AudioCodes™ Element Management System (EMS)

User's Manual

Version 6.8

Table of Contents

Actions and Provisioning 223

Fault and Performance Management....265

Troubleshooting 383

List of Figures

List of Tables

Reader's Notes

Notice

This User Manual describes the use of AudioCodes' Element Management System (EMS) Graphical User Interface (GUI).

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

This document is subject to change without notice.

Date Published: June-17-2014

Trademarks

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

WEEE EU Directive

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

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Abbreviations and Terminology

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

Term	Description
Trunking Gateway	Refers to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway.
MG	Refers to the Media Gateway.
MediaPack	MediaPack collectively refers to the MP-102 (FXS), MP-104 (FXS and FXO), MP-108 (FXS and FXO), MP-112 (FXS), MP-114 (FXS), MP-118 (FXS) and MP-124 (FXS).
CPE (Customer Premises Equipment)	CPE refers to the following: • Mediant 9000 SBC • Mediant 4000 SBC • Mediant 3000 • Mediant 2600 SBC • Mediant 2000 • Mediant 1000 • Mediant 1000B Gateway and E-SBC • Mediant 1000 MSBR • Mediant 800B Gateway and E-SBC • Mediant 800 MSBR • Mediant 600 • Mediant 500 E-SBC • Mediant 500 MSBR and Mediant 500L MSBR • Mediant SE SBC and Mediant VE SBC • Mediant SBA products
DS3	Synonymous with the term 'T3'.
'Frame' and 'Screen'	Sometimes used interchangeably

Documentation Feedback

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

Related Documentation

Manual Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500 E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAMP Integration Guide
Element Management System (EMS) User's Manual
SEM User's Manual
Element Management System (EMS) Online Help
Mediant 5000 / 8000 Media Gateway Installation, Operation and Maintenance Manual
Mediant 5000 / 8000 Media Gateway Release Notes
Mediant SBC Series and Mediant Software SBC Series OAMP Guide
Mediant 3000 TP-8410 OAMP Guide
Mediant 3000 TP-6310 OAMP Guide
Mediant 1000 E-SBC OAMP Guide
Mediant 500 E-SBC and Mediant 800 Gateway and E-SBC OAMP Guide Ver. 6.8
Mediant MSBR Series OAMP Guide

Reader's Notes

1 Introducing the AudioCodes Element Management System

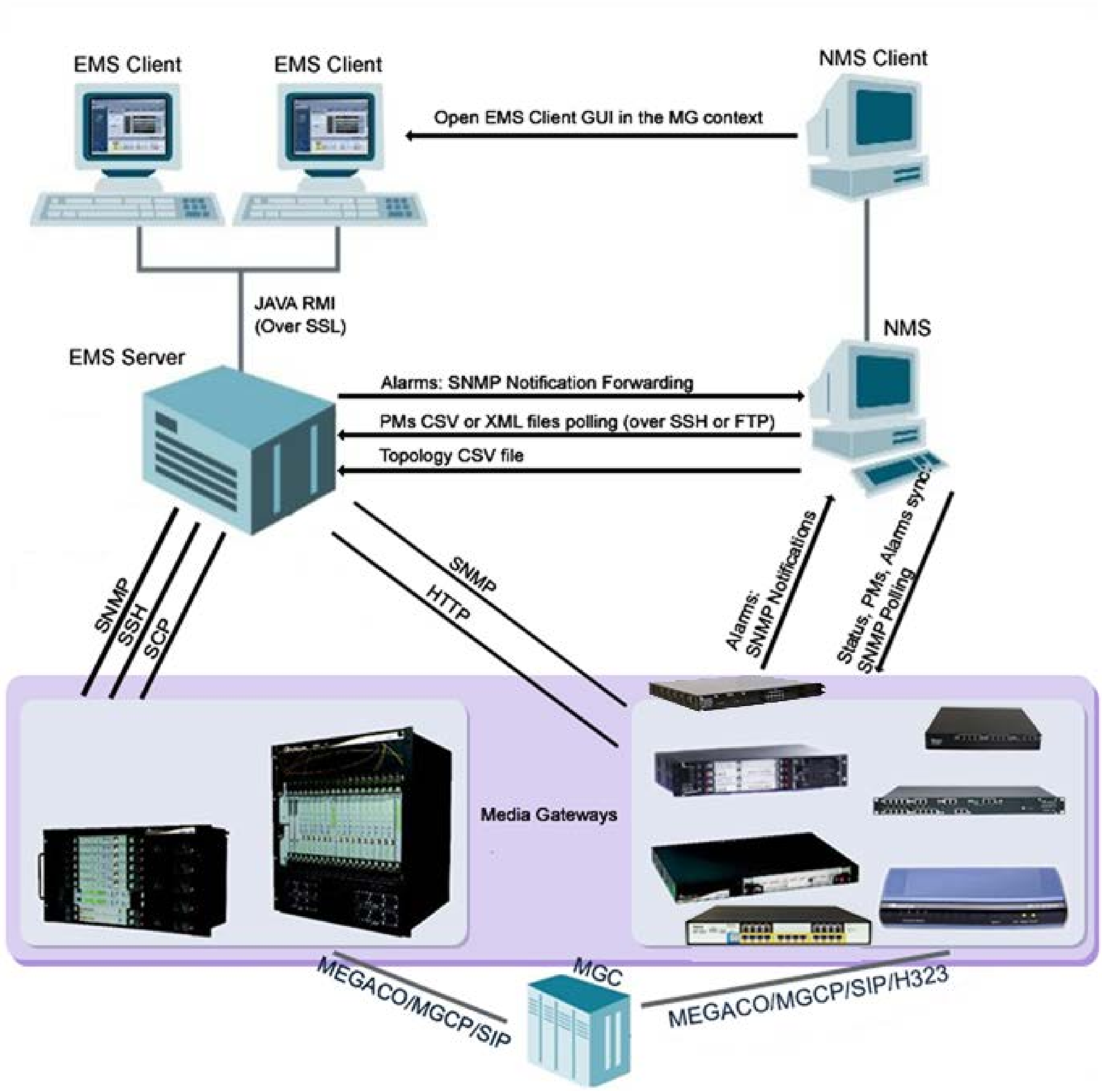
The Element Management System (EMS) is an advanced solution for standards-based management of multiple media gateways within VoIP networks. This management covers all areas vital for the efficient operation, administration, management and pr ovisioning (OAM and P) of the AudioCodes' families of digital Media Gateway systems and their modules, analog VoIP Media Gateways, Multi-Service Business Routers (MSBRs) and Session Border Controllers (SBCs).

The EMS enables Network Equipment Providers (NEPs) and System Integrators (SIs) the ability to offer customers rapid time-to-market and i nclusive, 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 figure below shows the EMS integrated in a network system.

Figure 1-1: EMS Integrated in a Network System



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

1.1 Specifications

- Software Version Number: **6.8**
- Release Date: **Q2 2014**
- Package and Upgrade Distribution: DVD

Table 1-1: Specifications

Subject	Description
TMN Standards	ITU-T Recommendation M.3010 series FCAPS functionality support
Fault Management	▪ 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	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. A Summary of all managed gateways' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.
Media Gateways Provisioning	▪ 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, as well as for the 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.

Subject	Description
Security Management	Complies with T1M1.5/2003-007R4 and covers two aspects: Network communication security and EMS application security. 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. 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. **Network Communications Security** EMS server's network is configured and its ports opened during installation. Interoperation with firewalls, protecting against unauthorized access by crackers and hackers. MediaPack, Mediant 1000, Mediant 2000, Mediant 3000 can be managed behind the NAT. EMS client-server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). EMS server - media gateway communication is secured using SNMPv2c/SNMPv3, HTTP/HTTPS, Telnet and FTP over IPSec / SSH and SCP. **Application Security** User Management using a Radius server for centralized user authentication and Authorization or in the EMS application. 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 EMS application: Actions Journal of operators' activities, various filtering and search options. **EMS Server Hardening** 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.
Performance Management	▪ Real-Time Graphics ▪ Historical Data Collection and Analysis

Subject	Description
Session Experience Management	▪ 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	Mediant 8000 Media Gateway and Mediant 5000 Media Gateway: ▪ 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. Mediant 600, Mediant 800, Mediant 1000, Mediant 2000, Mediant 3000, and MediaPack: ▪ 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.

1.2 Supported VoIP Equipment

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

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 MediaPack	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. (Refer to the product documentation for detailed information.)
 Mediant 500 E-SBC	The Mediant 500 Enterprise Session Border Controller (E-SBC), hereafter referred to as *the device*, is a member of AudioCodes family of E-SBCs, enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device provides voice-over-IP (VoIP) SBC functionality. The device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 500 MSBR **Mediant 500L MSBR** **Mediant 800 MSBR** **Mediant 1000 MSBR**	These Multi-Service Business Routers (MSBR) 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. 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. 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. (Refer to the specific product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
Mediant 1000 Media Gateway	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 flexibile, 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).
Mediant 600 Media Gateway	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. (Refer to the product documentation for detailed information.)

Table 1-3: Supported VoIP Equipment

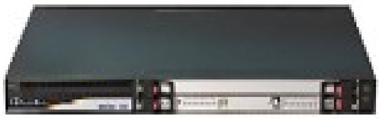
Supported VoIP Equipment	Description
 **Mediant 2000 Media Gateway**	The Mediant 2000 Media Gateway contains the TP-1610 cPCI VoIP communication board, an ideal building block for deploying high-density, high availability Voice over IP (VoIP) and wireless enterprise systems. The Mediant 2000 incorporates 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. (Refer to the product documentation for detailed information).
Mediant 500 Enterprise Session Border Controller (E-SBC)	The Mediant 500 Enterprise Session Border Controller (E-SBC), hereafter referred to as *the device*, is a member of AudioCodes family of E-SBCs, enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device provides voice-over-IP (VoIP) SBC functionality. The device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 2600 E-SBC	AudioCodes' Mediant 2600 E-SBC is a member of AudioCodes family of Enterprise Session Border Controllers (E-SBC), enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. The SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.
   AudioCodes Mediant Software Enterprise Session Border Controllers	AudioCodes Mediant Software Enterprise Session Border Controllers (E-SBC) are pure-software products, enabling connectivity and security between Enterprises' and Service Providers' VoIP networks. The Mediant Software product line include the following product variants: **Mediant Server Edition SBC:** x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements. **Mediant Virtual Edition SBC:** Installed and hosted in a virtual machine environment that complies to specified requirements .

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
Mediant 3000 Media Gateway	The Mediant 3000 Media Gateway is the medium-sized member of the family of market-ready, standards-compliant, media gateway systems. 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 Applications: VoP Trunking gateways, IP-Centrex Gateways, VoP Access gateways 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 (Refer to the product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
Mediant 4000 E-SBC	AudioCodes' Mediant 4000 E-SBC is a member of AudioCodes family of Enterprise Session Border Controllers (E-SBC), enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. The SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.

