACO Product Reference Manual
Mediant 4000 E-SBC User’s Manual
MediaPack User’s Manual
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAMP Integration Guide
Element Management System (EMS) User’s Manual

<b>Manual Name</b>
Element Management System (EMS) Online Help
Mediant 5000 / 8000 Media Gateway Installation, Operation and Maintenance Manual
Mediant 5000 / 8000 Media Gateway Release Notes
Mediant 5000 / 8000 Media Gateway Programmer's User Manual
Mediant 3000 TP-8410 OAM Guide
Mediant 3000 TP-6310 OAM Guide
Mediant 2000 OAM Guide
Mediant 1000 E-SBC OAM Guide
Mediant 1000 MSBG OAM Guide
Mediant 800 E-SBC OAM Guide
Mediant 800 MSBG OAM Guide
Mediant 600 OAM Guide

**Reader's Notes**

# 1 Overview

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

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

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

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

**Reader's Notes**



# Part I

## Pre-installation Information

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



## 2 Component Information

The EMS comprises the following components:

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

### 2.1.1 Managed Devices for All EMS Server Versions

The following products (**bold** font indicates new products / versions) are managed by the EMS:

- Mediant 8000 Media Gateway (MEGACO & SIP): versions **6.6**, 6.2
- Mediant 5000 Media Gateway (MEGACO & SIP): versions **6.6**, 6.2
- Mediant 4000 E-SBC (SIP): version **6.6**
- Mediant 3000 Media Gateways (MEGACO & SIP): versions **6.6**, 6.4, 6.2
- Mediant 2600 E-SBC (SIP): version **6.6**
- Mediant 2000 Media Gateways (SIP): versions **6.6**, 6.4, 6.2
- Mediant 1000, Mediant 1000 E-SBC and Media Gateway and Mediant 1000 MSBG (SIP): versions **6.6**, 6.4, 6.2
- Mediant 850 (SIP): version **6.6**
- Mediant 800 E-SBC and Mediant 800 MSBG (SIP): versions **6.6**, 6.4, 6.2
- Mediant 600 (SIP): versions 6.4, 6.2
- MediaPack 11x Media Gateways (SIP): versions **6.6**, 6.2

### 2.1.2 SEM Monitored Devices

The following lists the devices monitored by the SEM:

- Mediant 4000 E-SBC
- Mediant 3000 Media Gateways
- Mediant 2600 E-SBC
- Mediant 2000 Media Gateways
- Mediant 1000, Mediant 1000 Gateway and E-SBC and Mediant 1000 MSBG
- Mediant 850 MSBG
- Mediant 800 Gateway and E-SBC and Mediant 800 MSBG
- MediaPack 11x Media Gateways

Note that all the devices monitored by the SEM should be version 6.6.

### 2.1.3 SEM Server Disk Requirements

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

The maximum available calls storage on the dedicated EMS server hardware is 7 million calls.

In the virtual environment, the three configurations shown in the table below are supported:

**Table 2-1: SEM Virtual Environment Server Disk Requirements**

Size	Maximum Storage Size
<b>Small</b>	2 million calls.
<b>Typical</b>	4.5 million calls.
<b>Large</b>	7 million calls.

## 3 Hardware and Software Requirements

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

### 3.1 EMS Server and Client Requirements

This section lists the platform and software required to run the EMS Dedicated Hardware version and the VMware version.

**Table 3-1: EMS- Minimal Platform Requirements**

Resource	EMS/SEM Server			EMS Client	
	Dedicated EMS Server – Solaris OS	Dedicated EMS Server - Linux OS			VMware vSphere– Linux OS
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▪ Sun™ Fire™ V240<sup>1</sup></li> <li>▪ Sun™ Fire™ V215<sup>1</sup></li> <li>▪ Sun™ Netra™ T2000<sup>2</sup></li> <li>▪ Sun Netra T5220<sup>1</sup></li> <li>▪ Sun Netra T4-1</li> </ul>	HP DL360 G6	HP DL360p G8		Monitor resolution: 1152*864 or higher
<b>Operating System</b>	<ul style="list-style-type: none"> <li>▪ For Sun Netra T4-1:               <ul style="list-style-type: none"> <li>✓ Solaris™ 64-bit, version 10, Rev 8</li> </ul> </li> <li>▪ For all other machines:               <ul style="list-style-type: none"> <li>✓ Solaris™ 64-bit, version 10, Rev 7</li> </ul> </li> </ul>	Linux CentOS 64-bit, kernel version 5.3, Rev4	Linux CentOS 64-bit, kernel version 5.9, Rev5	Linux CentOS 64-bit, kernel version 5.3 Rev4,	Windows™ 2000 / XP/ Vista/7
<b>Memory</b>	<ul style="list-style-type: none"> <li>▪ 1 GB RAM for:               <ul style="list-style-type: none"> <li>✓ Sun™ Fire™ V240</li> <li>✓ Sun™ Fire™ V215</li> <li>✓ Sun™ Netra™ T2000</li> </ul> </li> </ul>	2 GB RAM	8 GB RAM	2 GB RAM	512 MB RAM

<sup>1</sup> Version 6.6 on Sun Solaris platforms is available for selected customers pending approval from AudioCodes Product Management.

<sup>2</sup> Rev 7 is the recommended OS Revision for all Solaris Hardware platforms with the exception of the Sun™ Netra™ T4-1 platform, which is released with OS Revision 8 only.

Resource	EMS/SEM Server			VMware vSphere– Linux OS	EMS Client
	Dedicated EMS Server – Solaris OS	Dedicated EMS Server - Linux OS			
	<ul style="list-style-type: none"> <li>▪ 8 GB RAM for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T5220</li> </ul> </li> <li>▪ 16 GB RAM for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T4-1</li> </ul> </li> </ul>				
<b>Disk space</b>	<ul style="list-style-type: none"> <li>▪ 73 GB for:               <ul style="list-style-type: none"> <li>✓ Sun™ Fire™ V240</li> <li>✓ Sun™ Fire™ V215</li> <li>✓ Sun™ Netra™ T2000</li> </ul> </li> <li>▪ 300 GB for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T5220</li> <li>✓ Sun Netra T4-1</li> </ul> </li> </ul>	✓ 146 GB	✓ 300 GB	Three configurations are available: <ul style="list-style-type: none"> <li>▪ Small – 60 GB</li> <li>▪ Typical – 85 GB</li> <li>▪ Large – 120 GB</li> </ul>	300 MB
<b>Processor</b>	<ul style="list-style-type: none"> <li>▪ UltraSPARC IIIli for:               <ul style="list-style-type: none"> <li>✓ Sun™ Fire™ V240</li> <li>✓ Sun™ Fire™ V215</li> </ul> </li> <li>▪ UltraSPARC-T2 for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T5220</li> </ul> </li> <li>▪ SPARC-T4 for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T4-1</li> </ul> </li> </ul>	Intel Xeon E5504 (4M Cache, 2.00 GHz)	Intel Xeon E5-2620 (6 cores 2.00 GHz, 6×256KB L2 Cache, 15MB L3 Cache)	1 core not less than 2 GHz	600 MHz Pentium III or higher
<b>Swap space</b>	<ul style="list-style-type: none"> <li>▪ 2 GB for:               <ul style="list-style-type: none"> <li>✓ Sun™ Fire™ V240</li> <li>✓ Sun™ Fire™ V215</li> <li>✓ Sun™ Netra™ T2000</li> </ul> </li> <li>▪ 8.9 GB for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T5220</li> </ul> </li> <li>▪ 15 GB for:               <ul style="list-style-type: none"> <li>✓ Sun Netra T4-1</li> </ul> </li> </ul>	4 GB	8 GB	4 GB	1 GB

Resource	EMS/SEM Server			EMS Client
	Dedicated EMS Server – Solaris OS	Dedicated EMS Server - Linux OS	VMware vSphere– Linux OS	
DVD-ROM	Local			

- 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.

## 3.2 EMS and SEM Bandwidth Requirements

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

### 3.2.1 EMS Bandwidth Requirements

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

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

### 3.2.2 SEM Bandwidth Requirements

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

**Table 3-2: SEM Bandwidth Requirements**

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



## 4 EMS Software Deliverables

This section describes the EMS software deliverables.

### 4.1 Dedicated Hardware Installation – DVDs 1-4

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

■ **DVD1:** Operating System DVD for Solaris or Linux:

- Solaris 10 Installation for EMS server, Solaris 10 REV7 and REV8

The following machines are currently supported:

- ◆ Sun™ Netra™ T2000, Sun™ Fire™ V215, Sun™ Fire™ V240, 64-bit Solaris 10 11/06 REV 7
- ◆ Sun Netra T5220, 64-bit Solaris 10 09/10 Rev7
- ◆ Sun Netra T4-1, 64-bit Solaris 10 08/11 Rev8
- Linux (CentOS) 5.3 Installation for EMS server, Linux CentOS 5.3 REV4 and 5.9 REV5

The following machines are currently supported:

- ◆ HP DL360 G6 - Linux (CentOS) 64-bit kernel version 5.3 Installation for EMS server, Linux CentOS 5.3 REV4.
- ◆ HP DL360p G8 - Linux (CentOS) 64-bit kernel version 5.9 Installation for EMS server, Linux CentOS 5.9 REV5.

■ **DVD2:** Oracle Installation: Oracle installation version 11g DVD for both the Linux and Solaris platforms.

■ **DVD3:** Software Installation and Documentation DVD for Solaris or Linux:

The DVD 'SW Installation and Documentation' DVD comprises the following folders:

- Documentation – All documentation related to the present EMS version. The documentation folder includes the following documents and sub-folders:
  - ◆ EMS Release Notes Document – includes the list of the new features introduced in the current software version as well as version restrictions and limitations.
  - ◆ EMS Server IOM Manual – Installation, Operation and Maintenance Guide.
  - ◆ EMS Product Description Document
  - ◆ EMS User's Manual Document
  - ◆ OAMP Integration Guide Document
  - ◆ 'GWs\_OAM\_Guides' folder – document set describing Provisioning parameters and Alarm/Performance measurements parameters supported for each one of the products or product families.
  - ◆ 'Private\_Labeling' folder – includes all the information required for the OEM to create a new private labeling DVD. EmsClientInstall – EMS client software to be installed on the operator's Windows™ based workstation.

- 'EmsClientInstall'-EMS client software to install on the designated client workstation PC.
- 'EmsServerInstall' – EMS server software, to install on the dedicated Solaris 10 or Linux 5.3 based EMS server machine.
- **DVD4:** (relevant for future releases) EMS Server Patches: Upgrade patches DVD containing OS (Linux and Solaris) patches, Oracle patches, java patches or any other EMS required patches. This DVD enables the upgrading of the required EMS patches without the EMS application upgrade.

## 4.2 VMware vSphere Installation– DVD 5

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

- Virtual Appliance for clean install
- EMS Client Install
- Documentation

# Part II

## EMS Server Installation

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



## 5 Testing Installation Requirements - Dedicated Hardware

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

### 5.1 Hardware Requirements

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

To determine the system OS, enter the following command:

```
uname
```

This command returns **SunOS** or **Linux**. Proceed to one of the following sections (according to the relevant operating system):

- Testing Hardware Requirements on Solaris OS (see below)
- Testing Hardware Requirements on Linux OS (see Section 5.1.2 on page 35).

#### 5.1.1 Testing Hardware Requirements on the Solaris Platform

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

- **RAM** - A minimum of 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.

**Figure 5-1: Solaris Testing Requirements**

```

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 <73400057856 bytes>
EMS-Server39:/ [root] =>
    
```



**Note:** Use AudioCodes' DVD to install the Solaris 10 operating system (see Section 6 on page 37).

## 5.1.2 Testing Hardware Requirements on the Linux Platform

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

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

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

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

- **Swap Space** - Disk space twice the system's physical memory, or 2 GB, whichever is greater.

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

```
more /proc/meminfo | grep SwapTotal
```

**Disk Space** - A minimum of 146 GB for the EMS Dedicated.

Hardware version (on the same disk or under RAID - Redundant Arrays of Independent Disks) and up to 120 GB for the VMware version (for more information, see Section 3 on page 25).

To determine the amount of disk space on your system, enter the following command:

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

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

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

Figure 5-2: Linux Testing Requirements

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



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

### Reader's Notes

## Reader's Notes



## 6 Installing the EMS Server on Dedicated Hardware

The EMS server installation process supports both the Solaris and Linux platforms. The installation includes four separate components, where each component is supplied on a separate DVD:

- **DVD1:** OS installation: OS installation DVD; separate DVDs for both Linux and Solaris.
- **DVD2:** Oracle Installation: Oracle installation DVD for both Linux and Solaris platforms.
- **DVD3:** EMS application: EMS server application installation DVD for both the Linux and Solaris platforms.
- **DVD4:** (relevant for future releases) EMS Server Patches: Upgrade patches DVD containing OS (Linux and Solaris) patches, Oracle patches, java patches or any other EMS required patches. This DVD enables the upgrading of the EMS required patches without the EMS application upgrade.

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

## 6.1 Installing the EMS Server on the Solaris Platform

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



**Note:** If you are installing Solaris on Oracle/Sun Netra T5220 or Netra T4-1 and wish to configure RAID 1 on this machine, you must perform this configuration prior to the installation of the Solaris OS. See Section H on page 249 to apply the RAID 1 configuration.

### 6.1.1 DVD1: Solaris 10 Rev 7 / Rev 8 Installation

This section describes how to install the Solaris 10 operating system from the supplied DVD.

#### 6.1.1.1 Accessing the OK Prompt

To install the Solaris operating system, you need to switch to the **OK**> prompt. The method for accessing the **OK** prompt depends on the hardware platform.

##### Sun Fire V240 and Netra 240 Servers

The procedure below describes how to access the **OK** prompt for Sun Fire V240 and Netra 240 servers.

➤ **To access the OK prompt on Sun Fire V240 and Netra 240:**

1. Connect to the machine through the management serial port.
2. Press the <Alt> and <B> keys.

##### Sun Netra T5220 and Netra T4-1 Servers

The procedure below describes how to access the **OK** prompt for the Sun Netra T5220 and Sun Netra T4-1 servers. You can access the **OK** prompt using the `init 0` command or by using Sun's Integrated Lights Out Manager (ILOM) tool.

➤ **To access the OK prompt on Netra T5220 and Netra T4-1 using 'init 0':**

1. Connect to the machine through the management serial port.
2. Run the following command in the terminal server:

```
init 0
```

3. Wait for the machine to reboot and for the **OK** prompt to appear.

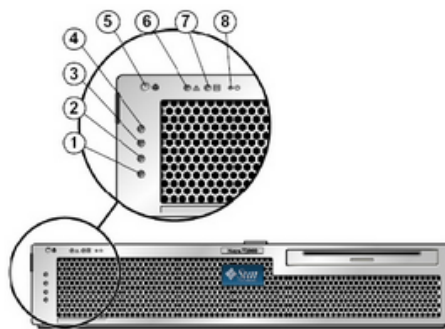
➤ **To access the OK prompt on Netra T5220 and Netra T4-1 using ILOM:**

1. Connect to the machine through the management serial port.
2. Plug in the EMS server's power cable.
3. Wait for the ILOM login prompt in the serial terminal.
4. Log in with the following credentials:
  - SUNSP00144FAC6F3D login: **root**
  - Password: **changeme**
5. At the prompt, type the following:

```
set /HOST/bootmode script="setenv auto-boot? false"
```

6. Turn on the power using the front power button (item 8 in the figure below):

**Figure 6-1: Sun Server Power Button**



7. When the prompt appears, type the following:

```
set /HOST send_break_action=break
start /SP/console
```

8. At the prompt, confirm the last command by typing the following:

```
Y
```

9. Wait until the **OK** prompt is displayed.

### 6.1.1.2 Installing the Solaris 10 Operating System

The procedure below describes how to install Solaris 10 from the supplied DVD (this procedure takes approximately one hour on Netra T5220 machines).

➤ **To install Solaris 10:**

1. Insert the DVD that contains Solaris 10 Rev 7 for EMS into the DVD ROM on the EMS server.
2. Connect the EMS server to your PC through the serial port with a terminal application.
3. Log in as the 'root' user.
4. Access the **OK** prompt (as described in Section 6.1.1.1 on page 38).
5. At the prompt, type the following and then press **Enter**:
  - When installing Solaris 10 Rev7 on Netra T5220, Netra T4-1 or Netra T2000:

```
boot cdrom - install
```

- When installing Solaris 10 Rev7 on Sun Fire V240 / Netra 240 or Solaris 10 Rev6 on T2000:

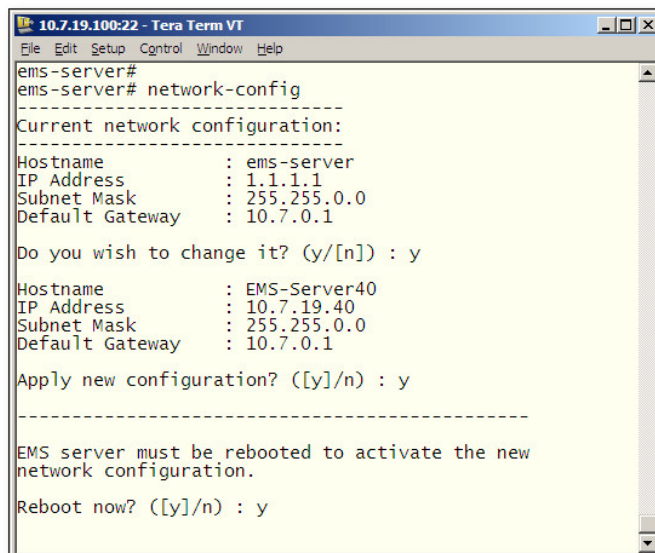
```
boot cdrom
```

6. Wait for the installation to complete.
7. Reboot your machine (if it doesn't reboot automatically).
8. Log in as the 'root' user user with the *root* password.
9. At the prompt, type the following and then press **Enter**:

```
network-config
```

The current configuration is displayed, as shown below:

**Figure 6-2:Installing Solaris 10-Current Configuration**



```

10.7.19.100:22 - Tera Term VT
File Edit Setup Control Window Help
ems-server#
ems-server# network-config
-----
Current network configuration:
-----
Hostname       : ems-server
IP Address     : 1.1.1.1
Subnet Mask    : 255.255.0.0
Default Gateway : 10.7.0.1

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

Hostname       : EMS-Server40
IP Address     : 10.7.19.40
Subnet Mask    : 255.255.0.0
Default Gateway : 10.7.0.1

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

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

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

- 10.** At the prompt, type the following to modify configuration:

- 11.** At the prompt, enter your hostname, IP address, subnet mask, and default gateway.

- 12.** At the prompt, confirm your changes by typing the following:

- 13.** At the prompt, confirm reboot by typing the following:

### 6.1.2 DVD2: Oracle DB Installation

The procedure below describes how to install the Oracle database. This procedure takes approximately 40 minutes.



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

➤ **To perform DVD2 installation:**

1. Insert **DVD2-Oracle DB installation** into the DVD ROM.
2. Login into the EMS server by TELNET as 'root' user and enter *root* password.
3. Run the installation script from its location:

```
# cd /cdrom/ems_dvd2/
# ./install
```

**Figure 6-3: Oracle DB Installation-Solaris**

```
EMS-Server40%
EMS-Server40%
EMS-Server40% su - root
Password:
EMS-Server40# cd /cdrom/ems_dvd2/
EMS-Server40# ./install
Start installValues
chmod: WARNING: can't access /etc/zshenv
/cdrom/ems_dvd/ac_ems_deploy/: No such file or directory
"my" variable $date masks earlier declaration in same scope at AllSystemChecks.pm line 1302.
Found = in conditional, should be == at ./FastOracleInstall.pl line 120.
Start executing User Login Check script at Thu Sep 16 18:12:53 IST 2010

Login Check Successfully Passed.

>>> Verifying OS version - Thu Sep 16 18:12:53 IST 2010

...
SOFTWARE EVALUATION LICENSE AGREEMENT

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

4. Type **y** and press **Enter** to accept the License agreement.

**Figure 6-4: Oracle DB Installation-Solaris-License Agreement**

```
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
```



### 6.1.3 DVD3: EMS Server Application Installation

The procedure below describes how to install the EMS server application. This procedure takes approximately 30 minutes.



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

➤ **To perform DVD3 installation:**

1. Insert **DVD3-EMS server application installation** into the DVD ROM.
2. Login into the EMS server by SSH, as 'root' user, and provide *root* password.
3. Run the installation script from its location:

```
cd /cdrom/ems_dvd/EmsServerInstall/
./install
```

**Figure 6-7: EMS Server Application Installation (Solaris)**

```
EMS-Server17%
EMS-Server17% su - root
Password:
EMS-Server17# cd /cdrom/ems_dvd/EmsServerInstall
EMS-Server17# ./install
```

4. Type **y** and press **Enter** to accept the License agreement.

**Figure 6-8: EMS Server Installation (Solaris) - License Agreement**

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

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

5. OS packages removal. After this step, you are prompted to press **Enter** to reboot.
6. After the EMS server has rebooted, repeat steps 2 to 4.
7. OS patches are installed.



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

**Figure 6-9: EMS Server Installation (Solaris) - Patches Installation**

```
The following patches were successfully installed:
118666-27;118667-27;141500-08;

Reboot is needed

+++++
EMS Server must be rebooted to proceed with the installation.

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

Press Enter to reboot...
█
```

8. After the EMS server has rebooted, repeat steps 2 to 4.
9. Accept the Java License agreement by typing **y** and pressing **Enter**.

**Figure 6-10: EMS Server Installation (Solaris) – Java License Agreement**

```
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 UPON THE CONDITION
THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY
CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS
(COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT

I. Installation and Auto-Update. The Software's
installation and auto-update processes transmit a limited
amount of data to Sun (or its service provider) about those
specific processes to help Sun understand and optimize
them. Sun does not associate the data with personally
identifiable information. You can find more information
about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150
Network Circle, Santa Clara, California 95054, U.S.A.

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

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

**Figure 6-11: EMS Server Installation (Solaris) – Java Installation (cont)**

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

Press Enter to continue.....
█
```

11. Accept the Java License agreement by typing **y** and pressing **Enter**.

**Figure 6-12: EMS Server Installation (Solaris) – Java License Agreement**

```
I. Installation and Auto-Update. The Software's
installation and auto-update processes transmit a limited
amount of data to Sun (or its service provider) about those
specific processes to help Sun understand and optimize
them. Sun does not associate the data with personally
identifiable information. You can find more information
about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150
Network Circle, Santa Clara, California 95054, U.S.A.

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

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

**Figure 6-13: EMS Server Installation (Solaris) Java Installation (cont)**

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

Press Enter to continue....

```

13. Wait for the installation to complete and reboot the EMS server by typing **reboot**.

**Figure 6-14: EMS Server Installation (Solaris) Java Installation Complete**

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

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

Unzipping the installation archive
Shutting down database instance
Stopping TNS listener
Applying Oracle patch
Starting database instance
Loading modified .sql files
Recompiling DB views
Recompiling invalid objects
Starting TNS listener
Fixing hardening configuration
Removing temporary files

Done
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
EMS-Server40#
```

14. When the EMS server successfully restarts, log into the EMS server by 'root' user and verify Date and Time are set correctly. See Section 10.4.3 on page 165 to set the date and time.
15. Verify that the EMS server is up (See Section 10.1.1 on page 88) and login by client to verify successful installation.

## 6.2 Installing the EMS Server on the Linux Platform

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

### 6.2.1 DVD1: Linux CentOS 5.3 and CentOS 5.9

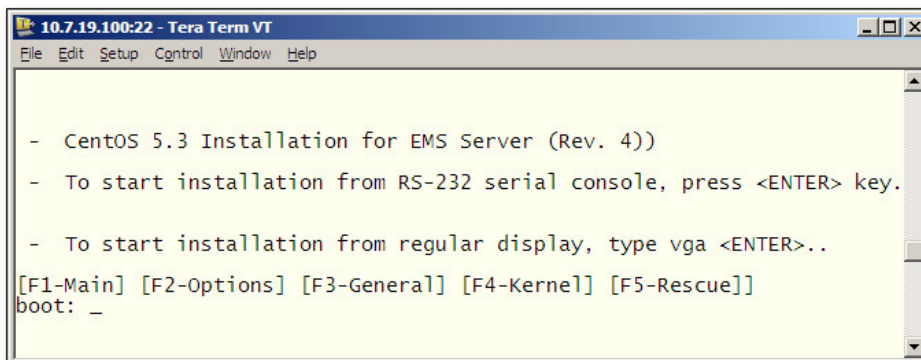
The procedure below describes how to install Linux CentOS 5.3 and Linux CentOS 5.9. This procedure takes approximately 20 minutes.

➤ **To perform DVD1 installation:**

1. Insert the **DVD1-Linux for EMS Rev 4** (CentOS 5.3) or **DVD1-Linux for EMS Rev 5** (CentOS 5.9) into the DVD ROM.
2. Connect the EMS server via the serial port with a terminal application and login with 'root' user.
3. Perform EMS server machine reboot by specifying the following command:
 

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

**Figure 6-15: Linux CentOS Installation**



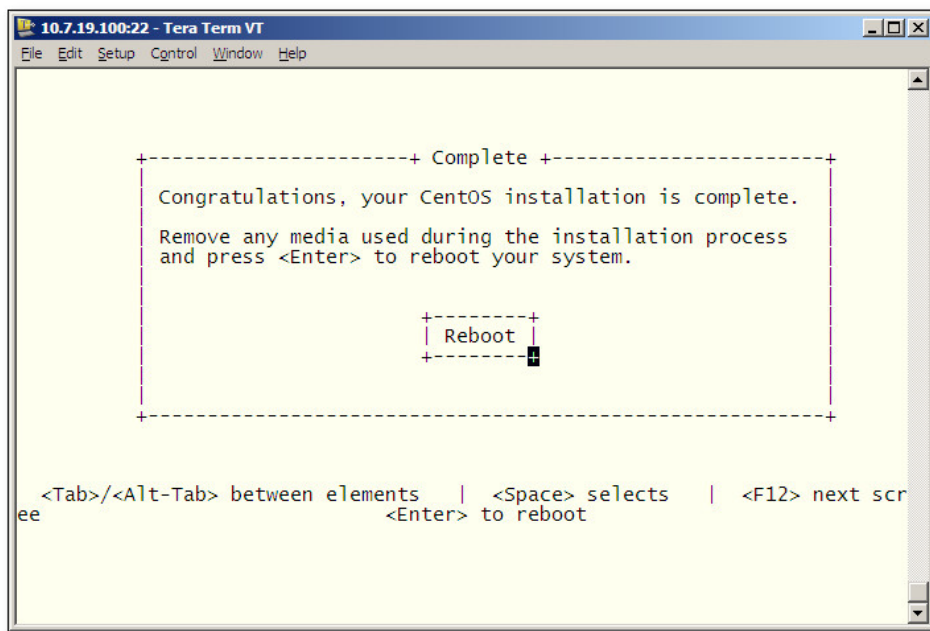
```

10.7.19.100:22 - Tera Term VT
File Edit Setup Control Window Help
- CentOS 5.3 Installation for EMS Server (Rev. 4)
- 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-Kerne] [F5-Rescue]
boot: _
  
```

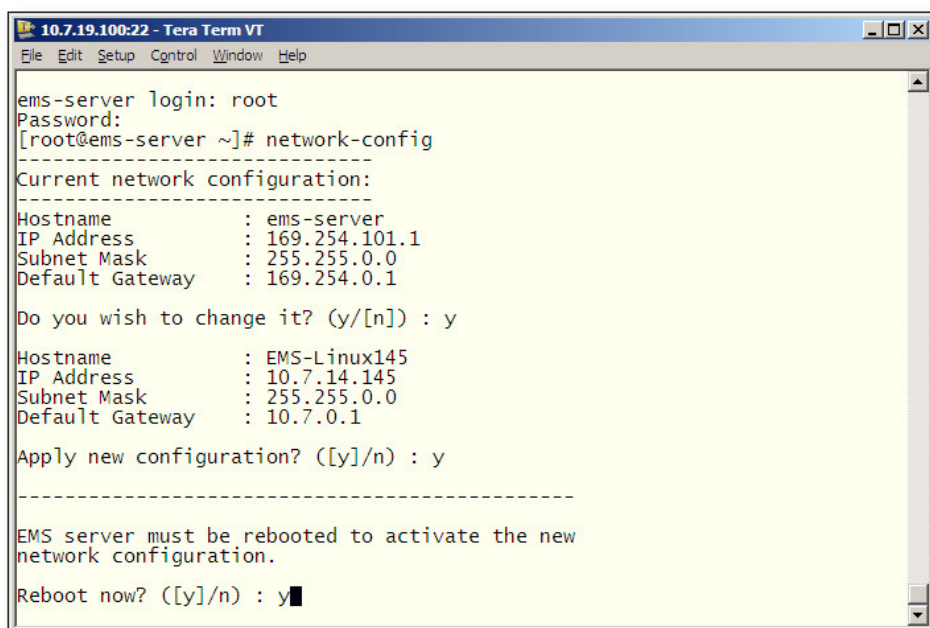
6. Wait for the installation to complete.
7. Reboot your machine by pressing **Enter**.



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

**Figure 6-16: Linux CentOS Installation Complete**

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

**Figure 6-17: Linux CentOS Network Configuration**

10. You are prompted to change the configuration; enter **y**.
11. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.
12. Confirm the changes by entering **y**.
13. You are prompted to reboot; enter **y**.

## 6.2.2 DVD2: Oracle DB Installation

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



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file

➤ **To perform DVD2 installation:**

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

```
su - root
```

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

```
mount /misc/cd
```

5. Run the installation script from its location:

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

**Figure 6-18: Oracle DB Installation (Linux)**

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

Login Check Successfully Passed.

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

...
SOFTWARE EVALUATION LICENSE AGREEMENT

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

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





## 6.2.3 DVD3: EMS Server Application Installation

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

➤ **To perform DVD3 installation:**

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

```
su - root
```

4. Run the installation script from its location:

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

**Figure 6-22: EMS Server Application Installation (Linux)**

```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/  
[root@EMS-Linux2 EmsServerInstall]# ./install  
DIR Name /misc/cd/EmsServerInstall  
Start installValues  
  >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...  
Login Check Successfully Passed.  
  
