

Product Description

Version 6.6



Table of Contents

1	Introducing AudioCodes' Element Management System (EMS)	13
1.1	Characteristics	13
1.1.1	EMS System Characteristics	13
1.1.2	Versatile System	13
1.1.3	FCAPS	13
1.1.4	Open Standard Design	14
1.1.5	Private Labeling	14
1.2	Architecture Overview	14
1.2.1	EMS Client Login on all EMS server Network Interfaces	15
1.3	Specifications	16
1.4	Supported VoIP Equipment	20
2	Fault Management	25
2.1	Alarm Processing	25
2.2	Alarm Context-Based View	26
2.3	Graphical Alarm Reports	26
2.4	Carrier-Grade Alarms System between the EMS and the Media Gateways	27
2.5	Alarm Priorities	27
2.6	Automatic Alarms and Events Clearing	27
2.7	Traps forwarding to the NMS	27
2.8	Save alarms into .csv file	27
2.9	Alarm Types	28
2.10	Alarms Actions	28
2.11	Detailed Information	28
2.12	Active and History Alarm Printing	28
2.13	Searching and Filtering Options	28
2.14	Change Alarm Browser View and Level	28
2.15	Audio Indication on Receipt of Alarms	29
2.16	Security	29
2.17	Alarm Archiving (History)	30
3	Session Experience Manager (SEM)	31
3.1	SEM Data Views	32
4	Entity Management and Configuration	35
4.1	Automatic Gateway Software Version Detection	35
4.2	Media Gateway Status Summary	35
4.3	Real-Time Color-Coded Media Gateway View	37
4.4	One-Click Access to Element Provisioning and Actions	37
4.5	Modular Workflow Process	38
4.5.1	Navigation Desktop	38
4.5.2	Configuration Desktop	38
4.5.3	Alarms Desktop	38
4.5.4	Performance Desktop	39
4.5.5	Context-Sensitive Behavior	39
4.6	Media Gateway Provisioning	40
4.6.1	Provisioning Types	41
4.6.2	Provisioning Frame - HA Indication	41
4.6.3	Color-Coding	41
4.6.4	Export / Import / Save Provisioning Data	41
4.6.5	Configuration Profiles for Quick Provisioning	41
4.6.6	Parameters Search	42

4.6.7	Master Profile.....	42
4.6.8	Media Gateway Offline Configuration.....	42
4.6.9	Configuration Verification, Upload and Download.....	42
4.6.10	Capability to Save and Restore Gateway Configuration	43
4.6.11	Upload INI file from the Gateway.....	43
4.6.12	Security.....	43
4.7	Media Gateways Maintenance Actions	44
4.7.1	CPE and Blades	44
4.7.1.1	Software Upgrade and Regional Files Distribution	44
4.7.1.2	Save Configuration into Flash Memory	44
4.7.1.3	Download INI file to Device	45
4.7.1.4	Configuration Data file Download and Upload Support	45
4.7.1.5	Multiple Gateways Lock / Unlock	45
4.7.1.6	Resetting a Gateway	45
4.7.1.7	Actions on Multiple MGs in one command.....	45
4.7.2	Mediant 5000, 8000 Maintenance Actions	45
4.7.2.1	Element Provisioning and Actions in Once	46
4.7.2.2	Online Software Upgrade Wizard.....	46
4.7.2.3	Backup / Restore of the Media Gateway Configuration	46
4.7.2.4	GW Log Files Collection.....	46
4.7.2.5	TP INI file Collection.....	46
4.7.2.6	Move TP Board	46
5	Performance Management	47
5.1	Alarm Severity and Gateway/Board/Channel Distribution Summary Screens	48
5.2	Real-Time Performance Monitoring – Pre-defined Graphs	49
5.3	Customized Real-Time and History (Background) Graphs	49
5.3.1	Real-Time Graphs	50
5.3.2	History (Background) Performance Monitoring	50
5.4	Aggregated PMs	50
5.5	Performance Thresholds	50
6	Security Management	51
6.1	FIPS Compliance	51
6.2	Network Communication Security	52
6.2.1	EMS Client <-> EMS Server.....	53
6.2.2	EMS Server <-> Mediant 5000/8000 Media Gateways	53
6.2.3	EMS Server <-> Mediant 600/800/1000/2000/3000 and MediaPack.....	53
6.2.4	Media Gateways Access Control.....	53
6.3	EMS Operator Authentication and Authorization.....	54
6.3.1	Centralized RADIUS or TACACS+ Servers User Profile.....	55
6.3.2	EMS Application User Profile	55
6.3.2.1	EMS User Management: Session Inactivity Timer.....	56
6.3.2.2	EMS User Management: User Accounts Inactivity Timer	56
6.3.2.3	EMS User Management: Password Complexity and Maintenance Extensions	56
6.3.2.4	Operator Password Expiration Extension	56
6.3.2.5	EMS User Security Levels.....	57
6.3.2.6	Login Information Display.....	58
6.3.3	Integration with CAC Card.....	58
6.3.4	Actions Journal	59
7	Virtualized EMS Server	61
8	EMS Server Management	63
8.1	EMS Server High Availability (HA).....	63
8.2	EMS Server File System Security and Maintenance.....	63

8.2.1	EMS Server Hardening.....	63
8.2.2	EMS Server File Integrity Checking.....	63
8.2.3	Intrusion Detection System.....	63
8.2.4	EMS Server Security Patches Loading during version Installation and Upgrade ...	64
8.2.5	Disk Mirroring (RAID 1) on Netra T5220	64
8.2.6	Syslog and Debug Recording.....	64
9	Northbound Interface.....	65

List of Figures

Figure 1-1: EMS Architecture	15
Figure 2-1: Alarm Browser in EMS Main Screen.....	25
Figure 2-2: Graphical Alarm Reports.....	26
Figure 2-3: Alarms History.....	30
Figure 4-1: Mediant 8000 Media Gateway 6310 Status Pane	35
Figure 4-2: Mediant 5000 Media Gateway 6310 Status Pane	36
Figure 4-3: Mediant 5000 8410 Status Pane.....	36
Figure 4-4: Mediant 3000 Status Pane.....	36
Figure 4-5: Mediant 800 MSBG Status Pane	36
Figure 4-6: Mediant 1000 Status Pane.....	36
Figure 4-7: Mediant 2000 Status Pane.....	37
Figure 4-8: MediaPack Media Gateway Status Pane	37
Figure 4-9: EMS Toolbar	38
Figure 4-10: Trunk Parameters Provisioning Screen	40
Figure 4-11: Maintenance Actions (Mediant 600/800/1000/2000/3000, MediaPacks)	44
Figure 4-12: Actions Bar Example- Mediant 5000/Mediant 8000Gateway Context.....	45
Figure 4-13: Right-click Maintenance Actions (Mediant 5000, 8000)	45
Figure 4-14: Maintenance Actions Icon and Popup Menu	46
Figure 5-1: Performance Measurement Displays.....	47
Figure 5-2: Alarm Severity and Board Distribution Summary Screens	48
Figure 5-3: Alarm Severity and Gateway/Channel Distribution.....	49
Figure 6-1: Firewall Configuration Schema	52
Figure 6-2: EMS Client Login Screen.....	54
Figure 6-3: EMS Users List	55
Figure 6-4: Actions Journal.....	59

List of Tables

Table 1-1: Element Management System (EMS) Specifications	16
Table 1-2: User Interface and External Interfaces Specifications	19
Table 1-3: Supported VoIP Equipment.....	20

Reader's Notes

Notice

This document describes the features for the AudioCodes' Element Management System (EMS).

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

© 2013 AudioCodes Inc. All rights reserved

This document is subject to change without notice.

Date Published: July-15-2013



Note: The Element Management System supports the following products:

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

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

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

Customer Support

Customer technical support and service are 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.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

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 600 and 1000 SIP User's Manual
Mediant 800 Gateway and E-SBC SIP User's Manual
Mediant 800 MSBR SIP User's Manual
Mediant 850 MSBR SIP User's Manual
Mediant 1000 Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2000 SIP User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 3000 SIP User's Manual
MGCP-MEGACO Product Reference Manual
Mediant 4000 E-SBC User's Manual
MediaPack User's Manual
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAMP Integration Guide
Element Management System (EMS) User's Manual
Element Management System (EMS) Online Help
Mediant 5000 / 8000 Media Gateway Installation, Operation and Maintenance Manual
Mediant 5000 / 8000 Media Gateway Release Notes
Mediant 5000 / 8000 Media Gateway Programmer's User Manual
Mediant 3000 TP-8410 OAM Guide
Mediant 3000 TP-6310 OAM Guide
Mediant 2000 OAM Guide
Mediant 1000 E-SBC OAM Guide
Mediant 1000 MSBG OAM Guide
Mediant 800 E-SBC OAM Guide
Mediant 800 MSBG OAM Guide
Mediant 600 OAM Guide

Reader's Notes

1 Introducing AudioCodes' Element Management System (EMS)

AudioCodes' Element Management System (EMS) is an advanced solution for standards-based management of Media Gateways within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of AudioCodes' families of Media Gateways, namely, the Mediant and MediaPack Series Analog VoIP Gateways.

The EMS enables Network Equipment Providers (NEPs) and System Integrators (SIs) the capability to offer customers rapid time-to-market and inclusive, cost-effective management of next-generation networks.

The standards-compliant EMS for media gateways uses distributed SNMP-based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a feature-rich management framework. It supports fault management, configuration and security. The EMS simultaneously manages AudioCodes' full line of multiple digital Media Gateway systems and their modules, as well as AudioCodes' analog VoIP Media Gateway Customer Premises Equipment (CPE).

1.1 Characteristics

1.1.1 EMS System Characteristics

The EMS features a Client/Server architecture, enabling customers to access the EMS from multiple, remotely located work centers and workstations. The entire system is designed in Java™, based on a consistent, vendor-neutral framework, and following recognized design patterns. Client - Server communication is implemented with Java™ RMI (Remote Method Invocation) protocol over TCP (Transmission Control Protocol).

The EMS enables multiple work centers and workstations to simultaneously access the EMS server (up to 25 concurrent clients connected to the server).

EMS Server, running on Sun™ Microsystems' Solaris™ (version 10) or on CentOS Linux (kernel version 5.3) . All management data is stored in the server, using Oracle 11g relational database software. EMS server High Availability is available for EMS server applications running on the Linux platform.

EMS Client, running on Microsoft™ Windows™, displays the EMS GUI screens that provide operators access to system entities. The operator-friendly GUI and hierarchical organization and Microsoft™ Explorer™ paradigm increase productivity and minimize the learning curve.

1.1.2 Versatile System

The EMS can simultaneously manage all platforms, even with different software versions running on these products.

The EMS application is backward compatible with the last three major versions of the gateway. For example, EMS version 6.6 manages gateway versions 6.6, 6.4 and 6.2.

1.1.3 FCAPS

AudioCodes' EMS supports **FCAPS** functionality:

- Fault management – see Section 2 page 25.
- Configuration and Entity management – see Section 4 page 35.
- Accounting (managed by a higher – level management system such as an NMS)
- Session Experience Manager (SEM) – see Section 3 on page 31 and Performance management – see Section 5 on page 47.
- Security management – see Section 6 on page 51.

1.1.4 Open Standard Design

EMS's open standard design allows for a seamless flow of information within and between the layers of the Telecommunications Management Network (TMN) model in accordance with the International Telecommunications Union (ITU) M.3010. It also enables smooth integration with existing and future network and service (NMS/Network Management System, OSS/Operation Support System) management solutions.

1.1.5 Private Labeling

Customization and labeling of the EMS and Media Gateways is performed according to their customer specific requirements. The private labeling feature enables telephone companies to use the EMS under their own corporate name, gateway name, logos and images.

The customization procedure involves preparing files and images and rebuilding a customized DVD.