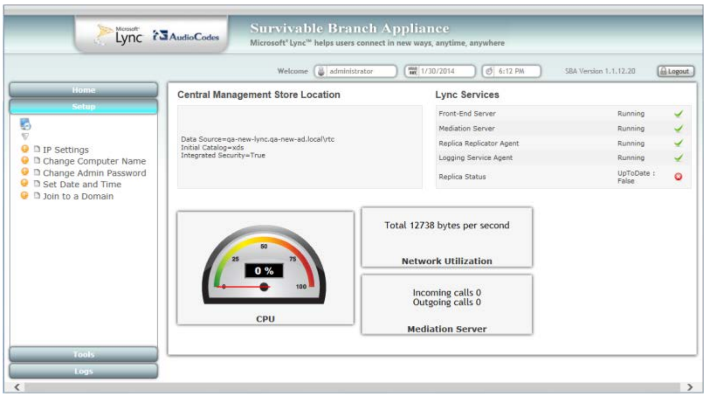
Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 5000 Media Gateway	The Mediant 5000 is the medium-sized member of the family of market-ready, standards-compliant, media gateway systems. **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 **Applications**: VoP Trunking Gateways, IP-Centrex Gateways, VoP Access Gateways 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 (Refer to the product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 8000 Media Gateway	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. 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. **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 **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. (Refer to the product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 9000 SBC	AudioCodes Mediant 9000 Session Border Controller is a highly scalable Session Border Controller (SBC) designed for deployment in large enterprise and contact center locations and as an access SBC for service provider environments. The Mediant 9000 is a high-capacity SBC, supporting thousands of concurrent sessions and extensive SIP connectivity with wide-ranging interoperability, enhanced perimeter defense against cyber-attacks, and advanced voice quality monitoring. The device also supports active/standby (1+1) redundancy (High Availability) by employing two devices in the network. The device offers branch survivability during WAN failure, ensuring call service continuity.
Survivable Branch Appliance (SBA)  Microsoft Lync AudioCodes Survivable Branch Appliance Microsoft® Lync™ helps users connect in new ways, anytime, anywhere Welcome administrator 1/30/2014 6:12 PM SBA Version 1.1.12.20 Logout Home Setup IP Settings Change Computer Name Change Admin Password Set Date and Time Join to a Domain Tools Logs 0 % 0 25 50 75 100 CPU Network Utilization Mediation Server Central Management Store Location Data Source=qa-new-lync.qa-new-ad.local\rtc Initial Catalog=xds Integrated Security=True Lync Services Front-End Server Running ✓ Mediation Server Running ✓ Replica Replicator Agent Running ✓ Logging Service Agent Running ✓ Replica Status UpToDate : False ✗ Total 12738 bytes per second Incoming calls 0 Outgoing calls 0	The Survivable Branch Appliance (SBA) is an AudioCodes product designed for Microsoft Lync Server which allows remote branch resiliency in a Microsoft Lync Server network (Microsoft Lync Server 2010 and Microsoft Lync Server 2013). The AudioCodes SBA resides on the OSN server platform of the Mediant 800B and the Mediant 1000B running on a Microsoft Windows 2008 Telco R2 operating system. In the EMS, the SBA is displayed as a module of the Mediant 800B and the Mediant 1000B gateways. When you add either of these platforms to the EMS, there is an option to enable the SBA module. The SBA module has a separate IP address and FQDN Name.

1.3 Managed VoIP Equipment

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

- **Mediant 9000 SBC: version 6.8**
- *Mediant 8000 Media Gateway: versions 6.6, 6.2
- *Mediant 5000 Media Gateway: versions 6.6, 6.2
- Mediant 4000 SBC: versions **6.8**, 6.6
- Mediant 2600 E-SBC: versions **6.8**, 6.6
- **Mediant SE SBC: version 6.8**
- **Mediant SE-H SBC: version 6.8**
- **Mediant VE SBC: version 6.8**
- **Mediant VE-H SBC: version 6.8**
- Mediant 3000 Media Gateways: versions **6.8**, 6.6, 6.4
- Mediant 2000 Media Gateways: versions 6.6, 6.4
- *Mediant 1000 Gateway: versions 6.6 and 6.4
- Mediant 1000B Gateway and E-SBC and Mediant 1000B MSBR: versions **6.8**, 6.6, 6.4
- Mediant 800B Gateway and E-SBC and Mediant 800B MSBR: versions **6.8**, 6.6, 6.4
- *Mediant 600: versions 6.6, 6.4
- **Mediant 500 E-SBC**
- **Mediant 500L MSBR and Mediant 500 MSBR: versions 6.8**
- MediaPack 11x (MP-11x) Media Gateways: versions 6.6
- *Mediant 800 SBA, *Mediant 1000 SBA and *Mediant 2000 SBA devices with SBA version **1.1.13.0** and above and gateway versions 6.6 and **6.8**

Notes:

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

1.4 SEM Server Disk Requirements

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

The three configurations shown in the table below are supported:

Table 1-4: SEM Server Disk Requirements

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

1.5 EMS Server and Client Requirements

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

Table 1-5: EMS- Minimal Platform Requirements

Resource	EMS/SEM Server				EMS Client
	Dedicated EMS Server - Linux OS		Virtual EMS - Low Profile	Virtual EMS - High Profile	
Hardware	HP DL360 G6	HP ProLiant DL360p Gen8	_	_	Monitor resolution: 1152*864 or higher
Operating System	Linux CentOS 64-bit, kernel version 5.9, Rev6	Linux CentOS 64-bit, kernel version 5.9, Rev6	Linux CentOS 64-bit, kernel version 5.9 Rev6,	Linux CentOS 64-bit, kernel version 5.9 Rev6,	Windows™ 2000 / XP/ Vista/Windows 7/Windows 8
Memory	2 GB RAM	32 GB RAM	2 GB RAM	32 GB RAM	512 MB RAM
Disk space	146 GB	Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0	170 GB	1200 GB	300 MB

Resource	EMS/SEM Server				EMS Client
	Dedicated EMS Server - Linux OS		Virtual EMS - Low Profile	Virtual EMS - High Profile	
Processor	Intel Xeon E5504 (4M Cache, 2.00 GHz)	CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each)	1 core not less than 2 GHz	6 cores not less than 2 GHz	600 MHz Pentium III or higher
DVD-ROM	Local		_	_	_

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

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

1.6 EMS and SEM Bandwidth Requirements

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

1.6.1 EMS Bandwidth Requirements

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

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

1.6.2 SEM Bandwidth Requirements

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

Table 1-6: SEM Bandwidth Requirements

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

1.7 Characteristics

This section describes the EMS System Characteristics.

The EMS features client/server architecture, enabling customers to access it 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).

The EMS consists of the following components:

- **EMS Server**, running on Linux 5 (**CentOS**). All management data is stored in the server, using Oracle 11*g* relational database software.
- **EMS Client**, running on Microsoft™ Windows™, displays the EMS GUI screens that provide operators access to system entities. The operator-friendly GUI, hierarchical organization and Microsoft™ Explorer™ paradigm increase productivity and minimize the learning curve.

1.7.1 Versatile System

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

1.7.2 FCAPS

The EMS supports FCAPS functionality:

- 'Fault management' on page 267
- 'Configuration management' on page 77
- Accounting (managed by a higher-level management system such as an NMS)
- 'Performance Management' on page 307
- 'Security Management' on page 333

1.7.3 Open Standard Design

The open standard design of the EMS 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.

1.7.4 Private Labeling

Private labeling enables you to customize and label the EMS and media gateways, 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 i mages and r ebuilding a customized CD or DVD.

The private labeling procedure covers the following items:

- The license 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.

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

Reader's Notes

Part I

Getting Started

This section describes how to start using the EMS.

2 Installing the EMS Client on a PC

Installation of the EMS comprises installation of EMS Server and installation of EMS Client.

For detailed information on installing the EMS Server, refer to the *EMS Server Installation and Maintenance Manual, Document #: LTRT-941xx*.

> **Note:** When installing and running EMS Client on Windows 7 laptops, user must have Administrator permissions.

2.1 Installing the EMS using the Supplied DVD

This section describes how to install EMS using the supplied DVD.

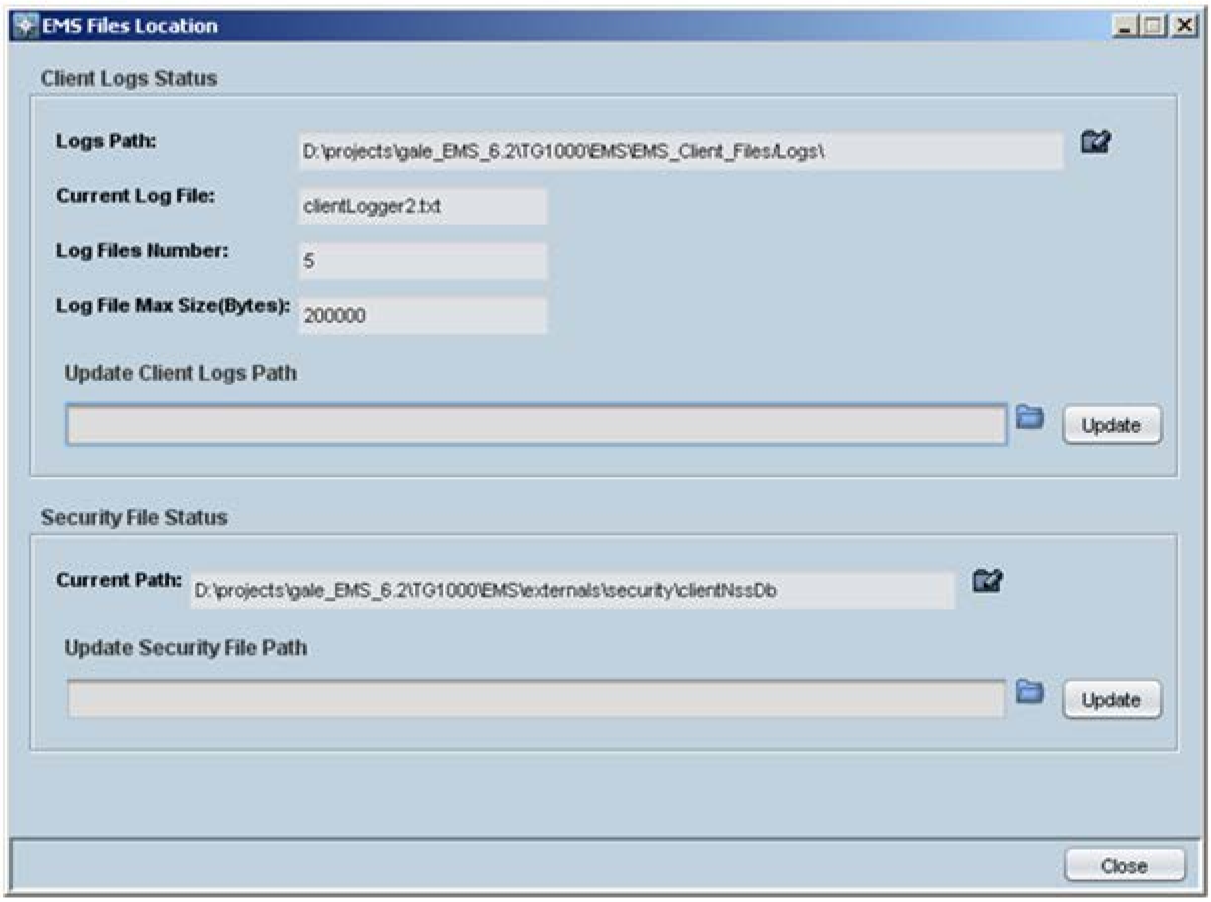
➢ **To install the EMS from the supplied DVD:**

1. Insert AudioCodes' EMS installation disk.
2. Double-click the EMS Client (PC) Installation ac_ems_setup_win32.exe file and follow the installation instructions; as a result of installation process, the EMS Client icon is added to the desktop.

   During the EMS Client installation, writable folders are created for log files and for security files. These folders are by default created under the client installation folder. In case the customer for security or any other reason wishes to change the location of these folders, this can be performed using the File > Client Files Location menu in the EMS client.

The screen below displays the current location of these files and allows the user to update the relevant paths.

Figure 2-1: EMS Files Location



Logs Path: D:\projects\gale_EMS_6.2\TG1000\EMS\EMS_Client_Files/Logs\

Current Log File: clientLogger2.txt

Log Files Number: 5

Log File Max Size(Bytes): 200000

Current Path: D:\projects\gale_EMS_6.2\TG1000\EMS\externals\security\clientNssDb

2.2 Installing the EMS on a Client PC using JAWS

This section describes how to install the EMS on a client PC using JAWS.