  >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
  >>> >>> PASSED  
  ...  
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
SOFTWARE LICENSE AGREEMENT  
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I  
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (M  
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND  
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG  
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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



Figure 6-23: EMS Server Application Installation (Linux) – License Agreement

```

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

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

```

- When you are prompted to change the *acems* and *root* passwords, enter new passwords or enter existing passwords. You are then prompted to reboot the EMS server machine; press **Enter**.

Figure 6-24: EMS Server Application Installation (Linux) (cont)

```

udev.x86_64          095-14.20.e15_3      ems-local
wget.x86_64         1.11.4-2.e15_4.1    ems-local
wireshark.x86_64    1.0.11-1.e15_5.5    ems-local

Hardening Linux OS for DoD STIG compliancy

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

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

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

Press Enter to reboot...

```

- After the EMS server has successfully rebooted, repeat steps 2 – 4.
- At the end of Java installation, press **Enter** to continue.

**Figure 6-25: EMS Server Application Installation (Linux) - Java Installation**

```

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

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

9. Wait for the installation to complete and reboot the EMS server by typing **reboot**.

**Figure 6-26: EMS Server Application Installation (Linux) – Oracle CPU Patch**

```

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

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

Unzipping the installation archive
Shutting down database instance
Stopping TNS listener
Applying Oracle patch
Starting database instance
Loading modified .sql files
Recompiling DB views
Recompiling invalid objects
Starting TNS listener
Fixing hardening configuration
Removing temporary files

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

10. When the EMS server has successfully restarted, login as 'acems' user, switch to 'root' user and verify that the Date and Time are set correctly. See Sections 10 on page 83 and 10.4.3 on page 165 to set the date and time.
11. Verify that the EMS server is up and running (See Sections 10 on page 83 and 10.1.1 on page 88) and login by client to verify a successful installation.

## 6.3 EMS Server Users

EMS server OS user permissions are differentiated according to the specific application task. This feature is designed to prevent security breaches and to ensure that a specific OS user is authorized to perform a subset of tasks on a subset of machine directories. The EMS server includes the following OS user permissions:

- 'root' user: User permissions for installation, upgrade, maintenance using EMS server manager and EMS application execution.
- *acems* user: The **only available user** for Login/ Telnet/FTP tasks.
- *emsadmin* user: User with permissions for mainly the EMS server manager and EMS application for data manipulation and database access.
- *oracle* user: User permissions for the Oracle database access for maintenance such as installation, patches upgrade, backups and other Oracle database tasks.
- *oralsnr* user: User in charge of oracle listener startup.

**Reader's Notes**

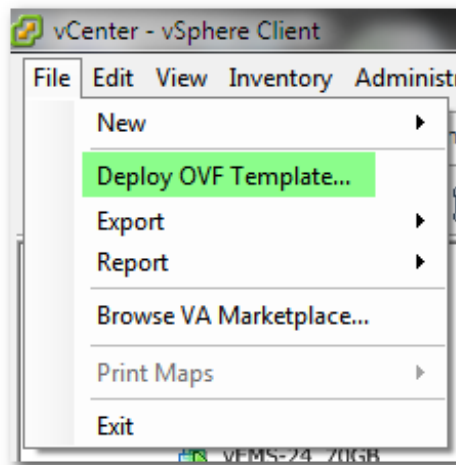
## 7 Installing the EMS Server on the VMware Platform

This section describes how to install the EMS server on the VMware vSphere platform. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Section 5.1.2 on page 35) and depends largely on the hardware machine where the VMware vSphere platform is installed.

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

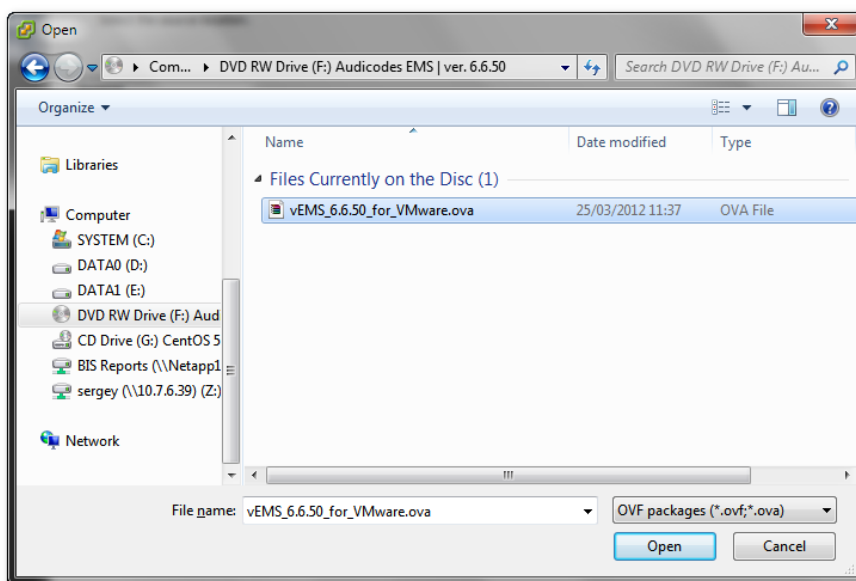
1. Insert the vEMS installation DVD into the disk reader on the PC where the installed vSphere client is installed.

**Figure 7-1: Deploy OVF Template Option**



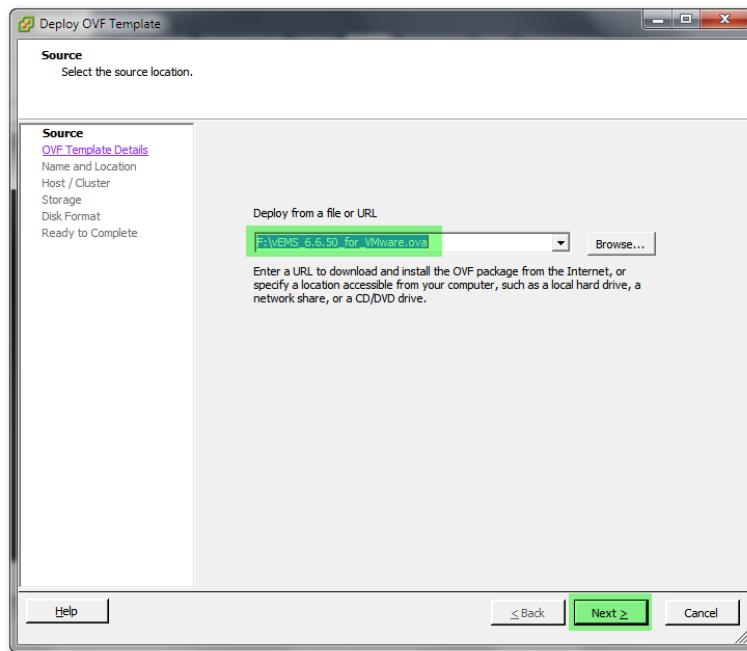
2. On the vSphere client, from the menu, choose **File > Deploy OVF Template**.

**Figure 7-2: Open OVA Package**

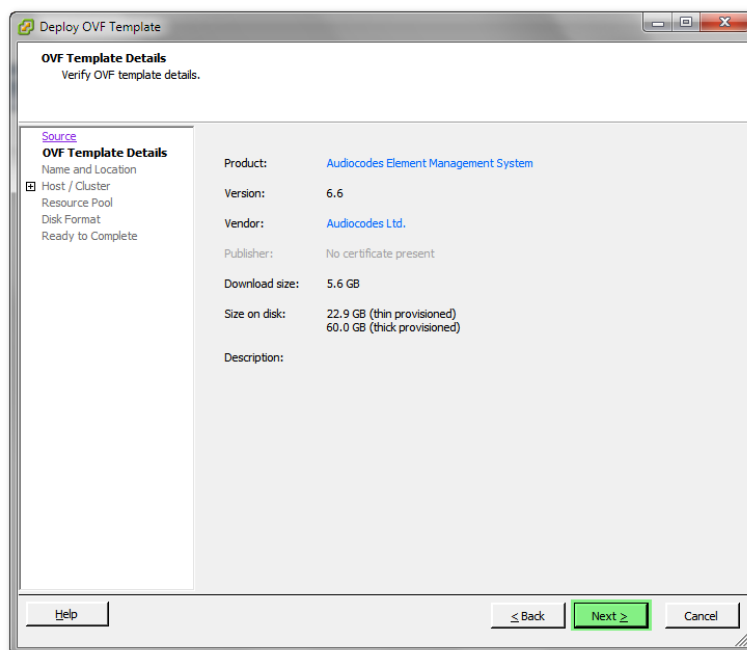


3. Select the vEMS virtual appliance file with extension OVA from the inserted DVD disk, and then click **Next**.

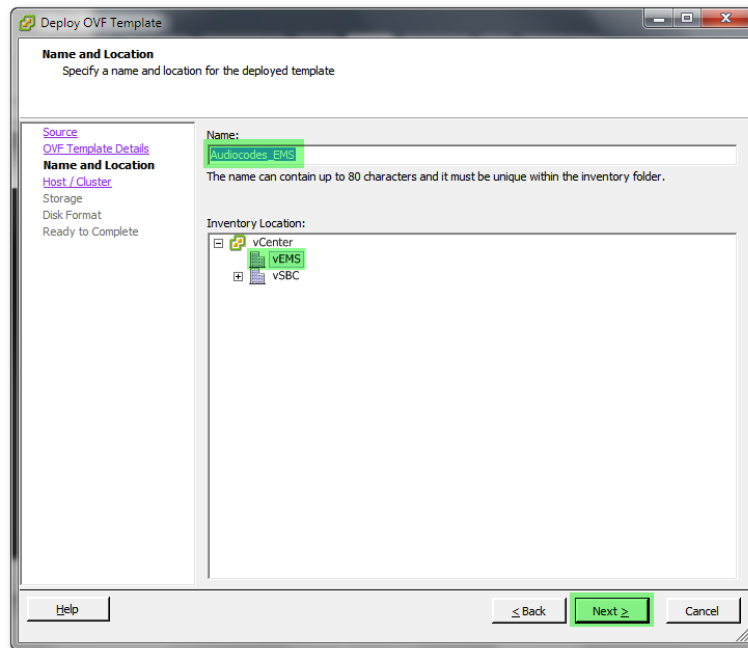
**Figure 7-3: OVF Template Source Screen**



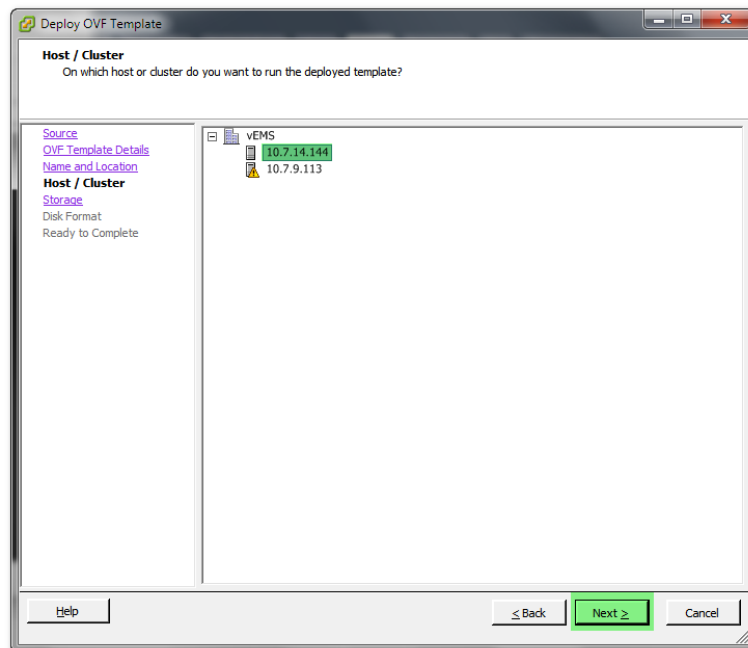
**Figure 7-4: OVF Template Details Screen**



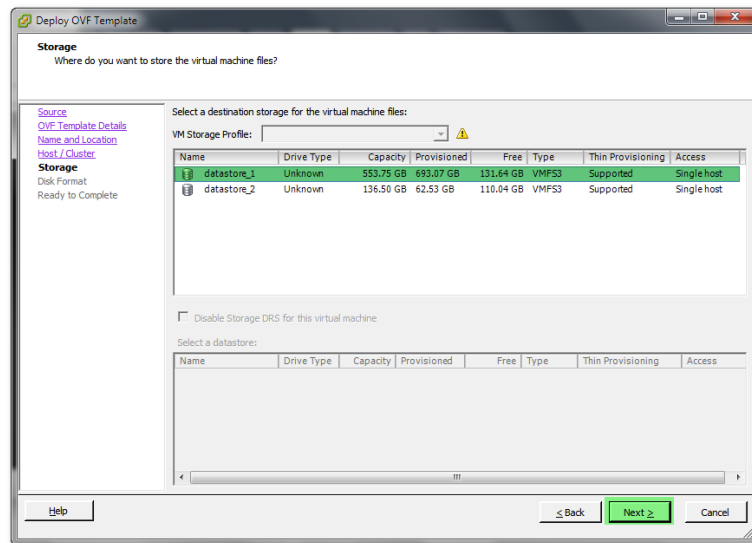
4. In the OVF Template Details screen, click **Next**.

**Figure 7-5: Virtual Machine Name and Location Screen**

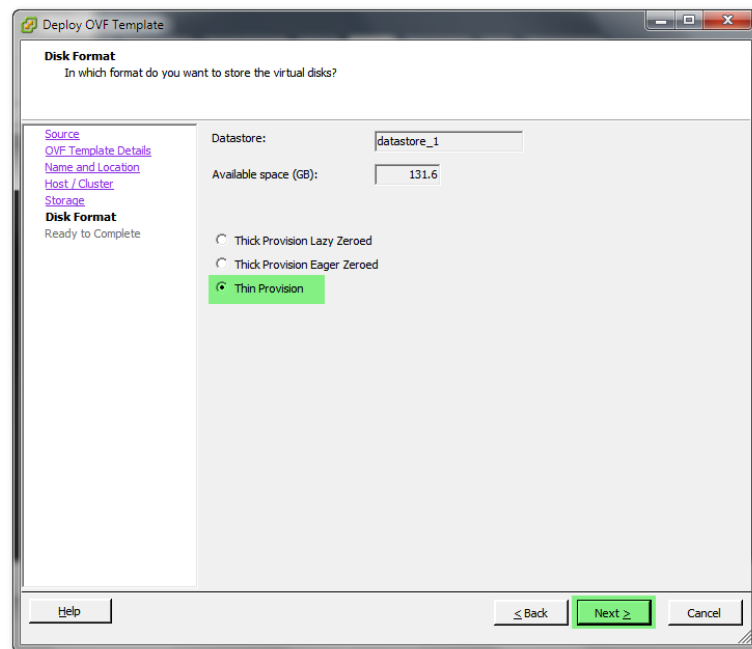
5. In the Name and Location screen, enter the desired virtual machine name and choose the inventory location (the data center to locate the machine), and then click **Next**.

**Figure 7-6: Host / Cluster Screen**

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

**Figure 7-7: Destination Storage Screen**


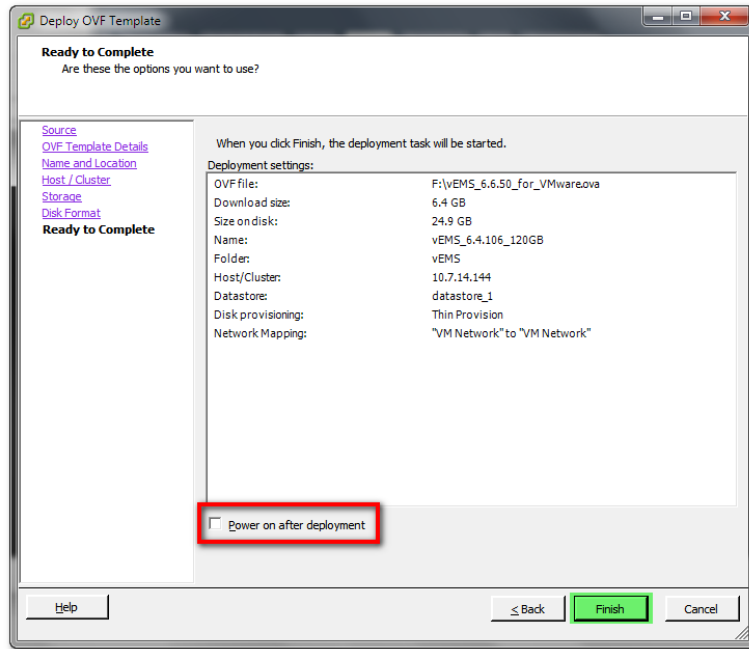
- In the Storage screen, select the data store where you'd like to locate your machine, and then click **Next**.

**Figure 7-8: Disk Format Screen**


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

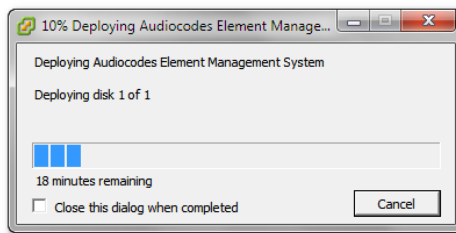


Figure 7-9: Ready to Complete Screen

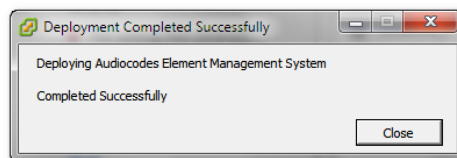


- In the Ready to Complete screen, leave the option 'Power on after deployment' unchecked, and then click **Finish**.

Figure 7-10: Deployment Progress Screen

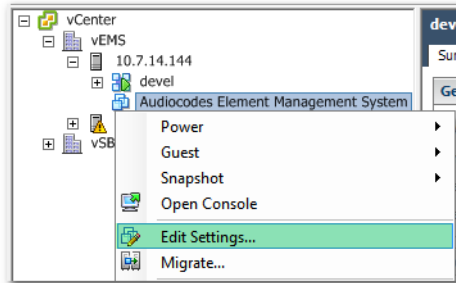
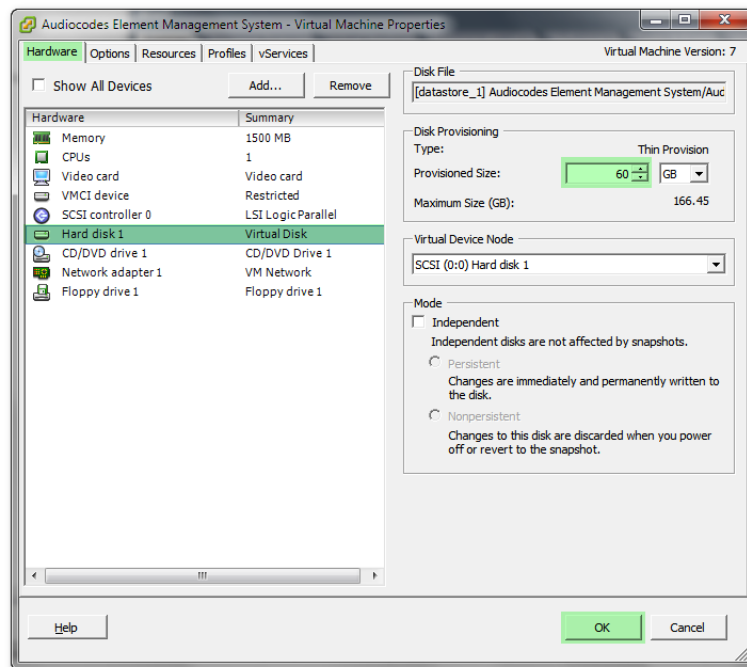


Recent Tasks			
Name	Target	Status	Requested Start Time
Deploy OVF template	Audiocodes Element Management System	14%	21/05/2012 09:32:26



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

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

**Figure 7-11: Edit Settings option**

**Figure 7-12: Hard Disk Settings**


12. In the **Hardware** tab, select the **Hard disk** item, and then set the 'Provisioned Size' parameter accordingly to the desired EMS server VMware Disk Space allocation (see Section 3 on page 25), and then click **OK**.



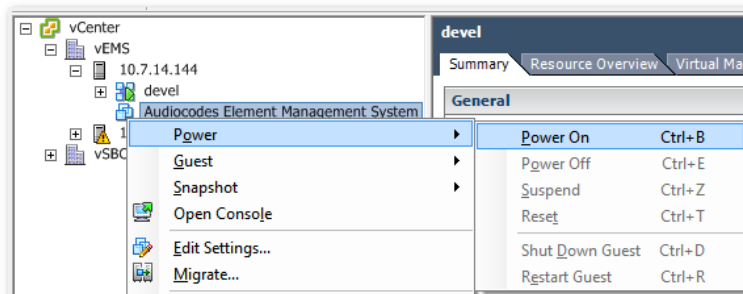
**Note:** Once the hard disk space allocation has been increased, it cannot be reduced to a lower amount.

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

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

- Power on the machine; in the vCenter tree, right-click the AudioCodes Element Management System and in the drop-down menu, choose Power > Power On. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications (see Section 3 on page 25).

Figure 7-13: Power On



- Wait until the boot process is complete, and then connect the running server via the vSphere client console.

Figure 7-14: vSphere Client Console

```

Audiocodes Element Management System
Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views

Loading mibs for MG v5.8 machine ...
Loading mibs for MG v6.0 machine .....
Loading mibs for MG v6.2 machine .....
Loading mibs for MP v6.0 machine .....
Loading mibs for MP v6.2 machine .....
Loading mibs for MP v6.4 machine .....
All mibs loaded successfully.
Finish SNMP Handler: Tue May 22 14:36:41 BST 2012
Binding the EMS server to the RMI registry...
=====
EMS Server 6.4.115 is up!
=====
Start Up At:Tue May 22 14:36:43 BST 2012

CentOS release 5.3 (Final)
Kernel 2.6.18-194.32.1.el5 on an x86_64

ems-server login: Http Secured: null

CentOS release 5.3 (Final)
Kernel 2.6.18-194.32.1.el5 on an x86_64

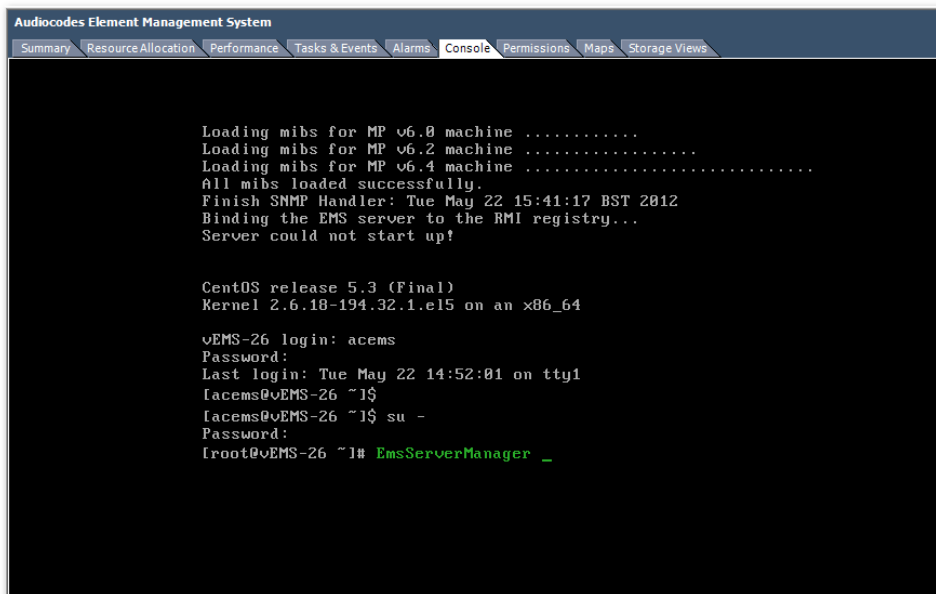
ems-server login: _

```

- Login to the server as **acems** user and enter *acems* password.
- Switch user to 'root' and enter password *root*.

18. Proceed to the network configuration using the Ems Server Manager. To run the manager type 'EmsServerManager' and press **Enter**.

**Figure 7-15: EMS Server Manager Prompt**



```

Audiocodes Element Management System
Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views

Loading mibs for MP v6.0 machine .....
Loading mibs for MP v6.2 machine .....
Loading mibs for MP v6.4 machine .....
All mibs loaded successfully.
Finish SNMP Handler: Tue May 22 15:41:17 BST 2012
Binding the EMS server to the RMI registry...
Server could not start up!

CentOS release 5.3 (Final)
Kernel 2.6.18-194.32.1.el5 on an x86_64

vEMS-26 login: acems
Password:
Last login: Tue May 22 14:52:01 on tty1
[acems@vEMS-26 ~]$
[acems@vEMS-26 ~]$ su -
Password:
[root@vEMS-26 ~]# EmsServerManager _
    
```

19. In the Ems Server Manager, choose the **Change Server's IP Address** option. This menu option is most likely not visible due to low console resolution, therefore type **3** and **Enter** to display the network configuration menu.

**Figure 7-16: Element Management System Menu Option**



```

Audiocodes Element Management System
Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views

10 ) Configure Server SNMPv3 Engine ID

Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options

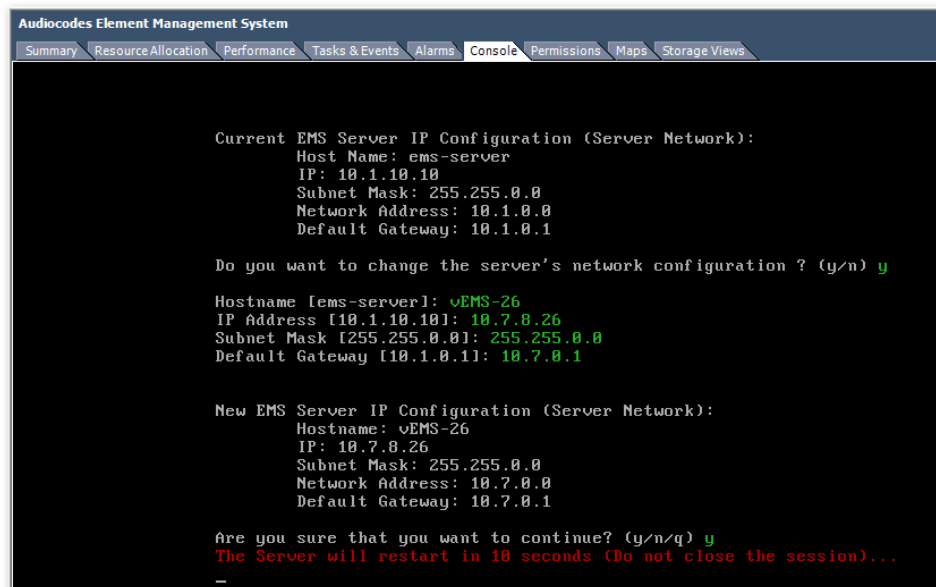
Maintenance:
17 ) Configure NTP
18 ) Change System Timezone
19 ) Change System Time & Date
20 ) Start/Stop EMS Server
21 ) Web Server Configuration
22 ) Backup the EMS Server
23 ) Schedule Backup for the EMS Server
24 ) Restore the EMS Server
25 ) Reboot the EMS Server
26 ) HA Configuration
27 ) Syslog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

q ) Quit
: 3_
    
```

20. In the Network Configuration menu, type **y** to modify the configuration, and then provide the desired details, such as hostname, IP address, subnet mask and default gateway.