The private labeling procedure covers the following items:

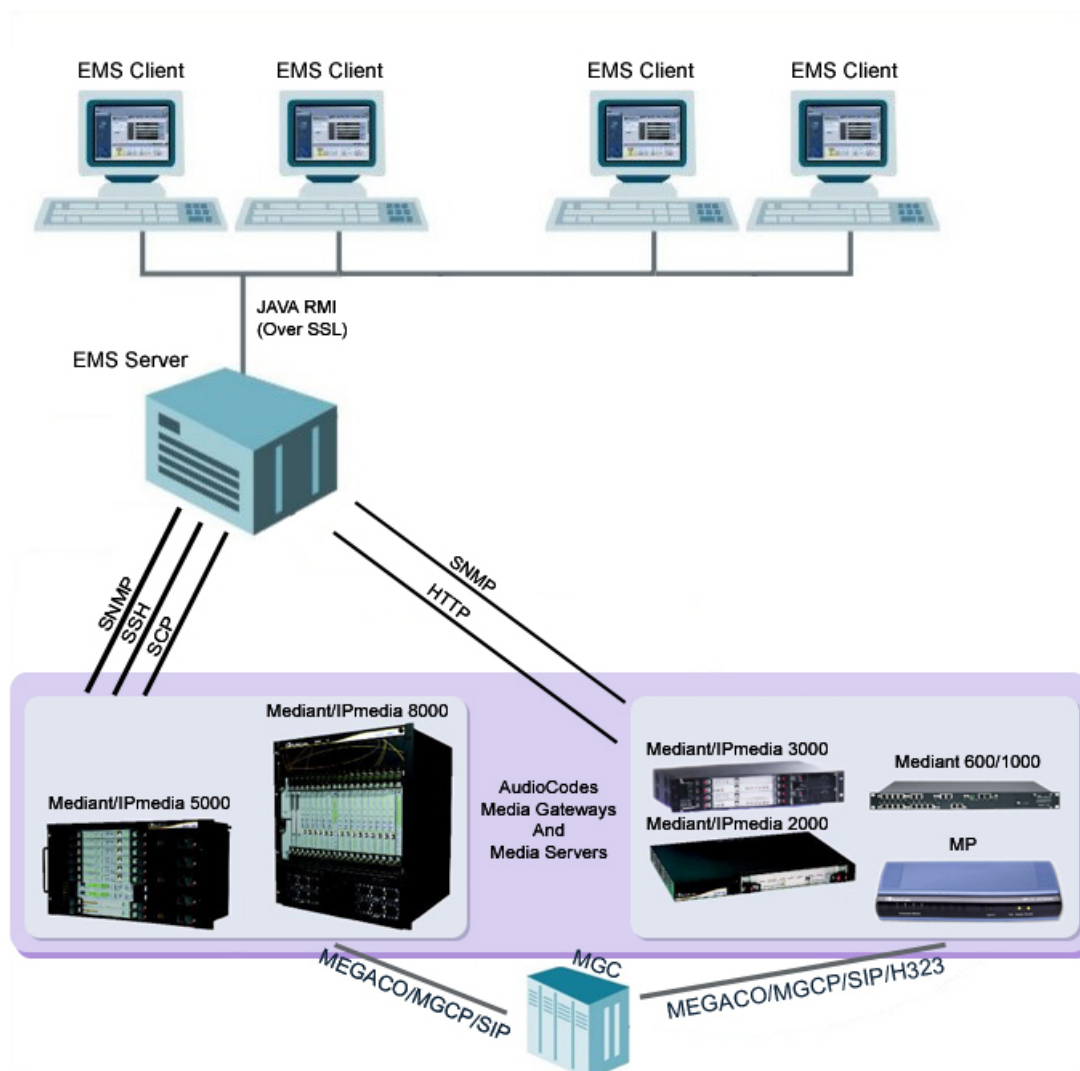
- The licence agreement presented during the installation process
- The telephone company's logos and icons
- The name of the telephone company, the names of its media gateways, and the names of the TP boards populating the gateways
- Online Help

1.2 Architecture Overview

The EMS is an open, standard-based, scalable management tool. Typically, the EMS manages the functions and capabilities within each gateway; however does not manage the connectivity between different gateways within the network. To support management of the connectivity between itself and other network elements, the EMS communicates upward to higher-level Network Management Systems (NMSs), according to ITU.T (International Telecommunication Union -Telecommunication Standardization Sector) M3.100 standards on the Telecommunications Management Network (TMN) layered model. This TMN-defined architecture for a layered Operations Support System (OSS) enables service providers to meet customer needs for rapid deployment of new services, as well as meet stringent quality of service (QoS) requirements. Figure 1-1 shows the EMS integrated in a network system.

1.2.1 EMS Client Login on all EMS server Network Interfaces

Figure 1-1: EMS Architecture



Note: The above figure is *representative*. It applies to *all* VoIP equipment supplied by AudioCodes.

1.3 Specifications

- Software Version Number: 6.6
- Release Date: Q2 2012
- Package and Upgrade Distribution: DVD

Table 1-1: Element Management System (EMS) Specifications

Subject	Description
TMN Standards	ITU-T Recommendation M.3010 series FCAPS functionality support
Fault Management	<ul style="list-style-type: none"> ■ Alarm fields and actions, according to ITU-T Recommendation X.733, 3GPP Recommendation 3G TS 32.111-1. ■ Alarm processing: 30 traps per second, continuously ■ Alarm archiving: up to six-month history for all Media Gateways (depending on disk size available). ■ Application includes context-sensitive Alarm Browser and Alarm History with various filtering and search options, detailed alarm description, Acknowledge and Delete actions processing and audio indication on receipt of alarms. ■ Automatic and Manual Alarm Clearing ■ Carrier-Grade alarms system performing constant re-synchronization of EMS and managed gateways to ensure that all the alarms are synchronized and up to date. ■ Combined alarms and journal allow users to correlate possible influence of user actions on systems behavior and alarms. ■ Alarms reports graphical representation. ■ Traps Forwarding to the Northbound Interface via SNMP, Mail, SMS or Syslog protocols. ■ Save alarms in a csv file
Media Gateways Automatic Detection and Monitoring	<p>When the MediaPack is connected to the network for the first time, it is automatically detected by the EMS and added to the managed gateways.</p> <p>A Summary of all managed gateways' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.</p>
Media Gateways Provisioning	<ul style="list-style-type: none"> ■ Adapts rapidly to changes in new Media Gateway software releases. ■ Based on hierarchy of managed objects concepts. ■ Online parameter provisioning support, with icons indicating provisioning type. ■ Profile-based provisioning, including Master Profile for all VoIP gateways and media servers, as well as for the TP-1610, TP-6310 and TP-8410 boards. ■ Search provisioning parameter ■ Configuration database of small gateways is kept inside the EMS. ■ Configuration database of large gateways is kept inside the Media Gateways.

Table 1-1: Element Management System (EMS) Specifications

Subject	Description
Security Management	<p>Complies with T1M1.5/2003-007R4 and covers two aspects: Network communication security and EMS application security.</p> <p>The EMS application complies with the USA Department of Defense standard-FIPS 140-2 (FIPS-Federal Information Processing Standards-US Government Security Standards for Cryptography modules) and the JITC (Joint Interoperability Test Command) lab.</p> <p>Encryption and authentication related software are now implemented using FIPS compliant third party software, Therefore, all encryption modules used by the EMS application are FIPS 140-2 certified.</p> <p>Network Communications Security</p> <p>EMS server's network is configured and its ports opened during installation.</p> <p>Interoperation with firewalls, protecting against unauthorized access by crackers and hackers. MediaPack, Mediant 1000, Mediant 2000, Mediant 3000 can be managed behind the NAT.</p> <p>EMS client-server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer).</p> <p>EMS server - Media Gateway communication is secured using SNMPv2c/SNMPv3, HTTP/HTTPS, Telnet and FTP over IPSec / SSH and SCP.</p> <p>Application Security</p> <p>User Management using a Radius server for centralized user authentication and Authorization or in the EMS application.</p> <p>EMS application: Users List. Authentication-based operator access according to user name, password, security level, login machine IP. Modification of user details and access rights, user removal, forced logout, user suspension, releasing users from suspension and user password change</p> <p>EMS application: Actions Journal of operators' activities, various filtering and search options.</p> <p>EMS Server Hardening</p> <p>EMS server hardening enables you to harden the Solaris 10 and Linux platforms for enhanced security performance. The hardening protects the EMS server from unauthorized access and hostile attack.</p>
Performance Management	<ul style="list-style-type: none"> ▪ Real-Time Graphics ▪ Historical Data Collection and Analysis

Table 1-1: Element Management System (EMS) Specifications

Subject	Description
Session Experience Management	<ul style="list-style-type: none"> ▪ Modular tool with separate views for Network, Statistics, Calls, Alarms and Reports. ▪ Graphic representation of managed devices/links in a Table, Map and Regions view with a popup summary of critical metrics. ▪ Voice quality diagnostics for devices/links and users in the VoIP network. ▪ Real-time, as well as historical monitoring of VoIP network traffic health. ▪ Call quality rating metrics (MOS, jitter, packet loss, delay (or latency) and echo). ▪ Call trend statistics according to key metrics, traffic load, average call duration and call success. ▪ SEM alerts based on user defined call success rate and quality thresholds. ▪ Active alarms and history alarms display. ▪ Monitoring of links quality between AudioCodes and non-AudioCodes devices such as Microsoft Lync 2010 Server. ▪ Filtering according to time range, devices and links.
Media Gateways Maintenance Actions	<p>Mediant 8000 Media Gateway and Mediant 5000 Media Gateway:</p> <ul style="list-style-type: none"> ▪ Online software upgrade via a Wizard ▪ Gateway installation, startup and shutdown ▪ All maintenance actions (lock, unlock, switchover, add / remove board, etc.) for each media gateway entity, via a convenient Graphical User Interface. ▪ Various Debug tools allowing collection of the data during the troubleshooting process. <p>Mediant 600, Mediant 800, Mediant 1000, Mediant 2000, Mediant 3000, and MediaPack:</p> <ul style="list-style-type: none"> ▪ Software files and Regional properties files (such as Voice Prompts, CAS and other files) can be loaded to the set of gateways. ▪ Actions (such as Lock / Unlock, Reset, Configuration Download, Upload, etc.) can be performed to the set of gateways.

Table 1-2: User Interface and External Interfaces Specifications

Subject	Description
User Access Control	Local EMS application or centralized RADIUS / TACACS+ users authentication and authorization.
Northbound Interface	Topology as CSV file, Alarms as SNMP v2c / SNMPv3 traps, PMs as CSV / XML files.
Southbound Interface	SNMPv2c / SNMPv3 , HTTP/HTTPS, SSH, SCP, NTP (possible over IPsec).
Multi-Platform	Java-based, JDK version 1.6.
Relational Database	Oracle 11g relational database is used for data storage.

1.4 Supported VoIP Equipment

The table below describes the supported VoIP equipment by the EMS application.

Table 1-3: Supported VoIP Equipment





Supported VoIP Equipment	Description
 MediaPack	<p>These analog VoIP gateways incorporate up to 24 analog ports to be connected either directly to an enterprise PBX (FXO), to phones, or to fax (FXS), supporting up to 24 simultaneous VoIP calls.</p> <p>(Refer to the product documentation for detailed information.)</p>
 Mediant 800 MSBG  Mediant 1000 MSBG	<p>These Multi-Service Business Gateways (MSBG) are networking devices that combine multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server.</p> <p>The device's Stand Alone Survivability (SAS) functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX.</p> <p>The devices also provide an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing.</p> <p>(Refer to the product documentation for detailed information.)</p>
 Mediant 1000 Media Gateway	<p>The Mediant 1000 media gateway is a convergence platform integrating an enterprise's data and telephony (voice/fax) communications providing a cost-effective, cutting-edge technology solution with superior voice quality and optimized packet voice streaming (voice, fax and data traffic) over the IP network. Designed to interface between TDM and IP networks in enterprises as well as in small-scale carrier locations, the Mediant 1000 Media Gateway supports multiple analog and digital modules with a variety in the number of spans, as well as mixed digital and analog configurations. The gateway supports up to 4 digital trunks (fully flexible, from a single trunk per module all the way to a single module with all 4 trunks) or as a purely analog configuration, supporting up to 24 analog ports (6 modules with 4 ports on each).</p>

Table 1-3: Supported VoIP Equipment



Supported VoIP Equipment	Description
 <p>Mediant 600 Media Gateway</p>	<p>The Mediant 600 media gateway supports multiple analog and digital modules with a variety in the number of spans, as well as mixed digital and analog configurations. The gateway supports up to 2 E1/T1/J1 spans (including fractional E1/T1); up to 8 ISDN Basic Rate Interface (BRI) interfaces; up to four FXO interfaces (RJ-11 ports) - for connecting analog lines of an enterprise's PBX or the PSTN to the IP network; up to 4 FXS interfaces (RJ-11 ports) - for connecting legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS interfaces can be connected to the external trunk lines of a PBX.</p> <p>(Refer to the product documentation for detailed information.)</p>
 <p>Mediant 2000 Media Gateway</p>	<p>The Mediant 2000 media gateway contains the TP-1610 cPCI VoIP communication board, an ideal building block for deploying high-density, high availability Voice over IP (VoIP) and wireless enterprise systems.</p> <p>The Mediant 2000 incorporates 2, 4, 8 or 16 E1 or T1 spans for connection, either directly to PSTN telephony trunks, or to an enterprise PBX, and two 10/100 Base-T Ethernet ports for redundant connection to the LAN.</p> <p>(Refer to the product documentation for detailed information.)</p>

Table 1-3: Supported VoIP Equipment


Supported VoIP Equipment	Description
 <p>Mediant 3000 Media Gateway</p>	<p>The Mediant 3000 media gateway is the medium-sized member of the family of market-ready, standards-compliant, media gateway systems.</p> <p>Main features: Redundant common equipment (Power, Controller, Ethernet Switch); Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SS7/SIGTRAN Interworking (SS7/PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant</p> <p>Applications: VoP Trunking gateways, IP-Centrex Gateways, VoP Access gateways</p> <p>Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; VoiceCoders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall-back to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1, SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP</p> <p>(Refer to the product documentation for detailed information).</p>

Table 1-3: Supported VoIP Equipment



Supported VoIP Equipment	Description
 <p>Mediant 5000 Media Gateway</p>	<p>The Mediant 5000 is the medium-sized member of the family of market-ready, standards-compliant, media gateway systems.</p> <p>Main features: Redundant common equipment (Power, Controller, Ethernet Switch) ; Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SS7/SIGTRAN Interworking (SS7/PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant</p> <p>Applications: VoP Trunking Gateways, IP-Centrex Gateways, VoP Access Gateways</p> <p>Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; VoiceCoders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall-back to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1, SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP</p> <p>(Refer to the product documentation for detailed information).</p>

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 <p>Mediant 8000 Media Gateway</p>	<p>The Mediant 8000 is the large-scale member of the family of market-ready, standards-compliant media gateway Voice Network products designed for the carrier environment.</p> <p>The Mediant 8000 reliability features include N+1 redundancy for media gateway boards, external interface redundancy and 1+1 redundancy for common equipment. The density of the gateway allows for a much smaller footprint in central office locations where space is at a premium.</p> <p>Main features: Redundant common equipment (Power, Fans, Controller, Ethernet switch); Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Field-proven, high voice quality; SS7/SIGTRAN Interworking; Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant Applications: VoP Trunking Gateways, IP Centrex gateways, VoP Access Gateways</p> <p>Selected Specifications: Up to 7,200 independent, simultaneous LBR VoP to PSTN voice calls; Voice coders include G.711, G.723.1, G.726, G.728, G.729A, Independent dynamic vocoder selection per channel; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall back to G.711 analog, fax and modem support; Call progress tones, VAD, CNG, Dynamic programmable jitter buffer, Modem detection, DTMF detection and generation.</p> <p>(Refer to the product documentation for detailed information).</p>

2 Fault Management

The EMS's high-level fault management functionality manages and displays all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system. The EMS's fault management comprises the Alarm browser and Alarms History.