Java Web Start (JAWS) enables you to install the EMS client (compatible with your EMS server version) without using any CDs.

➢ To install the EMS on a client PC using JAWS:

1. Open Internet Explorer and type the EMS Server IP in the Address field and add /jaws as suffix, for example:

   http://10.7.6.5/jaws/

2. Follow the online instructions.

2.3 Running the EMS Client

This section describes how to run the EMS client.

2.3.1 Running the EMS Client after DVD Installation

This section describes how to run the EMS client after the DVD Installation.

➢ **To run the EMS client after DVD installation:**

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

2.3.2 Running the EMS Client after JAWS Installation via URL

This section describes how to run the EMS client after the JAWS installation via URL.

➢ **To run the EMS client after JAWS installation via URL:**

- Specify the path 'http://<server_ip>/jaws'; an 'EMS Login Screen' is opened.

  For example: http://10.7.6.18/jaws/

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

  For example: http://10.7.6.18/jaws/?username=acladmin&password=pass_1234

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

  Supported arguments are as follows:

  - username - should include the username
  - password - should include clear text password
  - (optional) nodeip - when requested the EMS client will be opened to the requested node status screen. Default - globe view on the status screen.
  - (optional) showtree - two values supported: true/false. Default value is true.
  - (optional) showalarmbrowser - two values supported: true/false. Default value is true.

  For example: http://10.7.6.18/jaws/?username=acladmin&password=pass_1234&challenge=nomatter&showtree=false&showalarmbrowser=false&nodeip=10.7.5.201

2.4 Management Procedure

Follow this procedure when managing your VoIP equipment with the EMS:

1. Define authentication and Authorization policy (centralized or local EMS users).
2. Define and evoke your VoIP devices.
3. Perform advanced provisioning.
4. Monitor your VoIP devices.
5. Maintain one of more VoIP devices with one action.
6. Manage faults and performance.
7. Manage security.

3 Getting Started with the EMS

This section describes how to start using the EMS client and to understand it's basic orientation.

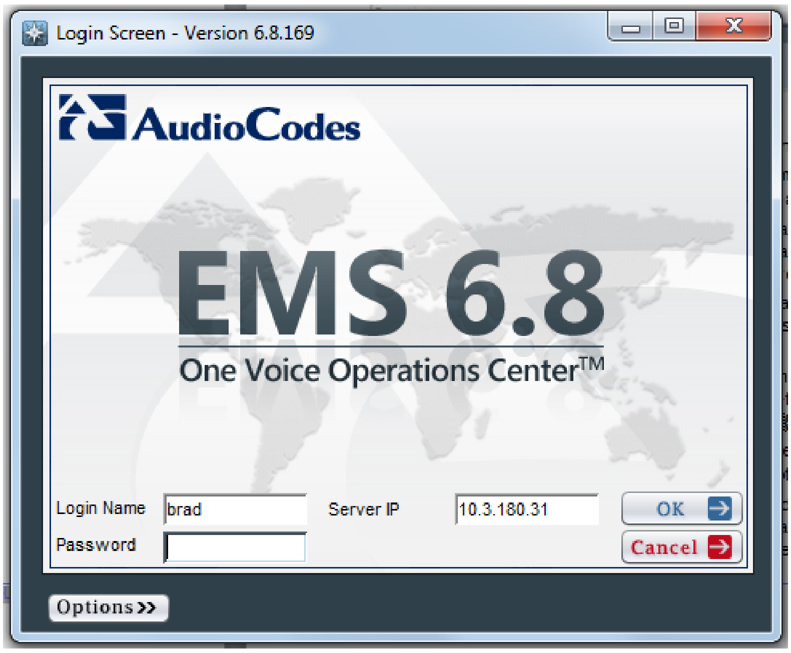
3.1 Logging In

This section describes how to login to the EMS client.

➢ To log in to the EMS client:

1. Double-click the EMS Client icon on your desktop, or run **Start>Programs>EMS Client**; the EMS Login screen is displayed:

Figure 3-1: Login Screen



Login Screen - Version 6.8.169

Login Name: brad

Password:

Server IP: 10.3.180.31

2. Choose one of the following login options:
   - **Username and Password:**
     a. In the EMS login screen, enter the username and password (note that Login Name and Password are case-sensitive). After the first successful login, the EMS application requires the user to enter only their Password. The other fields are saved by the application and displayed to the user.

Note: When entering the EMS for the first time, set the fields User Name to 'acladmin' and Password to 'pass_1234' or 'pass_12345'. These first-time access defaults are case sensitive. The Administrator can modify these first-time access defaults later, after defining system Users.

b. Enter the IP address of the EMS server to which you wish to connect.

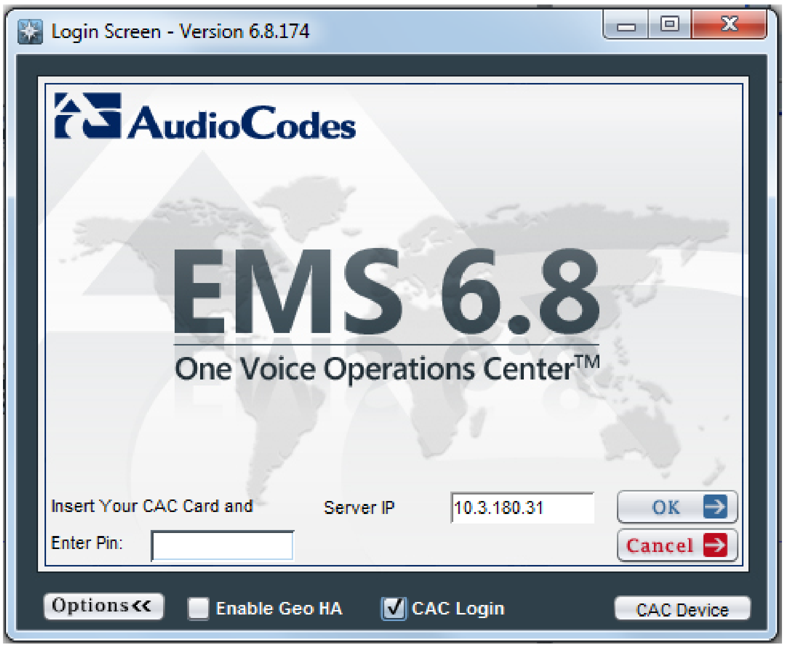
c. If your EMS server is enabled for HA, proceed to step 3 below or click **OK**.

- **Authentication using CAC card:**

a. In the EMS login screen, select the **CAC PIN Number** check box and then enter the CAC PIN number to login to the EMS client.

b. Enter the IP address of the EMS server to which you wish to connect.

Figure 3-2: CAC Login Screen



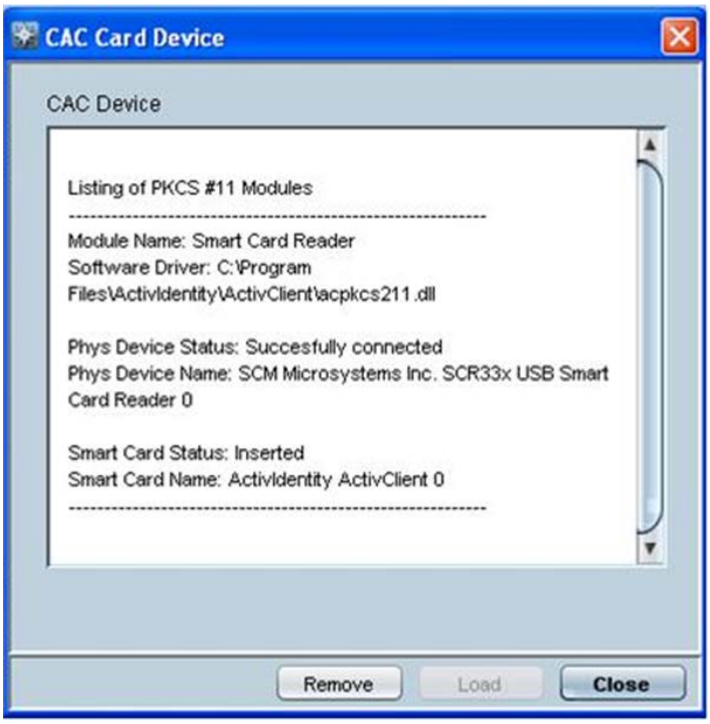
Insert Your CAC Card and Enter Pin:

Server IP 10.3.180.31

□ Enable Geo HA ☑ CAC Login

c. To view the status of the CAC Device, select the **CAC Device** button; the CAC Card Device status screen is displayed.

Figure 3-3: CAC Card Device



```
Listing of PKCS #11 Modules
---------------------------------------------------------
Module Name: Smart Card Reader
Software Driver: C:\Program
Files\ActivIdentity\ActivClient\acpkcs211.dll

Phys Device Status: Succesfully connected
Phys Device Name: SCM Microsystems Inc. SCR33x USB Smart
Card Reader 0

Smart Card Status: Inserted
Smart Card Name: ActivIdentity ActivClient 0
---------------------------------------------------------
```

d. Enter the IP address of the EMS server to which you wish to connect.

e. If your EMS server is enabled for HA, proceed to step 3 below or click **OK**.

3. **Geo HA option**

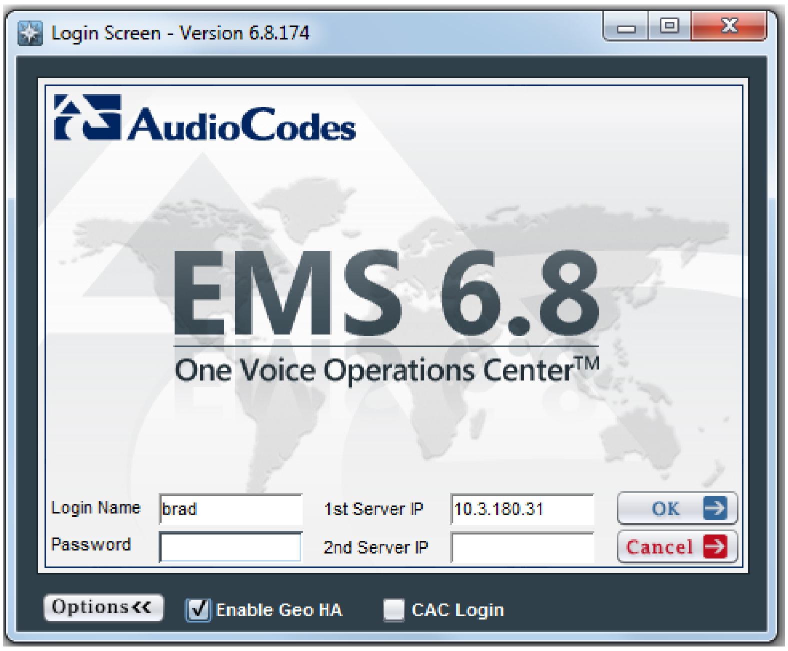
   In the case where the EMS application has been enabled for HA (High Availability) (via the EMS Server Manager-refer to the *EMS Server IOM*), and only when two EMS servers are located in different subnets, do the following:

   a. Select the **Enable Geo HA** checkbox.

   b. Enter the 1st Server IP Address, and then enter the 2nd Server IP Address and click **OK**.

   After a successful login, the EMS application searches for the active EMS server machine and connect to it.

Figure 3-4: Geo HA Option



Login Name: brad

Password:

1st Server IP: 10.3.180.31

2nd Server IP:

☑ Enable Geo HA

□ CAC Login

4. If any the above fields are incorrectly defined, a prompt is displayed indicating that the fields must be redefined correctly.

Once you successfully login to the EMS, the main screen is displayed (as described in the following section).