21. Enter **y** to apply the new configuration; the EMS server is automatically restarted to complete the configuration process.

**Figure 7-17: EMS Server Network Configuration Details**



```
Audiocodes Element Management System
Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views

Current EMS Server IP Configuration (Server Network):
Host Name: ems-server
IP: 10.1.10.10
Subnet Mask: 255.255.0.0
Network Address: 10.1.0.0
Default Gateway: 10.1.0.1

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

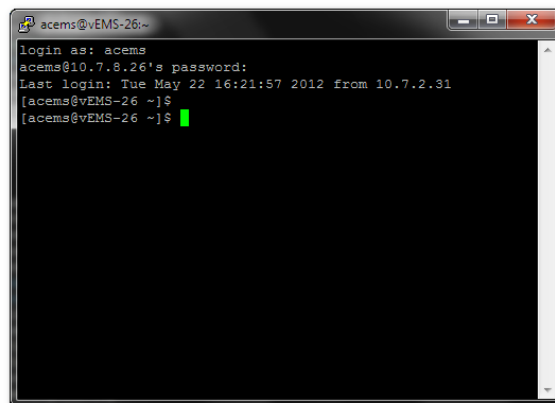
Hostname [ems-server]: vEMS-26
IP Address [10.1.10.10]: 10.7.8.26
Subnet Mask [255.255.0.0]: 255.255.0.0
Default Gateway [10.1.0.1]: 10.7.0.1

New EMS Server IP Configuration (Server Network):
Hostname: vEMS-26
IP: 10.7.8.26
Subnet Mask: 255.255.0.0
Network Address: 10.7.0.0
Default Gateway: 10.7.0.1

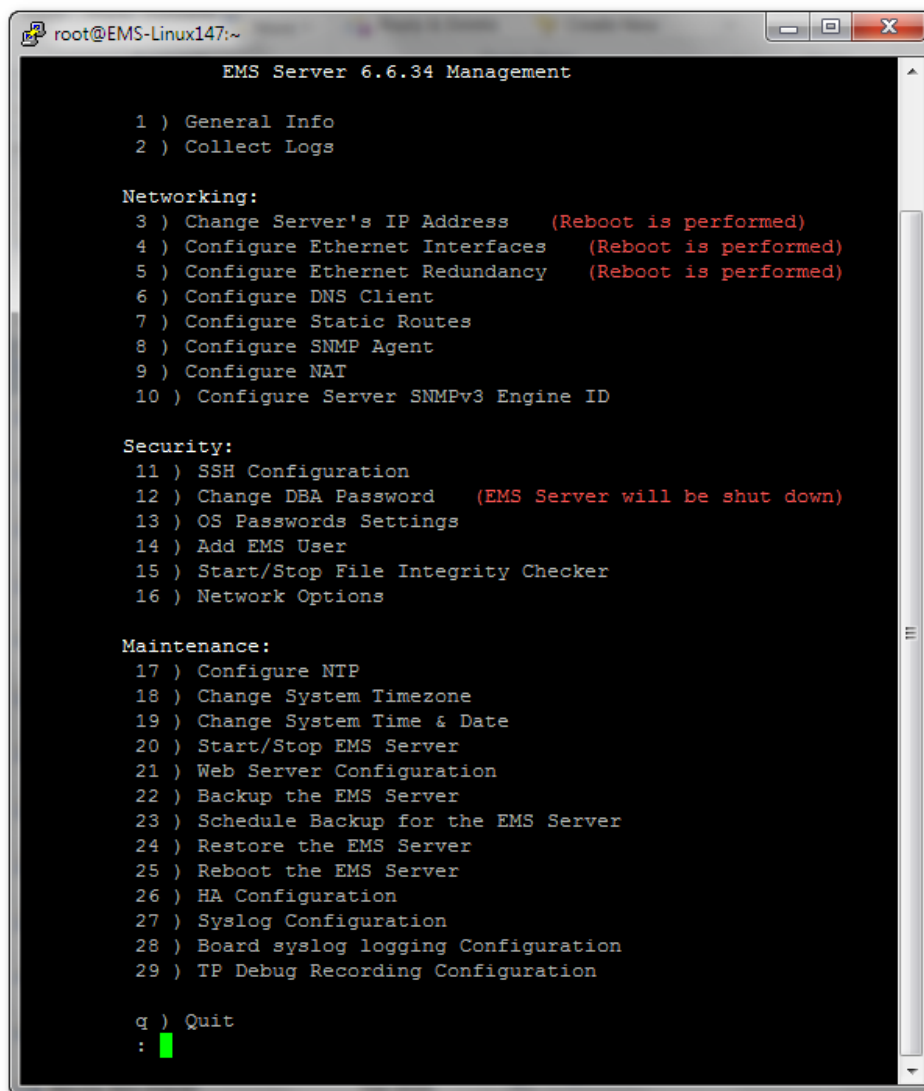
Are you sure that you want to continue? (y/n/q) y
The Server will restart in 10 seconds (Do not close the session)...
```

Following the reboot, the user has the option to connect to the EMS Server Manager using the SSH client.

**Figure 7-18: SSH Client Login**



```
acems@vEMS-26:~$ ssh acems@10.7.8.26
login as: acems
acems@10.7.8.26's password:
Last login: Tue May 22 16:21:57 2012 from 10.7.2.31
[acems@vEMS-26 ~]$
[acems@vEMS-26 ~]$
```

**Figure 7-19: EMS Server Manager - Main Menu**


```

root@EMS-Linux147:~
EMS Server 6.6.34 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
10 ) Configure Server SNMPv3 Engine ID

Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options

Maintenance:
17 ) Configure NTP
18 ) Change System Timezone
19 ) Change System Time & Date
20 ) Start/Stop EMS Server
21 ) Web Server Configuration
22 ) Backup the EMS Server
23 ) Schedule Backup for the EMS Server
24 ) Restore the EMS Server
25 ) Reboot the EMS Server
26 ) HA Configuration
27 ) Syslog Configuration
28 ) Board syslog logging Configuration
29 ) TP Debug Recording Configuration

q ) Quit
: █
    
```

- 22.** Perform configuration actions as required using the EMS Server Manager. See Section 10 on page 83.

# Part III

## EMS Server Upgrade

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





## 8 Upgrading the EMS Server on Dedicated Hardware

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



**Important:** Prior to performing the upgrade, it is highly recommended to perform a complete backup of the EMS server. For more information, see Section B on page 221.

You can perform the EMS version upgrade using one of the following methods:

- Upgrade from the AudioCodes supplied DVD3
- Upgrade from the AudioCodes supplied TAR file
  
- For EMS versions 2.2, 3.0, 3.2, 5.0, 5.2, 5.4 and 5.6:  
A major version upgrade of the EMS from above versions is not supported. Instead, users must perform a full installation of version 6.6 as described in Section 6 on page 37.
- For EMS versions 6.4, 6.2 and 6.0:  
A major and minor version upgrade of the EMS from the above versions is supported. For a detailed procedure, see the following section.

## 8.1 Upgrading the EMS Server on the Solaris Platform

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

To upgrade the EMS server to version 6.6, only DVD3 is required.



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

➤ **To upgrade the EMS server:**

1. Insert **DVD3-EMS server application** into the DVD ROM.
2. Login into the EMS server by SSH, as 'acems' user, and enter *acems* password.
3. Switch to 'root' user and provide *root* password by specifying the following command:

```
su - root
```

4. Verify access to the EMS server's CDROM drive. There is a possibility that specific hardened servers may block access to this CDROM. To regain access, type the following command as 'root' user:

```
mount -F hsfs -r /dev/dsk/c0t0d0s0 /cdrom
```

5. Run the installation script from its location by specifying the following command:

```
cd /cdrom/ems_dvd/EmsServerInstall/  
./install
```

**Figure 8-1: EMS Server Upgrade (Solaris)**

```
EMS-Server17%  
EMS-Server17% su - root  
Password:  
EMS-Server17# cd /cdrom/ems_dvd/EmsServerInstall  
EMS-Server17# ./install
```

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

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

```

based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respect
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall remain
11.5. Assignment Neither this Agreement or any of Licensee's rights or obligations
without the prior written permission of Licensor and any attempt to do so shall be without effect.
(ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regulated
export commodity, and may require a license to export such. Licensee is solely responsible
for obtaining any such license.
11.7. Relationship of Parties Nothing herein shall be deemed to create an agency
relationship between the parties. Neither party shall have the right to bind the other to any
contract or agreement not entered into by the party.
11.8. Integration This Agreement is the complete and exclusive agreement between
the parties hereto. Any Licensee purchase order issue for the software, documentation or
services hereof.
11.9. Counterparts This Agreement may be executed in multiple original counterparts,
each of which shall be deemed to be an original and all of which together shall constitute
one and the same agreement. This Agreement shall be binding upon the parties upon the
obtaining an authorized signature of Licensor and Licensee.

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

```

7. OS patches are installed.

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



**Note:** This step is optional and depends upon which version you are upgrading.

Figure 8-3: EMS Server Upgrade (Solaris) – Patch Installation

```

The following patches were successfully installed:
118666-27;118667-27;141500-08;

Reboot is needed

+++++
EMS Server must be rebooted to proceed with the installation.

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

Press Enter to reboot...

```

8. After the EMS server has rebooted, repeat steps 2 – 6.
9. Accept the Java License agreement by entering **y** and pressing **Enter**.



**Note:** This step is optional and depends upon which version you are upgrading.

**Figure 8-4: EMS Server Upgrade (Solaris) - License Agreement (Java)**

```
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 UPON THE CONDITION
THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY
CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS
(COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT
```

```
I. Installation and Auto-Update. The Software's
installation and auto-update processes transmit a limited
amount of data to Sun (or its service provider) about those
specific processes to help Sun understand and optimize
them. Sun does not associate the data with personally
identifiable information. You can find more information
about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150
Network Circle, Santa Clara, California 95054, U.S.A.

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

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



**Note:** This step is optional and depends upon which version you are upgrading.

**Figure 8-5: EMS Server Upgrade (Solaris) - License Agreement (Java) (cont)**

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

Press Enter to continue....

```

11. Accept the Java License agreement, by pressing **y** and **Enter**.

**Figure 8-6: EMS Server Upgrade (Solaris) - License Agreement (Java) (cont)**

```
I. Installation and Auto-Update. The Software's
installation and auto-update processes transmit a limited
amount of data to Sun (or its service provider) about those
specific processes to help Sun understand and optimize
them. Sun does not associate the data with personally
identifiable information. You can find more information
about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150
Network Circle, Santa Clara, California 95054, U.S.A.

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

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

**Figure 8-7: EMS Server Upgrade (Java) (cont)**

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

Press Enter to continue.....

```

- Wait for the installation to complete, and then reboot the EMS server.

**Figure 8-8: EMS Server Upgrade (Solaris) Complete**

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

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

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

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

## 8.2 Upgrading the EMS Server on the Linux Platform

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

To upgrade the EMS server on the Linux platform to version 6.6, only DVD3 is required. Verify in the EMS Manager 'General Info' screen that you have installed the latest Linux revision (OS Revision **Rev4**), see Section 10.1.1 on page 88. If you have an older OS revision, a clean installation must be performed using all three DVDs (see Section 6.2 on page 48).



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file

### ➤ To upgrade the EMS server on the Linux platform:

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

```
su - root
```

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

```
mount /misc/cd
```

5. Run the installation script from its location:

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

**Figure 8-9: EMS Server Upgrade (Linux)**

```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/  
[root@EMS-Linux2 EmsServerInstall]# ./install  
DIR Name /misc/cd/EmsServerInstall  
Start installValues  
  >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...  
Login Check Successfully Passed.  
  
  >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
  >>> >>> PASSED  
  ...  
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
SOFTWARE LICENSE AGREEMENT  
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I  
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N  
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND  
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG  
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

Figure 8-10: EMS Server Upgrade (Linux) – License Agreement

```

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

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

```

7. OS patches are installed.

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



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

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

```

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

```

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

Figure 8-11: EMS Server Application Upgrade (Linux) - Java Installation

```

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

Press Enter to continue....

```

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



**Figure 8-12: EMS Server Upgrade (Linux) Complete**

```

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

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

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

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



## 8.3 Upgrading from the Installation TAR file

This section describes how to upgrade from the AudioCodes supplied installation TAR file. This procedure is identical for both the Linux and Solaris platforms.



**Important:** If you are performing a minor version upgrade using the supplied TAR file, consult with your AudioCodes representative to verify whether any new OS or Database patches have been issued (the TAR installation file package does not include OS and Database patches).



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

### ➤ To upgrade from the Installation TAR file:

1. Log into the EMS server as 'acems' user with password *acems*.
2. Transfer TAR file using SFTP to */export/home/acems* directory.
3. Switch to 'root' user by specifying the following command:

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

4. Copy TAR file into */ACEMS* directory.

Figure 8-13: EMS Server Upgrade from TAR File

```
Netra-T5220# cd /ACEMS
Netra-T5220# ls -l
total 885672
drwxr-xr-x  2 root    root          512 May 28 09:12 auto_config_scripts
drwxr-xr-x  2 oracle dba           512 May 29 11:01 backup_scripts
-rw-r--r--  1 root    root            0 May 27 14:47 cd2flag
drwxr-xr-x  6 root    root          512 May 27 17:27 EMS-VQ
-rw-----  1 root    root    446876160 Jun 12 17:53 emsServerDeploy_6.6.165.tar
drwxr-xr-x  5 root    root          512 May 27 17:16 HA
-rw-r--r--  1 acems  root        4384 May 27 16:57 installPatches.log
drwxr-xr-x  2 emsadmin dba         1024 May 27 17:19 lib
drwxr-x---  8 emsadmin nbif          512 Jun 11 18:37 NBIF
drwxr-xr-x  2 oracle dba           512 May 27 17:31 opatch
drwxr-xr-x  3 oracle dba         1024 May 27 17:28 oracle_hardening
-rw-r--r--  1 root    root    6317087 May 27 16:44 os_patch.log
drwxr-xr-x  5 root    root          512 May 27 13:55 preinstall_scripts
drwxr-xr-x  2 root    root          512 May 27 17:15 recovery_scripts
drwxr-xr-x  2 oracle dba         1536 May 27 17:28 schema_scripts
drwxr-xr-x 11 root    root        1536 Jun 11 18:37 server_6.6.164
drwxr-xr-x  2 emsadmin dba          512 May 29 10:58 yafic
Netra-T5220#
```

5. If the previous installation or upgrade was performed from the installation TAR file, remove the folder '/ACEMS/EmsServerInstall' by specifying the following command:

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

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

```
> tar -xf emsServerDeploy_6.6.xx.tar
```

7. When the installation TAR file has opened successfully, the new directory '/ACEMS/EmsServerInstall' is created.

8. In the directory '/ACEMS/EmsServerInstall' run the installation script:

```
> cd /ACEMS/EmsServerInstall  
> ./install
```

9. Perform steps 6 to 13 in Section 8.1 on page or perform steps 6 and 6 in Section 8.2 on page 74.

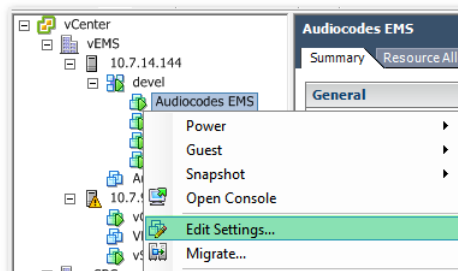
## 9 Upgrading the EMS Server on the VMware Platform

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

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

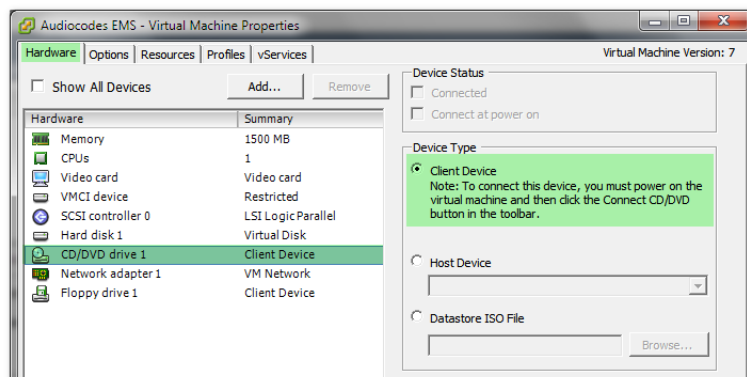
1. Insert the vEMS installation DVD into the disk reader on the PC with the installed vSphere client.
2. In the vCenter navigation tree, right-click the AudioCodes EMS node and choose the **Edit Settings** option.

**Figure 9-1: Edit Settings Option**



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

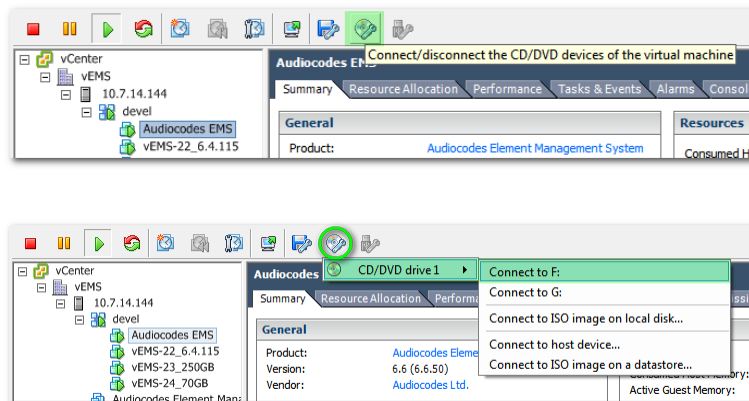
**Figure 9-2: Hardware Tab**



Name	Target	Status	Requested Start Time	Start Time	Completed Time
Reconfigure virtual machine	AudioCodes EMS	Completed	21/05/2012 10:00:08	21/05/2012 10:00:08	21/05/2012 10:00:19

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

**Figure 9-3: Connect/disconnect Button**



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

```
su -
```

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



**Note:** Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

- Change directory to `/misc/cd/EmsServerInstall` and run the install script.

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

**Figure 9-4: EMS Server Installation Script**

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

>>> Check CD Sequence - Mon May 21 08:29:59 BST 2012
...
>>> >>> PASSED
...
>>> Verifying OS version - Mon May 21 08:29:59 BST 2012
...
SOFTWARE EVALUATION LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS SOFTWARE
EVALUATION AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE
AGREEMENT FOR THE AUDIOCODES SOFTWARE (THE "PROGRAM") AND
THE ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE
```

- Proceed to step 6 in Section 8.2 on page 74.

# Part IV

## EMS Server Machine Maintenance

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



## 10 EMS Server Manager

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



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



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

You can either run the EMS Server Manager utility locally or remotely:

- If you wish to run it remotely, then you connect to the EMS server using Secure Shell (SSH).
- If you wish to run it locally, then connect using the management serial port or keyboard and monitor.



**Note:**

- If you are logging into a Solaris machine and have not performed hardening, then you can also connect using Telnet.
- If you connect remotely using SSH, the full menu is displayed including hardening options, such as Basic Hardening, Advanced Hardening and Strict PKI Configuration.

➤ **Do the following:**

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

```
# EmsServerManager
```

The EMS Server Manager menu is displayed.

Figure 10-1: EMS Server Manager Menu (All options with SSH connection on Solaris)

```

    EMS Server 6.6.164 Management

    1 ) General Info
    2 ) Collect Logs

    Networking:
    3 ) Change Server's IP Address (Reboot is performed)
    4 ) Change Additional SNMP Manager's IP Address
    5 ) Configure Ethernet Interfaces (Reboot is performed)
    6 ) Configure Ethernet Redundancy (Reboot is performed)
    7 ) Configure DNS Client
    8 ) Configure Static Routes
    9 ) Configure SNMP Agent
    10 ) Configure NAT
    11 ) Configure Server SNMPv3 Engine ID

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

    Maintenance:
    20 ) Configure NTP
    21 ) Change System Timezone (Reboot is performed)
    22 ) Change System Time & Date
    23 ) Start/Stop EMS Server
    24 ) Web Server Configuration
    25 ) Enable/Disable Jumpstart Services
    26 ) Backup the EMS Server
    27 ) Schedule Backup for the EMS Server
    28 ) Restore the EMS Server
    29 ) Reboot the EMS Server
    30 ) Syslog Configuration
    31 ) Board syslog logging Configuration
    32 ) TP Debug Recording Configuration

    q ) Quit
    : █
  
```



Figure 10-2: Ems Server Manager Menu (Linux)

```
EMS Server 6.6.164 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
10 ) Configure Server SNMPv3 Engine ID

Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
17 ) Start/Stop Software Integrity Checker (AIDE) and Prelinking
18 ) Enable/Disable USB Storage
19 ) Auditd Options

Maintenance:
20 ) Configure NTP
21 ) Change System Timezone
22 ) Change System Time & Date
23 ) Start/Stop EMS Server
24 ) Web Server Configuration
25 ) Backup the EMS Server
26 ) Schedule Backup for the EMS Server
27 ) Restore the EMS Server
28 ) Reboot the EMS Server
29 ) HA Configuration
30 ) Syslog Configuration
31 ) Board syslog logging Configuration
32 ) TP Debug Recording Configuration

q ) Quit
: █
```


**Important:**

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

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

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

- [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)
- Change Additional SNMP Manager's IP Address (only on a Solaris based server)
- Configure Ethernet Interfaces (Reboot is performed)
- Configure Ethernet Redundancy (Reboot is performed)
- Configure DNS Client
- Configure Static Routes
- Configure SNMP Agent
- Configure NAT
- Configure Server SNMPv3 Engine ID

- [Security](#) – These options manage all the relevant security configurations.

Security full menu:

- Basic Hardening (only with SSH connection, on a Solaris based server, reboot is performed).
- Advanced Hardening (only with SSH connection on a Solaris based server, reboot is performed).
- SSL Tunneling Configuration (only with SSH connection, on a Solaris based server)

- Strict PKI Configuration (only with SSH connection on a Solaris based server)
- SSH Configuration (only with SSH connection on a Linux based server)
- Change DBA Password (EMS Server will be shut down)
- OS Passwords Settings
- Add EMS User
- Start/Stop File integrity checker
- Network Options (only on a Linux based server)
- Start/Stop Software Integrity Checker (AIDE) and Prelinking (only on a Linux based server)
- Enable/Disable USB Storage (only on a Linux based server)
- Auditd Options (only on a Linux based server)
- **Maintenance** – These options manage all system maintenance actions.  
Maintenance menu:
  - Configure NTP
  - Change System Timezone (Reboot is performed on Solaris based server)
  - Change System Time & Date
  - Start / Stop the EMS Server
  - Web Server Configuration
  - Enable/Disable Jumpstart Services (only on Solaris based server)
  - Backup the EMS Server
  - Schedule Backup for the EMS Server
  - Restore the EMS Server
  - Reboot the EMS Server
  - HA Configuration (only on Linux based server)
  - Syslog Configuration
  - Board Syslog Logging Configuration
  - TP Debug Recording Configuration
  - Quit



**Note:** The screens displaying the Main menu options in the procedures described in this section are based on a Linux installation with 'root' user permissions.

## 10.1 General Info and Logs Collection

This section describes the General Information and Logs collection options.

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

➤ **To view General Info:**

- In the EMS Server Management menu, choose **General Info** option, and then press **Enter**.

**Figure 10-3: EMS Server Manager – General Info**

```

EMS Server 6.6.44 Management

1 ) General Info
2 ) Collect Logs

```

The **General Information** screen is displayed.

**Figure 10-4: General Info Display**

```

General Info
EMS Version: 6.6.44
OS Version: Linux 2.6.18-194.32.1.el5 x86_64
OS Revision: CentOS 5.3 for EMS Server (Rev. 4)

Java Version: java full version "1.6.0_31-b04"
Memory Size: 2057676 kB
ACEMS Disk Usage:
Swap Spaces:
Filename                Type          Size   Used   Priority
/dev/mapper/vg-swap      partition    3080184 347176  -1
EMS Watchdog Status: Up
EMS Server Process Status: Up
EMS SEM Server Process Status: Up
Tomcat Server Process Status: Up
EMS Security Status: , Oracle Hardening

Apache Server Status: Up
Apache Version:
Server version: Apache/2.2.3
Server built:   Aug 30 2010 12:28:40
Oracle Server Processes Status:
DB Processes Status: Up
Oracle Listner Status: Up
Number of DB Connections: 8
SNMP Agent Status: Up
NTP Daemon Status: Up
=====
remote      refid      st t when poll reach  delay  offset  jitter
=====
*LOCAL(0)   .LOCL.    10 1   13  64  377  0.000  0.000  0.001
Time: [19/06/2012 12:18:57]
Time Zone: GMT

NAT Configuration:
Not configured

```

Figure 10-5: General Info Display (cont)

```

Network Configuration:
Server's Network:
    Interface      : eth0
    Host Name      : EMS-Linux143
    IP Address     : 10.7.14.143
    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:
    Not configured

Session Type: SSH
User: root (Full Control)

Press Enter to Continue

```

## 10.1.2 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**.

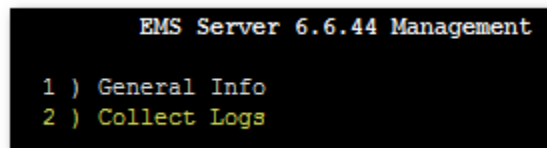
The following log files are collected:

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

➤ **To collect logs:**

- In the EMS Server Management menu, choose **Collect Logs** option, and then press **Enter**.

**Figure 10-6: EMS Server Manager – Collect Logs**



```
EMS Server 6.6.44 Management
1 ) General Info
2 ) 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.

## 10.2 Networking

This section describes the networking options in the EMS Server Manager. The following options are described in this section:

- Change Server's IP Address. See Section 10.2.1 on page 92.
- Add SNMP Manager. See Section 10.2.2 on page 94.
- Configure Ethernet Interfaces. See Section 10.2.3 on page 95.
- Configure Ethernet Redundancy (Linux). See Section 10.2.4 on page 100.
- Configure Ethernet Redundancy (Solaris). See Section 10.2.5 on page 105.
- Configure the DNS Client. See Section 10.2.6 on page 109.
- Configure Static Routes. See Section 10.2.7 on page 111.
- SNMP Agent. See Section 10.2.8 on page 113.
- Configure NAT. See Section 10.2.9 on page 115.
- Configure Server SNMPv3 Engine ID. See Section 10.2.10 on page 116.

### 10.2.1 Change Server's IP Address

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



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

#### ➤ To change Server's IP Address:

1. In the EMS Server Manager menu, choose **Change Server's IP address** option, and then press **Enter**.

**Figure 10-7: EMS Server Manager – Change Server's IP Address**

```

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
10 ) Configure Server SNMPv3 Engine ID
    
```

The current IP Configuration is displayed.