Figure 2-1: Alarm Browser in EMS Main Screen

The screenshot displays the AudioCodes EMS Alarm Browser. The main window shows a list of 22 alarms. The left sidebar contains a navigation tree with options like Management, Networking, Call Control, Redundancy, Security, PSTN, Media, Time And Date, Inventory, Troubleshooting, and Boards. The top bar shows the user is logged in as 'gal54' with administration authorization.

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
<input type="checkbox"/>	minor	18:14:35 Feb 21 ...	10.77.10.130	RedundancyGroup#0	High Availability Alarm	Redundancy group have some HA mismatches. Boards :Board#1
<input type="checkbox"/>	major	18:14:35 Feb 21 ...	10.77.10.130	Board#17	Operative State Change	Board#17 is Disabled
<input type="checkbox"/>	major	18:14:35 Feb 21 ...	10.77.10.130	Board#17	Hardware Error Alarm	Board extraction from the chassis is underway (release button p
<input type="checkbox"/>	major	18:14:23 Feb 21 ...	10.77.10.130	Board#17	Operative State Change	Board#17 is Disabled
<input type="checkbox"/>	major	18:14:23 Feb 21 ...	10.77.10.130	Board#17	Hardware Error Alarm	Board extraction from the chassis is underway (release button p
<input type="checkbox"/>	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
<input type="checkbox"/>	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
<input type="checkbox"/>	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
<input type="checkbox"/>	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
<input type="checkbox"/>	major	14:23:44 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
<input type="checkbox"/>	major	14:23:47 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
<input type="checkbox"/>	major	14:21:05 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
<input type="checkbox"/>	major	02:47:12 Feb 19 ...	10.77.10.130	Board#6	Clock Synchronization Alarm	Clock synchronization state is free run
<input type="checkbox"/>	major	02:47:59 Feb 19 ...	10.77.10.130	Board#6	Clock Synchronization Alarm	Clock synchronization state is free run
<input type="checkbox"/>	major	16:07:17 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run
<input type="checkbox"/>	major	16:06:53 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run
<input type="checkbox"/>	major	16:06:47 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run

2.1 Alarm Processing

The EMS can typically process 20 SNMP traps per second continuously. When an alarm is received, it is parsed, stored in the database and immediately displayed in the Alarm browser. The Alarm browser displays current system faults at the top of the alarms list, allowing operators to identify the entity generating the alarm.

Operators can pause automatic updating of the displayed alarms to take a system snapshot.

2.2 Alarm Context-Based View

The EMS Alarm browser displays alarms and events according to an operator-selected context: Region, Media Gateway or board. This capability (to view the faults of an operator-specified system entity) enables operators to quickly and efficiently isolate and pinpoint a problem's precise location.

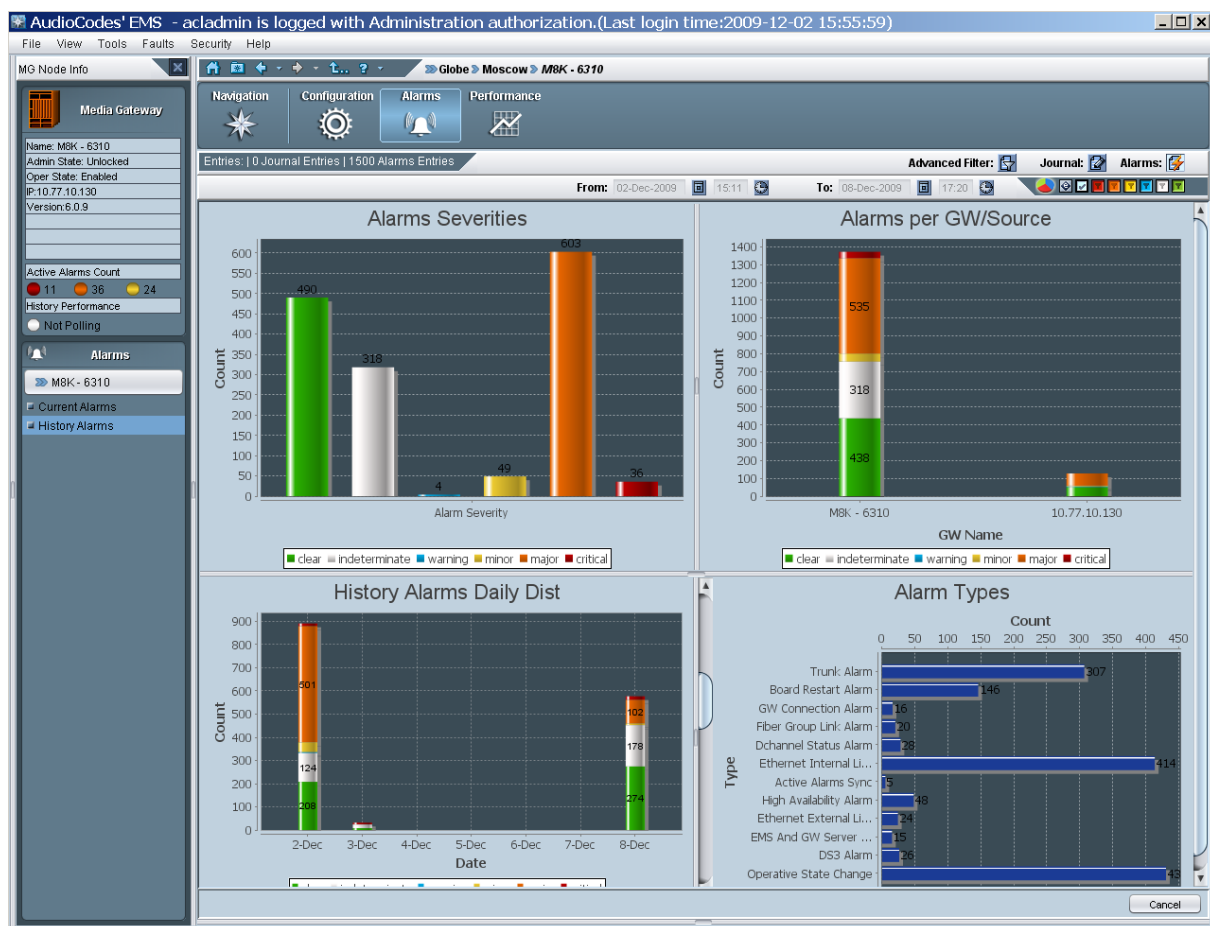
In addition to the context-sensitive current alarms view, operators can also view all Journal records and the Alarms History related to the selected context.

The EMS can display a combined table with all the alarms, events and journal records to correlate user activities with system behavior and responses. For example, you can filter according to time interval or gateway IP address.

2.3 Graphical Alarm Reports

The active and history alarms can be displayed as a set of predefined graphical reports upon a user request. Reports are generated according to the data that is displayed in the Active or History Alarm browser. Graphs include Alarms Severity and Types distribution.

Figure 2-2: Graphical Alarm Reports



2.4 Carrier-Grade Alarms System between the EMS and the Media Gateways

The EMS can synchronize with the media gateways on missed alarms which could occur due to network connectivity or other problems. EMS retrieves these missed alarms and adds them to the Alarm browser / History windows. Upon alarms retrieval, depending on the trap forwarding rules, alarms are also forwarded.

2.5 Alarm Priorities

According to industry-standard management and communication protocols (ITU-T Recommendation X.733, 3GPP Recommendation 3G TS 32.111-1), the EMS supports 6 prioritized alarm levels (Critical, Major, Minor, Warning, Info and Clear). Each is color-coded so that operators can quickly and easily comprehend severity level and prioritize corrective actions.

2.6 Automatic Alarms and Events Clearing

Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms browser (and transferred to Alarms History) by *the same entity (source) and the same Media Gateway* that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature is available for system debug purposes. Operators view the list of *only the currently active alarms*.

Events are automatically cleared from the Alarm browser after a predefined period of time (default – 3 days).

You can easily sort between alarms and events or filter events from the Alarm browser and Alarm History windows.

2.7 Traps forwarding to the NMS

All traps received by the EMS from managed media gateways (both proprietary and standard traps as well as those issued by the EMS application itself) can be forwarded to the NMS (Network Management System).

SNMP trap forwarding from the EMS application to a Northbound interface includes the following features:

- Multiple trap forwarding destinations
- Media gateway and EMS alarms and events can be forwarded in the following different types: SNMPv2c or SNMPv3 traps, Mail notifications, Mail to SMS, or Syslog messages.
- Each one of the trap destination users can filter trap forwarding according to the following trap types: (Event or Alarm); the source (EMS or Media Gateway); Alarm Severity or Media Gateway IP addresses.

2.8 Save alarms into .csv file

Viewed alarms can be saved in a *.csv file from the Alarm browser and Alarms History screens. The alarms in a *.csv file include all alarm fields viewed in the Alarm Details screen. The saved *.csv file can be viewed in Microsoft™ Excel™, enabling all Excel features (statistics, graphs) on it.

2.9 Alarm Types

The EMS classifies alarms under five basic types as required by network management standards:

- Communications Alarm: an alarm of this type is principally associated with the procedures and/or processes required to convey information from one point to another.
- QoS alarm: alarms notifying operators of Quality of Service degradation.
- Processing Error Alarm: software or processing fault.
- Equipment Alarm: alarms associated with an equipment fault, such as board or power supplier failures.
- Environmental Alarm: alarms such as temperature, power, fire, etc., associated with the physical environment in which the equipment is located.

2.10 Alarms Actions

Operators can perform the following actions regarding the displayed alarms:

- Acknowledge: informs the other operators that a problem diagnosis is underway.
- Manual clearing: removes inactive alarms from the operator's view.
- Last operator action performed on alarms, including 'User Name' and 'Action Time' can be viewed in the Alarms History pane.

2.11 Detailed Information

Quick access to detailed information on each alarm, including alarm type, probable cause and trap-specific information facilitates diagnosis and troubleshooting. Operators can add free text explaining how to resolve the problem or add information on each alarm displayed in the Alarm browser.

2.12 Active and History Alarm Printing

The EMS client can print the EMS alarms details and the Alarms History table.

2.13 Searching and Filtering Options

In addition to alarms displayed according to their context (entity) selected, alarms and events can be filtered according to their severity level, acknowledge status, and date and time.

In addition to severity, event, ack state, date and time filters, users can perform a string search in the Alarms History screen.

2.14 Change Alarm Browser View and Level

Operators can modify the Alarm browser's column order according to their preference. In addition, alarms can be sorted by any column (default sorting is according to time). Each user can select the alarms filtering level they wish to apply in their Alarm browser.

The following options are supported: Current Level Alarms (default), Node Level Alarms, Region Level Alarms, All Alarms - globe level.

2.15 Audio Indication on Receipt of Alarms

Users can choose whether to enable/disable an audio indication (a bell) when new alarms arrive.

2.16 Security

The actions that an operator is authorized to perform on alarms depends on the operator's security level, previously allocated to them by the administrator. Permission *to view* alarms is separate from permission *to respond* to alarms. All operator actions, such as alarm acknowledgement and clearing are logged in the EMS's Actions Journal (see Section [6.3.4](#) on page [51](#)).

2.17 Alarm Archiving (History)

All alarms received by the EMS are archived in the database. Extensive information related to the alarm is saved, together with the alarm itself; Region and Media Gateway placement and the failed entity's physical attributes.

The Alarms History screen provides EMS operators with a view of the alarms' history over an extended period of time (a history of at least one month, and up to 6 month is provided, depending on disk space available: 1000 alarms per day for digital media gateways and 100 alarms per day for analog media gateways). The Alarms History screen informs operators of the actions performed on each alarm, including the alarm's current state, the last action performed on the alarm and the name of the operator who performed the last action on this alarm.