3.2 Getting Oriented in the EMS

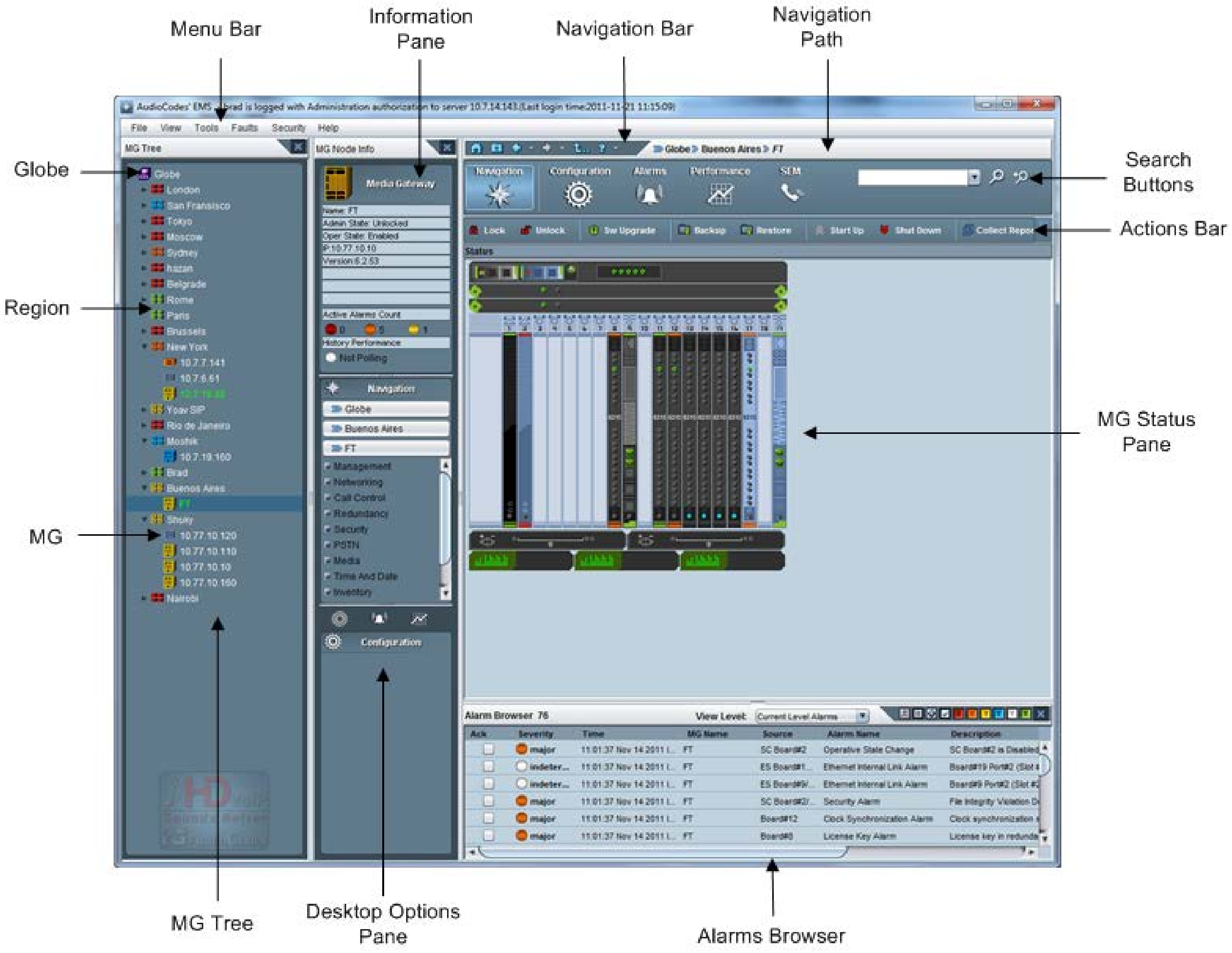
This subsection acquaints operators with the EMS. Read this section to quickly orient yourself to navigating in the EMS. The section explains the following:

- 'Navigating Down and Up System Hierarchy' on page 55.
- 'Selecting an Interface in the Context of an Element' on page 60 (and the concept of context-oriented screens).
- 'Using Color Coding to Assess Element Status' on page 62.

3.2.1 Navigating Down and Up System Hierarchy

The figure below shows the various components of the EMS main screen.

Figure 3-5: Main Screen Indicating Navigation Concepts



The EMS's main screen components are described as follows:

- **Menu bar** (File, View, Security) - Displays EMS system menus for access to various elements in the system.
- **Navigation Bar**- Located on the upper left side of the EMS status screen. This bar provides the shortcut navigation buttons. For more information, see EMS Navigation buttons below.
- **MG Tree** - media gateways Tree panel located in the left pane of the main screen.
- **MG Node Info pane** – Located to the right of the MG Tree. This pane provides preview information about the selected managed object. For example, the 'Admin' and 'Op State', the board type and Application type.
- **Navigation pane**–Located to the right of the MG Tree, below the MG Node Info pane. This pane displays the hierarchy of navigation logical options for the media gateway.
- **Main Pane** – Displays the various status screens of the EMS for the selected MG or internal managed object. MOs Lists– the various MOs lists are displayed in this screen after you have selected the desired provisioning option in the Navigation pane.

  This pane is replaced with the relevant desktop upon user selection, and can represent Status, Provisioning, Alarms or Performance Desktops. Each one of the desktops will have the Navigation pane available on the left side.
- **Actions bar**– Located below the Desktop toolbar, displays buttons that enable the user to perform the most commonly used actions for a specific provisioning entity. The items displayed in the Actions bar always reflect the current provisioning location. For example, when you view the 'Files' List screen, you see the 'Download File', 'Add File' and 'Remove File' actions in the Actions bar. All other actions available for each one of the navigation levels are available via Right-click options.
- **Desktop toolbar**–Located at the top of the screen below the navigation bar. The buttons allows you to navigate to the various management modes for the selected MG or internal managed object. The different management desktops available for selection include: Navigation; Configuration; Alarm and Performance. For more information on the different EMS management desktops, see 'EMS Management Desktops' below.
- **Desktop Options pane** – Located below the Navigation pane. Displays options for each desktop (Configuration pane, Alarms pane and Performance pane).You can also click the icons at the top of this pane to navigate between the different desktops.

3.2.1.1 EMS Management Desktops

This section introduces the different management desktops of the EMS. EMS entities are provisioned through an intuitive workflow process consisting of management desktops. At any point you can move easily between these desktops by clicking the appropriate button in the Desktop Navigation. The EMS includes the following management modes:

Note: For each EMS Management desktop, the Desktop pane is referred to according to the currently active working mode i.e. Navigation pane.

- **Navigation Desktop**

  When you select a gateway in the MG Tree, the EMS by default displays the media gateway Status screen. By default, top-level gateway provisioning options are displayed in the Navigation pane. When you select a media gateway board or other gateway component in the Status screen, different provisioning options are displayed in the Navigation pane.

  Once you select a top-level provisioning option, sub-level provisioning options may be displayed. Once you have navigated to the desired provisioning option in the navigation hierarchy, the respective MO's list is displayed in the Main pane. In addition, in the Configuration pane (down the Navigation pane) you can see all the provisioning screens relevant to this navigation level. Clicking on each one of them will transfer you to the Configuration desktop and open the selected screen.

  Use the MG Tree (displayed in the Navigation pane) to view and navigate down/up the system's hierarchical provisioning layers. The following different navigation hierarchy scenarios may be displayed in the MG Tree:

  - Globe>Region>MG>Top-level Navigation level(for example, Globe>Region>MG>Networking)
  - Globe>Region>MG>Top-level Navigation level>Sub-level (for example, Globe>Region>MG>Networking>Subnet #1)
  - Globe>Region>MG>TP Board>Navigation level >Trunk (for example, Globe>Region>MG>TP Board>PSTN>Trunk)

  Fast index transition allows the user to perform 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.

- **Configuration Desktop**

  Once you have selected the desired navigation option in the Navigation pane, you can configure the gateway, board or specific MO. In some cases, the desired provisioning option is automatically displayed in the Configuration pane (located below the Navigation pane). In other cases, you need to initially select an MO in the respective MO's list in the Main pane e.g. Subnets List. Once you click the desired provisioning option, the respective MO Provisioning frame is displayed.

  An option to lock/unlock the relevant MO is displayed in the Provisioning screens. At any time, you can return to the Navigation mode view by clicking the Navigation button in the Desktop toolbar.

  All the Provisioning frames opened in the desktop will remain open, until the user closes them. You can navigate back to view these frames by clicking **Configuration** in the Desktop toolbar. When you have finished provisioning, and do not require specific Provisioning frames, close them. Right-click configuration desktop option 'Close All' enables you to close all frames in a specific action and to close all frames associated with a media gateway after it has been removed from the EMS tree.

- **Alarms Desktop**

  You can display the Alarms browser for the relevant MO by selecting the relevant MO in the Navigation desktop and then clicking the **Alarms** button in the Desktop 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 MO. See Section 'Fault Management' on page 267.

- **Performance Desktop**

  You can run Performance Monitoring for the relevant MO by selecting the relevant MO in the Navigation desktop and then clicking the **Performance** button in the Desktop toolbar. In the Performance desktop, choose to run either History or Real-time performance monitoring. The respective Performance Monitoring provisioning screens are displayed. For History Performance Monitoring, you must first pre-configure the PM parameters in the PM History Configuration screen. 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. See Section 'Performance Management' on page 307.

- **SEM Desktop**

  You can open the SEM tool Web interface by clicking the **SEM** button in the Desktop toolbar. The SEM tool enables VoIP network administrators to identify the metric or metrics responsible for degradation in the quality of any VoIP call made over the network, seek to prevent this degradation and to optimize quality of experience for VoIP users. Data analysis is presented in various easy to view formats, such as pie-charts, bar charts and sortable tables. You can also filter information according to specific time periods and according to devices. See Section 'Introducing the Session Experience Manager' on page 330.

3.2.1.2 EMS Navigation Buttons

The following navigation buttons are displayed in the upper right side of the EMS Status screen:

Figure 3-6: EMS Navigation Buttons

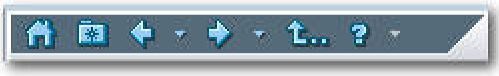


Table 3-1: Navigation Pane Description

Navigation Icon	Name	Description
⌂	Home	Click this icon to return to the main MG status screen from a lower navigation layer.
✱	Favorites	Click this icon to Add or Remove this location to the list of your favorites. Select your predefined favorite destination from the list.
←	Back	Use this button to return to the previous screen that was viewed.
▾	Back List	To view one of the last few screens you visited, click the arrow to the side of the Back button, and then click the screen you want from the list.
→	Forward	To view a screen you viewed before clicking the Back button, click the **Forward** button.
▾	Forward List	To view one of the last few screens you visited before Back button, click the small down arrow beside the **Forward** button, and then click the screen you want from the list.
↰..	Up Button	Click it to return from an element of a low hierarchical level (e.g., Trunk) up to an element of a higher hierarchical level (e.g., media gateway).
?	Online Help	Opens the context-sensitive EMS Online Help. The topic pertaining to the specific element that the user has navigated to open.

3.2.2 Selecting an Interface in the Context of an Element

This section describes how to select an interface in the context of an element.