2. Configure IP configuration parameters as desired.



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

**Figure 10-8: 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
```

**Figure 10-9: User Configuration Updates**

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

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

3. Type **y** to confirm the changes, and then press **Enter**.  
The EMS server is restarted automatically to update this action.

**Figure 10-10: IP Configuration Complete**

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

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

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

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

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

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

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

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

## 10.2.2 Add SNMP Manager

This option is used to add an additional SNMP Manager to all managed devices.

When adding a device to EMS, EMS sets its IP address in the device's Trap Destinations table. When setting an IP address in "Change Additional SNMP Manager's IP Address" option, this IP address will also be added to the device's Trap Destinations table.



**Note:** When this operation has completed, restart the EMS manually for the changes to take effect.

### ➤ To change Server's IP Address:

1. In the EMS Server Manager menu, choose **Change Additional SNMP Manager's IP Address** option, and then press **Enter**.

Figure 10-11: EMS Server Manager – Change Additional SNMP Manager's IP Address

```

EMS Server 6.6.164 Management

1 ) General Info
2 ) Collect Logs

Networking:
3 ) Change Server's IP Address (Reboot is performed)
4 ) Change Additional SNMP Manager's IP Address
5 ) Configure Ethernet Interfaces (Reboot is performed)
6 ) Configure Ethernet Redundancy (Reboot is performed)
7 ) Configure DNS Client
8 ) Configure Static Routes
9 ) Configure SNMP Agent
10 ) Configure NAT
11 ) Configure Server SNMPv3 Engine ID
  
```

2. Configure the additional SNMP manager IP address and confirm by typing **y**.

Figure 10-12: Additional Manager's Configuration

```

Additional Manager's Configuration:
Additional Manager's IP Address (-1 to disable this feature) [-1]: 10.3.180.80
Are you sure that you want to continue ? (y/n/q)y
  
```

## 10.2.3 Configure Ethernet Interfaces

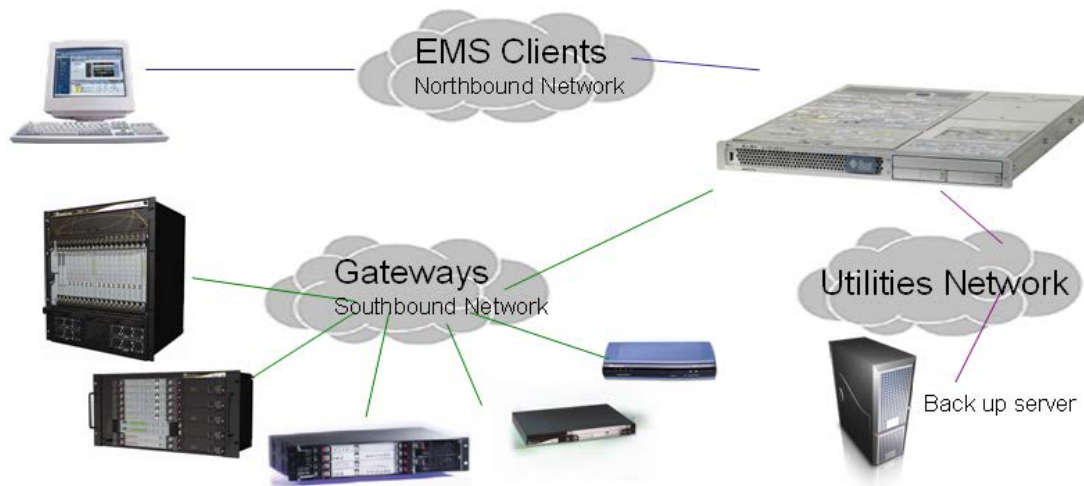
This section describes how to configure ethernet interfaces.

### 10.2.3.1 EMS Client Login on all EMS server Network Interfaces

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

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

**Figure 10-13: EMS Server: Triple Ethernet Interfaces**



In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound Network' to each one of the subnets. For Static Routes configuration, see Section 10.2.7 on page 111.

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

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

➤ **To configure Ethernet Interfaces:**

1. In the EMS Server Manager menu, choose **Configure Ethernet Interfaces** option, and then press **Enter**.

**Figure 10-14: EMS Server Manager – Configure Ethernet Interfaces**

```

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
10 ) Configure Server SNMPv3 Engine ID
  
```



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

The 'Ethernet Interface Configuration' sub-menu is displayed.

**Figure 10-15: Physical Interface Configuration Menu**

```

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. See Section 10.2.3.2 on page 97.
  - **Remove Interface** – Removes an existing interface from the EMS server. See Section 10.2.3.3 on page 98.
  - **Modify Interface** – Modifies an existing interface from the EMS server. See Section 10.2.3.4 on page 99.

### 10.2.3.2 Add Interface

This section describes how to add a new interface.

➤ **To Add a New Interface:**

1. Choose option **1**; a list of currently available interfaces (not yet configured) is 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. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

**Figure 10-9: Add Interface Parameters**

```
Add Interface:

Choose Interface:
  1) 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
```

### 10.2.3.3 Remove Interface

This section describes how to remove an interface.

➤ **To remove an existing interface:**

1. Choose option **2**.
2. Choose the interface to remove.  
A list of currently configured interfaces is displayed.
3. Type **y** to confirm the changes; the EMS server reboots for the changes to take effect.

**Figure 10-9: 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
  
```

### 10.2.3.4 Modify Interface

This section describes how to modify an existing interface.

➤ **To modify an existing interface:**

1. Choose option **3**.
2. Choose the interface to modify; a list of currently configured interfaces is displayed.
3. Change the interface parameters.
4. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

**Figure 10-16: 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
```

## 10.2.4 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.

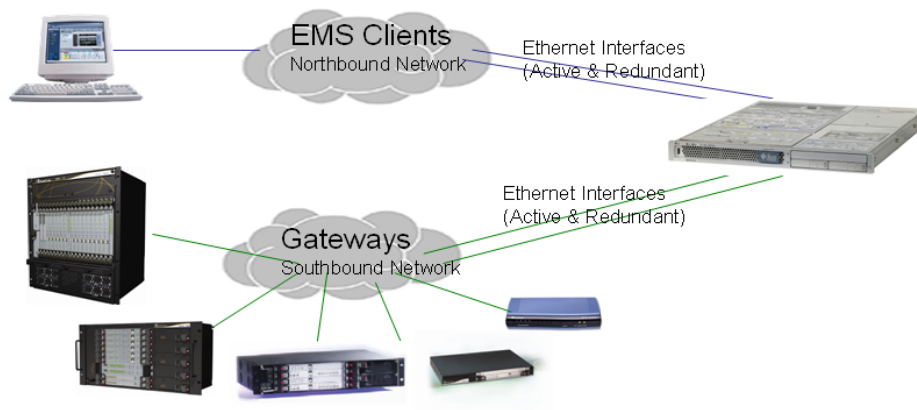
The EMS server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, EMS Clients [Northbound] and Gateways [Southbound]).

This option enables you to configure Ethernet ports redundancy.



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

**Figure 10-17: Physical Ethernet Interfaces Redundancy**





➤ **To configure Ethernet Redundancy:**

1. In the EMS Server Management menu, choose **Configure Ethernet Redundancy** option, and then press **Enter**.

**Figure 10-18: EMS Server Manager – Configure Ethernet Redundancy**

```
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
10 ) Configure Server SNMPv3 Engine ID
```

The 'Ethernet Redundancy Configuration' sub-menu is displayed.

**Figure 10-19: 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. See Section 10.2.4.1 on page 102.
  - Remove Redundant Interface. See Section 10.2.4.2 on page 103.
  - Modify Redundant Interface. See Section 10.2.4.3 on page 104.

### 10.2.4.1 Add Redundant Interface

Use this option under the following circumstances:

- When you have configured an interface (see Section **Error! Reference source not found.** on page **Error! Bookmark not defined.**).
- When your default router can respond to a ping command due to a heartbeat procedure between interfaces and the default router (to verify activity).

➤ **To add redundant interface:**

1. Choose option 1.
2. Choose the network type for which to create a new redundant interface (for example, **EMS Client-Server Network**).
3. Choose the interface in the selected network that you wish to make redundant (for example, **bge1, bge2, bge3**).
4. 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. Type **y** to confirm the changes; the EMS automatically reboots for changes to take effect.

**Figure 10-20: 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
  
```

### 10.2.4.2 Remove Ethernet Redundancy

This section describes how to remove an Ethernet redundancy interface.

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

1. Choose option **2**.
2. Choose the Ethernet Redundancy Interface to remove; the current network type Ethernet Redundancy configuration is displayed.
3. Type **y** to confirm the changes; the EMS automatically reboots for the changes to take effect.

**Figure 10-21: 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
```

### 10.2.4.3 Modify Redundant Interface

This section describes how to modify a redundant interface.

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

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

**Figure 10-22: 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
  
```

## 10.2.5 Configure Ethernet Redundancy on Linux

This section describes how to configure Ethernet Redundancy on Linux.

➤ **To configure Ethernet Redundancy:**

1. In the EMS Server Management menu, choose **Configure Ethernet Redundancy** option, and then press **Enter**.

```
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
10 ) Configure Server SNMPv3 Engine ID
```

The Ethernet Redundancy sub-menu is displayed.

**Figure 10-23: EMS Server Manager Ethernet Redundancy Configuration**

```
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 one of the following options:
  - Add Redundant Interface. See Section 10.2.5.1 on page 106.
  - Remove Redundant Interface. See Section 10.2.5.2 on page 107.
  - Modify Redundant Interface. See Section 10.2.5.3 on page 108.

### 10.2.5.1 Add Redundant Interface

Use this option when:

- You have configured an Ethernet interface (see Section **Error! Reference source not found.** on page **Error! Bookmark not defined.**).
- Your default router can respond to a 'ping' command, due to a heartbeat procedure between interfaces and the default router (to verify activity).

➤ **To add redundant interface:**

1. Choose option 1.
2. Choose the network type for which to create a new redundant interface (for example, **EMS Client-Server Network**).
3. Choose the interface in the selected network that you wish to make redundant (for example, **bge1, bge2, bge3**).
4. Choose the redundancy mode (for example, **balance-rr, active-backup**).
5. Type **y** to confirm the changes; the EMS automatically reboots for changes to take effect.

**Figure 10-24: Add Redundant Interface (Linux)**

```

Ethernet Redundancy Configuration

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

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

Add Redundant Interface:

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

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

Ethernet Redundancy Settings:

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

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

### 10.2.5.2 Remove Ethernet Redundancy

This section describes how to remove an Ethernet Redundancy interface.

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

1. Choose option **2**.
2. Choose the Ethernet Redundancy Interface to remove.  
The current network type Ethernet Redundancy configuration is displayed.
3. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

**Figure 10-25: 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
```

### 10.2.5.3 Modify Redundant Interface

This section describes how to modify a redundant interface.

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

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

**Figure 10-26: Modify Redundant Interface (Linux)**

```

Ethernet Redundancy Configuration

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

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

Modify Redundant Interface:

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

Ethernet Redundancy Settings:

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

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



## 10.2.6 Configure 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 refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

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

### ➤ To Configure the DNS Client:

1. In the EMS Server Management menu, choose **Configure DNS Client** option, and then press **Enter**.

**Figure 10-27: EMS Server Manager – Configure DNS Client**

```
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
10 ) Configure Server SNMPv3 Engine ID
```

The 'DNS Configuration' menu is displayed.

**Figure 10-28: DNS Client Sub-menu**

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

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

**Figure 10-29: Configure DNS Client – Specify Domain Name/Search List**

```

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 10-30: 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) █
  
```

## 10.2.7 Static Routes

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

### ➤ To configure static routes:

1. In the EMS Server Management menu, choose **Static Routes** option, and then press **Enter**.

**Figure 10-31: EMS Server Manager – Static Routes**

```

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
10 ) Configure Server SNMPv3 Engine ID

```

The Static Routes menu and all current static rules are displayed.

**Figure 10-32: 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**.
2. Enter the Destination Network Address.
3. Enter the router's IP address.
4. Type **y** to confirm these changes.

**Figure 10-33: 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**.
2. Enter the Destination Network Address for the static route you wish to remove.
3. Enter the router's IP address.
4. Type **y** to confirm these changes.

## 10.2.8 SNMP Agent

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

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

➤ **To configure SNMP Agent:**

1. In the EMS Server Manager root menu, choose **Configure SNMP Agent** option, and then press **Enter**.

**Figure 10-34: EMS Server Manager – Configure SNMP Agent**



```
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
10 ) Configure Server SNMPv3 Engine ID
```

The SNMP Manager screen is displayed with the Process ID information.

2. Choose from 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.

### 10.2.8.1 SNMP Manager Configuration

This section describes the SNMP Manager configuration.

➤ **To configure the SNMP Manager:**

1. Choose option 1.
2. Enter the **NMS IP address**.
3. Enter the **Community string**.
4. Type **y** to continue.

**Figure 10-35: 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) █
  
```

### 10.2.8.2 Sending System Alarms

This section describes how to send system alarms.

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

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

### 10.2.8.3 Stopping System Alarms

This section describes how to stop sending system alarms.

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

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

## 10.2.9 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. In the EMS Server Manager root menu, choose **Configure NAT** option, and then press **Enter**.

**Figure 10-36: EMS Server Manager – Configure NAT**

```
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
10 ) Configure Server SNMPv3 Engine ID
```

2. At the prompt, type the NAT IP address.
3. Type **y** to confirm the changes.
4. Stop and start the EMS server for the changes to take effect.

➤ **To remove NAT configuration:**

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

## 10.2.10 Configure Server SNMPv3 Engine ID

The EMS Server Manager includes the **Configure Server SNMPv3 Engine ID** option under the Networking sub-menu.

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

➤ **To configure the SNMPv3 Engine ID:**

1. In the EMS Server Manager root menu, choose **Configure Server SNMPv3 Engine ID** option, and then press **Enter**.

The 'SNMPv3 Engine ID' sub-menu is displayed:

**Figure 10-37: EMS Server Manager – Configure SNMPv3 Engine ID**

```

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
10 ) Configure Server SNMPv3 Engine ID
  
```

**Figure 10-38: EMS Server Manager – SNMPv3 Engine ID Configuration (cont)**

```

SNMPv3 Engine ID Configuration

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

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



**Figure 10-39: SNMPv3 Engine ID Configuration – Complete Configuration**

```
SNMPv3 Engine ID Configuration

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

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

## 10.3 Security

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

This Section describes the following options:

- Basic Hardening. See Section [10.3.1](#) on page [119](#).
- Advanced Hardening. See Section [10.3.2](#) on page [124](#).
- SSL Tunneling Configuration. See Section [10.3.3](#) on page [125](#).
- Strict PK Configuration. See Section [10.3.4](#) on page [127](#).
- SSH Server Configuration Manager. See Section [10.3.5](#) on page [128](#).
- Changing DBA Password. See Section [10.3.6](#) on page [149](#).
- OS Password Settings. See Section [10.3.7](#) on page [150](#).
- Add EMS User. See Section [10.3.8](#) on page [155](#).
- Start / Stop File Integrity Checker. See Section [10.3.9](#) on page [156](#).
- Network Options. See Section [10.3.10](#) on page [156](#).
- Start/Stop Software Integrity Checker (AIDE) and Pre-linking. See Section [10.3.11](#) on page [158](#).
- Enable/Disable USB Storage. See Section [10.3.12](#) on page [159](#).
- Auditd Options. See Section [10.3.13](#) on page [160](#).

### 10.3.1 Basic Hardening

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, see Section 11 on page 207.

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



**Note:** This option is not supported on the Linux operating system.



**Notes:**

- This option is only available when using secured shell (ssh).
- When the operation is finished, the EMS automatically reboots for the changes to take effect.
- 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 (CPE products), 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 Manager root menu, choose **Basic Hardening** option, and then press **Enter**.

**Figure 10-40: 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 'Hardening' sub-menu is displayed.

2. Choose one of the following options:
  - **1. Start Hardening - Close all services** – to close all services.
  - **2. Rollback (Open all services)** – to open all services.

### 10.3.1.1 Start Basic Hardening

This section describes how to start basic hardening.

➤ **To start basic hardening:**

1. Choose option 1.

The following prompt is displayed:

**Figure 10-41: 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?
  - Type **yes** to run the JASS package.
3. Wait a few minutes.
4. Choose a new password for the 'acems' user and for 'root' user. 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 EMS server without them.

Figure 10-42: 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 EMS automatically reboots for changes to take effect.

### 10.3.1.2 Rollback

This section describes how to rollback to open all services.

➤ To perform a rollback:

1. Choose option 2.



**Note:** If the EMS server is in an advanced hardened status (i.e., the script *emsAdvancedHarden.pl* has already been run on this server), see Section 10.3.2 on page 124.

Figure 10-43: 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 option 1 to roll back the last hardened package.

**Figure 10-44: 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 option 5 ALWAYS Keep.

**Figure 10-45: 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 fi
les:
4. ALWAYS Backup.
5. ALWAYS Keep.
6. ALWAYS Force.

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

```

4. Type y to remove the package.

**Figure 10-46: 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.  
When finished, the EMS automatically reboots for changes to take effect.

## 10.3.2 Advanced Hardening

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. This script changes file permissions/groups for several files in the system (Operating system and EMS application files) and removes the snoop utility from the system.

In addition, the Advanced Hardening script adds password and login restrictions, such as password aging limitations for 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 \(STIG\)](#)".



**Note:** Before performing Advanced Hardening, you must perform Basic Hardening (see Section 10.3.1 above). This option is not supported on the Linux Operating System.



**Note:**

- This option is only available when using secured shell (ssh).
- When the operation is finished, the EMS automatically reboots for the changes to take effect.
- Before implementing Advanced Hardening, please contact your AudioCodes FAE.
- During this procedure, do not press Ctrl+C.

### ➤ To configure advanced hardening:

1. In the EMS Server Manager root menu, choose **Advanced Hardening** option, and then press **Enter**.

**Figure 10-47: Activating the Advanced Hardening Feature**

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

2. Choose one of the following options:
  - **Option 1:** Enter **1** to start additional hardening of the system. The EMS server is now in 'Advanced Hardening' mode.
  - **Option 2:** Enter **2** to rollback to a non-secured system.



**Figure 10-48: 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 EMS server default status, see Section 10.3.1 on page 119.

### 10.3.3 SSL Tunneling Configuration

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.



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

#### ➤ To configure the EMS server for SSL Tunneling:

1. In the EMS Server Manager root menu, choose **SSL Tunneling Configuration** option, and then press **Enter**.

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

**Figure 10-49: 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. Choose option **2**. 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 10.3.3.1 on page 126 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**.
3. Choose option **3** to ensure that SSL Tunneling is the only possible communication option between the EMS client and the EMS server.

➤ **To disable SSL Tunneling:**

1. Choose option **3**.
2. Connect the EMS server via SSH.
3. Choose option **1**.

### 10.3.3.1 EMS Client-SSL Tunneling Configuration

This section describes the 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.

### 10.3.4 Strict PKI Configuration

The Strict PKI Configuration applies additional DOD PKI validations to the EMS server, EMS client or watchdog. For a full list of validations, see Section G.1 on page 243.



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

➤ **To enable Strict PKI Configuration:**

1. In the EMS Server Manager root menu, choose **Strict PKI Configuration** option.

**Figure 10-50: EMS Server Manager – Strict PKI Configuration**

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

The Strict PKI Configuration Manager displays the **Strict PKI Status**.

**Figure 10-51: EMS Server Manager – Strict PKI Configuration (cont)**

```
Strict PKI Configuration Manager:
Strict PKI Status: Disable

1) Enable Strict PKI
2) Back to Main Menu
: █
```

2. Choose option **1** to enable the Strict PKI validations.

## 10.3.5 SSH Server Configuration Manager

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

➤ **To configure SSH:**

1. In the EMS Server Manager root menu, choose **SSH Configuration** option.

**Figure 10-52: EMS Server Manager – SSH Configuration**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
```

The SSH Configuration Manager's sub-menu opens.

**Figure 10-53: SSH Configuration (cont)**

```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Disable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: █
```

This section describes the following options:

- Configure SSH Log Level. See Section [10.3.5.1](#) on page [129](#).
- Configure SSH Banner. See Section [10.3.5.2](#) on page [130](#).
- Configure SSH on Ethernet Interfaces. See Section [10.3.5.3](#) on page [132](#).
- Disable SSH Password Authentication. See Section [10.3.5.4](#) on page [136](#).
- Enable SSH IgnoreUserKnownHosts Parameter. See Section [10.3.5.5](#) on page [138](#).
- Configure SSH Allowed Hosts. See Section [10.3.5.6](#) on page [139](#).

### 10.3.5.1 Configure SSH Log Level

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

➤ **To configure the SSH Log Level:**

1. Choose option **1** to configure the SSH Log Level.  
The SSH sub-menu opens.

**Figure 10-54: SSH Log Level Manager**

```
SSH Log Level Manager:
Current LogLevel DEFAULT
Note: Changing LogLevel will restart SSH

1) QUIET
2) FATAL
3) ERROR
4) INFO
5) VERBOSE
6) DEBUG
7) DEBUG1
8) DEBUG2
9) DEBUG3
10) DEFAULT
11) Back to SSH Configuration Manager Menu
: █
```

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press **Enter**.  
The SSH daemon restarts automatically.

**Figure 10-55: SSH Log Level Manager Options**

```
SSH Log Level Manager:
Current LogLevel DEFAULT
Note: Changing LogLevel will restart SSH

1) QUIET
2) FATAL
3) ERROR
4) INFO
5) VERBOSE
6) DEBUG
7) DEBUG1
8) DEBUG2
9) DEBUG3
10) DEFAULT
11) Back to SSH Configuration Manager Menu
: 2
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
█
```

As an indication of a successful configuration, the Current Log Level status is updated to the value that you chose.

**Figure 10-56: SSH Log Current Level**

```
SSH Log Level Manager:
Current LogLevel FATAL
Note: Changing LogLevel will restart SSH
```

### 10.3.5.2 Configure SSH Banner

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

**Figure 10-57: Configure SSH Banner**

```
SSH Banner Manager:
Current Banner State: DISABLED
To change SSH Banner, please, change /etc/issue file.
Note: Changing Banner state will restart SSH

1) Enable SSH Banner
2) Back to SSH Configuration Manager Menu
: █
```

#### ➤ To configure the SSH banner:

1. Choose option **1** to configure the SSH Banner, and then press **Enter**.
2. Edit a '/etc/issue' file with the desired text.

**Figure 10-58: SSH Banner Manager**

```
SSH Banner Manager:
Current Banner State: DISABLED
To change SSH Banner, please, change /etc/issue file.
Note: Changing Banner state will restart SSH

1) Enable SSH Banner
2) Back to SSH Configuration Manager Menu
: 1
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
█
```

As an indication of a successful configuration, the Current Banner State displays the status **Enabled**.

**Figure 10-59: SSH Banner Manager State**

```
SSH Banner Manager:
Current Banner State: ENABLED
To change SSH Banner, please, change /etc/issue file.
Note: Changing Banner state will restart SSH
```

The default message is displayed as follows:

**Figure 10-60: SSH Banner Manager Configuration Complete**

```
Connecting to 10.7.14.143:22...
Connection established.
Escape character is '^@]'.
CentOS release 5.3 (Final)
Kernel \r on an \m
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Wed Jul  6 18:59:26 2011 from 10.7.2.31
Can't open perl script "/bin/check_max_sessions.pl": Permission denied
[acems@EMS-Linux143 ~]$
```

### 10.3.5.3 Configure SSH on Ethernet Interfaces

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

➤ **To configure SSH on ethernet interfaces:**

1. Choose option 3, and then press **Enter**.

**Figure 10-61: Configure SSH on Ethernet Interfaces**

```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Disable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: █
```

The 'Ethernet Interfaces – SSH Manager' sub-menu, including the list of currently configured Ethernet interfaces is displayed:

**Figure 10-62: Configure SSH on Ethernet Interfaces (cont)**

```
Ethernet Interfaces - SSH Manager:

SSH Listener Statuses:
ALL - SSH enabled on all the Interfaces
Yes - SSH enabled on specific Interface
No - SSH disabled on specific Interface

Interface | SSH Listener Status | IP Address | Host Name
-----|-----|-----|-----
eth0      | YES                  | 10.7.14.143 | EMS-Linux143
eth1      | NO                   | 10.7.14.215 | ems-215

1) Add SSH to All Ethernet Interfaces
2) Add SSH to Ethernet Interface
3) Remove SSH from Ethernet Interface
4) Back to SSH Configuration Manager Menu
: █
```



### 10.3.5.3.1 Add SSH to All Ethernet Interfaces

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

➤ **To add SSH to All Ethernet Interfaces:**

1. Choose option **ALL**, and then press **Enter**.

The SSH daemon restarts automatically to update this configuration action.

**Figure 10-63: Ethernet Interfaces – SSH Manager**

```

Ethernet Interfaces - SSH Manager:

      SSH Listener Statuses:
      ALL - SSH enabled on all the Interfaces
      Yes - SSH enabled on specific Interface
      No  - SSH disabled on specific Interface

Interface | SSH Listener Status | IP Address | Host Name
-----|-----|-----|-----
eth0     | YES                 | 10.7.14.143 | EMS-Linux143
eth1     | NO                  | 10.7.14.215 | ems-215

1) Add SSH to All Ethernet Interfaces
2) Add SSH to Ethernet Interface
3) Remove SSH from Ethernet Interface
4) Back to SSH Configuration Manager Menu
: 1
Stopping sshd: [ OK ]
Starting sshd: [ OK ]

```

A successful configuration is indicated when the column 'SSH Listener Status' displays ALL for all interfaces.

**Figure 10-64: SSH Listener Status - ALL**

```

Interface | SSH Listener Status | IP Address | Host Name
-----|-----|-----|-----
eth0     | ALL                 | 10.7.14.143 | EMS-Linux143
eth1     | ALL                 | 10.7.14.215 | ems-215

```

### 10.3.5.3.2 Add SSH to Ethernet Interface

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

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

1. Choose option **Yes**, and then press **Enter**.  
After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.
2. Enter the appropriate interface number, and then press **Enter**.  
The SSH daemon restarts automatically to update this configuration action.

**Figure 10-65: Configurable Ethernet Interfaces**

```

Ethernet Interfaces that can be configured:

 1) eth1 | 10.7.14.215 | EMS-Linux215
 2) Cancel
 : █
    
```

A successful configuration is indicated in the column 'SSH Listener Status' where **YES** is displayed for the configured interface.

**Figure 10-66: SSH Listener Status - YES**

Interface	SSH Listener Status	IP Address	Host Name
eth0	YES	10.7.14.143	EMS-Linux143
eth1	<u>YES</u>	10.7.14.215	ems-215

### 10.3.5.3.3 Remove SSH from Ethernet Interface

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

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

1. Choose option **3**, and then press **Enter**.  
All the interfaces to which SSH access is currently enabled are displayed.
2. Enter the desired interface number, and then press **Enter**.  
The SSH daemon restarts automatically to update this configuration action.

**Figure 10-67: Removing Ethernet Interface**

```

Ethernet Interfaces that can be configured:

 1) eth0 | 10.7.14.143 | EMS-Linux143
 2) eth1 | 10.7.14.215 | ems-215
 3) Cancel
 : 2
array ip: 10.7.14.215
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
█
    
```

A successful configuration is indicated in the column 'SSH Listener Status' where **No** is displayed for the denied interface.

**Figure 10-68: SSH Listener Status - NO**

Interface	SSH Listener Status	IP Address	Host Name
eth0	YES	10.7.14.143	EMS-Linux143
eth1	<u>NO</u>	10.7.14.215	ems-215



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

**Figure 10-69: Configurable Ethernet Interfaces**

```
Ethernet Interfaces that can be configured:  
You can't remove SSH from last Interface  
Press Enter to continue  
█
```

### 10.3.5.4 Disable SSH Password Authentication

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

➤ **To disable SSH Password Authentication:**

1. Select option **4**, and then press **Enter**.

**Figure 10-70: Disable SSH Password Authentication**

```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Disable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: █
```

2. Type **y**, and then press **Enter**.

The SSH daemon restarts automatically to update this configuration action.

**Figure 10-71: Disable SSH Password Authentication - Confirm**

```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.

Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Disable SSH Password Authentication?(y/n) y
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
█
```



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

### 10.3.5.4.1 Re-enable SSH Password Authentication

Once you have disabled SSH username/password authentication, you can re-enable this feature using the same option in the SSH Configuration Manager (as described in Section 10.3.5.4 on page 136).

➤ **To re-enable SSH Password Authentication:**

1. Choose option **4**, and then press **Enter**.

**Figure 10-72: Enable SSH Password Authentication**

```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Enable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: 4
```

2. The 'Enable SSH Password Authentication' sub-menu is displayed.

**Figure 10-73: Enable SSH Password Authentication -Confirm**

```
Enable SSH Password Authentication:

Current SSH Password Authentication is DISABLED.

Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Enable SSH Password Authentication?(y/n) y
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
```

3. Type **y** to confirm this action.

The SSH daemon restarts automatically to update the configuration action.

### 10.3.5.5 Enable SSH IgnoreUserKnownHosts Parameter

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

➤ **To enable SSH IgnoreUserKnownHosts parameter:**

1. Type option **5**, and then press **Enter**.

**Figure 10-74: Enable SSH IgnoreUserKnownHosts Parameter**

```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Enable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: 4
```

The 'Enable SSH IgnoreUserKnownHosts parameter' sub-menu is displayed.

