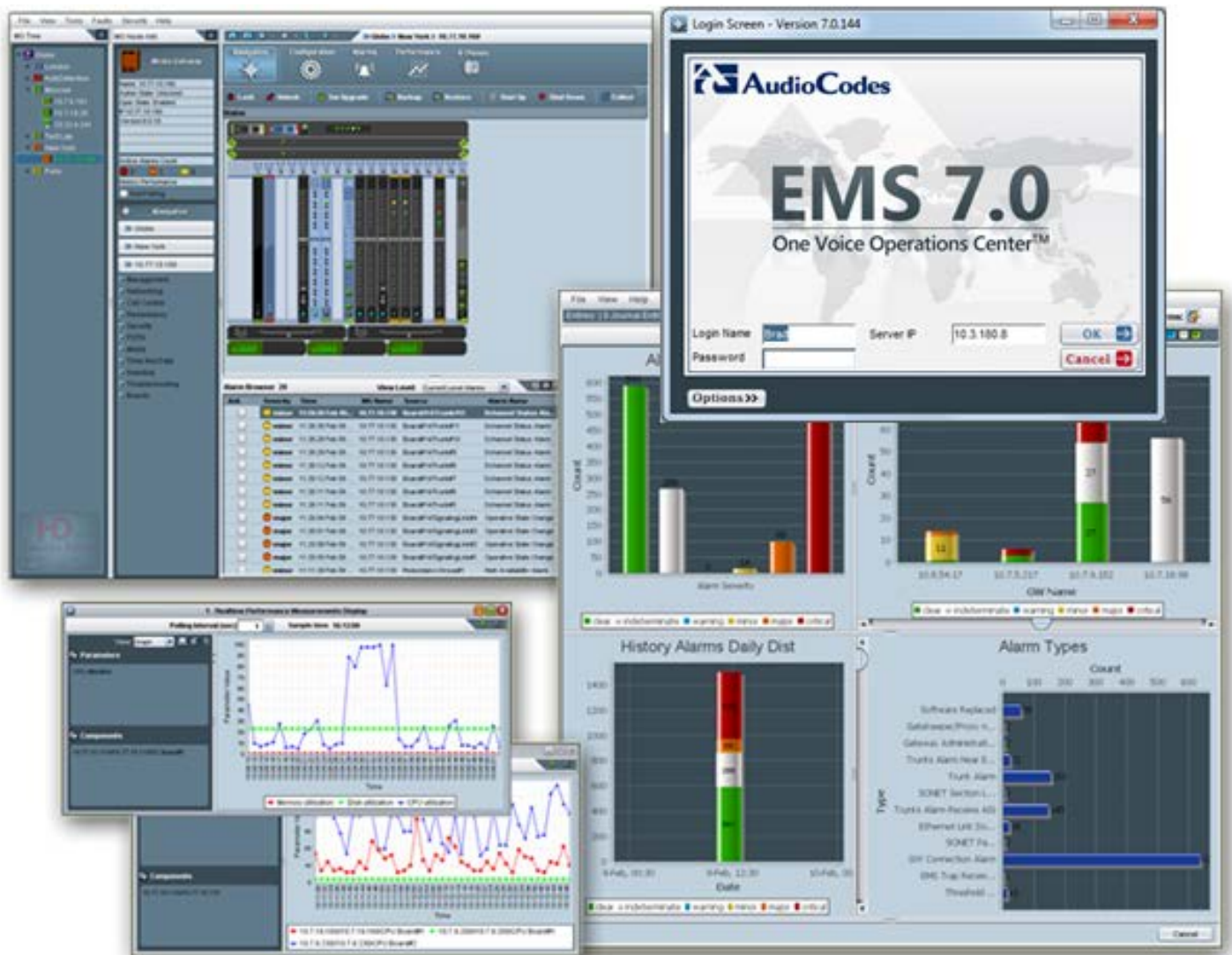


# AudioCodes One Voice Operations Center

EMS, SEM and IP Phones Management

## Installation, Operation and Maintenance Manual

Version 7.0





---

## Table of Contents

---

<b>1</b>	<b>Overview .....</b>	<b>17</b>
<hr/>		
	<b>Pre-installation Information .....</b>	<b>19</b>
<b>2</b>	<b>Managed VoIP Equipment .....</b>	<b>21</b>
<b>3</b>	<b>Hardware and Software Specifications .....</b>	<b>23</b>
<b>3.1</b>	<b>EMS Server and Client Requirements .....</b>	<b>23</b>
<b>3.2</b>	<b>Bandwidth Requirements .....</b>	<b>24</b>
3.2.1	EMS Bandwidth Requirements .....	24
3.2.2	SEM Bandwidth Requirements .....	24
<b>3.3</b>	<b>Performance and Data Storage .....</b>	<b>26</b>
<b>3.4</b>	<b>Microsoft Lync Monitoring SQL Server Prerequisites .....</b>	<b>27</b>
<b>4</b>	<b>EMS Software Deliverables .....</b>	<b>29</b>
<b>4.1</b>	<b>Dedicated Hardware Installation – DVDs 1-4.....</b>	<b>29</b>
<b>4.2</b>	<b>VMware – DVD 5 .....</b>	<b>30</b>
<b>4.3</b>	<b>Hyper-V – DVD 5 .....</b>	<b>30</b>
<hr/>		
	<b>EMS Server Installation.....</b>	<b>31</b>
<b>5</b>	<b>Testing Installation Requirements -Dedicated Hardware .....</b>	<b>33</b>
<b>5.1</b>	<b>Hardware Requirements .....</b>	<b>33</b>
5.1.1	Testing Hardware Requirements on the Linux Platform.....	33
<b>6</b>	<b>Installing the EMS Server on Dedicated Hardware.....</b>	<b>35</b>
<b>6.1</b>	<b>ISO Files Verification.....</b>	<b>35</b>
6.1.1	Windows .....	35
6.1.2	Linux .....	36
<b>6.2</b>	<b>Installing the EMS Server on the Linux Platform.....</b>	<b>37</b>
6.2.1	DVD1: Linux CentOS 5.9.....	37
6.2.2	DVD2: Oracle DB Installation .....	40
6.2.3	DVD3: EMS Server Application Installation .....	42
<b>6.3</b>	<b>EMS Server Users.....</b>	<b>45</b>
<b>7</b>	<b>Installing the EMS on Virtual Server Platform .....</b>	<b>47</b>
<b>7.1</b>	<b>Installing the EMS Server on the VMware Platform.....</b>	<b>47</b>
7.1.1	Configuring EMS Virtual Machines (VMs) in a VMware Cluster .....	56
7.1.1.1	Site Requirements .....	56
7.1.1.2	Cluster Host Node Failure .....	61
<b>7.2</b>	<b>Installing the EMS Server on Microsoft Hyper-V Platform.....</b>	<b>61</b>
7.2.1	Installing the Virtual Machine.....	62
7.2.2	Configuring the Virtual Machine to run the EMS server .....	66
7.2.3	Changing MAC Addresses from 'Dynamic' to 'Static' .....	68
7.2.4	Hard Drive Location.....	69
7.2.5	Expanding Disk Capacity.....	69

7.2.6	Assigning EMS Server IP Address to Network .....	73
7.2.7	Configuring EMS Virtual Machines in a Microsoft Hyper-V Cluster .....	74
7.2.7.1	Site Requirements .....	74
7.2.7.2	Add the EMS VM in Failover Cluster Manager .....	75
7.2.7.3	Cluster Node Failure .....	78

## **EMS Server Upgrade .....79**

<b>8</b>	<b>Upgrading the EMS Server on Dedicated Hardware .....</b>	<b>81</b>
8.1	Upgrading the EMS Server-DVD.....	81
8.2	Upgrading the EMS Server-ISO File .....	84
<b>9</b>	<b>Upgrading the EMS Server on the VMware Platform .....</b>	<b>85</b>

## **EMS Server Machine Backup and Restore.....87**

<b>10</b>	<b>EMS Server Backup .....</b>	<b>89</b>
<b>11</b>	<b>EMS Server Restore .....</b>	<b>91</b>

## **EMS Server Machine Maintenance.....95**

<b>12</b>	<b>EMS Server Manager.....</b>	<b>97</b>
12.1	Getting Started with EMS Server Manager .....	97
12.1.1	Connecting to the EMS Server Manager .....	97
12.1.2	Using the EMS Server Manager .....	100
12.2	Status .....	100
12.3	General Information .....	101
12.4	Collect Logs .....	103
12.5	Application Maintenance .....	105
12.5.1	Start /Stop the Application .....	106
12.5.2	Web Servers .....	107
12.5.2.1	JAWS IP Configuration .....	108
12.5.3	Change Schedule Backup Time .....	108
12.5.4	Restore .....	108
12.5.5	License.....	109
12.5.6	Shutdown the EMS Server Machine .....	110
12.5.7	Reboot the EMS Server Machine .....	110
12.6	Network Configuration .....	111
12.6.1	Server IP Address .....	112
12.6.2	Ethernet Interfaces .....	113
12.6.2.1	EMS Client Login on all EMS Server Network Interfaces.....	113
12.6.2.2	Add Interface .....	115
12.6.2.3	Remove Interface .....	116
12.6.2.4	Modify Interface .....	116
12.6.3	Ethernet Redundancy.....	117
12.6.3.1	Add Redundant Interface.....	118
12.6.3.2	Remove Ethernet Redundancy .....	120
12.6.3.3	Modify Redundant Interface.....	121
12.6.4	DNS Client .....	122



12.6.5	NAT .....	123
12.6.6	Static Routes .....	124
12.6.7	SNMP Agent .....	125
12.6.8	Server SNMPv3 Engine ID .....	125
<b>12.7</b>	<b>Date and Time Settings .....</b>	<b>126</b>
12.7.1	NTP .....	127
12.7.1.1	Stopping and Starting the NTP Server .....	128
12.7.1.2	Restrict Access to NTP Clients .....	128
12.7.2	Time Zone Settings .....	129
12.7.3	Date and Time .....	129
<b>12.8</b>	<b>Security .....</b>	<b>130</b>
12.8.1	Add EMS User .....	131
12.8.2	SSH Server Configuration Manager .....	132
12.8.2.1	SSH Log Level .....	133
12.8.2.2	SSH Banner .....	134
12.8.2.3	SSH on Ethernet Interfaces .....	135
12.8.2.4	Enable/Disable SSH Password Authentication .....	138
12.8.2.5	Enable SSH IgnoreUserKnownHosts Parameter .....	139
12.8.2.6	SSH Allowed Hosts .....	140
12.8.3	DB Password .....	145
12.8.4	OS Passwords Settings .....	145
12.8.4.1	General Password Settings .....	146
12.8.4.2	Operating System Users Security Extensions .....	147
12.8.5	Start / Stop File Integrity Checker .....	149
12.8.6	Start/Stop Software Integrity Checker (AIDE) and Pre-linking .....	149
12.8.7	USB Storage .....	150
12.8.8	Network Options .....	151
12.8.9	Auditd Options .....	151
12.8.10	Enable SEM Client Secured Connection .....	152
12.8.11	Enable EMS4IPPhones Client and JAWS Secured Communication .....	152
<b>12.9</b>	<b>Diagnostics .....</b>	<b>153</b>
12.9.1	Syslog Configuration .....	153
12.9.2	Board Syslog Logging Configuration .....	155
12.9.3	TP Debug Recording Configuration .....	156
<b>HA (High Availability) .....</b>		<b>157</b>
<b>13</b>	<b>Getting Started with HA (High Availability) .....</b>	<b>159</b>
13.1	EMS HA Pre-requisites .....	160
13.2	EMS HA Data Synchronization .....	161
13.2.1	Replicate EMS Server Manager Actions .....	161
13.3	EMS Server Manager .....	161
13.4	EMS Client .....	162
13.5	EMS Server Upgrade .....	162
13.6	EMS Server Restore .....	162
<b>14</b>	<b>EMS HA Configuration .....</b>	<b>163</b>
14.1	Primary Server HA Installation in Global IP Model .....	164
14.2	Primary Server HA Installation in Geo HA Model .....	166
14.2.1	Ping Nodes .....	168

14.3	Secondary Server HA Installation .....	169
14.4	HA Status .....	170
14.4.1	Advanced Status View.....	172
14.5	EMS Server Manual Switchover .....	173
14.6	EMS HA Uninstall .....	174
<b>Configuring the Firewall and Installing the EMS Client .....</b>		<b>177</b>
15	Configuring the Firewall .....	179
16	Installing the EMS Client .....	185
16.1	Running the EMS Client on a PC or Laptop .....	188
16.2	Initial Login .....	188
16.3	Installing and Running the EMS Client on a PC using Java Web Start (JAWS) .....	189
<b>Appendices .....</b>		<b>191</b>
A	Frequently Asked Questions (FAQs).....	193
A.1	After installing JAWS - the EMS application icon is not displayed on the desktop .....	193
A.2	After Rebooting the Machine.....	194
A.3	Changes Not Updated in the Client.....	194
A.4	Removing the EMS Server Installation .....	194
B	Site Preparation.....	195
C	Daylight Saving Time (DST) .....	197
D	EMS Application Acceptance Tests.....	199
D.1	Introduction.....	199
D.2	Configuration .....	199
D.2.1	Client Installation .....	199
D.2.2	Server Installation.....	200
D.2.3	Add Auxiliary File.....	200
D.2.4	Add Media Gateway .....	200
D.2.5	Provisioning – Mediant 5000/ Mediant 8000 .....	201
D.2.6	Provisioning – CPE Devices .....	201
D.2.7	Entity Profile – Digital CPE Devices.....	202
D.2.8	Entity Profile – Analog CPE Devices .....	203
D.3	Faults.....	204
D.3.1	Alarm Receiver.....	204
D.3.2	Delete Alarms.....	204
D.3.3	Acknowledge Alarm.....	204
D.3.4	Forwarding Alarms .....	205
D.4	Security .....	206
D.4.1	Users List.....	206
D.4.2	Non Repetitive Passwords .....	206
D.4.3	Removing Operator .....	206

D.4.4	Journal Activity .....	207
<b>D.5</b>	<b>Utilities .....</b>	<b>208</b>
D.5.1	Configuration Parameter Search .....	208
D.5.1.1	Basic Search.....	208
D.5.1.2	Advanced MG Search.....	209
D.5.2	MG Search.....	210
D.5.3	Online Help .....	211
D.5.4	Backup and Recovery .....	211
<b>E</b>	<b>Configuring RAID-0 for AudioCodes EMS on HP ProLiant DL360p Gen8 Servers .....</b>	<b>213</b>
<b>E.1</b>	<b>Prerequisites .....</b>	<b>213</b>
<b>E.2</b>	<b>Hardware Preparation .....</b>	<b>213</b>
<b>E.3</b>	<b>Configuring RAID-0 .....</b>	<b>214</b>
<b>F</b>	<b>Managing Clusters .....</b>	<b>221</b>
<b>F.1</b>	<b>Migrating EMS Virtual Machines in a VMware Cluster .....</b>	<b>221</b>
<b>F.2</b>	<b>Moving EMS VMs in a Hyper-V Cluster.....</b>	<b>224</b>
<b>G</b>	<b>Installing X.509 User-Defined Certificates .....</b>	<b>227</b>
<b>G.1</b>	<b>Installing User-Defined Certificates on EMS Server .....</b>	<b>229</b>
G.1.1	Step 1: Generate a new Private Key for EMS Server .....	229
G.1.2	Step 2: Generate a Certificate Signing Request (CSR) for EMS Server.....	229
G.1.3	Step 3: Receive the New Certificates from the CA.....	231
G.1.4	Step 4: Transfer the New Certificates to the EMS Server .....	231
G.1.5	Step 5: Update Apache Configuration .....	232
G.1.6	Step 6: Updating Apache Certificates .....	232
G.1.7	Step 7: Restart Apache .....	233
<b>G.2</b>	<b>Installing User-Defined Certificates on EMS Client .....</b>	<b>233</b>
G.2.1	Step 1: Generate a new Private Key for EMS Client.....	233
G.2.2	Step 2: Generate a Certificate Signing Request (CSR) for EMS Client.....	234
G.2.3	Step 3: Receive the New Certificates from the CA.....	235
G.2.4	Step 4: Transfer the New Certificates to the EMS Server .....	235
G.2.5	Step 5: Generate the Client Keystore .....	236
G.2.6	Step 6: Transfer Client Keystore File to PC .....	237
G.2.7	Step 7: Stop EMS Client Application.....	237
G.2.8	Step 8: Update EMS Client Configuration.....	238
G.2.9	Step 9: Update Java Web Start Client Certificate .....	239
G.2.9.1	Connecting to JAWS for Advanced Versions .....	241
<b>G.3</b>	<b>Installing User-Defined Certificates on SEM Server .....</b>	<b>245</b>
G.3.1	Step 1: Generate Keystore for SEM Server .....	245
G.3.2	Step 2: Update SEM Server Configuration .....	246
G.3.3	Step 3: Update Tomcat Server Configuration .....	247
G.3.4	Step 4: Redirecting SEM Client Browser to HTTPS URL.....	248
G.3.5	Step 5: Setting Web Browser HTTPS Compatibility.....	248
<b>G.4</b>	<b>Installing User-Defined Certificates on AudioCodes Devices .....</b>	<b>251</b>
G.4.1	Enterprise Gateways and SBC Devices .....	251
G.4.1.1	Step 1: Generate a Certificate Signing Request (CSR) .....	251
G.4.1.2	Step 2: Receive the New Certificates from the CA.....	252
G.4.1.3	Step 3: Update Device with New Certificate.....	253
G.4.1.4	Step 4: Update Device's Trusted Certificate Store .....	254

G.4.1.5	Step 5: Configure HTTPS Parameters on the Device .....	255
G.4.1.6	Step 6: Reset Device to Apply the New Configuration .....	256
G.4.2	MP-1xx Devices .....	257
G.4.2.1	Step 1: Generate a Certificate Signing Request (CSR) .....	257
G.4.2.2	Step 2: Receive the New Certificates from the CA.....	258
G.4.2.3	Step 3: Update Device with New Certificate.....	258
G.4.2.4	Step 4: Update Device's Trusted Certificate Store .....	259
G.4.2.5	Step 5: Configure HTTPS Parameters on Device .....	261
G.4.2.6	Step 6: Reset Device to Apply the New Configuration .....	261
G.5	Cleanup .....	262
H	Transferring Files .....	263
I	Verifying and Converting Certificates .....	265

---

## List of Figures

---

Figure 5-1: Linux Testing Requirements .....	34
Figure 6-1: ISO File Integrity Verification .....	36
Figure 6-2: Linux CentOS Installation .....	37
Figure 6-3: CentOS 5 .....	38
Figure 6-4: Linux CentOS Installation Complete .....	38
Figure 6-5: Linux CentOS Network Configuration .....	39
Figure 6-6: Oracle DB Installation (Linux) .....	40
Figure 6-7: Oracle DB Installation - License Agreement (Linux) .....	41
Figure 6-8: Oracle DB Installation (Linux) (cont) .....	41
Figure 6-9: Oracle DB Installation (Linux) (cont) .....	41
Figure 6-10: EMS Server Application Installation (Linux) .....	42
Figure 6-11: EMS Server Application Installation (Linux) – License Agreement .....	43
Figure 6-12: EMS Server Application Installation (Linux) (cont) .....	43
Figure 6-13: EMS Server Application Installation (Linux) - Java Installation .....	44
Figure 7-1: Deploy OVF Template Option .....	47
Figure 7-2: Open OVA Package .....	48
Figure 7-3: OVF Template Source Screen .....	49
Figure 7-4: OVF Template Details Screen .....	50
Figure 7-5: Virtual Machine Name and Location Screen .....	51
Figure 7-6: Host / Cluster Screen .....	51
Figure 7-7: Destination Storage Screen .....	52
Figure 7-8: Disk Format Screen .....	52
Figure 7-9: Ready to Complete Screen .....	53
Figure 7-10: Deployment Progress Screen .....	53
Figure 7-11: Edit Settings option .....	54
Figure 7-12: Hard Disk Settings .....	54
Figure 7-13: Recent Tasks .....	55
Figure 7-14: Power On .....	55
Figure 7-15: Storage Adapters .....	56
Figure 7-16: Turn On vSphere HA .....	57
Figure 7-17: Activate HA on each Cluster Node .....	57
Figure 7-18: Networking .....	58
Figure 7-19: Switch Properties .....	59
Figure 7-20: Protected VM .....	60
Figure 7-21: Installing the EMS server on Hyper-V – Hyper-V Manager .....	62
Figure 7-22: Installing EMS server on Hyper-V – Import Virtual Machine Wizard .....	63
Figure 7-23: Installing EMS server on Hyper-V – Locate Folder .....	63
Figure 7-24: Installing EMS server on Hyper-V – Choose Import Type .....	64
Figure 7-25: Installing EMS server on Hyper-V – Choose Destination .....	64
Figure 7-26: Installing EMS server on Hyper-V – Choose Storage Folders .....	65
Figure 7-27: File Copy Progress Bar .....	65
Figure 7-28: Adjusting VM for EMS server – Settings - Memory .....	66
Figure 7-29: Adjusting VM for EMS server - Settings - Processor .....	67
Figure 7-30: Advanced Features - Network Adapter – Static MAC Address .....	68

Figure 7-31: Expanding Disk Capacity .....	69
Figure 7-32: Edit Virtual Hard Disk Wizard.....	70
Figure 7-33: Edit Virtual Hard Disk Wizard-Choose Action.....	70
Figure 7-34: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk.....	71
Figure 7-35: Edit Virtual Hard Disk Wizard-Completion .....	72
Figure 7-36: Power On Virtual Machine .....	73
Figure 7-37: Choose Virtual Machine.....	76
Figure 7-38: Virtual Machine Successfully Added.....	77
Figure 8-1: EMS Server Upgrade (Linux).....	82
Figure 8-2: EMS Server Upgrade (Linux) – License Agreement.....	82
Figure 8-3: EMS Server Application Upgrade (Linux) - Java Installation.....	83
Figure 8-4: EMS Server Upgrade (Linux) Complete .....	83
Figure 8-5: EMS Server Upgrade (Linux).....	84
Figure 9-1: Edit Settings Option .....	85
Figure 9-2: Hardware Tab .....	85
Figure 9-3: Connect/disconnect Button .....	86
Figure 9-4: EMS Server Installation Script .....	86
Figure 12-1: EMS Server Manager Menu .....	98
Figure 12-2: Application Status .....	100
Figure 12-3: General Information .....	101
Figure 12-4: General Information .....	102
Figure 12-5: EMS Server Manager – Collect Logs .....	103
Figure 12-6: TAR File Location.....	104
Figure 12-7: Application Maintenance.....	105
Figure 12-8: Start or Stop the EMS Server .....	106
Figure 12-9: – Web Servers .....	107
Figure 12-10: JAWS IP Configuration .....	108
Figure 12-11: License Configuration Manager.....	109
Figure 12-12: Network Configuration .....	111
Figure 12-13: EMS Server Manager – Change Server's IP Address.....	112
Figure 12-14: IP Configuration Complete.....	112
Figure 12-15: EMS Server: Triple Ethernet Interfaces .....	113
Figure 12-16: EMS Server Manager – Configure Ethernet Interfaces .....	114
Figure 12-17: Physical Ethernet Interfaces Redundancy.....	117
Figure 12-18: Ethernet Redundancy Configuration.....	118
Figure 12-19: Add Redundant Interface (Linux).....	119
Figure 12-20: Ethernet Redundancy Interface to Disable .....	120
Figure 12-21: Modify Redundant Interface (Linux).....	121
Figure 12-22: DNS Setup .....	122
Figure 12-23: Routing Table and Menu.....	124
Figure 12-24: EMS Server Manager – Configure SNMPv3 Engine ID .....	125
Figure 12-25: SNMPv3 Engine ID Configuration – Complete Configuration .....	126
Figure 12-26: EMS Server Manager - Change System Time & Date .....	126
Figure 12-27: EMS Server Manager - Configure NTP .....	127
Figure 12-28: Change System Time and Date Prompt.....	129
Figure 12-29: Security Settings .....	130

Figure 12-30: SSH Configuration .....	132
Figure 12-31: SSH Log Level Manager .....	133
Figure 12-32: SSH Banner Manager .....	134
Figure 12-33: Configure SSH on Ethernet Interfaces .....	135
Figure 12-34: Disable Password Authentication .....	138
Figure 12-35: SSH IgnoreUserKnowHosts Parameter - Confirm .....	139
Figure 12-36: Configure SSH Allowed Hosts .....	140
Figure 12-37: Add Host/Subnet to Allowed Hosts .....	142
Figure 12-38: Add Host/Subnet to Allowed Hosts-Configured Host .....	143
Figure 12-39: EMS Server Manager – Change DB Password .....	145
Figure 12-40: OS Passwords Settings with Security Extensions .....	148
Figure 12-41: Maximum Active SSH Sessions.....	148
Figure 12-42: Software Integrity Checker (AIDE) and Pre-linking.....	149
Figure 12-43: USB Storage .....	150
Figure 12-44: Network Options.....	151
Figure 12-45: Auditd Options.....	151
Figure 12-46: Diagnostics.....	153
Figure 12-47: Syslog Configuration.....	154
Figure 12-48: Forward Messages to an External Server .....	154
Figure 14-1: EMS Server Manager - HA Configuration.....	163
Figure 14-2: Primary HA Server Menu .....	164
Figure 14-3: Primary HA Server Sub-menu .....	164
Figure 14-4: HA Configuration Display .....	165
Figure 14-5: HA Server Configured as Primary Server - Confirmation .....	165
Figure 14-6: Primary HA Server Menu .....	166
Figure 14-7: Primary HA Server Sub-menu .....	166
Figure 14-8: HA Configuration Display .....	167
Figure 14-9: HA Server Configured as Primary Server - Confirmation .....	167
Figure 14-10: Primary HA Server IP.....	169
Figure 14-11: Secondary HA Server Configuration.....	169
Figure 14-12: EMS HA Status .....	170
Figure 14-13: EMS HA Status - Example Display .....	170
Figure 14-14: Advanced Status View .....	172
Figure 14-15: Manual Switchover.....	173
Figure 14-16: Switchover Status .....	173
Figure 14-17: Status after Switchover .....	174
Figure 14-18: Uninstall EMS HA Status Display .....	175
Figure 15-1: Firewall Configuration Schema .....	182
Figure 16-1: EMS Client Installation-Run as Administrator.....	185
Figure 16-2: EMS Client Installation File-Windows 8 Properties.....	186
Figure 16-3: EMS Client Installation File-Compatibility Tab.....	187
Figure 16-4: Running EMS Client-Run as Administrator.....	188
Figure A-1: EMS Client Removal .....	193
Figure A-2: Java Control Panel .....	193
Figure B-1: Save MGs Tree Command.....	195
Figure D-1: Alarm Receiver .....	204



Figure D-2: Destination Rule Configuration.....	205
Figure D-3: Users List.....	206
Figure D-4: Actions Journal.....	207
Figure D-5: Configuration Parameter Search drop-down list box .....	208
Figure D-6: Configuration Parameter: Advanced Search.....	209
Figure D-7: Media Gateway Search .....	210
Figure E-1: Hardware Preparation .....	213
Figure E-2: HP Array Configuration Utility (ACU).....	214
Figure E-3: RAID-Latest Firmware Versions .....	215
Figure E-4: Actions Menu .....	215
Figure E-5: Clear Configuration.....	216
Figure E-6: Summary Screen.....	216
Figure E-7: Main Screen.....	217
Figure E-8: Logical Drive .....	217
Figure E-9: Summary Screen.....	218
Figure E-10: Set Bootable Logical Drive/Volume.....	218
Figure E-11: Set Bootable Logical Drive/Volume.....	219
Figure E-12: Exit Application .....	219
Figure E-13: Power Button .....	220
Figure E-14: Reboot Button.....	220
Figure F-1: Migration .....	221
Figure F-2: Change Host.....	222
Figure F-3: Target Host for Migration .....	222
Figure F-4: Migration Process Started .....	223
Figure F-5: Hyper-V Live Migration .....	224
Figure F-6: Move Virtual Machine .....	225
Figure F-7: Hyper-V Migration Process Started .....	226
Figure G-1: User-Defined Certificates .....	228
Figure G-2: Java Keystore.....	237
Figure G-3: Java Control Panel (Version 7.2) .....	242
Figure G-4: Java Control Panel (Version 8.0) .....	243
Figure G-5: Exception Site List.....	244
Figure G-6: Continue to Website.....	248
Figure G-7: Mozilla Firefox Settings .....	249
Figure G-8: Chrome Browser Settings .....	250
Figure G-9: Certificate Signing Request Group .....	252
Figure G-10: Upload Certificate Files from your Computer Group.....	253
Figure G-11: Importing Certificate into Trusted Certificates Store .....	254
Figure G-12: TLS Contexts.....	255
Figure G-13: TLS Contexts: Edit Record.....	256
Figure G-14: Device Reset.....	256
Figure G-15: Certificate Signing Request Group .....	257
Figure G-16: Maintenance Actions Page .....	261

---

## List of Tables

---

Table 3-1: EMS- Minimal Platform Requirements .....	23
Table 3-2: SEM Bandwidth Requirements .....	24
Table 3-3: Performance and Data Storage .....	26
Table 7-1: Virtual Machine Configuration .....	66
Table 15-1: Firewall Configuration Rules .....	179
Table 15-2: OAM&P Flows: NOC ↔ Device/ IP Phone/ SBA/ EMS .....	183
Table 15-3: OAM&P Flows: Device/ IP Phone/ SBA/ EMS ↔ NOC .....	183
Table D-1: Acceptance Test – Client Installation .....	199
Table D-2: Acceptance Test – Server Installation .....	200
Table D-3: Acceptance Test – Add Auxiliary File .....	200
Table D-4: Acceptance Test – Add MG .....	200
Table D-5: Acceptance Test – Provisioning: Mediant 5000/ Mediant 8000 .....	201
Table D-6: Acceptance Test – Provisioning: CPE Devices .....	201
Table D-7: Acceptance Test – Entity Profile: Digital CPE Devices .....	202
Table D-8: Acceptance Test – Analog CPE Devices .....	203
Table D-9: Acceptance Test – Alarm Receiver .....	204
Table D-10: Acceptance Test – Delete Alarms .....	204
Table D-11: Acceptance Test – Acknowledge Alarm .....	204
Table D-12: Acceptance Test – Forwarding Alarms .....	205
Table D-13: Acceptance Test – Add an Operator .....	206
Table D-14: Acceptance Test – Non Repetitive Passwords .....	206
Table D-15: Acceptance Test – Removing Operator .....	206
Table D-16: Acceptance Test – Journal Activity .....	207
Table D-17: Acceptance Test – Configuration Parameter: Basic Search .....	208
Table D-18: Acceptance Test – Configuration Parameter: Advanced Search .....	209
Table D-19: Acceptance Test – MG Search .....	211
Table D-20: Acceptance Test – Online Help .....	211
Table D-21: Acceptance Test – Backup and Recovery .....	211

This page is intentionally left blank.

## Notice

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

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

**© 2015 AudioCodes Inc. All rights reserved**

This document is subject to change without notice.

Date Published: December-30-2015

## Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, OSN, SmartTAP, VMAS, VocaNOM, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX and One Box 365 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).

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

## Related Documentation

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

# 1 Overview

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

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

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

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

This page is intentionally left blank.



# Part I

## Pre-installation Information

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



## 2 Managed VoIP Equipment

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

- Mediant 9000 SBC – versions **7.0**, 6.8
- \*Mediant 8000 Media Gateway – versions 6.6 and 6.2
- \*Mediant 5000 Media Gateway – versions 6.6 and 6.2
- Mediant 4000 SBC – versions **7.0**, 6.8 and 6.6
- **Mediant 4000B SBC** – version **7.0**
- Mediant 2600 E-SBC – versions **7.0**, 6.8 and 6.6
- **Mediant 2600B E-SBC** – version **7.0**
- Mediant SE SBC – versions **7.0** and 6.8
- Mediant SE-H SBC – versions **7.0** and 6.8
- Mediant VE SBC – versions **7.0** and 6.8
- Mediant VE-H SBC – versions **7.0** and 6.8
- Mediant 3000 Media Gateways – versions **7.0**, 6.8 and 6.6
- Mediant 2000 Media Gateways – version 6.6
- \*Mediant 1000 Gateway – version 6.6
- Mediant 1000B Gateway and E-SBC – versions **7.0**, 6.8 and 6.6
- Mediant 1000B MSBR – versions 6.6
- Mediant 800B Gateway and E-SBC – versions **7.0**, 6.8 and 6.6
- Mediant 800B MSBR – versions 6.8 and 6.6
- \*Mediant 600 – version 6.6
- Mediant 500L MSBR and Mediant 500 MSBR – version 6.8
- MP-11x and MP-124 MediaPacks – version 6.6
- \*Mediant 800B SBA, \*Mediant 1000B SBA, and \***Mediant 2600B** SBA devices with SBA version **1.1.12.x** and above and gateway version **6.6**
- IP Phone models 420HD, 430HD and 440HD (for both Lync and Non-Lync environments).



### Notes:

- \* Refers to products that are not supported by the SEM.
- All version 7.0 and 6.8 VoIP equipment work with the SIP control protocol.

This page is intentionally left blank.

## 3 Hardware and Software Specifications

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

### 3.1 EMS Server and Client Requirements

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

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

Resource	EMS/SEM Server			EMS Client
	Dedicated EMS Server - Linux OS	Virtual EMS - Low Profile	Virtual EMS - High Profile	
Hardware	HP ProLiant DL360p Gen8	—	—	Monitor resolution: 1152*864 or higher
Operating System	Linux CentOS 64-bit, kernel version 5.9, Rev7	Linux CentOS 64-bit, kernel version 5.9 Rev7	Linux CentOS 64-bit, kernel version 5.9 Rev7	Windows™ 2000 / XP/ Vista/Windows 7/ Windows 8/Windows 8.1
Virtualization platform	—	VMware: ESXi 4.1 and 5.0		—
		VMware HA cluster: VMware ESXi 5.5		
		Microsoft Hyper-V Windows server 2012R2		
Memory	32 GB RAM	4 GB RAM	32 GB RAM	512 MB RAM
Disk space	Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0	250 GB	1.2 TB	300 MB
Processor	CPU: Intel Xeon E5- 2690 (8 cores 2.9 GHz each)	1 core not less than 2 GHz	6 cores not less than 2 GHz	
DVD-ROM	Local	—	—	—

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


**Notes:**

- The JDK and Oracle database component versions mentioned above are provided as part of the EMS server and EMS client installation images.
- The above browsers are supported to run the following client applications: EMS/devices Single-Sign On, JAWS, NBIF, SEM and IP Phone Manager.

## 3.2 Bandwidth Requirements

This section lists the EMS and SEM bandwidth requirements.

### 3.2.1 EMS Bandwidth Requirements

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

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

### 3.2.2 SEM Bandwidth Requirements

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

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

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

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



### 3.3 Performance and Data Storage

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

**Table 3-3: Performance and Data Storage**

Machine Specifications	HP DL360p G8	VMware/Microsoft HyperVLow	VMware/Microsoft HyperV High
EMS Managed Devices	5000	100	5000
EMS for IP Phones Managed	10000	1000	5000
SEM			
Maximum number of CAPS (calls attempts per second) per device.	160	30	120
Maximum number of CAPS per server (SBC and Microsoft Lync).	300	30	120
Maximum concurrent sessions	30,000	3,000	12,000
Maximum number of devices per region	500	100	300
Maximum number of managed devices.	3,000	100	1,200
Maximum number of links between devices.	6,000	200	2,400
Call Details Storage - Detailed information per Call	Up to two months or 80 million calls.	Up to two months or 6 million rows.	Up to two months or 80 million rows.
Calls Statistics Storage - Statistic information storage.	Up to six months or 150 million intervals.	Up to six months or 12 million rows.	Up to six months or 150 million rows.

## 3.4 Microsoft Lync Monitoring SQL Server Prerequisites

Following are the Microsoft Lync Monitoring SQL Server prerequisites:

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

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

This page is intentionally left blank.

## 4 EMS Software Deliverables

This section describes the EMS software deliverables.

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

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

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

- Linux (CentOS) 5.9 Installation for EMS server, REV7

The following machine is currently supported:

- ◆ HP DL360p G8 - Linux (CentOS) 64-bit kernel version 5.9 Installation for EMS server, Linux CentOS 5.9 REV7.

■ **DVD2:** Oracle Installation: Oracle installation version *11g* DVD for the Linux platform.

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

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

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

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

## **4.2 VMware – DVD 5**

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

- VMware for clean install
- EMS client Install
- Documentation

## **4.3 Hyper-V – DVD 5**

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

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

# Part II

## EMS Server Installation

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





## 5 Testing Installation Requirements - Dedicated Hardware

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

### 5.1 Hardware Requirements

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

To determine the system OS, enter the following command:

```
uname
```

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

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

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

To ensure that your machine meets the minimal hardware requirements for 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 23).

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

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

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

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

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

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



**Note:** Use the AudioCodes' DVD1 to install the Linux Operating System.

## 6 Installing the EMS Server on Dedicated Hardware

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

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

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

### 6.1 ISO Files Verification

If you have received an ISO file from AudioCodes instead of a burned DVD, its contents must be verified using an MD5 checksum. As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications, and is also commonly used to check the integrity of file, and verify download. Perform the following verifications on the relevant platform:

- Windows (see below)
- Linux (see Section 6.1.2).

#### 6.1.1 Windows

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

- Verify the checksum with WinMD5 (see [www.WinMD5.com](http://www.WinMD5.com))

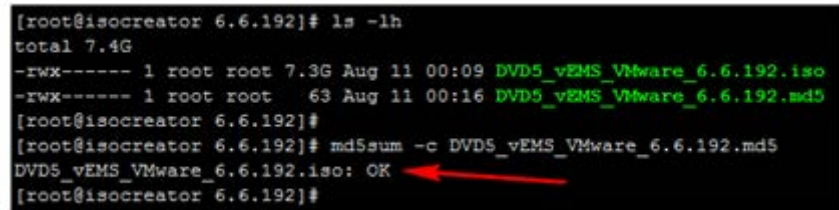
## 6.1.2 Linux

Copy the checksum and the ISO files to a Linux machine, and then run the following command:

```
md5sum -c filename.md5
```

The “OK” result should be displayed on the screen (see figure below).

**Figure 6-1: ISO File Integrity Verification**



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

## 6.2 Installing the EMS Server on the Linux Platform

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

### 6.2.1 DVD1: Linux CentOS 5.9

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



**Note:** If you are installing the EMS server on an HP ProLiant DL360p Gen8 server, before commencing this procedure, you must configure RAID-0 (see Appendix E on page 213).

➤ **To perform DVD1 installation:**

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

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

**Figure 6-2: Linux CentOS Installation**

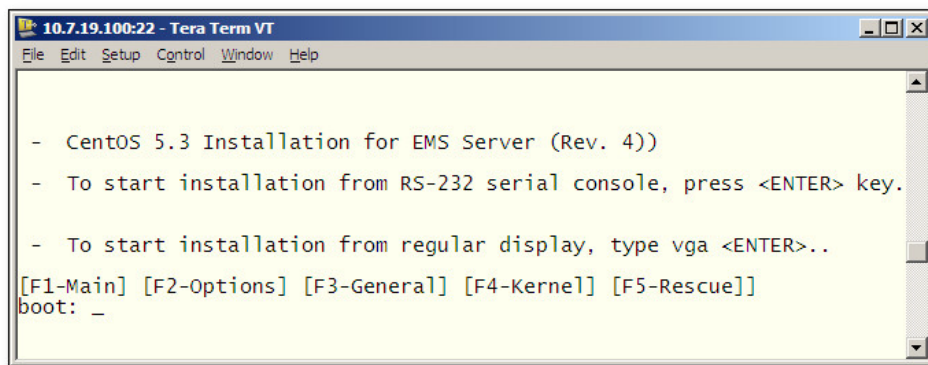
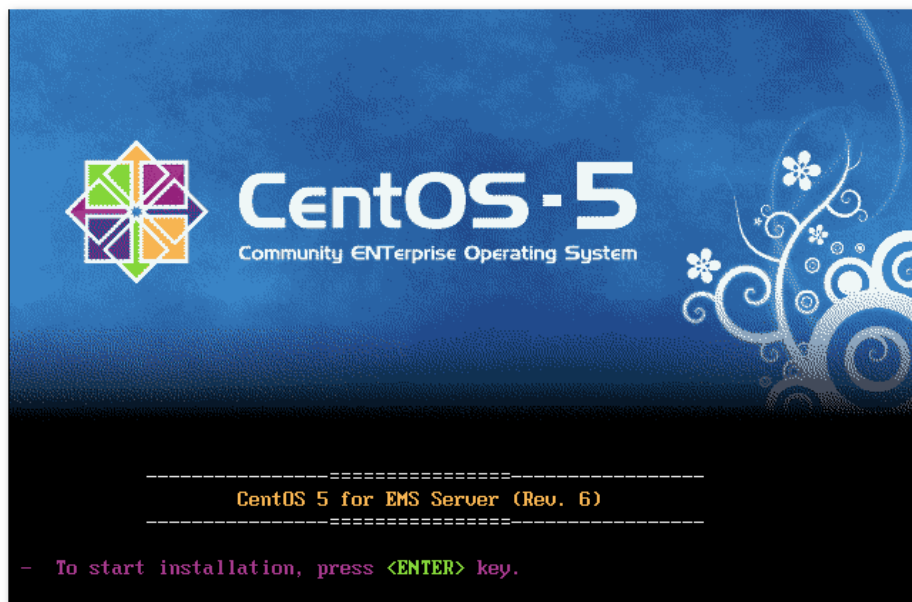


Figure 6-3: CentOS 5

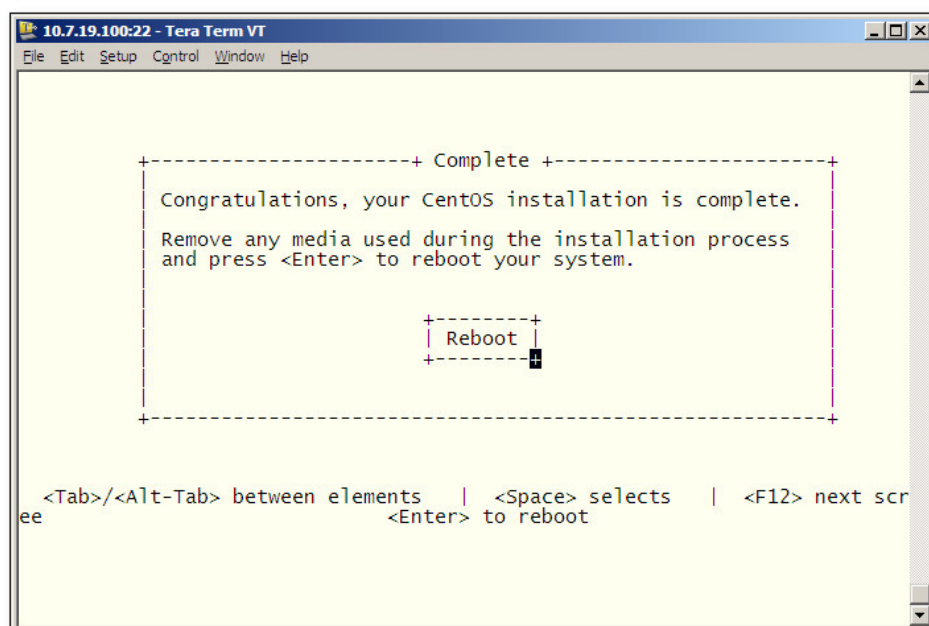


6. Wait for the installation to complete.
7. Reboot your machine by pressing Enter.



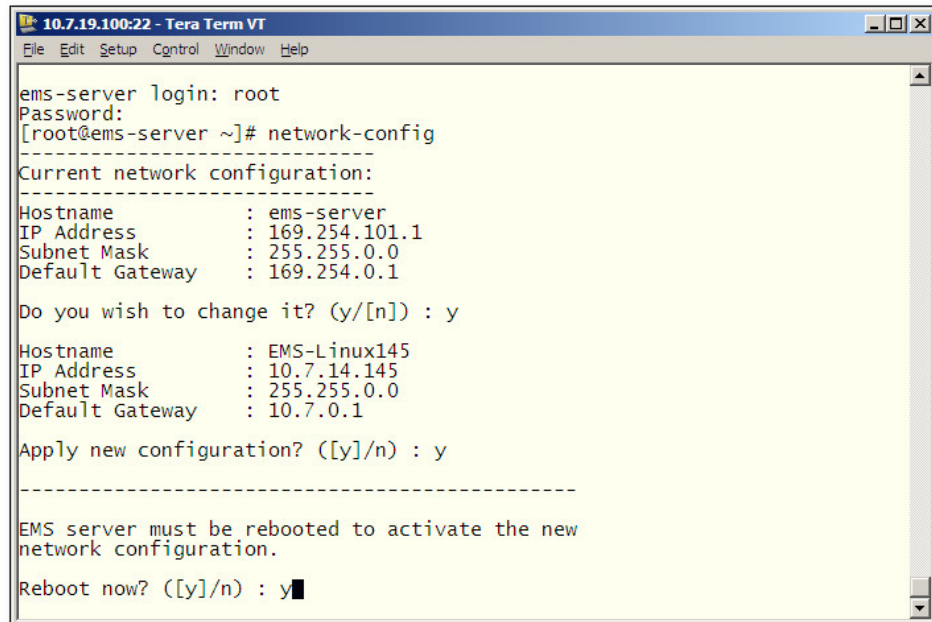
**Note:** Do not forget to remove the Linux installation DVD from the DVD-ROM before rebooting your machine.