Figure 2-3: Alarms History

AudioCodes' EMS - acldmin is logged with Administration authorization. Last login time:2009-12-05 15:55:59

File View Tools Faults Security Help

MG Node Info

Media Gateway

Name: M8K - 6310

Admin State: Unlocked

Oper State: Enabled

IP: 172.17.10.130

Version: 6.0.9

Active Alarms Count

● 11

● 36

● 23

History Performance

☐ Not Polling

Alarms

▶ M8K - 6310

Current Alarms

History Alarms

Navigation

Configuration

Alarms

Performance

Entries: 5 Journal Entries | 49 Alarms Entries

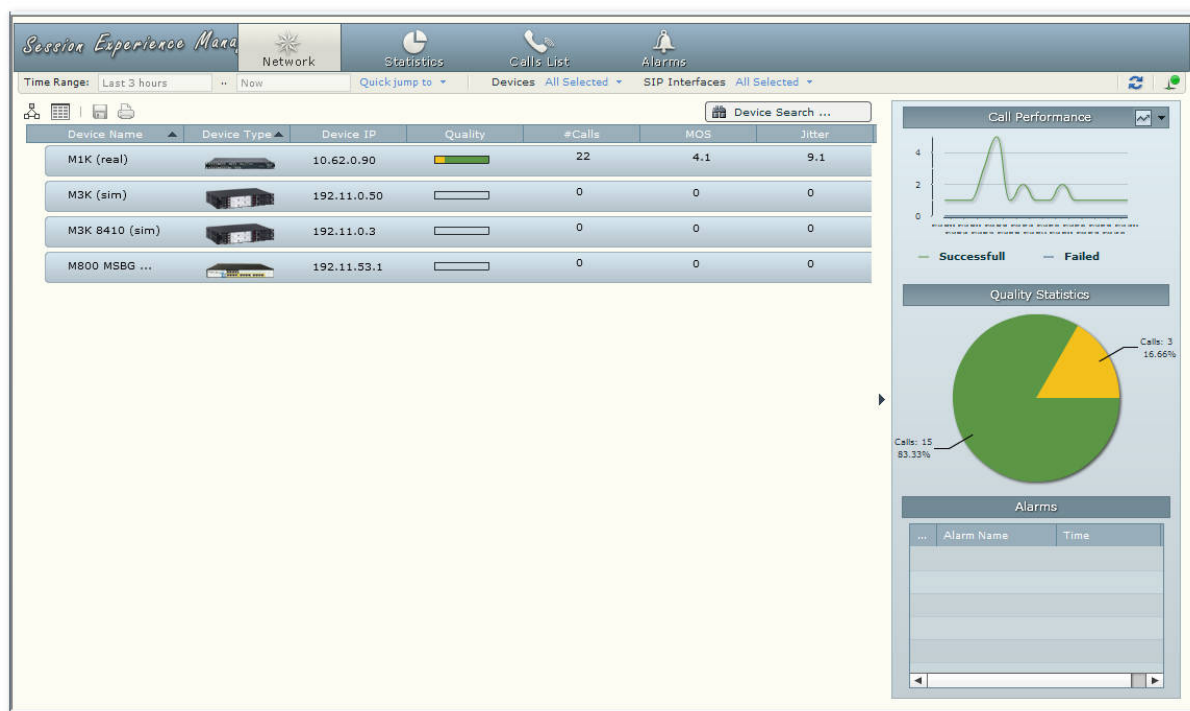
Advanced Filter: Journal: Alarms:

From: 02-Dec-2009 15:11 To: 08-Dec-2009 17:20

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator	Ack	Last Action
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:45 Dec 08...
minor	17:19:28 Dec 08 ...	M8K - 6310	Redundancy...	High Availability Alarm	Redundancy group have some HA ...	Moscow		Automatic Cleared	
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow	acldmin	Ack	14:31:32 Dec 09...
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow	acldmin	Ack	14:31:35 Dec 09...
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow	acldmin	Ack	14:31:33 Dec 09...
minor	17:19:28 Dec 08 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow	acldmin	Ack	14:31:32 Dec 09...
Journal	12:54:30 Dec 08 ...	M8K - 6310	BMS Server	Faults: Ack Alarm	Updated Alarm(s):Alarm 1.3.6.1.4...	Moscow	acldmin		
Journal	12:53:54 Dec 08 ...	M8K - 6310	BMS Server	Faults: Ack Alarm	Updated Alarm(s):Alarm 1.3.6.1.4...	Moscow	acldmin		
Journal	12:53:49 Dec 08 ...	M8K - 6310	BMS Server	Faults: Ack Alarm	Updated Alarm(s):Alarm 1.3.6.1.4...	Moscow	acldmin		
Journal	12:53:48 Dec 08 ...	M8K - 6310	BMS Server	Faults: Ack Alarm	Updated Alarm(s):Alarm 1.3.6.1.4...	Moscow	acldmin		
minor	20:39:04 Dec 02 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	20:39:04 Dec 02 ...	M8K - 6310	Redundancy...	High Availability Alarm	Redundancy group have some HA ...	Moscow	acldmin	Cleared	15:19:15 Dec 08...
minor	20:39:04 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow	acldmin	Ack	12:54:30 Dec 08...
minor	20:39:04 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	20:39:04 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	20:39:04 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	19:33:55 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	M8K - 6310	Redundancy...	High Availability Alarm	Redundancy group have some ...	Moscow		New	
minor	18:28:40 Dec 02 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	18:28:40 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	M8K - 6310	Redundancy...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Board#10.Tru...	D-channel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	M8K - 6310	Redundancy...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	

3 Session Experience Manager (SEM)

The SEM is a valuable new tool that delivers important technical and business statistics, based on AudioCodes methodologies, developed over years of VoIP experience.



The tool enables VoIP network managers to do the following:

- Rapidly identify the metric or metrics responsible for degradation in the quality of any VoIP call made over the network.
- Accurately diagnose and troubleshoot quality problems in response to VoIP user criticism.
- Proactively prevent VoIP quality degradation and optimize quality of experience for VoIP users.

The following describes examples of key issues addressed by the SEM module:

- Identifies overall Voice Quality in the network.
- Identifies on which device or link 'Failed' calls or 'Poor' Quality calls were reported.
- Identifies which metrics caused a deterioration in voice quality.
- Identifies whether performance deteriorates as the numbers of calls increases.
- Identifies which users have the most call time.
- Identifies which metric most affected a specific users call's quality.
- Identifies how much bandwidth the network is utilizing.

The SEM provides a real-time, as well as historical monitoring and VoIP network health model.

Examples of critical call quality metrics that are calculated by the SEM include: the Mean Opinion Score (MOS) Jitter; Delay (or latency); Packet Loss and Echo.

3.1 SEM Data Views

The SEM features the following different views:

■ Network:

- Displays a graphic representation of devices in the network in one of the three views:
 - ◆ Table view (the default) – displays a list of all the monitored devices (or links) with a summary of the most important metrics.
 - ◆ Map view – displays a map of devices/links with color coded status summary.
 - ◆ Regions view – displays a list of devices/links according to the regions.
- Displays each device's call quality metrics in a color-coded bar on the device icon
- Displays a table matrix for devices and voice metrics.
- Displays the distribution of successful / failed calls over a timeline.
- Lists the names of the most recently active alarms, each alarm's Severity level (color-coded), the Time it was received, and the name of the device triggering it.

The Network view can be displayed in three different modes:

■ Statistics:

- Displays Success / Failed calls rate (average success rate (ASR)) of calls over time; or Average Call Duration, or Failed Calls ratio.
- Displays the quality rating of each call (Good, Fair and Failed) over time and quality metrics: MOS, Jitter, Delay, Packet Loss and Echo level over time.
- Displays the counts and distribution of the Received / Transmitted Octets and Packets over time.

■ Calls:

The Calls view lists detailed information on each call for both Caller and Callee sides:

- Displays a summary of Call Quality metrics, such as MOS, Jitter and Packet Loss (%), Round Trip Delay (msec) and Echo Level.
- Displays Control Info metrics Source and Destination SIP IP, SIP Port and URIs, as well as the Control Protocol logical entities involved in the call, such as SRD.
- Displays Media Source and Destination SIP IP and Ports.
- Displays call trend - Pre-defined linear graphs showing call behavior over time based on events sent by the VoIP device.
- Lists alarms received from the relevant equipment during the specific call.

The Calls view includes filters for rapid and focused search such as: Success / Failed calls; Cause: MOS / Jitter / Packet loss / Delay / Echo and the Monitoring Endpoint Type: SBC, IP2IP, FXS, FXO, etc.

The Network and Statistics views graphs includes context links to the Calls view.

■ Reports:

The report view allows the user to focus on different aspects of the call analysis:

- **Network Status** – displays a summary analysis of key call metrics during a specified time period with a separate row entry for each device/link. For example, the 'Calls Statistics by Device' report summarizes for selected devices/links, the total percentage of successful and failed calls and metrics such as 'Number Of Calls' and 'Calls Quality'.
- **Trends** – displays the 'over time' behavior (monitored for a specific device/link over specified time intervals) where the same call metrics (described above) are displayed.
- **Top Users** – includes a list of users sorted according to one of the following metrics: 'Number Of Calls'; 'Calls Duration' and 'Users Who Experienced Most Poor Quality Calls' (based on specific metrics).

Reports can be easily customized using filters such as specific devices / links and date/time, columns can be added, users can also generate them based on a specific searched text string and they can be saved in PDF format.

■ Alarms:

The SEM's alarms functionality supports both Active Alarms as well as Historical Alarms. Alarms are displayed for calls made on specified devices and time range.

For each of the above views, data can be filtered according to time range, devices, SIP interfaces and links.

In addition, SEM can be configured to issue SEM Threshold based alerts, which are also displayed in the Alarms list. Threshold based alerts are an ideal network operator tool for automatic quality analysis. SEM alerts help to avoid false alarms when defining the appropriate minimal number of calls and criteria thresholds.

Threshold based alerts are generated as a result of the SEM application data analysis. Alerts are raised and cleared based upon user-defined policies and rules. The alerts are displayed in the 'Alarms' view as regular alarms.

Rules are provisioned according to criteria, such as specific devices/links, rule frequency and rule time.

Reader's Notes

4 Entity Management and Configuration

This section describes the Entity Management and Configuration features.

4.1 Automatic Gateway Software Version Detection

During the gateway definition in the EMS (Add Gateway action or Auto Detection), EMS connects to the gateway and automatically determines its version (in the case of a new gateway installation).

4.2 Media Gateway Status Summary

The EMS enables operators to navigate up and down the entities' hierarchy from the Navigation pane. Regions listed under Globe in the MG Tree expand to display the media gateways under them. These media gateways are also displayed in the MGs List pane. Each is represented by an icon. Each icon is color-coded to enable operators to quickly determine their status and size/shape to enable operators to immediately identify the media gateway type. One glance at the EMS Status pane provides operators with the specified media gateway status and the status of its various components, as well as the overall network status for all gateways managed by the EMS.

Figure 4-1: Mediant 8000 Media Gateway 6310 Status Pane



Figure 4-2: Mediant 5000 Media Gateway 6310 Status Pane



Figure 4-3: Mediant 5000 8410 Status Pane

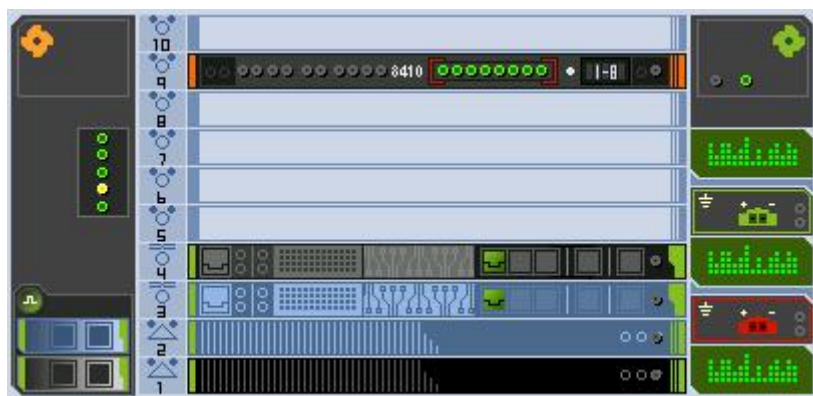


Figure 4-4: Mediant 3000 Status Pane

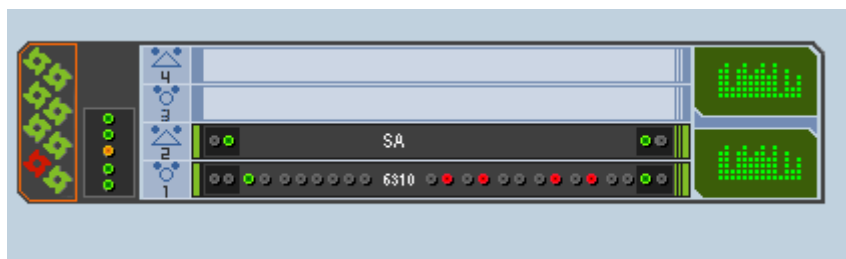


Figure 4-5: Mediant 800 MSBG Status Pane



Figure 4-6: Mediant 1000 Status Pane



Figure 4-7: Mediant 2000 Status Pane

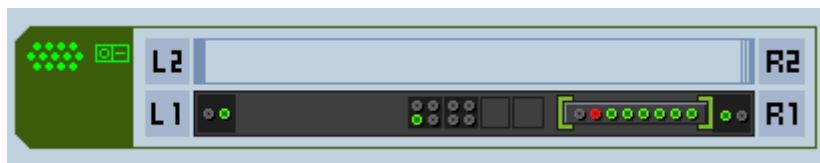
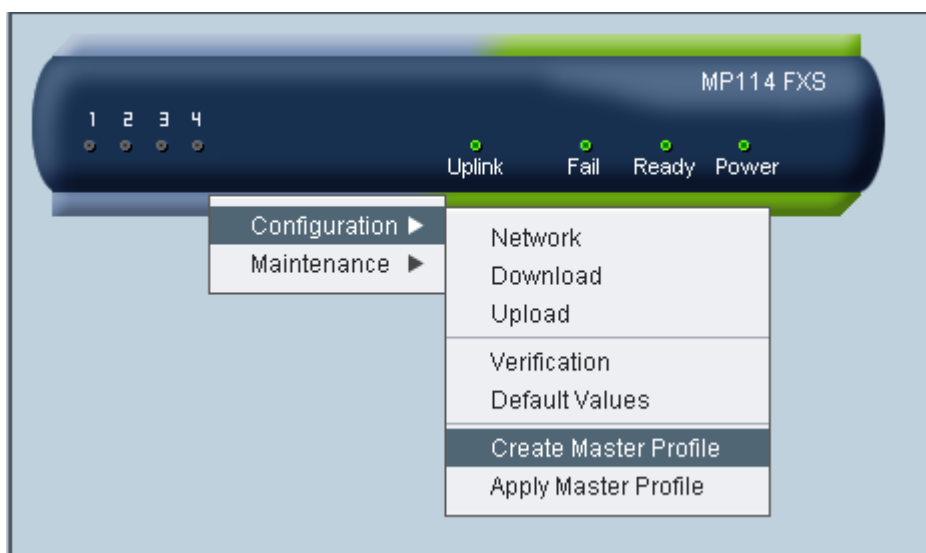


Figure 4-8: MediaPack Media Gateway Status Pane



4.3 Real-Time Color-Coded Media Gateway View

The EMS graphically represents the media gateway's status, as well as enabling intuitive, hierarchical navigation to physical and logical entities within each media gateway. It shows every board's status (SC, ES, TP/SB, Alarm Card) and trunk status for TP/SB boards. All hardware entities' alarm statuses are graphically represented: power suppliers, fans, and hard disks.