**Figure 10-75: SSH IgnoreUserKnownHosts Parameter - Confirm**

```
Enable SSH IgnoreUserKnownHosts parameter:
Current SSH IgnoreUserKnownHosts parameter value is NO.
Are you sure you want to Change SSH IgnoreUserKnownHosts value to YES?(y/n) y
```

2. Type **y**, and then press **Enter**.

**Figure 10-76: SSH IgnoreUserKnownHosts Parameter - YES**

```
Disable SSH IgnoreUserKnownHosts parameter:
Current SSH IgnoreUserKnownHosts parameter value is YES.
Are you sure you want to Change SSH IgnoreUserKnownHosts value to NO?(y/n) y
```

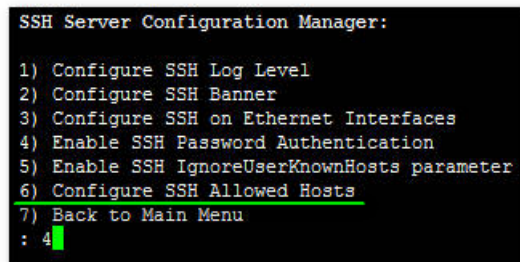
### 10.3.5.6 Configure SSH Allowed Hosts

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

➤ **To Configure SSH Allowed Hosts:**

1. Choose option **6**, and then press **Enter**.

**Figure 10-77: SSH Allowed Hosts**



```
SSH Server Configuration Manager:
1) Configure SSH Log Level
2) Configure SSH Banner
3) Configure SSH on Ethernet Interfaces
4) Enable SSH Password Authentication
5) Enable SSH IgnoreUserKnownHosts parameter
6) Configure SSH Allowed Hosts
7) Back to Main Menu
: 4
```

This section describes the following options:

- Allow ALL Hosts. See below.
- 10.3.5.6.2Deny ALL Hosts. See Section [10.3.5.6.2](#) on page [141](#).
- Add Host/Subnet to Allowed Hosts / Add IP Address. See Section [10.3.5.6.3](#) on page [142](#).
- Remove Host/Subnet from Allowed Hosts | Remove IP Address. See Section [10.3.5.6.4](#) on page [143](#).
- Add Host/Subnet to Allowed Hosts | Add Subnet. See Section [10.3.5.6.5](#) on page [144](#).
- Remove Host/Subnet from Allowed Hosts | Remove Subnet. See Section [10.3.5.6.6](#) on page [146](#).
- Add Host/Subnet to Allowed Hosts | Add Host Name. See Section [10.3.5.6.7](#) on page [147](#).
- Remove Host/Subnet from Allowed Hosts | Remove Host Name. See Section [10.3.5.6.8](#) on page [148](#).

### 10.3.5.6.1 Allow ALL Hosts

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

➤ **To allow ALL Hosts:**

1. Choose option **1**, and then press **Enter**.

**Figure 10-78: Allow ALL Hosts**

```
SSH Allow/Deny Host Manager:
SSH NOT Allowed for ALL Hosts.

1) Allow ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: 1
```

2. Type **y** to confirm your choice, and then press **Enter**.

**Figure 10-79: Allow ALL Hosts - Confirm**

```
Allow ALL Hosts:

Are you sure you want to Allow All Hosts?(y/n) y
```

The appropriate status is displayed:

**Figure 10-80: Allow ALL Hosts – Display Configuration**

```
SSH Allow/Deny Host Manager:
SSH Allowed for ALL Hosts.

1) Deny ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: 
```



### 10.3.5.6.2 Deny ALL Hosts

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

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

1. Choose option **2**, and then press **Enter**.

**Figure 10-81: Deny ALL Hosts**

```
SSH Allow/Deny Host Manager:

Current Allowed Hosts/Subnets:

IP Addresses:
10.7.2.31

1) Allow ALL Hosts
2) Deny ALL Hosts
3) Add Host/Subnet to Allowed Hosts
4) Remove Host/Subnet from Allowed Hosts
5) Back to SSH Configuration Manager Menu
: 2
```

The 'Deny ALL Hosts' sub-menu is displayed:

**Figure 10-82: Deny ALL Hosts - Confirm**

```
Deny ALL Hosts:

Are you sure you want to Deny All Hosts?(y/n) y
```

The appropriate status is displayed;

**Figure 10-83: Deny ALL Hosts – Display Configuration**

```
SSH Allow/Deny Host Manager:

SSH NOT Allowed for ALL Hosts.

1) Allow ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: 
```



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

### 10.3.5.6.3 Add Host/Subnet to Allowed Hosts / Add IP Address

This option enables you to allow or deny different SSH access methods to different remote hosts. Once you have provided the desired remote host IP, you can connect to the EMS server via SSH.

➤ **To add Host/Subnet to Allowed Hosts:**

1. Choose option **2**, and then press **Enter**.

**Figure 10-84: Add Host /Subnet to Allowed Hosts**

```
SSH Allow/Deny Host Manager:

SSH Allowed for ALL Hosts.

1) Deny ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: 2
```

The 'Add Host to Allowed List' sub-menu is displayed.

2. Choose option **1**, and then press **Enter**.

**Figure 10-85: Add Host to Allowed List**

```
Add Host to Allowed List:

1) Add IP Address (x.x.x.x)
2) Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
3) Add Host Name (without "/" or "," characters)
4) Back to SSH Configuration Manager Menu
: 1
```

3. Enter the desired IP address, and then press **Enter**.
4. Type **y** to confirm the entered address, and then press **Enter** again.

**Figure 10-86: Insert IP Address**

```
Insert IP Address: 10.7.2.31

IP Address: 10.7.2.31
Are you sure you want to Add this IP Address to SSH Allowed Hosts?(y/n)y
```

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

**Figure 10-87: Insert IP Address-Confirm**

```
Insert IP Address: 10.7.2.31

This IP Address already added.
You want to try again?(y/n)
```

When the allowed hosts IPs have been successfully added, the IP addresses of these hosts are displayed in the header of the 'SSH Allow/Deny Host Manager' sub-menu.

**Figure 10-88: SSH Allow/Deny Host Manager – Display Configuration**

```
SSH Allow/Deny Host Manager:

Current Allowed Hosts/Subnets:

IP Addresses:
10.7.2.31
10.7.2.23

1) Allow ALL Hosts
2) Deny ALL Hosts
3) Add Host/Subnet to Allowed Hosts
4) Remove Host/Subnet from Allowed Hosts
5) Back to SSH Configuration Manager Menu
: █
```

#### 10.3.5.6.4 Remove Host/Subnet from Allowed Hosts | Remove IP Address

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

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

1. Choose option **1**, and then press **Enter**.  
The 'Remove from Allowed List' sub-menu is displayed.

**Figure 10-89: Remove from Allowed List**

```
Remove Host from Allowed List:

1) Remove IP Address
2) Back to SSH Configuration Manager Menu
: █ 1
```

2. Choose the desired IP address to remove from the Allowed Hosts list, i.e. to deny access to the EMS server via SSH connection, and then press **Enter** again.

**Figure 10-90: Current IP Addresses Allowed List**

```
Current IP Addresses Allowed List:

1) 10.7.2.31
2) 10.7.2.23
3) Cancel
: █ 2
```

Note that the chosen IP address has been removed from the Allowed Hosts list.

Figure 10-91: IP Address Allowed List – Removed IP Address

```
SSH Allow/Deny Host Manager:

Current Allowed Hosts/Subnets:

IP Addresses:
10.7.2.31

1) Allow ALL Hosts
2) Deny ALL Hosts
3) Add Host/Subnet to Allowed Hosts
4) Remove Host/Subnet from Allowed Hosts
5) Back to SSH Configuration Manager Menu
: █
```



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

Figure 10-92: SSH NOT Allowed for ALL Hosts - Display Configuration

```
SSH Allow/Deny Host Manager:

SSH NOT Allowed for ALL Hosts.

1) Allow ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: █
```

### 10.3.5.6.5 Add Host/Subnet to Allowed Hosts | Add Subnet

This option enables you to define an Allowed Host as a Subnet/Netmask template.

➤ **To define an Allowed Host as a Subnet/Netmask:**

1. Choose option **2**, and then press **Enter**.

Figure 10-93: Add Subnet

```
Add Host to Allowed List:

1) Add IP Address (x.x.x.x)
2) Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
3) Add Host Name (without "/" or "," characters)
4) Back to SSH Configuration Manager Menu
: 1 █
```

2. Enter the appropriate subnet netmask separated by a slash (as shown below), and then press **Enter**.
3. Type **y** to confirm your input, and then press **Enter**.

**Figure 10-94: Add Subnet-Confirm**

```
Insert Subnet (n.n.n.n/m.m.m.m - network/netmask): 10.7.0.0/255.255.0.0
Subnet: 10.7.0.0/255.255.0.0
Are you sure you want to Add this Sunet to SSH Allowed Hosts?(y/n)y
```

When the allowed subnets have been successfully added, they are displayed in the header of the 'SSH Allow/Deny Host Manager' sub-menu.

**Figure 10-95: SSH Allow/Deny Host Manager - Display Configuration**

```
SSH Allow/Deny Host Manager:
Current Allowed Hosts/Subnets:
Subnet Masks:
 10.7.0.0/255.255.0.0

1) Allow ALL Hosts
2) Deny ALL Hosts
3) Add Host/Subnet to Allowed Hosts
4) Remove Host/Subnet from Allowed Hosts
5) Back to SSH Configuration Manager Menu
:
```

### 10.3.5.6.6 Remove Host/Subnet from Allowed Hosts | Remove Subnet

This option enables you to remove a subnet mask from the Allowed Hosts list.

➤ **To remove a host/subnet mask from the Allowed Host list:**

1. Choose option **1**, and then press **Enter**.

**Figure 10-96: Remove Host/Subnet Mask**

```
Remove Host from Allowed List:
1) Remove Subnet
2) Back to SSH Configuration Manager Menu
: 1
```

The desired subnet address is removed from the Allowed Hosts list, i.e. each host belonging to this subnet is denied access to the EMS server via an SSH connection.

2. Type **y** to confirm the action.

**Figure 10-97: Remove Host/Subnet Mask - Confirm**

```
Current Subnets Allowed List:
1) 10.7.0.0/255.255.0.0
2) Cancel
: 1
```



**Note:** When you remove the only existing Subnet in the Allowed Hosts list, there are no remote hosts with access to connect to the EMS server using SSH. When this action is performed, you are disconnected from the EMS server and may not be able to reconnect via SSH. Therefore, prior to disabling SSH access, ensure that alternative connection methods have been provisioned. For example, serial management connection or KVM connection.

**Figure 10-98: Remove Host/Subnet Mask - Display Configuration**

```
SSH Allow/Deny Host Manager:
SSH NOT Allowed for ALL Hosts.
1) Allow ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: 1
```

### 10.3.5.6.7 Add Host/Subnet to Allowed Hosts | Add Host Name

This option enables you to append the name of a host to the allowed Hosts list.



**Note:** Before using this option, verify your remote host name appears in the DNS server database and your EMS server has an access to the DNS server.

#### ➤ To add the host/subnet to the allowed hosts list:

1. Choose option **3**, and then press **Enter**.

**Figure 10-99: Add Host to Allowed List**

```
Add Host to Allowed List:
1) Add IP Address (x.x.x.x)
2) Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
3) Add Host Name (without "/" or "," characters)
4) Back to SSH Configuration Manager Menu
: 1
```

2. Provide the host name of the desired network interface defined in “/etc/hosts” file, and then press **Enter**.
3. Type **y** to confirm your input, and then press **Enter**.

**Figure 10-100: Add Host to Allowed List - Confirm**

```
Insert Host Name (without "/" or "," characters): EMS-Linux144
Host Name: EMS-Linux144
Are you sure you want to Add this Host Name to SSH Allowed Hosts?(y/n)y
```

When the allowed host name has been successfully added, this name is displayed in the 'SSH Allow/Deny Host Manager' sub-menu.

**Figure 10-101: SSH Allow/Deny Host Manager - Display Configuration**

```
SSH Allow/Deny Host Manager:
Current Allowed Hosts/Subnets:
Host Names:
EMS-Linux144
1) Allow ALL Hosts
2) Deny ALL Hosts
3) Add Host/Subnet to Allowed Hosts
4) Remove Host/Subnet from Allowed Hosts
5) Back to SSH Configuration Manager Menu
: 
```

### 10.3.5.6.8 Remove Host/Subnet from Allowed Hosts | Remove Host Name

This option enables you to remove the appended Host Name from the Allowed Hosts list.

➤ **To remove the Host/Subnet name from the Hosts list:**

1. Choose option **1**, and then press **Enter**.

**Figure 10-102: Remove Host/Subnet from Allowed Hosts**

```
Remove Host from Allowed List:
1) Remove Host Name
2) Back to SSH Configuration Manager Menu
: █
```

The 'Remove Host from Allowed List' sub-menu is displayed.

2. Choose the desired host name to remove from the Allowed Hosts list, and then press **Enter** to confirm the action.

**Figure 10-103: Remove Host/Subnet from Allowed Hosts - Hosts List**

```
Current Host Names Allowed List:
1) EMS-Linux144
2) Cancel
: 1 █
```



**Note:** When you remove the only existing Host Name in the Allowed Hosts list, there are no remote hosts with access to connect to the EMS server using SSH. When this action is performed, you are disconnected from the EMS server and may not be able to reconnect via SSH. Therefore, prior to disabling SSH access, ensure that alternative connection methods have been provisioned. For example, serial management connection or KVM connection.

**Figure 10-104: Remove Host/Subnet from Allowed Hosts - Display Configuration**

```
SSH Allow/Deny Host Manager:
SSH NOT Allowed for ALL Hosts.
1) Allow ALL Hosts
2) Add Host/Subnet to Allowed Hosts
3) Back to SSH Configuration Manager Menu
: █
```



### 10.3.6 Changing DBA Password

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

➤ **To change the DBA Password:**

1. In the EMS Server Manager root menu, choose option **Change DB Password**, and then press **Enter**.

**Figure 10-105: EMS Server Manager – Change DBA Password**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
```

The 'Changing the DB Password' sub-menu is displayed.

**Figure 10-106: Changing the DB Password Sub-menu**

```
-----
*****
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 10-107: Changing the DB Password – Confirmation Display**

```

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

```

### 10.3.7 OS Passwords Settings

This section describes how to change the OS password settings.

➤ **To change OS passwords:**

1. In the EMS Server Manager root menu, choose the **OS Passwords Settings** option, and then press **Enter**.

**Figure 10-108: EMS Server Manager – OS Password Settings**

```

Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options

```

Perform one of the following procedures:

- General Password Settings. See Section [10.3.7.1](#) below
- Operating System User Security Extensions. See Section [10.3.7.2](#) on page [153](#).

### 10.3.7.1 General Password Settings

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

➤ **To modify general password settings:**

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

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

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

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

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

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

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

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

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

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

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

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

**Figure 10-109: Changing OS 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 10-110: 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 password less for SSH Login. When you provide a new password for **NBIF** user, a normal login is allowed. When changing passwords, retain these passwords for future access.

### 10.3.7.2 Operating System Users Security Extensions

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

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

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure in [Figure 10-111](#)).

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

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

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

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

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

3. Enter the Username upon which you wish to place limitations, and then press **Enter**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Figure 10-111: OS Passwords Settings with Security Extensions**

```

OS Passwords Settings

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

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

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

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

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

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

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

**Figure 10-112: Maximum Active SSH Sessions**

```

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

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



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

### 10.3.8 Add EMS User

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

➤ **To add an EMS user:**

1. Choose **Add EMS User** option, and then press **Enter**.

**Figure 10-113: EMS Server Manager – Add EMS User**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
```

The 'Add EMS User' sub-menu is displayed.



**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.

### 10.3.9 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 Manager root menu, choose **Start / Stop File Integrity Checker** option, and then press **Enter**.

**Figure 10-114: EMS Server Manager – Start/Stop File Integrity Checker**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
```

### 10.3.10 Network Options

The Linux Operating System security can be improved by slightly modifying the behavior of its TCP/IP implementation.

➤ **To configure Network Options:**

1. In the EMS Server Manager root menu, choose **Network Options** option.

**Figure 10-115: EMS Server Manager – Network Options**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
```



The 'Network Options' sub-menu is displayed.

**Figure 10-116: Network Options Sub-menu**

```
Network Options

Log packets with impossible addresses to kernel log: Disabled
Ignore all ICMP ECHO requests: Disabled
Ignore all broadcast and multicast ICMP ECHO and TIMESTAMP requests: Disabled
Send ICMP redirect messages: Disabled
Accept ICMP redirect messages: Disabled

1) Enable log packets with impossible addresses to kernel log
2) Enable ignore all ICMP ECHO requests
3) Enable ignore all ICMP ECHO and TIMESTAMP requests to broadcast and multicast addresses
4) Enable send ICMP redirect messages
5) Enable accept ICMP redirect messages
6) Back to Main Menu
: █
```

2. Choose option **1**, and then press **Enter**.

This parameter is enabled (the 'Log packets with impossible addresses to kernel log setting is displayed as 'Enabled').

- **Log Martians**

Log and drop 'Martian' packets. A 'Martian' packet is a packet where the host does not have a route back to the source IP address. These days most hosts have a default route, implying that such Martian packets do not exist; however for additional assurance, it's recommended to enable this parameter.

3. Choose option **2**, press **Enter**, choose option **3**, and then press **Enter**. These settings are enabled (the 'Ignore all ICMP ECHO requests' and 'Ignore all broadcast and multicast ICMP ECHO and TIMESTAMP requests' parameters are displayed as 'Enabled').

- **Ignore ICMP and Ignore Broadcasts**

'Ignore ICMP' and 'Ignore Broadcast' options disables ICMP broadcast echo activity. This prevents the EMS server undergoing a Smurf attack.

### 10.3.11 Start/Stop Software Integrity Checker (AIDE) and Pre-linking

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

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

➤ **To start AIDE and disable pre-linking:**

1. In the EMS Server Manager root menu, choose **Start/Stop Software Integrity Checker (AIDE) and Pre-linking** option.

**Figure 10-117: Software Integrity Checker (AIDE) and Pre-linking**

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

Software integrity checker (AIDE) is disabled and Prelinking is enabled.
Enable integrity checker, and disable prelinking? (y/n)y
```

2. Type **y** to enable AIDE and disable pre-linking.

### 10.3.12 Enable/Disable USB Storage

If USB storage devices are not being used, this option prevents the loading of the USB-storage kernel module, for security reasons.

➤ **To disable USB storage:**

1. In the EMS Server Manager root menu, choose **Enable/Disable USB Storage** option.

**Figure 10-118: Enable/Disable USB**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
17 ) Start/Stop Software Integrity Checker (AIDE) and Prelinking
18 ) Enable/Disable USB Storage
19 ) Auditd Options
```

2. Type **y** to disable USB Storage.

**Figure 10-119: USB Storage**

```
USB Storage:

USB Storage is enabled.

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

### 10.3.13 Auditd Options

The audit service is provided for system auditing. This service audits SELinux AVC denials and certain types of security-relevant events, such as system logins, account modifications, Use of Print Command, Startup and Shutdown events and authentication events performed by programs such as 'sudo'. By default, this service is enabled and configured to a basic security level.

This option enables you to enhance the security level of the audit service, according to STIG recommendations.

➤ **To change auditd settings according to STIG recommendations:**

1. In the EMS Server Manager root menu, choose **Auditd Options**:

**Figure 10-120: Auditd Options**

```
Security:
11 ) SSH Configuration
12 ) Change DBA Password (EMS Server will be shut down)
13 ) OS Passwords Settings
14 ) Add EMS User
15 ) Start/Stop File Integrity Checker
16 ) Network Options
17 ) Start/Stop Software Integrity Checker (AIDE) and Prelinking
18 ) Enable/Disable USB Storage
19 ) Auditd Options
```

2. Type **y** to change auditd settings according to STIG recommendations:

**Figure 10-121: Auditd Options Prompt**

```
Auditd Options:

Not using STIG recommendations for auditd

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

## 10.4 Maintenance

This section describes the maintenance procedures provided by the EMS Server Manager. The following procedures are described in this section:

- Configure NTP. See Section [10.4.1](#) on page [162](#).
- Change System Timezone. See Section [10.4.2](#) on page [163](#).
- Change System Time and Date. See Section [10.4.3](#) on page [165](#).
- Start/Stop the EMS Server. See Section [10.4.4](#) on page [166](#).
- Web Server Configuration. See Section [10.4.5](#) on page [166](#).
- Backup the EMS Server. See Section [10.4.6](#) on page [169](#).
- See Section Schedule Backup for the EMS Server. See Section [10.4.7](#) on page [171](#).
- Restore the EMS Server. See Section [10.4.8](#) on page [176](#).
- Reboot the EMS Server. See Section [10.4.9](#) on page [176](#).
- HA (High Availability) Configuration. See Section [10.4.10](#) on page [179](#).
- Syslog Configuration. See Section [10.4.11](#) on page [199](#).
- Board Syslog Logging Configuration. See Section [10.4.12](#) on page [201](#).
- TP Debug Recording Configuration. See Section [10.4.13](#) on page [202](#).

## 10.4.1 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:

1. In the EMS Server Management root menu, choose **Configure NTP** option, and then press **Enter**.

**Figure 10-122: EMS Server Manager - Configure NTP**

```

Maintenance:
17 ) Configure NTP
18 ) Change System Timezone
19 ) Change System Time & Date
20 ) Start/Stop EMS Server
21 ) Web Server Configuration
22 ) Backup the EMS Server
23 ) Schedule Backup for the EMS Server
24 ) Restore the EMS Server
25 ) Reboot the EMS Server
26 ) HA Configuration
27 ) Syslog Configuration
  
```

The Configure 'NTP' menu is displayed.

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

➤ **To start NTP services:**

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

**Figure 10-123: 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 starts and configuration data is displayed.

## 10.4.2 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 **Change System Time Zone** option, and then press **Enter**.

**Figure 10-124: EMS Server Manager - Change System Timezone**

```
Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
```

2. Enter the required time zone.



**Note:** On the Solaris platform, when the operation has completed, the EMS automatically reboots for the changes to take effect.

**Figure 10-125: Change System Time Zone – Enter New Time Zone**

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



### 10.4.3 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 **Change System Time and Date** option, and then press **Enter**.

**Figure 10-126: EMS Server Manger - Change System Time & Date**

```
Maintenance:
17 ) Configure NTP
18 ) Change System Timezone
19 ) Change System Time & Date
20 ) Start/Stop EMS Server
21 ) Web Server Configuration
22 ) Backup the EMS Server
23 ) Schedule Backup for the EMS Server
24 ) Restore the EMS Server
25 ) Reboot the EMS Server
26 ) HA Configuration
27 ) Syslog Configuration
```

The date and time is displayed.

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 10-127: Change System Time and Date Prompt**

```
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
█
```

## 10.4.4 Start /Stop the EMS Server

- In the EMS Server Management menu, choose **Start / Stop the EMS Server** option, and then press **Enter**.

**Figure 10-128: EMS Server Manager – Start/ Stop EMS Server**

```

Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
  
```

## 10.4.5 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 root menu, choose **Web Server Configuration** option, and then press **Enter**.

**Figure 10-129: EMS Server Manager – Web Server Configuration**

```

Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
  
```

The Web server configuration sub-menu is displayed.

Figure 10-130: Web Server Configuration Sub-menu

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

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

➤ **To start/stop the Apache server:**

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

➤ **To start/stop the Tomcat server:**

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

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

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

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

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

➤ **To disable JAWS:**

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

### 10.4.5.1 Changing the JAWS Login Interface

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

➤ **To change the JAWS login interface:**

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

**Figure 10-131: JAWS IP Configuration**

```
JAWS IP Configuration
IP Address[10.7.14.145]:10.77.10.216
Are you sure that you want to continue? (y/n/q) y
```

## 10.4.6 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 to safeguard against malfunction.

The backup generates the following files:

- **EMSexport.dmp** contains server database information
- **emsServerBackup.tar** contains all version directories. =

All the EMS server files and the database are backed up to one of these files, which are located under the folder '/ACEMS/NBIF/emsBackup'.

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

The created backup file can only be restored on 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:**

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

For additional EMS backup procedures, see Section B on page 221.

➤ **To backup the EMS server:**

- In the EMS Server Management root menu, choose **Backup the EMS Server** option, and then press **Enter**.

**Figure 10-132: EMS Server Manager – Backup the EMS Server**

```
Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
```

Backup data is displayed; a confirmation message is displayed at the end of the backup process.

## 10.4.7 Schedule Backup for the EMS Server

This option enables you to schedule backup to run automatically at predefined time intervals. This option enables you to configure the EMS backup system. The following parameters may be configured:

- Backup Schedule: days of week and hours that you wish to perform EMS server backup.
- Number of saved backups may be configured in range from 1 to 3 backup file sets.

This section describes the following options:

- Schedule New Backup. See below.
- View Scheduled Backups. See Section 10.4.7.2 on page 173.
- Remove Scheduled Backup. See Section 10.4.7.3 on page 174.
- Set Number of Scheduled Backups to Save. See Section 10.4.7.4 on page 175.

### ➤ To schedule backup of the EMS Server:

- In the EMS Server Management menu, choose **Schedule Backup for the EMS Server** option, and then press **Enter**.

Figure 10-133: EMS Server Manager – Scheduled Backup for the EMS Server

```
Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
```

### 10.4.7.1 Schedule New Backup

You can schedule the backup according to the desired weekday and hour. For example, if you wish to schedule the backup session at 3 AM on each Sunday, see the example in the screen below.

➤ **To schedule a new backup configuration:**

**Figure 10-134: Schedule New Backup**

```

Schedule Backup Menu

1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: 1

The backup files can be used later only for the same EMS version.
Are you sure that you want to continue? (y/n)y
---- Scheduling backup ---
The data will be exported once a day/week, to a file named EMSexport_<yyymmdd>.dmp
you should backup this file to another machine.
choose a day of the week to perform weekly backup (0-6) or 7 for daily
or type 8 to exit back to previous menu
0-Sunday, 1-Monday, 2-Tuesday, 3-Wednesday, 4-Thursday, 5-Friday, 6-Saturday, 7-Daily:
0 ←
choose an hour to perform backup (0-23)
3 ←
----finished----

Press Enter to continue.

```

1. Choose option **1**, and then press **Enter**.
2. Choose the day of the week for the EMS to perform backup.
4. Choose an hour to perform backup (0-23), and then press **Enter**.  
A confirmation message is displayed.



### 10.4.7.2 View Scheduled Backups

To verify your session is successfully set, use this option to display already configured backup sessions.

➤ To view scheduled backup configuration:

Figure 10-135: View Scheduled Backups

```
Schedule Backup Menu
1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: █
```

- Choose option **3**, and then press **Enter**.  
The scheduled backup time is displayed.

Figure 10-136: Schedule Backup Time

```
Schedule Backup Menu
1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: 3

---- Scheduled Backups List ---
1. on Sunday at hour:3

Press Enter to continue.
█
```

### 10.4.7.3 Remove Scheduled Backup

Use this option to remove previously configured backup sessions.

➤ **To remove scheduled backup:**

**Figure 10-137: Remove Scheduled Backup**

```

Schedule Backup Menu
1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: █
    
```

1. Choose option **2**, and then press **Enter**.

The list of scheduled backups is displayed:

**Figure 10-138: List of Scheduled Backups**

```

---- Please choose a scheduled backup to remove from list ----
1. on Wednesday at hour:16
2. on Wednesday at hour:17
3. on Wednesday at hour:18
4. on Wednesday at hour:19
5. on Wednesday at hour:20
6. Quit
3
----finished----
Press Enter to continue.
█
    
```

2. Enter the number corresponding to the scheduled session you wish to remove from the list, and then press **Enter**.
3. To verify that the sessions have been properly removed, use the option described in Section [10.4.7.2](#) on page [173](#).

**Figure 10-139: Scheduled Backups List**

```

---- Scheduled Backups List ----
1. on Wednesday at hour:16
2. on Wednesday at hour:17
3. on Wednesday at hour:19
4. on Wednesday at hour:20
Press Enter to continue.
█
    
```

### 10.4.7.4 Set Number of Scheduled Backups to Save

This option determines how many backup file sets are saved. This option may be configured in range from '1' to '3'. The default number of saved backup file sets is '1'.

➤ To set the number of scheduled backups to save:

Figure 10-140: Set Number of Scheduled Backups to Save

```
Schedule Backup Menu
1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: █
```

- Choose option 4, and then press **Enter**.

Figure 10-141: Number of Backups to Store

```
Schedule Backup Menu
1) Schedule New Backup
2) Remove Scheduled Backup
3) View Scheduled Backups
4) Set Number of Scheduled Backups to Save
5) Back to Main Menu
: 4

Number of backups to store (1-3): [3]: 3
```

For example, if this parameter was set to '3', after three backup sessions, you see three file sets saved in the EMS backup directory.

Figure 10-142: EmsBackup File

```
[root@EMS-Linux142 ~]# ls -l /ACEMS/NBIF/emsBackup/
total 515024
drwxrwx--- 3 emsadmin dba      4096 Jul 12 03:00 DBEMS
-rw-r----- 1 emsadmin nbif    425984 Jul 13 19:00 EMSEXport_1107131900.dmp
-rw-r----- 1 emsadmin nbif    425984 Jul 13 20:00 EMSEXport_1107132000.dmp
-rw-r----- 1 emsadmin nbif    425984 Jul 14 11:46 EMSEXport_1107141146.dmp
-rw-r----- 1 emsadmin nbif 175185920 Jul 13 19:00 emsServerBackup_1107131900.tar
-rw-r----- 1 emsadmin nbif 175185920 Jul 13 20:00 emsServerBackup_1107132000.tar
-rw-r----- 1 emsadmin nbif 175185920 Jul 14 11:47 emsServerBackup_1107141146.tar
drwxrwx--- 2 oracle  dba      4096 Jul 14 03:02 RmanBackup
[root@EMS-Linux142 ~]# █
```



**Note:** When the EMS server works for long periods of time, its database contains a large volume of information. Different types of configuration or firmware files are collected on the disk space, all of which is saved to backup files. Therefore, when you configure how many file sets are saved in the backup directory, it's important to verify your current free disk space.

## 10.4.8 Restore the EMS Server

This feature enables you to restore the EMS server from one of the saved backup files (See Section 10.4.7 on page 171).



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

- The EMS server configuration should be performed prior to the restore procedure, for example Security and Networking.
- The EMS server security level should be the same level as the pre-restored server (Hardening level).
- 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. Ensure that the saved backup files **EMSexport.dmp** and **emsServerBackup.tar** are located in the directory **/ACEMS/NBIF/emsBackup**.
2. In the EMS Server Management menu, choose **Restore the EMS Server** option, and then press **Enter**.

**Figure 10-143: EMS Server Manager – Restore the EMS Server**

```
Maintenance:
17 ) Configure NTP
18 ) Change System Timezone
19 ) Change System Time & Date
20 ) Start/Stop EMS Server
21 ) Web Server Configuration
22 ) Backup the EMS Server
23 ) Schedule Backup for the EMS Server
24 ) Restore the EMS Server
25 ) Reboot the EMS Server
26 ) HA Configuration
27 ) Syslog Configuration
```

The Saved Backups sub-menu is displayed.

**Figure 10-144: Saved Backups Sub-menu**

```
1. backup file from: 15:00 23.07.11
2. backup file from: 15:00 24.07.11
3. backup file from: 15:00 25.07.11
4. Quit
2
EMS Server is down.
Press Enter to continue.