➢ **To select an interface in the context of an element:**

1. After expanding a region and navigating to the level of a media gateway in the MG Tree, select a gateway in the MGs List; the MG Node Info pane is immediately updated with basic information (if available) corresponding to the selected gateway.
2. Double-click the gateway listed under the MGs List; the gateway level Status pane graphically representing the gateway is displayed, including the navigation buttons.
3. In the Navigation pane, navigate to the desired provisioning entities.
4. In the media gateway status pane, double-click a gateway component to open that component's Status pane or interface list. For example, when you double-click the TP board, the PSTN interface list is displayed, or when you double-click the SA/RTM board, the SAT component's status screen is displayed (see Section 'Accessing a TP-6310 in the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway (v2.1)' on page 139. After you select a TP board in the Status pane, the MG Node Info pane displays data relevant for the selected TP board. Then when you select the navigation options in the Navigation desktop, and select an MO in a List screen, the MG Node Info pane displays data relevant to the selected MO. For example, when you select the **PSTN** ► **DS1** option or select **PSTN** ► **SS7** ► **SS7 Links** and then select a DS1 trunk or SS7 link in the respective List screens, the MG Node Info pane changes correspondingly. Selecting these MOs in a List screen and then clicking 'Configuration' in the Navigation desktop opens those MOs provisioning parameters screens. The same principle applies to working at the gateway level; however at this level, in some cases you can access a provisioning screen directly without having to select an MO in a List screen. For example, the 'Networking' provisioning option.

3.2.2.1 Blades and CPE

This section describes how to select an interface in the context of an el ement for blades and CPEs.

➢ **To select an interface in the context of an element:**

1. Double-click a device's module to open that module's Status pane.
2. In the Navigation pane, navigate to the desired provisioning entities.

3.2.3 Context-Sensitive Behavior

The Status pane as well as the navigation bar allows operators to move up and down the system hierarchy. Operators can always determine their exact location/level in the system hierarchy from the location/level indication at the top of the screen. Note that even a single click changes the location/level. 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, and 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 e.g.. 'Lock,' 'Unlock' or 'Activate', 'Deactivate' .

3.2.4 Using Color Coding to Assess Element Status

Color codes apply to all EMS GUI screens and elements/entities represented in those screens: the Status pane, icons, alarms, LEDs, etc. Assess the status of any system entity/element in the EMS according to the following color code scheme:

Table 3-2: Assessing System Entity Status via Icon Color

System Entity Status	Color	Region Icon	AudioCodes Device Icon
Clear (OK)	Green	🟩	🟩 🟩 🟩 🟩 🟩
Warning	Blue	🟦	🟦 🟦
Minor	Yellow	🟨	🟨 🟨
Major	Orange	🟧	🟧 🟧
Critical	Red	🟥	🟥 🟥 🟥 🟥 🟥
Shutting Down	Gray Gradient		▨ ▨
Locked	Gray		▨ ▨
Unable to Connect	Red Gradient		🟥 🟥 🟥 🟥 🟥
Unknown entity	? ?	🟪	

Note: These icons are examples. The other VoIP devices supported by the EMS use the same color convention as the icons in these examples.

4 EMS Application License Key

Note: This feature is currently not supported.

Starting from version EMS 5.8, when the EMS server runs on the Linux OS, a Feature Key file for Enterprise Gateways is required to support Gateways Management. This feature is not applicable for the Mediant 3000 / 5000 / 8000 high density Gateways.

The License Key file specifies the supported/managed Gateway number and types per specific EMS server machine. Server machine identification is performed according to the machine 'hostid'. The EMS server application checks the Feature Key file during the application startup, and in case it's missing or invalided/expired, refers the user to the AudioCodes support representative to receive an appropriate License Key file.

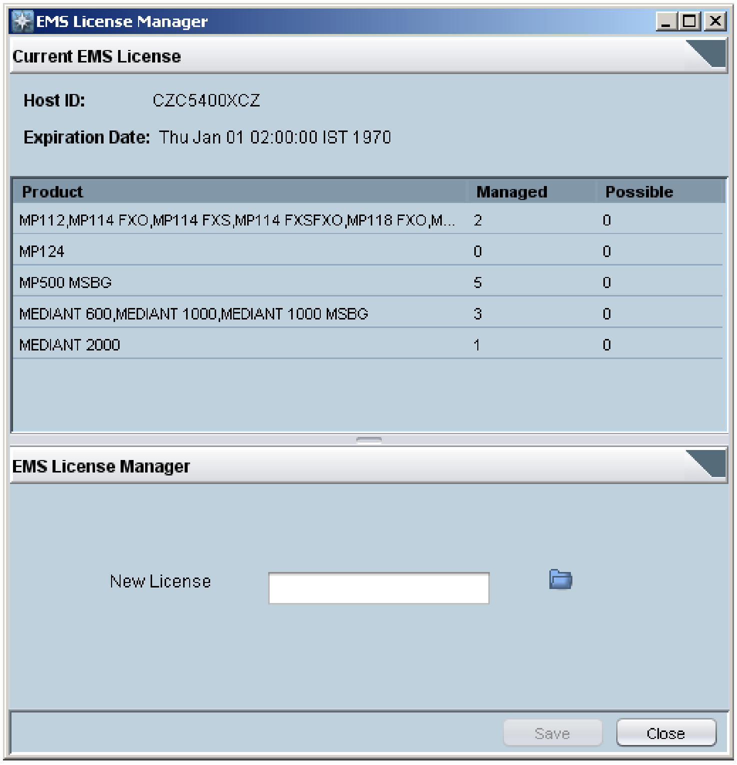
4.1 Viewing your Current License Key

This section describes how to view your current License Key.

➢ **To view your current license key:**

- Select the **File -> EMS License menu** option to view your current License Key; the screen below is displayed:

Figure 4-1: EMS License Manager



Host ID: CZC5400XCZ

Expiration Date: Thu Jan 01 02:00:00 IST 1970

Product	Managed	Possible
MP112,MP114 FXO,MP114 FXS,MP114 FXSFXO,MP118 FXO,M...	2	0
MP124	0	0
MP500 MSBG	5	0
MEDIANT 600,MEDIANT 1000,MEDIANT 1000 MSBG	3	0
MEDIANT 2000	1	0

For each Gateway, the number of currently managed Gateways (Managed column) that are provisioned by License Key (Possible column) are displayed.

4.2 Loading a New License Key

This section describes how to load a new License Key.

➢ To load a new license key file:

- Click the file chooser in the bottom of the screen, select the file, and click **Save**.

The upper screen pane is updated. Note, each license key file should include the entire number of managed Gateways. This action overwrites the previous license key file content.

5 Software Manager

The EMS Software Manager (Tools > Software Manager) enables operators to view, add or remove configuration files and regional files. During the Gateway definition in the EMS (Add Gateway action or Auto Detection), EMS connects to the Gateway and automatically determine its version. However, each new Gateway version, fix or software update provided to customers must be added to the Software Manager to enable a media gateway Software Upgrade.

The Software Manager stores files in the EMS and provides operators with the capability to load files to the VoIP device while testing and verifying file type and software version with device type.

Filter check boxes in the Software Manager facilitate easy access to device-specific files.

When using the Products Filtering option, note that some of the products are arranged in groups. For example, when searching for MP software files, all the MPs must be selected, as the same CMP file is suitable for all the MP gateways.

Note: The Software manager is context sensitive when it is opened during the Gateway software upgrade; therefore it only displays filtered files which are relevant to the selected Gateway.

The following information is displayed on each file stored in the Software Manager:

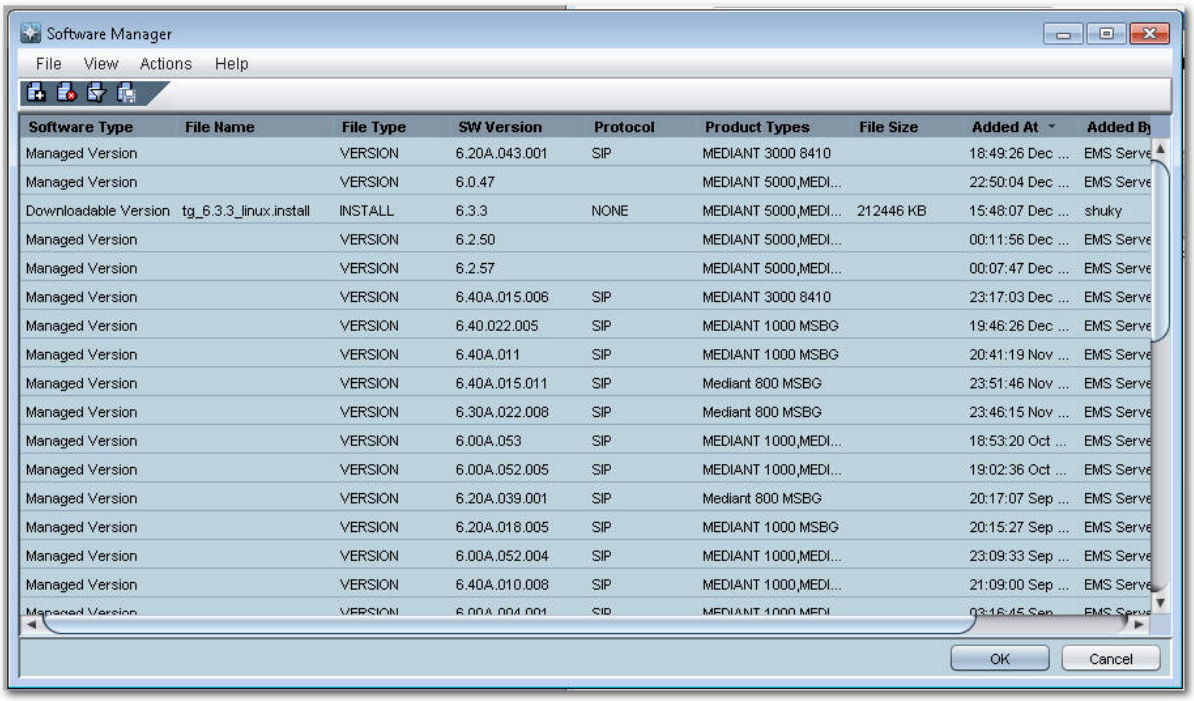
- **Software Type**

  Three software types are supported:

  - Downloadable version: media gateways of this version are recognized and managed by the EMS and users can load the version to the media gateway.
  - Managed version: media gateways of this version are recognized and managed by the EMS. The version cannot be loaded to any media gateway.
  - Auxiliary file: An auxiliary file can be loaded to any MG.
    - **File Name**
    - **File Type**: *cmp, tar* or *tar.gz*, *cpt, vp*, *cas* and *dat*. Refer below for detailed information.
    - **SW Version**: This column is relevant only to software files.
    - **Protocol**: This column is relevant to CPE software versions only. Control protocols supported: MGCP, MEGACO and SIP.
    - **Product Types**: This column includes 'MGs Types' to which the listed version applies.
    - **File Size** - the actual software file size, in bytes. Applicable for loadable versions of the software file, and Regional Files.

- **Added At** - the time when the software version or regional file was added.
- **Added By** - the name of the operator who defined the software version or regional file.
- **Description** - a description of the file written by the operator when defining the file in the Software Manager.