Figure 6-4: Linux CentOS Installation Complete



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

**Figure 6-5: Linux CentOS Network Configuration**



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

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

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

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

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

-----

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

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

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

## 6.2.2 DVD2: Oracle DB Installation

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



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

### ➤ To perform DVD2 installation:

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

```
su - root
```

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

```
mount /misc/cd
```

5. Run the installation script from its location:

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

Figure 6-6: Oracle DB Installation (Linux)

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

Login Check Successfully Passed.

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

...
SOFTWARE EVALUATION LICENSE AGREEMENT

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

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



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

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

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

7. Type the 'SYS' user password, type **sys** and then press Enter.

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

```
SQL> Connected to an idle instance.
SQL> ORACLE instance started.

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

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

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

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

### Figure 6-9: Oracle DB Installation (Linux) (cont)

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

## 6.2.3 DVD3: EMS Server Application Installation

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

### ➤ To perform DVD3 installation:

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

```
su - root
```

4. Run the installation script from its location:

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

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

```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/  
[root@EMS-Linux2 EmsServerInstall]# ./install  
DIR Name /misc/cd/EmsServerInstall  
Start installValues  
  >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...  
Login Check Successfully Passed.  
  
  >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
  >>> >>> PASSED  
  ...  
  >>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013  
  
  ...  
SOFTWARE LICENSE AGREEMENT  
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I  
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (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 AC  
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

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

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

```

based upon the net income of Licensors.
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 Licensors and any attempt to do so shall be without effe
ffered 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 Licensors and Licensee.

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

```

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

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

```

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

Hardening Linux OS for DoD STIG compliancy

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

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

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

Press Enter to reboot...