The color of each entity indicates its status. Special color-coding indicates various fault states of the entities (Critical, Major, Minor, Warning, OK) as well as board High Availability status; active, redundant standby or redundant active.

4.4 One-Click Access to Element Provisioning and Actions

Board actions can be performed using either the right-click menu or by selecting the appropriate action in the Actions bar. The right-click menu consists of the following sub-menus: Configuration, Maintenance and Performance. The items displayed in the Actions bar are context sensitive and therefore reflect the selected entity. For more information, see page 44.

4.5 Modular Workflow Process

EMS entities are provisioned through an intuitive workflow process consisting of navigation desktops. You can easily navigate between these desktops by clicking on the relevant button in a quick access Toolbar e.g. Configuration.

Figure 4-9: EMS Toolbar



4.5.1 Navigation Desktop

When you select a gateway in the MG Tree, the EMS displays the Media Gateway Status screen. A hierarchy tree of provisioning options representing the selected gateway are displayed in the Navigation pane. The options displayed in the hierarchy tree changes according to the selected entity. For example, if you select the Media Gateway board, then all relevant provisioning options for the Media Gateway board are displayed.

An MG Tree (displayed in the Navigation pane) enables you to easily view and navigate up/down the provisioning hierarchy tree. For example, *Globe > Region > Gateway > Board > Networking*.

Navigation improvements allow fast transitions between the same status views on different instance indexes. For example, moving from Board #1 to board #3, or from Board #2/Trunk#3 to Board#4/Trunk#7 does not require you to navigate between the boards on the Status screen, and instead can be performed using an index in the Navigation pane.

The root navigation level for all the SIP related parameters for the Mediant 800, Mediant 800 MSBG, Mediant 1000, Mediant 1000 MSBG and Mediant 3000 devices is based on the SIP application types i.e, GW and IP to IP, and SBC.

4.5.2 Configuration Desktop

Once you have selected the desired provisioning option in the Navigation pane and/or selected an entry in the entity list, you can quickly access the Provisioning screens by clicking the 'Configuration' button in the Toolbar.

An option to lock/unlock the relevant entity is displayed in the Provisioning screens. At any time, you can return to the Navigation desktop view by clicking the 'Navigation' button in the Toolbar.

When provisioning, operators always view in the provisioning screen a location-level indicator (the path of the EMS-managed entity), the Administrative / Operational State (for Mediant 8000) and the Reset State (for other gateways) of the entity being provisioned.

Unlock (for Mediant 8000) and Reset (for other gateways) actions to enable the Media Gateway to start operating with the new parameter values can be performed from the provisioning screens.

You can keep multiple configuration frames open at the same time and close them one by one, or close all open frames in a single action. In addition, you can close all frames associated with the Media Gateway after it has been removed from the EMS tree.

4.5.3 Alarms Desktop

You can display the Alarms browser for the relevant entity by selecting the relevant entity in the Navigation mode and then clicking the 'Alarms' button in the Toolbar. In the Alarms pane, you can choose to view either the Current or History Alarms browser. In the Alarms browser Actions bar, you can click the pie-chart to view different graphical statistical representations of the alarms for the selected entity. For more information, see Section 2 on page 25.

4.5.4 Performance Desktop

You can run Performance Monitoring for the relevant entity by selecting the relevant entity in the Navigation mode and then clicking the 'Performance' button in the Toolbar. In the Performance pane, you can view either History or Real-time performance monitoring. The respective Performance Monitoring provisioning screens are displayed. Starting and Stopping of Polling can be performed from the Main Actions bar or from the Actions bar in the respective Performance Monitoring provisioning screens. For more information, see Section 5 on page 47.

4.5.5 Context-Sensitive Behavior

The Status pane as well as the navigation bar allows operators to move up and down the provisioning hierarchy. Operators can always determine their exact location/level in the provisioning hierarchy from the location/level indication at the top of the screen. The Information pane always displays details regarding the current location/level.

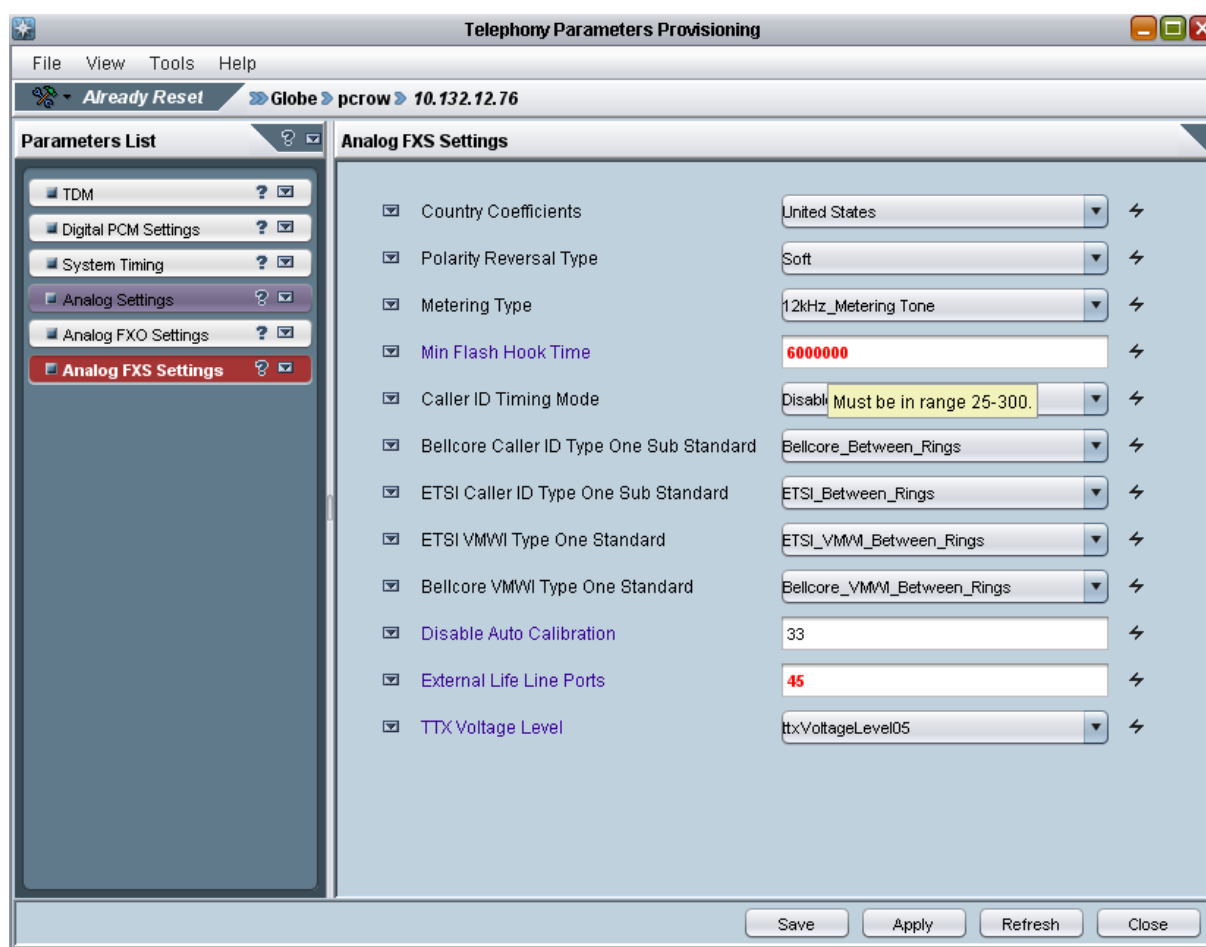
The entire EMS's GUI is context-based, affected by any change in location/level:

- The MG Node Info pane shows details of the selected MOs at the current location/level
- MG Tree shows the current region / media gateway, as selected
- Alarms displayed in the Alarm Browser are contextualized; only alarms associated with the entity selected in the MG Tree/Status pane/Board are displayed.
- The Actions bar always reflects the current provisioning location. For example, when you view the Gateway status screen, you see the most commonly used actions for the Gateway displayed in the Actions bar i.e. Lock, Unlock, Backup, Restore. Alternatively, when a Trunk is selected in the Trunk List at the TP board level, you see the most commonly used actions for the trunk i.e. 'Lock,' 'Unlock', 'Activate', 'Deactivate', 'Create Loopback' And 'Remove Loopback'.

4.6 Media Gateway Provisioning

This section describes the Media Gateway Provisioning features.

Figure 4-10: Trunk Parameters Provisioning Screen



Provisioning gateway entities is straightforward and operator-friendly via the EMS. Gateway entities such as boards, trunks, call control protocols, etc., are provisioned using the EMS's Parameters Provisioning screens. Parameter values are loaded to the gateway via SNMP.

The Parameter Provisioning screens are easily and intuitively reached by navigating up and down the system hierarchy in the Navigation pane to the entity to be provisioned.

When provisioning, operators always view a location-level indicator (the path of the EMS-managed entity), the Administrative / Operational State (for Mediant 5000/8000) and the Reset State (for Mediant 600/800/1000/2000/3000 and MediaPack) of the entity being provisioned. After provisioning, operators perform the following actions: Unlock (for Mediant 5000/8000) and Reset (for for Mediant 600/800/1000/2000/3000 and MediaPack) to enable the gateway to start operating with the new parameter values.

Regional files are loaded in the Software Manager (see Section 4.7.1.1 on page 44).

4.6.1 Provisioning Types

Three provisioning parameter types are supported in provisioning screens adjacent to modifiable parameters:

- Instant (changes are applied to the gateway after clicking Apply/OK)
- Online (the modified entity must be locked prior to applying the changes)
- Offline/Reset' (the modified entity must be locked prior to applying the changes and the physical component (board or Media Gateway) and unlocked (or reset) after applying the changes). These actions can be performed from the Provisioning screen menu. This feature facilitates the parameter provisioning/modifying process for operators.

4.6.2 Provisioning Frame - HA Indication

Each provisioning parameter can possibly impact the system's High Availability configuration. Therefore, an icon in the Provisioning Frame indicates whether changing the parameter's value impacts HA.

4.6.3 Color-Coding

The Parameters List pane in the Parameters Provisioning screens categorizes all provisioning parameters under *category tabs*. The tabs are color-coded for quick operator assessment. For example, if a parameter is provisioned illegally, the invalid parameter is colored red and a tool tip with the corrective instructions appears. The category tab name is colored red as well. Drop-down combo boxes adjacent to each category tab and to each parameter field in this category, list two actions that operators can optionally perform (for each individual parameter and for each category): "Undo modification/s" and "Factory default value". A Provisioned parameter tooltip with the parameter range upon mouse click exists for all parameters regardless of their state.

4.6.4 Export / Import / Save Provisioning Data

The EMS enables operators to export an entity's entire parameters provisioning screen as a file. This file is in readable XML format.

Operators can use this file to import the parameters provisioning screen configuration into another entity of the same type. For example, the parameters provisioning screen configuration of a board can be imported into another board. Alternatively the parameters provisioning screen configuration of a trunk can be imported into another trunk, etc.

The entity into which the file is imported can be in another EMS system or in the same EMS system. After the operator has imported the entity configuration file into the EMS, it is suggested to use profiles to replicate the configuration to the different entities of the objects managed by this EMS.

The EMS also enables operators to export an entity's entire parameters provisioning screen as a printable and easily readable file. This file is in readable *txt* format.

4.6.5 Configuration Profiles for Quick Provisioning

The EMS's Profile Management enables operators to rapidly provision values to entity parameters by loading a profile. The Profile Manager feature is located in the lowermost pane of the Parameters Provisioning screen.

Operators can view all currently available profile types, select a profile type best suited to customer application requirements, attach the profile, view a visual representation of the parameter values modified and save it as a new profile.

4.6.6 Parameters Search

The context sensitive parameter search option enables you to search for configuration parameters in the gateways provisioning frames. The basic search option enables you to perform a random search for a 'contains' string. Advanced search options enable you to match an exact/any word and to search for a MIB parameter.

The configuration frames containing the results parameters can be opened directly after selecting the desired parameter path.