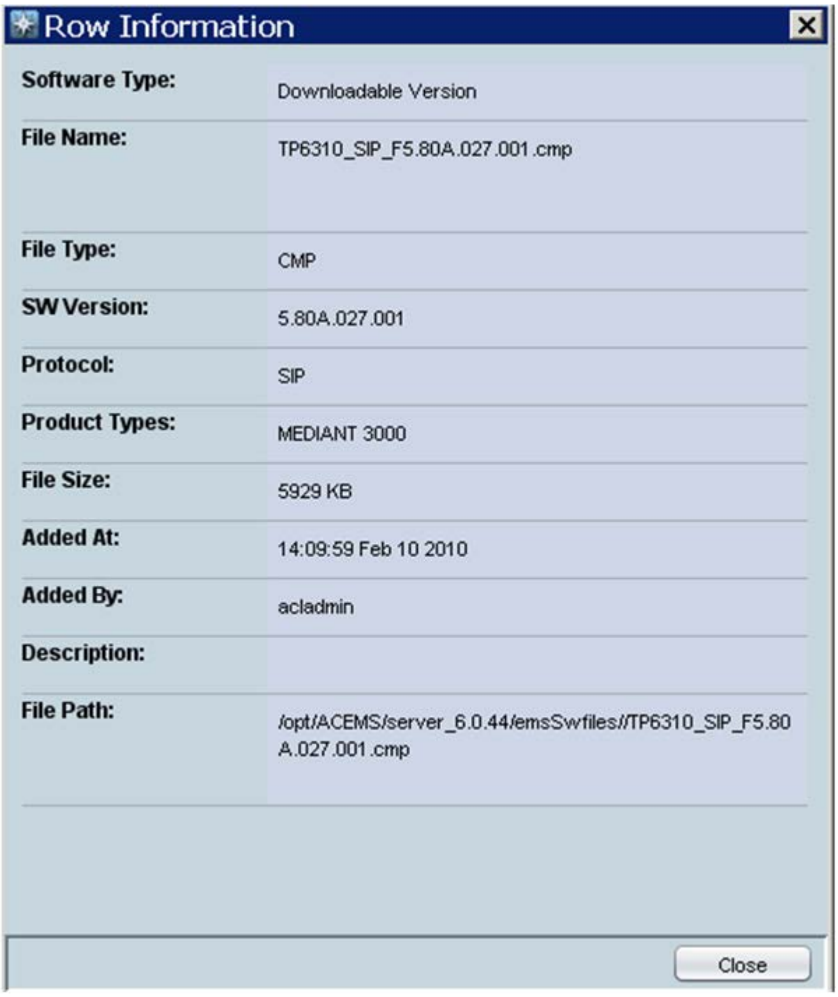
Figure 5-1: Software Manager



Software Type	File Name	File Type	SW Version	Protocol	Product Types	File Size	Added At	Added By
Managed Version		VERSION	6.20A.043.001	SIP	MEDIANT 3000 8410		18:49:26 Dec ...	EMS Serve
Managed Version		VERSION	6.0.47		MEDIANT 5000,MEDI...		22:50:04 Dec ...	EMS Serve
Downloadable Version	tg_6.3.3_linux.install	INSTALL	6.3.3	NONE	MEDIANT 5000,MEDI...	212446 KB	15:48:07 Dec ...	shuky
Managed Version		VERSION	6.2.50		MEDIANT 5000,MEDI...		00:11:56 Dec ...	EMS Serve
Managed Version		VERSION	6.2.57		MEDIANT 5000,MEDI...		00:07:47 Dec ...	EMS Serve
Managed Version		VERSION	6.40A.015.006	SIP	MEDIANT 3000 8410		23:17:03 Dec ...	EMS Serve
Managed Version		VERSION	6.40.022.005	SIP	MEDIANT 1000 MSBG		19:46:26 Dec ...	EMS Serve
Managed Version		VERSION	6.40A.011	SIP	MEDIANT 1000 MSBG		20:41:19 Nov ...	EMS Serve
Managed Version		VERSION	6.40A.015.011	SIP	Mediant 800 MSBG		23:51:46 Nov ...	EMS Serve
Managed Version		VERSION	6.30A.022.008	SIP	Mediant 800 MSBG		23:46:15 Nov ...	EMS Serve
Managed Version		VERSION	6.00A.053	SIP	MEDIANT 1000,MEDI...		18:53:20 Oct ...	EMS Serve
Managed Version		VERSION	6.00A.052.005	SIP	MEDIANT 1000,MEDI...		19:02:36 Oct ...	EMS Serve
Managed Version		VERSION	6.20A.039.001	SIP	Mediant 800 MSBG		20:17:07 Sep ...	EMS Serve
Managed Version		VERSION	6.20A.018.005	SIP	MEDIANT 1000 MSBG		20:15:27 Sep ...	EMS Serve
Managed Version		VERSION	6.00A.052.004	SIP	MEDIANT 1000,MEDI...		23:09:33 Sep ...	EMS Serve
Managed Version		VERSION	6.40A.010.008	SIP	MEDIANT 1000,MEDI...		21:09:00 Sep ...	EMS Serve
Managed Version		VERSION	6.00A.004.001	SIP	MEDIANT 1000,MEDI		03:16:45 Sep	EMS Serve

To view additional details for each Auxiliary file, double-click an Auxiliary file entry. The following screen is displayed:

Figure 5-2: Software Manager File Details



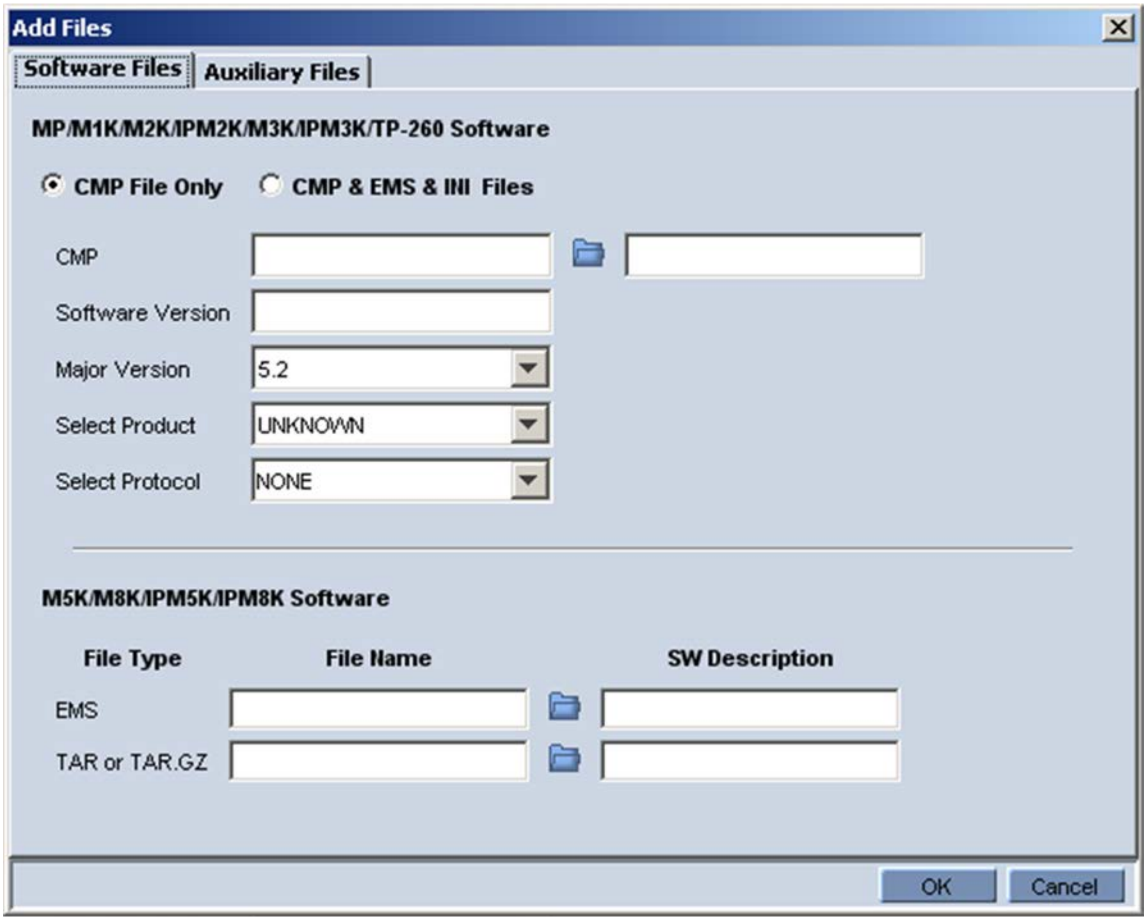
Software Type:	Downloadable Version
File Name:	TP6310_SIP_F5.80A.027.001.cmp
File Type:	CMP
SW Version:	5.80A.027.001
Protocol:	SIP
Product Types:	MEDIANT 3000
File Size:	5929 KB
Added At:	14:09:59 Feb 10 2010
Added By:	acladmin
Description:	
File Path:	/opt/ACEMS/server_6.0.44/emsSwfiles//TP6310_SIP_F5.80A.027.001.cmp

File types managed by the Software Manager are as follows:

- **Configuration files for CPE Products**
  - *cmp* file only
    - *cmp* file - This is the main software image file. Load the file to change the software version (for example).
    - Software version - automatically defined after adding the *cmp* file
    - Major version - automatically defined after adding the *cmp* file
    - Select a product (corresponding to the *cmp* file from list).
    - Select a protocol from the list e.g. SIP
  - *cmp* & *ini* & *ems* files

Note: This option is reserved for backward compatibility reasons, and must be used by AudioCodes FAEs only.

Figure 5-3: Add CMP File



● CMP File Only ○ CMP & EMS & INI Files

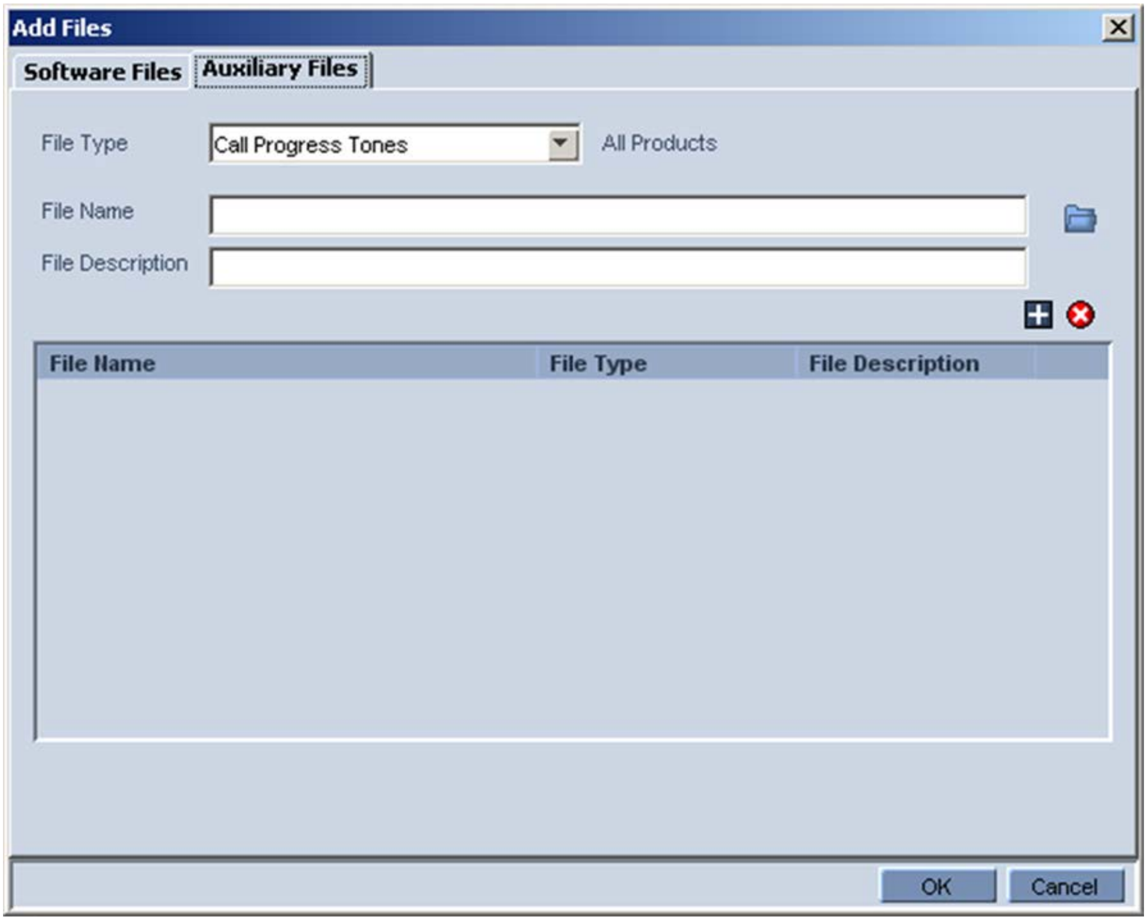
CMP	
Software Version	
Major Version	5.2
Select Product	UNKNOWN
Select Protocol	NONE

- Configuration files for the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway
  - **tar** or **tar.gz** file - This is the main software image file. Load the file to change the software version (for example). Note that you must change the default filename sc_software.tar.gz when loading it to the Software Manager as it's not possible for two files with the same name to be loaded in the Software Manager at the same time.
  - **ems** file - Includes information relating to the software version. For EMS use only. The file is not loaded to the gateway.
- **Auxiliary Files**

The table below summarizes the auxiliary files used for different gateways. A reset indication for the CPE products signifies that after performing a software download of an auxiliary file, the gateway must be reset for it to operate with the new file.