```

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

Figure 6-13: EMS Server Application Installation (Linux) - Java Installation

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

Press Enter to continue.....
█
```

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

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

10. When the EMS server has successfully restarted, login as 'acems' user, switch to 'root' user and verify that the Date and Time are set correctly (see Section 12.7 on page 126 to set the date and time).
11. Verify that the EMS server is up and running (see Section 12.5 on page 105) and login by client to verify a successful installation.

## 6.3 EMS Server Users

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

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

This page is intentionally left blank.

## 7 Installing the EMS on Virtual Server Platform

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

- Installing the EMS server on the VMware platform (see Section 7.1 on page 47).
- Installing the EMS server on Microsoft Hyper-V platform (see Section 7.2 on page 61).



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

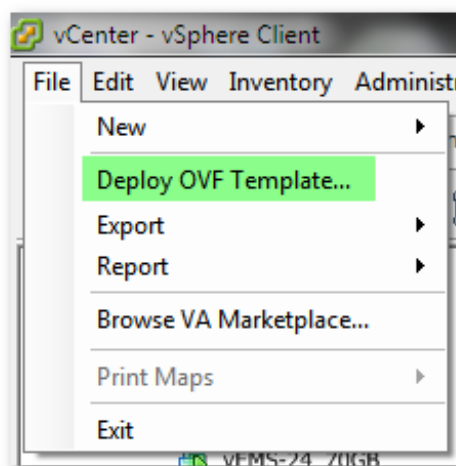
### 7.1 Installing the EMS Server on the VMware Platform

This section describes how to install the EMS server on the VMware vSphere platform. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Section 5.1.1 on page 33) and depends largely on the hardware machine where the VMware vSphere platform is installed.

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

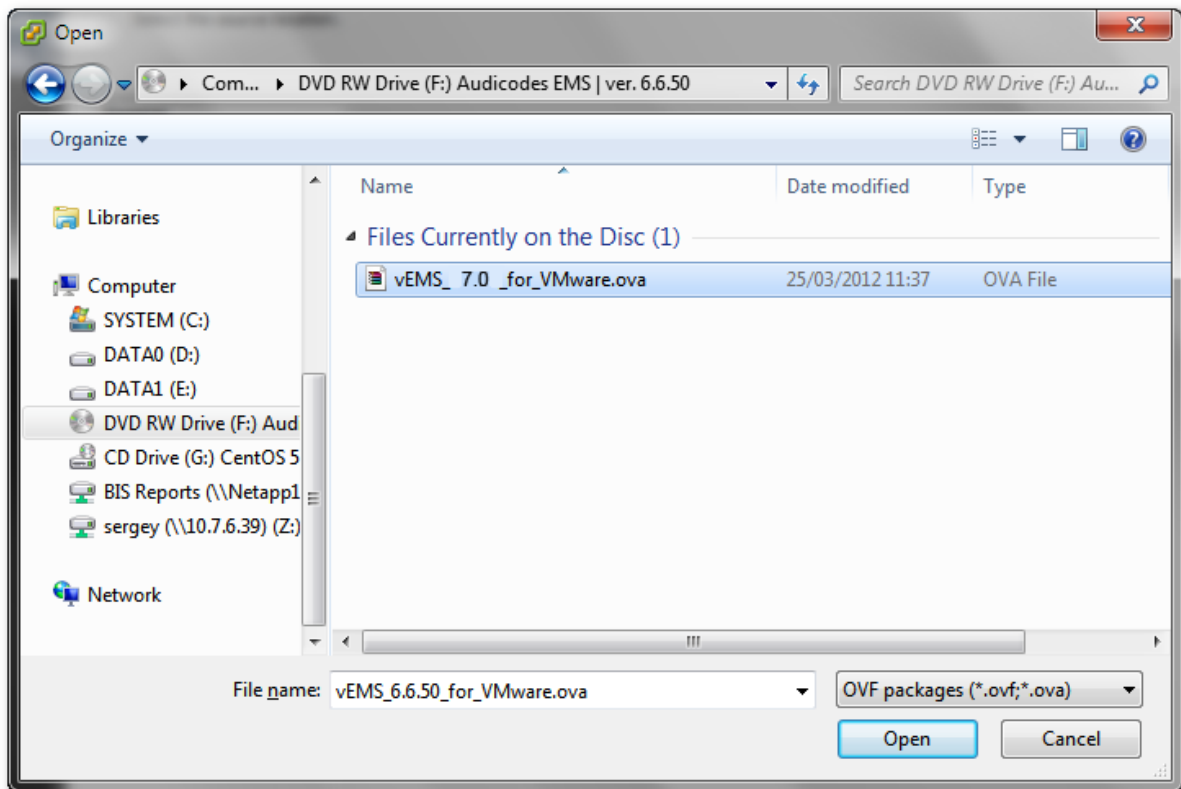
1. Insert the vEMS installation DVD (DVD5) into the disk reader on the PC where the vSphere client is installed.

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



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

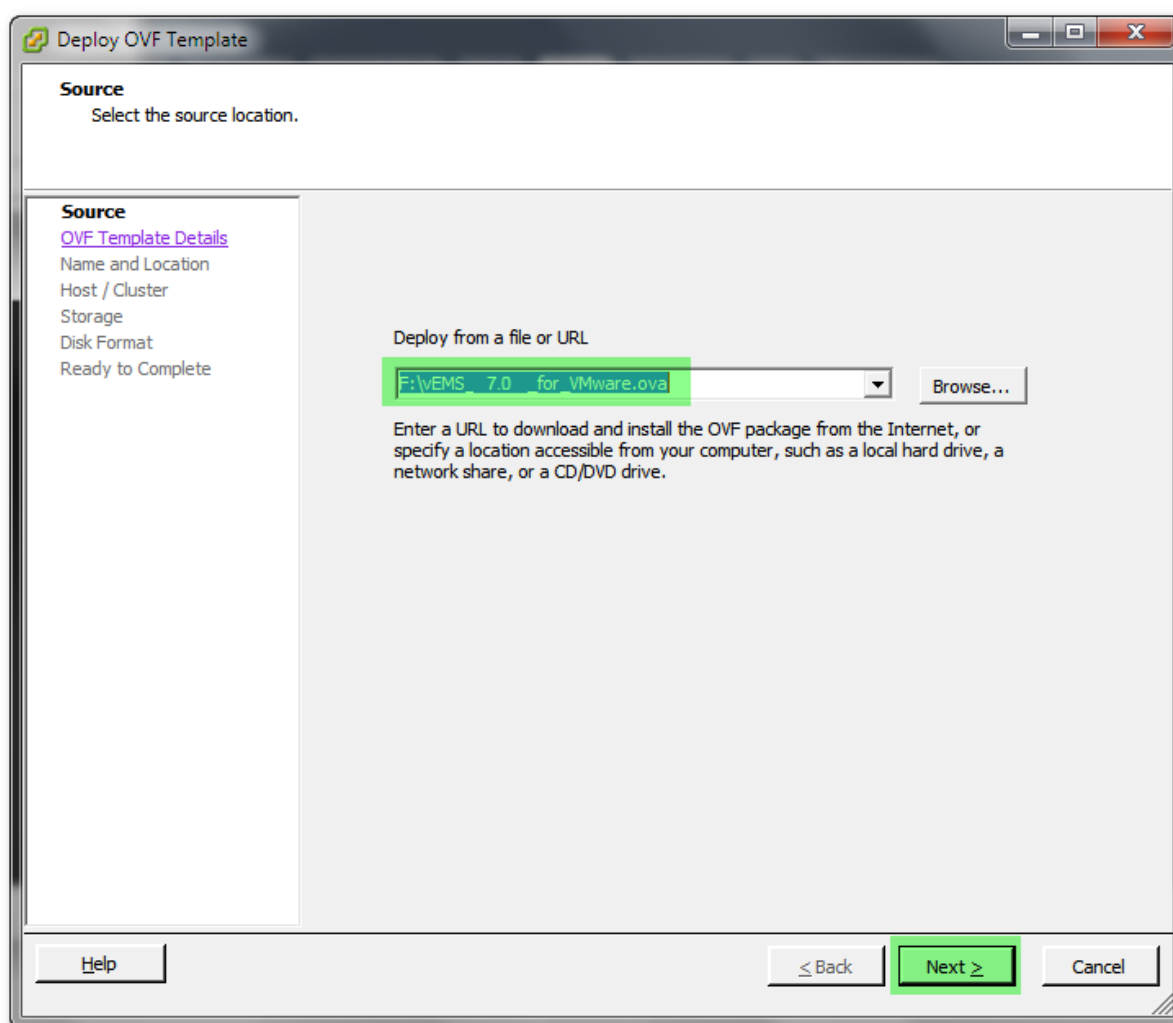
Figure 7-2: Open OVA Package

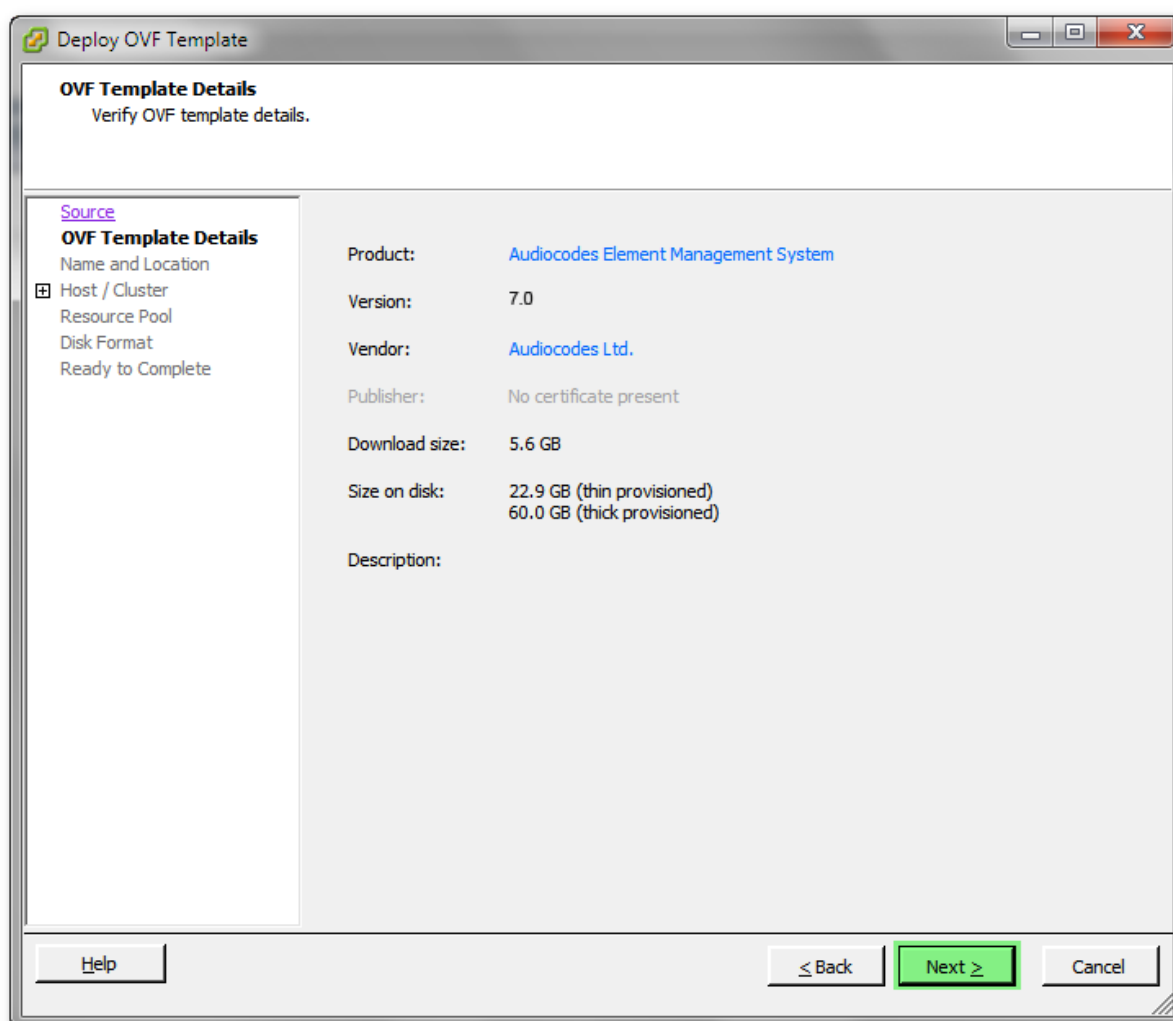


3. Select the vEMS virtual appliance file with extension OVA from the inserted DVD disk, and then click **Next**.

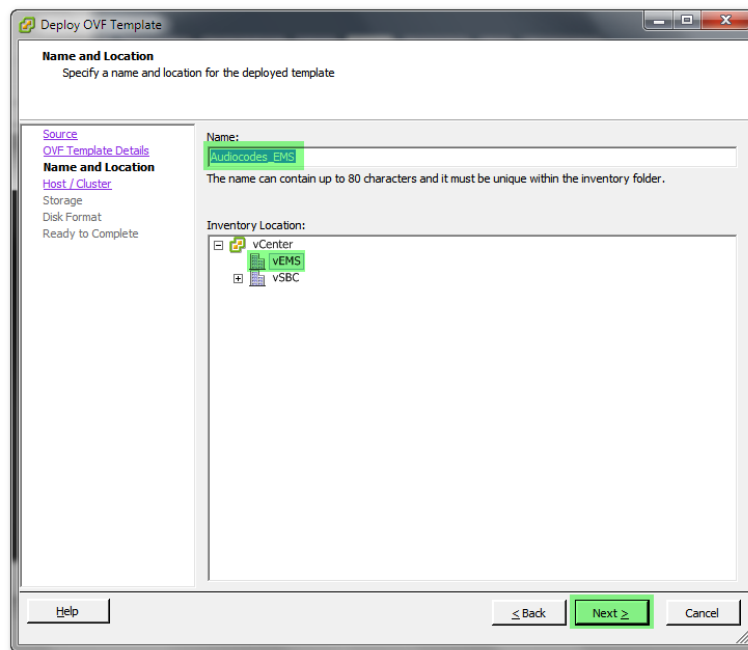


Figure 7-3: OVF Template Source Screen

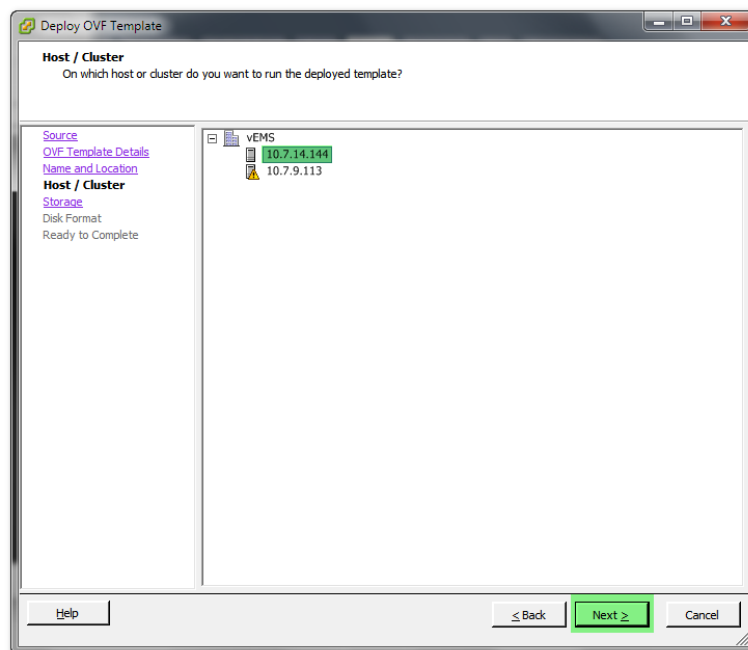


**Figure 7-4: OVF Template Details Screen**


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

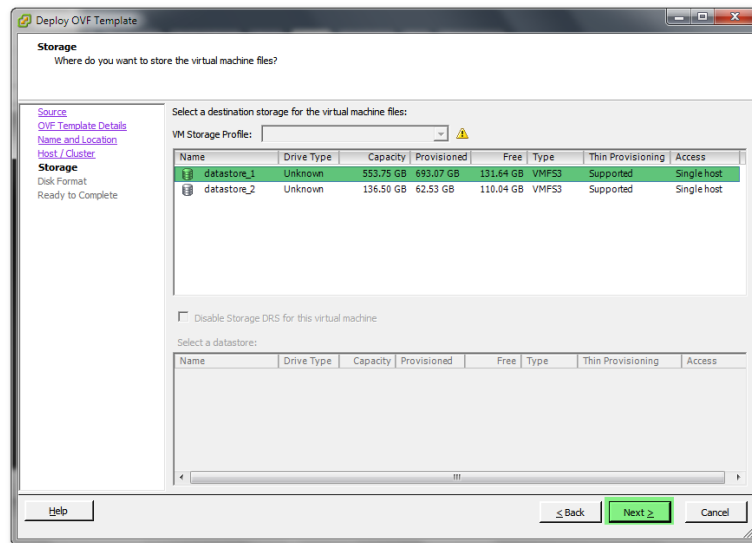
**Figure 7-5: Virtual Machine Name and Location Screen**

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

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

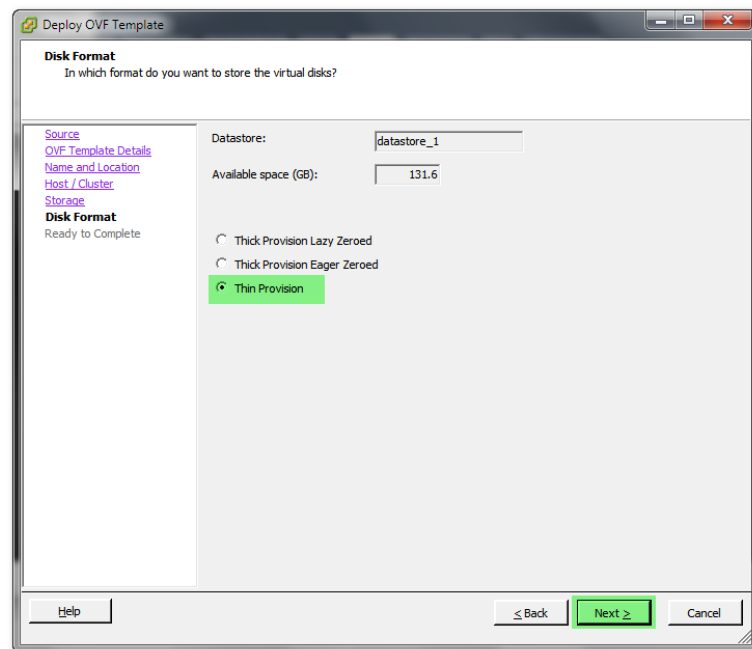
6. In the Host / Cluster screen, select the server to locate the virtual machine, and then click **Next**.

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



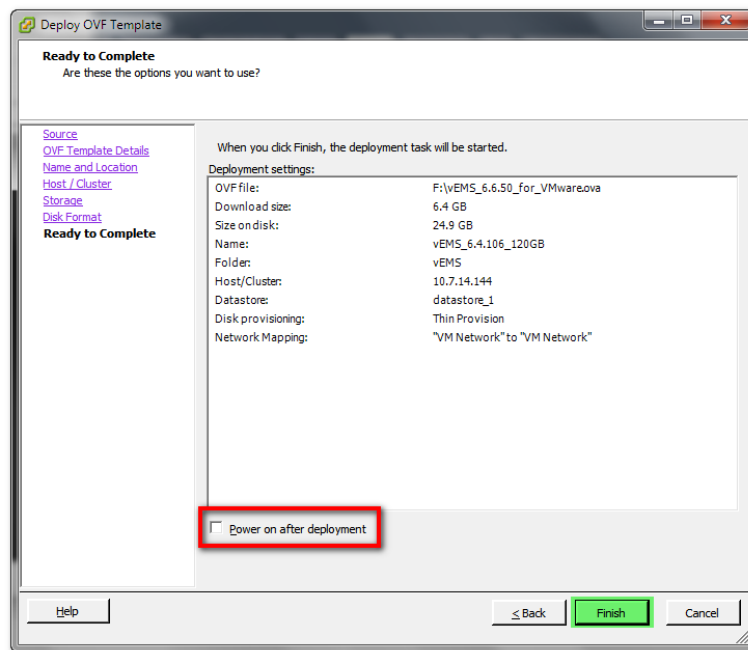
7. In the Storage screen, select the data store where you'd like to locate your machine, and then click **Next**.

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



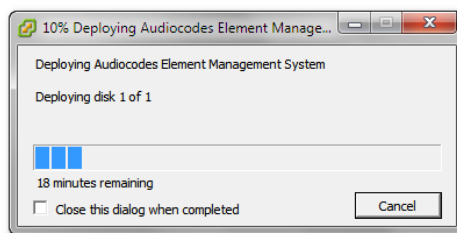
8. In the Disk Format screen, choose the desired provisioning option ('Thin Provisioning' is recommended), and then click **Next**.

Figure 7-9: Ready to Complete Screen

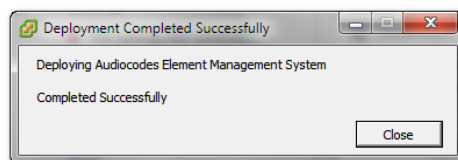


9. In the Ready to Complete screen, leave the option 'Power on after deployment' unchecked, and then click **Finish**.

Figure 7-10: Deployment Progress Screen



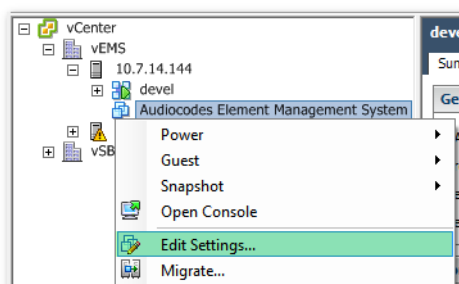
Recent Tasks			
Name	Target	Status	Requested Start Time
Deploy OVF template	Audiocodes Element Management System	14%	21/05/2012 09:32:26



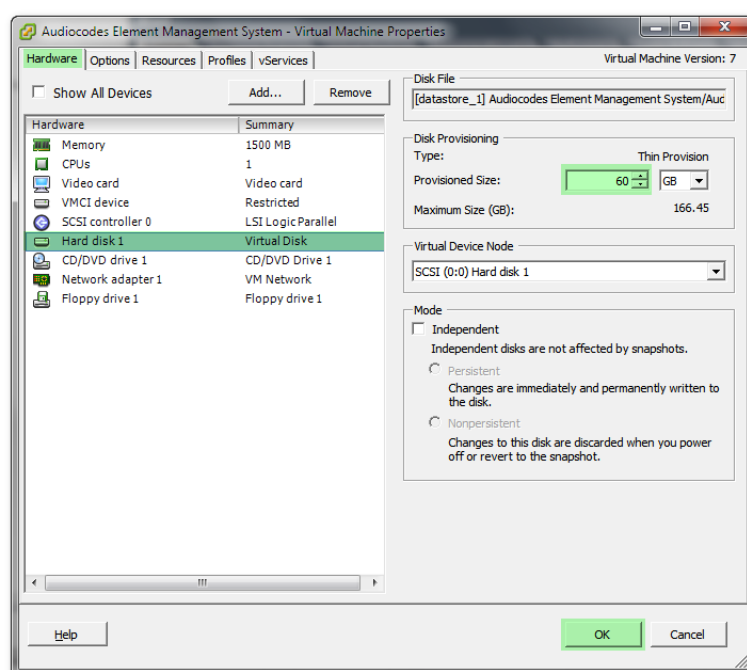
Recent Tasks					
Name	Target	Status	Requested Start Time	Start Time	Completed Time
Deploy OVF template	Audiocodes Element Management System	Completed	21/05/2012 09:32:26	21/05/2012 09:32:26	21/05/2012 10:06:12

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 23), and then click **OK**.



**Notes:**

- Once the hard disk space allocation has been increased, it cannot be reduced to a lower amount.
- If you wish to create an EMS VMs in a cluster environment that supports High Availability and has shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (see Section 7.1.1).

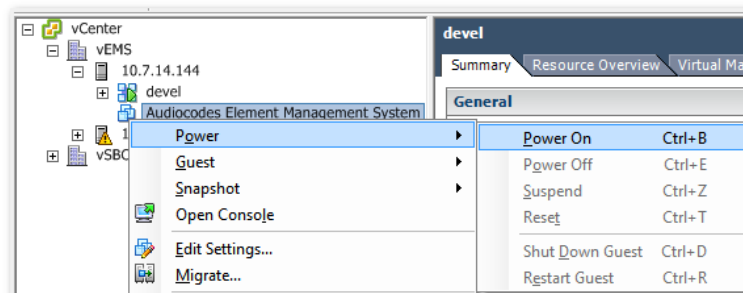
13. **Wait** until the machine reconfiguration process has completed.

**Figure 7-13: Recent Tasks**

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

14. Power on the machine; in the vCenter tree, right-click the AudioCodes Element Management System and in the drop-down menu, choose Power > Power On. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications (see Section 3 on page 23).

**Figure 7-14: Power On**



15. Wait until the boot process is complete, and then connect the running server through the vSphere client console.
16. Login to the server as 'acems' user and enter *acems* password.
17. Switch user to 'root' and enter password *root* (default password is *root*).
18. Proceed to the network configuration using the Ems Server Manager. To run the manager type 'EmsServerManager', and then press Enter.
19. Set the EMS server network IP address by following the steps in [12.6.1](#)
20. Perform configuration actions as required using the EMS Server Manager (see Section 12 on page 97).

## 7.1.1 Configuring EMS Virtual Machines (VMs) in a VMware Cluster

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

### 7.1.1.1 Site Requirements

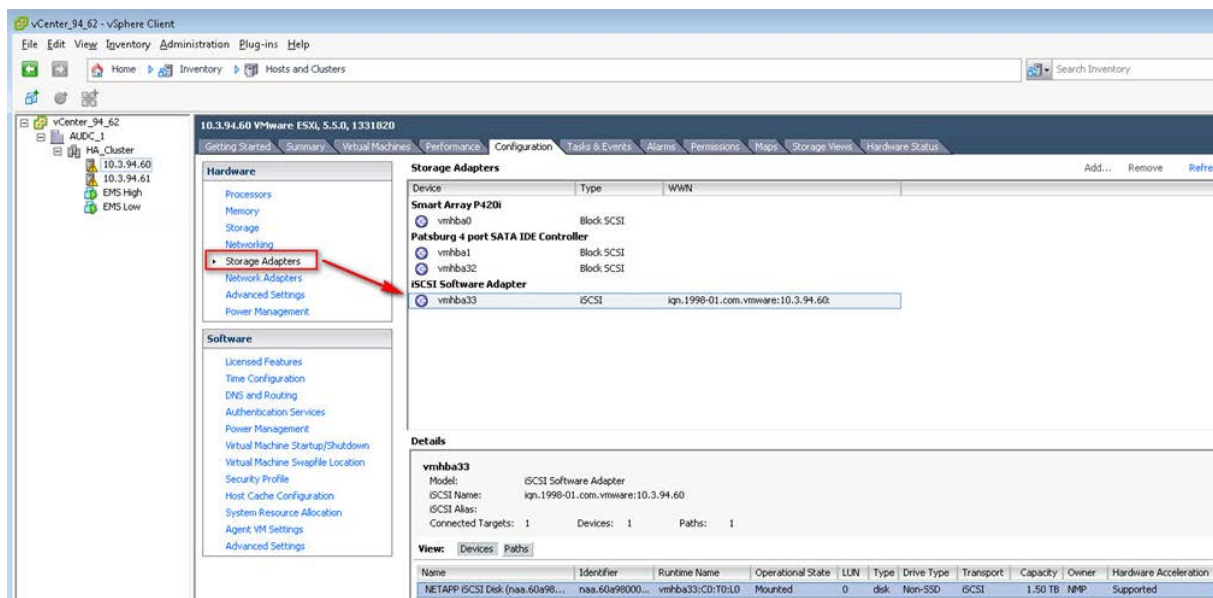
Ensure that your VM cluster site meets the following requirements:

- The configuration process assumes that you have a VMware cluster which contains at least two ESXi servers controlled by vCenter server.
- The clustered VM servers should be connected to a shared network storage of type iSCSI or any other types supported by VMware ESXi.

For example, a datastore “AUDC\_1” which contains a cluster named “HA\_Cluster” and is combined of two ESXi servers (see figure below).

- Verify that Shared Storage is defined and mounted for all cluster members:

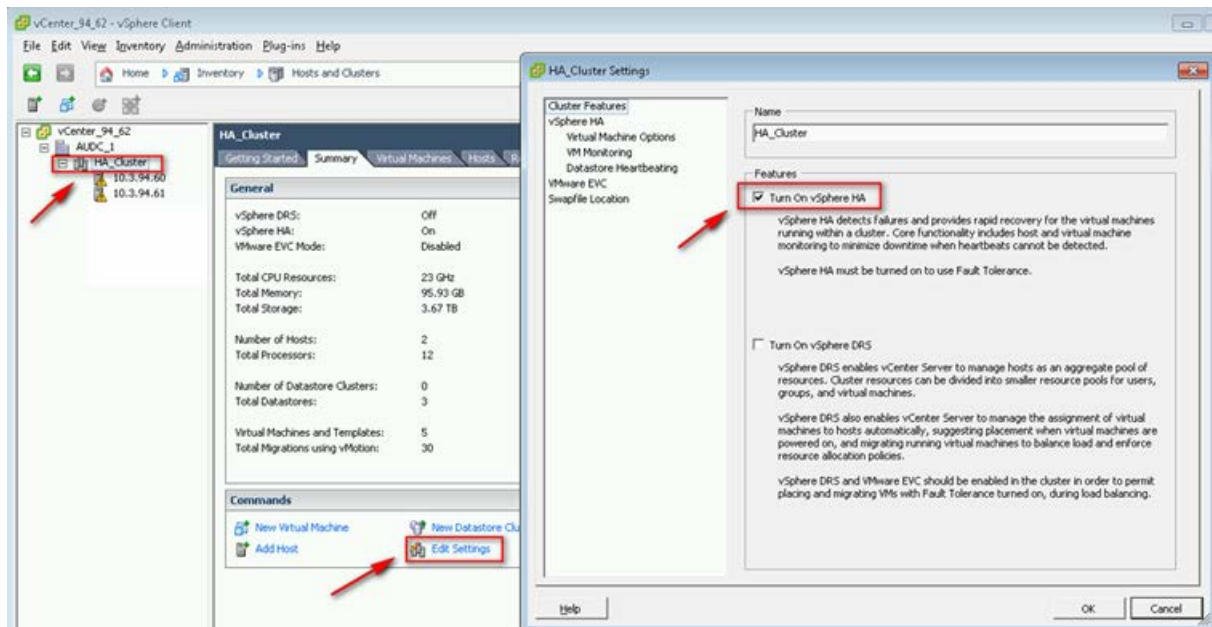
**Figure 7-15: Storage Adapters**





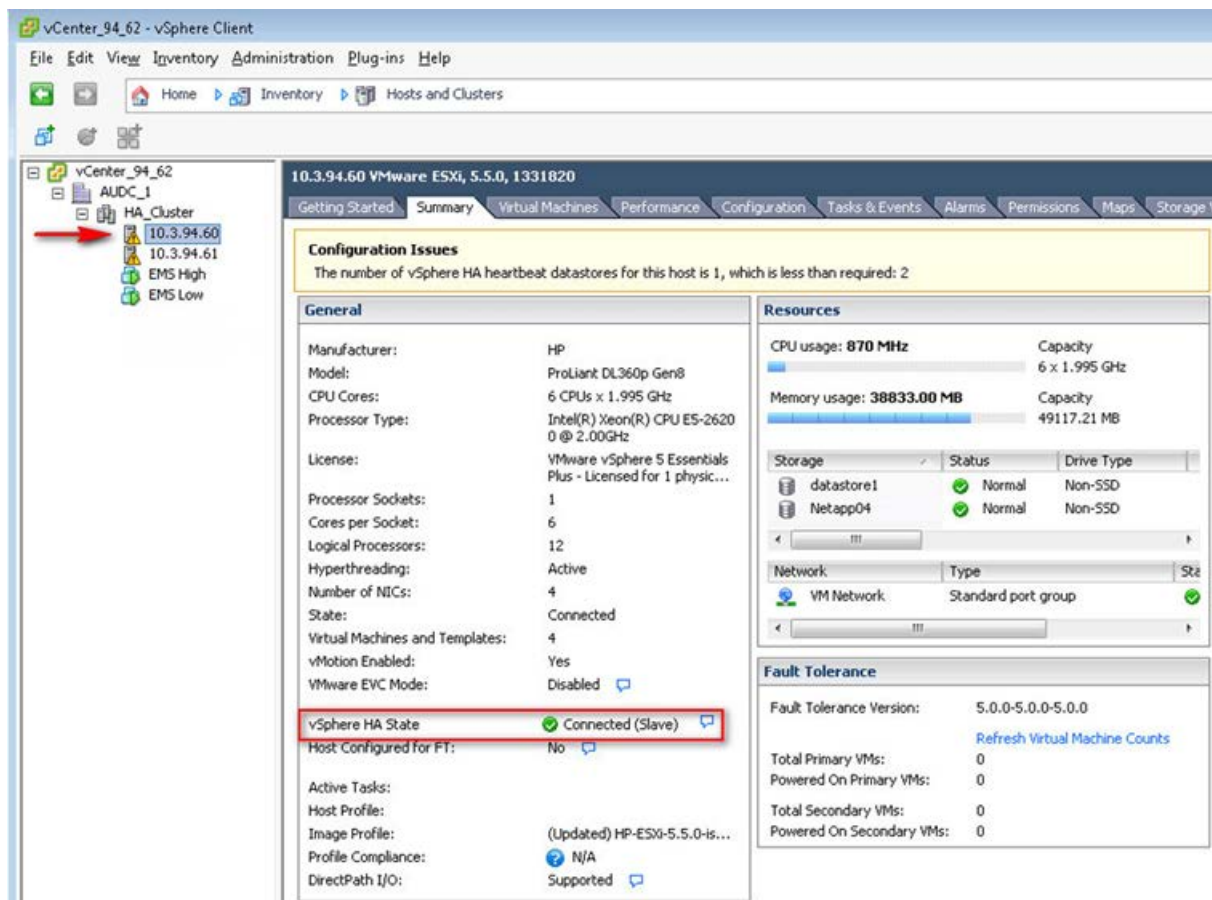
- Ensure that the 'Turn On vSphere HA' check box is selected:

Figure 7-16: Turn On vSphere HA



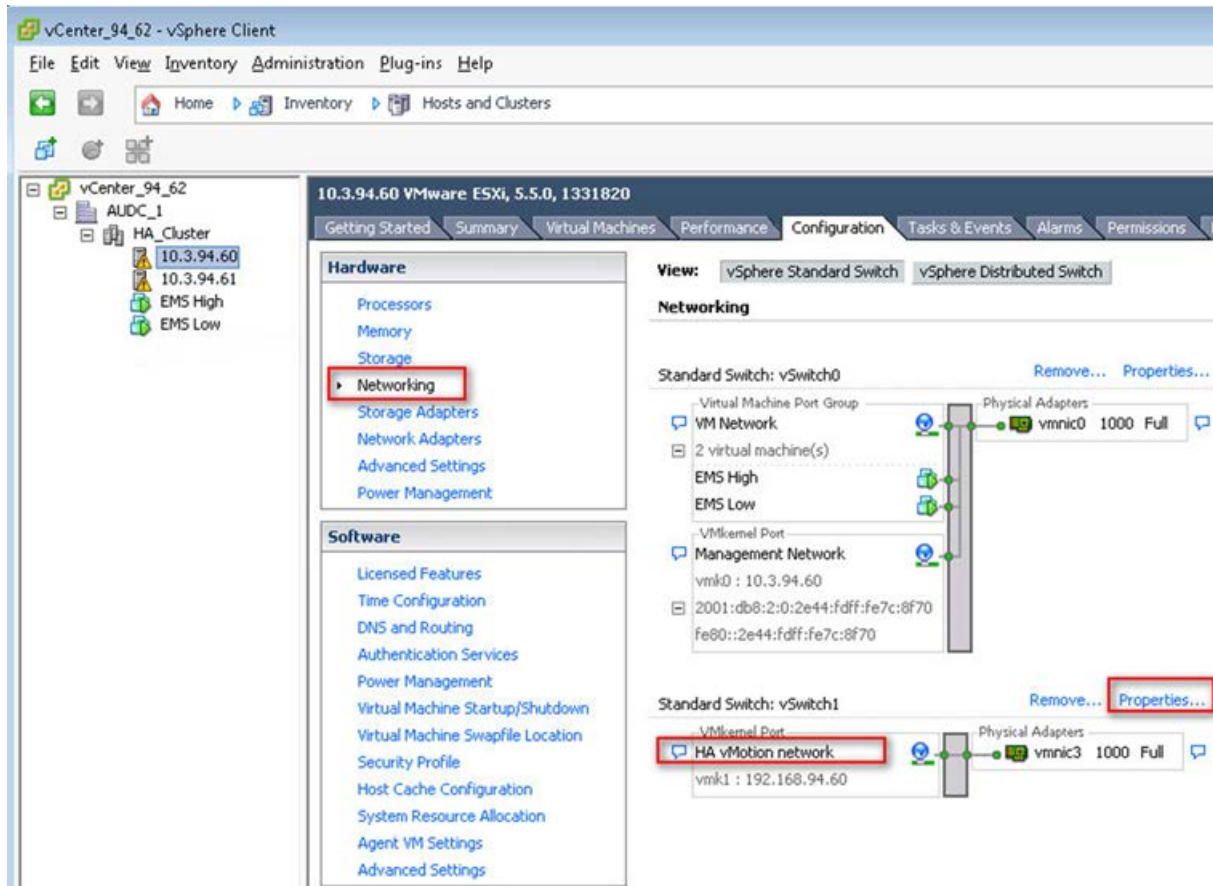
- Ensure that HA is activated on each cluster node:

Figure 7-17: Activate HA on each Cluster Node

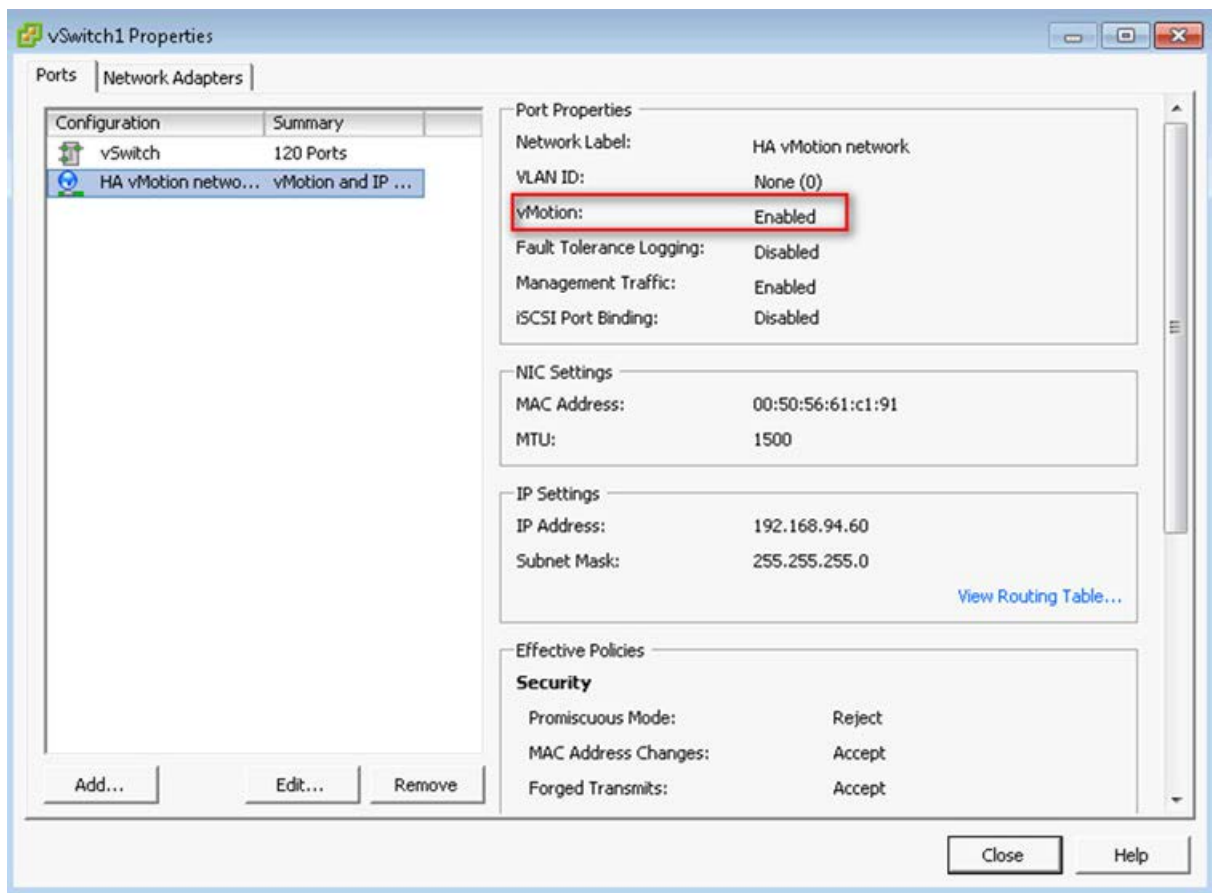


- Ensure that the networking configuration is identical on each cluster node:

**Figure 7-18: Networking**

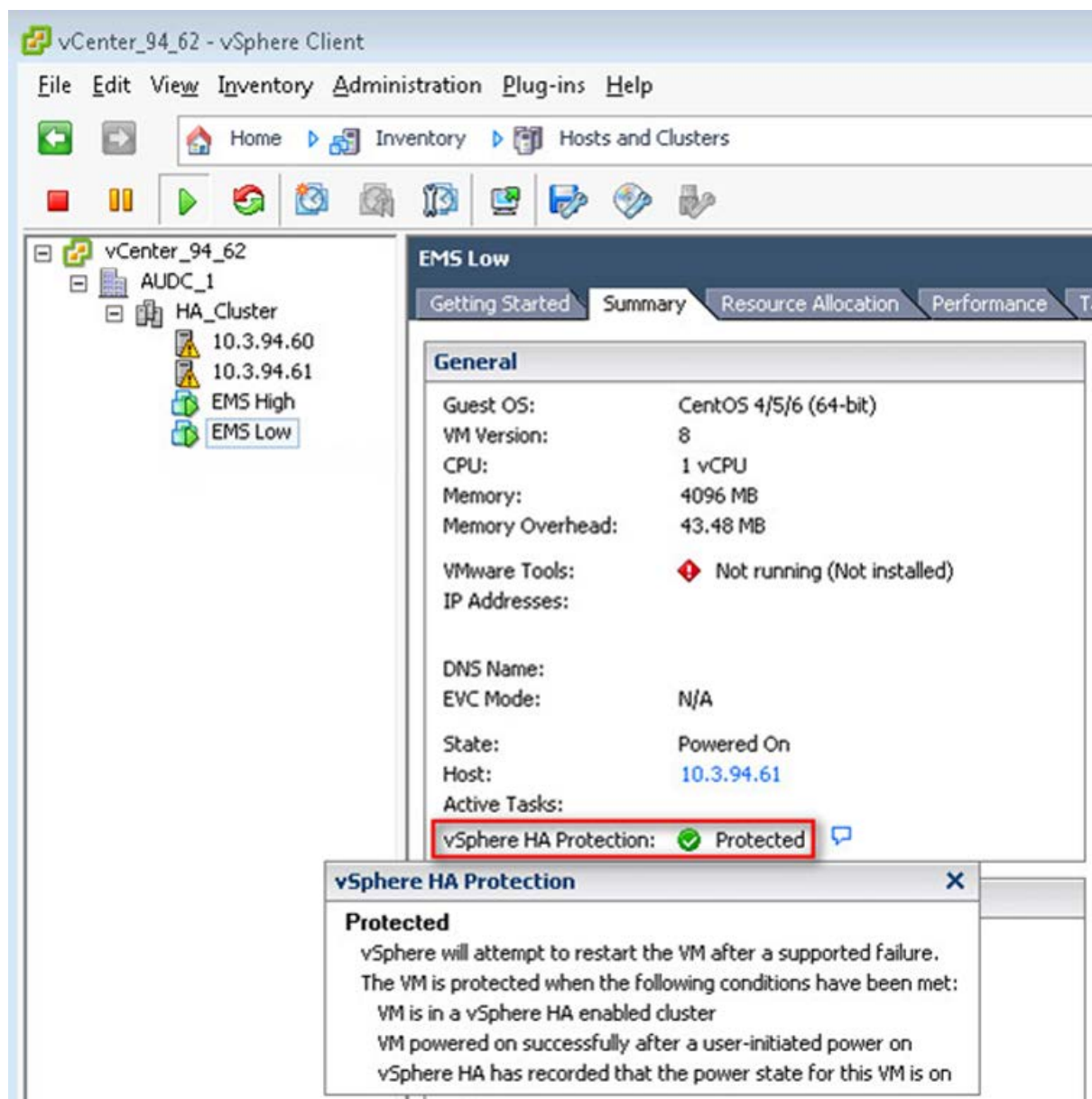


- Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

**Figure 7-19: Switch Properties**

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

**Figure 7-20: Protected VM**





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

### 7.1.1.2 Cluster Host Node Failure

In case an ESXi host node where the VM is running fails, then the VM is restarted on the redundant cluster node automatically.



**Note:** When one of the cluster nodes fail, the EMS VM is automatically migrated to the redundant host node. During this process, the EMS VM is restarted and consequently any running EMS or SEM processes are dropped. The migration process may take several minutes.

## 7.2 Installing the EMS Server on Microsoft Hyper-V Platform

This section describes how to install the EMS server on the Microsoft Hyper-V Server 2012 R2 platform. This procedure takes approximately 30 minutes and predominantly depends on the hardware machine where the Microsoft Hyper-V platform is installed.



**Note:** The Audiocodes EMS supports the Failover Clustering feature in Windows Server 2012 R2 (see Chapter 3 on page 17).

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

- Install the Virtual Machine (VM) (see Section 7.2.1 on page 62).
- Configure the deployed VM (see Section 7.2.2 on page 66).
- Changing MAC Addresses from 'Dynamic' to 'Static' (see Section 7.2.3 on page 68).
- Configure disk settings (see Section 7.2.4 on page 69 and Section 7.2.5 on page 69).
- Change the default IP address to suite your IP addressing scheme (see Section 7.2.6 on page 73).
- Configure VMs in a Cluster (see Section 7.2.7 on page 74)

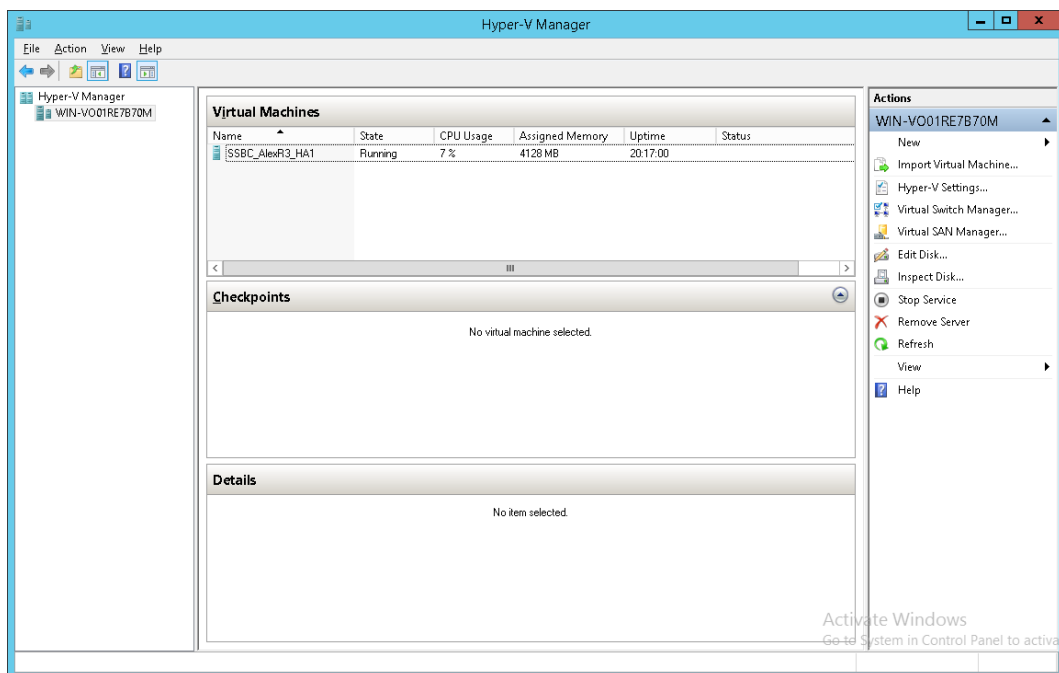
## 7.2.1 Installing the Virtual Machine

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

### ➤ To install the EMS server on Microsoft Hyper-V:

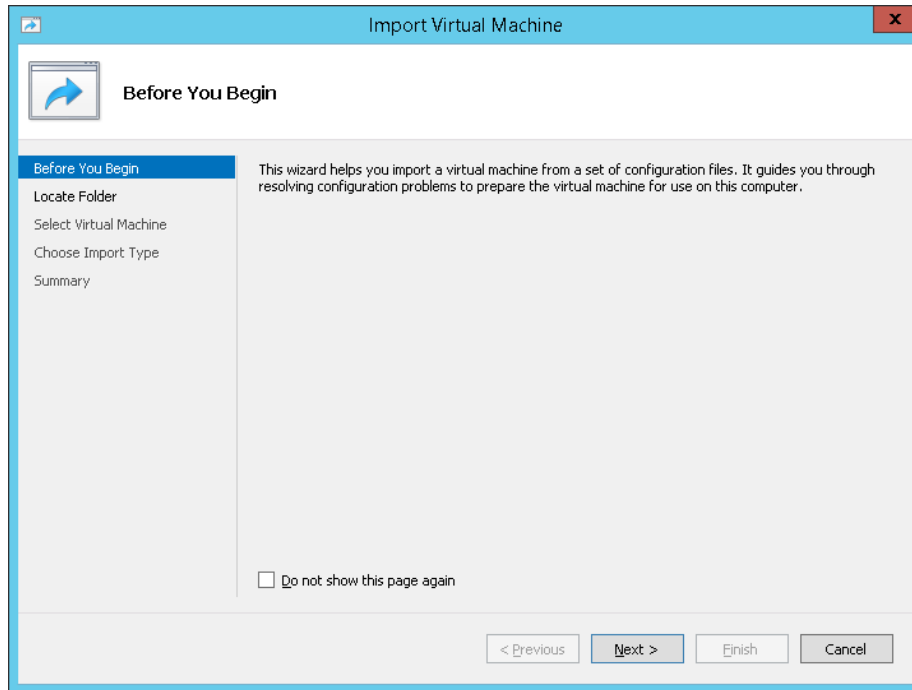
1. Extract the zip file containing the EMS server installation received from AudioCodes to a local directory on the Hyper-V server (see Appendix H on page 263 for instructions on how to transfer files ) .
2. Open Hyper-V Manager by clicking **Start > Administrative Tools > Hyper-V Manager**; the following screen opens:

Figure 7-21: Installing the EMS server on Hyper-V – Hyper-V Manager



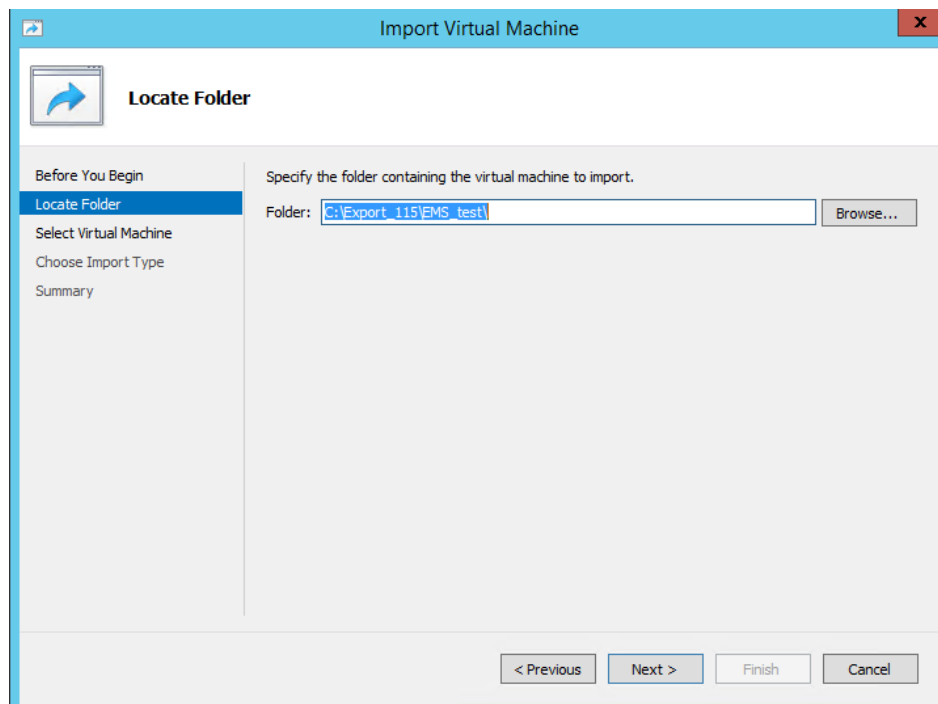
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

**Figure 7-22: Installing EMS server on Hyper-V – Import Virtual Machine Wizard**



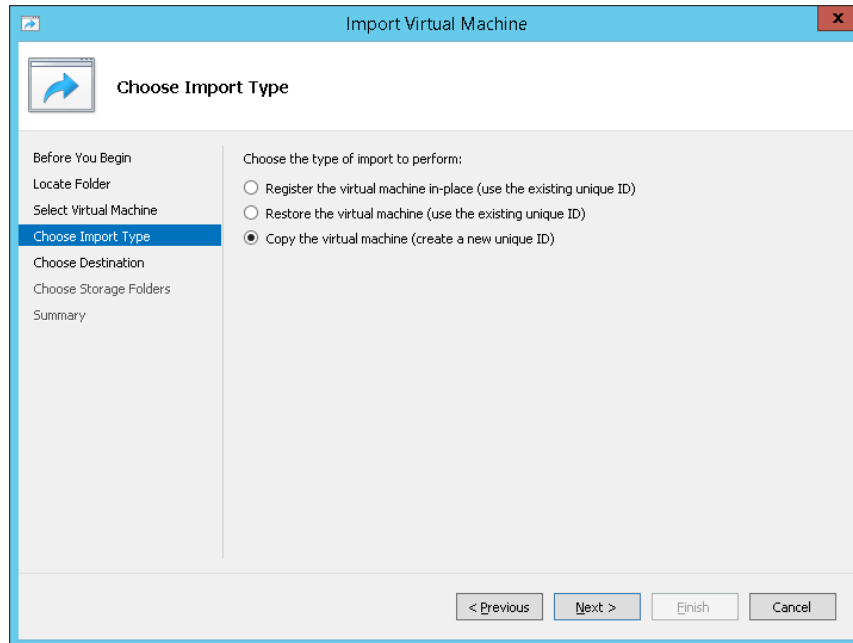
4. Click **Next**; the Locate Folder screen opens:

**Figure 7-23: Installing EMS server on Hyper-V – Locate Folder**



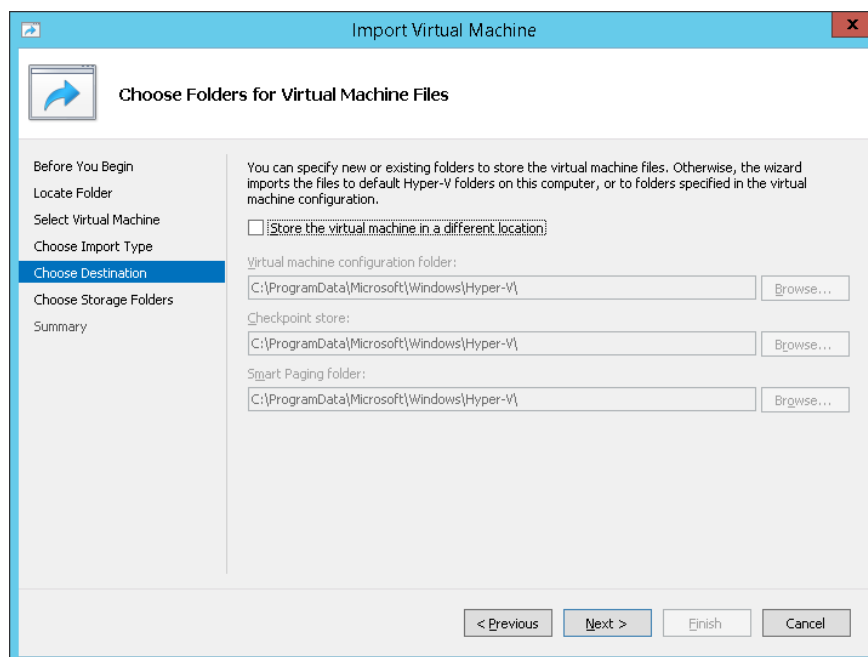
5. Enter the location of the VM installation folder which was previously extracted from the zip file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

**Figure 7-24: Installing EMS server on Hyper-V – Choose Import Type**



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

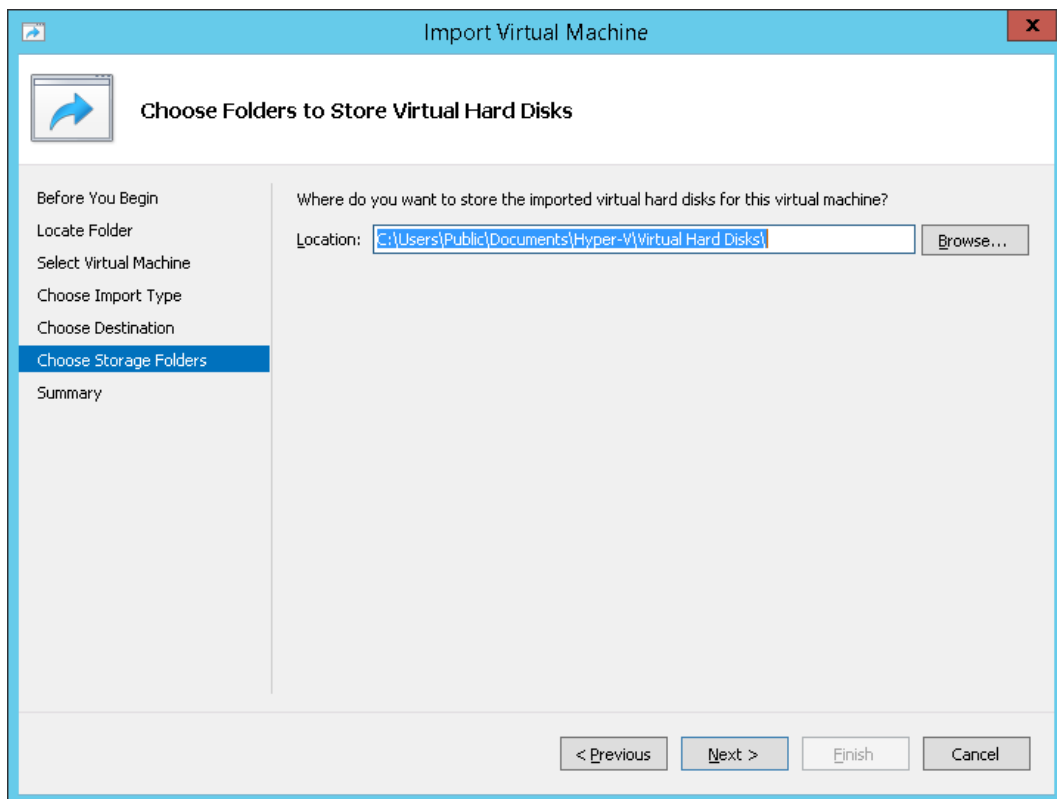
**Figure 7-25: Installing EMS server on Hyper-V – Choose Destination**





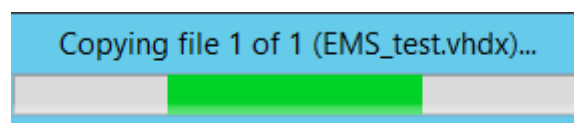
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

**Figure 7-26: Installing EMS server on Hyper-V – Choose Storage Folders**



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

**Figure 7-27: File Copy Progress Bar**



This step may take approximately 30 minutes to complete.

11. Proceed to Section 7.2.2 on page 66.

## 7.2.2 Configuring the Virtual Machine to run the EMS server

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

Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see Section 3 on page 23.

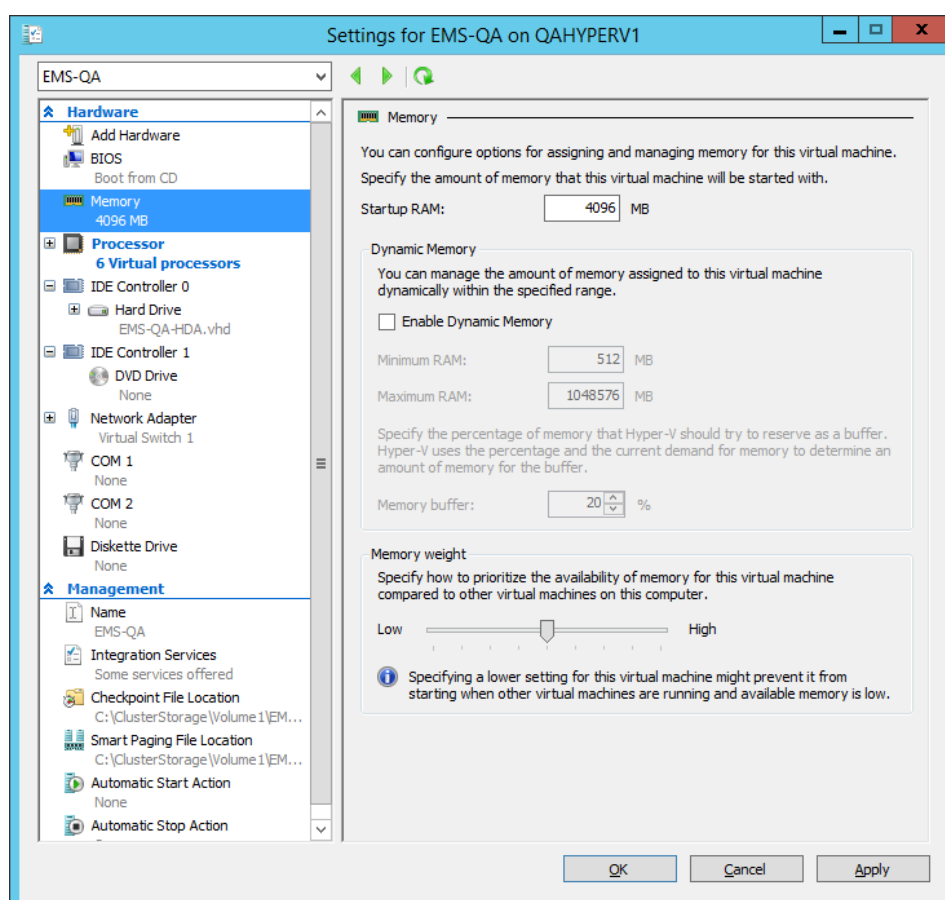
**Table 7-1: Virtual Machine Configuration**

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

### ➤ To configure the VM for EMS server:

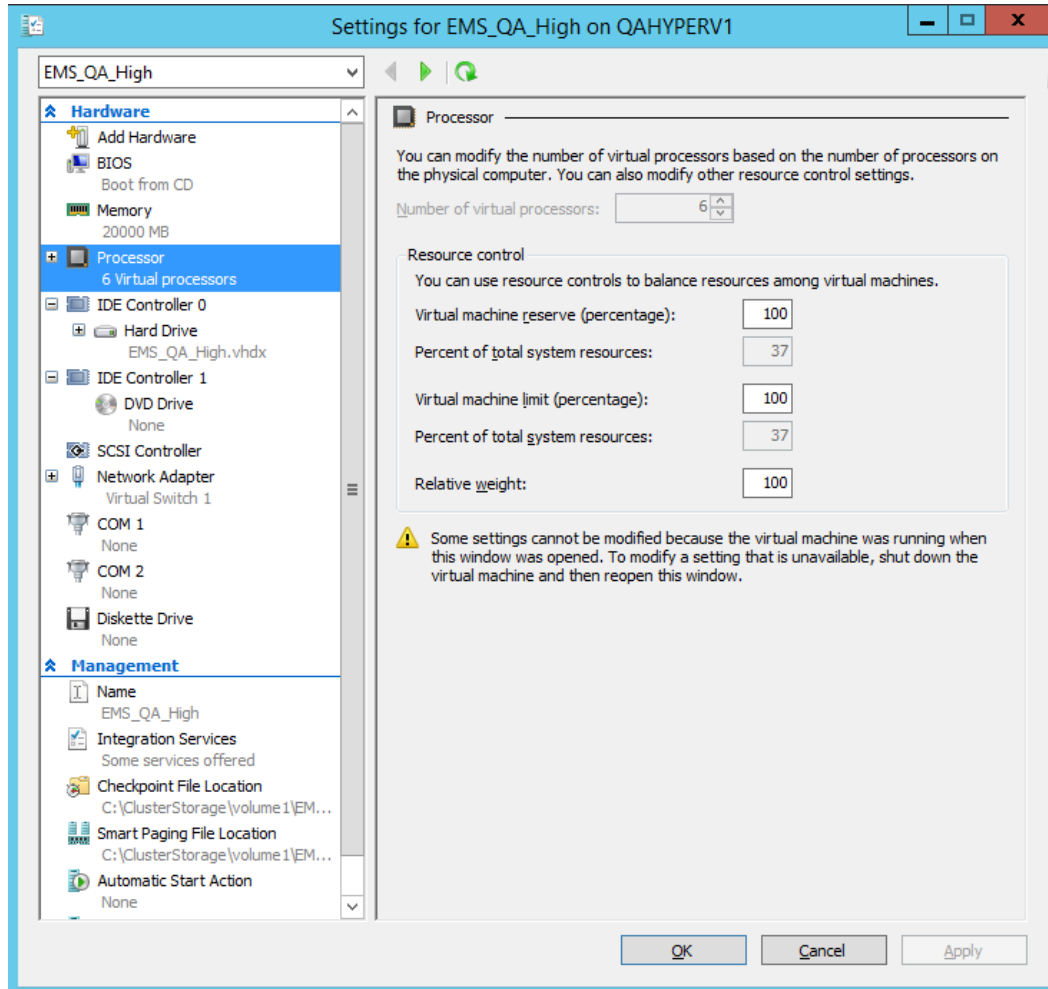
1. Locate the new EMS server VM in the tree in the Hyper-V Manager, right-click it, and then select **Settings**; the Virtual Machine Settings screen opens:

**Figure 7-28: Adjusting VM for EMS server – Settings - Memory**



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

**Figure 7-29: Adjusting VM for EMS server - Settings - Processor**



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

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

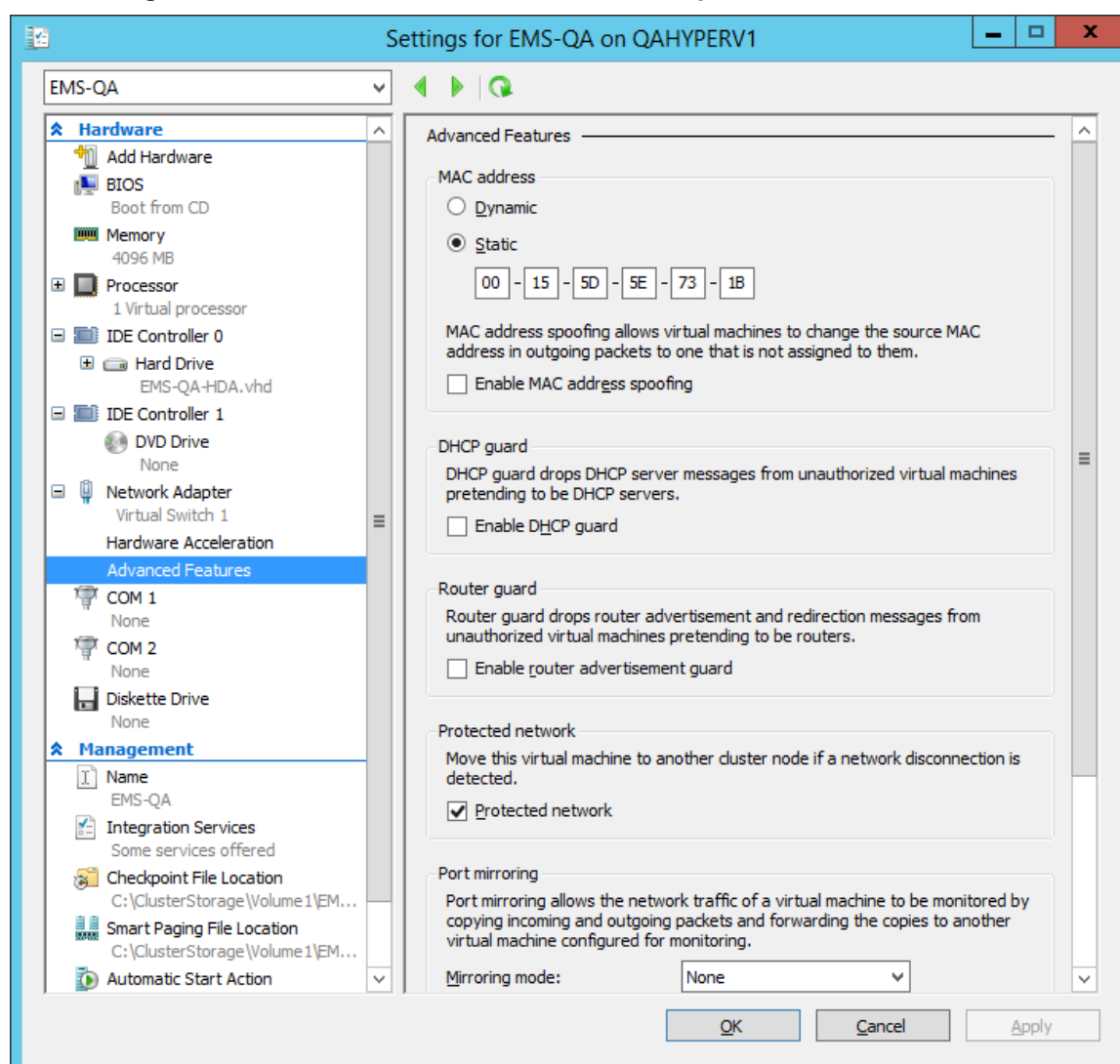
By default, the MAC addresses of the EMS server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license for features such as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

To prevent this from occurring, MAC Addresses should be changed from 'Dynamic' to 'Static'.

### ➤ To change the MAC address to 'Static' in Microsoft Hyper-V:

1. Shutdown the EMS server (see Section 12.5.6 on page 110).
2. In the Hardware pane, select **Network Adapter** and then **Advanced Features**.
3. Select the MAC address 'Static' option.
4. Repeat steps 2 and 3 for each network adapter.

**Figure 7-30: Advanced Features - Network Adapter – Static MAC Address**



## 7.2.4 Hard Drive Location

If you wish to create an EMS VMs in a cluster environment that supports High Availability and has shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (see Section 7.2.7 on page 74).

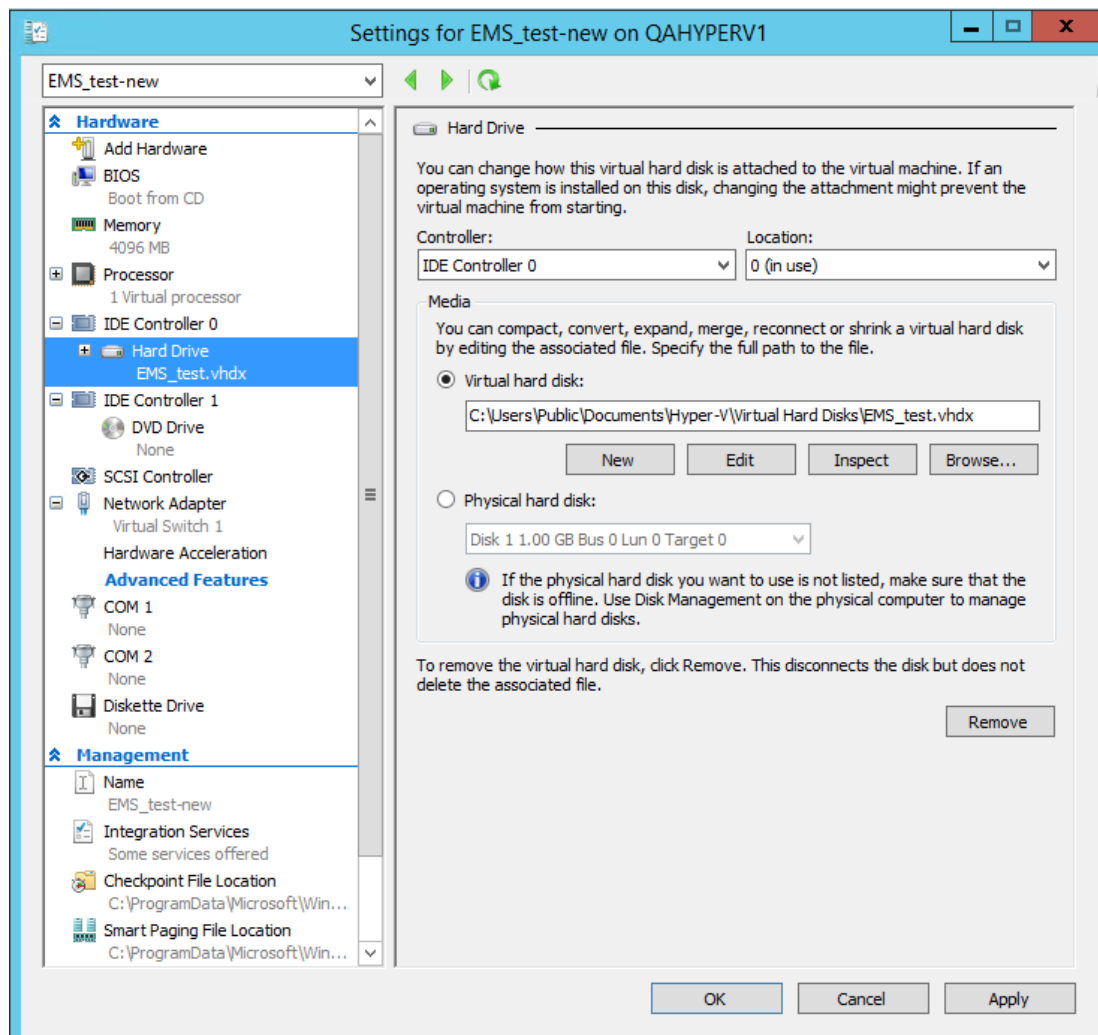
## 7.2.5 Expanding Disk Capacity

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

➤ **To expand the disk size:**

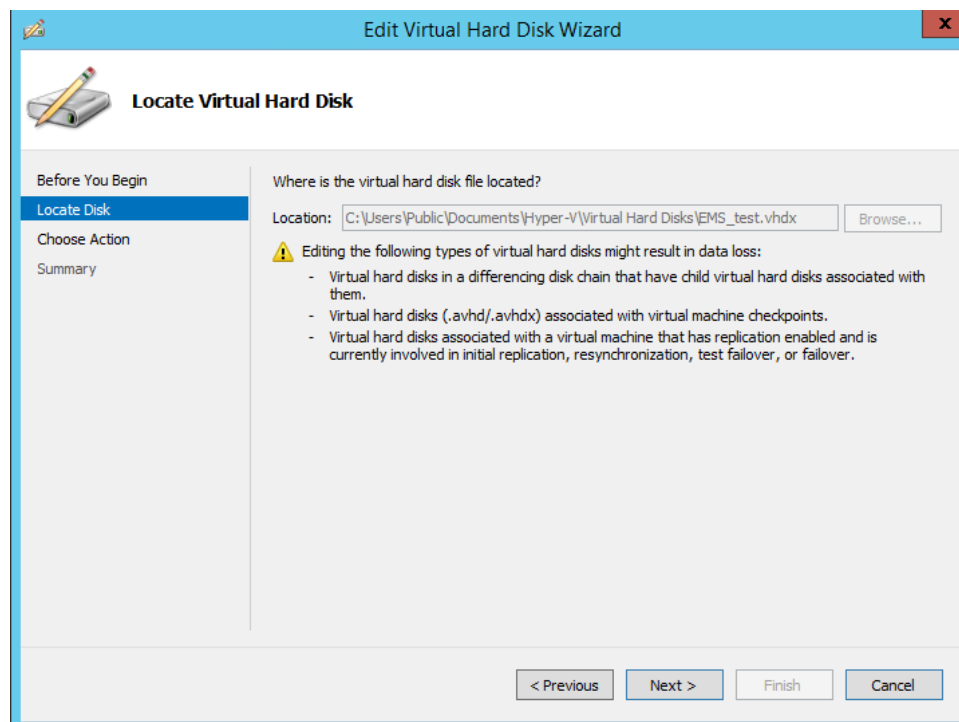
1. Make sure that the target EMS server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

**Figure 7-31: Expanding Disk Capacity**



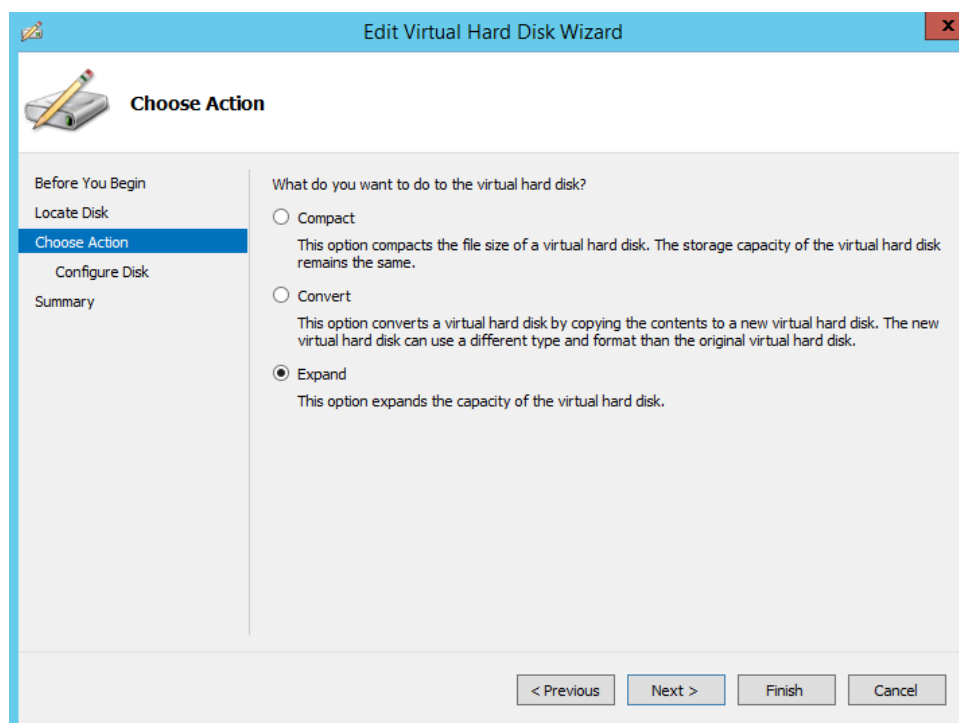
The Edit Virtual Disk Wizard is displayed as shown below.

**Figure 7-32: Edit Virtual Hard Disk Wizard**



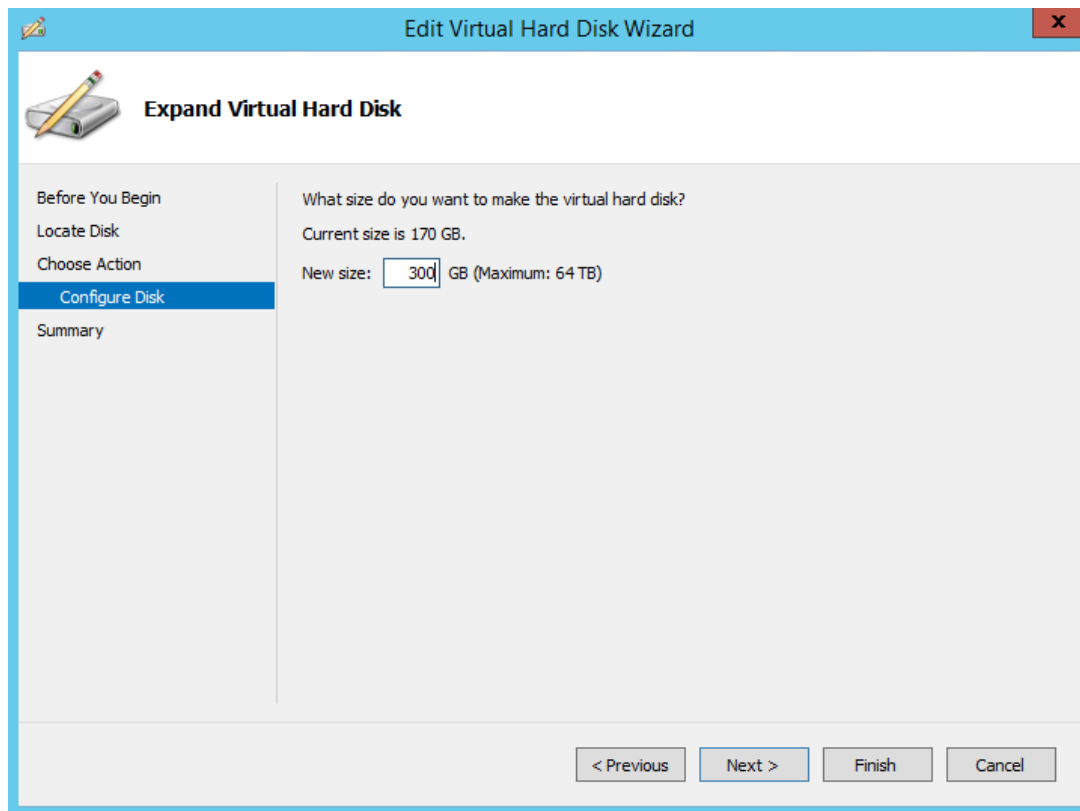
3. Click **Next**; the Choose Action screen is displayed:

**Figure 7-33: Edit Virtual Hard Disk Wizard-Choose Action**



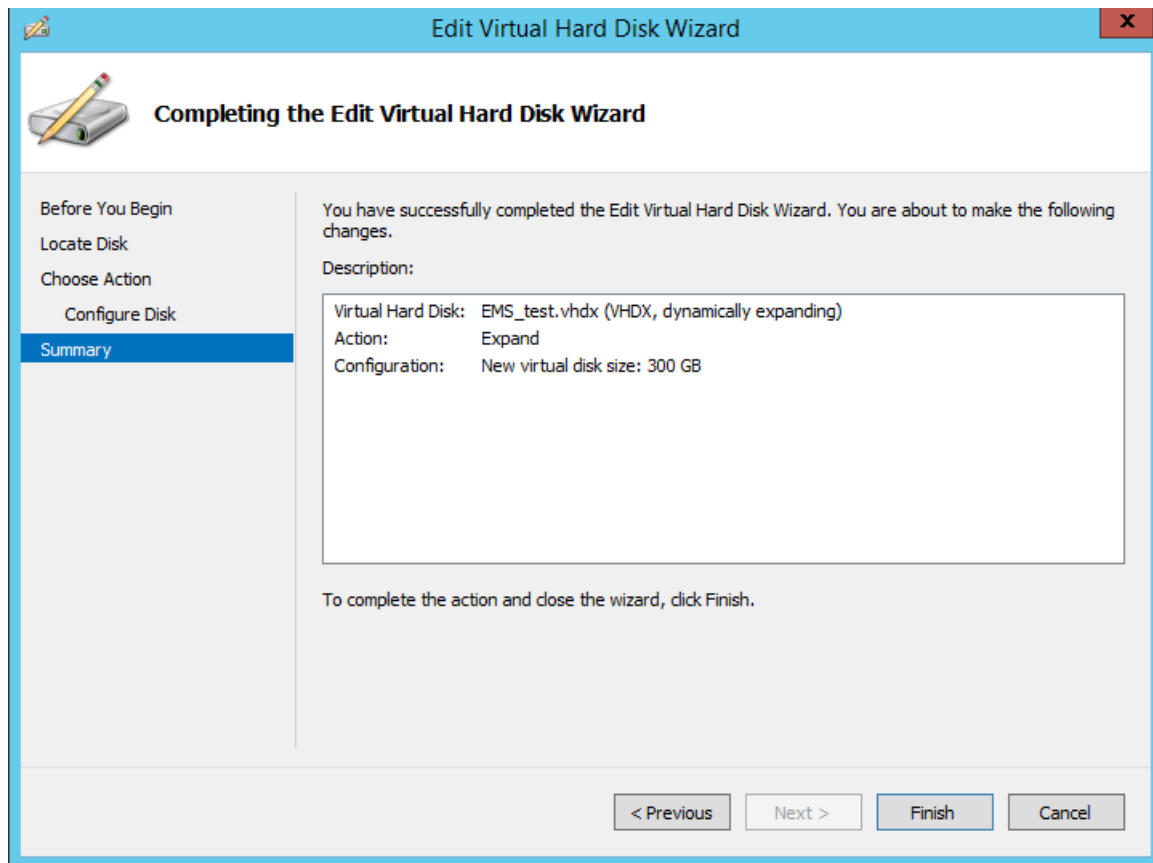
4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

**Figure 7-34: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk**



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

Figure 7-35: Edit Virtual Hard Disk Wizard-Completion



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



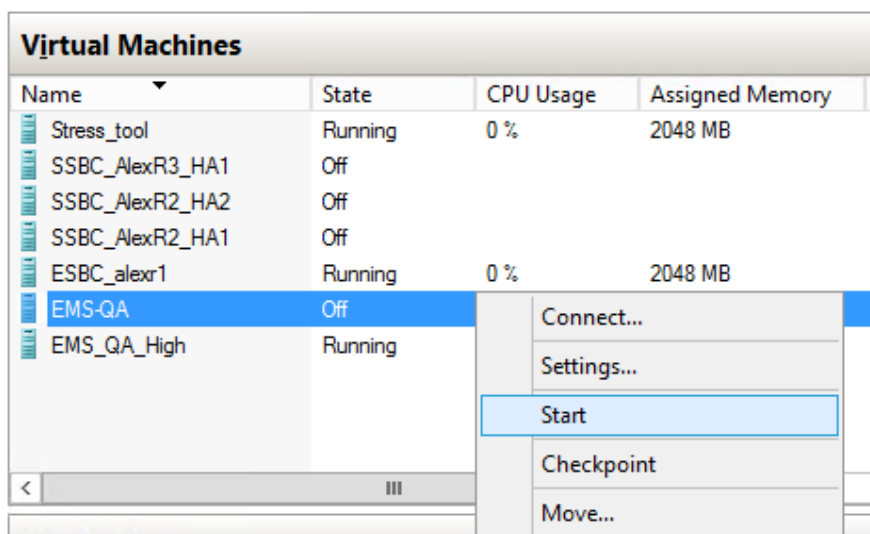
## 7.2.6 Assigning EMS Server IP Address to Network

After installation, the EMS server is assigned a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network interface card connected to the 'trusted' virtual network switch during the EMS server installation. You need to change this IP address to suit your IP addressing scheme.

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

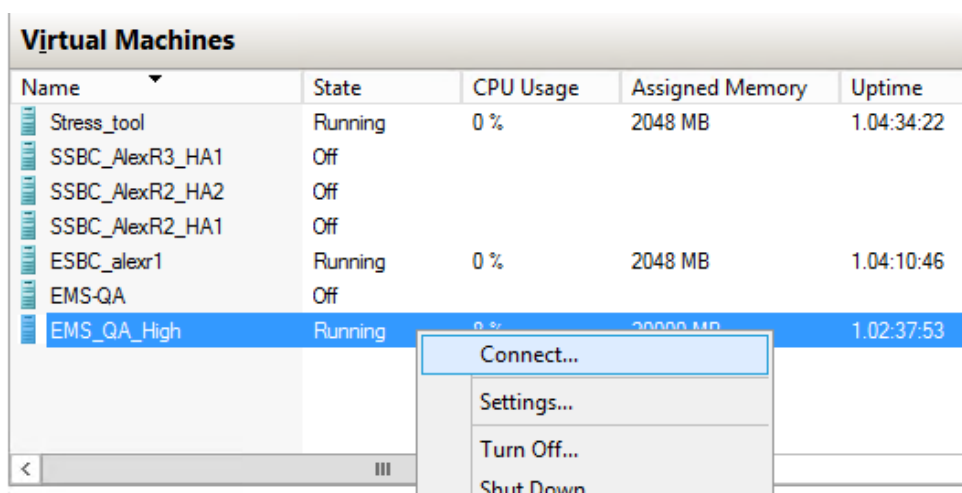
1. Start the EMS server virtual machine, on the Hyper-V tree, right-click the EMS server, and then in the drop-down menu, choose **Start**.

**Figure 7-36: Power On Virtual Machine**



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

**Connect to EMS Server Console**



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

4. Switch user to 'root', and then enter *root* password (default password is *root*).
5. Start the EMS Server Manager utility by specifying the following command:  