--- EMS recovery---

to import data, please copy your backup files named EMSexport_1107241500.dmp
and emsServerBackup_1107241500.tar to the directory NBIF/emsBackup, and press <ENTER>.
```

3. Select one of the saved backup files that you wish to recover, for example 2, and then press **Enter**.
4. The restore process proceeds automatically. Upon completion, a message is displayed; press **Enter**.

**Figure 10-145: Restore Process-Confirmation**

```

. . importing table "TRAP_FORWARD_CONFIG_NODES" 0 rows imported
. . importing table "TRAP_FWD_EMAIL2SMS_DEST_TYPE" 0 rows imported
. . importing table "TRAP_FWD_EMAIL_DEST_TYPE" 0 rows imported
. . importing table "TRAP_FWD_SNMP_DEST_TYPE" 0 rows imported
. . importing table "TRAP_FWD_SYSLOG_DEST_TYPE" 0 rows imported
About to enable constraints...
Import terminated successfully without warnings.
Revoking access

SQL*Plus: Release 11.1.0.7.0 - Production on Tue Jul 26 08:56:11 2011

Copyright (c) 1982, 2008, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production

Revoke succeeded.

Disconnected from Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production
-----finished-----
Press Enter to continue.

```

5. After completing the restore action, choose option 'Start/Stop EMS Server', and start the EMS server manually.



**Note:** When the restore process starts, the EMS server is down.

**Figure 10-146: EMS Server Manual Restart**

```

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

```

## 10.4.9 Reboot the EMS Server

This section describes how to reboot the EMS server.

➤ **To reboot the EMS Server:**

- In the EMS Server Management menu, choose **Reboot the EMS Server** option, and then press **Enter**.

**Figure 10-147: EMS Server Manager – Reboot the EMS Server**

```

Maintenance:
 17 ) Configure NTP
 18 ) Change System Timezone
 19 ) Change System Time & Date
 20 ) Start/Stop EMS Server
 21 ) Web Server Configuration
 22 ) Backup the EMS Server
 23 ) Schedule Backup for the EMS Server
 24 ) Restore the EMS Server
 25 ) Reboot the EMS Server
 26 ) HA Configuration
 27 ) Syslog Configuration
  
```

## 10.4.10 HA (High Availability) Configuration

This section describes the EMS HA Configuration options.

### 10.4.10.1 HA Overview

**EMS servers High Availability** is supported for EMS server applications running on the Linux platform.



**Note:** This feature is not supported on the Solaris platform.

Two EMS server machines are required to support High Availability: one machine serving as the Primary machine and the other serving as the Secondary machine. When the EMS application is active and running, all data stored in the EMS server machine and database is replicated from the Primary machine to the Secondary machine. Upon Primary machine failure recognition (either on the EMS application or on the Network), activity is automatically transferred from the Primary server machine to the Secondary server machine.



Two models of High Availability are supported:

- Both EMS servers are located in the same subnet. There is a single EMS server IP address - Global (Virtual) IP address defined for all the Network Components (EMS clients and Managed Gateways). Each of the EMS server machines has an internal Private IP address and the active EMS server machine performs binding to the Global (Virtual) IP address. This setup currently does not support working with gateways behind a NAT.
- Each one of the EMS servers is located in a different network subnet and has its own IP address. During the EMS client login dialog, the user should provision both IP addresses (Geo HA), and the EMS client application will constantly search for the currently active EMS server machine. All the managed gateways relevant applications (such as Trap Sending, NTP Server, and OCSP Server) should be aware of two possible EMS server machine addresses.



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

The HA Configuration menu option enables you to configure EMS server machines high availability, perform HA-related actions and review the HA status for both servers. Prior to configuring HA, both machines should be installed with an identical EMS server version and an identical operating system and network configuration.



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



### 10.4.10.2 EMS HA Pre-requisites

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

- Both servers have identical hardware. See EMS Server and Client Requirements section for supported machines (see Section 3 on page 25)
- An identical Linux OS is installed on both servers.
- An identical EMS version is installed on both servers.
- An identical interface configuration and the same subnets are connected to each server (N/A for Geo HA).
- An identical redundancy configuration on identical interfaces.
- The EMS application is down (use the EMS Server Manager to shutdown the EMS application).
- SSH communication between the Secondary and the Primary servers exists.
- Network Bandwidth requirements between two EMS servers are as follows:
  - Initial Synchronization process: at least 80 Mbps  
During the initial sync process, the entire /data partition is synchronized between the active and redundant servers. This partition size is 63GB on HP DL360 G6 servers and 150GB on HP DL360p G8 servers. A network speed of at least 80 Mbps is required to complete the initial sync process in up to 2 hours on G6 servers and 4 hours on G8 servers.  
Assuming a slower network, the process will take longer. For example, on G6 servers:
    - ◆ 20 Mbps -> 7 hours
    - ◆ 10 Mbps -> 14 hours
  - Ongoing server Synchronization: 10 Mbps.
  - Ping between two servers: the ping time between each EMS server machine should not exceed 200 msec.
- During the HA configuration process, entire /data partition is duplicated from the primary server to the secondary server. If any of the servers contain previous backup files, these files are deleted on the secondary server. These files should be backed up on an external storage machine prior to the HA configuration.

### 10.4.10.3 EMS HA Data Synchronization

The data synchronization is performed using a distributed replicated block device for the Linux operating system. This process allows a real-time mirror of the local block devices on a remote machine.

The replicated EMS data includes the following:

- EMS Database
- EMS NBIF files including the following:
  - Backup files
  - Alarms files
  - Topology files
  - Performance files
  - MG backup files
- EMS Software files (EMS Software Manager files)
  - MG configuration files, for upgrade and management
  - MG Auxiliary files

The initial synchronization time between two EMS server machines is estimated at 1.5-4 hours, depending on network speed/quality and servers' disk size.

### 10.4.10.4 EMS HA Configuration

This section describes the EMS HA Installation.

➤ **To configure the primary server:**

1. In the EMS Server Manager root menu, choose **HA Configuration**, and then press **Enter**.

**Figure 10-148: EMS Server Manager - HA Configuration**

```
Maintenance:
 20 ) Configure NTP
 21 ) Change System Timezone
 22 ) Change System Time & Date
 23 ) Start/Stop EMS Server
 24 ) Web Server Configuration
 25 ) Backup the EMS Server
 26 ) Schedule Backup for the EMS Server
 27 ) Restore the EMS Server
 28 ) Reboot the EMS Server
 29 ) HA Configuration
 30 ) Syslog Configuration
 31 ) Board syslog logging Configuration
 32 ) TP Debug Recording Configuration
```

The High Availability sub-menu is displayed.

**Figure 10-149: High Availability sub-menu**

```
High Availability Menu
 1 ) Configure Server As Primary
 2 ) Configure Server As Secondary
 3 ) HA Status
 4 ) Back to Main Menu
Choose: █
```

The following options are described in this section:

- Primary Server Installation. See Sections 10.4.10.4.1 on page 184. and 10.4.10.4.2 on page 186.
- Secondary Server Installation. See Section 10.4.10.4.3 on page 189.
- HA Status. See Section 10.4.10.7.2 on page 195.

#### 10.4.10.4.1 Primary HA Server Installation in Global IP Model

This section describes how to install the HA application on the designated Primary server in the Global IP address model.

➤ **To install the HA primary server:**

1. Choose option **1** to run the Primary server HA installation.
2. After the HA packages are installed, you are prompted for the HA model.  
For the first model, both EMS servers are located in the same subnet.
3. Choose option **1**.

**Figure 10-150: Primary HA Server Menu**

```
High Availability Menu
 1 ) Configure Global IP HA
 2 ) Configure Geo-Redundancy HA
 3 ) Back to Main Menu
Choose: 1
```

4. You are now prompted for the following network parameters:
  - 'Global IP' for each configured interface (physical or logical IF).
  - Secondary server's Host name and IP address.
  - Ping Nodes (for more information, see Section 'Ping Nodes' below).

**Figure 10-151: Primary HA Server Sub-menu**

```
Start Heartbeat Configuration
Primary Server IP: 10.7.14.141
Primary Server Host: EMS-Linux141
Global IP for eth0[-1]: 10.7.14.218
Secondary Server IP [-1]: 10.7.14.142
Secondary Server Host [-1]: EMS-Linux142
Ping IP [-1]: 10.7.0.1
Do you want to add another ping ip ? (y/n)
```

If you have several interfaces configured, you can add another "ping node". The current configuration is displayed for confirmation.

**Figure 10-152: HA Configuration Display**

```
HA Configuration:
Global IP(eth0): 10.7.14.218
Primary Server IP: 10.7.14.141
Primary Server Host: EMS-Linux141
Secondary Server IP: 10.7.14.142
Secondary Server Host: EMS-Linux142
Ping IP: 10.7.0.1
Are you sure that you want to continue ? (y/n/q)
```

- Type **y** to continue the installation process
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- “/data: device is busy” – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing.** In the case where the /data partition isn’t busy, the above message is not displayed.
- When prompted, press **Enter** to continue.
- When prompted “To abort waiting type ‘yes’ [1]:” – you can wait or press ‘yes’ to continue.

When the installation process for the Primary server has completed, the following message is displayed:

**Figure 10-153: HA Server Configured as Primary Server - Confirmation**

```
Server Configured As Primary
***** HA configuration finished *****
```



**Note:** After the installation process has completed, it takes several minutes until the HA status changes to “Online” and the EMS server status changes to ‘EMS server is running’.

#### 10.4.10.4.2 Primary HA Server Installation in Geo HA model

This section describes how to install the HA application on the designated Primary server in the Geo HA model.

➤ **To install the HA primary server:**

1. Choose option **1** to run the Primary server HA installation.
2. After the HA packages are installed, you are prompted for the HA model.  
For the Geo HA model, EMS servers are located in different subnets.
3. Choose option **2**.

**Figure 10-154: Primary HA Server Menu**

```
High Availability Menu
 1 ) Configure Global IP HA
 2 ) Configure Geo-Redundancy HA
 3 ) Back to Main Menu
Choose: 2
```

4. You are now prompted for the following network parameters:
  - 'Global IP' for each configured interface (physical or logical IF).
  - Secondary server's Host name and IP address.
  - Ping Nodes (for more information, see Section 'Ping Nodes' below).

**Figure 10-155: Primary HA Server Sub-menu**

```
Start Heartbeat Configuration
Primary Server IP: 10.3.180.2
Primary Server Host: EMS-Linux2
Secondary Server IP [-1]: 10.17.1.200
Secondary Server Host [-1]: vEMS-GeoHA-200
Ping IP [-1]: 10.3.180.80
Do you want to add another ping ip ? (y/n)
```

If you have several interfaces configured, you can add another "ping node". The current configuration is displayed for confirmation.

**Figure 10-156: HA Configuration Display**

```
HA Configuration:
Primary Server IP: 10.3.180.2
Primary Server Host: EMS-Linux2
Secondary Server IP: 10.17.1.200
Secondary Server Host: vEMS-GeoHA-200
Ping IP: 10.3.180.80
Are you sure that you want to continue ? (y/n/q)y
```

- Type **y** to continue the installation process.
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- “/data: device is busy” – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing.** In the event where the /data partition isn't busy, the above message is not displayed.
- When prompted, press **Enter** to continue.
- When prompted “To abort waiting type 'yes' [1]:” – you can wait or press 'yes' to continue.

When the installation process for the Primary server has completed, the following message is displayed:

**Figure 10-157: HA Server Configured as Primary Server - Confirmation**

```
Server Configured As Secondary
State change failed: (-12) Device is held open by someone
Command 'drbdsetup /dev/drbd0 secondary' terminated with exit code 11
command exited with code 11
***** HA configuration finished *****
```



**Note:** After the installation process has completed, it takes several minutes until the HA status changes to 'Online' and the EMS server status changes to 'EMS server is running'.

## Ping Nodes

The purpose of these nodes (IP address) is to ensure network connection along all EMS server configured interfaces. When an IP address is configured as “ping node”, this implies that the HA process sends ICMP packets (at a constant interval) to this address (through the appropriate Server Ethernet interface). If no response is returned from this ping node (during a constant period of time), the HA process determines that the specific network interface connection is down and acts accordingly (i.e. initiates a possible switchover). The ping node should be a reliable host in the network, such as router or any other machine which accurately reflects the network status.

It is possible to configure several “ping nodes”, where each ping node is considered to be a single point of failure, therefore if there is no connection to one of the ping nodes, a switchover is performed (unless the Secondary server cannot takeover due to the same or different network problems or during initial synchronization between the Primary and Secondary server).



**Note:** It's recommended to configure a separate ping node for each configured physical Ethernet interface (to the router connected to each of the subnets); however, if Ethernet Redundancy is configured between these two interfaces, then it's sufficient to configure a single ping node.



### 10.4.10.4.3 Secondary HA Server Installation

This section describes how to install the High Availability (HA) application on the designated Secondary server.

➤ **To install the secondary server:**

1. Choose option **2**, and then press **Enter**.

**Figure 10-158: Secondary HA Server Menu**

```
High Availability Menu
 1 ) Configure Server As Primary
 2 ) Configure Server As Secondary
 3 ) HA Status
 4 ) Back to Main Menu
Choose: 2
```



**Note:** The Secondary server configuration **MUST** be performed after the Primary server configuration has completed and its status is 'EMS Server is running'.

2. After the HA packages are installed, you are prompted for the 'Primary IP' and *acems* user password (you might also be prompted to answer 'yes' before connecting)

**Figure 10-159: Primary HA Server IP**

```
Start Heartbeat Configuration
  Primary Server IP:[-1]: 10.7.14.144
acems@10.7.14.144's password:
```

The Secondary server copies the HA configuration files from the Primary server and then starts the installation process.

**Figure 10-160: Secondary HA Server Configuration**

```

Start Heartbeat Configuration
  Primary Server IP:[-1]: 10.7.14.143
acems@10.7.14.143's password:
drbd.conf
ha.cf
cib.xml
haresources
Copy files from primary server:      [ OK ]
Update primary parameters in secondary:
  Global IP(eth0):                   10.7.14.215
  Global IP(eth1):                   10.77.10.215
  Primary IP:                        10.7.14.143
  Primary Host:                      EMS-Linux143
  Secondary IP:                      10.7.14.144
  Secondary Host:                    EMS-Linux144
  Ping IP:                           10.7.0.1,10.77.10.1

Press any key to continue... █
    
```

3. When prompted '[need to type **yes** to confirm]' press **yes**.
4. When prompted 'Press any key to continue...' press **Enter**.

### 10.4.10.5 EMS Server Manual Switchover

Manual switchover can be performed from either the Primary HA or Secondary HA server.

➤ **To manually switchover the active EMS server:**

1. Choose option **4**, and then press **Enter**.
2. Type **y** to confirm your selection.

**Figure 10-161: Manual Switchover**

```

High Availability Menu
 1 ) HA Status
 2 ) HA Switchover
 3 ) Uninstall HA
 4 ) Back to Main Menu
Choose: 2

You are about to switchover: EMS-Linux2 --> EMS-Linux6!!
Are you sure that you want to continue ? (y/n/q)

```

During the manual switchover process, the "switchover in process..." message is displayed in the EMS server machine where the command was activated. If you run the 'HA Status' command on the other server, it will display the HA status of the Primary server as STANDBY until the Secondary server becomes the Primary server.

**Figure 10-162: Switchover Status**

```

High Availability Status
-----

HA Heartbeat Service Status [ UP ]
HA DRBD Service Status [ UP ]

EMS-Linux2 HA Status [ STANDBY ]
EMS-Linux2 HA Location Status [ Primary ]
EMS-Linux2 Data Sync Status [ UpToDate ]

EMS-Linux6 HA Status [ ONLINE ]
EMS-Linux6 HA Location Status [ Secondary ]
EMS-Linux6 Data Sync Status [ UpToDate ]

Network Connection(10.3.180.80) [ OK ]

HA EMS Status [ EMS WatchDog process is not running!! ]

```

After the Secondary server becomes the Primary server, a few minutes are required until the EMS application is up and running.

**Figure 10-163: Status after Switchover**

```

High Availability Status
-----
HA Heartbeat Service Status      [  UP  ]
HA DRBD Service Status          [  UP  ]

EMS-Linux6 HA Status            [  ONLINE  ]
EMS-Linux6 HA Location Status    [  Primary  ]
EMS-Linux6 Data Sync Status     [  UpToDate  ]

EMS-Linux2 HA Status            [  ONLINE  ]
EMS-Linux2 HA Location Status    [  Secondary  ]
EMS-Linux2 Data Sync Status     [  UpToDate  ]

Network Connection(10.3.180.80) [  OK  ]

HA EMS Status                   [  EMS Server is running!!  ]
    
```

### 10.4.10.6 EMS HA Uninstall

The user should uninstall the EMS HA application on both the Primary and Secondary servers under the following circumstances:

- EMS Software version upgrade.
- EMS server network configuration changes.

➤ **To uninstall EMS HA:**

- Choose option **3**, and then press **Enter**.

**Figure 10-164: Uninstall EMS HA**

```

High Availability Menu
 1 ) HA Status
 2 ) HA Switchover
 3 ) Uninstall HA
 4 ) Back to Main Menu
Choose: 3
Are you sure that you want to continue ? (y/n)y
    
```

The uninstall process takes 1-2 minutes with the following output:

**Figure 10-165: Uninstall EMS HA Status Display**

```
CentOS release 5.3 (Final)
Stopping High-Availability services:
[ OK ]
Remove rpm: [ OK ]
Remove rpm: [ OK ]
Remove rpm: [ OK ]
Remove rpm: [ OK ]
error reading information on service heartbeat: No such file or directory
EMS Server is already stopped!
Stop EMS service: [ OK ]
Enable automatic DB stop : [ OK ]
Enable automatic DB start : [ OK ]
Enable automatic agent start : [ OK ]
Enable automatic listener start : [ OK ]
Enable automatic EMS start : [ OK ]
umount: /dev/drbd0: not mounted
Stopping all DRBD resources.

Stop drbd service: [ OK ]
Remove rpm: [ OK ]
/sbin/service
Stopping all DRBD resources.
warning: /etc/drbd.conf saved as /etc/drbd.conf.rpmsave
Remove rpm: [ OK ]
Re-mount data : [ OK ]
Update fstab : [ OK ]
***** HA uninstall finished *****
press any key to continue
```



**Note:** The EMS application doesn't start automatically after this process has completed. To start the EMS, reboot the EMS server or quit the EMS Server Manager and run it again using the 'Start EMS Server' option.

### 10.4.10.7 EMS HA – General Information

This section provides general information on the HA configuration.

#### 10.4.10.7.1 EMS Server Manager

EMS Server Manager displays dynamic menus. Each menu is displayed differently according to the current server's state.

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

- Start/Stop EMS Server

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

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

In some cases, the menu will only be updated after running EMS Server Manager again. For instance, after HA installation, the "Start/Stop EMS Server" option will be hidden after exiting the EMS Server Manager and running it again.

### 10.4.10.7.2 HA Status

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

➤ **To verify the EMS HA status:**

1. Choose option **1**, and then press **Enter** (Before performing HA configuration, "HA Status" is the 3<sup>rd</sup> option in the menu)

**Figure 10-166: EMS HA Status**

```
High Availability Menu
 1 ) HA Status
 2 ) HA Switchover
 3 ) Uninstall HA
 4 ) Back to Main Menu
Choose: 1
```

The following status view is displayed (Example only):

**Figure 10-167: EMS HA Status - Example Display**

```
High Availability Status
-----
HA Heartbeat Service Status [ UP ]
HA DRBD Service Status [ UP ]

EMS-Linux141 HA Status [ ONLINE ]
EMS-Linux141 HA Location Status [ Primary ]
EMS-Linux141 Data Sync Status [ UpToDate ]

EMS-Linux142 HA Status [ OFFLINE ]
EMS-Linux142 HA Location Status [ Unknown ]
EMS-Linux142 Data Sync Status [ DUnknown ]

Network Connection(10.7.0.1) [ OK ]

HA EMS Status [ EMS Server is running!! ]

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

- **HA Heartbeat Service Status:** Whether the heartbeat service is installed and running.
- **HA DRBD Service Status:** Whether the data replication service is installed and running.
- **<HOST\_NAME > HA Status:** The following states are available:
  - ◆ ONLINE – HA is enabled and heartbeat packets have been sent.
  - ◆ OFFLINE – HA is disabled or does not exist (this state usually appears for several minutes after the new installation).
  - ◆ IN Progress – HA has started (this state usually appears for several seconds immediately after the new installation).

- **<HOST\_NAME > HA Location Status:** the following states are available:
  - ◆ Unknown – Cannot resolve if the EMS server is Primary or Secondary
  - ◆ Primary - The current working server
  - ◆ Secondary - the redundant server
- **<HOST\_NAME > HA Data Sync Status:** the following states are available:
  - ◆ DUnknown - Cannot resolve whether the EMS server data is synchronized with the other server
  - ◆ UpToDate – The replicated data is synchronized with the Primary server
  - ◆ Inconsistent – The replicated data is in the progress of synchronizing with the Primary server
- **Network Connection (<Ping Node>)** - For each configured ping node, this status verifies if there is a network connection to it.
- **HA EMS Status:** The current state of the EMS server and watchdog processes:
  - ◆ The EMS server is running – the EMS server process is up.
  - ◆ The EMS is not installed
  - ◆ The EMS server is not running – the EMS watchdog is trying to start the EMS server.
  - ◆ The EMS watchdog is not running.
  - ◆ Unknown, Not Primary Server – This state is always displayed on the Secondary server. In addition, it displays when HA is not configured.



### 10.4.10.7.3 Advanced Status View

Figure 10-168: Advanced Status View

```

Heartbeat Advanced Status
-----
heartbeat OK [pid 21524 et al] is running on ems-linux6 [ems-linux6]...

=====
Last updated: Mon Jun 10 09:08:10 2013
Current DC: ems-linux2 (69778371-0a03-b402-faaf-657669826990)
2 Nodes configured.
1 Resources configured.
=====

Node: ems-linux6 (69778371-0a03-b406-faaf-657669826990): online
Node: ems-linux2 (69778371-0a03-b402-faaf-657669826990): online

Resource Group: group_1
  drbddisk_1 (heartbeat:drbddisk): Started ems-linux2
  Filesystem_2 (ocf::heartbeat:Filesystem): Started ems-linux2
  IPAddr-resource (ocf::heartbeat:IPAddr2): Started ems-linux2
  resource-EMS-Server (lsb:EMSServer): Started ems-linux2

DRBD Advanced Status
-----
drbd driver loaded OK; device status:
version: 8.2.4 (api:88/proto:86-88)
GIT-hash: fc00c6e00alb6039bfcebe37afa3e7e28dbd92fa build by root@EMS-Linux143, 2011-01-26 12:04:18
0: cs:SyncTarget st:Secondary/Primary ds:Inconsistent/UpToDate C r---
  ns:0 nr:2942588 dw:2941852 dr:0 al:0 bm:179 lo:24 pe:1372 ua:23 ap:0
  [>.....] sync'ed: 4.4% (63685/66557)M
  finish: 0:16:58 speed: 63,804 (56,556) K/sec
  resync: used:4/31 hits:185355 misses:196 starving:0 dirty:0 changed:196
  act_log: used:0/257 hits:0 misses:0 starving:0 dirty:0 changed:0

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

```

The advanced status view provides a more detailed view of the EMS HA status. This command is particularly important during the initial synchronization between the primary and secondary EMS servers when the precise percentage of the stage of the EMS HA synchronization process is displayed (highlighted in green in the above figure).

#### **10.4.10.7.4 EMS Client**

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

#### **10.4.10.7.5 EMS Server Upgrade**

EMS server version upgrade cannot be performed while HA is configured.

To upgrade the servers, HA must be uninstalled prior to the upgrade.

It is recommended to uninstall the secondary server first and only then the primary server.

- To uninstall HA, see Section [10.4.10.6](#) on page [192](#).
- To upgrade the EMS server, see Section [8.2](#) on page [74](#).

#### **10.4.10.7.6 EMS Server Restore**

EMS server restore cannot be performed while HA is configured.

To restore the EMS server, HA must be uninstalled prior to the restore.

It is recommended to uninstall the secondary server first and only then the primary server. After restoring the server, HA should be reconfigured.

- To uninstall HA, see Section [10.4.10.6](#) on page [192](#).
- To restore the EMS server see Section [10.4.8](#) on page [176](#).

### 10.4.11 Syslog Configuration

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

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

1. In the EMS Server Manager root menu, choose **Syslog Configuration** option, and then press **Enter**.
2. To send EMERG events to the system console, type **y**, press **Enter**, and then confirm by typing **y** again.