Note: Auxiliary files are not connected to the media gateway software version.

Figure 5-4: Software Manager-Adding Auxiliary Files



File Type: Call Progress Tones — All Products

File Name:

File Description:

File Name	File Type	File Description

Table 5-1: Auxiliary Files

File Type	MediaPack (Analog Gateway)	CPEs	Mediant 5000 / 8000 TP Lock / Unlock required
Call Progress Tone (All Products)	✓(Reset)	✓(Reset)	✓
Pre recorded Tones (All Products)	✓	✓	✓
Voice Prompts (All Products)	✓	✓	✓
APS Segments XML (IPM2K/IPM3K)	-	✓	-
VXML (IPM2K/IPM3K/IPM5K/IPM8K)	-	✓ IPmedia 2000 / 3000	✓ IPmedia 5000 / 8000
X509 Private Key File (All Products)	✓ (Reset)	✓ (Reset)	✓
X509 Server Certificate File (All Products)	✓ (Reset)	✓ (Reset)	✓
X509 Trusted Root Certificate File (All Products)	✓ (Reset)	✓ (Reset)	✓
CAS (All Digital Products)	-	✓ (Lock/Unlock Trunks)	✓
Dial Plan File (All Digital Products)	-	✓	✓
Coefficient File (Analog MP / M1K)	✓ (Reset)	-	-
User Information (All Products SIP)	✓ (Reset)	✓ (Reset)	✓
External Coders (All Products MGCP / MEGACO)	✓ (Reset)	✓ (Reset)	✓
License Keys (All Products)	-	✓	✓

File Type	MediaPack (Analog Gateway)	CPEs	Mediant 5000 / 8000 TP Lock / Unlock required
INI Stand Alone	✓	✓	-
Alarms Properties File (M5K/M8K)	-	-	-
Alarm Propagation Rules (M5K/M8K)	-	-	✓
V5.2 File	-	Mediant 3000 8410 only	-
AMD Sensitivity File	-	✓	-
Data Configuration File	-	MSBR Products only	-

- **Tones**
  - Call Progress Tones (all products) - This is a region-specific, telephone exchange-dependent file. Four common Call Progress Tones are: Dial tone, Busy tone, Ringback tone and Reorder tone. Call Progress Tones provide call status/call progress to customers, operators and connected equipment. Default Tone: U.S.A.
  - Pre-Recorded Tones – This dat file enhances the VoIP device's capabilities of playing telephone exchange tones. Tones that cannot be defined in the Call Progress Tones file can be defined in this file, thereby enabling the device to offer a wide range of tones.
  - Voice Prompts - Played by the VoIP device during the phone conversation on Call Agent/Gatekeeper/Proxy request. Load it if you have an application requiring Voice Prompts (All MEGACO/MGCP-configured analog and digital media gateways support Voice Prompts; the SIP-configured IPmedia 2000 also supports Voice Prompts).
- **MSecurity**
  - X509 Private Key File – X.509 Private Key
  - X509 Server Certificate File – X.509 Public Certificate
  - X509 Trusted Root Certificate File – X.509 Public Certificate of Trusted Root entity (CA)
- **Digital**
  - Dial Plan File – The source file for the Dial Plan configuration contains a list of the known prefixes (e.g. area codes, international telephone number patterns) for the PSTN to which the gateway is connected. The gateway uses this information to detect end-of-dialing in certain CAS configuration where the end-indicator (ST) is not used.

- CAS file: Includes E1/T1 CAS signaling files, which are not required for ISDN protocols.

- **Analog**
  - Coefficient file – This file (different for FXS and FXO gateways) contains telephony interface configuration data for the VoIP device. This information includes telephony interface characteristics such as DC and AC impedance, feeding current and ringing voltage. The file is specific to the type of telephony interface that the VoIP device supports. In most cases, you must load this file.

- **Additional Files**
  - **User Information** – Defines user information (for the SIP application)
  - **External Coders** – The External Coders file defines which coders are to be supported by the media gateway board.
  - **License Keys** – Customers can upgrade a single media gateway's features or multiple media gateways' features simultaneously by purchasing a feature key. The key is sent to customers in a license file which customers must save to their PC hard drive following receipt. To add the file to the EMS's Software Manager and to load to the VoIP device/s, See Section 'media gateway Installation, Software Upgrade and Regional Files Distribution' on page 249. The new key overwrites the previous key.
  - **INI Stand Alone**: Includes initial configuration of MediaPack parameters that cannot be configured after adding (defining) the device in the EMS.

    During the INI file download user can select one of the three options below:
    - 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).
  - **Alarms Properties File** – Used to customize the SNMP alarm's description and severities. When this file is absent (default state), the system generates SNMP alarms using the default descriptions and severities. Customers may override or modify properties of specific SNMP alarms by creating the Alarm Properties file. For additional information, refer to the *Programmer's User Guide*.
  - **Alarm Propagation Rules File** – When an alarm is raised on the MO, the Severity attribute of the MO itself is updated accordingly. In addition, the Severity attribute of the “father MO” may be updated as well. For example, when a major PSTN alarm is raised on Trunk, severity of the Trunk is set to a major and severity of the media gateway board where this trunk resides is set to minor. The alarm propagation behavior is tuned for each and every alarm and is not configurable.

- **AMD Sensitivity File** – This file is used to define the sensitivity levels for Answering Machine Detection (AMD) for all digital products, except the Mediant 800. The file is prepared in XML format and converted to a binary file by the DCONVERT utility, and can be downloaded to these specific devices at any time.
- **Data Configuration File (RMX)** – This file is used to store the Data related (router) configuration for the Mediant 800 MSBR and Mediant 1000 MSBR devices. This file can be downloaded to these specified devices or uploaded to them by the EMS application.
- **The V5.2 Configuration File** – includes V5.2 users defined for the Gateway. The file format is a CSV (coma separated file), where ";" in the beginning of the line represents a commented line. The file includes all of the V5.2 users of the media gateway.

  When a customer wishes to add or remove users, the file must be modified and re-downloaded to the Gateway again.

  The file should start from file format version. File format version defined today is 1.0. The first line in the file must be as follows:

  ;1.0 version

  Each row in the file identifies the V5.2 endpoint and should include the following attributes:

  - Command: add or del (defined for future use). In this version, the only applicable command is **add**.
  - V5.2 IF number: 1-30
  - Port/Line number: 0-4799
  - L3 Address: 0-32766

Note:

- Port/Line number and L3 Address must be unique within V5.2 IF
- During File download, all the V5.2 Interfaces must be Offline
- Maximal number of ports defined in the file must be 14,800
- User can define several files for a single Gateway (for example a separate file per V5.2 Interface) and download these files to the Gateway. When managing multiple files for a single Gateway, users should select the **Incremental File** download option.

Below is an example of a V5.2 endpoints file:

```
; 1.0 version
; Command (add/del), V5.2 IF number, Port/Line number, L3 Address
; add to interface 12 line/port 35 with L3 address 4000
1, 12, 35, 4000
;add to interface 17 line/port 22 with L3 address 2345
1,17,22,2345
```

5.1 Adding a New File to the Software Manager

This section describes how to add a new file to the Software Manager.

➢ **To add new files to the Software Manager:**

1. Click the **Add** File icon (indicated with a plus sign in the upper left corner of the Software Manager screen) or open the Actions menu and choose the option **Add File**; the Add Files screen (shown in the figure below) opens.
2. Click the icon of a folder located adjacent to the File Type to be added, and in the dialog box that opens, navigate to the file (saved in your PC); click **OK**.
3. Define fields in the Add Files screen according to your requirements and click **OK**; the name of the file/s is displayed defined in the **'**File Name' field in the Software Manager screen. Click **OK**; the files that you defined will now appear listed in the Software Manager.

5.2 Removing Files from the Software Manager

This section describes how to remove files from the Software Manager.

➢ **To remove a file (or files) from the Software Manager:**

- Select it/them in the Software Manager, click the **Remove File** icon (indicated with an 'x'), or open the Actions menu, choose the option **Remove File** and click **OK**; the file is removed.

Note: A file cannot be removed when another gateway is using it. When removing a *cmp* file, the *ini* file is removed with it.

5.3 Saving Files in Software Manager to the Network

You may save files on the Software Manager to a location on your network.

Note: A row defined as 'Managed Version' cannot be saved. Downloadable and Auxiliary files can be saved.

➢ To save a file from the Software Manager:

1. In the Software Manager, select the file that you wish to save to your network.
2. Click the **Save File** icon, or open the Actions menu and choose the option **Save File** and click **OK**.
3. In the File Location dialog, navigate to the required file location and click **OK**.

Reader's Notes

6 Defining VoIP Devices, Managing the MG Tree

After installing and getting started with the EMS, you're ready to define / configure your VoIP devices in the GUI so that you'll be capable of provisioning and managing them.

Each type of VoIP device is defined differently in the EMS. This section shows you how to define a VoIP device in the MG Tree, how to move it from one r egion to another and how to remove it from the EMS.

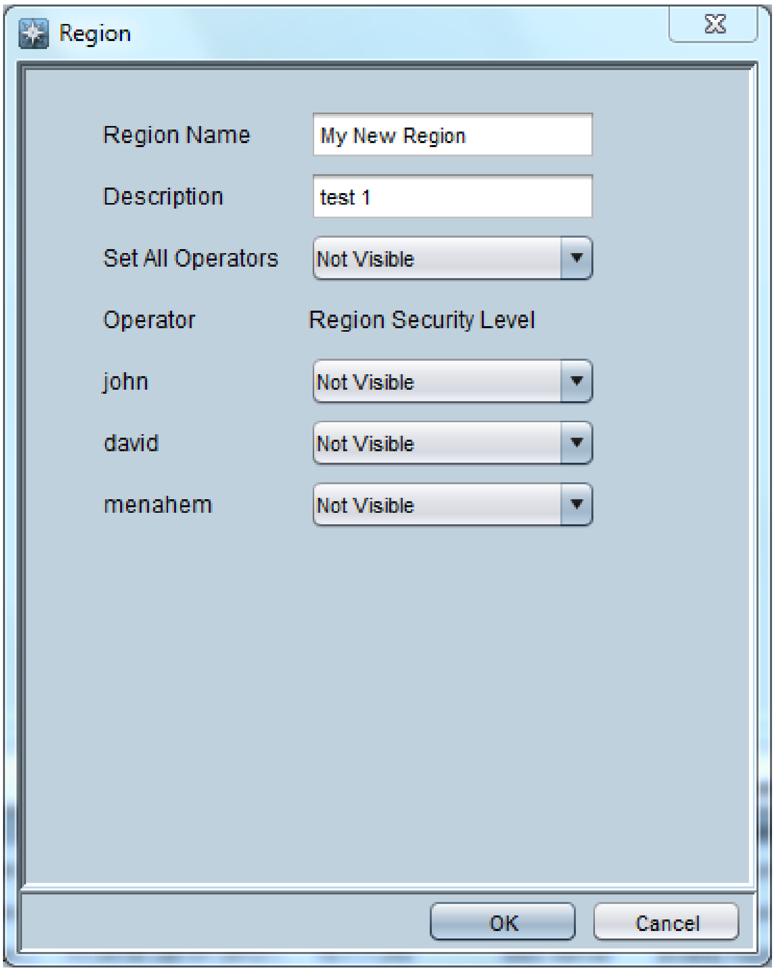
6.1 Configuring a Region

This section describes how to configure a region.