```
# EmsServerManager
```
6. Set the EMS server network IP address to suit your IP addressing scheme (see Section 12.6.1).
7. Perform other configuration actions as required using the EMS Server Manager (see Section 12 on page 97).

## 7.2.7 Configuring EMS Virtual Machines in a Microsoft Hyper-V Cluster

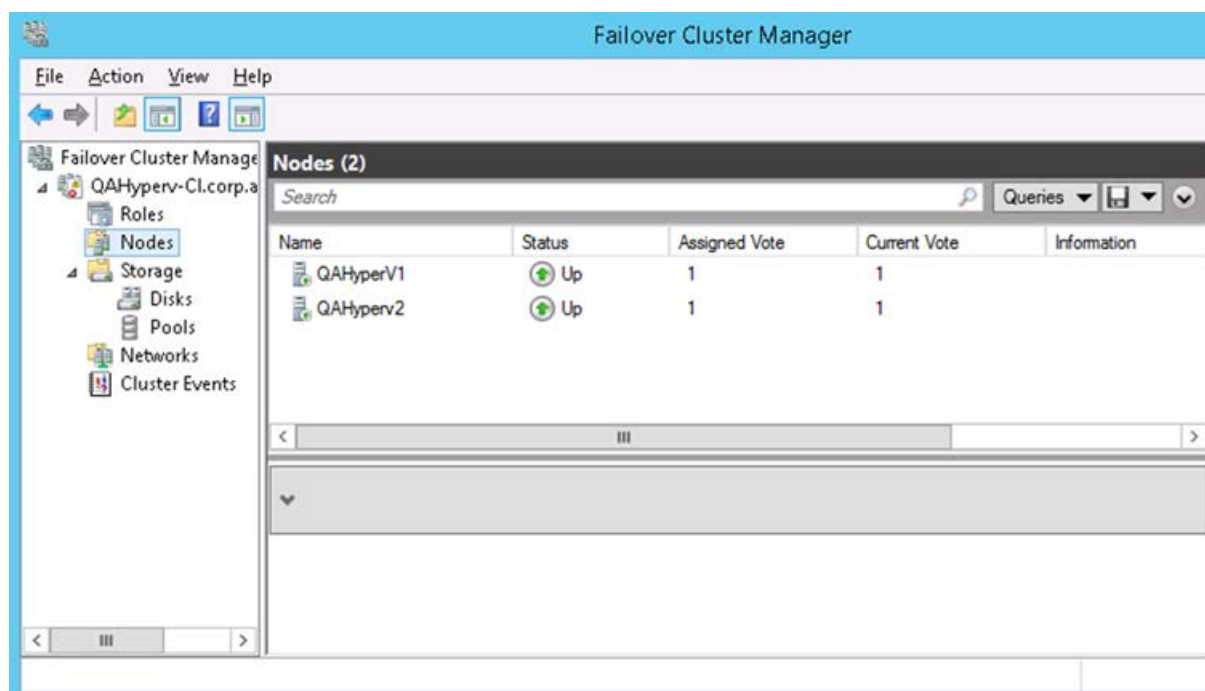
This section describes how to configure EMS VMs in a Microsoft Hyper-V cluster for HA.

### 7.2.7.1 Site Requirements

Ensure that your Hyper-V cluster site meets the following requirements:

- The configuration process assumes that your Hyper-V failover cluster contains at least two Windows nodes with installed Hyper-V service.
- The cluster should be connected to a shared network storage of iSCSI type or any other supported type. For example, “QAHyperv” contains two nodes.

**Figure 7: Hyper-V-Failover Cluster Manager Nodes**



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

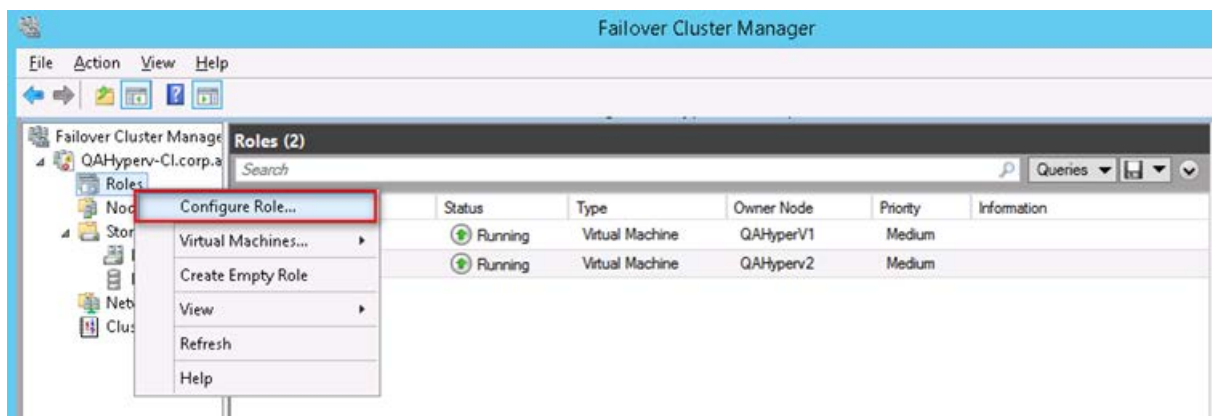
### 7.2.7.2 Add the EMS VM in Failover Cluster Manager

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

➤ To add the EMS VM in Failover Cluster Manager:

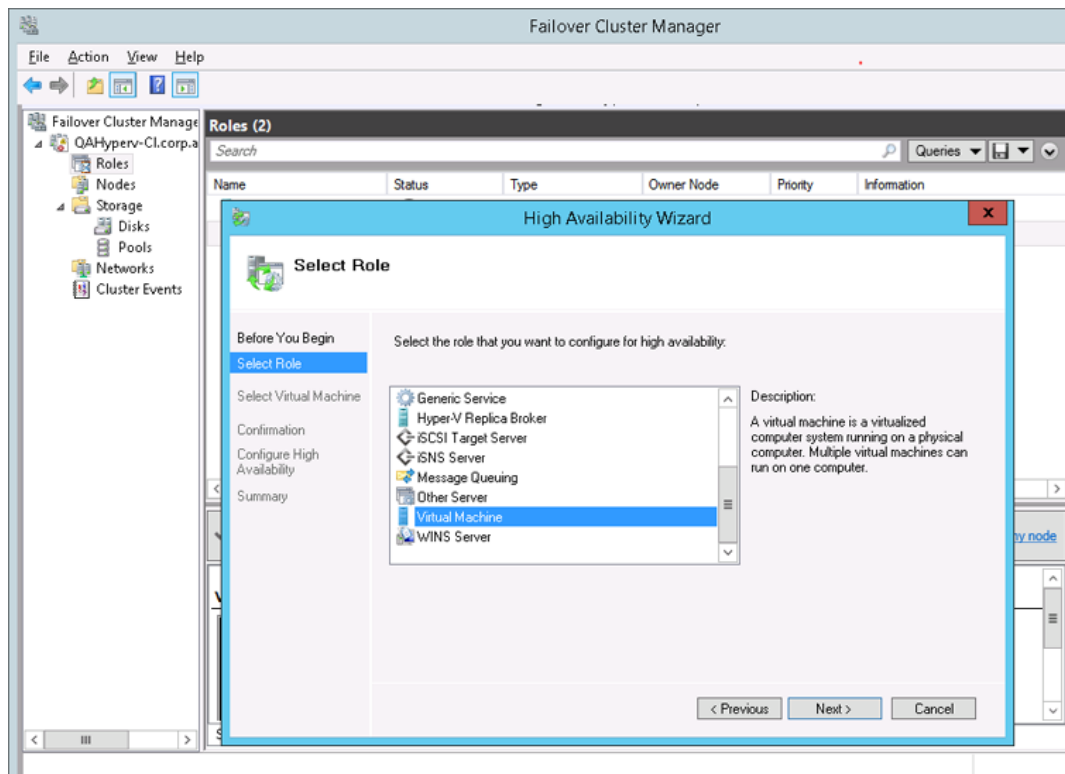
1. Right-click “Roles” and in the pop up menu, choose **Configure Role**:

**Figure 7: Configure Role**



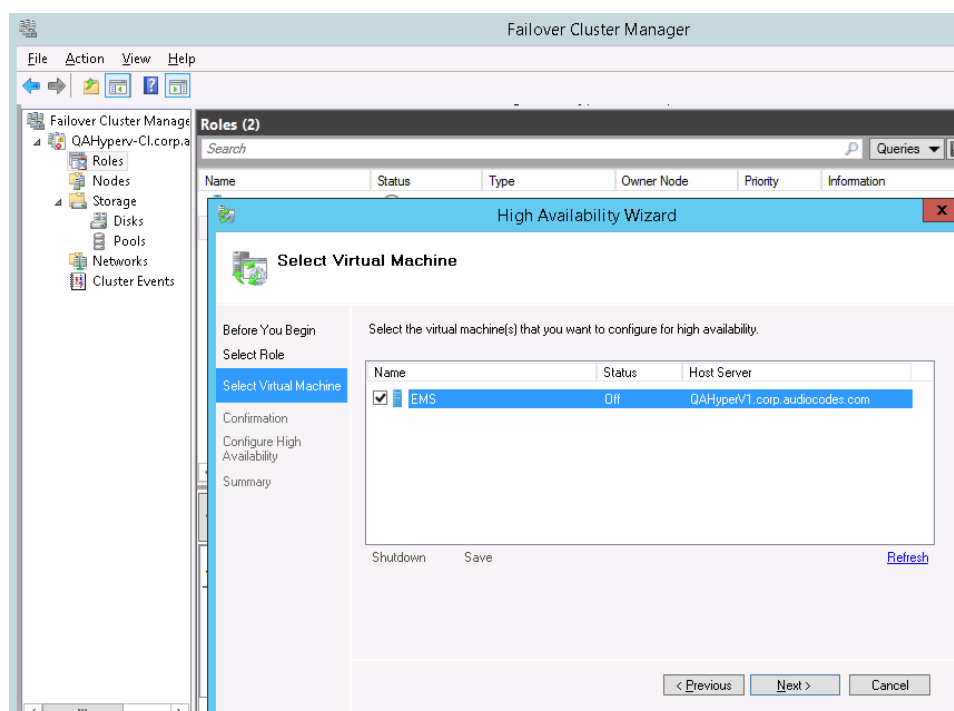
2. In the Select Role window, select the **Virtual Machine** option and then click **Next**.

**Figure 7-37: Choose Virtual Machine**



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

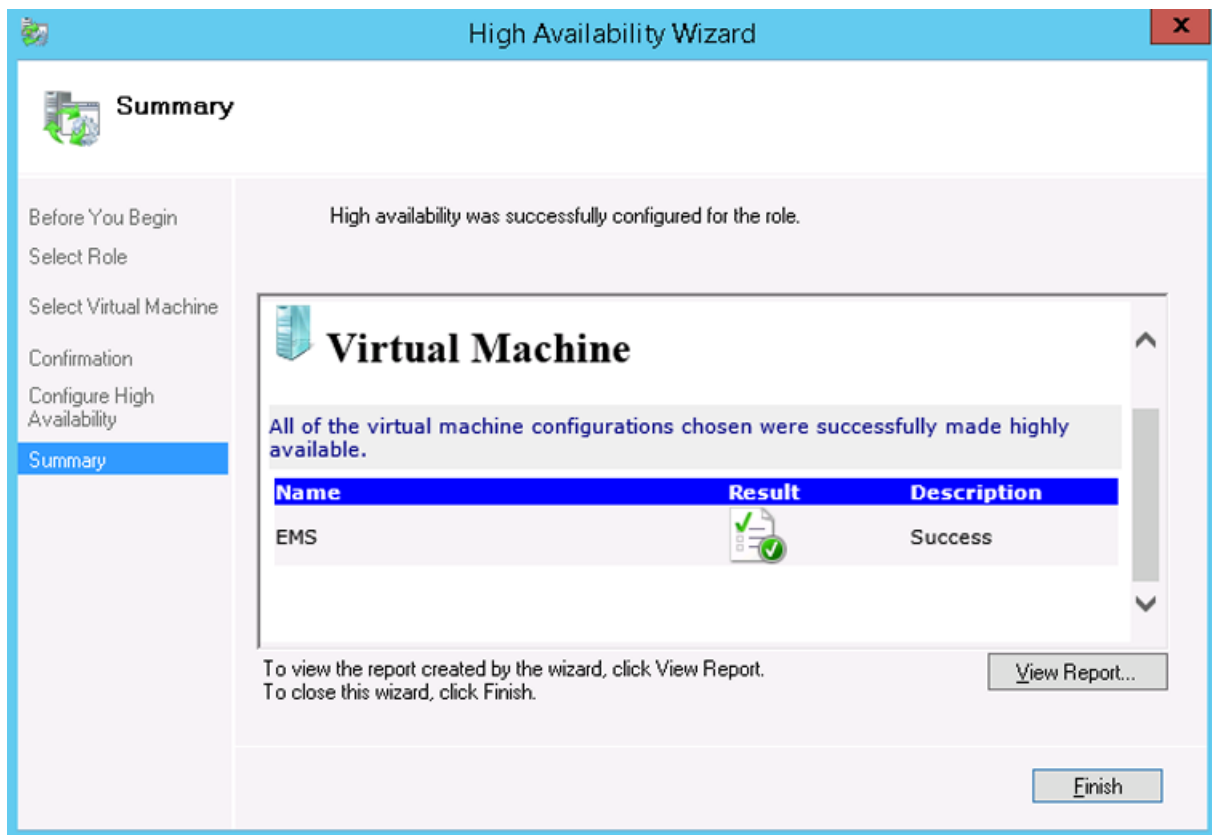
**Figure 7: Confirm Virtual Machine**



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

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

**Figure 7-38: Virtual Machine Successfully Added**



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

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



**Note:** If you wish to manually move the EMS VMs to another cluster node, see Appendix F on page 221.

### 7.2.7.3 Cluster Node Failure

In case an ESXi host node where the VM is running fails, then the VM is restarted on the redundant cluster host node automatically.



**Note:** When one of the cluster hosts fails, the EMS VM is automatically moved to the redundant server host node. During this process, the EMS VM is restarted and consequently any running EMS or SEM processes are dropped. The move process may take several minutes.

# 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 Appendix B on page 195.

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

- For EMS versions 2.2 until version 6.6

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

### 8.1 Upgrading the EMS Server-DVD

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

To upgrade the EMS server on the Linux platform to version 7.0, only DVD3 is required. Verify in the EMS Manager 'General Info' screen that you have installed the latest Linux revision (see Chapter 3 on page 23), see Section 12.3 on page 101. If you have an older OS revision, a clean installation must be performed using all three DVDs (see Section 6.2 on page 37).



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

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

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

```
su - root
```

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

```
mount /misc/cd
```

5. Run the installation script from its location:

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

11. If you have installed user-defined certificates on the EMS client

## 8.2 Upgrading the EMS Server-ISO File

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

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

### ➤ To upgrade using an ISO file:

1. Use SFTP or SCP to copy the iso file to /home/acems in the server
2. Replace "7.0.xxx" in the filename with the relevant version in two of the following commands.

```
mkdir /ins
cp ~acems/EMS_DVD3_7.0.xxx.iso /ins
mkdir /tmp/cd
umount -l /tmp/cd
mount -t iso9660 -o loop,ro /ins/EMS_DVD3_7.0.xxx.iso
/tmp/cd
cd /tmp/cd/EmsServerInstall
```

3. Run the installation script from its location:

```
cd ./install
```

Figure 8-5: 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
```

4. Proceed to step 12.5.5 in Section 8.1.

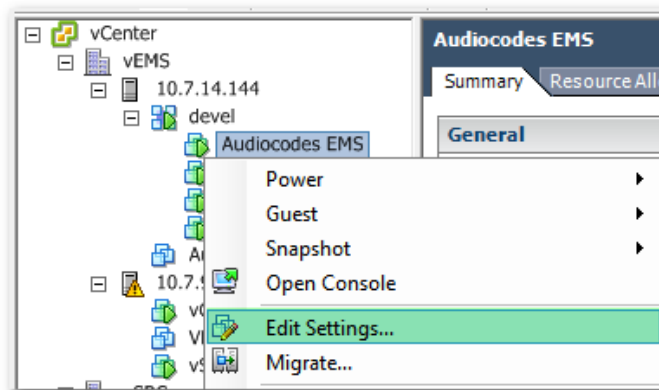
## 9 Upgrading the EMS Server on the VMware Platform

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

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

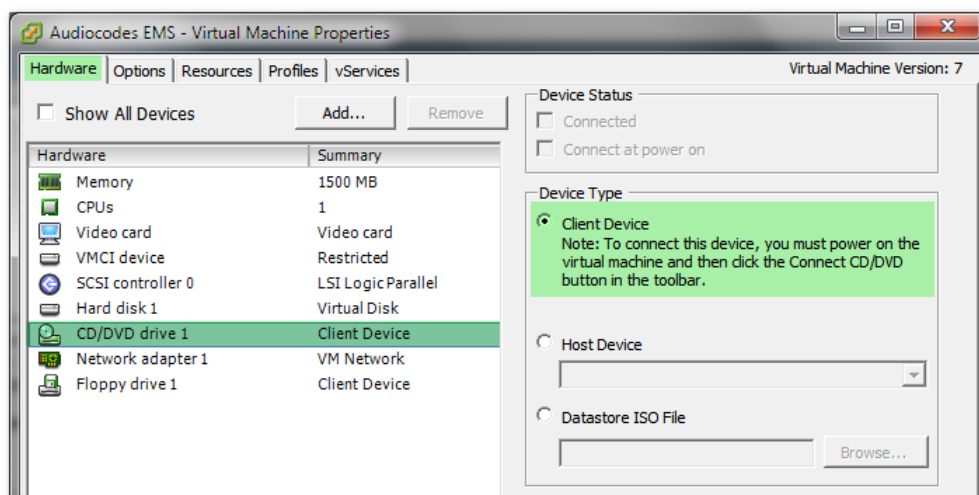
1. Insert the **DVD3-EMS Server Application Installation** into the disk reader on the PC with the installed vSphere client.
2. In the vCenter navigation tree, right-click the AudioCodes EMS node and choose the **Edit Settings** option.

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



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

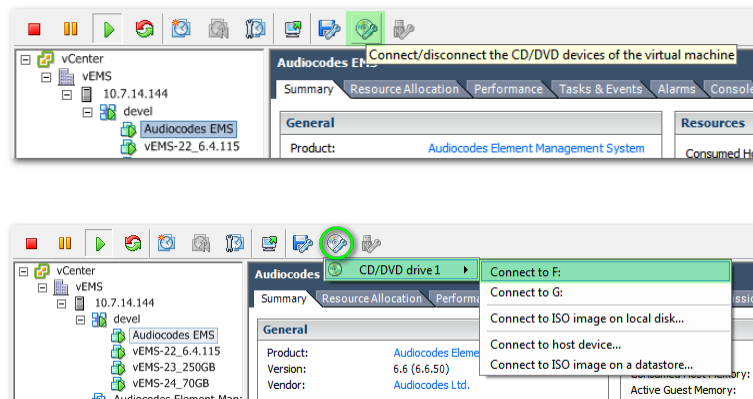
**Figure 9-2: Hardware Tab**



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

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

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



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

```
su -
```

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



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

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

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

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

```
[root@ems-server ~]#  
[root@ems-server ~]# cd /misc/cd/EmsServerInstall/  
[root@ems-server EmsServerInstall]#  
[root@ems-server EmsServerInstall]# ./install  
DIR Name /misc/cd/EmsServerInstall  
Start installValues  
  >>> Start executing User Login Check script at Mon May 21 08:29:59 BST 2012 ...  
Login Check Successfully Passed.  
  
  >>> Check CD Sequence - Mon May 21 08:29:59 BST 2012  
  
  ...  
  >>> >>> PASSED  
  ...  
>>> Verifying OS version - Mon May 21 08:29:59 BST 2012  
  
  ...  
      SOFTWARE EVALUATION LICENSE AGREEMENT  
  
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS SOFTWARE  
EVALUATION AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"  
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE  
AGREEMENT FOR THE AUDIOCODES SOFTWARE (THE "PROGRAM") AND  
THE ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE
```

7. Perform steps 6 to 10 in Section 8.1 on page 81.

# Part IV

## EMS Server Machine Backup and Restore

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





## 10 EMS Server Backup

There are two main backup processes that run on the EMS server:

- **Weekly backup:** runs once a week at a pre-configured date & time (default is Saturday 02:00). In this process, the whole database is backed up into several "RMAN" files that are located in /data/NBIF/emsBackup/RmanBackup directory. In addition, many other configuration and software files are backed up to a TAR file in the /data/NBIF/emsBackup directory. In general, this TAR file contains the entire /data/NBIF directory's content (except 'emsBackup' directory), EMS Software Manager content and server\_XXX directory's content.

To change the weekly backup's time and date, see Section 12.5.3.

- **Daily backup:** runs daily except on the scheduled week day (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.



**Warning:** The Backup process does not backup configurations performed using EMS Server Manager, such as networking and security.

It is highly recommended to maintain all backup files on an external machine.

These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user. These backup files are as follows:

- /data/NBIF/emsBackup/emsServerBackup\_<time&date>.tar file.
- All files in /data/NBIF/emsBackup/RmanBackup directory (including control.ctl and init.ora files)

This page is intentionally left blank.

# 11 EMS Server Restore

This section describes how to restore the EMS server. This can be done on the original machine that the backup files were created from or on any other machine.

**Note:**

- If you're running the restore process on a different machine, its disk size should be the same as the original machine from which the backup files were taken.
- Restore actions can be performed only with backup files which were previously created in the same EMS version.
- If you are restoring to a new machine, make sure that you have purchased a new license file machine ID. AudioCodes customer support will assist you to obtain a new license prior to the restore process.

➤ **To restore the EMS server:**

1. Install (or upgrade) EMS to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.  
For more details, see Chapter 8 on page 81.
2. Use the EMS Server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.  
For more details, see Chapter 12 on page 97.
3. Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
4. Copy all backup files to /data/NBIF directory by SCP or SFTP client using the 'acems' user.
5. In EMS Server Manager, go to the Application Maintenance menu and select the **Restore** option.
6. Follow the instructions during the process. For more details, see Section 12.5.4 on page 108.
7. After the restore process has completed, change the server's IP address using the EMS Server Manager option (Network Configuration > Server IP Address).  
For more details, see Section 12.6.1 on page 112.
8. After changing the server's IP, you will be asked to reboot the machine.
9. If you installed user-defined certificates prior to the restore, you must reinstall these certificates (see Appendix **Error! Reference source not found.**).



**This page is intentionally left blank.**



# Part J

## EMS Server Machine Maintenance

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





## 12 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 through the Linux OS shell. If you perform such actions, EMS application functionality may be harmed.



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

### 12.1 Getting Started with EMS Server Manager

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

#### 12.1.1 Connecting to the EMS Server Manager

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

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

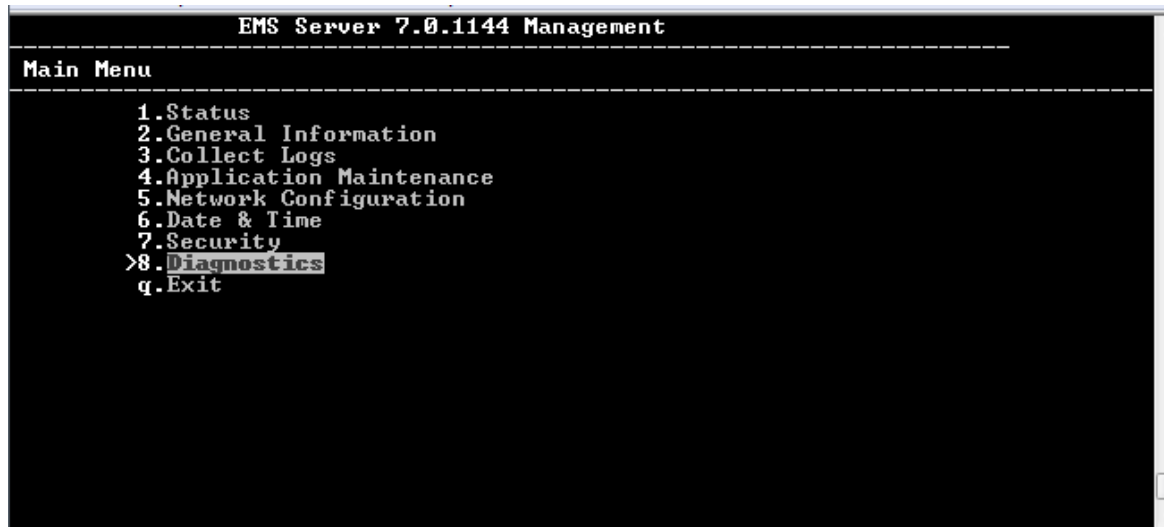
➤ **Do the following:**

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

```
# EmsServerManager
```

The EMS Server Manager menu is displayed:

**Figure 12-1: EMS Server Manager Menu**



**Important:**

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

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

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

- **Status** – Shows the status of current EMS processes (see Section 12.2 on page 100)
- **General Information** – Provides the general EMS server current information from the Linux operating system, including EMS Version, EMS Server Process Status, Oracle Server Status, Apache Server Status, Java Version, Memory size and Time Zone. See Section 12.3 on page 101.
- **Collect Logs** – Collates all important logs into a single compressed file (see Section 12.4 on page 103):
  - General Info
  - Collect Logs
- **Application Maintenance** – Manages system maintenance actions (see Section 12.5 on page 105):
  - SNMP Agent
  - Start / Stop the Application

- Upgrade Application
- Web Servers
- Schedule Automation Backup
- Backup
- Restore
- SEM License Configuration
- Shutdown the EMS server machine
- Reboot the EMS server machine
- **Network Configuration** – Provides all basic, advanced network management and interface updates (see Section 12.6 on page 111):
  - Server's IP Address (Reboot is performed)
  - Ethernet Interfaces (Reboot is performed)
  - Ethernet Redundancy (Reboot is performed)
  - DNS Client
  - NAT
  - Static Routes
  - SNMP Agent
  - SNMPv3 Engine ID
- **Date & Time** – Configures time and date settings (see Section 12.7 on page 126):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (see Section 12.8 on page 130):
  - EMS user
  - SSH Configuration
  - DB Password (EMS Server will be shut down)
  - OS Passwords Settings
  - File Integrity Checker
  - Software Integrity Checker (AIDE) and Prelinking
  - Enable SEM client secured connection
  - Enable EMS4IPPhones client & JAWS secured communication
- **Diagnostics** – Manages system debugging and troubleshooting (see Section 12.8 on page 130):
  - Syslog Configuration
  - Board Syslog Logging Configuration
  - TP Debug Recording Configuration

## 12.1.2 Using the EMS Server Manager

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

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

## 12.2 Status

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

➤ **To view the statuses of the current EMS applications:**

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

**Figure 12-2: Application Status**

```

-----Application-----|---Status---
|   EMS Watchdog         |   UP
|   EMS Server           |   UP
|   SEM Server           |   UP
|   Lync Server          |   UP
|   Tomcat Server        |   UP
|   Apache Server        |   UP
|   Oracle DB            |   UP
|   Oracle Listener      |   UP
|   SNMP Agent           |   DOWN
|   NTP Daemon           |   UP
-----
                                Press 'Enter' key to back to main menu...

```

## 12.3 General Information

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

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

➤ **To view General Information:**

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

**Figure 12-3: General Information**

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

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

Figure 12-4: General Information

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

<more>
-----
Network Configuration
Server's Network:
  Interface      : eth0
  Host Name      : global-logic-2
  IP Address     : 10.4.100.17
  Subnet Mask    : 255.255.0.0
  Network Address : 10.4.0.0
-----
Network Time Protocol
Server #1
Peer:           : *LOCAL(0)
Sync source     : .LOCL.
Stratum:        : 13
Type            : Local
Last response   : 47 seconds ago
Polling interval: 64 seconds
Reach : 377 (all attempts successful)
Delay : 0.000 ms.
Offset : 0.000 ms.
Jitter : 0.001 ms.

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

## 12.4 Collect Logs

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

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

➤ **To collect logs:**

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

**Figure 12-5: EMS Server Manager – Collect Logs**

```
Collecting logs

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

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

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

**Figure 12-6: TAR File Location**

```

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

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

Press Enter to continue

```



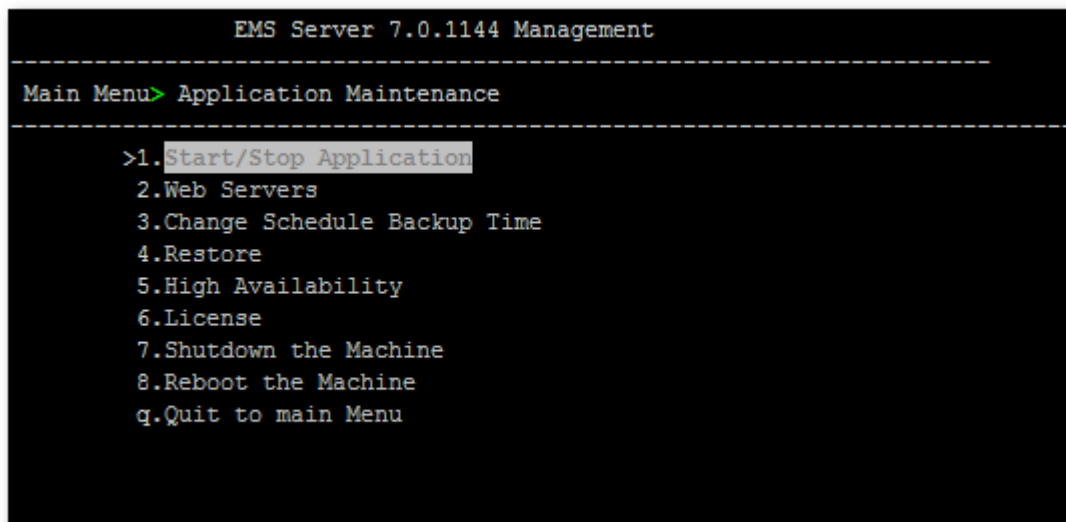
## 12.5 Application Maintenance

This section describes the application maintenance.

➤ **To configure application maintenance:**

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

**Figure 12-7: Application Maintenance**

A screenshot of a terminal window titled "EMS Server 7.0.1144 Management". The window shows a menu structure. At the top, it says "Main Menu> Application Maintenance". Below this, a list of options is displayed: 1. Start/Stop Application (highlighted with a light blue background), 2. Web Servers, 3. Change Schedule Backup Time, 4. Restore, 5. High Availability, 6. License, 7. Shutdown the Machine, 8. Reboot the Machine, and q. Quit to main Menu.

```
EMS Server 7.0.1144 Management
-----
Main Menu> Application Maintenance
-----
>1. Start/Stop Application
  2. Web Servers
  3. Change Schedule Backup Time
  4. Restore
  5. High Availability
  6. License
  7. Shutdown the Machine
  8. Reboot the Machine
  q. Quit to main Menu
```

This menu includes the following options:

- Start/Stop Application (see Section 12.5.1 on page 106).
- Web Servers (see Section 12.5.2 on page 107).
- Change Schedule Backup Time (see Section 12.5.3 on page 108).
- Restore (see Section 12.5.4 on page 108).
- SEM License (see Section 12.5.5 on page 109)
- High Availability (see Chapter 13 on page 159).
- Shutdown the Machine (see Section 12.5.6 on page 110).
- Reboot the Machine (see Section 12.5.7 on page 110).

## 12.5.1 Start /Stop the Application

This section describes how to start or stop the application.

➤ **To start/stop the application:**

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

**Figure 12-8: Start or Stop the EMS Server**



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

## 12.5.2 Web Servers

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

Figure 12-9: – Web Servers

```
EMS Server 7.0.1144 Management
-----
Main Menu> Application Maintenance> Web Servers
-----
!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
b. Back
q. Quit to main Menu
```

➤ **To stop the Apache server:**

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

➤ **To stop the Tomcat server:**

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

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

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

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

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

➤ **To disable JAWS:**

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

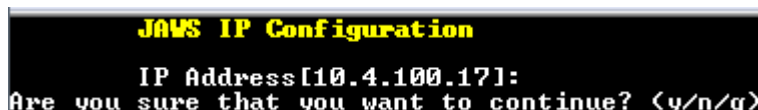
### 12.5.2.1 JAWS IP Configuration

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

➤ **To change the JAWS login interface:**

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

**Figure 12-10: JAWS IP Configuration**



```

JAWS IP Configuration
IP Address[10.4.100.17]:
Are you sure that you want to continue? <y/n/q>
    
```

### 12.5.3 Change Schedule Backup Time

This step describes how to schedule backup time.

➤ **To schedule backup time:**

1. From the Application Maintenance menu, choose **Change Schedule Backup Time**.
2. Choose the day of the week that you wish to perform the backup.
3. Copy all files in /data/NBIF/emsBackup/RmanBackup/ directory to an external machine.
4. Copy /data/NBIF/emsBackup/emsServerBackup\_<time&date>.tar file to an external machine.

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

### 12.5.4 Restore

This step describes how to restore the EMS server.

➤ **To restore the EMS server:**

1. Copy all files that you backed up in Section 12.5.3 to the /home/acems directory on the Restore server. Overwrite existing files if required.
2. From the EMS server Application Maintenance menu, choose **Restore**; a script is started.
3. Follow the instructions; you might need to press Enter a few times.
4. After the restore operation has completed, reboot the EMS server (see Section 12.5.7 on page 110).

### 12.5.5 License

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

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

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

**Figure 12-11: License Configuration Manager**

```
EMS Server 7.0.1144 Management
-----
Main Menu> Application Maintenance> License
-----

License Configuration Manager:
Server Machine ID: 203D6D61D6CE
License Status: ENABLED
SEM Number Of Devices: 64000
SEM Number Of Sessions: 64000
SEM Number Of Users: 0
EMS Number Of IP Phones: 0

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

- The number of devices supported by the SEM is displayed.
  - The number of simultaneous call sessions supported by the SEM is displayed.
  - The number of users supported by the SEM is displayed.
  - The number of IP Phones supported by the SEM is displayed.
2. To load a new license, choose option 1.
  3. Enter the license file path and name.
  4. Restart the EMS server.

## 12.5.6 Shutdown the EMS Server Machine

This section describes how to shutdown the EMS Server machine.

➤ **To shutdown the EMS server machine:**

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

## 12.5.7 Reboot the EMS Server Machine

This section describes how to reboot the EMS server machine.

➤ **To reboot the EMS server machine:**

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

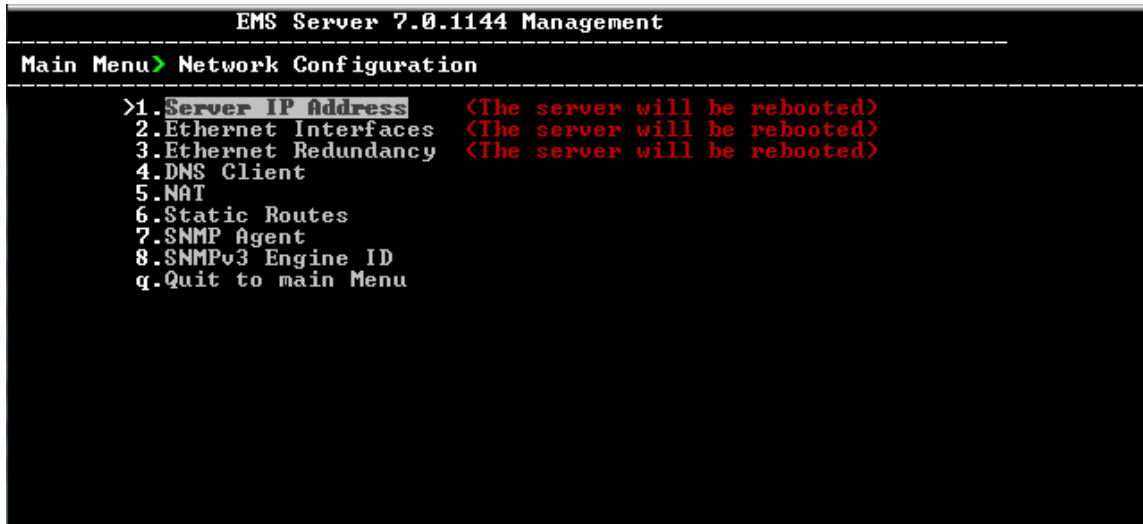
## 12.6 Network Configuration

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

➤ **To run the network configuration:**

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

**Figure 12-12: Network Configuration**



```
EMS Server 7.0.1144 Management
-----
Main Menu> Network Configuration
-----
>1.Server IP Address      <The server will be rebooted>
2.Ethernet Interfaces    <The server will be rebooted>
3.Ethernet Redundancy    <The server will be rebooted>
4.DNS Client
5.NAT
6.Static Routes
7.SNMP Agent
8.SNMPv3 Engine ID
q.Quit to main Menu
```

This menu includes the following options:

- Server's IP address (see Section 12.6.1 on page 112).
- Ethernet Interfaces (see Section 12.6.2 on page 113).
- Ethernet Redundancy (see Section 12.6.3 on page 117).
- DNS Client (see Section 12.6.4 on page 122).
- NAT (see Section 12.6.5 on page 123).
- Static Routes (see Section 12.6.6 on page 124).
- SNMP Agent (see Section 12.6.7 on page 125).
- SNMPv3 Engine ID (see Section 12.6.8 on page 125).

## 12.6.1 Server IP Address

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



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

### ➤ To change Server's IP address:

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

Figure 12-13: EMS Server Manager – Change Server's IP Address

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

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

2. Configure IP configuration parameters as desired.  
Each time you press Enter, the different IP configuration parameters of the EMS server are displayed. These parameters include the Server Host Name, IP address, Subnet Mask, Network Address and Default Gateway.
3. Type **y** to confirm the changes, and then press Enter.

Figure 12-14: IP Configuration Complete

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

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

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

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

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

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

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

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



## 12.6.2 Ethernet Interfaces

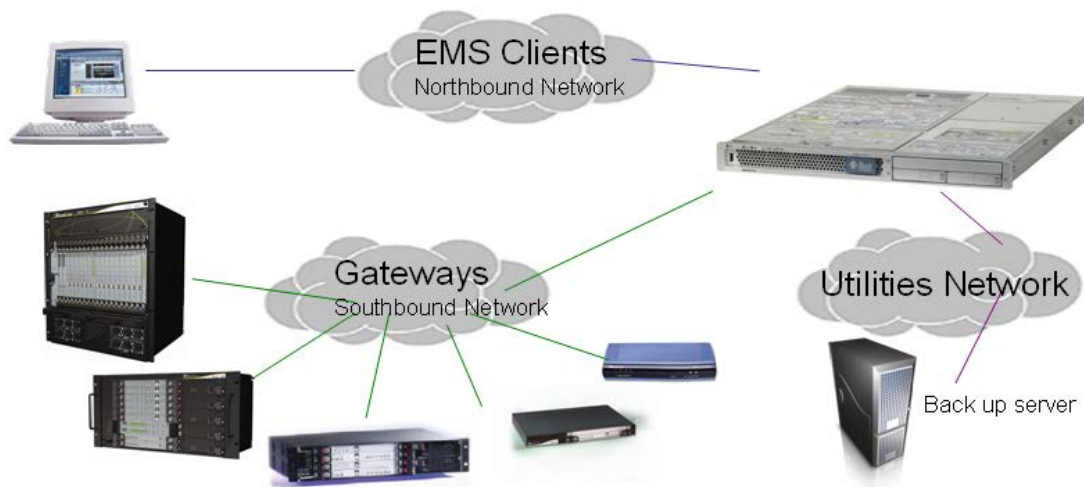
This section describes how to configure ethernet interfaces.

### 12.6.2.1 EMS Client Login on all EMS Server Network Interfaces

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

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

**Figure 12-15: EMS Server: Triple Ethernet Interfaces**



In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound Network' to each one of the subnets. For Static Routes configuration, see Section 12.6.6 on page 124.

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

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

➤ **To configure Ethernet Interfaces:**

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

**Figure 12-16: EMS Server Manager – Configure Ethernet Interfaces**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Network Configuration> Ethernet Interfaces
-----
>1. Add Interface
  2. Remove Interface
  3. Modify Interface
  b. Back
  q. Quit to main Menu
  
```

2. Choose from one of the following options:
  - **Add Interface** – Adds a new interface to the EMS server (see Section 12.6.2.2 on page 115).
  - **Remove Interface** – Removes an existing interface from the EMS server (see Section 12.6.2.3 on page 116).
  - **Modify Interface** – Modifies an existing interface from the EMS server (see Section 3 on page 116).

### 12.6.2.2 Add Interface

This section describes how to add a new interface.

➤ **To add a New Interface:**

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

**Figure 12-9: Add Interface Parameters**

```
Add Interface:

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

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

New Interface Parameters:

IP Address : 10.4.100.55
Hostname : GWs
Subnet Mask : 255.255.0.0

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

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

### 12.6.2.3 Remove Interface

This section describes how to remove an interface.

➤ **To remove an existing interface:**

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

### 12.6.2.4 Modify Interface

This section describes how to modify an existing interface.

➤ **To modify an existing interface:**

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

### 12.6.3 Ethernet Redundancy

This section describes how to configure Ethernet Redundancy.

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

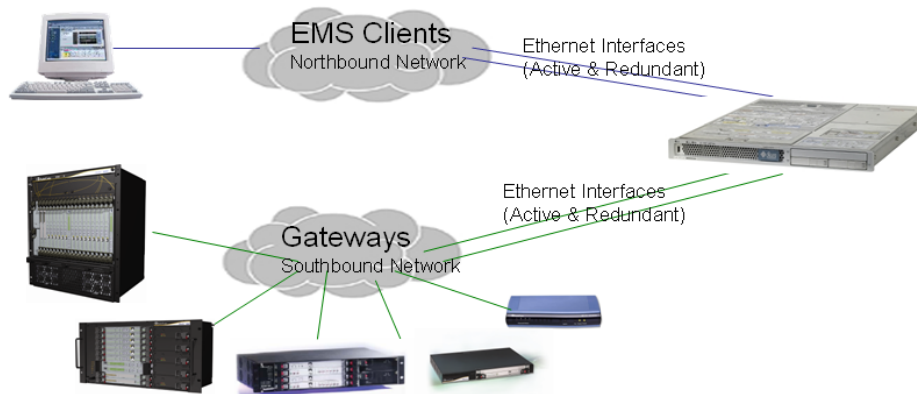
The EMS server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, EMS clients [Northbound] and Gateways [Southbound]).