4.6.7 Master Profile

Mediant 600/800/1000/2000/3000 Media Gateway and MediaPack products:

After configuring the gateway parameters, operators can save the configuration as a master profile. The master file comprises five entity profiles: GW, Network, Telephony, VoP Media and VoP Control. Operators can then attach the master profile to a media gateway or to multiple media gateways of the same type.

TP-6310, TP-8410 Master Profile (Mediant 5000 and 8000 Media Gateways):

After configuring the profiles parameters of a TP-6310/ TP-8410 board, operators can save the configuration as a master profile. The master profile comprises the following entity profiles:

- Board Provisioning Frame
- Trunks Provisioning Frame (for all trunks)
- All the signaling profiles (SN Timers, SS7 Link Set Timers, MTP2 Profiles, for all defined entities).

After saving the configuration as a master profile, operators can attach it to the TP-6310/ TP-8410 board or to multiple boards.

4.6.8 Media Gateway Offline Configuration

This feature is relevant for the Mediant 600/800/1000/2000/3000 Media Gateway and MediaPack products.

The media gateway configuration can be performed even if the device is not connected to the network. The EMS saves all configuration changes performed by operators in its database and loads the configuration when "Configuration Download" is requested. This feature is used to configure smaller media gateways prior to customer delivery and connection to the network, thereby substantially reducing customer deployment time.

4.6.9 Configuration Verification, Upload and Download

This feature is relevant for the Mediant 600/800/1000/2000/3000 Media Gateway and MediaPack products.

Configuration Verification is used to verify that the configuration saved in the EMS database tallies with the actual gateway configuration. The configuration verification compares both the provisioning parameters values as well as the auxiliary files stored in the EMS and loaded to the gateway. User display information includes a separate view for provisioning parameters and auxiliary files.

In the event of inconsistencies, operators are notified of the mismatch, which they can then correct by working with the EMS's parameter provisioning screens. To perform an overall parameters sync you can perform 'Configuration Upload' (when all the gateway parameters values are saved in the EMS database), or 'Configuration Download' (when all parameter values and auxiliary files, previously saved in EMS are downloaded to the gateway).

These actions can be performed for a set of gateways.

4.6.10 Capability to Save and Restore Gateway Configuration

This feature is relevant for the Mediant 600/800/1000/2000/3000 Media Gateway and MediaPack products.

The configurations of the small gateways are saved in the EMS database. If a gateway is replaced, this capability enables customers to quickly restore the original gateway's configuration.

4.6.11 Upload INI file from the Gateway

The Gateway INI file can be uploaded from the gateway to the EMS client. The INI file is defined as a Debug interface and is used to assist AudioCodes FAEs to perform problem debugging.

4.6.12 Security

The EMS's security management feature enables the operator who holds the Administrator security level to exert control over other operators' access to system resources. Thus, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexperienced operators. Security management is performed in the Users List screen and in the Actions Journal screen. The Actions Journal displays all logged user actions, enabling the Administrator to verify appropriate user access to system resources and to provide the Administrator with the means to retroactively analyze actions previously performed by users. See Section 6 on page 51.

The EMS supports X.509 Public Key Infrastructure and therefore enables you to generate self-signed certificates, private files and CSR requests.

4.7 Media Gateways Maintenance Actions

Mediant 5000, 8000 Maintenance Actions can be performed from either the Actions bar or by right-clicking the relevant entity in the MG Status screen.

The Actions bar always reflects the current provisioning location. For example, when you view the Gateway status screen, you see the most commonly used actions for the Gateway displayed in the Actions bar i.e. Lock, Unlock, Backup, Restore. Alternatively, when a Trunk is selected in the Trunk List at the TP board level, you see the most commonly used actions for the trunk i.e. 'Lock,' 'Unlock,' 'Activate,' 'Deactivate,' 'Create Loopback' And 'Remove Loopback'.

4.7.1 CPE and Blades

Figure 4-11: Maintenance Actions (Mediant 600/800/1000/2000/3000, MediaPacks)

MGs List						
Name	IP Address	Version	Product Type	Protocol	Admin State	Oper State
10.7.19.41	10.7.19.41	6.00A.006	MEDIANT 1000	SIP	Unlocked	
M1K MSBG 10.7.14.212	10.7.14.212	6.00AL.006....	MEDIANT 1000 M...	SIP		
MP500 10.7.14.203		6.00AL.006....	MP500 MSBG	SIP		

Configuration ▶
Maintenance ▶
Performance ▶

Download
Upload
Verification
Default Values
Create Master Profile
Apply Master Profile
SNMP Configuration

4.7.1.1 Software Upgrade and Regional Files Distribution

EMS operators can load files for a single gateway or for a set of selected gateways. The file loading process is accompanied by an extensive progress report and final loading status indication.

Gateway software files and regional properties files (such as Voice Prompts, CAS and other files) can be loaded to the gateway. They're listed in the Software Manager screen.

The Software Manager screen enables operators to view, add or remove configuration and regional files. Each new version, fix or updated file provided to customers is added to the Software Manager.

4.7.1.2 Save Configuration into Flash Memory

After completing the gateway configuration process, users can save the configuration and regional files into the gateway's flash memory. Consequently the gateway will not lose its configuration after Reset.

4.7.1.3 Download INI file to Device

You can download an INI file to a device prior to software version download to eliminate the process of validating the INI file with the device's existing configuration (prior to software upgrade). The following options are available for downloading an INI file to a device:

- Full Configuration INI file download– with validation and apply (recommended).
- Full Configuration INI file download– without validation and apply (for software upgrade).
- Incremental INI file download (previous configuration remains).

4.7.1.4 Configuration Data file Download and Upload Support

A configuration file 'Configuration Data' is used to store the data related (router) configuration for the Mediant 800 MSBG and Mediant1000 MSBG devices. This file can be downloaded to these specified devices or uploaded to them by the EMS application.

4.7.1.5 Multiple Gateways Lock / Unlock

It's possible to perform a single and multiple lock/unlock of the gateways from either the MG Status Screen or from the MGs Table screen. The locked gateway is color-coded gray in the MGs Tree and Status screen.

4.7.1.6 Resetting a Gateway

Users can reset a gateway by selecting the 'Reset' option in the Maintenance pop-up menu.

4.7.1.7 Actions on Multiple MGs in one command

All the actions described above can be performed on multiple gateways in a single command.

4.7.2 Mediant 5000, 8000 Maintenance Actions

Figure 4-12: Actions Bar Example- Mediant 5000/Mediant 8000Gateway Context



Figure 4-13: Right-click Maintenance Actions (Mediant 5000, 8000)



The figure below shows the Maintenance Actions Icon in the Provisioning screen menu. This icon enables you to lock and unlock the selected entity and also displays the 'Operational State' of the selected entity.

Figure 4-14: Maintenance Actions Icon and Popup Menu



4.7.2.1 Element Provisioning and Actions in Once

Right clicking on any GUI component provides you with the appropriate action menus. In addition, Gateway Start Up and Shut Down is possible from the Actions bar.

4.7.2.2 Online Software Upgrade Wizard

An online software upgrade is performed when both System Controllers are up and running. The software upgrade process upgrades both Self Controller and TP boards' software. An upgrade is best performed at night when traffic volume is low. If an upgrade process fails, users can perform a rollback to previous software and the previous configuration.

The Online Software Upgrade Wizard GUI includes a 'Wizard Stages' screen pane and a 'Summary Table' screen pane.



Note: Ensure that an upgrade from the specific media gateway version is supported. AudioCodes officially supports upgrade to Version 6.6 from the last two major software versions (Version 6.4 and Version 6.2) only. For additional information and clarifications contact AudioCodes Technical Support.

4.7.2.3 Backup / Restore of the Media Gateway Configuration

A backup of the gateway configuration file can be performed automatically according to user provisioned frequency or manually. Gateway Backup Files are stored at the EMS Server machine.

4.7.2.4 GW Log Files Collection

You can select from which SC boards they wish to collect gateway log files (primary or secondary) and which type of files to collect (SC Log, Core file, VoP Boards log file and/or GW configuration file). Log files should serve customers and FAEs for troubleshooting purposes.

4.7.2.5 TP INI file Collection

The TP board INI file can be saved from the EMS. This option is available from the main status screen by right clicking on a specific TP board. The INI file is used by customers and FAEs for troubleshooting.

4.7.2.6 Move TP Board

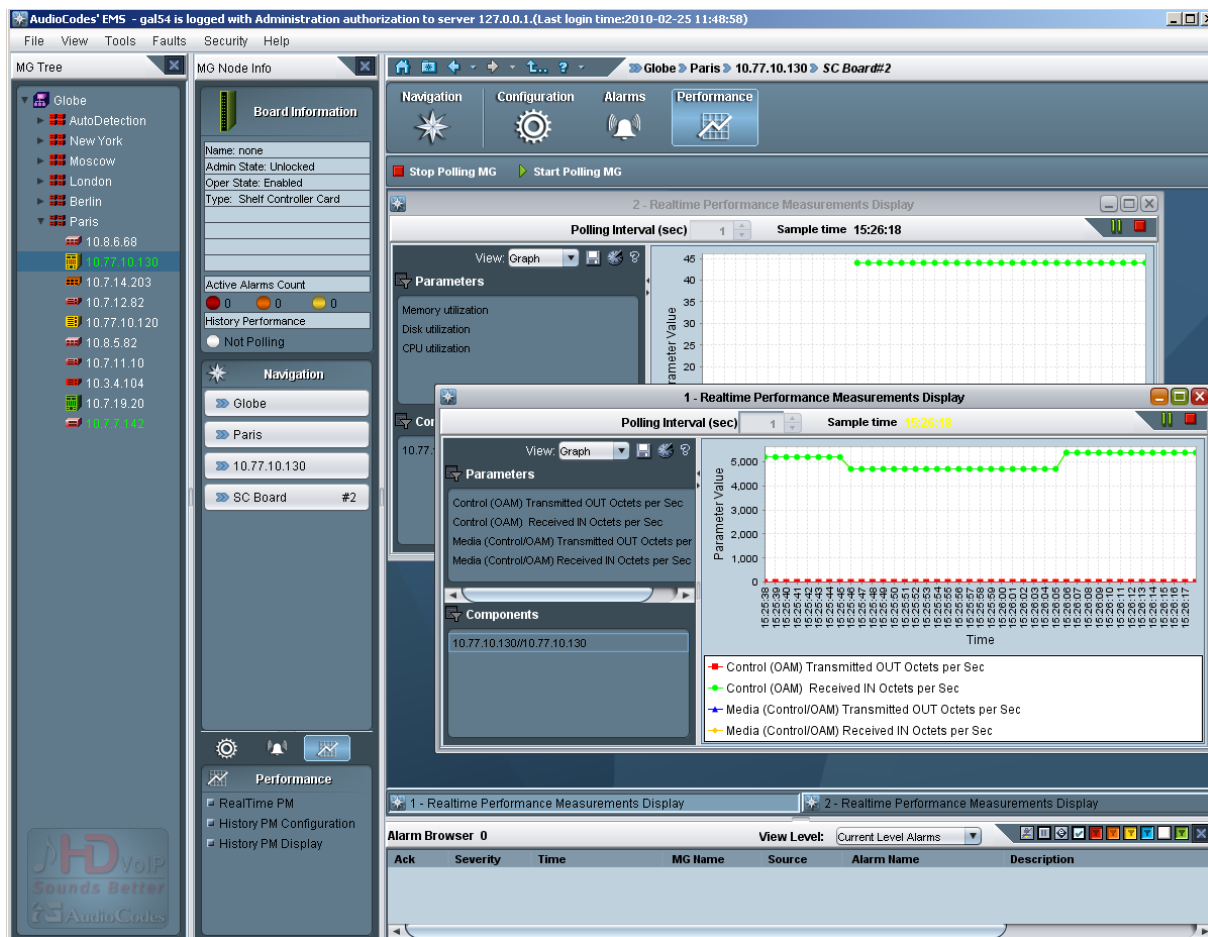
The right-click TP Board Maintenance action "Move TP Board' is available from the MG Status Screen. This option allows you to move an existing TP board, along with its entire configuration to another free slot on the media gateway.

5 Performance Management

After service is provisioned for a subscriber under a given QoS level, the service provider must ensure that the purchased level of service is delivered. In the domain of EMSs this process involves high-level fault and performance management of the managed entities.

The EMS's Performance Management is composed of real-time and historical data monitoring.