**Figure 10-169: Syslog Configuration**

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

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

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

**Figure 10-170: Forward Messages to an External Server**

```

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

3. To forward messages to an external server, type **y**, press **Enter**, type the desired **Facility** from the list, and then press **Enter**.
4. Type the desired **Severity** from the list and press **Enter**, and then type the external server host name or IP address.

## 10.4.12 Board Syslog Logging Configuration

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



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

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the EMS server machine.

The syslog log file 'syslog' is located in the following EMS server directory:

```
/opt/ACEMS/NBIF/mgDebug/syslog'
```

The syslog file is automatically rotated once a week or when it reaches 100 MB. Up to four syslog files are stored.

### ➤ To enable device syslog logging:

1. In the EMS Server Manager root menu, choose **Board Syslog Logging Configuration** option, and then press **Enter**.

**Figure 10-171: Board Syslog Logging Configuration**

```
Board Syslog Logging configuration
Board Syslog Logging Disabled

Enable board syslog logging ? (y/n) y
```

2. Type **y**, and then press **Enter**.

### 10.4.13 TP Debug Recording Configuration

Debug recordings packets from all managed machines can be logged directly to the EMS server without the need for a 3<sup>rd</sup> party network sniffer in the same local network.



**Note:** This feature is only relevant for CPE products. Debug recording packets are collected according to the device's configured Debug parameters. For more information, see the relevant device's *User's manual*.

The EMS server runs the Wireshark network sniffer, which listens on a particular configured port. The sniffer records the packets to a network capture file in the Debug Recording (DR) directory. You can then access this file from your PC via FTP.

The EMS Server Manager is used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the EMS server IP.

The DR capture file is located in the following EMS server directory:

`'/opt/ACEMS/NBIF/mgDebug/DebugRecording'`

The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close i.e. if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the EMS server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

➤ **To enable TP Debug Recording:**

1. In the EMS Server Management menu, choose **TP Debug Recording Configuration** option, and then press **Enter**.
2. Type **y** and then press **Enter** twice.

**Figure 10-172: Board Syslog Logging Configuration**

```
Board Syslog Logging configuration
TP Debug Redording Disabled

Enable TP Debug Redording ? (y/n) y
Don't forget to disable TP Debug Recording when you are done.
Press Enter to continue...
```

Recording files are saved in /data/NBIF/mgDebug directory on the server.



**Note:** It is highly recommended to disable the 'TP Debug Recording' feature when you have completed recording because this feature heavily utilizes system resources.

**Reader's Notes**



# Part V

## Configuring the Firewall and Installing the EMS Client

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



# 11 Configuring the Firewall

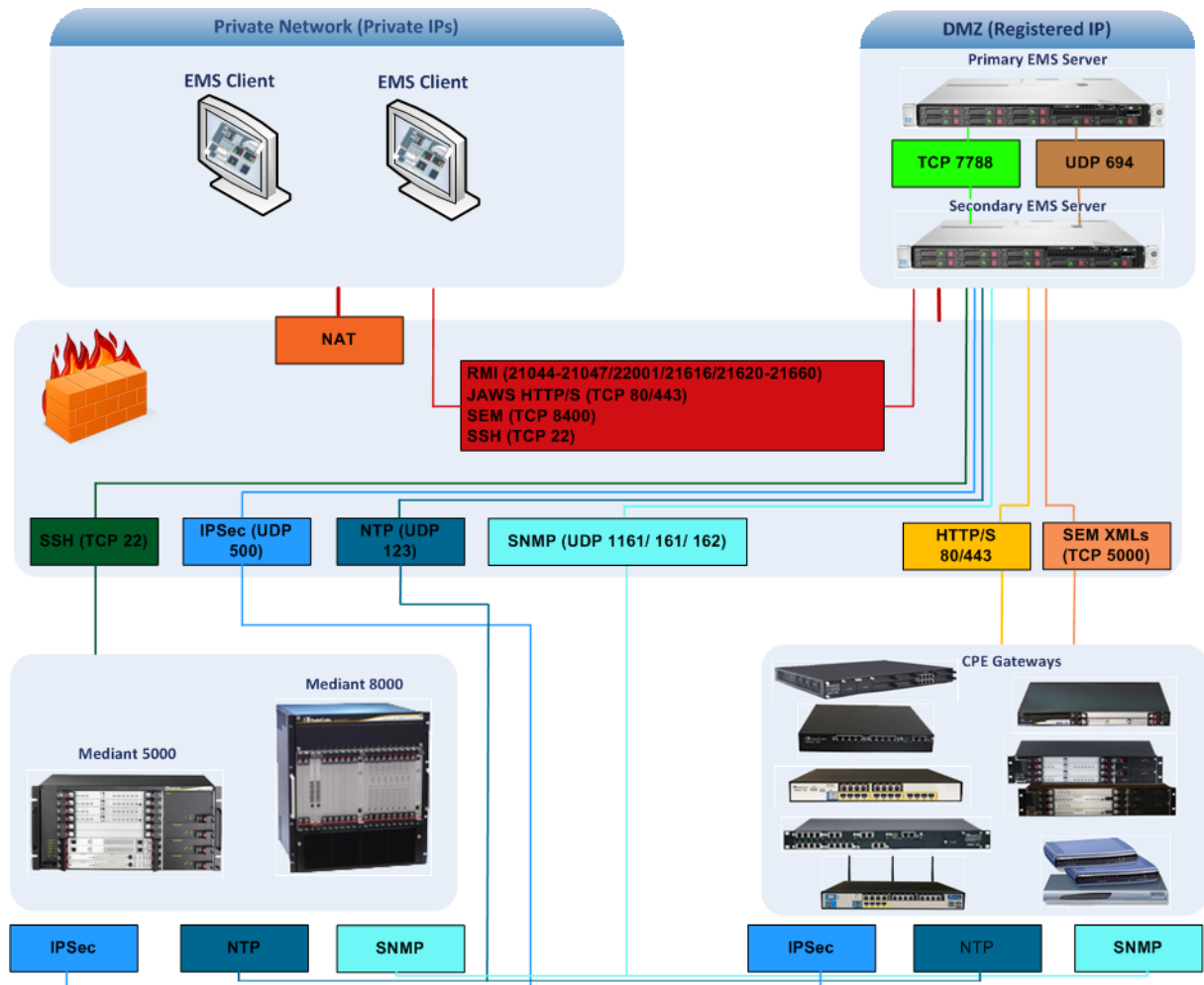
To enable EMS Client ↔ EMS Server ↔ Managed Gateways communication according to [Figure 11-1](#), define the rules specified in the Firewall Configuration Rules table below:

**Table 11-1: Firewall Configuration Rules**

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
<b>EMS Client ↔ EMS Server</b>	TCP	22001, 21044-21047, 21616 and 21620-21660	RMI communication. Initiator: EMS Client	EMS Server side / Bi-Directional
	TCP	22	SSH communication between EMS server and client PC. Initiator: Client PC	EMS Server side / Bi-Directional
	TCP	80	HTTP for JAWS. Initiator: Client PC	EMS Server side / Bi-Directional
	TCP	443	HTTPS for JAWS and NBIF. Initiator: Client PC	
<b>EMS server ↔ All Media Gateways</b>	UDP	1161	SNMP communication. Initiator: EMS Server	EMS Server side / Bi-Directional
	UDP	162	SNMP Traps. Initiator: MG	EMS Server side / Receive only.
	UDP	161	SNMP communication. Initiator: EMS Server	MG side / Bi-Directional
	UDP	123	NTP synchronization. Initiator: MG (and EMS Server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-Directional
	UDP	500	IPSec communication. Initiator: Both sides	Both sides / Bi-Directional

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
<b>EMS Server ↔ All Media Gateways except M5K &amp; M8K</b>	TCP	80	HTTP connection for files transfer. Initiator: EMS Server	EMS Server side / Bi-Directional
	TCP	443	HTTPS connection for files transfer. Initiator: EMS Server	
<b>EMS Server ↔ Mediant 5000/8000 Media Gateways</b>	TCP	22	SSH communication for files transfer. Note, ports should be open for both Global IP and SC private IP Addresses. Initiator: EMS Server	Mediant 5000/Mediant 8000 side / Bi-Directional
<b>Media Gateways ↔ SEM server</b>	TCP	5000	XML based SEM communication. Initiator: MG	EMS Server side / Bi-Directional
<b>SEM client ↔ Tomcat server</b>	TCP	8400	SEM connection between the user's browser and Tomcat server. Initiator: Client's PC.	EMS Server side / Bi-Directional
<b>Primary EMS Server ↔ Secondary EMS Server (HA Setup)</b>	TCP	7788	Database replication between the servers. Initiator: Both Servers	Both EMS Servers / Bi-Directional
	UDP	694	Heartbeat packets between the servers. Initiator: Both Servers	

Figure 11-1: Firewall Configuration Schema



**Note:** The above figure displays images of example CPE gateways. For the full list of supported products, see Section 2.1.1 on page 23.

- NOC ↔ EMS (Server) ports

**Table 11-2: 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 11-3: 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

## 12 Installing the EMS Client

This section describes how to install the EMS client.

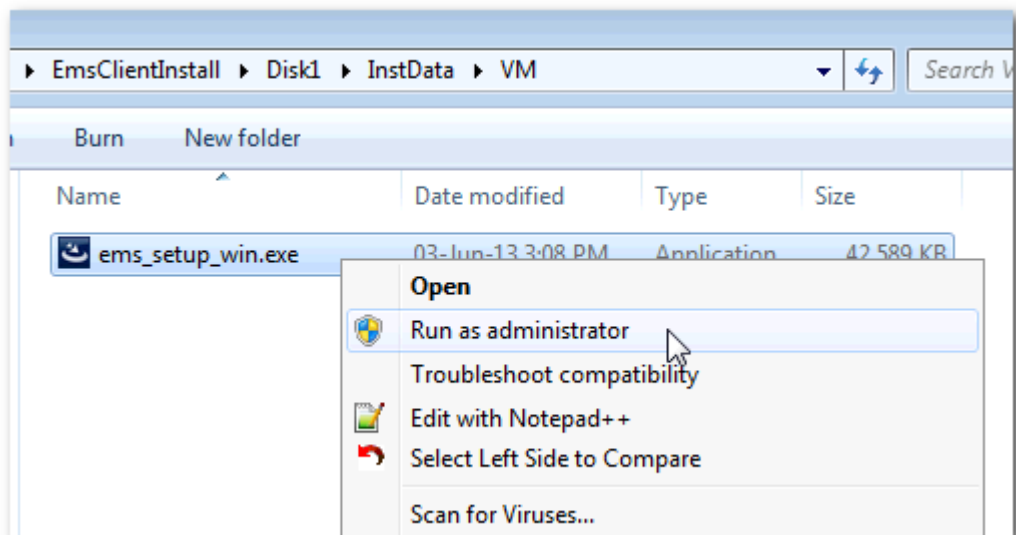
### 12.1 Installing the EMS Client on a Client PC or Laptop

➤ To install the EMS on a client PC or Laptop:

1. Insert AudioCodes' EMS installation disk into the CDROM.
2. Open the EmsClientInstall\Disk1\InstData\VM directory.
3. On a PC: Double-click the EMS client Installation file `ems_setup_win.exe` and follow the installation instructions.

On a Laptop installed with Windows 7: Right-click the EMS client Installation file `ac_ems_setup_win.exe` and select 'Run as Administrator' from the menu:

**Figure 12-1: EMS Client Installation-Run as Administrator**



4. 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`.

## 12.2 Running the EMS on a Client PC or Laptop

This section describes how to run the EMS client.

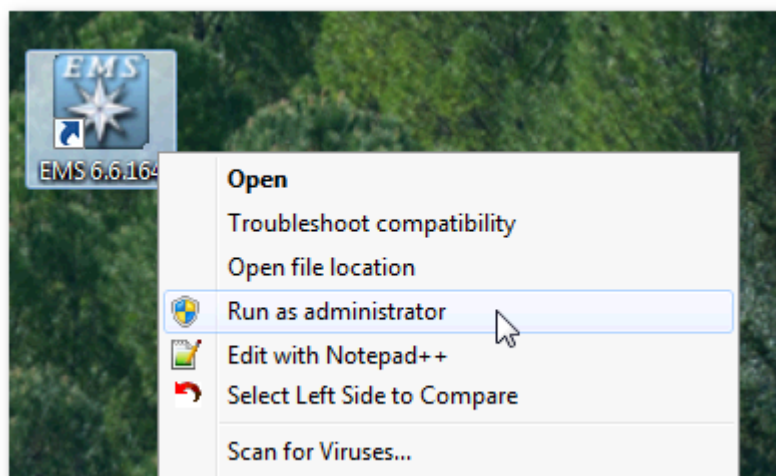
➤ **To run the EMS on a client PC:**

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

➤ **To run the EMS on a client Laptop:**

- Right-click the EMS client icon on your desktop and select 'Run as Administrator' from the menu:

**Figure 12-2: Running EMS Client-Run as Administrator**





## 12.3 Initial Login

This section describes how to initially login to the EMS client.

➤ **To initially login to the EMS client:**

1. Log in as user 'acladmin' with password 'pass\_1234' or 'pass\_12345'.



**Note:** First-time access defaults are case sensitive. After you login to the EMS for the first-time, you are prompted to change the default password. If you incorrectly define these or the field Server IP Address, a prompt is displayed indicating that the fields should be redefined correctly.



**Note:** First-time access defaults are case sensitive. After you login to the EMS for the first-time, you are prompted to change the default password. If you incorrectly define these or the field Server IP Address, a prompt is displayed indicating that the fields should be redefined correctly.

2. In the main screen, open the 'Users List' and add new users according to your requirements.

## 12.4 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:

- 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 as follows:

- **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`

# Part VI

## Appendices

This part describes additional EMS server procedures.



## A Frequently Asked Questions (FAQs)

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

### A.1 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.

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

**Figure A-1: Sun Solaris Server Power Button**



### A.2 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**.

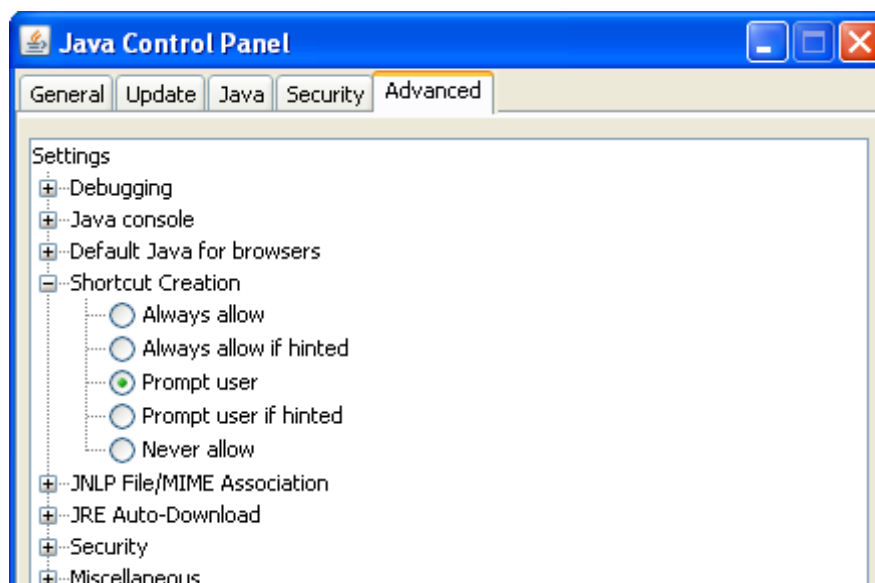
**Figure A-2: EMS Client Removal**



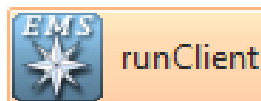
3. After removing the EMS application, go to **Start>Settings>Control Panel**

4. Double-click the Java Icon .

5. Choose the **Advanced** tab.

**Figure A-3: Java Control Panel**


6. Choose Shortcut Creation in the Settings dialog.
7. Select the **Always allow** box to always create an icon on desktop or Prompt user to ask before icon creation.
8. Install client using Jaws. For more information, see Section 12.4 on page 214.
9. After the installation has completed, the new Icon is created on your desktop:



## A.3 After Rebooting the Machine

- Q:** The database doesn't start automatically after the machine is rebooted.
- A:** Perform the procedure below:

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

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

## A.4 Changes Not Updated in the Client

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

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

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

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

## A.5 Removing the EMS Server Installation

**Q:** How do I remove the EMS server installation?

**A:** See Section 6.1 on page 38.

**Reader's Notes**



## B Site Preparation

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



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

1. EMS server data backup should be performed prior to machine formatting. For more information, see Section 10.4.6 on page 169. The Backup files should be transferred to another machine prior to the EMS server installation. Note, that these backup files cannot be used for other versions. They should be kept in case the user fails to install the 6.2 version, and decides to roll back to the previous version.
2. EMS Users: all the users' names and permissions should be saved. After the new EMS version is installed, these users should be defined manually with default passwords. To perform this task, in the EMS menu, choose Security > User's List menu.
4. EMS Tree: the user can export the gateways tree using the File > MGs Report command (example of the file is attached). This file is a CSV file and does not preserve secured information such as passwords. Therefore, we recommend extending it manually with columns including: SNMP read and write community strings, or SNMPv3 user details, IPsec pre-shared key and (Mediant 5000 / 8000) root password. This information will be required during the Media Gateway's definition in the newly installed EMS system. It's also highly recommended to perform gateway removal and adding and to ensure that the EMS <-> GW connection has been established.

**Figure B-1: Save MGs Tree Command**

	B	C	D	E	F	G	H	I	J	K	L
1	IP Address	Node Name	RegionName	Description	Product Type	Software	Connectio	Administra	Operative	Mismatch	Last Ch.
2	10.7.19.88	10.7.19.88	gena		MEDIANT 8000	5.8.57	Connectec	Unlocked	Enabled	No Misma	2009-11
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**

## C Daylight Saving Time (DST)

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

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

The following major changes are implemented:

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

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

### ■ EMS Server

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

New DST settings are fully supported starting v5.6.

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

### ■ EMS Client

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

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

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

## C.1 EMS Client

To apply new DST settings to the EMS client, update the Windows operating system (see Section C.3 on page 225).

## C.2 Windows

Install Windows OS patches as specified in the following URL:

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

### C.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
```

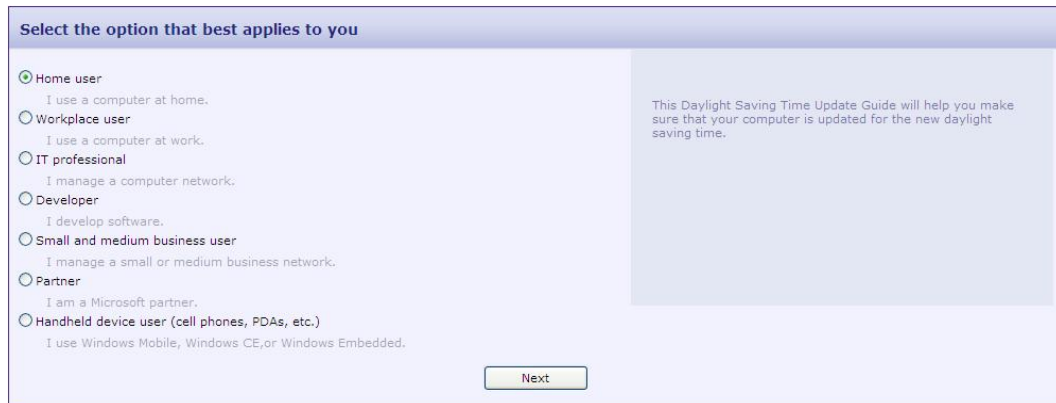
## C.3 Example of Installing Windows Patches on the EMS Client

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 (see below).

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



Select the option that best applies to you

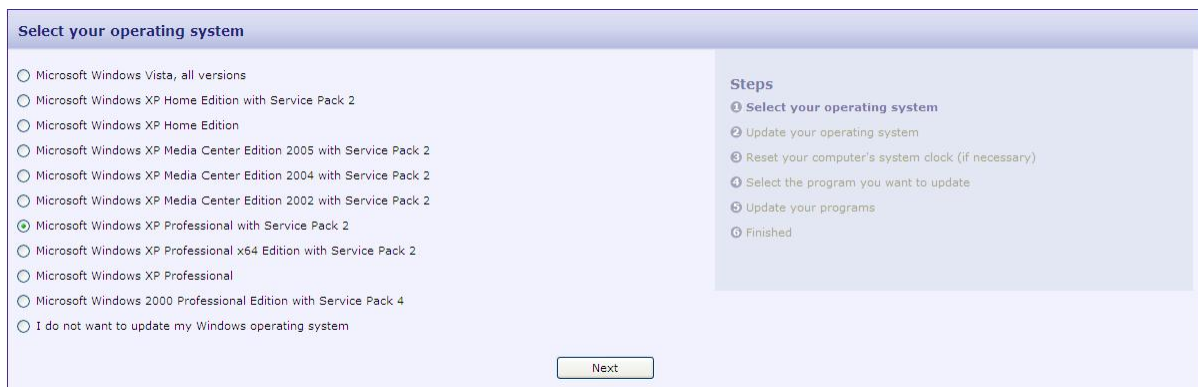
- Home user  
I use a computer at home.
- Workplace user  
I use a computer at work.
- IT professional  
I manage a computer network.
- Developer  
I develop software.
- Small and medium business user  
I manage a small or medium business network.
- Partner  
I am a Microsoft partner.
- Handheld device user (cell phones, PDAs, etc.)  
I use Windows Mobile, Windows CE, or Windows Embedded.

This Daylight Saving Time Update Guide will help you make sure that your computer is updated for the new daylight saving time.

Next

3. Select your operating system information.

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



Select your operating system

- Microsoft Windows Vista, all versions
- Microsoft Windows XP Home Edition with Service Pack 2
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Media Center Edition 2005 with Service Pack 2
- Microsoft Windows XP Media Center Edition 2004 with Service Pack 2
- Microsoft Windows XP Media Center Edition 2002 with Service Pack 2
- Microsoft Windows XP Professional with Service Pack 2
- Microsoft Windows XP Professional x64 Edition with Service Pack 2
- Microsoft Windows XP Professional
- Microsoft Windows 2000 Professional Edition with Service Pack 4
- I do not want to update my Windows operating system

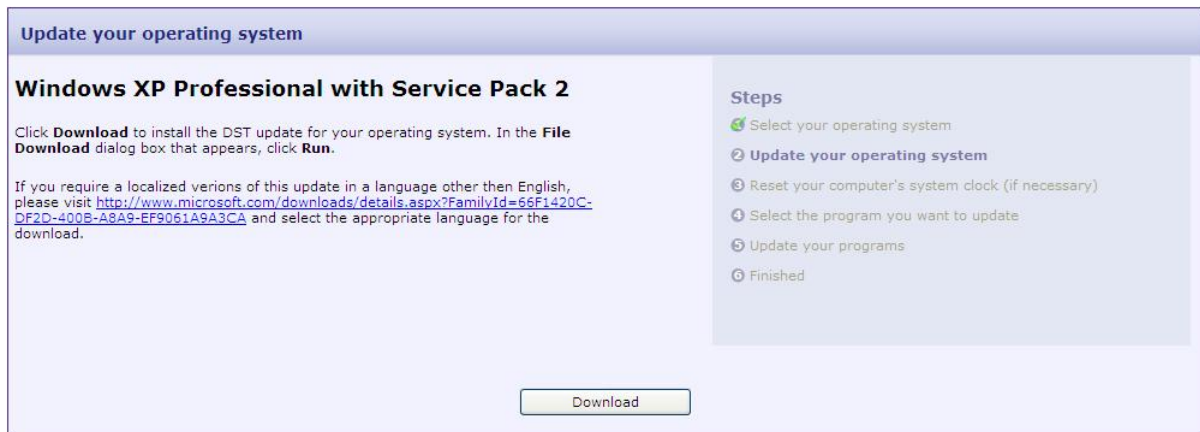
Steps

- 1 Select your operating system
- 2 Update your operating system
- 3 Reset your computer's system clock (if necessary)
- 4 Select the program you want to update
- 5 Update your programs
- 6 Finished

Next

4. Download and install the patch.

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



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

## D OpenCA OCSP Daemon (OCSPD) v1.5.2

This appendix describes the OpenCA OCSP Daemon (OCSPD) v1.5.2.

### D.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

### D.2 Installation

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

➤ **To install OpenCA OCSPD:**

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
```

### D.3 Viewing OCSPD Logs

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

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

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

## D.4 Starting/Stopping OCSPD

OCSPD is automatically started after reboot (via `/etc/rc2.d/S90ocspd` script). In addition, 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`

## D.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
```



## D.6 Configuring OCSPD

The OCSPD configuration is stored in the `/usr/local/etc/ocspd/ocspd.conf` file. Edit this file after the OCSPD package installation and configure the location of the 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 1<sup>st</sup> 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:

```
http://[user[:pwd]@]server[:port]/path_to_crl
```

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

1. Choose the correct database configuration section by removing comments for the `"dbms = dbms_http"` line and commenting out `"dbms = dbms_file"` line??.
2. In the `[dbms_http]` section, ensure that comments are removed for the 1<sup>st</sup> – `"0.ca = @http_ca_1"` and the 2<sup>nd</sup> – `"1.ca = @http_ca_2"` lines.
3. 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 1<sup>st</sup> CA. Use the following syntax when specifying URL:

```
https://[user[:pwd]@]server[:port]/path_to_crl
```

4. 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 2<sup>nd</sup> 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:

1. 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
```

2. Submit the generated CSR file – **/tmp/ocspd.csr** – to the CA. In response, you will receive a certificate file signed by this CA.
3. Place the certificate signed by the CA, together with the certificate of the CA itself, into the **/usr/local/etc/ocspd/certs** directory.
4. 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
```

## E Working with HTTPS

This appendix describes the actions required to work with HTTPS and AudioCodes self-signed certificates.

### E.1 Working with HTTPS on CPE Media Gateways

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



**Note:** If you wish to work with HTTPS and external certificates that are signed by an external trusted CA, perform the procedure described in Section F on page 235.

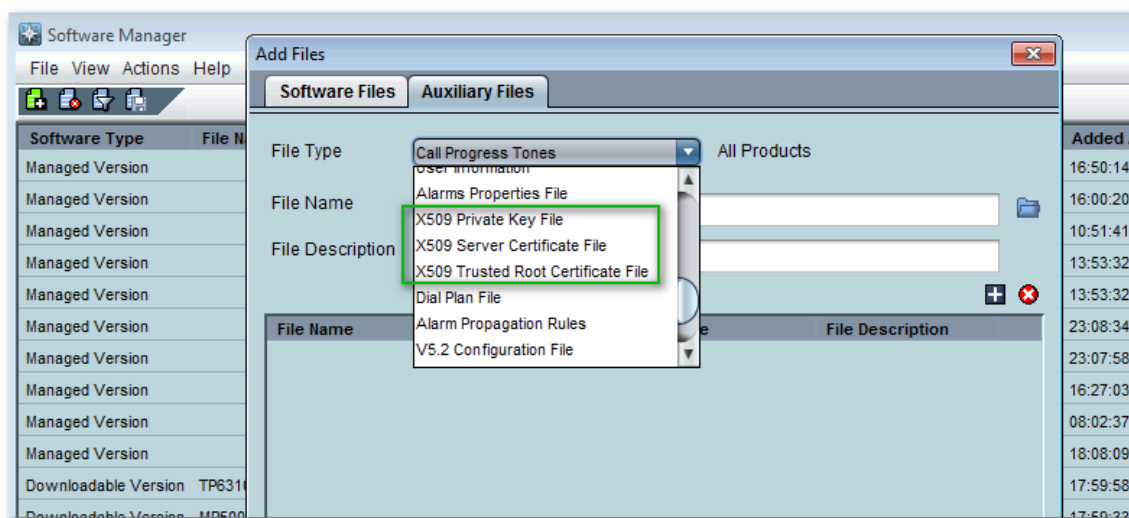
When working in *secure mode* (HTTPS enabled), the “appropriate” gateway certificate (the certificate that is signed by the same CA as the EMS server certificate) **must** be added to the EMS Software Manager. In addition, the CA certificate must also be loaded on the Media Gateway devices.

➤ **To set up an HTTPS connection with the Media Gateway:**

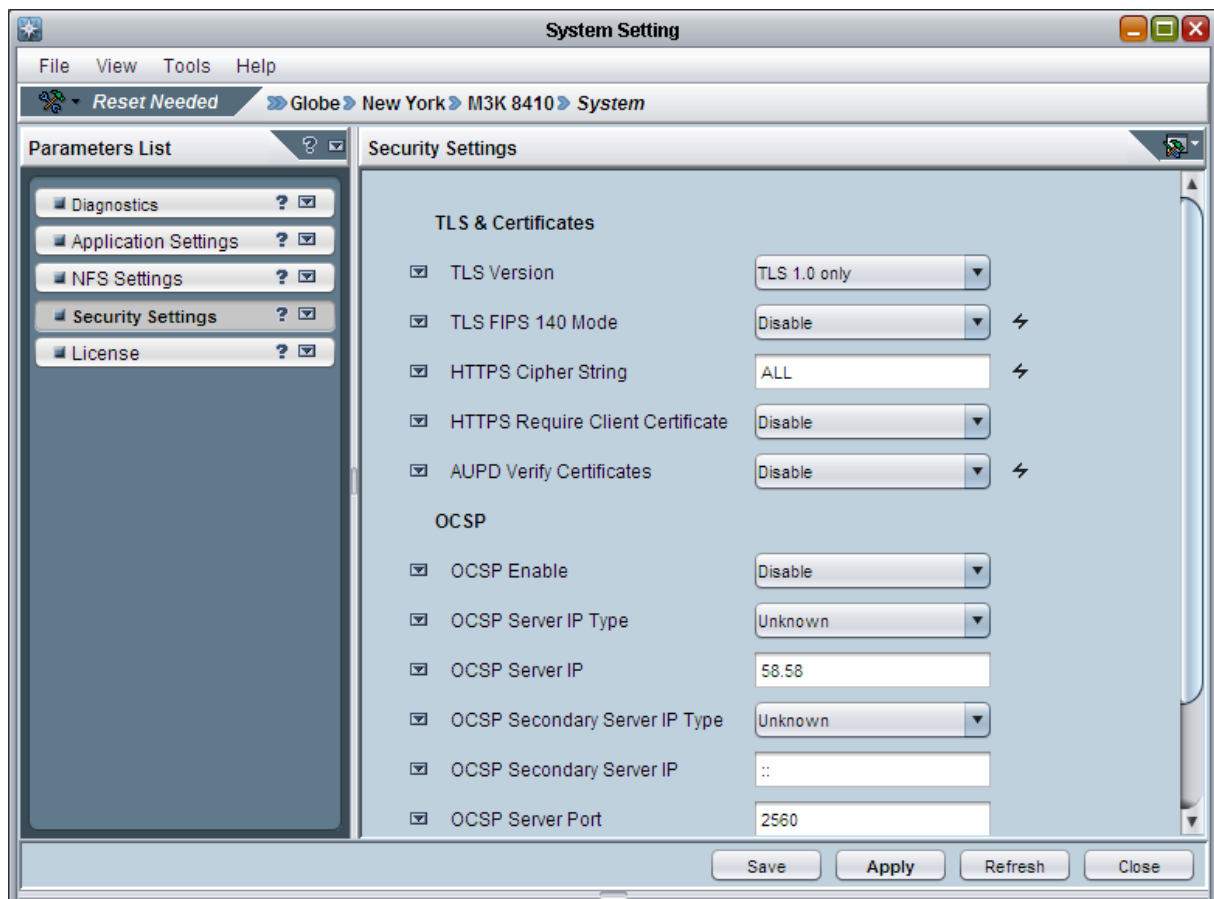
1. Install and login to the EMS client.
2. Add the following files to the EMS Software Manager from the EMS client folder path: externals\security\clientNssDb\boardCertFiles – ‘board\_cert.pem’, ‘root.pem’, ‘board\_pkey.pem’.