This option enables you to configure Ethernet ports redundancy.



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

**Figure 12-17: Physical Ethernet Interfaces Redundancy**



➤ **To configure Ethernet Redundancy:**

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

**Figure 12-18: Ethernet Redundancy Configuration**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Network Configuration> Ethernet Redundancy
-----
Interface: eth0
Network: Server's Network
IP Address: 10.3.180.10
Interface: eth1
Not configured
Interface: eth2
Not configured
Interface: eth3
Not configured
>1.Add Redundant Interface
2.Remove Redundant Interface
3.Modify Redundant Interface
b.Back
q.Quit to main Menu

```

2. This menu includes the following options:
  - Add Redundant Interface (see Section 12.6.3.1 on page 118).
  - Remove Redundant Interface (see Section 12.6.3.2 on page 120).
  - Modify Redundant Interface (see Section 12.6.3.3 on page 121).

### 12.6.3.1 Add Redundant Interface

Remove a redundant interface under the following circumstances:

- You have configured an Ethernet interface (see Section 12.6.2 on page 113).
- Your default router can respond to a 'ping' command, due to a heartbeat procedure between interfaces and the default router (to verify activity).

➤ **To add a redundant interface:**

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

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

**Figure 12-19: Add Redundant Interface (Linux)**

```
Ethernet Redundancy Configuration

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

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

Add Redundant Interface:

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

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

Ethernet Redundancy Settings:

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

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

### 12.6.3.2 Remove Ethernet Redundancy

This section describes how to remove an ethernet redundancy interface.

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

1. From the Ethernet Redundancy menu, choose option **2**.
2. Choose the network redundancy to remove.  
The current ethernet redundancy configuration is displayed.
3. Type **y** to confirm the changes; the EMS server automatically reboots for the changes to take effect.

**Figure 12-20: 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

```



### 12.6.3.3 Modify Redundant Interface

This section describes how to modify a redundant interface.

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

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

**Figure 12-21: Modify Redundant Interface (Linux)**

```
Ethernet Redundancy Configuration

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

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

Modify Redundant Interface:

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

Ethernet Redundancy Settings:

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

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

## 12.6.4 DNS Client

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

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

### ➤ To Configure the DNS Client:

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

Figure 12-22: DNS Setup

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

DNS IP Address 1: 10.1.1.10
DNS IP Address 2: 10.1.1.11
DNS IP Address 3: 10.1.1.12

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

Are you sure that you want to continue? <y/n/q> █
```

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

## 12.6.5 NAT

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

➤ **To configure NAT:**

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

➤ **To remove NAT configuration:**

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

## 12.6.6 Static Routes

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

### ➤ To configure static routes:

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

Figure 12-23: Routing Table and Menu

```

EMS Server 7.0.1144 Management
-----
Main Menu> Network Configuration> Static Routes
-----

Static Routes Configuration

Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt  Iface
10.3.0.0         0.0.0.0        255.255.0.0     U       0  0          0     eth0
11.200.0.0       10.3.180.20    255.255.0.0     UG      0  0          0     eth0
169.254.0.0      0.0.0.0        255.255.0.0     U       0  0          0     eth0
0.0.0.0          10.3.0.1       0.0.0.0         UG      0  0          0     eth0
>1.Add Static Route
  2.Remove Static Route
  b.Back
  q.Quit to main Menu

```

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

### ➤ To add a static route:

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

### ➤ To remove a static route:

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

### 12.6.7 SNMP Agent

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

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

➤ **To configure SNMP Agent:**

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

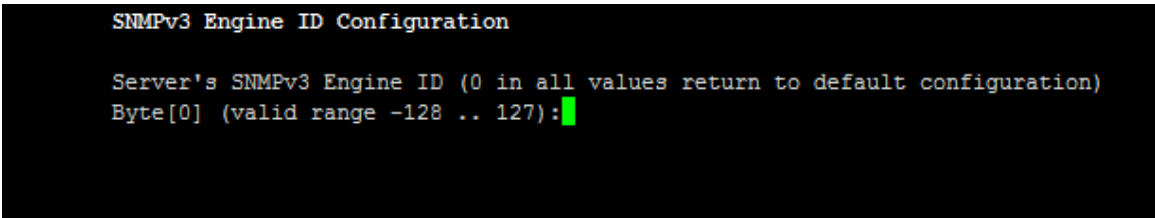
### 12.6.8 Server SNMPv3 Engine ID

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

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

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

**Figure 12-24: EMS Server Manager – Configure SNMPv3 Engine ID**



```
SNMPv3 Engine ID Configuration

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

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

Figure 12-25: SNMPv3 Engine ID Configuration – Complete Configuration

```

SNMPv3 Engine ID Configuration

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

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

```

## 12.7 Date and Time Settings

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

### ➤ To change system time and date:

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

Figure 12-26: EMS Server Manager - Change System Time & Date

```

EMS Server 7.0.1144 Management
-----
Main Menu> Date & Time
-----
>1.NTP
2.Timezone Settings
3.Date & Time Settings
q.Quit to main Menu

```

This menu includes the following options:

- NTP (see Section 12.7.1 on page 127)
- Time Zone Settings (see Section 12.7.2 on page 129)
- Date & Time Settings (see Section 12.7.3 on page 129)

## 12.7.1 NTP

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

This option enables you to configure the EMS server to obtain its clock from an external NTP clock source and in addition this enables other devices that are connected to the EMS server in the IP network to synchronize with this clock source. 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 in the IP network to synchronize their clocks according to the EMS server clock.



### Notes:

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

### ➤ To configure NTP:

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

Figure 12-27: EMS Server Manager - Configure NTP

```

EMS Server 7.0.1144 Management
-----
Main Menu> Date & Time> NTP
-----
Current NTP status: ON
Allow/Restrict access to NTP clients: Allow

=====
remote      refid      st t when poll reach  delay  offset  jitter
=====
bzq-218-194-48. .RMOT.    16 u   - 1024    0    0.000    0.000    0.000
ntp-v6.laika.pa .INIT.    16 u   - 1024    0    0.000    0.000    0.000
*LOCAL(0)     .LOCL.    10 l   41    64   377    0.000    0.000    0.001
=====
>1. Configure NTP
2. Stop NTP
3. Restrict access to NTP clients
4. Activate DDoS protection
5. Add authorized subnet of devices to sync by NTP
6. Remove authorized subnet of devices from NTP rules
b. Back
q. Quit to main Menu

```

2. From the NTP menu, choose option **1** to configure NTP.

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

### 12.7.1.1 Stopping and Starting the NTP Server

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

#### ➤ To start NTP services:

- From the NTP menu, choose option **2**, and then choose one of the following options:

- If NTP Service is on: **Stop NTP**
- If NTP Service is off: **Start NTP**

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

### 12.7.1.2 Restrict Access to NTP Clients

This section describes how to restrict access to NTP clients.

#### ➤ To allow access to NTP clients:

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



## 12.7.2 Time Zone Settings

This option enables you to change the time zone of the EMS server.

➤ **To change the system time zone:**

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

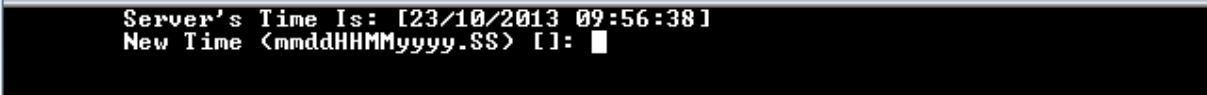
## 12.7.3 Date and Time

This option enables you to set the date and time.

➤ **To set the date and time:**

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

**Figure 12-28: Change System Time and Date Prompt**



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

2. Enter the new time as shown in the following example:  
mmddHHMMyyyy.SS : month(08),day(16),Hour(16),Minute(08),year(2007),"."  
Second.

## 12.8 Security

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

➤ **To configure security settings:**

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

**Figure 12-29: Security Settings**

```

EMS Server 7.0.1164 Management
-----
Main Menu> Security
-----
>1.Add EMS User
2.SSH
3.DB Password (EMS & SEM applications will be stopped)
4.OS Users Passwords
5.File Integrity Checker
6.Software Integrity Checker (AIDE) and Prelinking
7.USB Storage
8.Network options
9.Audit Agent Options (The server will be rebooted)
10.Enable SEM client secured communication
11.Enable EMS4IPPhones client & JAWS secured communication
q.Quit to main Menu

```

This menu includes the following options:

- Add EMS User (see Section 12.8.1 on page 131).
- SSH Server Configuration Manager (see Section 12.8.2 on page 125).
- DB Password (see Section 12.8.3 on page 145).
- OS Password Settings (see Section 12.8.4 on page 145).
- Start / Stop File Integrity Checker (see Section 12.8.5 on page 149).
- Software Integrity Checker (AIDE) and Prelinking (see Section 12.8.6 on page 149).
- USB Storage (see Section 12.8.7 on page 150).
- Network options (see Section 12.8.8 on page 151).
- Audit Agent Options (see Section 12.8.9 on page 151).
- Enable SEM client secured connection (see Section 12.8.10 on page 152)
- Enable EMS4IPPhones client & JAWS secured communication (see Section 12.8.11 on page 152).

## 12.8.1 Add EMS User

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

➤ **To add an EMS user:**

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



**Note:** Note and retain these passwords for future access.

## 12.8.2 SSH Server Configuration Manager

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

➤ **To configure SSH:**

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

**Figure 12-30: SSH Configuration**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH
-----
>1.Configure SSH Log Level
2.Configure SSH Banner
3.Configure SSH on Ethernet Interfaces
4.Disable SSH Password Authentication
5.Enable SSH IgnoreUserKnownHosts parameter
6.Configure SSH Allowed Hosts
b.Back
q.Quit to main Menu

```

This menu includes the following options:

- Configure SSH Log Level (see Section [12.8.2.1](#) on page [133](#)).
- Configure SSH Banner (see Section [12.8.2.2](#) on page [134](#)).
- Configure SSH on Ethernet Interfaces (see Section [12.8.2.3](#) on page [135](#)).
- Disable SSH Password Authentication (see Section [12.8.2.4](#) on page [138](#)).
- Enable SSH Ignore User Known Hosts Parameter (see Section [12.8.2.5](#) on page [139](#)).
- Configure SSH Allowed Hosts (see Section [12.8.2.6](#) on page [140](#)).

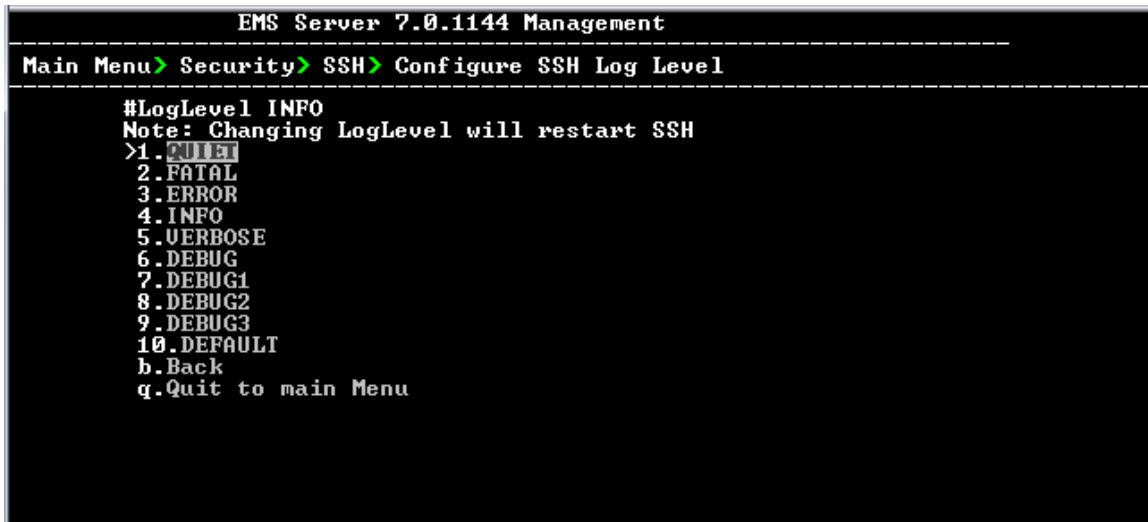
### 12.8.2.1 SSH Log Level

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

➤ **To configure the SSH Log Level:**

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

**Figure 12-31: SSH Log Level Manager**



```
EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH Log Level
-----
#LogLevel INFO
Note: Changing LogLevel will restart SSH
>1. QUIET
2. FATAL
3. ERROR
4. INFO
5. VERBOSE
6. DEBUG
7. DEBUG1
8. DEBUG2
9. DEBUG3
10. DEFAULT
b. Back
q. Quit to main Menu
```

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press Enter.  
The SSH daemon restarts automatically.  
The Log Level status is updated on the screen to the configured value.

### 12.8.2.2 SSH Banner

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

➤ To configure the SSH banner:

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

Figure 12-32: SSH Banner Manager

```

EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH Banner
-----
Current Banner State: DISABLED
To change SSH Banner, please, change /etc/issue file.
Note: Changing Banner state will restart SSH

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

2. Edit a '/etc/issue' file with the desired text.
3. Choose option **1** to enable or disable the SSH banner.  
Whenever you change the banner state, SSH is restarted.  
The 'Current Banner State' is displayed in the screen.

### 12.8.2.3 SSH on Ethernet Interfaces

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

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

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

**Figure 12-33: Configure SSH on Ethernet Interfaces**

```

-----
EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH on Ethernet Interfaces
-----
Ethernet Interfaces - SSH Manager:
SSH Listener Statuses:
  ALL - SSH enabled on all the Interfaces
  Yes - SSH enabled on specific Interface
  No  - SSH disabled on specific Interface

Interface : SSH Listener Status : IP Address      : Host Name
eth0      : ALL                  : 10.3.180.10   : G8-EMS10
>1.Add SSH to All Ethernet Interfaces
2.Add SSH to Ethernet Interface
3.Remove SSH from Ethernet Interface
b.Back
q.Quit to main Menu

```

This menu includes the following options:

- Add SSH to All Ethernet Interfaces (see Section [12.8.2.3.1](#) on page [136](#)).
- Add SSH to Ethernet Interface (see Section [12.8.2.3.2](#) on page [137](#)).
- Remove SSH from Ethernet Interface (see Section [12.8.2.3.3](#) on page [137](#)).

#### 12.8.2.3.1 **Add SSH to All Ethernet Interfaces**

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

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

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

The SSH daemon restarts automatically to update this configuration action.

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



### 12.8.2.3.2 Add SSH to Ethernet Interface

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

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

1. From the Configure SSH on Ethernet Interfaces menu, choose option **2**, and then press Enter.  
After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.
2. Enter the appropriate interface number, and then press Enter.  
The SSH daemon restarts automatically to update this configuration action.  
The column 'SSH Listener Status' displays 'YES' for the configured interface.

### 12.8.2.3.3 Remove SSH from Ethernet Interface

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

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

1. From the Configure SSH on Ethernet Interfaces menu, choose option **3**, and then press Enter.  
All the interfaces to which SSH access is currently enabled are displayed.
2. Enter the desired interface number, and then press Enter.  
The SSH daemon restarts automatically to update this configuration action.  
The column 'SSH Listener Status' displays 'No' for the denied interface.



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

#### 12.8.2.4 Enable/Disable SSH Password Authentication

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

➤ **To disable SSH Password Authentication:**

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

**Figure 12-34: Disable Password Authentication**

```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.

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

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

The SSH daemon restarts automatically to update this configuration action.



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

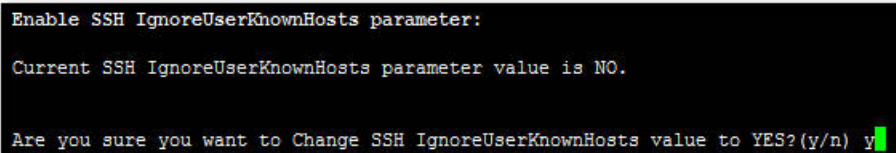
### 12.8.2.5 Enable SSH IgnoreUserKnownHosts Parameter

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

➤ **To enable SSH IgnoreUserKnownHosts parameter:**

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

**Figure 12-35: 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** to change this parameter value to either 'YES' or 'NO' or type **n** to leave as is, and then press Enter.

### 12.8.2.6 SSH Allowed Hosts

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

➤ **To Configure SSH Allowed Hosts:**

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

**Figure 12-36: Configure SSH Allowed Hosts**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----
SSH Allowed for ALL Hosts.
>1.Deny ALL Hosts
  2.Add Host/Subnet to Allowed Hosts
  b.Back
  q.Quit to main Menu
  
```

This menu includes the following options:

- Allow ALL Hosts (see Section [12.8.2.6.1](#) on page [141](#)).
- Deny ALL Hosts (see Section [12.8.2.6.2](#) on page [141](#)).
- Add Host/Subnet to Allowed Hosts (see Section [12.8.2.6.3](#) on page [142](#)).
- Remove Host/Subnet from Allowed Hosts (see Section [12.8.2.6.4](#) on page [144](#)).

### 12.8.2.6.1 Allow ALL Hosts

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

➤ **To allow ALL Hosts:**

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter.
2. Type **y** to confirm, and then press Enter.  
The appropriate status is displayed in the screen.

### 12.8.2.6.2 Deny ALL Hosts

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

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

1. From the Configure SSH Allowed Hosts menu, choose option **2**, and then press Enter.
2. Type **y** to confirm, and then press Enter.  
The appropriate status is displayed in the screen.



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

### 12.8.2.6.3 Add Hosts to Allowed Hosts

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

#### ➤ To add Hosts to Allowed Hosts:

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

**Figure 12-37: Add Host/Subnet to Allowed Hosts**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allowed Hosts
-----
>1.Add IP Address <x.x.x.x>
2.Add Subnet <n.n.n.n/m.m.m.m - network/netmask>
3.Add Host Name <without "/" or "," characters>
b.Back
q.Quit to main Menu

```

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



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

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

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

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

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

Figure 12-38: Add Host/Subnet to Allowed Hosts-Configured Host

```
EMS Server 7.0.1144 Management
-----
Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----
Current Allowed Hosts/Subnets:

IP Addresses:
10.13.22.3

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

#### 12.8.2.6.4 Remove Host/Subnet from Allowed Hosts

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

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

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

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



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



### 12.8.3 DB Password

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

➤ **To change the DB Password:**

1. From the Security menu, choose **DB Password**, and then press Enter; the EMS server is rebooted.
2. Press Enter until the New Password prompt is displayed.

**Figure 12-39: EMS Server Manager – Change DB Password**

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

*****
Oracle Change password Script start
*****

User name:
EMSADMIN
Current Password:
*****
New Password:  <Password should contain at least one digit, one character and one punctuation>

```

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



**Notes:**

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

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

### 12.8.4 OS Passwords Settings

This section describes how to change the OS password settings.

➤ **To change OS passwords:**

1. From the Security menu, choose **OS Users Passwords**, and then press Enter. Proceed to one of the following procedures:
  - General Password Settings (see Section 12.8.4.1 on page 146.
  - Operating System User Security Extensions (see Section 12.8.4.2 on page 147).

### 12.8.4.1 General Password Settings

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

➤ **To modify general password settings:**

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

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

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

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

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

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

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

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

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

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

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

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



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

### 12.8.4.2 Operating System Users Security Extensions

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

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

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure in [Figure 12-40](#)).

➤ **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 12-40: 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 12-41: Maximum Active SSH Sessions**

```

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

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

```



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

### 12.8.5 Start / Stop File Integrity Checker

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

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

### 12.8.6 Start/Stop Software Integrity Checker (AIDE) and Pre-linking

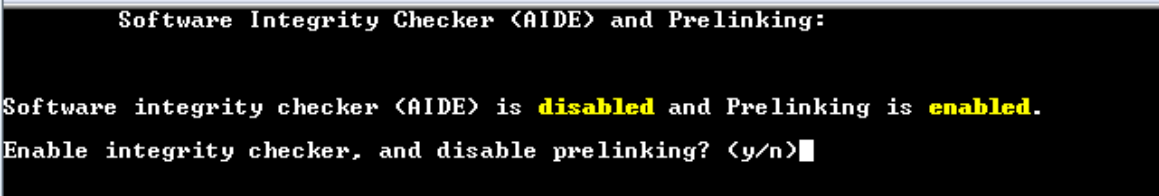
AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

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

➤ **To start AIDE and disable pre-linking:**

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

**Figure 12-42: Software Integrity Checker (AIDE) and Pre-linking**



```
Software Integrity Checker <AIDE> and Prelinking:

Software integrity checker <AIDE> is disabled and Prelinking is enabled.
Enable integrity checker, and disable prelinking? <y/n>■
```

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

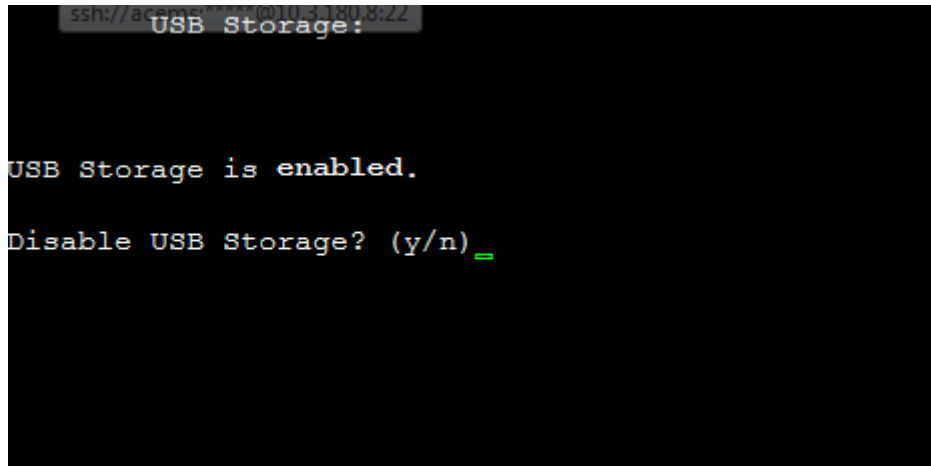
## 12.8.7 USB Storage

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

➤ **To enable USB storage:**

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

**Figure 12-43: USB Storage**



2. Enable or disable USB storage as required.

## 12.8.8 Network Options

This menu option provides several items to enhance network security.

➤ **To enable network options:**

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

**Figure 12-44: Network Options**

```

EMS Server 7.0.1144 Management
-----
Main Menu> Security> Network options
-----
!Log packets with impossible addresses to kernel log: DISABLED
!Ignore all ICMP ECHO requests: DISABLED
!Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
!Send ICMP redirect messages: DISABLED
!Accept ICMP redirect messages: DISABLED
>1.Enable log packets with impossible addresses to kernel log
2.Enable ignore all ICMP ECHO requests
3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
4.Enable send ICMP redirect messages
5.Enable accept ICMP redirect messages
b.Back
q.Quit to main Menu

```

2. Set the required network options.

## 12.8.9 Auditd Options

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

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

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

**Figure 12-45: Auditd Options**

```

Auditd Options:

Not using STIG recommendations for auditd

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

```

2. Enable or disable Auditd options as required.

### 12.8.10 Enable SEM Client Secured Connection

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

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

- From the Security menu, choose **Enable SEM Client Secured Connection**; the connection is secured.

### 12.8.11 Enable EMS4IPPhones Client and JAWS Secured Communication

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

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

- From the Security menu, choose **EMS4IPPhones client & JAWS Secured Communication**; the connection is secured.



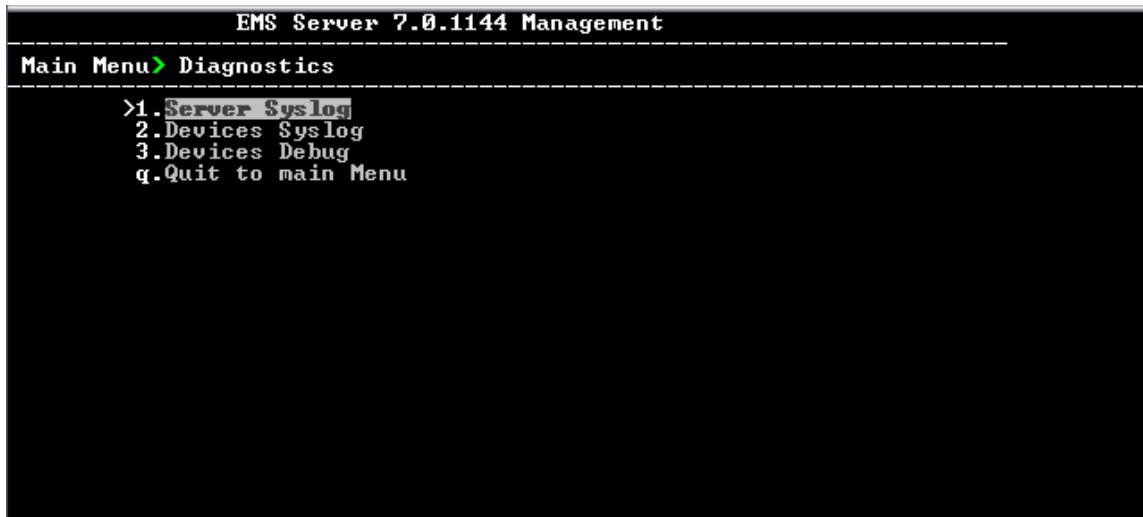
## 12.9 Diagnostics

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

➤ **To run EMS Server diagnostics:**

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

**Figure 12-46: Diagnostics**



This menu includes the following options:

- Syslog Configuration (see Section 12.9.1 on page 155).
- Board Syslog Logging Configuration (see Section 12.9.2 on page 155).
- TP Debug Recording Configuration (see Section 12.9.3 on page 156).

### 12.9.1 Syslog Configuration

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

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

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

Figure 12-47: Syslog Configuration

```

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

Send EMERG events to system console ? <y/n> y
Logging of many events on console when RS-232 console is used may cause severe p
erformance degradation <due to 9600 baud rate>.
Are you sure ? <y/n>

```

Figure 12-48: Forward Messages to an External Server

```

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

```

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

## 12.9.2 Board Syslog Logging Configuration

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



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

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the EMS server machine.

The syslog log file 'syslog' is located in the following EMS server directory:

/data/NBIF/mgDebug/syslog

The syslog file is automatically rotated once a week or when it reaches 100 MB. Up to four syslog files are stored.

### ➤ To enable device syslog logging:

1. From the Diagnostics menu, choose **Devices Syslog**, and then press Enter.
2. You are prompted whether you wish to send EMER events to system console; type **Y** or **N**.
3. You are prompted whether you wish to send events to an external server; type **Y** or **N**.

## 12.9.3 TP Debug Recording Configuration

Debug recordings packets from all managed machines can be logged directly to the EMS server without the need for a 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 through FTP.

The EMS Server Manager is used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the EMS server IP.

The DR capture file is located in the following EMS server directory:

/data/NBIF/mgDebug/DebugRecording

The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close i.e. if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the EMS server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

### ➤ To enable or disable TP Debug Recording:

1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.  
A message is displayed indicating that debug recording is either enabled or disabled.
2. Type **y**, and then press Enter.  
Recording files are saved in /data/NBIF/mgDebug directory on the server.



**Note:** It is highly recommended to disable the 'TP Debug Recording' feature when you have completed recording because this feature heavily utilizes system resources.

# Part V=

## HA (High Availability)

This section describes the EMS HA Configuration options.



## 13 Getting Started with HA (High Availability)

**EMS servers High Availability** is supported for EMS server applications running on the Linux platform.

Two EMS server machines are required to support High Availability: one machine serving as the Primary machine and the other serving as the Secondary machine. When the EMS application is active and running, all data stored in the EMS server machine and database is replicated from the Primary machine to the Secondary machine. Upon Primary machine failure recognition (either on the EMS application or on the Network), activity is automatically transferred from the Primary server machine to the Secondary server machine.

Two models of High Availability are supported:

- Both EMS servers are located in the same subnet. There is a single EMS server IP address - Global (Virtual) IP address defined for all the Network Components (EMS clients and Managed Gateways). Each of the EMS server machines has an internal Private IP address and the active EMS server machine performs binding to the Global (Virtual) IP address. This setup currently does not support working with gateways behind a NAT.
- Each one of the EMS servers is located in a different network subnet and has its own IP address. During the EMS client login dialog, the user should provision both IP addresses (Geo HA), and the EMS client application will constantly search for the currently active EMS server machine. All the managed gateways relevant applications (such as Trap Sending, NTP Server, and OCSP Server) should be aware of two possible EMS server machine addresses.

The HA Configuration menu option enables you to configure EMS server machines high availability, perform HA-related actions and review the HA status for both servers.

Prior to configuring HA, both machines should be installed with an identical EMS server version and an identical operating system and network configuration.

## 13.1 EMS HA Pre-requisites

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

- Both servers have identical hardware. See EMS Server and Client Requirements section for supported machines (see Section 3 on page 23).
- An identical Linux OS is installed on both servers.
- An identical EMS version is installed on both servers.
- An identical database password should be configured on both servers.
- An identical interface configuration and the same subnets are connected to each server (N/A for Geo HA).
- An identical redundancy configuration on identical interfaces.
- The EMS application is down (use the EMS Server Manager to shut down the EMS application).
- SSH communication between the Secondary and the Primary servers exists.
- Network Bandwidth requirements between two EMS servers are as follows:
  - Initial Synchronization process: at least 80 Mbps  
During the initial sync process, the entire /data partition is synchronized between the active and redundant servers. This partition size is 63GB on HP DL360 G6 servers and 900GB on HP DL360p G8 servers. A network speed of at least 80 Mbps is required to complete the initial sync process in up to 2 hours on G6 servers and 4 hours on G8 servers.  
Assuming a slower network, the process will take longer. For example, on G6 servers:
    - ◆ 20 Mbps -> 7 hours
    - ◆ 10 Mbps -> 14 hours
  - Ongoing server Synchronization: 10 Mbps.
  - Ping between two servers: the ping time between each EMS server machine should not exceed 200 msec.
- During the HA configuration process, entire /data partition is duplicated from the primary server to the secondary server. If any of the servers contain previous backup files, these files are deleted on the secondary server. These files should be backed up on an external storage machine prior to the HA configuration.
- If you are using user-defined certificates (see Appendix [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)), they must be preinstalled on both primary and secondary machines before commencing the HA process.



## 13.2 EMS HA Data Synchronization

The data synchronization is performed using a distributed replicated block device for the Linux operating system. This process allows a real-time mirror of the local block devices on a remote machine.

The replicated EMS data includes the following:

- EMS Database
- EMS NBIF files including the following:
  - Backup files
  - Alarms files
  - Topology files
  - Performance files
  - MG backup files
  - Debug recording
- EMS Software files (EMS Software Manager files)
  - MG configuration files, for upgrade and management
  - MG Auxiliary files

The initial synchronization time between two EMS server machines is estimated at 1.5-4 hours, depending on network speed/quality and servers' disk size.

### 13.2.1 Replicate EMS Server Manager Actions

Any actions performed using the EMS Server Manager prior to the HA configuration should be manually updated on both EMS server machines. EMS Server Manager actions are logged in the following file:

```
/var/log/ems/EmsServerManager.txt
```



**Note:** The EMS HA process does not automatically replicate actions executed using the EMS Server Manager on the primary server to the secondary server.

## 13.3 EMS Server Manager

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

The EMS Server Manager displays dynamic menus. Each menu is displayed differently according to the current server's state.

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

- Start/Stop Application
- Change Server's IP Address
- Configure Ethernet Interfaces
- Configure Ethernet Redundancy
- Configure NAT

- Restore the EMS Server
- DB Password

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

- Start/Stop Application
- Change Server's IP Address
- Configure Ethernet Interfaces
- Configure Ethernet Redundancy
- Configure NAT
- Add EMS User
- Restore the EMS Server
- DB Password

In some cases, the menu will only be updated after running EMS Server Manager again. For instance, after HA installation, the “Start/Stop EMS Server” option is hidden after exiting the EMS Server Manager and running it again.

## 13.4 EMS Client

Once the switchover has successfully completed, the EMS client logs in again to the active server and a “Server Startup” alarm is displayed.

## 13.5 EMS Server Upgrade

EMS server version upgrade cannot be performed while HA is configured.

To upgrade the servers, HA must be uninstalled prior to the upgrade.

It is recommended to firstly uninstall the secondary server, and then the primary server.

- To uninstall HA, see Section [14.6](#) on page [174](#).
- To upgrade the EMS server, see Section [8.1](#) on page [81](#).

## 13.6 EMS Server Restore

EMS server restore cannot be performed while HA is configured.

To restore the EMS server, HA must be uninstalled prior to the restore.

It is recommended to firstly uninstall the secondary server, and only then the primary server. After restoring the server, HA should be reconfigured.

To uninstall HA, see Section [14.6](#) on page [174](#).

## 14 EMS HA Configuration

This section describes the EMS HA Installation.

➤ **To configure the primary server:**

1. In the EMS Server Manager root menu, choose **Application Maintenance**, in the sub-menu, choose **High Availability**, and then press Enter; the following is displayed:

**Figure 14-1: EMS Server Manager - HA Configuration**

A screenshot of a terminal window showing the EMS Server Manager interface. The title bar reads "EMS Server 7.0.1144 Management". The main menu path is "Main Menu>Application maintenance>High Availability". Below this, a list of options is displayed: "1. Configure Server As Primary", "2. Configure Server As Secondary", "3. HA Status", "4. Back", and "5. Back to main Menu". The first option, "1. Configure Server As Primary", is highlighted with a green cursor.

```
EMS Server 7.0.1144 Management
-----
Main Menu>Application maintenance>High Availability
-----
>1. Configure Server As Primary
2. Configure Server As Secondary
3. HA Status
4. Back
5. Back to main Menu
```

This menu includes the following options:

- Primary Server Installation in Global IP Model (see Section 14.1 on page 164).
- Primary Server Installation in in Geo HA model (see Section 14.2 on page 166).
- Secondary Server Installation (see Section 14.3 on page 166).
- HA Status (see Section 14.4 on page 170).

## 14.1 Primary Server HA Installation in Global IP Model

This section describes how to install the HA application on the designated Primary server in the Global IP address model.



**Note:** When alarms are forwarded from the EMS, you can configure the global IP address as a source address. For more information, refer to the *EMS User's Manual*.

➤ **To install the HA primary server in Global IP Model:**

1. In the High Availability menu, choose option **1** to run the Primary server HA installation, and then press Enter.
2. After the HA packages are installed, you are prompted for the HA model:

**Figure 14-2: Primary HA Server Menu**

```
High Availability Menu
 1 ) Configure Global IP HA
 2 ) Configure Geo-Redundancy HA
 3 ) Back to Main Menu
Choose: 1
```

For the Global IP HA model, both EMS servers are located in the same subnet.

3. In the High Availability sub-menu, choose option **1 (Configure Global IP HA)**.
4. You are now prompted for the following network parameters:
  - 'Global IP' for each configured interface (physical or logical IF).
  - Secondary server's Host name and IP address.
  - Ping Nodes - If you have several interfaces configured, you can add another 'ping node' (for more information, see Section 14.2.1 on page 168).

**Figure 14-3: Primary HA Server Sub-menu**

```
Start Heartbeat Configuration
Primary Server IP: 10.7.14.141
Primary Server Host: EMS-Linux141
Global IP for eth0[-1]: 10.7.14.218
Secondary Server IP [-1]: 10.7.14.142
Secondary Server Host [-1]: EMS-Linux142
Ping IP [-1]: 10.7.0.1
Do you want to add another ping ip ? (y/n)
```

The current configuration is displayed for confirmation:

**Figure 14-4: HA Configuration Display**

```
HA Configuration:
  Global IP(eth0):  10.7.14.218
  Primary Server IP: 10.7.14.141
  Primary Server Host: EMS-Linux141
  Secondary Server IP: 10.7.14.142
  Secondary Server Host: EMS-Linux142
  Ping IP: 10.7.0.1
Are you sure that you want to continue ? (y/n/q)
```

- Type **y** to continue the installation process
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- “/data: device is busy” – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing.** In the case where the /data partition isn’t busy, the above message is not displayed.
- When prompted, press Enter to continue.
- When prompted “To abort waiting type 'yes' [1]:” – you can wait or press 'yes' to continue.

When the installation process for the Primary server has completed, the following message is displayed:

**Figure 14-5: HA Server Configured as Primary Server - Confirmation**

```
Server Configured As Primary
***** HA configuration finished *****
```



**Note:** After the installation process has completed, it takes several minutes until the HA status changes to “Online” and the EMS server status changes to 'EMS server is running'.

## 14.2 Primary Server HA Installation in Geo HA Model

This section describes how to install the HA application on the designated Primary server in the Geo HA model.

➤ **To install the HA primary server in Geo HA model:**

1. In the High Availability menu, choose option **1** to run the Primary server HA installation, and then press Enter.
2. After the HA packages are installed, you are prompted for the HA model:

**Figure 14-6: Primary HA Server Menu**

```
High Availability Menu
 1 ) Configure Global IP HA
 2 ) Configure Geo-Redundancy HA
 3 ) Back to Main Menu
Choose: 2
```

For the Geo HA model, EMS servers are located in different subnets.

3. In the High Availability sub-menu, choose option **2 (Configure Geo-Redundancy HA)**.
4. You are now prompted for the following network parameters:
  - Secondary server's Host name and IP address.
  - Ping Nodes - If you have several interfaces configured, you can add another 'ping node' (for more information, see Section 14.2.1 on page 168).

**Figure 14-7: Primary HA Server Sub-menu**

```
Start Heartbeat Configuration
Primary Server IP: 10.3.180.2
Primary Server Host: EMS-Linux2
Secondary Server IP [-1]: 10.17.1.200
Secondary Server Host [-1]: vEMS-GeoHA-200
Ping IP [-1]: 10.3.180.80
Do you want to add another ping ip ? (y/n)
```

The current configuration is displayed for confirmation:

**Figure 14-8: HA Configuration Display**

```
HA Configuration:
Primary Server IP: 10.3.180.2
Primary Server Host: EMS-Linux2
Secondary Server IP: 10.17.1.200
Secondary Server Host: vEMS-GeoHA-200
Ping IP: 10.3.180.80
Are you sure that you want to continue ? (y/n/q)y
```

- Type **y** to continue the installation process.
- Type **n** to reconfigure all parameters
- Type **q** to stop the installation process

The installation process starts (this process may take a few minutes). During the installation, you may encounter one or more of the following system responses:

- “/data: device is busy” – When the /data partition is currently in use by another prompt or application. **You must un-mount the /data partition before continuing.** In the event where the /data partition isn't busy, the above message is not displayed.
- When prompted, press Enter to continue.
- When prompted “To abort waiting type 'yes' [1]:” – you can wait or press 'yes' to continue.

When the installation process for the Primary server has completed, the following message is displayed:

**Figure 14-9: HA Server Configured as Primary Server - Confirmation**

```
Server Configured As Secondary
State change failed: (-12) Device is held open by someone
Command 'drbdsetup /dev/drbd0 secondary' terminated with exit code 11
command exited with code 11
***** HA configuration finished *****
```



**Note:** After the installation process has completed, it takes several minutes until the HA status changes to 'Online' and the EMS server status changes to 'EMS server is running'.

## 14.2.1 Ping Nodes

The purpose of these nodes (IP address) is to ensure network connection along all EMS server configured interfaces. When an IP address is configured as “ping node”, this implies that the HA process sends ICMP packets (at a constant interval) to this address (through the appropriate Server Ethernet interface). If no response is returned from this ping node (during a constant period of time), the HA process determines that the specific network interface connection is down and acts accordingly (i.e. initiates a possible switchover). The ping node should be a reliable host in the network, such as router or any other machine which accurately reflects the network status.

It is possible to configure several “ping nodes”, where each ping node is considered to be a single point of failure, therefore if there is no connection to one of the ping nodes, a switchover is performed (unless the Secondary server cannot takeover due to the same or different network problems or during initial synchronization between the Primary and Secondary server).



**Note:** It's recommended to configure a separate ping node for each configured physical Ethernet interface (to the router connected to each of the subnets); however, if Ethernet Redundancy is configured between these two interfaces, then it's sufficient to configure a single ping node.



## 14.3 Secondary Server HA Installation

This section describes how to install the High Availability (HA) application on the designated Secondary server.

➤ **To install the secondary server:**

1. In the High Availability menu, choose option **2** to run the Secondary HA Server installation, and then press Enter.



**Note:** The Secondary server configuration MUST be performed after the Primary server configuration has completed and its status is 'EMS Server is running'.

2. After the HA packages are installed, you are prompted for the 'Primary IP' and *acems* user password (you might also be prompted to answer **yes** before connecting).

**Figure 14-10: Primary HA Server IP**

```
Start Heartbeat Configuration
Primary Server IP:[-1]: 10.7.14.144
acems@10.7.14.144's password: █
```

The Secondary server copies the HA configuration files from the Primary server and then starts the installation process.

**Figure 14-11: Secondary HA Server Configuration**

```
Start Heartbeat Configuration
Primary Server IP:[-1]: 10.7.14.143
acems@10.7.14.143's password:
drbd.conf
ha.cf
cib.xml
haresources
Copy files from primary server:      [ OK ]
Update primary parameters in secondary:
Global IP(eth0):                    10.7.14.215
Global IP(eth1):                    10.77.10.215
Primary IP:                         10.7.14.143
Primary Host:                       EMS-Linux143
Secondary IP:                       10.7.14.144
Secondary Host:                     EMS-Linux144
Ping IP:                            10.7.0.1,10.77.10.1
Press any key to continue... █
```

3. When prompted '[need to type **yes** to confirm]' press **yes**.
4. When prompted 'Press any key to continue...' press Enter.

## 14.4 HA Status

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

### ➤ To verify the EMS HA status:

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

Figure 14-12: EMS HA Status

```

High Availability Status

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

HA EMS Status                    [ Unknown - Not Primary Server ]

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

```

The following status view is displayed (Example only):

Figure 14-13: EMS HA Status - Example Display

```

High Availability Status
-----

HA Heartbeat Service Status      [ UP ]
HA DRBD Service Status          [ UP ]

EMS-Linux141 HA Status          [ ONLINE ]
EMS-Linux141 HA Location Status [ Primary ]
EMS-Linux141 Data Sync Status   [ UpToDate ]

EMS-Linux142 HA Status          [ OFFLINE ]
EMS-Linux142 HA Location Status [ Unknown ]
EMS-Linux142 Data Sync Status   [ DUnknown ]

Network Connection(10.7.0.1)    [ OK ]

HA EMS Status                   [ EMS Server is running!! ]

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

```

- **HA Heartbeat Service Status:** Whether the heartbeat service is installed and running.
- **HA DRBD Service Status:** Whether the data replication service is installed and running.
- **<HOST\_NAME > HA Status:** The following states are available:
  - ◆ ONLINE – HA is enabled and heartbeat packets have been sent.
  - ◆ OFFLINE – HA is disabled or does not exist (this state usually appears for several minutes after the new installation).
  - ◆ IN Progress – HA has started (this state usually appears for several seconds immediately after the new installation).
- **<HOST\_NAME > HA Location Status:** the following states are available:
  - ◆ Unknown – Cannot resolve if the EMS server is Primary or Secondary
  - ◆ Primary - The current working server
  - ◆ Secondary - the redundant server
- **<HOST\_NAME > HA Data Sync Status:** the following states are available:
  - ◆ DUnknown - Cannot resolve whether the EMS server data is synchronized with the other server
  - ◆ UpToDate – The replicated data is synchronized with the Primary server
  - ◆ Inconsistent – The replicated data is in the progress of synchronizing with the Primary server
- **Network Connection (<Ping Node>):-** For each configured ping node, this status verifies if there is a network connection to it.
- **HA EMS Status:** The current state of the EMS server and watchdog processes:
  - ◆ The EMS server is running – the EMS server process is up.
  - ◆ The EMS is not installed
  - ◆ The EMS server is not running – the EMS watchdog is trying to start the EMS server.
  - ◆ The EMS watchdog is not running.
  - ◆ Unknown, Not Primary Server – This state is always displayed on the Secondary server. In addition, it displays when HA is not configured.

## 14.4.1 Advanced Status View

This section describes the advanced status view.

➤ To view the advanced status:

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

**Figure 14-14: Advanced Status View**

```
Heartbeat Advanced Status
-----
heartbeat OK [pid 21524 et al] is running on ems-linux6 [ems-linux6]...