Figure 5-1: Performance Measurement Displays



5.1 Alarm Severity and Gateway/Board/Channel Distribution Summary Screens

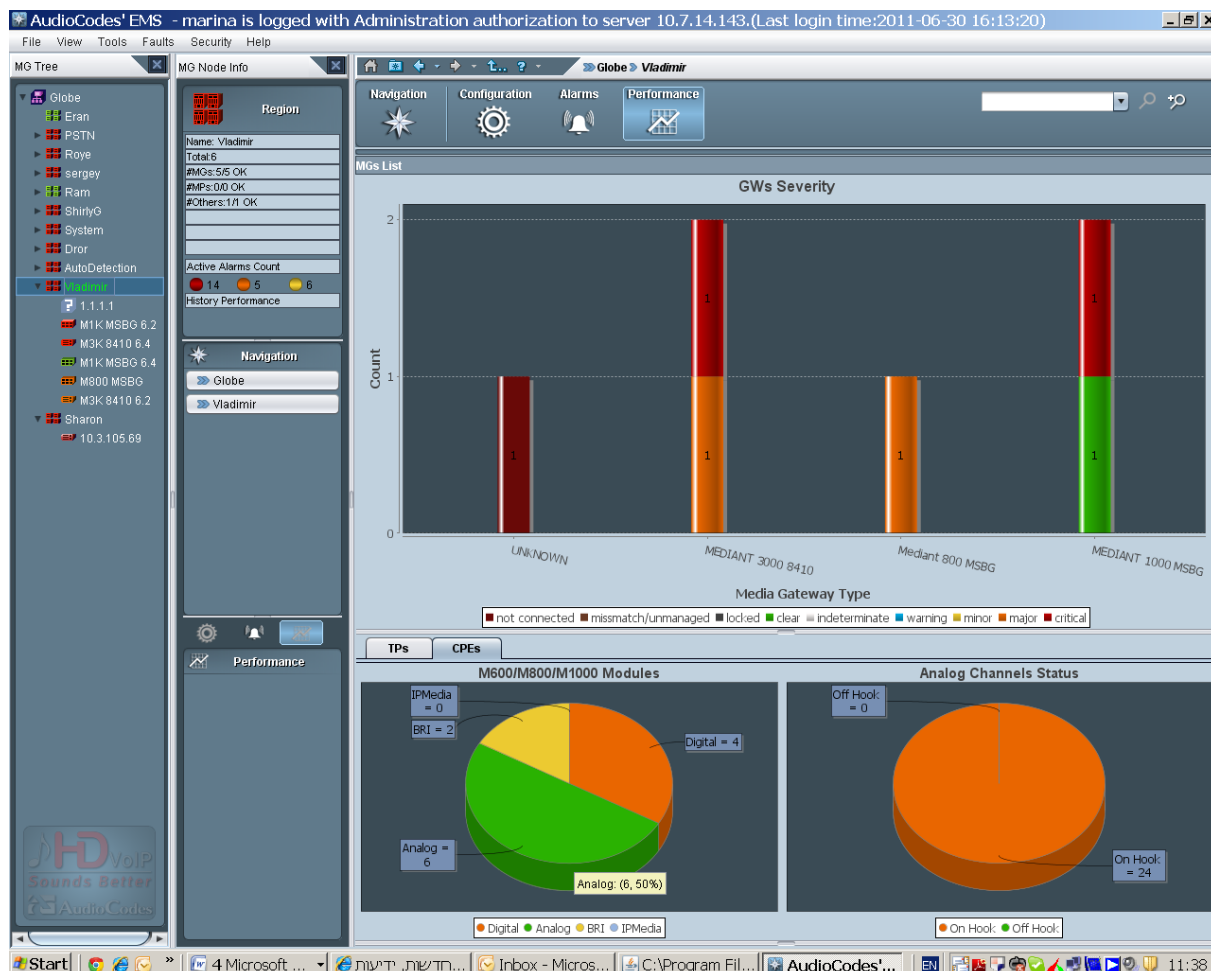
An auto-refreshable summary screen in the Performance Monitoring desktop enables you to view the following:

- Alarm severity and connection status of all devices managed by the EMS server, categorized according to regions.
- Alarm severity and connection status of all devices loaded to a specific region, categorized according to the device product.
- Distribution between the Active and Redundant boards for all the devices in the corresponding level (globe or region). This view consists of separate pie charts for each of the TP boards respectively (in the Mediant 2000, 3000, Mediant 5000 or Mediant 8000 chassis). The TP boards are categorized according to the protection type.
- Distribution of modules for the Mediant 600, Mediant 800, Mediant 800 MSBG, Mediant 1000 and Mediant 1000 MSBG devices (Digital, Analog, BRI, IPmedia) and channels status distribution – on hook / off hook. This view consists of two pie charts; one for the module distribution and another for the channels status distribution.

Figure 5-2: Alarm Severity and Board Distribution Summary Screens



Figure 5-3: Alarm Severity and Gateway/Channel Distribution



5.2 Real-Time Performance Monitoring – Pre-defined Graphs

The Performance Monitoring desktop automatically displays a pre-defined real-time graph showing the progress of key parameters. You can close the pre-defined graph, and/or open and configure additional real-time or history performance monitoring windows.

For each one of the managed devices and for each navigation level, the appropriate parameters are selected and displayed to the user.

5.3 Customized Real-Time and History (Background) Graphs

The Performance Monitoring desktop enables you to generate customized real-time and history (background) performance monitoring graphs. You can choose from a range of different parameters.

5.3.1 Real-Time Graphs

Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. In a single graph, users can compare different parameters of the same gateway, or the same parameter over different gateways.

Users can use two graph types to analyze their performance data: table view and line graph. A line graph is generally used when only a few parameters are compared. Table view is used when extensive data is displayed and analyzed.

5.3.2 History (Background) Performance Monitoring

Historical data can be used for long-term network analysis and planning. The PM profile, specifying those parameters that users wish to collect from EMS background monitoring can easily be transferred from one gateway to another.

In addition to storing PM background monitoring data in the EMS server database, an *xml* or *csv* file can also be created per time interval. The file is created at the end of the PM polling interval in accordance with a user-defined PM profile, and then stored in the EMS server under directory 'Pmfiles'. Users can choose whether to receive a trap when each file is created. The trap contains information as to the file name and the time it was created.

5.4 Aggregated PMs

This feature is supported for the Mediant 5000/8000 products.

Performance monitoring parameters can be aggregated for all the VoP board statistics. These parameters are defined at the Media Gateway level. For a detailed specification of the parameters list, refer to the *Mediant 5000 8000 OAM Guide*.

5.5 Performance Thresholds

This feature provides the customer with a powerful and flexible tool for monitoring the healthiness of the system.

Users can define high and low threshold values for History PMs, for both counters and gauge PM types table.

When defined high thresholds are exceeded, an appropriate alarm is issued by the gateway and displayed in the EMS. For example: once 'Lifetime in Seconds (Max)' has exceeded the user defined 'Lifetime High Threshold', a threshold exceed alarm is generated. The alarm is cleared when the PMs value passes below the defined low threshold value.

The severity of the generated alarm can also be configured by the user.

6 Security Management

EMS Security Management includes the following features:

- Network Communication Security
- EMS Users Authentication and Authorization
- Using Centralized Radius Server
- Local Users Management
- EMS Users Actions Journal
- EMS Server Machine Security & Hardening (including UNIX and Oracle related items, for more details, refer to the *EMS IOM Guide*)

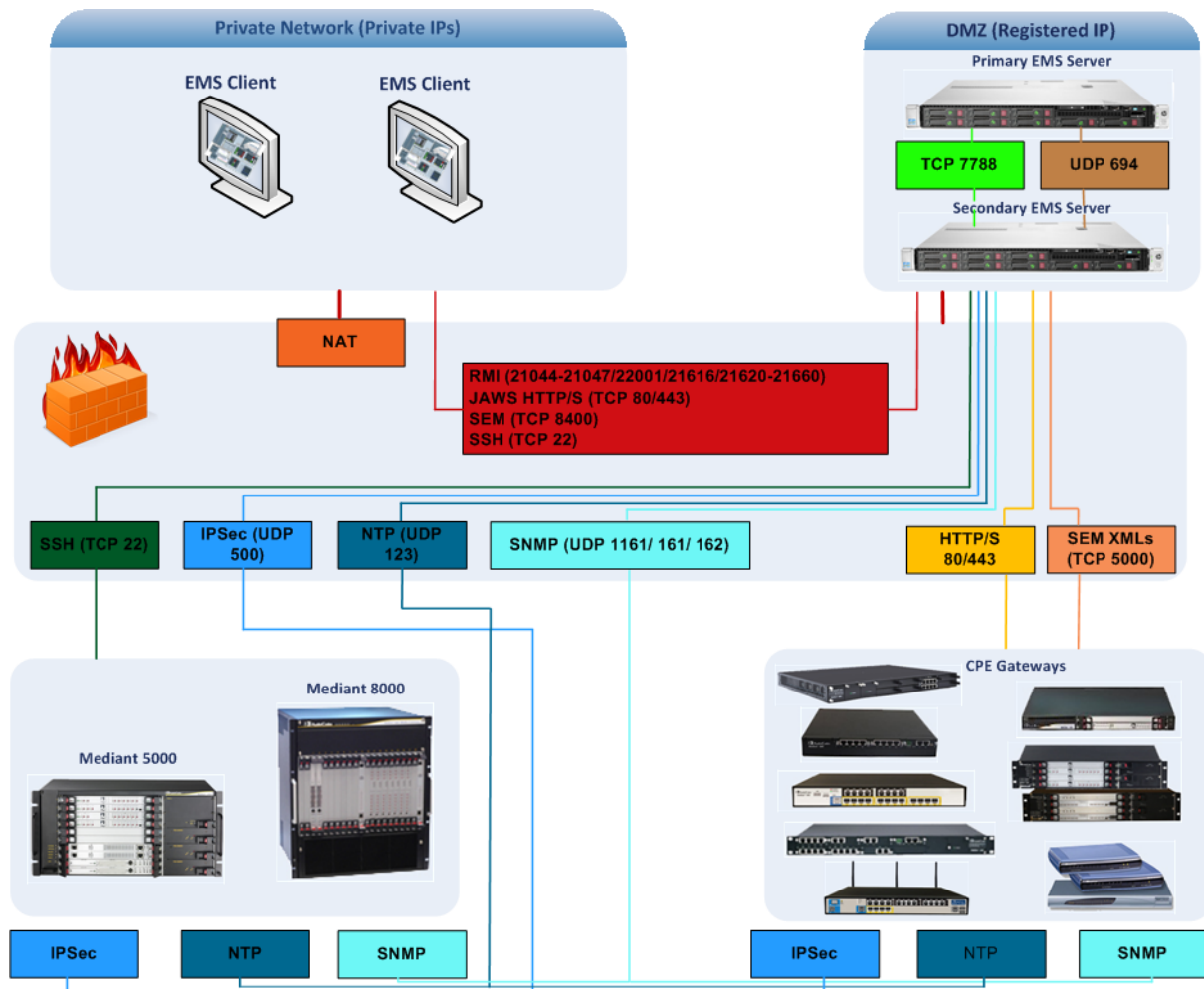
6.1 FIPS Compliance

The EMS application is certified by the USA Department of Defense FIPS 140-2 standard-(FIPS-Federal Information Processing Standards-US Government Security Standards for cryptography modules) (relevant for low and medium density gateway products).

Encryption and authentication related software are now implemented using FIPS compliant third party software; all encryption modules used by the EMS application are FIPS 140-2 certified.

6.2 Network Communication Security

Figure 6-1: Firewall Configuration Schema



The EMS interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. Define rules in your firewall to enable communications between EMS client, server and managed media gateways (refer to the figure above).

6.2.1 EMS Client <-> EMS Server

The EMS comprises EMS client and server machines, intercommunicating via RMI protocol over TCP. To secure EMS client-server communications, RMI protocol runs over Secure Socket Layer (RMI over SSL).

6.2.2 EMS Server <-> Mediant 5000/8000 Media Gateways

- SNMPv3 or SNMPv2c over IPSec for provisioning, maintenance actions, fault and performance management.
- SSH and SCP for installation, software upgrade and auxiliary files management.

6.2.3 EMS Server <-> Mediant 600/800/1000/2000/3000 and MediaPack

- SNMPv3 or SNMPv2c over IPSec for provisioning, maintenance actions and fault management.
- HTTPS for upgrading software and loading regional files.

6.2.4 Media Gateways Access Control

All user names and passwords used by the EMS application to access gateways (including SNMP, HTTP and SSH) are stored encrypted in the EMS database.

6.3 EMS Operator Authentication and Authorization

Initial access to the EMS application is secured via the Login screen, where access control consists of authentication and authorization with a user name and password.

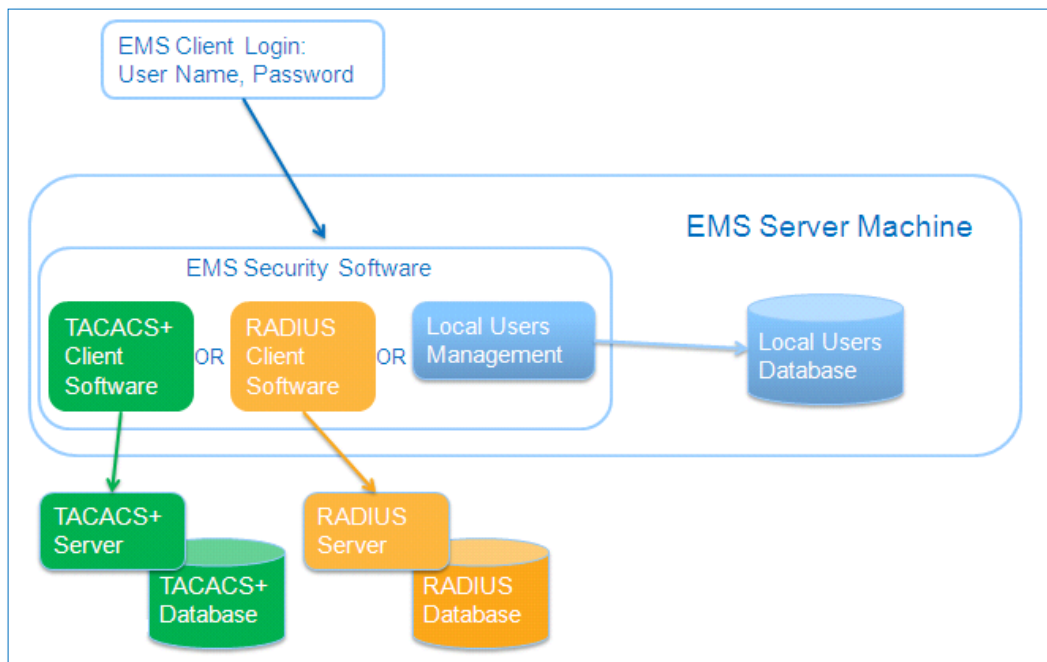
An EMS operator is authenticated and authorized to the EMS application using either the local EMS users management tools or a centralized Radius or TACACS+ server. By default, the EMS application manages its users in the local EMS server.