Each one of these files has its own file type in the Software Manager:

**Figure E-1: X509 Files-Software Manager**

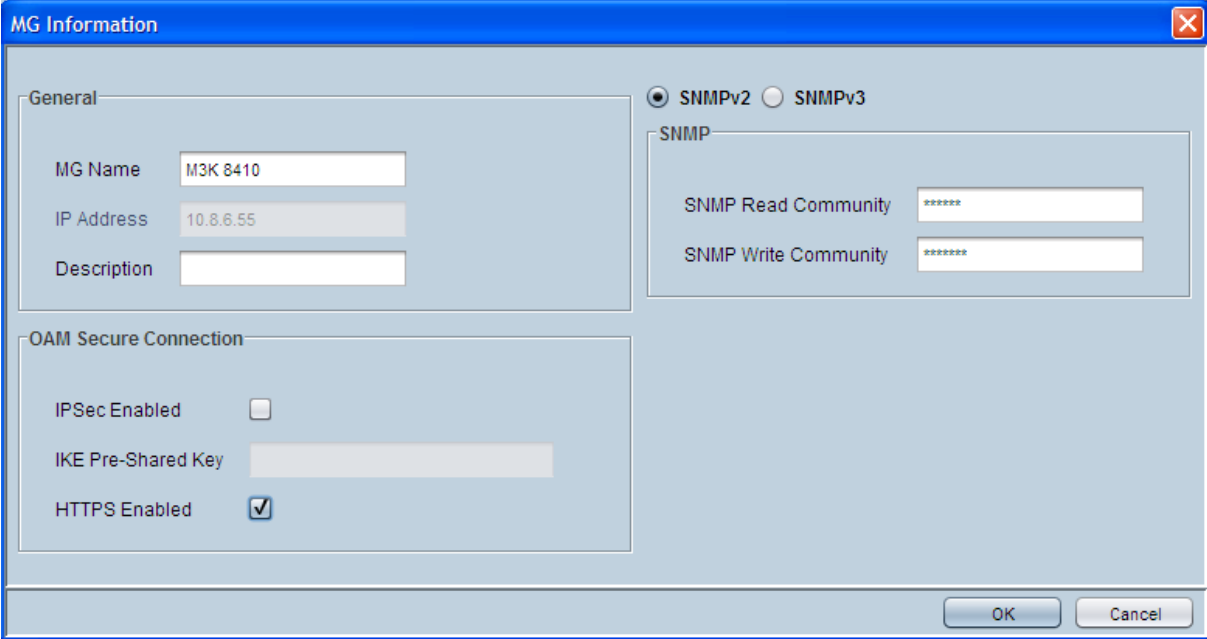


3. Download these files to the Media Gateway as Server Certificate, Trusted Root Certificate Store and Private Key respectively, using the 'Software Upgrade' option by HTTP.  
It is recommended to perform this action in a private internal network.
4. Open the 'System Settings' configuration frame and select the 'General Settings' Tab.
5. Set the parameters 'TLS Version' to 'TLS 1.0 only' and 'HTTPS Cipher String' to 'ALL' as illustrated below:

**Figure E-2:: System Settings**


6. Reset the Media Gateway.
7. Select the 'HTTPS Enabled' check box as illustrated in the figure below.

Figure E-3: MG Information



The image shows a dialog box titled "MG Information" with a blue header bar and a close button in the top right corner. The dialog is divided into several sections:

- General:** Contains three text input fields: "MG Name" with the value "M3K 8410", "IP Address" with the value "10.8.6.55", and "Description" which is empty.
- SNMP:** Located at the top right, it has two radio buttons: "SNMPv2" (selected) and "SNMPv3". Below them are two text input fields: "SNMP Read Community" and "SNMP Write Community", both containing six asterisks (\*\*\*\*\*).
- OAM Secure Connection:** Located at the bottom left, it contains three items: "IPSec Enabled" with an unchecked checkbox, "IKE Pre-Shared Key" with a text input field, and "HTTPS Enabled" with a checked checkbox.

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

8. Perform the desired HTTPS secure action (software upgrade or auxiliary file download).

For more information, refer to the relevant *CPE Gateway User's Manual*.

## E.2 Working with HTTPS for JAWS and NBIF

Load 'clientcert.crt' file from the EMS client to your web browser. This file includes the certificate for working with a web browser. The file is located under the directory: 'externals\security\clientNssDb\clientcert.crt'.

**Reader's Notes**

# F External Security Certificates-Signing Procedure

This appendix describes the External Security Certificates Signing Procedure.

## F.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.

## F.2 Installing External CA Certificates on the EMS Server

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

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



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

### ➤ To install external CA Certificates on the EMS server:

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

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

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

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

echo fips140-2 > /tmp/pwdfilename.txt

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

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

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

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

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

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

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

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

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

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

9. Cleanup temporary files.

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

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





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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

## F.6 Client – Server Communication Test

- Verify the Client – Server communication.

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

## F.7 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. Under these circumstances, the certificate should be in PKCS12 format and be loaded to the browser.

**Reader's Notes**

## G EMS Client and Server Certificates Extensions and DoD PKI

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

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

### ■ DoD PKI Validation Extensions

Validation extensions are implemented on the EMS server and client for addressing the DoD PKI requirements, such as certificate approval during SSL handshake information logging. By default, DoD PKI validations are disabled.

### ■ Certificate Management

Certificate management has been improved. Now the management of the certificates location and usage is easily configurable.

## G.1 DoD PKI Validation Extensions

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

### G.1.1 The CA Trust Chain

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

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

## G.1.2 DoD PKI Strict Validations

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

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

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

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

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

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

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

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



### G.1.3 Debugging

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

## G.2 DoD PKI and Certificate Management Extension

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

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

### G.2.1 SSL Handshake Process

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

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

### G.2.2 NSS Database Parameters

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

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

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

### G.2.3 HTTPS Client

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

'Externals\configurationProperties\clientNssConfig.properties'

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

### G.2.4 DoD PKI Strict Validations

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

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

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

- 'externals/configurationProperties/serverNssConfig.properties'

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

- 'externals/configurationProperties/clientNssConfig.properties'

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

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

The entire list of strict certification validations are described in Section [G.1.2](#) on page 244.

The option EmsServerManager – 'Strict PKI Configuration' under the 'Security' sub menu (see Section 10.3.4 on page 127) displays the status of the 'requireStrictCert' parameter and allows you to enable or disable this feature.



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

## G.2.5 Debugging

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

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

This directive indicates whether 'Strict PKI' is enabled.

- In the case of Java Web Start, the NSS database is located at the same path as the regular EMS client:

```
'externals\security\clientNssDb'
```

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

In addition, the file

```
'externals\configurationProperties\clientNssConfig.properties'
```

is located under the same relative path, and is configurable after the initial launch of the same version.

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

**Reader's Notes**

## H RAID 1 Configuration in Oracle/Sun Netra T5220

This appendix describes the procedure for configuring RAID 1 (Redundant Array of Independent Disks Level RAID 1) in Netra T5220 machines. This configuration implements disk mirroring, where data is written to two duplicate disks simultaneously, thereby providing data redundancy. As a consequence, RAID enhances performance and delivers fault tolerance. Redundancy is maintained, so long as at least one of the disk drives in the mirrored set is functioning.

Before creating the RAID device, you must create disk partitions on the different disk drives. Each RAID device can have multiple underlying devices (partitions). When using RAID1, it is recommended that these partitions be of the same size to avoid disk-space loss due to mirroring. A disk partition configured with RAID can no longer be managed as a regular partition, but only be controlled by the RAID device. From the moment RAID is configured, it is the RAID device that can be shared, scanned, formatted and mounted as a regular partition.



**Note:** This procedure has to be performed prior to the Solaris OS installation, since it **erases** all existing data on the machine's disks.

### ➤ To configure RAID1 on an Oracle/Sun Netra T5220 machine:

1. Connect via management serial port to the Netra T5220.
2. Plug in the EMS server's power cable.
3. Wait for the ILOM login prompt in the serial port and login:

```
SUNSP00144FAC6F3D login: root
Password: changeme
```

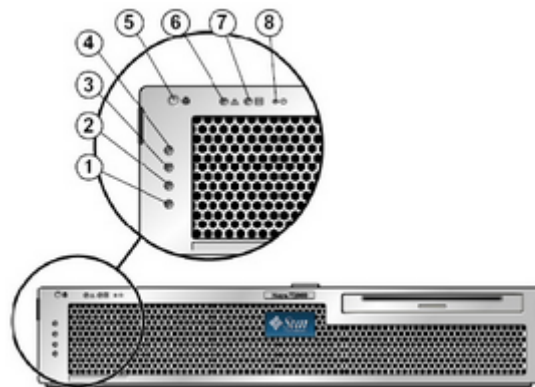


**Note:** This is the default password, you should change it.

4. Type the following command:

```
-> set /HOST/bootmode script="setenv auto-boot? false"
```

5. Turn on the power, using the front power button, #8 in the following image:

**Figure H-1: Sun Server Power Button**


6. Type the following commands:

```
-> set /HOST send_break_action=break
-> start /SP/console
```

7. Confirm the last command by pressing **y** and wait until you get the ok prompt:

```
{0} ok
```

8. Type the following commands to identify the default boot device:

```
{0} ok printenv boot-device
boot-device =          disk net
{0} ok devalias disk
disk                /pci@0/pci@0/pci@2/scsi@0/disk@0
```

9. Insert Netra's Solaris installation disk into the EMS server's CDROM and type the following command to use the CDROM for booting into single user mode:

```
{0} ok boot cdrom -s
```

10. Use the following command to determine the disk aliases (marked in red):

```
# cfgadm -al
Ap_Id          Type          Receptacle  Occupant
Condition
c1             scsi-sata    connected   configured
unknown
c1::dsk/c1t0d0 disk         connected   configured
unknown
c1::dsk/c1t1d0 disk         connected   configured
unknown
usb0/1         unknown     empty       unconfigured ok
usb0/2         unknown     empty       unconfigured ok
```

11. Configure RAID 1 using the following command (use the aliases from previous step) and confirm it by typing **Yes** (ignore messages about label corruption, this issue will be handled in the next step):

```
# raidctl -c -r 1 clt0d0 clt1d0
Creating RAID volume will destroy all data on spare space
of
member disks, proceed (yes/no)? yes
Volume clt0d0 is created successfully!
```

12. Configure and label the RAID volume. Always select the disk name that represents the RAID volume that you have configured:

```
# format
Searching for disks...
done
clt0d0: configured with capacity of 278.99GB
AVAILABLE DISK SELECTIONS:
    0. clt0d0 <LSILOGIC-LogicalVolume-3000 cyl 65533 alt
    2 hd 32 sec 279>
        /pci@0/pci@0/pci@2/scsi@0/sd@0,0
Specify disk (enter its number): 0
selecting clt0d0
[disk formatted]
WARNING: /pci@0/pci@0/pci@2/scsi@0/sd@0,0 (sd0):
    Corrupt label - bad geometry
Disk not labeled. Label it now?          Label says
585925000 blocks; Drive says 585805824 blocks
Yes
...
FORMAT MENU:
    disk          - select a disk
    type          - select (define) a disk type
    partition     - select (define) a partition table
    current       - describe the current disk
    format        - format and analyze the disk
    repair        - repair a defective sector
    label         - write label to the disk
    analyze       - surface analysis
    defect        - defect list management
    backup        - search for backup labels
    verify        - read and display labels
    save          - save new disk/partition definitions
    inquiry       - show vendor, product and revision
    volname       - set 8-character volume name
    !<cmd>        - execute <cmd>, then return
quit
format> type

AVAILABLE DRIVE TYPES:
    0. Auto configure
    1. Quantum ProDrive 80S
    2. Quantum ProDrive 105S
    3. CDC Wren IV 94171-344
    4. SUN0104
    5. SUN0207
    6. SUN0327
    7. SUN0340
```

```

      8. SUN0424
      9. SUN0535
     10. SUN0669
     11. SUN1.0G
     12. SUN1.05
     13. SUN1.3G
     14. SUN2.1G
     15. SUN2.9G
     16. Zip 100
     17. Zip 250
     18. Peerless 10GB
     19. LSILOGIC-LogicalVolume-3000
     20. other
Specify disk type (enter its number)[19]: 0
clt0d0: configured with capacity of 278.99GB
<LSILOGIC-LogicalVolume-3000 cyl 65533 alt 2 hd 32 sec 279>
selecting clt0d0
[disk formatted]
format> label
Ready to label disk, continue? Y
format> disk
AVAILABLE DISK SELECTIONS:
      0. clt0d0 <LSILOGIC-LogicalVolume-3000 cyl 65533 alt
2 hd 32 sec 279>
      /pci@0/pci@0/pci@2/scsi@0/sd@0,0
  
```



```
Specify disk (enter its number)[0]: 0
selecting clt0d0
[disk formatted]
format> quit
# reboot
```

13. Now you can install the operating system using the Solaris 10 OS installation DVD for Netra T5220.

**Reader's Notes**

# I EMS Application Acceptance Tests

This appendix describes the EMS Application Acceptance tests.

## I.1 Introduction

The following series of tests are defined as acceptance tests for the EMS application and cover all the major areas and features of the application.

The tests should run sequentially as a single test with dependencies. For example, you can't add a Media Gateway to the EMS before you have added a software file.

It is also recommended to integrate the below test plan in the Acceptance Test Plan (ATP) of the complete solution of which the EMS is a component. The ATP is typically developed by the solution integrator and covers all solution components (e.g. Softswitch, Media Gateway, IP routers etc). The ATP typically verifies "end to end" functionality, for example, the calls running through the solution. The below test plan should be integrated in the ATP as part of this "end to end" functionality testing (e.g. you may send and receive calls through the Media Gateway, perform Media Gateway board switchover and verify that calls are recovered on the redundant board).

Prior to running the tests described below, the tester should have a basic understanding of how to operate the product. Next to each test case there is a reference to the relevant chapter in the documentation. The tester should read these chapters to acquire the required tools to run this test. Running this test can also be considered as an excellent hand's-on initial training session.

## I.2 Configuration

This section describes the EMS application configuration acceptance tests.

### I.2.1 Client Installation

**Table I-1: Acceptance Test – Client Installation**

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

## I.2.2 Server Installation

**Table I-2: Acceptance Test – Server Installation**

Step Name	Description	Expected Result
<b>Server</b>	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.
<b>Reboot</b>	Reboot the EMS server	The EMS server starts automatically.
<b>Connect</b>	Connect to the EMS server with the EMS client	The connection should succeed.

## I.2.3 Add Auxiliary File

**Table I-3: Acceptance Test – Add Auxiliary File**

Step Name	Description	Expected Result
<b>Software Manager</b>	Open the Software Manager Tools >> SW manager	The Software Manager window opens.
<b>Auxiliary Tab</b>	Choose the auxiliary tab	A new tab is opened with all the available auxiliary files.
<b>Add Auxiliary File</b>	Choose an auxiliary file that you usually work with such as: Call Progress Tone	A new file was added to the SW Manager.
<b>Add file browser</b>	Click the Add file Button (Plus sign)	Software File added to the Software Manager.



## I.2.4 Add Media Gateway

**Table I-4: Acceptance Test – Add MG**

Step Name	Description	Expected Result
<b>Add MG</b>	Add MG to the EMS	The Media Gateway appears in the EMS GUI.
<b>MG Status</b>	Click on the Media Gateway	The Media Gateway status is available in the GUI, including all LEDS and boards.



## I.2.5 Provisioning – Mediant 5000/ Mediant 8000

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

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

## I.2.6 Provisioning – CPE Devices

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



Step Name	Description	Expected Result
<b>Go to network frame</b>	Click on the network button.	Network configuration is displayed.
<b>RTP Settings tab</b>	Press on the application tab	Applications settings are displayed.
<b>Set parameter “NTP Server IP Address”</b>	Set the parameter to your PC IP address. 	The new value is set on the Media Gateway. 
<b>Restore parameter value</b>	Set the parameter back to your NTP Server IP address.	The old value was restored.



**Note:** CPE devices include the following products: MediaPack; Mediant 600; Mediant 800 MSBG; Mediant 800 Gateway and E-SBC, Mediant 850 MSBG, Mediant 1000 MSBG; Mediant 1000 Gateway and E-SBC; Mediant 1000, Mediant 2000, Mediant 2600 E-SBC, Mediant 3000 and Mediant 4000 E-SBC.

## I.2.7 Entity Profile – Digital CPE Devices

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




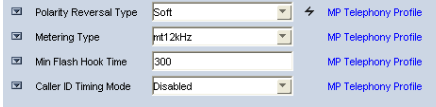
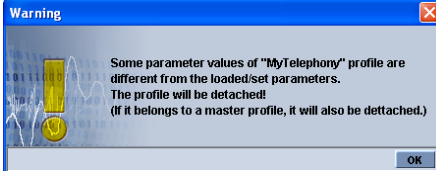
Step Name	Description	Expected Result
<b>Go to trunk level</b>	Drill down to trunk level	Trunks list appears according to board type.
<b>Trunk Properties</b>	Open trunk#1 properties	The frame provisioning opens and all the parameters are available.
<b>Trunk Configuration</b>	Configure the trunk	The new set of values appears on the provisioning screen.
<b>Apply</b>	Apply the new configuration	Action successful and there were no errors and no purple tabs.
<b>Save profile</b>	Save the profile, choose an appropriate name. 	The new profile appears in the profiles list. 
<b>Apply to All</b>	Download this configuration easily to all trunks by using the apply to all	Open trunk#2 and verify the configuration is equal to trunk#1.



**Note:** Digital CPE devices include the following products: Mediant 600; Mediant 800 MSBG; Mediant 800 Gateway and E-SBC, Mediant 850 MSBG, Mediant 1000 MSBG; Mediant 1000 Gateway and E-SBC; Mediant 1000, Mediant 2000 and Mediant 3000.

## I.2.8 Entity Profile – Analog CPE Devices

Table I-8: Acceptance Test – Analog CPE Devices

Step Name	Description	Expected Result
<b>Go to telephony frame</b>	Click on the telephony button	Telephony configuration is displayed.
<b>Save profile</b>	Save the profile, choose an appropriate name 	The new profile is displayed in the profiles list. 
<b>Expose profile parameters</b>	Press on the “show profile parameters” button 	All profiles parameters are marked with the profile name. 
<b>Detach profile</b>	Change one of the profile parameters and press <b>Apply</b> .	A detach profile pop up message is displayed. 



**Note:** Analog CPE devices include the following products: MediaPack; Mediant 600; Mediant 800 MSBG; Mediant 1000 MSBG; Mediant 800 E-SBC; Mediant 1000 E-SBC and Mediant 1000.



**Note:** Analog CPE devices include the following products: MediaPack; Mediant 600; Mediant 800 MSBG; Mediant 800 Gateway and E-SBC, Mediant 850 MSBG, Mediant 1000 MSBG; Mediant 1000 Gateway and E-SBC and Mediant 1000.

## I.3 Faults

### I.3.1 Alarm Receiver

Figure I-1: Alarm Receiver



Table 1-9: Acceptance Test – Alarm Receiver

Step Name	Description	Expected Result
<b>Raise Alarm</b>	Lock one of the elements in the MG, such as the trunk.	The alarm is received in the EMS.
<b>Clear Alarm</b>	Unlock one of the elements in the Media Gateway, such as a trunk.	The clear alarm is received in the EMS.

### I.3.2 Delete Alarms

Table I-10: Acceptance Test – Delete Alarms

Step Name	Description	Expected Result
<b>Delete Alarms</b>	Right-click the alarms in the alarm browser and delete all the alarms	The alarm browser is empty.

### I.3.3 Acknowledge Alarm

Table I-11: Acceptance Test – Acknowledge Alarm

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



### I.3.4 Forwarding Alarms

Figure I-2: Destination Rule Configuration

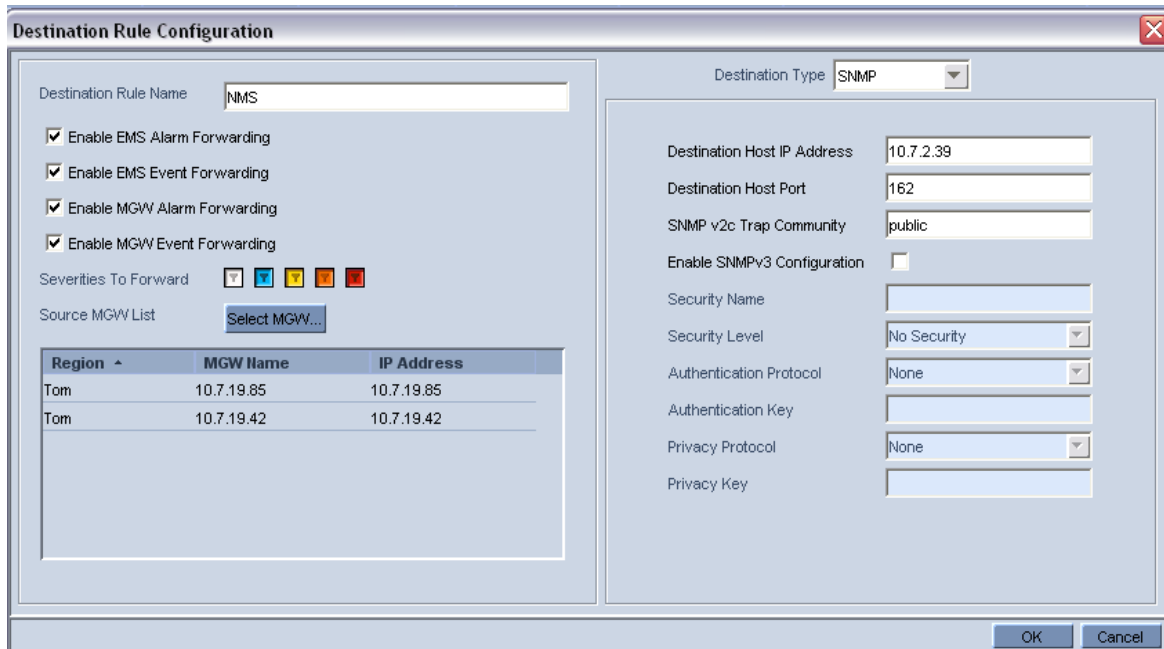


Table I-12: Acceptance Test – Forwarding Alarms

Step Name	Description	Expected Result
IP	Enable the Alarm Forwarding feature Tools >> trap configuration Add rule	Verify that you receive the Traps in the requested IP address on port 162.
Port	Change the Port number	Verify that you receive the Traps in the requested IP address on the new port.

## I.4 Security

This section describes the EMS application security tests.

### I.4.1 Users List

Figure I-3: Users List



User Name	Security Level	Full Name ^	Status	Valid IPs To Login From
demo	Monitoring		SUSPENDED	10.7.2.33
acladmin	Administration	Admin user	ACTIVE	
keith	Administration	Keith Brown	NOT ACTIVE	

Table I-13: Acceptance Test – Add an Operator

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

### I.4.2 Non Repetitive Passwords

Table I-14: Acceptance Test – Non Repetitive Passwords

Step Name	Description	Expected Result
<b>Change password</b>	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."

### I.4.3 Removing Operator

Table I-15: Acceptance Test – Removing Operator

Step Name	Description	Expected Result
<b>Remove</b>	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.
<b>Verify</b>	Select the <b>OK</b> button.	Verify that the user you selected was removed from the operators table.

## I.4.4 Journal Activity

Figure I-4: Actions Journal

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator
Journal	16:35:13 Dec 15 2009...	10.77.10.130	10.77.10.130	Configuration: Update	Action UnLock was performed	Mor	mor
Journal	16:35:07 Dec 15 2009...	10.77.10.130	10.77.10.130	Configuration: Update	Action Lock was performed	Mor	mor
Journal	16:35:06 Dec 15 2009...	10.77.10.130	10.77.10.130	Configuration: Update	Update Parameters: Field-tgMGInfoActio...	Mor	mor

Table I-16: Acceptance Test – Journal Activity

Step Name	Description	Expected Result
<b>Activity</b>	Open the action journal.	Check that all actions that you performed until now are registered.
<b>Filter</b>	Use the filter: time, user and action.	Time, user, action filter are working OK.

## I.5 Utilities

This section describes the EMS application utilities acceptance tests.


### I.5.1 Configuration Parameter Search

#### I.5.1.1 Basic Search

**Figure I-5: Configuration Parameter Search drop-down list box**




**Table I-17: Acceptance Test – Configuration Parameter: Basic Search**

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

### I.5.1.2 Advanced MG Search

Figure I-6: Configuration Parameter: Advanced Search

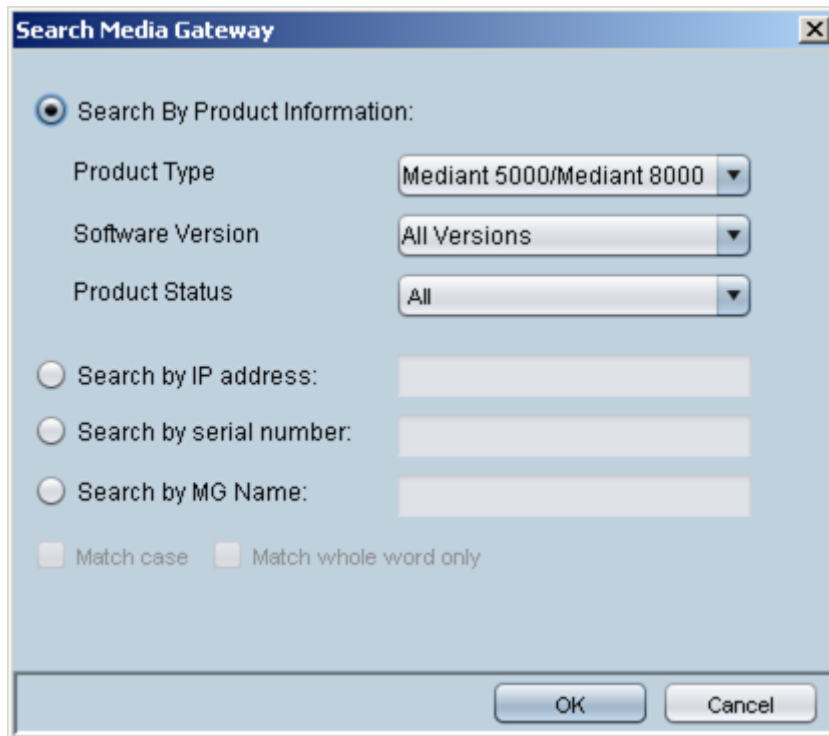
Table I-18: Acceptance Test – Configuration Parameter: Advanced Search

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

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

## I.5.2 MG Search

**Figure I-7: Media Gateway Search**



**Table I-19: Acceptance Test – MG Search**

Step Name	Description	Expected Result
<b>Search Box</b>	Open the MG search dialog by choosing Tools >> Search MG in the EMS Main menu.	Search MG tool opens.
<b>IP</b>	Search /MG/Unknown machine by IP address.	Displays a dialog with a list of results according to selected criteria.
<b>Serial Number</b>	Search /MG/Unknown machine by serial number.	Displays a dialog with a list of results according to selected criteria.
<b>MG Name</b>	Search /MG/Unknown machine by MG Name.	Displays a dialog with a list of results according to selected criteria.
<b>Additional Search Options</b>	Search /MG/Unknown machine by matching case or by matching a whole word.	Displays a dialog with a list of results according to selected criteria.

### I.5.3 Online Help

**Table I-20: Acceptance Test – Online Help**

Step Name	Description	Expected Result
<b>Alarms</b>	Select one alarm and verify that the help opens in the correct context in the online help	Relevant information, clear and user friendly.
<b>Status</b>	Stand on one MG status screen and open the online help	Relevant information, clear and user friendly.
<b>Provisioning</b>	Stand on one tab in the provisioning windows and open the online help	Relevant information, clear and user friendly.

### I.5.4 Backup and Recovery

**Table I-21: Acceptance Test – Backup and Recovery**

Step Name	Description	Expected Result
<b>Backup</b>	Create backup file in the EMS server according to the EMS Installation & Maintenance manual	A backup will be created in the same folder.
<b>Recovery</b>	Perform recovery on the new machine according to the EMS Installation & Maintenance manual	The new server is identical to the previous server.

# **Installation, Operation and Maintenance Manual**

## **Element Management System (EMS) Server**

**Version 6.6**



[www.audiocodes.com](http://www.audiocodes.com)