=====
Last updated: Mon Jun 10 09:08:10 2013
Current DC: ems-linux2 (69778371-0a03-b402-faaf-657669826990)
2 Nodes configured.
1 Resources configured.
=====

Node: ems-linux6 (69778371-0a03-b406-faaf-657669826990): online
Node: ems-linux2 (69778371-0a03-b402-faaf-657669826990): online

Resource Group: group_1
  drbddisk_1 (heartbeat:drbddisk): Started ems-linux2
  Filesystem_2 (ocf::heartbeat:Filesystem): Started ems-linux2
  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: fc00c6e00a1b6039bfcebe37afa3e7e28dbd92fa build by root@EMS-Linux143, 2011-01-26 12:04:18
0: cs:SyncTarget st:Secondary/Primary ds:Inconsistent/UpToDate C r---
   ns:0 nr:2942588 dw:2941852 dr:0 al:0 bm:179 lo:24 pe:1372 ua:23 ap:0
   [>.....] sync'ed: 4.4% (63685/66557)M
   finish: 0:16:58 speed: 63,804 (56,556) K/sec
   resync: used:4/31 hits:185355 misses:196 starving:0 dirty:0 changed:196
   act_log: used:0/257 hits:0 misses:0 starving:0 dirty:0 changed:0

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

The advanced status view provides a more detailed view of the EMS HA status. This command is particularly important during the initial synchronization between the primary and secondary EMS servers when the precise percentage of the stage of the EMS HA synchronization process is displayed (highlighted in green in the above figure).

## 14.5 EMS Server Manual Switchover

Manual switchover can be performed from either the Primary HA or Secondary HA server.

➤ **To manually switchover to the active EMS server:**

1. In the High Availability menu, choose option **2 (HA Switchover)**, and then press Enter.

Figure 14-15: Manual Switchover

```

      EMS Server 7.0.1144 Management
-----
Main Menu> Application Maintenance> High Availability
-----
>1.HA Status
  2.HA Switchover
  3.Uninstall HS
  b.Back
  q.Quit to main Menu
  
```

2. Type **y** to confirm your selection.

During the manual switchover process, the "switchover in process..." message is displayed in the EMS server machine where the command was activated. If you run the 'HA Status' command on the other server, it will display the HA status of the Primary server as STANDBY until the Secondary server becomes the Primary server.

Figure 14-16: Switchover Status

```

      High Availability Status
      -----
HA Heartbeat Service Status      [ UP ]
HA DRBD Service Status          [ UP ]

EMS-Linux2 HA Status            [ STANDBY ]
EMS-Linux2 HA Location Status    [ Primary ]
EMS-Linux2 Data Sync Status      [ UpToDate ]

EMS-Linux6 HA Status            [ ONLINE ]
EMS-Linux6 HA Location Status    [ Secondary ]
EMS-Linux6 Data Sync Status      [ UpToDate ]

Network Connection(10.3.180.80) [ OK ]

HA EMS Status                    [ EMS WatchDog process is not running!! ]
  
```

After the Secondary server becomes the Primary server, a few minutes are required until the EMS application is up and running.

Figure 14-17: Status after Switchover

```

High Availability Status
-----

HA Heartbeat Service Status      [  UP  ]
HA DRBD Service Status          [  UP  ]

EMS-Linux6 HA Status             [  ONLINE  ]
EMS-Linux6 HA Location Status    [  Primary  ]
EMS-Linux6 Data Sync Status      [  UpToDate  ]

EMS-Linux2 HA Status             [  ONLINE  ]
EMS-Linux2 HA Location Status    [  Secondary  ]
EMS-Linux2 Data Sync Status      [  UpToDate  ]

Network Connection(10.3.180.80) [  OK  ]

HA EMS Status                    [  EMS Server is running!!  ]

```

## 14.6 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
- User-defined certificate installations.

### ➤ To uninstall EMS HA:

- In the High Availability menu, choose option **3 (Uninstall HA)**, and then press Enter.

The uninstall process takes 1-2 minutes with the following output:

**Figure 14-18: Uninstall EMS HA Status Display**

```
CentOS release 5.3 (Final)
Stopping High-Availability services:
[ OK ]

Remove rpm: [ OK ]
Remove rpm: [ OK ]
Remove rpm: [ OK ]
Remove rpm: [ OK ]
error reading information on service heartbeat: No such file or directory
EMS Server is already stopped!
Stop EMS service: [ OK ]
Enable automatic DB stop : [ OK ]
Enable automatic DB start : [ OK ]
Enable automatic agent start : [ OK ]
Enable automatic listener start : [ OK ]
Enable automatic EMS start : [ OK ]
umount: /dev/drbd0: not mounted
Stopping all DREB resources.

Stop drbd service: [ OK ]
Remove rpm: [ OK ]
/sbin/service
Stopping all DREB resources.
warning: /etc/drbd.conf saved as /etc/drbd.conf.rpmsave
Remove rpm: [ OK ]
Re-mount data : [ OK ]
Update fstab : [ OK ]
***** HA uninstall finished *****
press any key to continue
```



**Note:** The EMS application doesn't start automatically after this process has completed. To start the EMS, reboot the EMS server or quit the EMS Server Manager and run it again using the 'Start EMS Server' option (see [12.5.1](#) on page 106).

This page is intentionally left blank.



# Part VI=

## Configuring the Firewall and Installing the EMS Client

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



## 15 Configuring the Firewall

To enable EMS Client ↔ EMS Server ↔ Managed Devices, SEM and IP Phones communication according to [Figure 15-1](#), define the rules specified in the Firewall Configuration Rules table below:

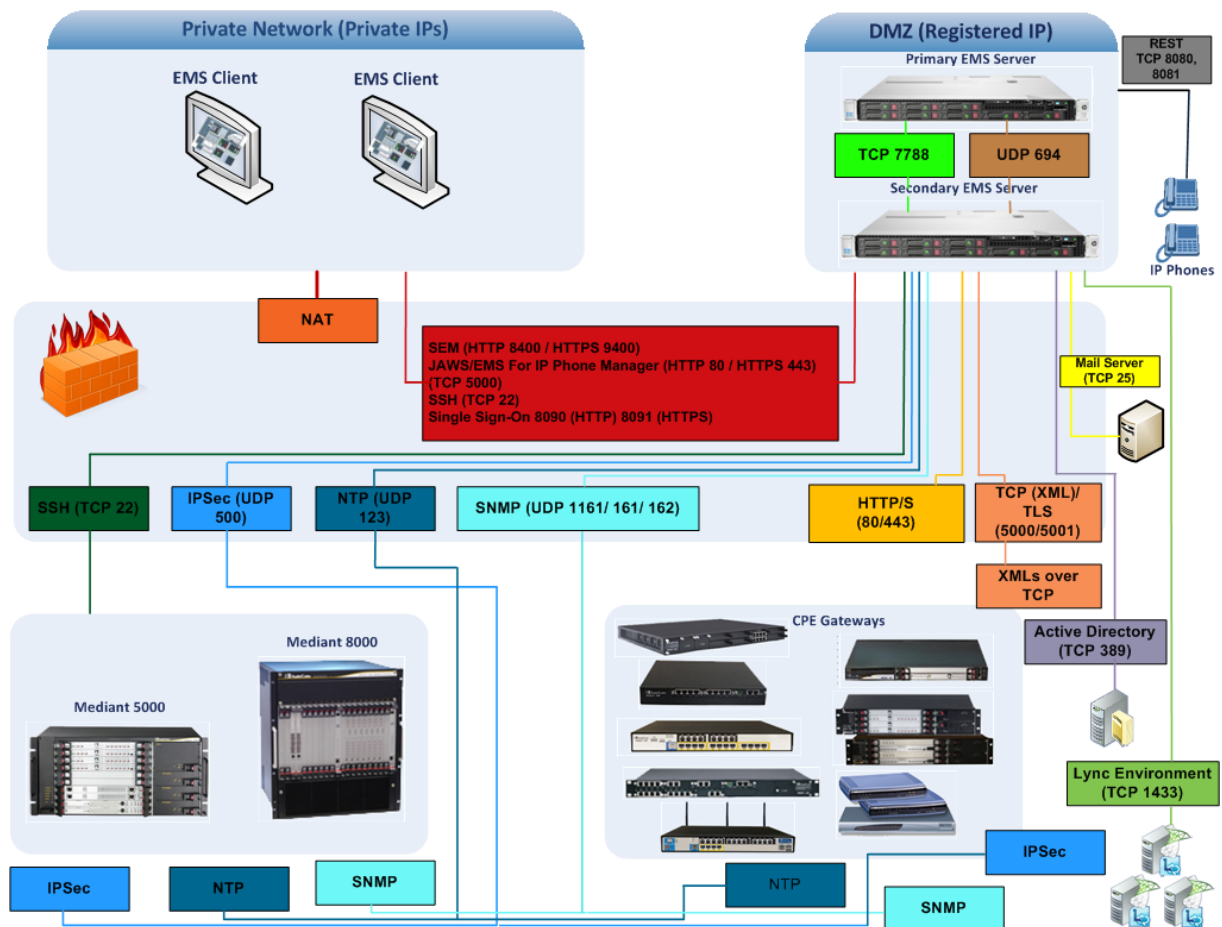
**Table 15-1: Firewall Configuration Rules**

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
<b>EMS Client ↔ EMS Server</b>	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 client/JAWS and NBIF. Initiator: Client PC	
<b>EMS Server ↔ All Media Gateways except M5K &amp; M8K</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
	TCP (HTTP)	8090	Direct HTTP connection between the device's embedded Web interface and the Management console (PC). Initiator: EMS Server	EMS server side / Bi-Directional

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
	TCP (HTTPS)	8091	Direct HTTPS connection between the device's embedded Web interface and the Management Console (PC). Initiator: EMS Server	EMS server side / Bi-Directional
	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 ↔ IP Phone Manager Browser</b>	TCP (HTTP)	80	HTTP connection between the EMS server and the IP Phone Manager Web browser.	EMS server side / Bi-Directional
	TCP (HTTPS)	443	HTTPS connection between the EMS server and the IP Phone Manager Web browser.	EMS server side / Bi-Directional
<b>EMS Server ↔ Mediant 5000/8000 Media Gateways</b>	TCP	22	SSH communication for file 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
	TCP (TLS)	5001	XML based SEM TLS secured communication. Initiator: MG	EMS Server side / Bi-Directional

Connection	Port Type	Port Number	Purpose	Port side / Flow Direction
<b>SEM client ↔ Tomcat server</b>	TCP (HTTP)	8400	SEM HTTP connection between the user's browser and Tomcat server. Initiator: Client's PC.	EMS Server side / Bi-Directional
	TCP (HTTPS)	9400	SEM HTTPS connection between the user's browser and Tomcat server. Initiator: Client's PC.	EMS Server side / Bi-Directional
<b>EMS server ↔ Lync SQL Server</b>	TCP	1433	Connection between the EMS server and the Lync SQL server.	Lync SQL server side / Bi-Directional
<b>EMS server ↔ Active Directory</b>	TCP	389	Connection between the EMS server and the Active Directory.	Active Directory 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	
<b>EMS server ↔ Mail Server</b>	TCP	25	Trap Forwarding by Mail Initiator: EMS Server	Mail Server side / Bi-Directional.
<b>EMS Server ↔ Endpoints (IP Phones)</b>	TCP	8080	REST based communication between EMS server and IP Phones. Initiator: Endpoint	EMS server side / Bi-Directional
	TCP	8081	REST based communication between EMS server and IP Phones. Initiator: Endpoint	EMS server side / Bi-Directional.

Figure 15-1: Firewall Configuration Schema



**Note:** The above figure displays images of example CPE gateways. For the full list of supported products, see Section 2 on page 21.

- NOC ↔ EMS (Server) ports

Table 15-2: OAM&amp;P Flows: NOC ↔ Device/ IP Phone/ SBA/ EMS

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

Table 15-3: OAM&amp;P Flows: Device/ IP Phone/ SBA/ EMS ↔ NOC

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
Device/IP Phone/ SBA/EMS	NOC/OSS	NTP	123	123
		SNMP Trap	1024 – 65535	162
		-	-	-

This page is intentionally left blank.



## 16 Installing the EMS Client

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

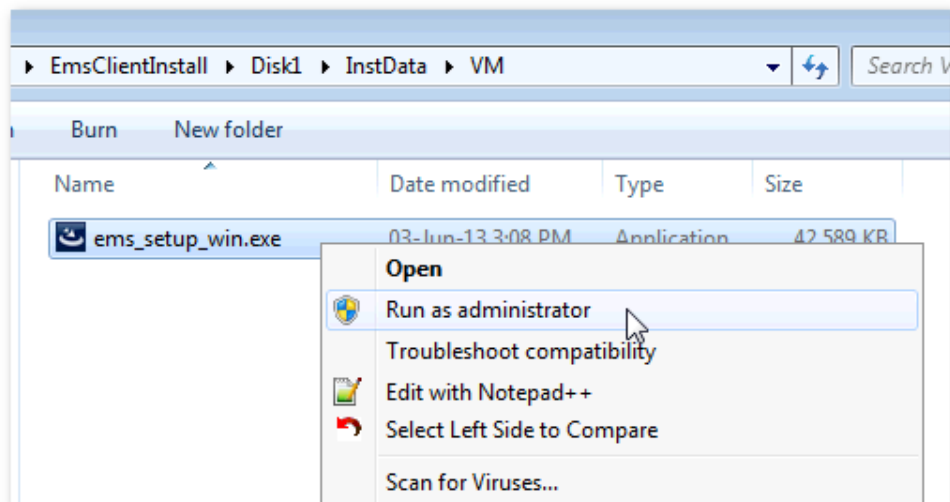


**Note:** Before you run the EMS Client exe file, ensure that you extract the entire Disk1 EMS client directory to your PC/laptop in the same relative path as the Disk image, and only then, run the exe file from this location.

➤ **To install the EMS client on a PC or Laptop:**

1. Insert AudioCodes' EMS installation disk into the CDROM.
2. Open the EmsClientInstall\Disk1\InstData\VM directory.
3. Do one of the following:
  - On **Windows 7**:
    - a. Right-click the EMS client Installation file ac\_ems\_setup\_win.exe, and then choose **Run as administrator**; the EMS client installation setup is displayed.
    - b. Follow the prompts to install the EMS client.

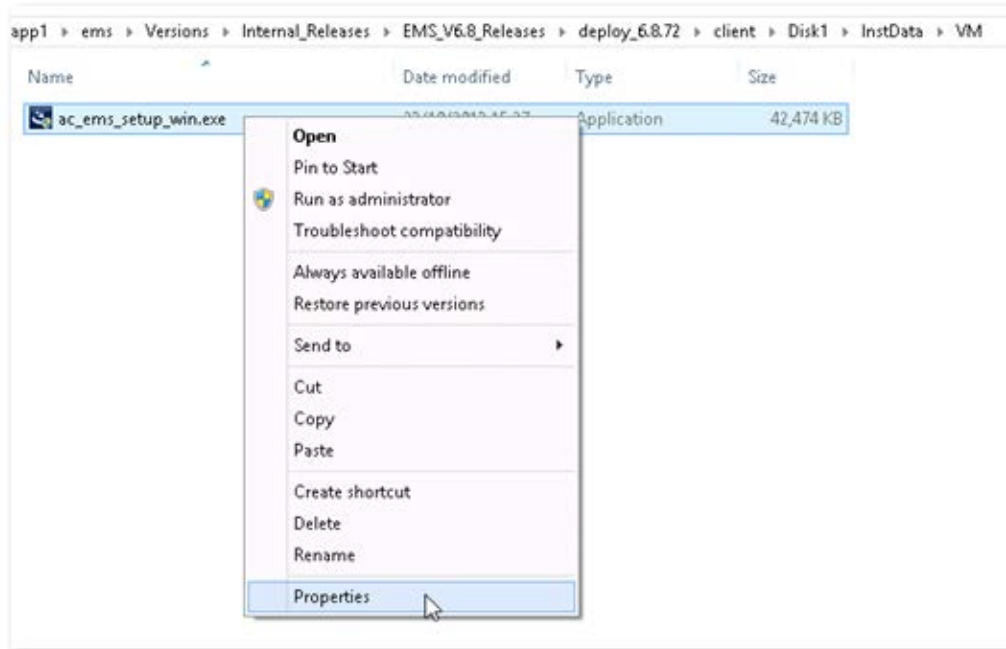
**Figure 16-1: EMS Client Installation-Run as Administrator**



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

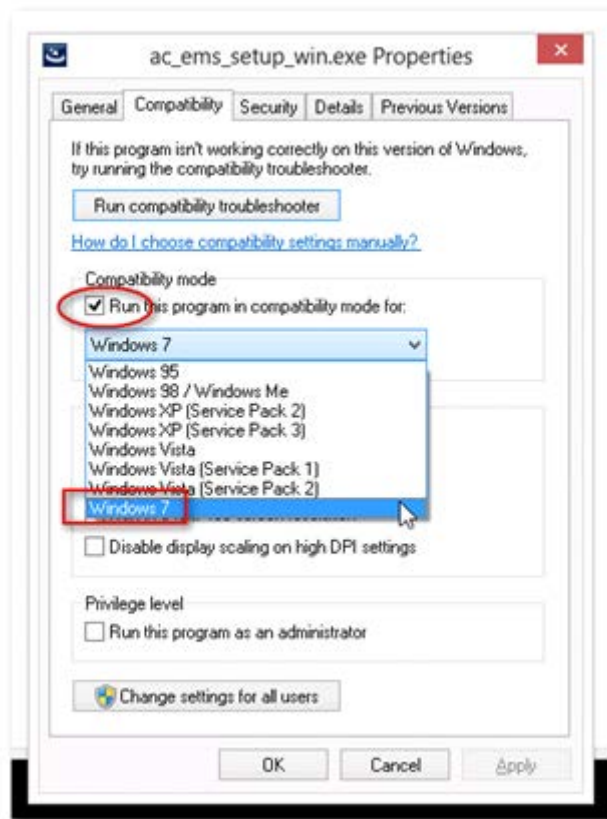
- On **Windows 8**:
  - a. Right-click the installation exe file, and then choose **Properties**; the Properties window is displayed:

**Figure 16-2: EMS Client Installation File-Windows 8 Properties**



- b. Select the **Compatibility** tab, and then select the checkbox **Run this program in compatibility mode for**.

Figure 16-3: EMS Client Installation File-Compatibility Tab



- c. In the Windows 7 pane, select **Windows 7**.
  - d. Click **OK**.
  - e. Right-click the EMS client installation file `ac_ems_setup_win.exe`, and then choose **Run as administrator**; the EMS client installation setup is displayed.
  - f. Follow the prompts to install the EMS client.
- Upon the completion of the installation process, the EMS client icon is added to the desktop.



**Note:** If you have replaced the “AudioCodes-issued” certificates with external CA certificates, and wish to uninstall the previous EMS client, ensure that you backup the `clientNssDb` files: `cert8.db`, `key3.db`, and `secmod.db`.

## 16.1 Running the EMS Client on a PC or Laptop

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

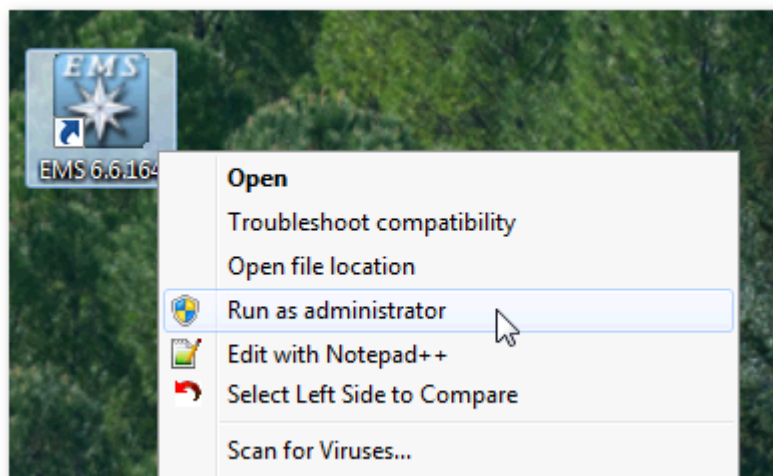
➤ **To run the EMS on Windows XP or older:**

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

➤ **To run the EMS on Windows 7 or later:**

- Right-click the EMS client icon on your desktop, and then choose **Run as Administrator**.

**Figure 16-4: Running EMS Client-Run as Administrator**



## 16.2 Initial Login

This section describes how to initially login to the EMS client.

➤ **To initially login to the EMS client:**

1. Log in as user 'acladmin' with password 'pass\_1234' or 'pass\_12345'.



**Note:** First-time access defaults are case sensitive. After you login to the EMS for the first-time, you are prompted to change the default password. If you incorrectly define these or the field Server IP Address, a prompt is displayed indicating that the fields should be redefined correctly.

2. In the main screen, open the 'Users List' and add new users according to your requirements.

## 16.3 Installing and Running the EMS Client on a PC using Java Web Start (JAWS)

Java Web Start (JAWS) enables you to install the EMS client (compatible with your EMS server version) without using any CDs.

➤ **To install the EMS client on a PC using JAWS:**

1. Open a browser and type the EMS server IP in the Address field and add /jaws as suffix, for example:  
<http://10.7.6.18/jaws/>
2. Follow the online instructions.

➤ **To run the EMS client after JAWS install through URL:**

- Specify the path `http://<server_ip>/jaws`.  
An 'EMS Login Screen' is opened.  
For example: `http://10.7.6.18/jaws/`

This page is intentionally left blank.

# Part VIII

## Appendices

This part describes additional EMS server procedures.





## A Frequently Asked Questions (FAQs)

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

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

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


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

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

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

**Figure A-1: EMS Client Removal**



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

**Figure A-2: Java Control Panel**



6. Choose Shortcut Creation in the Settings dialog.
7. Select the **Always allow** box to always create an icon on desktop or Prompt user to ask before icon creation.
8. Install client using Jaws. For more information, see Section 16.3 on page 189.
9. After the installation has completed, the new Icon is created on your desktop:



## A.2 After Rebooting the Machine

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

**A:** Perform the procedure below:

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

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

## A.3 Changes Not Updated in the Client

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

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

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

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

## A.4 Removing the EMS Server Installation

**Q:** How do I remove the EMS server installation?

**A:** See Section 14.6 on page 174.

## B Site Preparation

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



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

- EMS server data backup should be performed prior to machine formatting. The Backup files should be transferred to another machine prior to the EMS server installation. Note, that these backup files cannot be used for other versions. They should be kept in case the user fails to install the new version, and decides to roll back to the previous version.
- EMS Users: all the users' names and permissions should be saved. After the new EMS version is installed, these users should be defined manually with default passwords. To perform this task, in the EMS menu, choose Security > User's List menu.
- EMS Tree: the user can export the gateways tree using the File > MGs Report command (example of the file is attached). This file is a CSV file and does not preserve secured information such as passwords. Therefore, we recommend extending it manually with columns including: SNMP read and write community strings, or SNMPv3 user details, IPSec pre-shared key and Mediant 5000 and Mediant 8000 - *root* password. This information will be required during the Media gateway's definition in the newly installed EMS system. It's also highly recommended to perform gateway removal and adding and to ensure that the EMS <-> GW connection has been established.

**Figure B-1: Save MGs Tree Command**

	B	C	D	E	F	G	H	I	J	K	L
1	IP Address	Node Name	RegionName	Description	Product Type	Software	Connectio	Administra	Operative	Mismatch	Last Ch
2	10.7.19.88	10.7.19.88	gena		MEDIANT 8000	5.8.57	Connectec	Unlocked	Enabled	No Misma	2009-1:
3	10.7.5.220	10.7.5.220	Roye		UNKNOWN MP114 FXS/FXO	5.90A.006	Connected			No Misma	2009-1:
4	10.7.5.221	10.7.5.221	Roye		UNKNOWN	5.50.020	Connected			No Misma	2009-1:
5	10.7.5.217	10.7.5.217	Roye		MP112	5.80A.020	Not Connected			No Misma	2009-1:
6	10.7.5.214	10.7.5.214	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1:
7	10.7.5.211	10.7.5.211	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1:
8	10.7.5.222	10.7.5.222	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1:
9	10.7.5.215	10.7.5.215	Roye		UNKNOWN	unknown_	Not Connected			No Misma	2009-1:

This page is intentionally left blank.

## C Daylight Saving Time (DST)

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

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

The following major changes are implemented:

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

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

### ■ EMS Server

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

New DST settings are fully supported starting v5.6.

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

### ■ EMS Client

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

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

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

This page is intentionally left blank.

## D EMS Application Acceptance Tests

This appendix describes the EMS Application Acceptance tests.

### D.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.

### D.2 Configuration

This section describes the EMS application configuration acceptance tests.

#### D.2.1 Client Installation

**Table D-1: Acceptance Test – Client Installation**

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

## D.2.2 Server Installation

**Table D-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.

## D.2.3 Add Auxiliary File

**Table D-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.

## D.2.4 Add Media Gateway



**Table D-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.





## D.2.5 Provisioning – Mediant 5000/ Mediant 8000

**Table D-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.

## D.2.6 Provisioning – CPE Devices

**Table D-6: Acceptance Test – Provisioning: CPE Devices**



Step Name	Description	Expected Result
<b>Go to network frame</b>	Click the network button.	Network configuration is displayed.
<b>RTP Settings tab</b>	Click 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>	Restore the parameter to your NTP Server IP address.	The original value was restored.



**Note:** CPE devices include the following products: MediaPack, Mediant 500 MSBR, Mediant 500L MSBR, Mediant 600, Mediant 800 MSBR, Mediant 800B Gateway and E-SBC, Mediant 1000 MSBR, Mediant 1000B Gateway and E-SBC, Mediant 1000, Mediant 2000, Mediant 2600 E-SBC, Mediant 2600B E-SBC, Mediant 3000, Mediant 4000 SBC, Mediant 4000B SBC, Mediant 9000 SBC, Mediant SE and Mediant VE products.

## D.2.7 Entity Profile – Digital CPE Devices

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


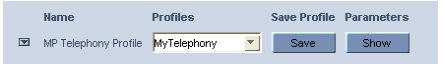

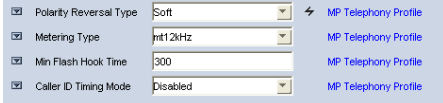
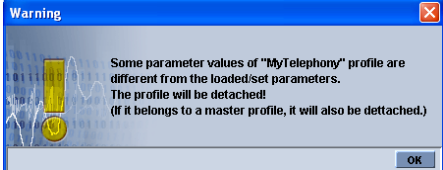
Step Name	Description	Expected Result
<b>Go to trunk level</b>	Drill down to trunk level	Trunks list appears according to board type.
<b>Trunk Properties</b>	Open trunk#1 properties	The frame provisioning opens and all the parameters are available.
<b>Trunk Configuration</b>	Configure the trunk	The new 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 500 MSBR, Mediant 500L MSBR, Mediant 600, Mediant 800B MSBR, Mediant 800B Gateway and E-SBC, Mediant 1000B MSBR, Mediant 1000B Gateway and E-SBC, Mediant 1000, Mediant 2000 and Mediant 3000.

## D.2.8 Entity Profile – Analog CPE Devices

Table D-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 then press <b>Apply</b> .	A detach profile pop up message is displayed. 



**Note:** Analog CPE devices include the following products: MediaPack, Mediant 600, Mediant 500 MSBR, Mediant 500L MSBR, Mediant 800B MSBR, Mediant 800B Gateway and E-SBC, Mediant 1000B MSBR; Mediant 1000B Gateway and E-SBC and Mediant 1000.

## D.3 Faults

### D.3.1 Alarm Receiver

Figure D-1: Alarm Receiver



Table D-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.

### D.3.2 Delete Alarms

Table D-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.

### D.3.3 Acknowledge Alarm

Table D-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.

## D.3.4 Forwarding Alarms

Figure D-2: Destination Rule Configuration

**Destination Rule Configuration**

Destination Rule Name:

☒ Enable EMS Alarm Forwarding  
☒ Enable EMS Event Forwarding  
☒ Enable MGW Alarm Forwarding  
☒ Enable MGW Event Forwarding

Severities To Forward: [Icons: Info, Error, Warning, Critical, Fatal]

Source MGW List:

Region	MGW Name	IP Address
Tom	10.7.19.85	10.7.19.85
Tom	10.7.19.42	10.7.19.42

Destination Type:

Destination Host IP Address:

Destination Host Port:

SNMP v2c Trap Community:

Enable SNMPv3 Configuration: ☐

Security Name:

Security Level:

Authentication Protocol:

Authentication Key:

Privacy Protocol:

Privacy Key:

Table D-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.

## D.4 Security

This section describes the EMS application security tests.

### D.4.1 Users List

Figure D-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 D-13: Acceptance Test – Add an Operator

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

### D.4.2 Non Repetitive Passwords

Table D-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."

### D.4.3 Removing Operator

Table D-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.

## D.4.4 Journal Activity

Figure D-4: Actions Journal



The screenshot shows the 'Actions Journal' application window. It has a menu bar with 'File', 'View', and 'Help'. Below the menu bar, it displays 'Entries: | 1500 Journal Entries | 0 Alarms Entries out of 9552'. There is an 'Advanced Filter' button and tabs for 'Journal' and 'Alarms'. The main area shows a table of entries with columns: Severity, Time, MG Name, Source, Action/Alarm Name, Details, Region, and Operator. The table contains three entries, all with a severity of 'Journal' and a time of '16:35:06 Dec 15 2009...'. The MG Name is '10.77.10.130' for all entries. The Action/Alarm Name is 'Configuration: Update' for all entries. The Details are 'Action UnLock was performed', 'Action Lock was performed', and 'Update Parameters: Field-tgMGintoActio...'. The Region is 'Mor' and the Operator is 'mor' for all entries.

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator
Journal	16:35:13 Dec 15 2009...	10.77.10.130		Configuration: Update	Action UnLock was performed	Mor	mor
Journal	16:35:07 Dec 15 2009...	10.77.10.130		Configuration: Update	Action Lock was performed	Mor	mor
Journal	16:35:06 Dec 15 2009...	10.77.10.130		Configuration: Update	Update Parameters: Field-tgMGintoActio...	Mor	mor

Table D-16: Acceptance Test – Journal Activity

Step Name	Description	Expected Result
Activity	Open the action journal.	Check that all actions that you performed until now are registered.
Filter	Use the filter: time, user and action.	Time, user, action filter are working OK.

## D.5 Utilities

This section describes the EMS application utilities acceptance tests.


### D.5.1 Configuration Parameter Search

#### D.5.1.1 Basic Search

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



Table D-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>	Displays a dialog with a list of results according to selected criteria.



### D.5.1.2 Advanced MG Search

Figure D-6: Configuration Parameter: Advanced Search

Table D-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</b>	Match exact word, any word or	Displays a dialog with a list of results

Step Name	Description	Expected Result
<b>search Options</b>	search for a MIB parameter.	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.

## D.5.2 MG Search

**Figure D-7: Media Gateway Search**



**Search Media Gateway**

☒ Search By Product Information:

Product Type: Mediant 5000/Mediant 8000

Software Version: All Versions

Product Status: All

☐ Search by IP address:

☐ Search by serial number:

☐ Search by MG Name:

☐ Match case ☐ Match whole word only

OK Cancel

**Table D-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.

### D.5.3 Online Help

**Table D-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.

### D.5.4 Backup and Recovery

**Table D-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.

This page is intentionally left blank.

## E Configuring RAID-0 for AudioCodes EMS on HP ProLiant DL360p Gen8 Servers

This appendix describes the required equipment and the steps for configuring the HP ProLiant server to support RAID-0 Disk Array configuration for the EMS server installation.



**Note:** This procedure erases any prior data residing on the designated disk drives.

### E.1 Prerequisites

This procedure requires the following:

- ProLiant DL360p Gen8 server pre-installed in a compatible rack and connected to power.
- Two 1.2TB SAS disk drives
- A VGA display, USB keyboard, and USB mouse must be connected to the server back I/O panel.

### E.2 Hardware Preparation

Make sure that two 1.2TB SAS disk drives are installed on slot 1 and 2 of the server. If required, refer to the *HP Service Manual*.

**Figure E-1: Hardware Preparation**



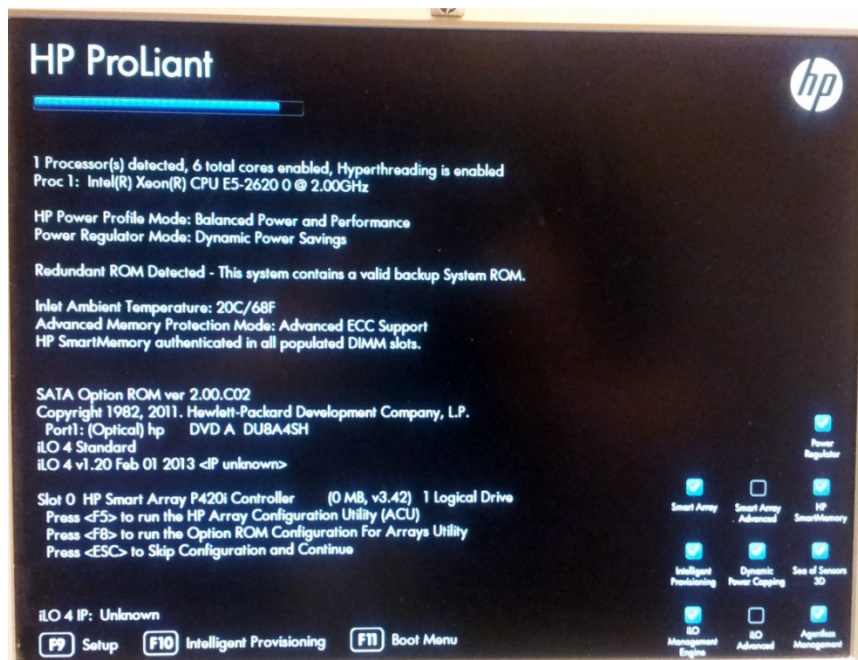
## E.3 Configuring RAID-0

This procedure describes how to configure RAID-0 using the HP Array Configuration Utility (ACU).

➤ **To configure RAID-0:**

1. Power up the server. If the server is already powered up and running, use the 'reboot' command (from system console as user root) to reboot the server.
2. While the server is powering up, monitor the server and wait for the following screen:

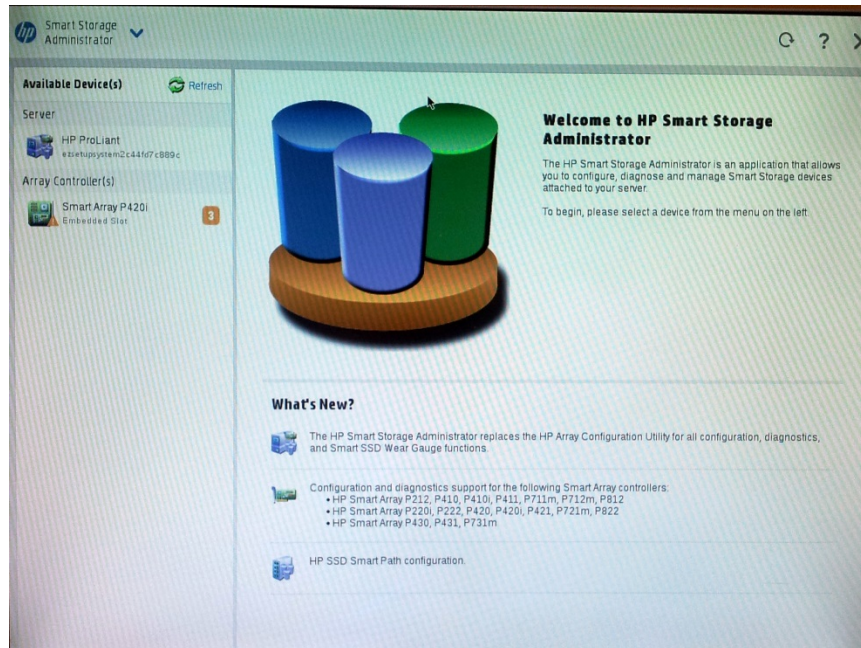
**Figure E-2: HP Array Configuration Utility (ACU)**



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

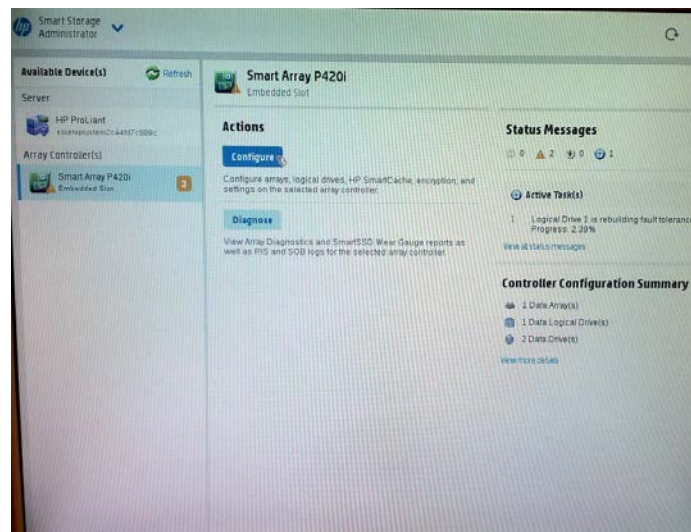
When the ACU is ready, the following screen is displayed:

**Figure E-3: RAID-Latest Firmware Versions**



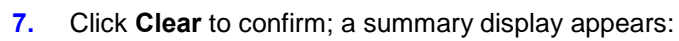
5. In the left-hand pane, select **Smart Array P420i**; an Actions menu is displayed:

**Figure E-4: Actions Menu**

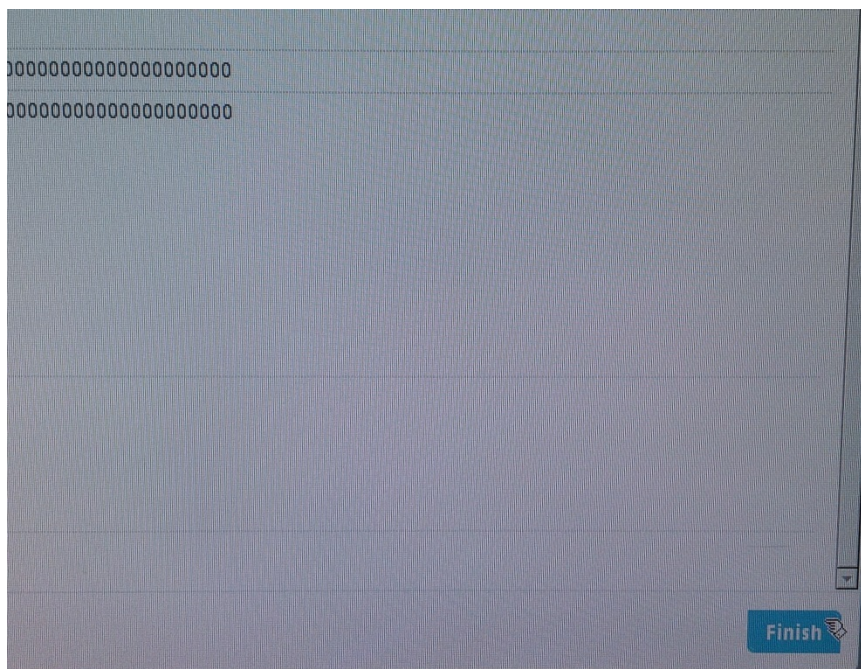




- ### Figure E-5: Clear Configuration



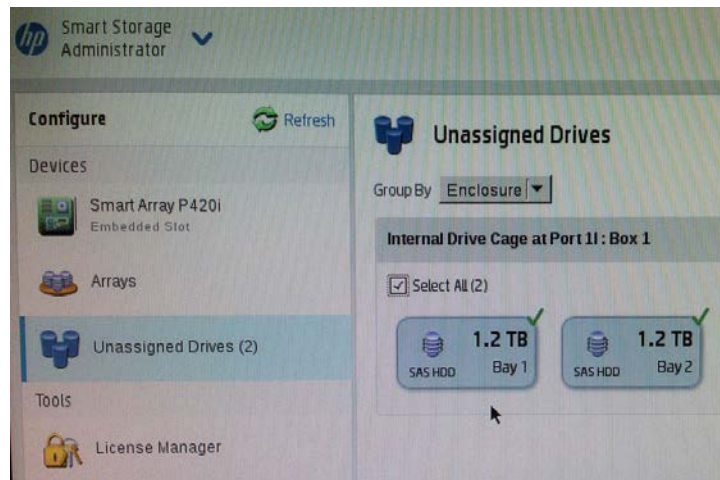
### Figure E-6: Summary Screen





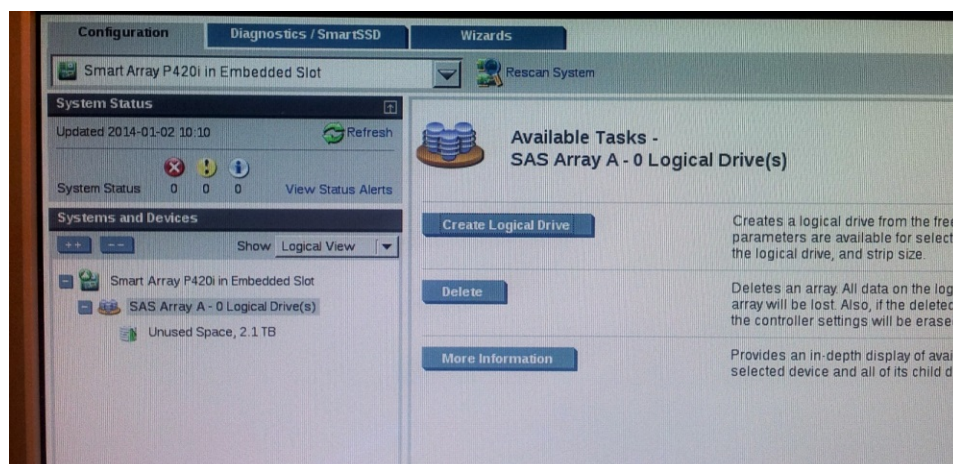
8. Click **Finish** to return to the main menu. The following screen is displayed:

**Figure E-7: Main Screen**



9. In the left-hand pane, select **Unassigned Drives (2)**; make sure that both the drives are selected, and then click **Create Array**.
10. Select **RAID 0** for RAID Level.
11. Select the 'Custom Size' check box, and then enter **2000 GiB**.
12. At the bottom of the screen, click **Create Logical Drive**; the following screen is displayed:

**Figure E-8: Logical Drive**

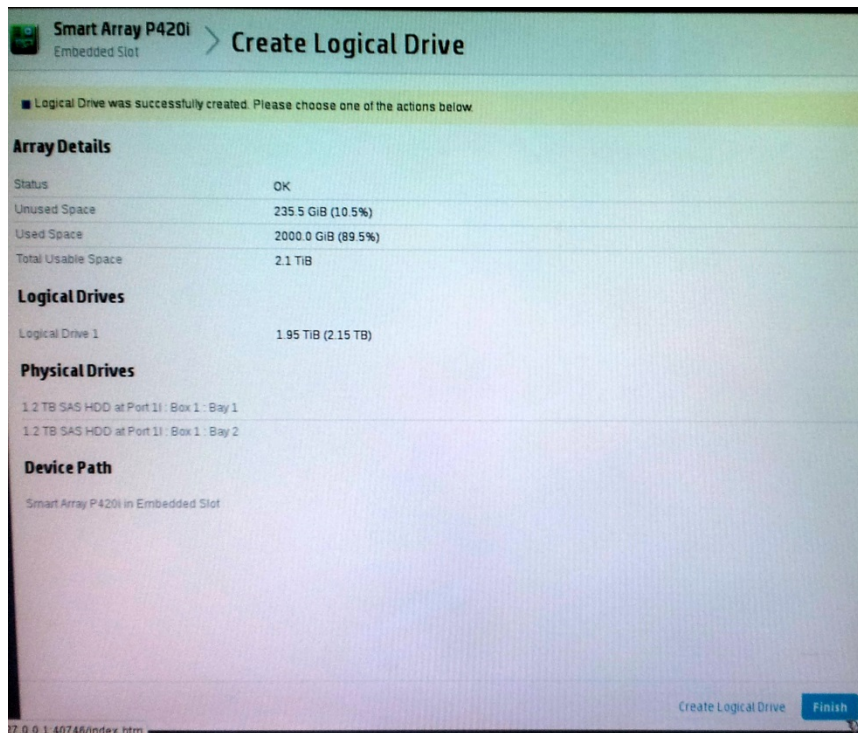


After the array is created, a logical drive should be created.