Figure 6-2: EMS Client Login Screen



6.3.1 Centralized RADIUS or TACACS+ Servers User Profile

Customers may enhance the security and capabilities of logging to the EMS application by using a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to store numerous usernames, passwords and access level attributes. This enables multiple user management on a centralized platform. The EMS server doesn't store the username and password (these users are not displayed in the EMS users list) and instead forwards them to the pre-configured RADIUS or TACACS+ server. The local EMS users and passwords defined in the Users' list can be used as a fallback mechanism in case the RADIUS servers does not respond.



6.3.2 EMS Application User Profile

All EMS users are defined in the EMS application User's list. This menu enables you to perform various user management actions, such as adding or removing a user.

Figure 6-3: EMS Users List

User Name	Security Level	Full Name	Status	Valid IPs To Login From
demo	Monitoring		SUSPENDED	10.7.2.33
acledmin	Administration	Admin user	ACTIVE	
keith	Administration	Keith Brown	NOT ACTIVE	
patrik	Monitoring	Patrik Smith	NOT ACTIVE	
Tom	Operation	Tom Clancy	ACTIVE	

6.3.2.1 EMS User Management: Session Inactivity Timer

The Session Inactivity Timer ensures that a malicious intruder cannot use the EMS application's active session after no action has been performed for a configured period of time. The user must enter their password to unlock the session. The Administrator can define a different Session Inactivity Timer per User.

6.3.2.2 EMS User Management: User Accounts Inactivity Timer

A User account is blocked when the user does not enter the EMS application for a configured period of time. The blocking of inactive user accounts is intended to prevent usage of these accounts by potential intruders.

6.3.2.3 EMS User Management: Password Complexity and Maintenance Extensions

The following user password complexity rules can be performed globally in the the EMS application (not for a single user):

- Password Length configuration. Default password length is 8 characters. Password length can vary from between 4 to 30 characters.
- The Number of Previous Not Reused Passwords can be configured between 5 (default) and 10 characters.
- The Number of Not Repetitive Digits from Previous Password can be configured between 0 (default) and 10.

Passwords can be defined with one of the following complexity rules:

- Must contain a mix of upper case letters, lower case letters, numbers, and special characters.
- Must contain three out of four of the above requirements.

Password verification will include text for weak passwords (including names or well known dictionary words) and will enforce the user not to use weak passwords.

6.3.2.4 Operator Password Expiration Extension

An option is provided to extend the number of logins after the user password has expired. This option is configured in the EMS users definitions. When enabled, the user can login to the EMS application during a 'pre-defined number of days' and 'days and login attempts' after their password has expired (without changing their password).

6.3.2.5 EMS User Security Levels

EMS operators can be allocated one of the following security levels:

- Monitoring Level (viewing only) (not visible)
- Operation Level (viewing and all system provisioning operations) (not visible)*
- Administration Level (viewing, all system provisioning operations, and user security management).
- 'Administrator Super User' Level (viewing, all system provisioning operations, and highest user security management).

The user name and security level are displayed in the title bar of the main screen, adjacent to 'AudioCodes EMS'.

When defining users locally, an operator is assigned the administrator security level to exert control over users' access to system resources so that sensitive system information cannot be accessed without appropriate authorization and that managed system elements cannot be sabotaged. The Administrator can define new users, change user security level, update/modify user details, remove a user from the Users List, perform the forced logout of an active user and/or suspend a user (as well as release an operator from suspension). The status of each user can be viewed in the Users List screen: ACTIVE, NOT ACTIVE, SUSPENDED or AUTOMATICALLY SUSPENDED.

The 'Not Visible' level allows you to filter views for EMS users with 'Operator' and 'Monitor' privileges according to sites. For example, an ITSP may have an EMS server installation that can manage multiple clients; where each client is assigned a separate region or alternatively a specific ITSP customer with global operations may wish to secure EMS information confidentially for each corporate region i.e. North West, North East and South.

6.3.2.6 Login Information Display

After a successful login to the EMS application, the user is notified with the following information:

- Latest successful login date, time and EMS client machine IP address.
- Number of unsuccessful logins since the latest successful login.
- Latest unsuccessful login date, time and EMS client machine IP address
- The user can determine whether to enable the last successful login message; lists the last successful and unsuccessful login time and date.

6.3.3 Integration with CAC Card

The EMS application can use the Common Access Card (CAC) as an alternative method for logging into the EMS client.

The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard and eligible contractor personnel.

The EMS application uses data from the CAC card, inserted into the smart card reader on a client PC where the EMS client is run, to perform the following main functions:

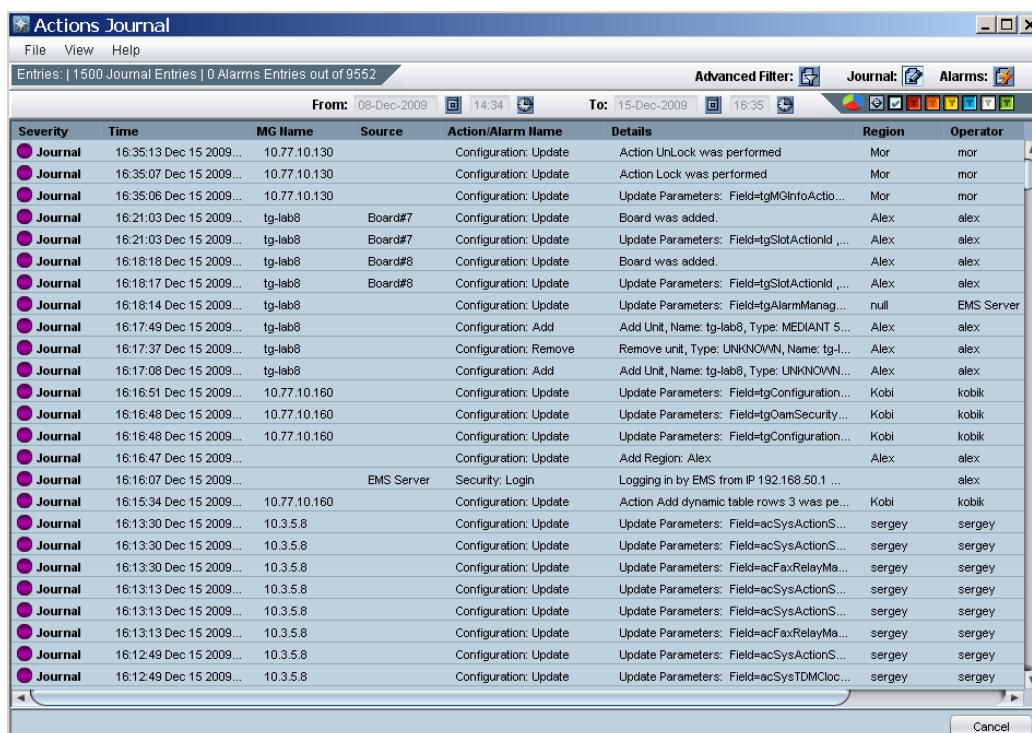
- Authentication (i.e. determines EMS username)
- Authorization (i.e. determines EMS user privilege level)
- Encryption (i.e. use the X.509 certificate from the CAC card to establish a TLS connection between the EMS client and the EMS server).

In the EMS login screen, the checkbox 'CAC PIN Number', when selected, displays a field to enter the CAC PIN number to login to the EMS client, instead of entering the EMS username and password.

6.3.4 Actions Journal

The Actions Journal displays all logged user actions, enabling the Administrator to verify appropriate user access to system resources and providing the Administrator with the means to retroactively analyze actions previously performed by users. Every action performed by any user is listed in the Actions Journal with information about the operator, action classification and the exact time the action was taken. The Actions Journal supports the following filters facilitating easy access to required information: User's Filter, Action Type Filter and the Date and Time Filter.

Figure 6-4: Actions Journal



Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator
Journal	16:35:13 Dec 15 2009...	10.77.10.130		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=mgInfoActio...	Mor	mor
Journal	16:21:03 Dec 15 2009...	tg-lab8	Board#7	Configuration: Update	Board was added.	Alex	alex
Journal	16:21:03 Dec 15 2009...	tg-lab8	Board#7	Configuration: Update	Update Parameters: Field=mgSlotActionId ,...	Alex	alex
Journal	16:18:18 Dec 15 2009...	tg-lab8	Board#8	Configuration: Update	Board was added.	Alex	alex
Journal	16:18:17 Dec 15 2009...	tg-lab8	Board#8	Configuration: Update	Update Parameters: Field=mgSlotActionId ,...	Alex	alex
Journal	16:18:14 Dec 15 2009...	tg-lab8		Configuration: Update	Update Parameters: Field=mgAlarmManag...	null	EMS Server
Journal	16:17:49 Dec 15 2009...	tg-lab8		Configuration: Add	Add Unit, Name: tg-lab8, Type: MEDIANT 5...	Alex	alex
Journal	16:17:37 Dec 15 2009...	tg-lab8		Configuration: Remove	Remove unit, Type: UNKNOWN, Name: tg-l...	Alex	alex
Journal	16:17:08 Dec 15 2009...	tg-lab8		Configuration: Add	Add Unit, Name: tg-lab8, Type: UNKNOWN...	Alex	alex
Journal	16:16:51 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=mgConfiguration...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=mgOamSecurity...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=mgConfiguration...	Kobi	kobik
Journal	16:16:47 Dec 15 2009...			Configuration: Update	Add Region: Alex	Alex	alex
Journal	16:16:07 Dec 15 2009...		EMS Server	Security: Login	Logging in by EMS from IP 192.168.50.1 ...		alex
Journal	16:15:34 Dec 15 2009...	10.77.10.160		Configuration: Update	Action Add dynamic table rows 3 was pe...	Kobi	kobik
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acFaxRelayMa...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acFaxRelayMa...	sergey	sergey
Journal	16:12:49 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:12:49 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysTDMCloc...	sergey	sergey

Reader's Notes

7 Virtualized EMS Server

The EMS server, in addition to the regular installation, is delivered as a virtual appliance (Hypervisor infra) on the VMware Virtual servers. The virtual environment allows the IT manager, carriers and all EMS customers to minimize dedicated hardware per application usage, and consequently leads to IT maintenance cost savings.

Reader's Notes

8 EMS Server Management

8.1 EMS Server High Availability (HA)

EMS servers High Availability (HA) 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:

- Regular: both servers are located in the same subnet. A single EMS server IP address - Global (Virtual) IP address is used for all the network components (EMS clients and managed gateways).
- Geographic: each server is located in a different network subnet and has its own IP address. The user provisions both these IP addresses in the client login dialog. The EMS client application constantly searches for the currently active EMS server machine.

8.2 EMS Server File System Security and Maintenance

The EMS server Management tool is a command line utility which enables the user to view information on the EMS server and configure its various components. The utility enables you to perform the following tasks:

- Collect information and logs
- Perform networking actions, such as changing the EMS server's IP address and configuring network Interfaces.
- Perform security actions such as basic and advanced hardening.
- Perform maintenance actions such as backup, restore and reboot.

8.2.1 EMS Server Hardening

Both Basic and Advanced Hardening can be performed on the EMS server. The purpose of basic hardening is to protect the EMS server from unauthorized access and hostile attack. It disables all Solaris services except those services used by the EMS. The purpose of Advanced Hardening is to remove OS packages that are not required by the system and are security vulnerable.

8.2.2 EMS Server File Integrity Checking

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

8.2.3 Intrusion Detection System

An Intrusion Detection tool scans predefined Solaris system files for specific danger patterns which might indicate whether the EMS server machine was accessed and/or modified by an external intruder. Intrusion Detection problems are reported via EMS Security Events. The Intrusion Detection tool runs on the EMS server machine.

8.2.4 EMS Server Security Patches Loading during version Installation and Upgrade

The EMS server installation performs an installation of security patches set as part of the application install or upgrade. It also removes unnecessary and unused Solaris packages.

8.2.5 Disk Mirroring (RAID 1) on Netra T5220

The EMS server machine (Netra T5220 server's on-board SAS controller) can perform disk mirroring for up to two configured RAID volumes. Disk mirroring (RAID 1) is a technique that uses data redundancy; two complete copies of all data stored on two separate disks, to protect against loss of data due to disk failure.

8.2.6 Syslog and Debug Recording

Syslog and Debug recordings from all managed machines can be logged directly to the EMS server without the need for a 3rd party server in the same local network.

9 Northbound Interface

EMS supports integration with higher management systems in the following areas:

- Remote Single Sign-On login from an NMS application to the EMS client via the EMS CLI.
- Support for Radius and TACACS+ server for centralized users authentication and authorization.
- Fault management (alarms and events forwarding via SNMP protocol).
- Performance Management (performance monitoring collection enable using XML or CSV files format).
- Managed Gateways Topology file using CSV file format.
- Mediant 5000/8000 backup files.
- EMS server backup files.

For more details, refer to the *OAMP Integration Guide*.

Product Description

Version 6.6



www.audiocodes.com