13. Click **Create Logical Drive**.

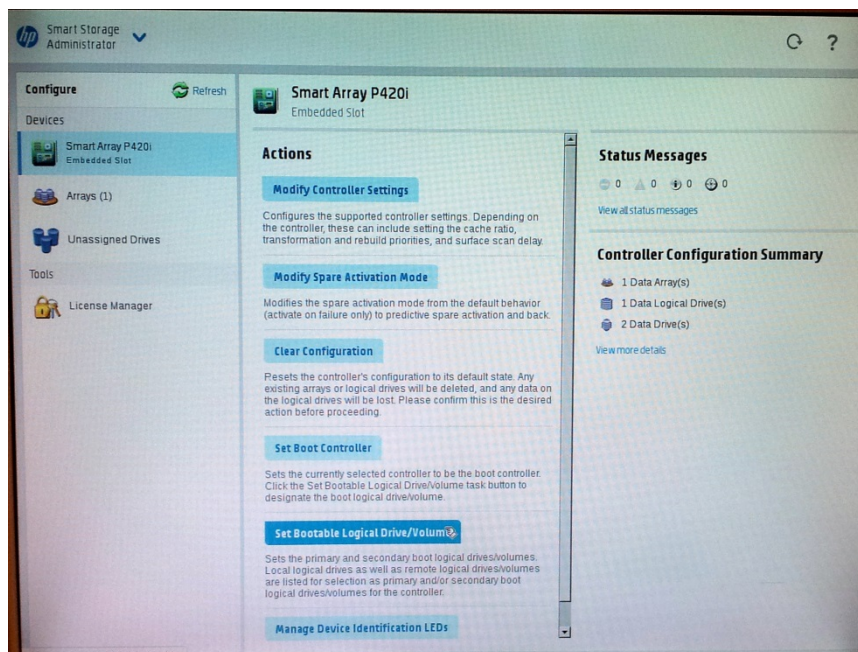
A summary screen is displayed:

Figure E-9: Summary Screen



14. Click **Finish**.

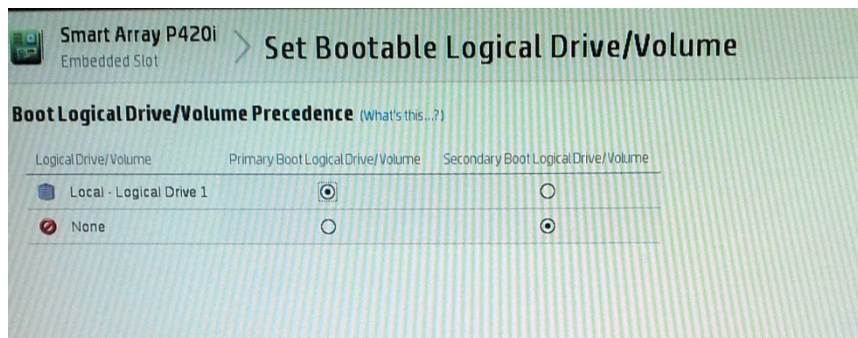
Figure E-10: Set Bootable Logical Drive/Volume



The new logical volume needs to be set as a bootable volume.

15. In the left-hand pane, select **Smart Array P420i**, and then click **Set Bootable Logical Drive/Volume**; the following screen is displayed:

**Figure E-11: Set Bootable Logical Drive/Volume**

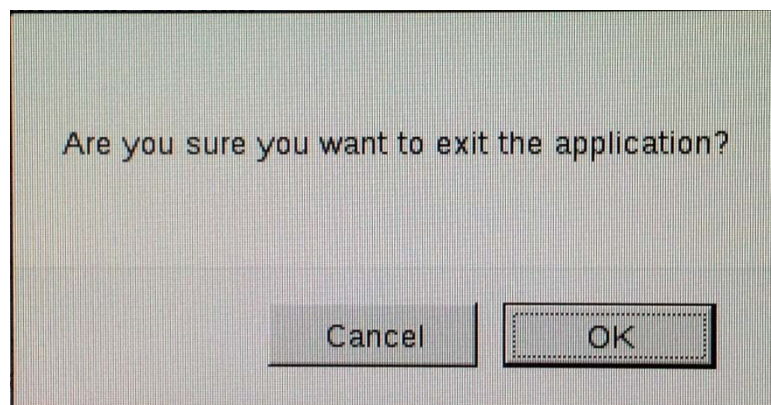


16. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.

A summary window is displayed.

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

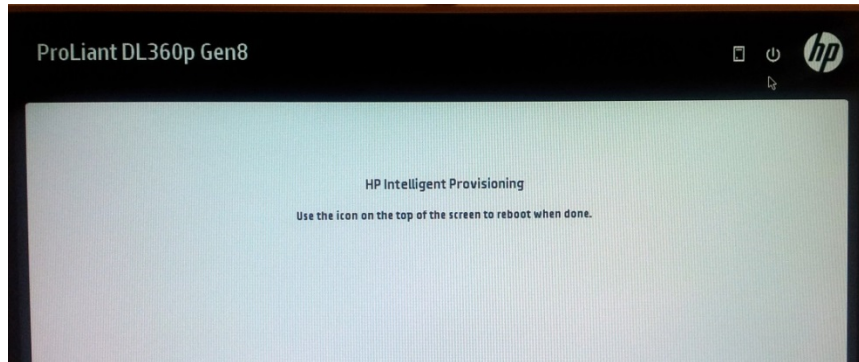
**Figure E-12: Exit Application**





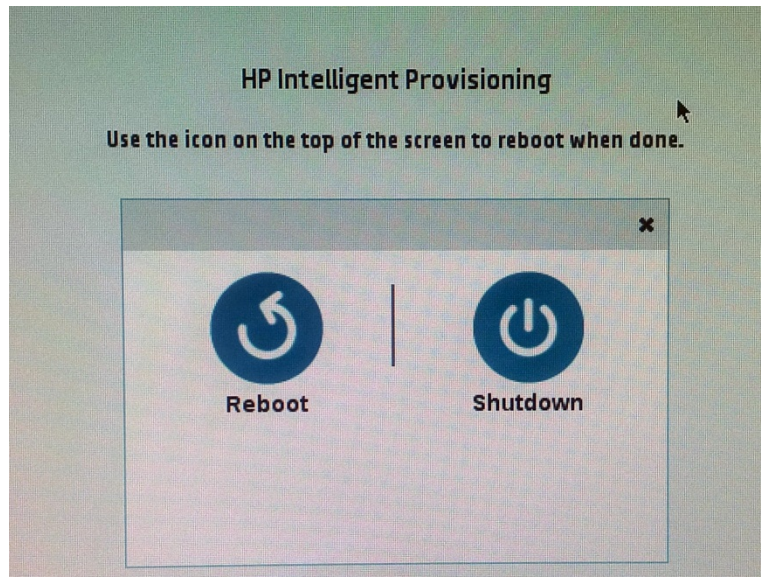
19. Click **Exit ACU** at the bottom left-hand corner of the screen; the following screen is displayed:

**Figure E-13: Power Button**



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

**Figure E-14: Reboot Button**



21. Click **Reboot** to reboot the server.  
The Disk Array configuration is now complete.
22. Install the EMS server installation (see Section 6.2 on page 37).

## F Managing Clusters

This appendix describes how to manually migrate or move EMS VMs to another cluster node.

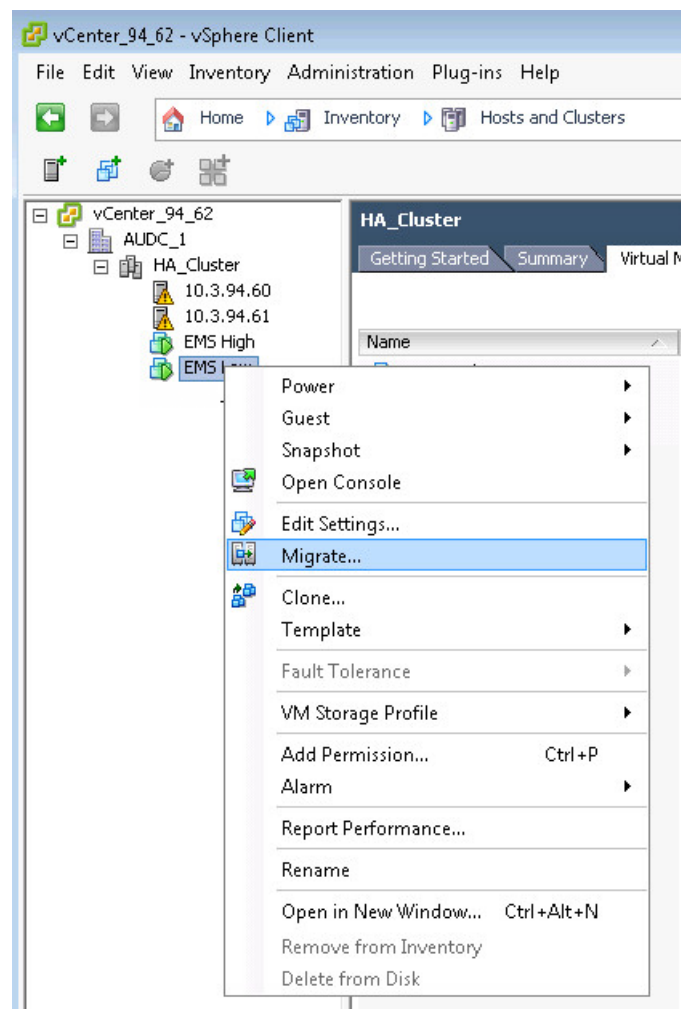
### F.1 Migrating EMS Virtual Machines in a VMware Cluster

This section describes how to migrate your EMS Virtual Machine from one ESXi host to another.

➤ **To migrate your EMS VM:**

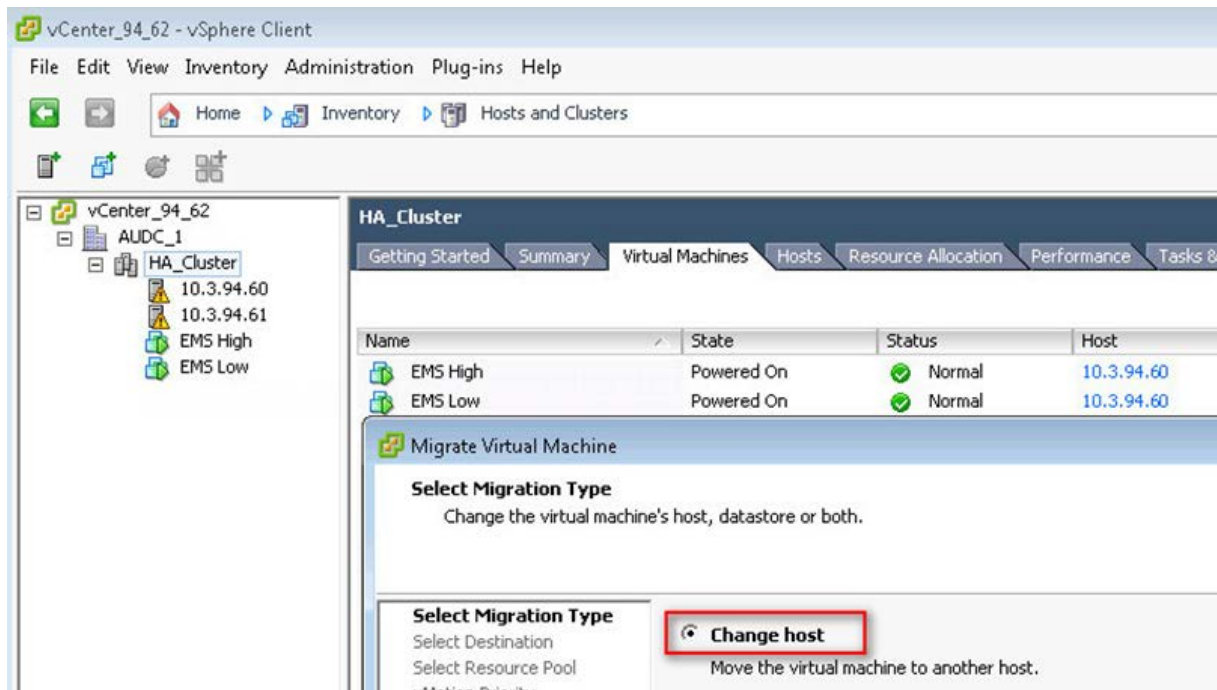
1. Select the EMS VM that you wish to migrate and then choose the **Migrate** option:

**Figure F-1: Migration**



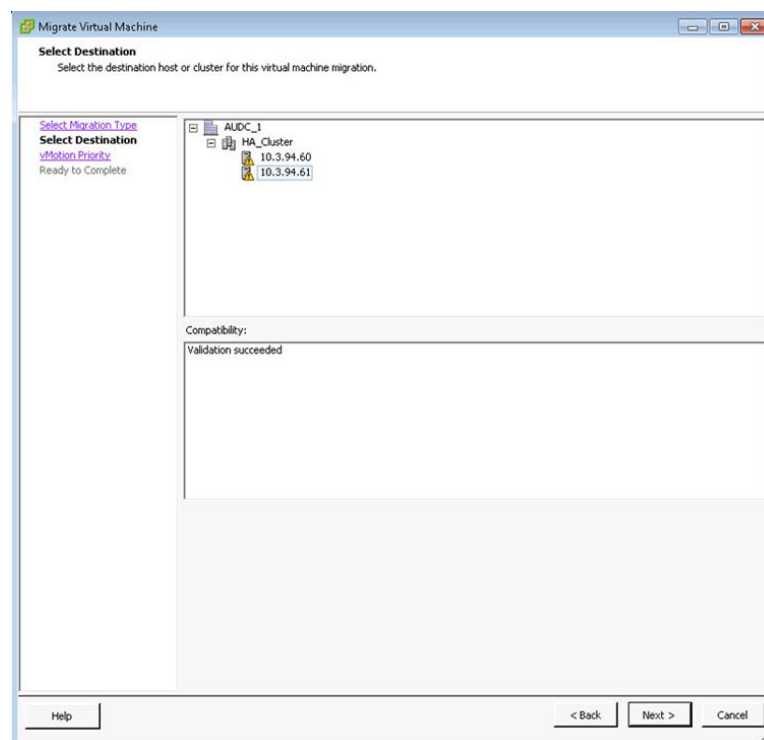
2. Change a cluster host for migration:

**Figure F-2: Change Host**



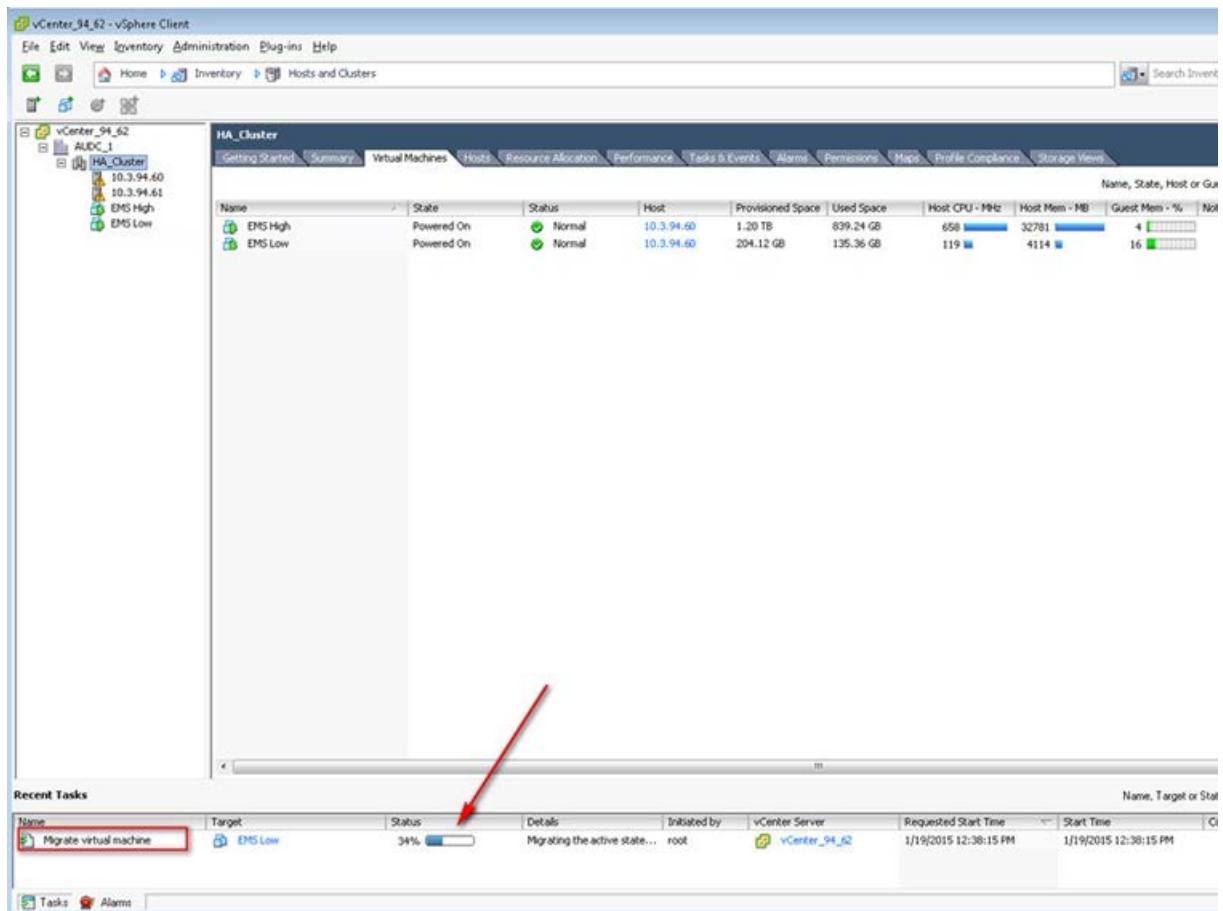
3. Choose the target host for migration:

**Figure F-3: Target Host for Migration**



The migration process commences:

**Figure F-4: Migration Process Started**



After the migration has completed, the EMS application will run seamlessly on the VM on the new cluster's host.

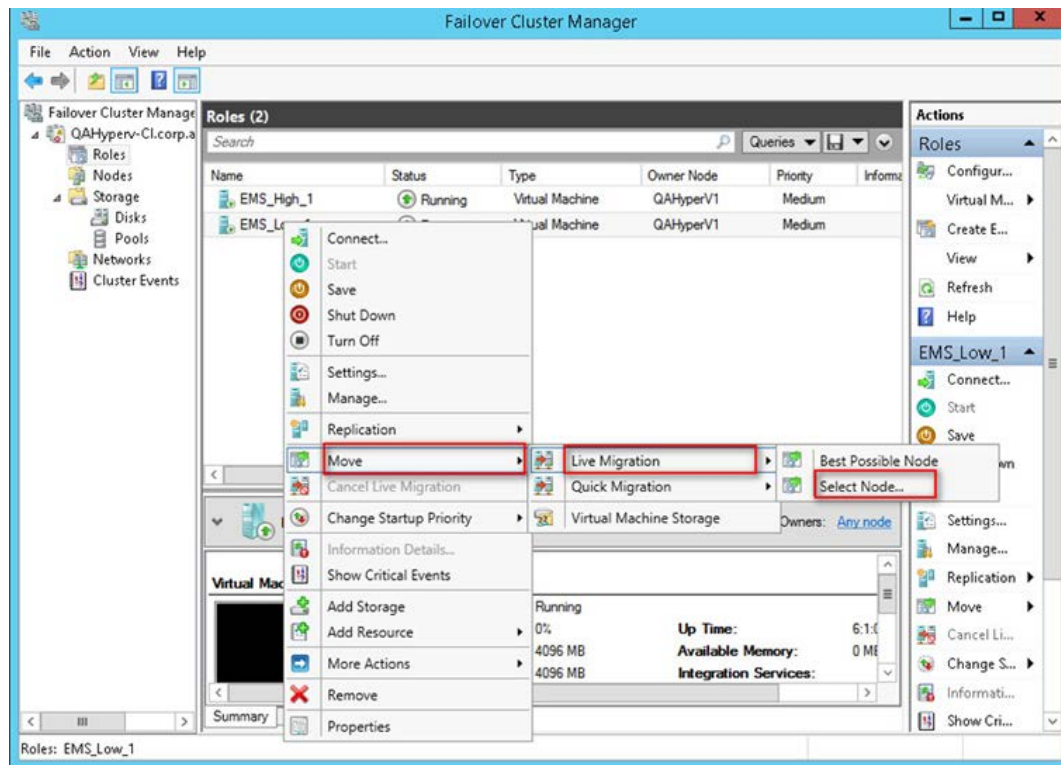
## F.2 Moving EMS VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

➤ To move a Virtual Machine to another node of the cluster:

1. Select the Virtual Machine, right-click and from the menu, choose **Move > Live Migration > Select Node**.

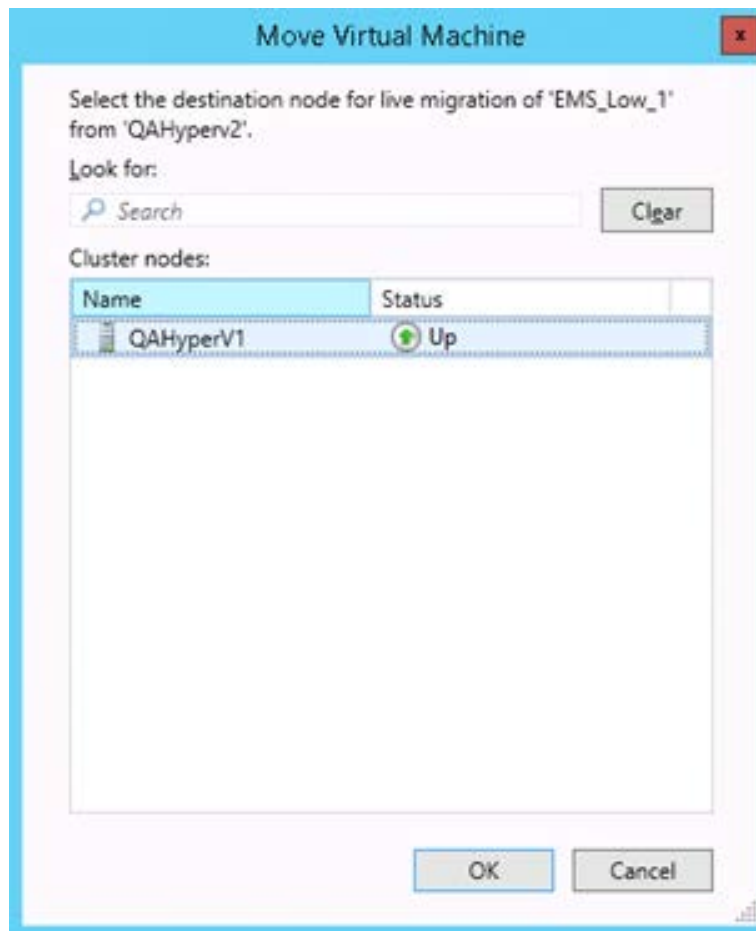
Figure F-5: Hyper-V Live Migration





The following screen is displayed:

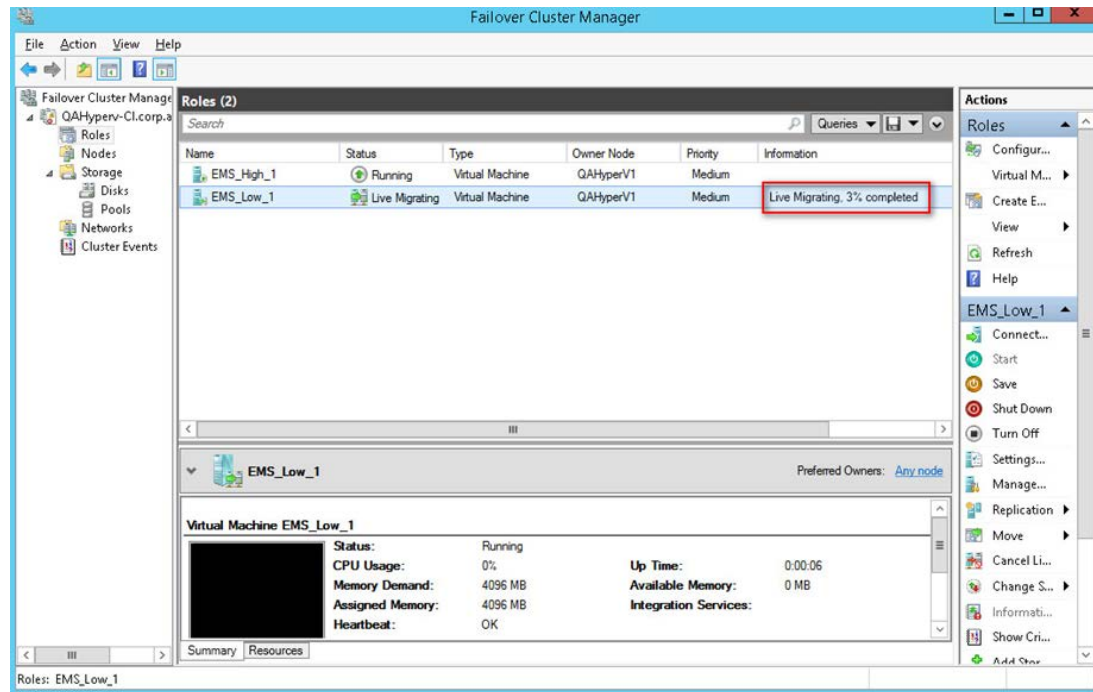
**Figure F-6: Move Virtual Machine**



2. Select the relevant node and click **OK**.

The migration process starts.

**Figure F-7: Hyper-V Migration Process Started**



After the migration has completed, the EMS application will run seamlessly on the VM on the new cluster's node.

## G Installing X.509 User-Defined Certificates

The procedures in this appendix describe how to install X.509 user-defined certificates on EMS server components and on AudioCodes devices where your site requires comprehensive security measures that may not be satisfied using the default certificates provided by AudioCodes.

**Note:**

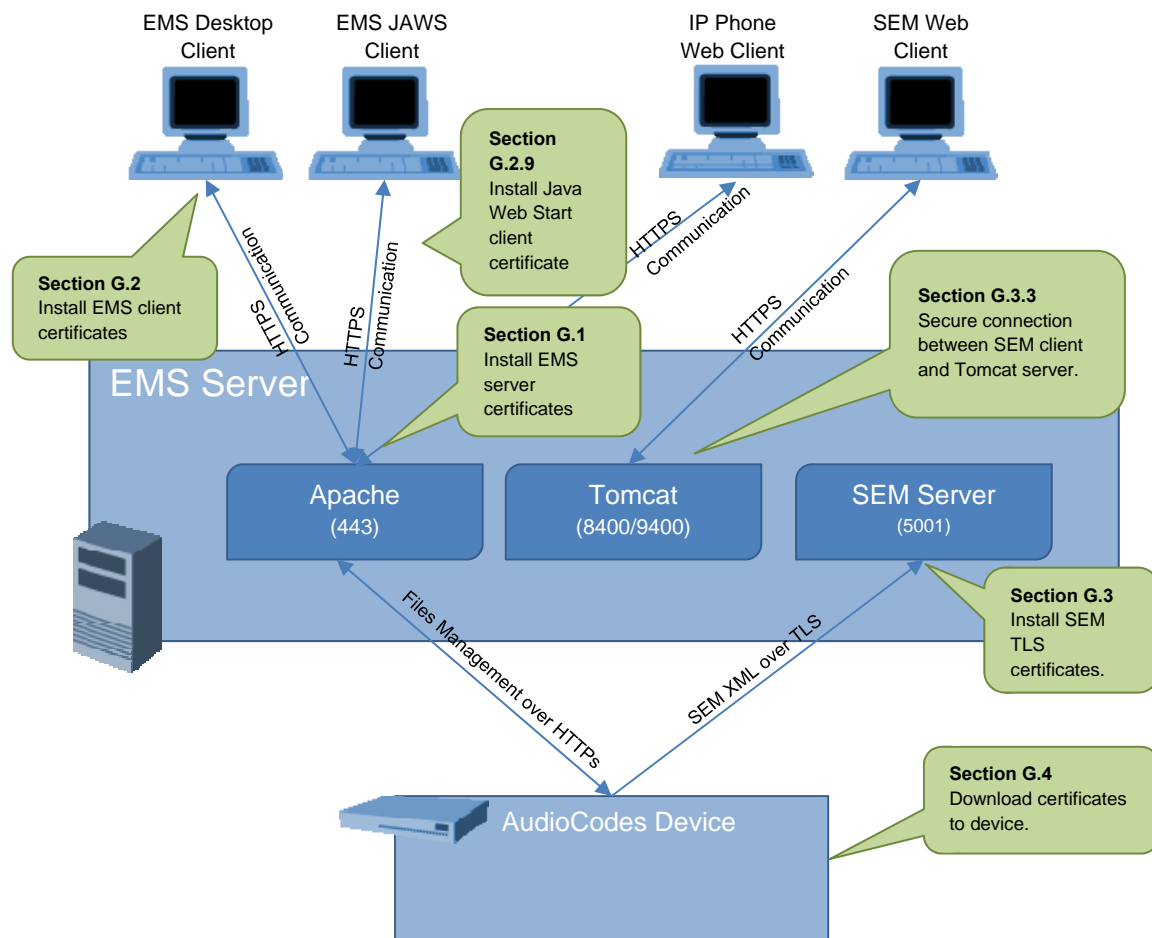
- It is highly recommended to read this appendix before commencing the procedures. The certificates request and signing process with the CA may take time and should therefore be completed before starting the certificate update procedures.
- The configuration described in this appendix is maintained following an upgrade of the EMS server.

This appendix describes the following procedures (which should be performed in the order shown below):

- Installing User-defined certificates on EMS server (see Section [G.1](#) on page [229](#)).
- Installing User-defined certificates on EMS client (see Section [G.2](#) on page [233](#)).
- Installing User-defined SEM TLS certificates (see Section [G.3](#) on page [245](#)).
- Downloading certificates to the AudioCodes device (see Section [G.4](#) on page [226](#)).
- Cleaning up directories (see Section [G.5](#) on page [262](#)).

The figure below illustrates the various EMS components and certificate implementations.

**Figure G-1: User-Defined Certificates**



## G.1 Installing User-Defined Certificates on EMS Server

This procedure describes how to install user-defined certificates on the EMS server.

### G.1.1 Step 1: Generate a new Private Key for EMS Server

This step describes how to generate a new Private Key for the EMS server.

➤ To generate a new private key for EMS server:

1. Login to the EMS server as *acems* user (default password is *acems*).
2. Switch user to *root* (default password is *root*).

```
su - root
```

3. Generate a server private key. When asked to enter the pass phrase – enter a unique passphrase, e.g. “pass\_1234”.

```
cd /etc/httpd/conf.d/ssl.key/  
mv server.key server.key.ORIG  
openssl genrsa -des3 -out server.key 2048  
  
Generating RSA private key, 2048 bit long modulus  
.....  
+++  
.....+++  
e is 65537 (0x10001)  
Enter pass phrase for server.key: pass_1234  
Verifying - Enter pass phrase for server.key: pass_1234
```

### G.1.2 Step 2: Generate a Certificate Signing Request (CSR) for EMS Server

This step describes how to generate a Certificate Signing Request (CSR) for the EMS server.

➤ To generate certificate signing request:

1. Create a new directory for server certificates:

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

2. Generate a Certificate Signing Request (CSR). When asked for the CSR fields, enter values that describe your site deployment:

```
cd /home/acems/server_certs  
openssl req -new -key /etc/httpd/conf.d/ssl.key/server.key -  
out server.csr  
  
Enter pass phrase for server.key: pass_1234  
You are about to be asked to enter information that will be  
incorporated into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]: **IL**

State or Province Name (full name) [Berkshire]: .

Locality Name (eg, city) [Newbury]: .

Organization Name (eg, company) [My Company Ltd]: **AudioCodes**

Organizational Unit Name (eg, section) []: .

Common Name (eg, your name or your server's hostname) []:

**EMS\_SERVER**

Email Address []: .

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

3. Apply the proper ownership for the generated CSR file:

```
chown acems:nbif server.csr
```

4. Transfer the CSR file to your PC (see Appendix [H](#) on page [263](#) for guidelines on how to transfer files).
5. Send the CSR file to the Certificate Authority (CA).

### G.1.3 Step 3: Receive the New Certificates from the CA

You will receive the following files from the CA:

- Your (EMS server) certificate – rename it to “server.crt”
- Root certificate – rename it to “root.crt”
- Intermediate CA certificates (if such certificates exist) – rename them to “ca1.crt”, “ca2.crt” etc.

Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGAlUEAxMM
RU1TlFJPTlQgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTE1MDUwMzA4NTE0MFowKjET
...
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuXNJol0
L6V8lzUYOfHrEiq/6g==
-----END CERTIFICATE-----
```

If you have not received PEM format certificates or you are not sure that the certificates files are in the correct format, see Appendix I on page 265 for guidelines on how to verify and convert certificates to the PEM format.



**Note:**

- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above because the Apache server is configured with these filenames.



**Important:** If you have installed an HA system and wish to install user-defined server certificates, the HA system must firstly be uninstalled, and then you must perform the following procedures separately on both server machines (as stand-alone machines). See Section 14.6 on page 174 for uninstalling the HA system.

### G.1.4 Step 4: Transfer the New Certificates to the EMS Server

This step describes how to transfer the new certificates to the EMS server.

➤ **To transfer the new certificates to the EMS server:**

- Transfer the new certificates files as described in the previous step – to the EMS server (see Appendix H on page 263 for guidelines on how to transfer files).

Place the new files in the `/home/acems/server_certs` directory.

## G.1.5 Step 5: Update Apache Configuration

This step describes how to update the Apache configuration.

### ➤ To update the Apache configuration:

- Open the file `/etc/httpd/conf.d/passphrase` and update the following line with the new passphrase (as specified in Section [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)).

```
echo "pass_1234"
```

## G.1.6 Step 6: Updating Apache Certificates

This step describes how to update Apache certificates.

### ➤ To update Apache certificates:

1. Login to the EMS server as user `root`.
2. Backup the existing Apache configuration:

```
cd /etc/httpd/conf.d/ssl.crt
mv server.crt server.crt.ORIG
mv server_root.crt server_root.crt.ORIG
mv server_chain.pem server_chain.pem.ORIG
```

3. Switch to the directory where you copied the certificate files:

```
cd /home/acems/server_certs
```

4. Create certificate chain file. Note that intermediate CA certificates (`ca1`, `ca2`) are optional and depend on your Certificate Authority.

```
cat ca1.crt >> server_chain.pem
cat ca2.crt >> server_chain.pem
cat root.crt >> server_chain.pem
```

5. Update Apache configuration:

```
cp server.crt /etc/httpd/conf.d/ssl.crt/server.crt
cp root.crt /etc/httpd/conf.d/ssl.crt/server_root.crt
cp server_chain.pem /etc/httpd/conf.d/ssl.crt/server_chain.pem
```

6. Apply proper ownership for new configuration files:

```
chown root:root /etc/httpd/conf.d/ssl.crt/*
```



## G.1.7 Step 7: Restart Apache

This step describes how to restart the Apache server.

➤ To restart the Apache server:

- Restart the Apache server to reload certificates.  
Execute the following command as user *root*:

```
service httpd restart
```

## G.2 Installing User-Defined Certificates on EMS Client

This procedure describes how to install user-defined certificates on the EMS client.

### G.2.1 Step 1: Generate a new Private Key for EMS Client

This step describes how to generate a new private key for the EMS client.

➤ To generate a certificate signing request:

1. Login to the EMS server as *acems* user (default password is *acems*).
2. Switch user to *root* (default password is *root*).

```
su - root
```

3. Create a new directory for client certificates:

```
mkdir /home/acems/client_certs  
chmod 777 /home/acems/client_certs
```

4. Generate a client private key. When asked to enter the pass phrase – enter a unique passphrase, e.g. “pass\_1234”.

```
cd /home/acems/client_certs  
openssl genrsa -des3 -out client.key 2048  
  
Generating RSA private key, 2048 bit long modulus  
.....  
+++  
.....+++  
e is 65537 (0x10001)  
Enter pass phrase for client.key: pass_1234  
Verifying - Enter pass phrase for client.key: pass_1234
```

## G.2.2 Step 2: Generate a Certificate Signing Request (CSR) for EMS Client

This step describes how to generate a Certificate Signing Request (CSR) for the EMS client.

### ➤ To generate a Certificate Signing Request (CSR):

1. Generate certificate signing request. When asked for the CSR fields, enter the appropriate values that describe your deployment:

```
cd /home/acems/client_certs
openssl req -new -key client.key -out client.csr
```

Enter pass phrase for client.key: **pass\_1234**

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]: **IL**

State or Province Name (full name) [Berkshire]: .

Locality Name (eg, city) [Newbury]: .

Organization Name (eg, company) [My Company Ltd]: **AudioCodes**

Organizational Unit Name (eg, section) []: .

Common Name (eg, your name or your server's hostname) []: **EMS\_CLIENT**

Email Address []: .

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:

2. Apply the proper ownership for the generated CSR file:

```
chown acems:nbif client.csr
```

3. Transfer the CSR file to your PC.
4. Send the CSR file to the Certificate Authority (CA).

### G.2.3 Step 3: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (EMS client) certificate – rename this file to “client.crt”.
- Root certificate – rename this file to “root.crt”; since you are submitting CSRs to the same CA – this is the same root certificate that was received from the CA (see Section [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)).
- Intermediate CA certificates (if such files exist) – rename these files to “ca1.crt”, “ca2.crt” etc.

Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGAlUEAxMM
RU1TIFJPTlQgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTE1MDUwMzA4NTE0MFowKjET
...
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IFl jnb+yvREuewprOz6TEExNJol0
L6V81zUYOfHrEiq/6g==
-----END CERTIFICATE-----
```



#### Notes:

- The above files are required in the following steps. Make sure that you obtain these files and save them on your PC before proceeding.
- Use the exact filenames as mentioned above because the Apache server is configured with these filenames.

### G.2.4 Step 4: Transfer the New Certificates to the EMS Server

This step describes how to transfer the new certificates to the EMS server.

#### ➤ To transfer the new certificates to the EMS server:

1. Transfer the new certificates files that you received from the CA (described in the previous step) to the EMS server (see Appendix [H](#) on page [263](#) for guidelines on how to transfer files.).

Copy the new files to the `/home/acems/client_certs` directory.

## G.2.5 Step 5: Generate the Client Keystore

This step describes how to generate the client keystore that contains all required certificates and the private key for the EMS client.

### ➤ To generate the client keystore:

1. Login to the EMS server as user *root*.
2. Switch to the directory where you copied the client certificate files:

```
cd /home/acems/client_certs
```

3. Create a certificate chain file. Note that intermediate CA certificates (ca1, ca2) are optional and depends on your Certificate Authority.

```
cat ca1.crt >> client_chain.pem
cat ca2.crt >> client_chain.pem
cat root.crt >> client_chain.pem
```

4. Create the PKCS#12 file:

```
openssl pkcs12 -export -name ems -in client.crt -inkey
client.key -certfile client_chain.pem -out client.p12
```

```
Enter pass phrase for client.key: pass_1234
Enter Export Password: password
Verifying - Enter Export Password: password
```

5. Verify the path to your Java JDK keytool to be used in the following steps to generate the keystore, e.g., /usr/java/jdk<jdk\_version>/bin/keytool.
6. Generate the keystore by executing the following command (in a single line). When asked for destination/source keystore password, type *password* or define your own custom passphrase.

```
"<Java JDK bin path>\keytool" -importkeystore -destkeystore
keystore.jks -srckeystore client.p12 -srcstoretype pkcs12 -
alias ems
```

```
Enter destination keystore password: password
Re-enter new password: password
Enter source keystore password: password
```

7. Import root certificate (root.crt) into the keystore. When asked for destination/source keystore password, type *password*. Confirm that you trust the certificate by answering **yes**.

```
"<Java JDK bin path>\keytool" -importcert -file root.crt -
keystore keystore.jks
```

```
Enter keystore password: password
Owner: CN=EMS_ROOT, O=ACL
Issuer: CN=EMS_ROOT, O=ACL
Serial number: 1
Valid from: Fri Jan 01 02:00:00 IST 2010 until: Wed Jan 01
02:00:00 IST 2020
Certificate fingerprints:
```

```
...
Trust this certificate? [no]: yes
Certificate was added to keystore
```

8. Change the ownership of the generated file:

```
chmod 777 keystore.jks
```

## G.2.6 Step 6: Transfer Client Keystore File to PC

This section describes how to transfer the client keystore file to the PC that runs the EMS client.

➤ **To transfer the keystore file to the EMS client:**

- Transfer the file /home/acems/client\_certs/keystore.jks from the EMS server to the PC that runs the EMS client.

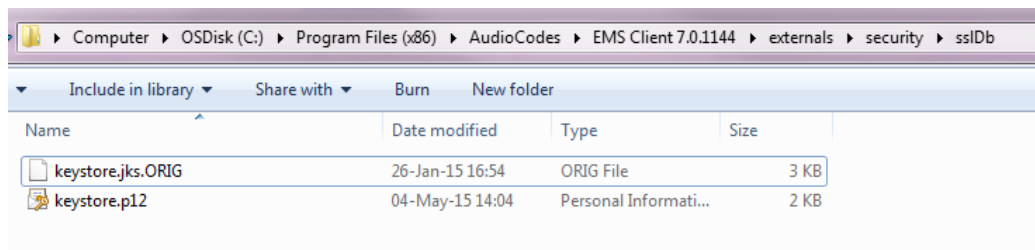
## G.2.7 Step 7: Stop EMS Client Application

This step describes how to stop the EMS client application.

➤ **To stop the EMS client:**

1. On the PC that runs EMS client, close EMS client application.
2. Navigate to: C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\security\sslDb
3. Rename the existing keystore.jks file to keystore.jks.ORIG.

**Figure G-2: Java Keystore**



**Note:** If you have performed an EMS upgrade, copy the keystore file generated in this step to the new EMS client.

## G.2.8 Step 8: Update EMS Client Configuration

This step describes how to update the EMS client configuration. Do one of the following:

- If you have installed the EMS client locally on the PC, update its configuration as described below.
- If you are using Java Web Start to connect to the EMS server, proceed to Section **Error! Reference source not found.** on page **Error! Bookmark not defined.**

➤ **To update the EMS client configuration:**

1. On the PC that runs EMS client, close the EMS client application.
2. Copy the generated java keystore file 'keystore.jks' to the following directory  
C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\security\sslDb
3. If you defined a custom (non-default) passphrase in Section G.2.8 on page 238 , open the file  
C:\Program Files (x86)\AudioCodes\EMS Client <Client-Version>\externals\configurationProperties\sslConfig.properties  
and update the following line with the new passphrase:

```
sslPassword=password
```

## G.2.9 Step 9: Update Java Web Start Client Certificate

This step describes how to update the Java Web Start Client Certificate.



**Note:** Apply this procedure if you are connecting to the EMS server using Java Web Start (i.e., <https://EMS-IP/jaws>). Skip this procedure when installing the EMS client using the AudioCodes-supplied Installation DVD.

### ➤ To update the Java Web Start client certificate:

1. Login to the EMS server as *acems* user (default password is *acems*) and then switch user to root (default password is *root*).
2. Change directory to jaws directory under EMS server main directory:

```
cd /ACEMS/server_X.Y.Z/jaws/
```

3. Run jaws\_certificates.sh script:

```
./jaws_certificates.sh
```

4. The certificate replacement process starts as follows:

```
*****
***** START JAWS CERTIFICATES PROCESS *****
*****
Please enter location of keystore.jks (default: /opt/ssl/)
```

5. Enter the path where you copied the client keystore.jks file (see G.2.6 on page 237) - */home/acems/client\_certs* and press Enter:

```
Enter keystore.jks path (press Enter for default):
/home/acems/client_certs
```

6. The Java Web Start will be updated with new client certificate. If warnings are produced in the process – ignore them.

```
checking /home/acems/client_certs/ ...
keystore.jks: OK

    Extracting jar files...
=====

=====
Start updating files... [Mon May 11 08:30:50 GMT 2015]
=====

    Creating jar for re-signing
=====
\t ---> configurationProperties
\t ---> emsSwVersionFiles
\t ---> help
\t ---> images
```

```

\t ---> localeProperties
\t ---> mibs
\t ---> sounds
\t ---> security

    Jars re-signing
=====
Linux OS
\t Signing jars with self created key
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not
timestamped. Without a timestamp, users may not be able to
validate this jar after the signer certificate's expiration
date (2025-05-08) or after any future revocation date.
jar signed.

.
.
.

*****
**** Customization Process Finished Successfully ****
*****

```



**Note:** If the provided path doesn't contain the keystore file (three retries are possible), the replacement process will fail, displaying the following errors:

```

Enter keystore.jks path (press Enter for default):
/home/acems/client_certs
checking /home/acems/client_certs ...
keystore.jks: Not Exists
Enter keystore.jks path (press Enter for default): /opt
checking /home/acems/client_certs .....
keystore.jks: Not Exists
Enter keystore.jks path (press Enter for default): /opt
checking /home/acems/client_certs ... ..
keystore.jks: Not Exists
*****
!!!!!! JAWS CERTIFICATE PROCESS FAILED !!!!!

```

Verify that you copied the keystore file in Section [G.2.6](#) on page 237.



7. Before connecting with JAWS, do one of the following:
  - JAWS For Chrome:  
Delete directory C:\Users\<pc user>\Downloads\JavaWebStart
  - JAWS for IE:  
Delete directory C:\Users\<pc user>\AppData\Local\Temp\JavaWebStart.
8. Redirect the JAWS URL for HTTPS using the EMS Server Manager (see Section 12.8.11 on page 152).

### G.2.9.1 Connecting to JAWS for Advanced Versions

If you have installed Java Versions 7 or 8 on your PC, you need to update the Java security level on your PC for your EMS client to function correctly.



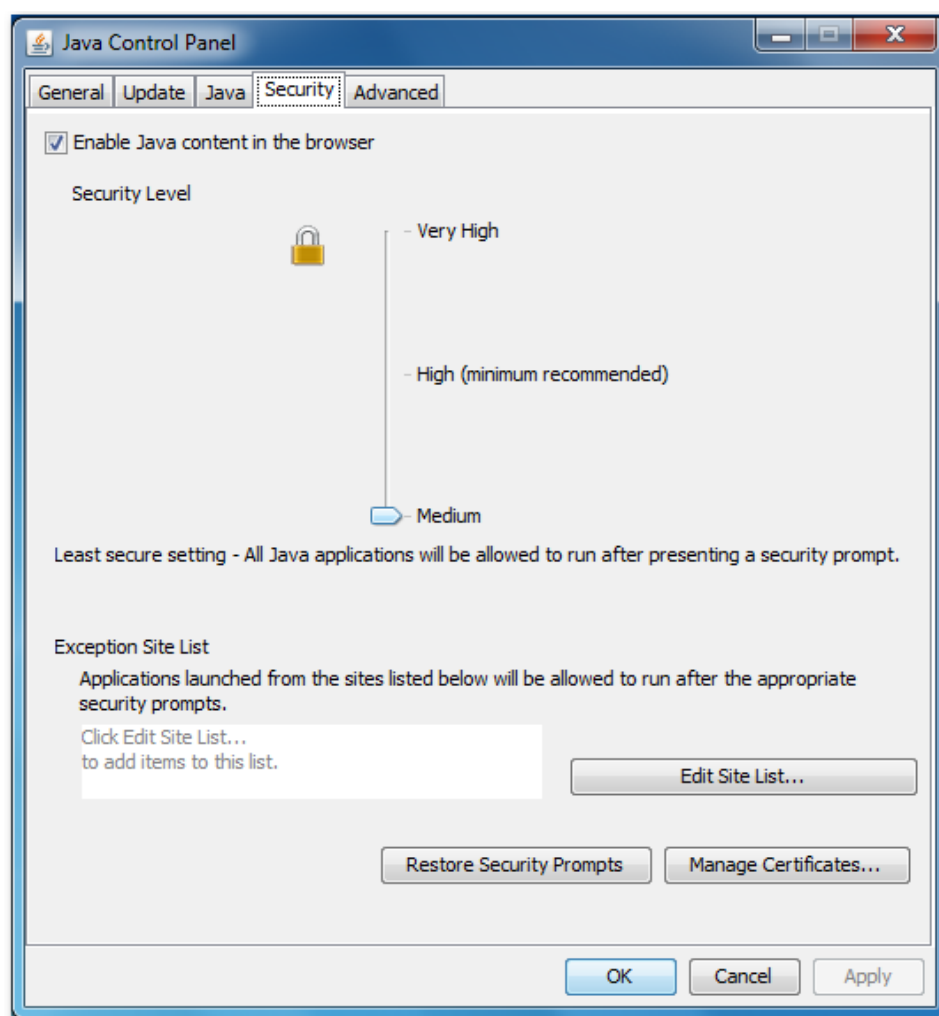
**Note:** This procedure is relevant for both HTTP and HTTPS connections.

#### G.2.9.1.1 Using Java Version 7

If you have installed Java Version 7 on your EMS client, do the following:

1. Open the Java Control Panel (**Start > Program Files > Control Panel > Java**).
2. Click the **Security** tab, and then set the 'Security Level' to **Medium**.

**Figure G-3: Java Control Panel (Version 7.2)**



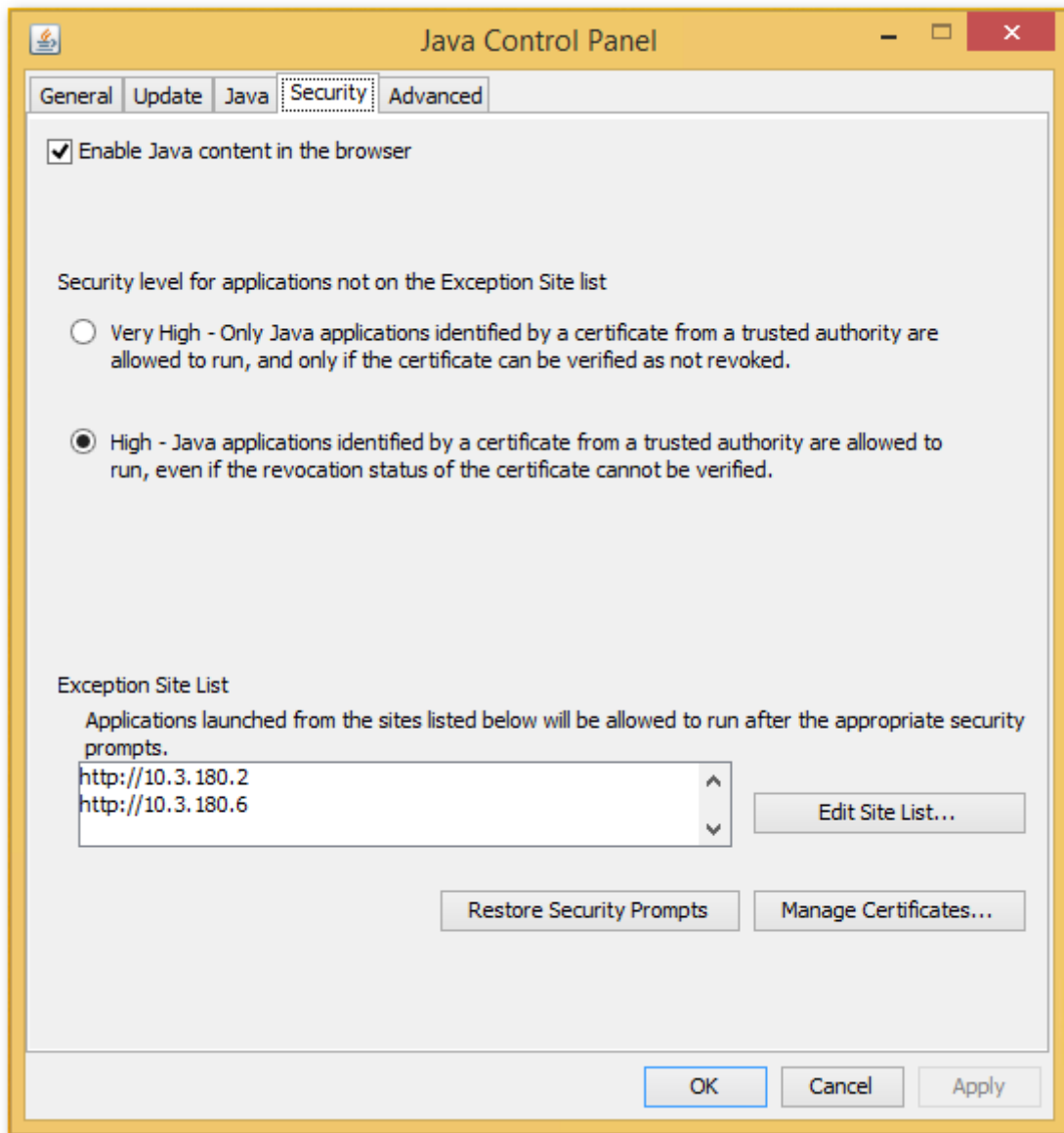
3. Click **OK**.

### G.2.9.1.2 Using Java Version 8

If you have installed Java Version 8 on your EMS client, do the following:

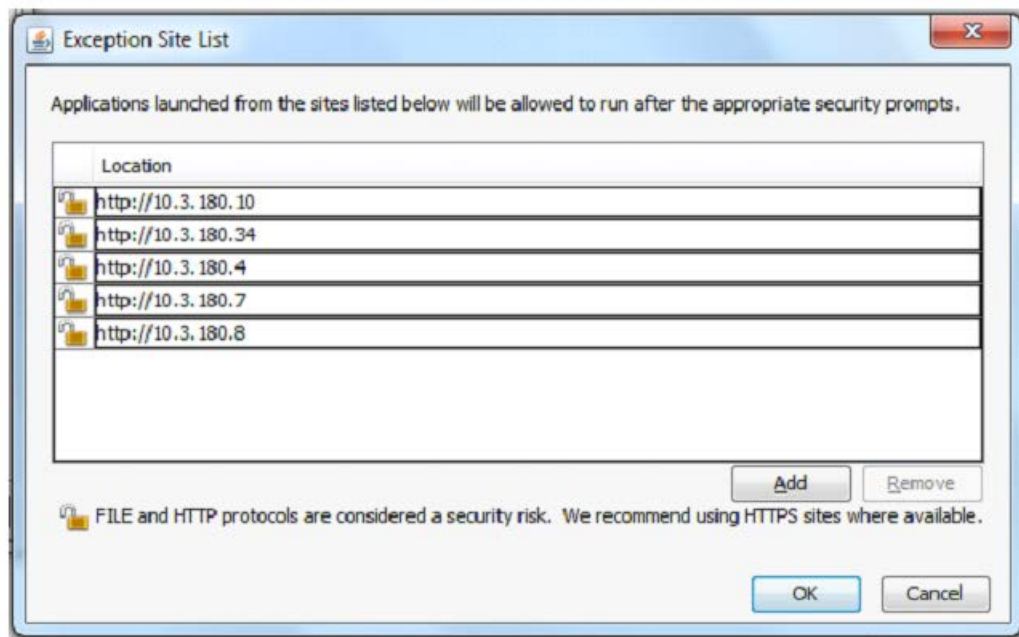
1. Open the Java Control Panel (**Start > Program Files > Control Panel > Java**).
2. Click the **Security** tab and set the Security Level to **High**.

**Figure G-4: Java Control Panel (Version 8.0)**



3. Click **Edit Site List...**, and then click **Add**.

**Figure G-5: Exception Site List**



4. Enter the server IP address in *http://<server IP>* format.
5. Click **OK** to close the Exception Site List window.
6. Click **OK** to close the Java Control Panel.

## G.3 Installing User-Defined Certificates on SEM Server

This procedure describes how to install user-defined certificates for the SEM server application, which is installed on the EMS server.



**Note:** The procedures described in this section are only required for customer sites where the SEM server is installed.

### G.3.1 Step 1: Generate Keystore for SEM Server

This step describes how to generate the keystore that contains all the required certificates and private key for the SEM server.



**Note:** This procedure uses the same certificates that were generated for the EMS server / Apache server in steps [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#) to [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)

➤ To generate the SEM server keystore:

1. Login to the EMS server as user *root*.
2. Switch to the directory where you copied the server certificate files:

```
cd /home/acems/server_certs
```

3. Create the server PKCS#12 file:

```
openssl pkcs12 -export -name ems -in server.crt -inkey  
/etc/httpd/conf.d/ssl.key/server.key -certfile  
server_chain.pem -out server.p12
```

Enter pass phrase for server.key: **pass\_1234**

Enter Export Password: **password**

Verifying - Enter Export Password: **password**

4. Verify the path to your Java JDK keytool to be used in the following steps to generate the keystore.  
e.g. `/usr/java/jdk<jdk_version>/bin/keytool`.
5. Generate the keystore by executing the following command (in a single line).  
When asked for destination/source keystore password, type *password*.

```
"<Java JDK bin path>\keytool" -importkeystore -destkeystore  
keystore.jks -srckeystore server.p12 -srcstoretype pkcs12 -  
alias ems
```

Enter destination keystore password: **password**

```
Re-enter new password: password
Enter source keystore password: password
```

6. Import the root certificate (root.crt) from the saved location (see Section [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)) to the keystore. When asked for destination/source keystore password, type *password*. Confirm that you trust the certificate by answering **yes**.

```
"<Java JDK bin path>\keytool" -importcert -file root.crt -
keystore keystore.jks

Enter keystore password: password
Owner: CN=EMS_ROOT, O=ACL
Issuer: CN=EMS_ROOT, O=ACL
Serial number: 1
Valid from: Fri Jan 01 02:00:00 IST 2010 until: Wed Jan 01
02:00:00 IST 2020
Certificate fingerprints:
...

Trust this certificate? [no]: yes
Certificate was added to keystore
```

## G.3.2 Step 2: Update SEM Server Configuration

This step describes how to update the SEM server configuration.

### ➤ To update SEM Server configuration:

1. Login to the EMS server as user *root*.
2. Backup the original SEM keystore:

```
cd /opt/ssl
mv keystore.jks keystore.jks.ORIG
```

3. Copy the new keystore.jks created above:

```
cp /home/acems/server_certs/keystore.jks .
chown emsadmin:dba keystore.jks
chmod 644 keystore.jks
```

4. If you configured a custom password(in Section [G.2.8](#) on page [238](#)) to protect keystore, update the following line in /ACEMS/server\_X.Y.Z/externals/configurationProperties/sslConfig.properties file:

```
sslPassword=password
```

5. To enable SEM server to work securely with ACL devices, update the following line in /ACEMS/server\_X.Y.Z/externals/configurationProperties/acVQMConfig.properties file (1 for TLS only, 2 For TLS/TCP combined mode):

```
SocketType = 0
```

6. Restart the EMS server (Stop/Start Application option) using the Ems Server Manager (see Section [12.5.1](#) on page [106](#)).

### G.3.3 Step 3: Update Tomcat Server Configuration

This section describes how to update the Tomcat server configuration to secure the connection between the Web browser and SEM server.

➤ **To update the Tomcat server configuration:**

1. Connect to the EMS server as user *root*.
2. Backup the original Tomcat keystore:

```
cd /ACEMS/EMS-VQ/tomcat/conf/  
mv keystore.jks keystore.jks.ORIG
```

3. Copy the new keystore created above:

```
cp /home/acems/server_certs/keystore.jks.  
chmod 644 keystore.jks
```

4. If you used a custom password to protect the keystore, update the following line in *server.xml* file:

```
keystoreFile="conf/keystore.jks" keystorePass="password"
```

5. Restart the Tomcat server:

- a. Login to the EMS Server Manager:

```
# EmsServerManager
```

- b. From the EMS Server Manager root menu, choose **Application Maintenance**.
- c. From the Application maintenance menu, choose **Web Servers**, and then press Enter.
- d. In the Web Servers menu, choose option **2** to stop the Tomcat Server.
- e. In the Web Servers menu, choose option **2** to start the Tomcat Server.

## G.3.4 Step 4: Redirecting SEM Client Browser to HTTPS URL

To automatically redirect the SEM client browser to an HTTPS URL, use the EMS Server Manager menu option (see Section 12.8.10 on page 152).

## G.3.5 Step 5: Setting Web Browser HTTPS Compatibility

This section describes how to set the Web browser to work properly with HTTPS.

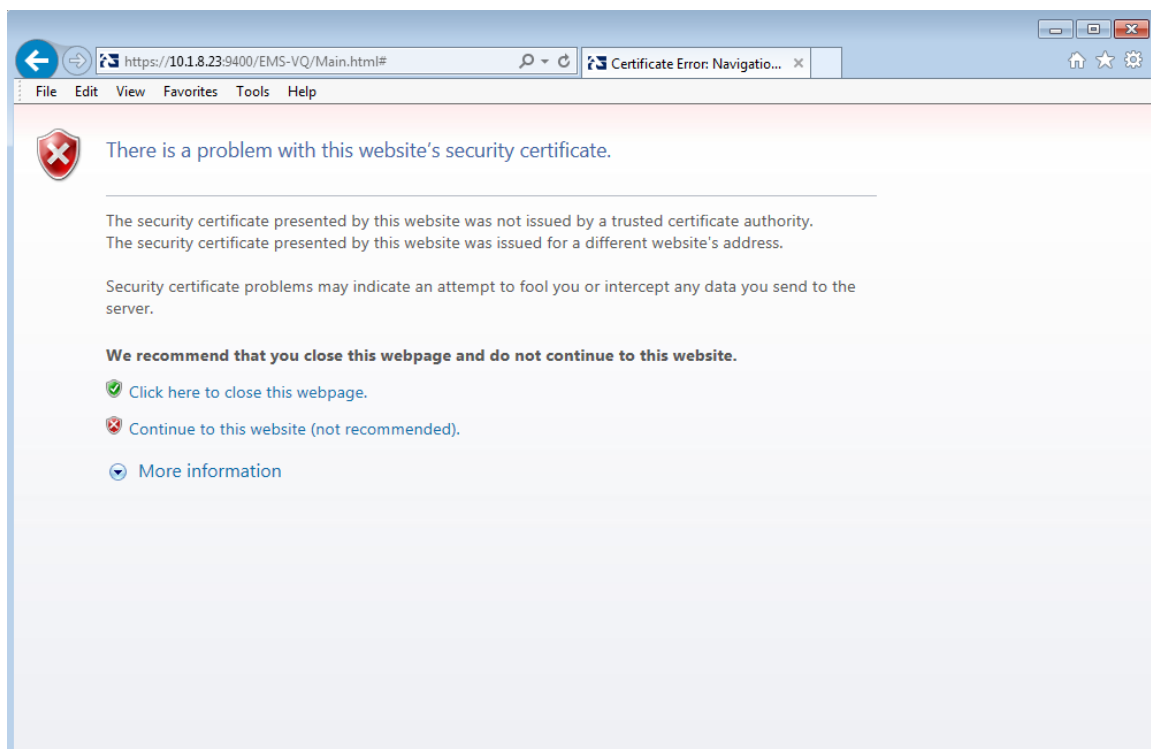
### G.3.5.1.1 Using an Internet Explorer Browser

This section describes how to set the Internet Explorer browser.

#### ➤ Do the following:

- When the following screen is displayed, select the “Continue to website (not recommended)” option.

**Figure G-6: Continue to Website**





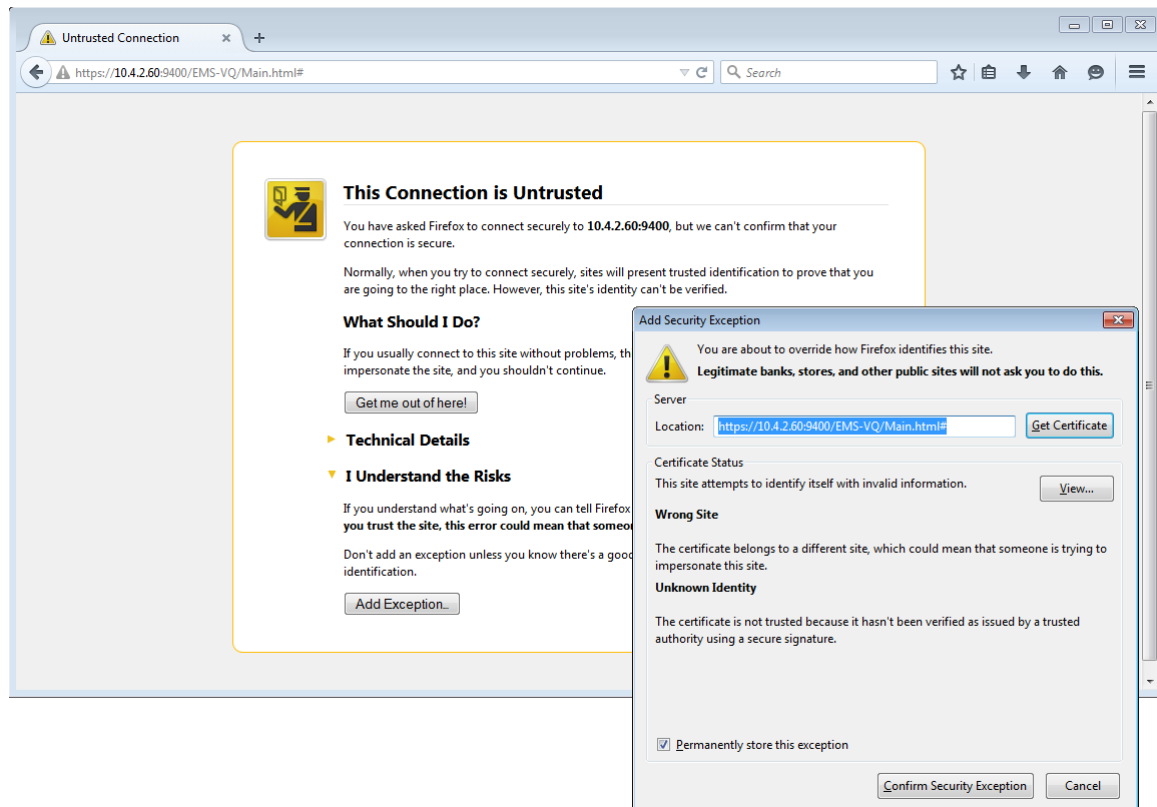
### G.3.5.1.2 Using a Mozilla Firefox Browser

This section describes how to set the Mozilla Firefox browser.

➤ **Do the following:**

1. When the following screen is displayed, click the “I Understand the Risks” option.
2. Click the **Add Exception** button, and then click the **Confirm Security Exception** button.

**Figure G-7: Mozilla Firefox Settings**



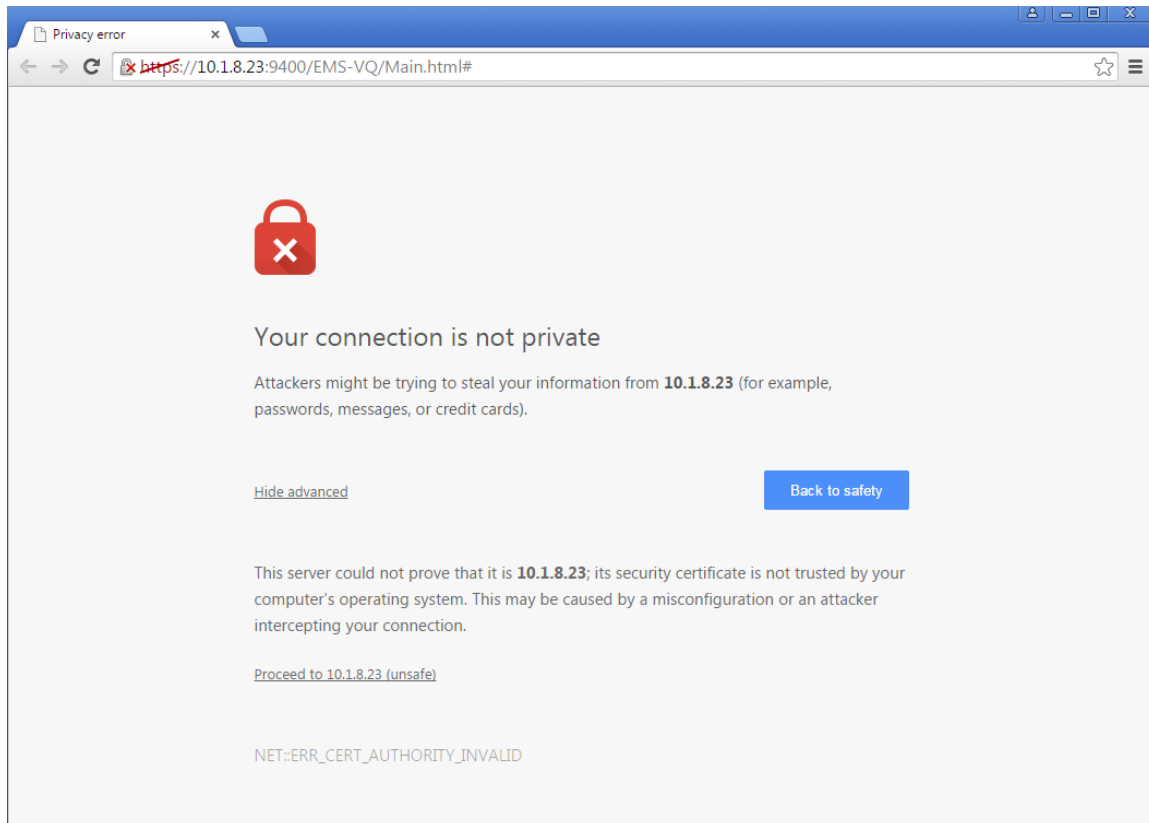
### G.3.5.1.3 Using a Chrome Browser

This section describes how to set the Chrome browser.

➤ **Do the following:**

1. When the following screen is displayed, click **Advanced** and then click the “Proceed to <Server IP> (unsafe)” link.

**Figure G-8: Chrome Browser Settings**



## G.4 Installing User-Defined Certificates on AudioCodes Devices

This section describes how to install user-defined certificates on AudioCodes devices. These certificates will be used to secure the connection between the device and EMS / SEM server.

This procedure is performed using the device's embedded Web server. This section describes how to install certificates for the following devices:

- Enterprise gateways and SBC devices (see Section [Error! Reference source not found.](#)).
- MP-1xx devices (see Section [Error! Reference source not found.](#) on page [Error! Bookmark not defined.](#)).

### G.4.1 Enterprise Gateways and SBC Devices


This section describes how to install user-defined certificates on Enterprise gateways and SBC devices.

The device uses TLS Context #0 to communicate with the EMS / SEM server. Therefore, the configuration described below should be performed for **TLS Context #0**.

#### G.4.1.1 Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➤ **To generate certificate signing request:**

1. Login to the device's Web server.
2. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
3. In the table, select the **TLS Context #0**, and then click the **TLS Context Certificate**  button, located below the table; the Context Certificates page appears.
4. Under the **Certificate Signing Request** group, do the following:
  - a. In the 'Subject Name [CN]' field, enter the device's DNS name, if such exists, or device's IP address
  - b. Fill in the rest of the request fields according to your security provider's instructions.
  - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

**Figure G-9: Certificate Signing Request Group**

▼ Certificate Signing Request

Subject Name [CN]	audio.com
Organizational Unit [OU] (optional)	Headquarters
Company name [O] (optional)	Corporate
Locality or city name [L] (optional)	Poughkeepsie
State [ST] (optional)	New York
Country code [C] (optional)	US

Create CSR

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwZjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLZwFk
cXVhcnRlcnMxZjAQBGNVBAOTCUNvbnBvcnF0ZTEVMBMGA1UEBxMMUG91Z2hrZWVw
c2llMREwDwYDVQQIEWhvZGZlc3Rk5Bw7F1ZFWCXQ7nvuocHtu7Nns071M
AQEBBQADgY0AMIGJAoGBAPhpf2t4OLy3FRk5Bw7F1ZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1ChoIPgoZNS0g6+5JAmJAA
lLNUnogjEsK7CF32uvolH//gFkhy5zleNvObI+25Pn38aJzEXc8DkGwZ19rROQRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbc1zkHdLFr+5BRuScKyGUXBM6
q7FGjFXAfzk1MmgnBMc/MYfSGTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LqoIi
nLnQpVCmbdva/B1QyEpFbQhZqpULJ8CSeSrrY3ru23AZeDUByyho90IkRbAp//+3
ZvnZZe5M5CB8Lg==
-----END CERTIFICATE REQUEST-----

```

- Copy the text and send it to the certificate authority (CA) to sign this request.

#### G.4.1.2 Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to "device.crt"
- Root certificate – rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) – rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```

-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0MFowKjET
...
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuXNJol0
L6V81zUYOfHrEiq/6g==
-----END CERTIFICATE-----

```


**Notes:**

- The above files are required in the following steps. Make sure that you obtain these files before proceeding and save them to the desired location.
- Use the exact filenames as mentioned above.

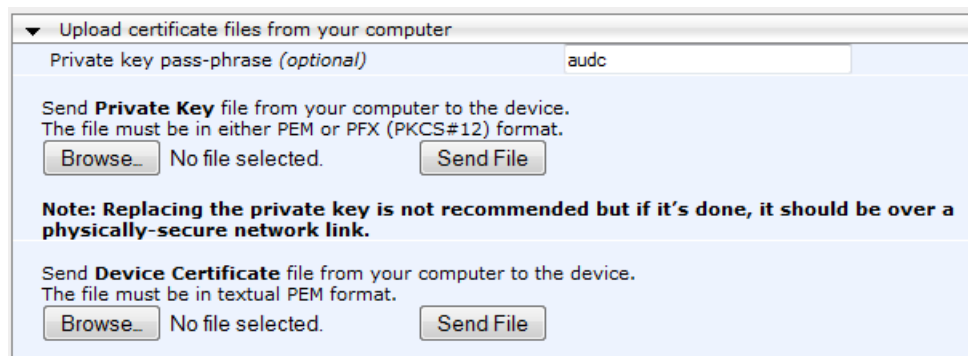
### G.4.1.3 Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

➤ **To update device with new certificate:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Certificate**  button, located below the table; the Context Certificates page appears.
3. Under the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.

**Figure G-10: Upload Certificate Files from your Computer Group**



▼ Upload certificate files from your computer

Private key pass-phrase (optional)

Send **Private Key** file from your computer to the device.  
The file must be in either PEM or PFX (PKCS#12) format.

No file selected.

**Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.**


Send **Device Certificate** file from your computer to the device.  
The file must be in textual PEM format.

No file selected.

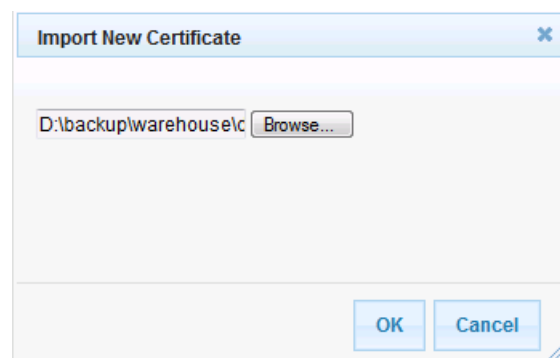
#### G.4.1.4 Step 4: Update Device's Trusted Certificate Store

This step describes how to update the device's Trusted Certificate Store.

➤ **To update device's trusted certificate store:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Trusted Root Certificates**  button, located below the table; the Trusted Certificates page appears.
3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

**Figure G-11: Importing Certificate into Trusted Certificates Store**



4. If you received intermediary CA certificates – ca1.crt, ca2.crt, etc. – import them in a similar way.

### G.4.1.5 Step 5: Configure HTTPS Parameters on the Device

This section describes how to configure HTTPS related parameters on the device.



#### Notes:

- You can optionally pre-stage the device with a pre-loaded ini file including this configuration (for more information, contact your AudioCodes representative).
- If you have enabled the Interoperability Automatic Provisioning feature, ensure that your template file is also configured as described in this procedure to maintain an active HTTPS connection after the template file has been loaded to the device.
- When you setup an HTTPS connection on the device, you must also enable HTTPS ("Enable HTTPS Connection") when adding the device to the EMS (refer to the *EMS User's manual*).

#### ➤ To configure HTTPS parameters on the device:

- Create a new text file using a text-based editor ( e.g., Notepad).
- Include the following ini file parameters for server-side authentication:
  - For Media Gateway and SBC Devices:

```
AUPDVerifyCertificates=1
```

- For MP-1xx devices, the ini file should include the following two lines:

```
AUPDVerifyCertificates=1
ServerRespondTimeout=10000
```

- Save and close the file.
- Load the generated file as "Incremental INI file" (**Maintenance** menu > **Software Update** > **Load Auxiliary Files** > **INI file** (incremental).
- Open the TLS Contexts page (**Configuration** menu > **System** > **TLS Contexts**).

Figure G-12: TLS Contexts

Index	Name	TLS Version	Cipher Server	Cipher Client	OCSP Server	Primary OCSP Server	Secondary OCSP Server	OCSP Port	OCSP Default Response
0	default	0	RC4:EXP	ALL:IADH	Disable	0.0.0.0	0.0.0.0	2560	Reject
1	EmptyCert	0	AES:RC4	ALL:IADH	Disable	0.0.0.0	0.0.0.0	2560	Reject
2	Context2	0	AES:RC4	ALL:IADH	Disable	0.0.0.0	0.0.0.0	2560	Reject
3	DTLSDefault	0	ALL	ALL:IADH	Disable	0.0.0.0	0.0.0.0	2560	Reject

Page 1 of 1. Show 10 records per page. View 1 - 4 of 4

**Selected Row #0**

Name: default  
 TLS Version: 0  
 Cipher Server: RC4:EXP  
 Cipher Client: ALL:IADH  
 OCSP Server: Disable  
 Primary OCSP Server: 0.0.0.0  
 Secondary OCSP Server: 0.0.0.0  
 OCSP Port: 2560  
 OCSP Default Response: Reject

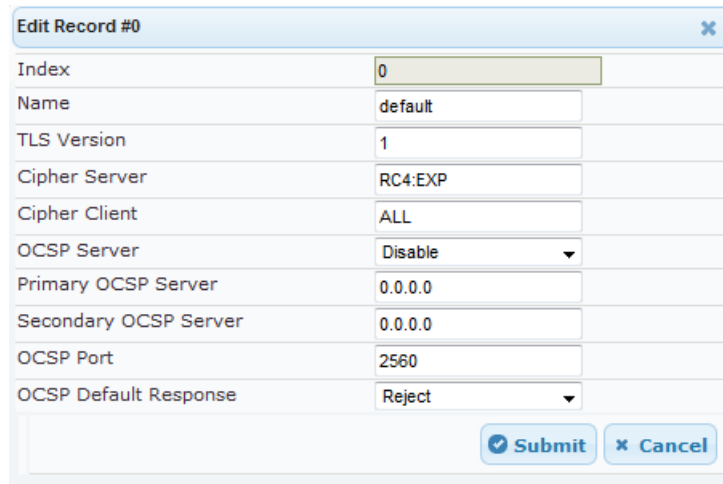
**Certificate Information**  
 Certificate subject: /CN=ACL\_4850326  
 Certificate issuer: /CN=ACL\_4850326  
 Time to expiration: 7239 days  
 Key size: 1024 bits  
 Private key: OK

**Links**  
 TLS Context Certificate  
 TLS Context Trusted Root Certificates

**TLS Expiry Settings**  
 TLS Expiry Check Start (days): 60  
 TLS Expiry Check Period (days): 7  
 Submit TLS Expiry Settings

6. In the table, select the **TLS Context #0**, and then click **Edit** button. The following screen is displayed:

**Figure G-13: TLS Contexts: Edit Record**



Index	0
Name	default
TLS Version	1
Cipher Server	RC4:EXP
Cipher Client	ALL
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

Submit Cancel

7. Set 'TLS Version' to **1** (TLS 1.0 only).
8. Set 'HTTPS Cipher Client' to **ALL**.

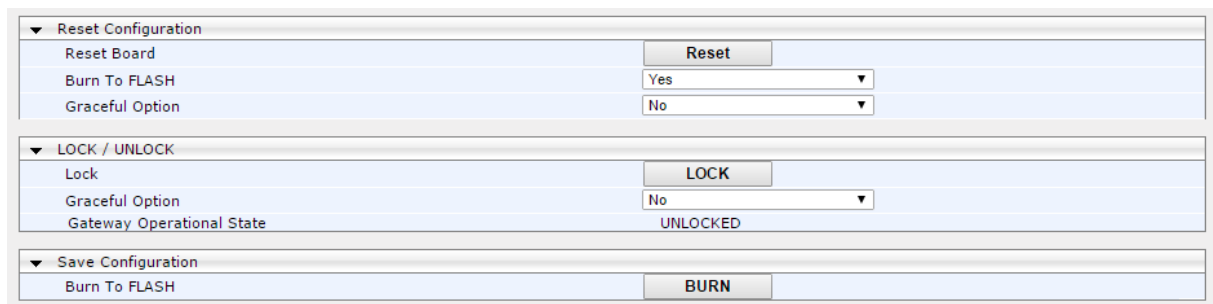
#### G.4.1.6 Step 6: Reset Device to Apply the New Configuration

This step describes how to reset the device to apply the new configuration.

➤ **To reset the device:**

1. In the top-level menu, click **Device Actions > Reset**. The following screen is displayed.

**Figure G-14: Device Reset**



<b>Reset Configuration</b>	
Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No
<b>LOCK / UNLOCK</b>	
Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED
<b>Save Configuration</b>	
Burn To FLASH	BURN

2. From the Burn to FLASH drop-down list, select **Yes**, and then click **Reset** button.  
The device will save the new configuration to non-volatile memory and reset itself.



## G.4.2 MP-1xx Devices

This section describes how to install user-defined certificates on the MP 1xx devices.

### G.4.2.1 Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➤ **To generate a CSR:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns\_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to **HTTP and HTTPS** (refer to the *MP-11x and MP-124 User's Manual*). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
3. Login to the MP-1xx Web server.
4. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
5. Under the **Certificate Signing Request** group, do the following:
  - a. In the 'Subject Name [CN]' field, enter the DNS name.
  - b. Fill in the rest of the request fields according to your security provider's instructions.
  - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

**Figure G-15: Certificate Signing Request Group**

▼ Certificate Signing Request

Subject Name [CN]	audio.com
Organizational Unit [OU] (optional)	Headquarters
Company name [O] (optional)	Corporate
Locality or city name [L] (optional)	Poughkeepsie
State [ST] (optional)	New York
Country code [C] (optional)	US

**Create CSR**

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwZjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLExxIZWFk
cXVhenRlcnMxEjAQBgNVBAoTCUNvbnBvcnF0ZTEVMBMGA1UEBxMMUG91Z2hrZWVw
c2llMRUwEwYDVQIEwhOZlMwYzZELMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPhpf2t4oLy3FRk5Bw7F1ZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CboIPgOZNS0g6+5JAmJAA
1LNUnocqjEsK7CF32uvolH//gFkhy5z1eNvObI+25Pn38aJzEXc8DkGwZ19rROqRZ
AgMBAAgGADANBgkqhkiG9w0BAQQAFAoBgQDihdqbclzkHdLFr+5BRusckYgUXBM6
q7FGjFXAfZk1MmgnBMc/MyfSGTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LqoIi
nLnQpVCmbdva/B1QyEpPhQhZqpULJ8CseSrrY3ru23AZeDUbYyhO90IkrBap//+3
ZvnZ2e5M5CB3Lg==
-----END CERTIFICATE REQUEST-----
```

6. Copy the text and send it to the certificate authority (CA) to sign this request.

### G.4.2.2 Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to “device.crt”
- Root certificate – rename this file to “root.crt”
- Intermediate CA certificates (if such files exist) – rename these files to “ca1.crt”, “ca2.crt” etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEw
JGUjETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBT
ZXJ2ZXVYMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1
UEBhMCRlIxEzARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9z
dGUxGzU2VydMvV1c jCCASEwDQYJKoZIhvcNAQEBBQADggEoADCCAQkCggEAPqd4Mz
iR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWUL
f7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMyb
FkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJ
uZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```



#### Notes:

- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above.

### G.4.2.3 Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

#### ➤ To update the device with the new certificate:

1. In the Certificates page, scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.
2. After the certificate successfully loads to the device, save the configuration with a device reset (see Section **Error! Reference source not found.** below).

#### G.4.2.4 Step 4: Update Device's Trusted Certificate Store

For the device to trust a whole chain of certificates you need to combine the contents of the root.crt and ca.crt certificates into a single text file (using a text editor).

➤ **To update the device with the new certificate:**

1. Open the root.crt file (using a text-based editor, e.g., Notepad).
2. Open the ca.crt file (using a text-based editor, e.g., Notepad).
3. Copy the content of the ca.crt file and paste it into the root.crt file above the existing content.

Below is an example of two certificate files combined (the file "ca2.crt" and the "root.crt") where the ca2.crt file contents are pasted above the root.crt file contents:

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNFQ0EyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNPWo6Gg5Ugxf1PjJeNggwnlQiUYhOK
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLdYzZp117J53FIsgnCSxpVqcYfMoBbCL/
0fmXKHWlPIIbovWpZddgz8UlpEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqe4yk
ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu
5B6wYNPOTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI
hfULeMjay4fzE4XnS9LDxZGjJ+nV9oJa7WaRB5t16nEJQ/7sLQIDAQABO3oweDAM
BgNVHRMEBTADAQH/MB0GA1UdDgQWBBrY2JQ1yZrvN4GifsXUB7AvctWvrTBjBgNV
HSMEQjBAGBTf6GbmQbo5b0CkLV8kW+Rg0AAhQElpCMwITEMMAoGA1UEChMDQUNM
MREwDwYDVQQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAdAsYyfcg
TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/o+
CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLrelGDC00yiKb4B0hlCq
hiemkXRe+eN7xcg0IfUo78VLTpuFMUhz0Bdn7Tue7QbiSayq2fy2ktHHOyDEKJGO
RUosIggVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V
XoAhN6pH17PMXLpClm9L/MlkVkmf0tp1bPmefrEBLO+np/O8F+P551uH0iOYA6Cc
Cj6oHGLq8RIndA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQQDFAhFTVNFUk9PVDCCASiWdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhnUQrS
667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+7/q
ebESJyW8pTLTszGQns2E214+U18sKHItPZvslDVUIX6xQiSYFDG1CDIPR5/70pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOI6LR72Ta9HMFJ4gyxJPUQA
jV3Led2Y4JObvBTnlka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPuf1wRjDwgl4G
BRw2MACYsu/M9z/H821UOICtsZ4oKUJMQbwjQ9lXI/HQkKRSTf8CAwEAAAN6MHgw
DAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAIYwSQYD
VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBAoTAF0FD
TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggEBAHqkg4F6
wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFCz1q4QVpQNYAwdBdEAKENznZttoP3aPZE
3EOx1C8Mw2uU4pOxD7B6pH0XO+oJ4LrxLB3SAJd5hW495X1RDF99BBA9eGUZ2nXJ
```

```
9pin4PWbnfc8eppq8Tp18jJMW0Zl3prfPt012q93iEalkDEZX+wxkHGZEqS4ayBn
8bU3NHt5qh0Egpa18hB/nth1xnAlm84lwxCbJW86AMRs2NznROyG695InAYaNlIo
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2k9STOpN
itSUGYwEagNsMU=
-----END CERTIFICATE-----
```



**Note:** The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

4. Save the combined content to a file named "chain.pem" and close the file.
5. Open the Certificates page and upload chain.pem file using the 'Trusted Root Certificate Store' field.

### G.4.2.5 Step 5: Configure HTTPS Parameters on Device

- Configure HTTPS Parameters on the device (see Section [Error! Reference source not found.](#) above).

### G.4.2.6 Step 6: Reset Device to Apply the New Configuration

This section describes how to apply the new configuration.

➤ To save the changes and reset the device:

1. Do one of the following:
  - On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
  - On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

Figure G-16: Maintenance Actions Page

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No <input type="button" value="v"/>
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

2. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
3. Click **OK** to confirm device reset; when the device begins to reset, a notification message is displayed.

## G.5 Cleanup

It is highly recommended to cleanup temporary files after certificates have been successfully installed. This is necessary to prevent access to security-sensitive material (certificates and private keys) by malicious users.

➤ **To delete temporary certificate files:**

1. Login to the EMS server as user *root*.
2. Remove the temporary directories:

```
rm -rf /home/acems/server_certs  
rm -rf /home/acems/client_certs
```

# H Transferring Files

This appendix describes how to transfer files to and from the EMS server using any SFTP/SCP file transfer application.



**Note:** .FTP by default is disabled in the EMS server.

➤ **To transfer files to and from the EMS server:**

1. Open your SFTP/SCP application, such as WinSCP or FileZilla.
2. Login with the acems/acems credential (all files transferred to the EMS server host machine are then by default saved to `/home/acems` directory).
3. Copy the relevant file(s) from your PC to the host machine (or vice-versa). For example using the FileZilla program, you drag the relevant file from the left pane i.e. in your PC directory to the right pane i.e. the `/home/acems` directory on the EMS server host machine.

This page is intentionally left blank.



# I Verifying and Converting Certificates

This appendix describes how to verify that certificates are in PEM format and describes how to convert them from DER to PEM if necessary.

➤ **To verify and convert certificates:**

1. Login to the EMS server as user *root*.
2. Transfer the generated certificate to the EMS server.
3. Execute the following command on the same directory that you transfer the certificate to verify that the certificate file is in PEM format:

```
openssl x509 -in certfilename.crt -text -noout
```

4. Do one of the following:
  - a. If the certificate is displayed in text format, then this implies that the file is in PEM format, and therefore you can skip the steps below.
  - b. If you receive an error similar to the one displayed below, this implies that you are trying to view a DER encoded certificate and therefore need to convert it to the PEM format.

```
unable to load certificate
12626:error:0906D06C:PEM routines:PEM_read_bio:no start
line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
```

5. Convert the DER certificate to PEM format:

```
openssl x509 -inform der -in certfilename.crt -out
certfilename.crt
```

# **Installation, Operation and Maintenance Manual**



[www.audiocodes.com](http://www.audiocodes.com)