➢ To configure a region:

1. Right-click Globe (the root) in the MG Tree and choose **Add Region** from the sub-menu; the following screen appears:

Figure 6-1: Configuring a Region



Region

Region Name: My New Region

Description: test 1

Set All Operators: Not Visible

Operator	Region Security Level
john	Not Visible
david	Not Visible
menahem	Not Visible

2. Define the region's name and type in an optional description.

3. Set users security rights for the new region (note: 'Set All Operators' selection sets the same security level for all users).
4. Click **OK**; the requested region is added.

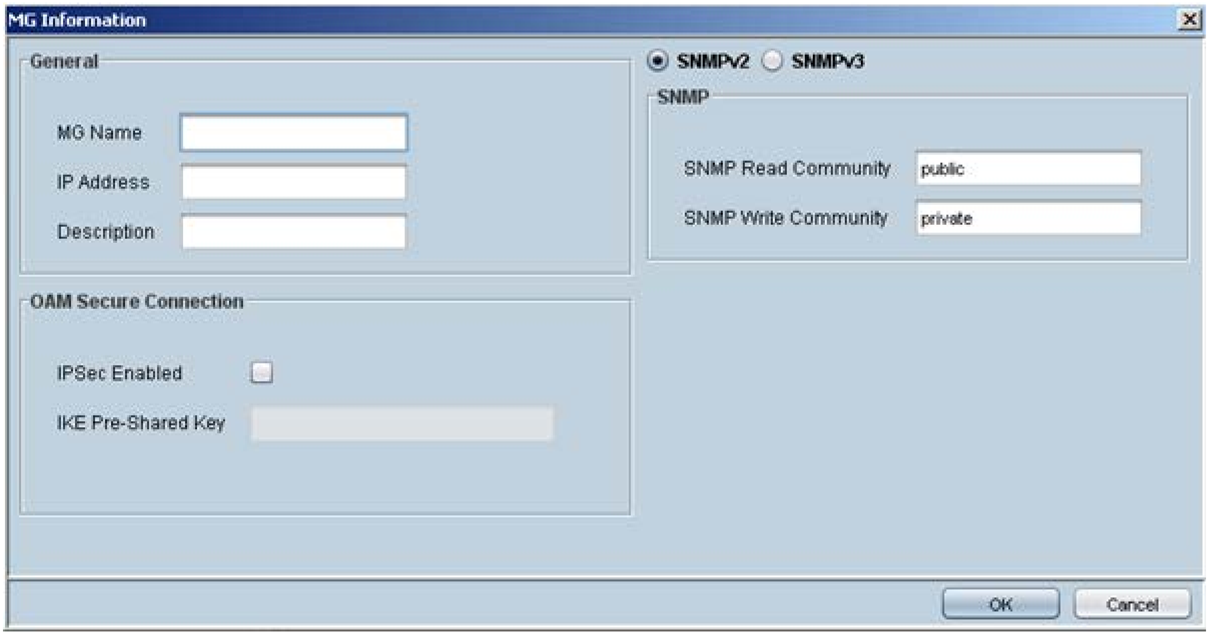
6.2 Defining a Mediant 5000, Mediant 8000

This section describes how to define a Mediant 5000 and Mediant 8000 Gateway.

➢ **To add a gateway, perform the following steps:**

1. Right-click the region in the Navigation tree to which to add a gateway and choose the option **Add MG** from the sub-menu; the MG Information screen appears:

Figure 6-2: MG Information - SNMP2



MG Information

General

MG Name

IP Address

Description

● SNMPv2 ○ SNMPv3

SNMP

SNMP Read Community: public

SNMP Write Community: private

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key

2. Define the gateway name as you would like it to be referenced in the EMS; enter the gateway's IP Address, Description, the gateway's SNMP and Security Information.

3. Configure the OAM Secure Connection; if you're operating over a secured connection over IPSec protocol, select the **IPSec Enabled** checkbox and enter the Pre-shared Key defined in the media gateway.

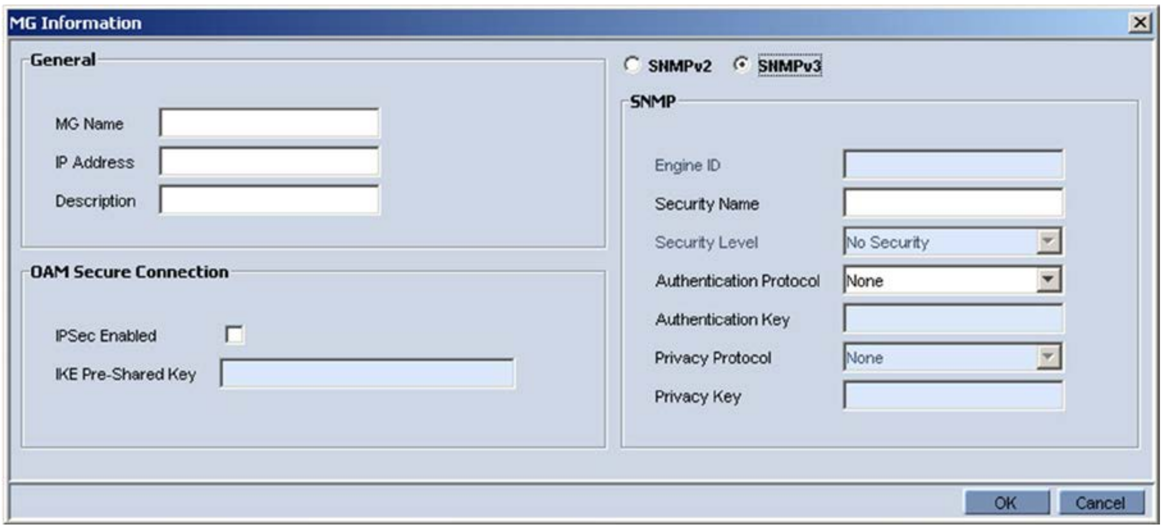
Note: The IPSec and SNMP related security settings configured in this procedure should match the media gateway installation definitions. The Pre-shared Key string defined in the EMS and in the media gateway must be identical.

4. Configure SNMP between the EMS and the media gateway; select either the **SNMPv2c** (default) or **SNMPv3** checkboxes.

5. If you are configuring SNMPv2c, enter values for the SNMP Read Community (default-public) and SNMP Write Community (default-private) fields.

If you selected SNMPv3, the following screen is displayed:

Figure 6-3: MG Information- SNMP3



○ SNMPv2 ● SNMPv3

Security Level: No Security

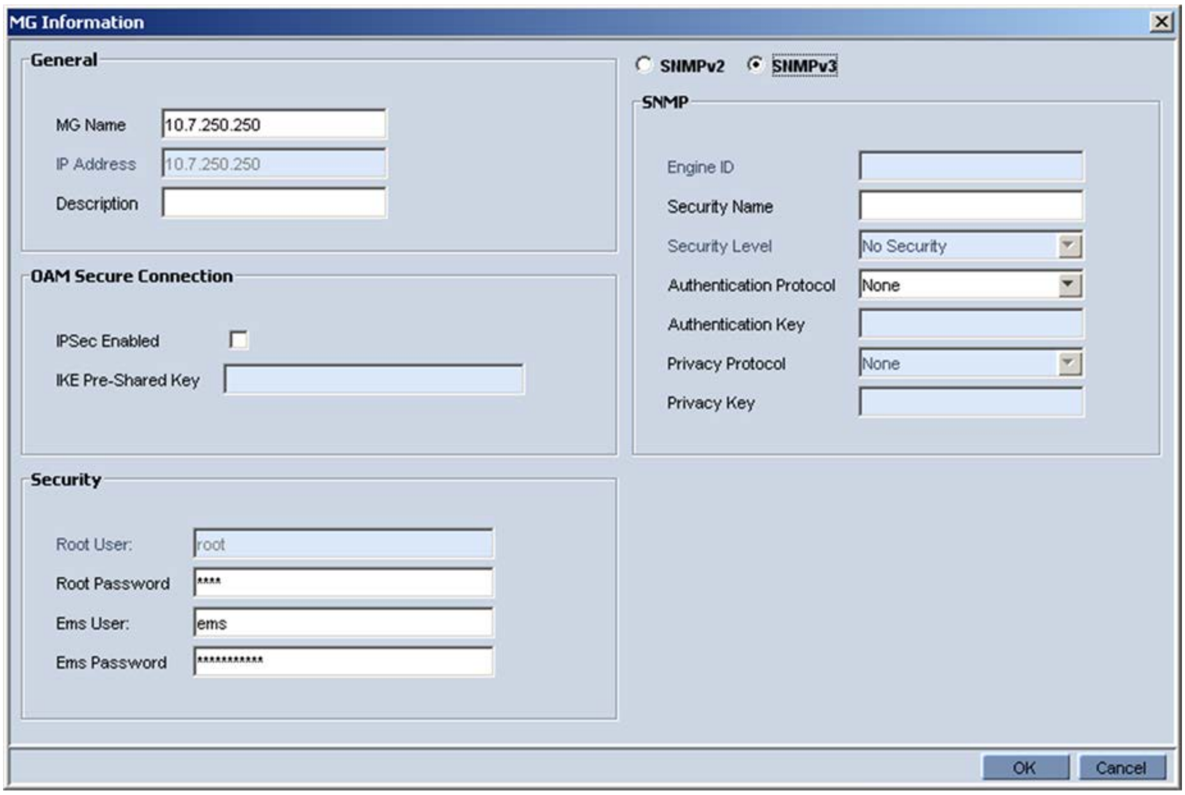
Authentication Protocol: None

Privacy Protocol: None

6. Do the following:
   - In the 'Security Name' field, enter the Security name of the SNMPv3 user.
   - In the 'Authentication Protocol' field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the Security Level field.
   - In the 'New Authentication Password' field, enter a new Authentication Password.
   - In the 'Privacy Protocol' field, from the drop-down list, select a Privacy Protocol .
   - In the 'New Privacy Password' field, enter a new Privacy Password.
7. Click **OK**; the requested gateway is added to the required region.
8. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of it, including its LEDs, must be displayed in the EMS's Status screen (refer to the figures of the status panes). If you do not view a graphic representation of the gateway in the Status screen, see Section 'Troubleshooting' on page 385 to resolve the issue.

The gateway is added with all fields set to their default values. To change the defaults, right-click the gateway in the MG Tree and choose **Details**; the MG Information screen opens (refer to the figure below).

Figure 6-4: MG Information - Secured Connection Enabled



MG Information

General

MG Name: 10.7.250.250

IP Address: 10.7.250.250

Description:

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key:

Security

Root User: root

Root Password: ****

Ems User: ems

Ems Password: ***********

○ SNMPv2 ● SNMPv3

SNMP

Engine ID:

Security Name:

Security Level: No Security

Authentication Protocol: None

Authentication Key:

Privacy Protocol: None

Privacy Key:

9. Define fields 'Root Password' and 'EMS Password' to be used during the Software Upgrade and Auxiliary Files download procedures. The defaults of these password fields in the gateway and the EMS are identical; if you remove/add a gateway, the passwords on the EMS side will be the defaults. If you change the default of a password on the EMS side, make sure the value in the gateway is identical, and vice-versa. To change a password, first change the password in the gateway and then open the screen 'MG Details' in the EMS and update the field accordingly.

10. Click **OK**; the requested gateway is added to the required region. Click **OK**; an Action Report is displayed, indicating the result of the add action for each gateway added.

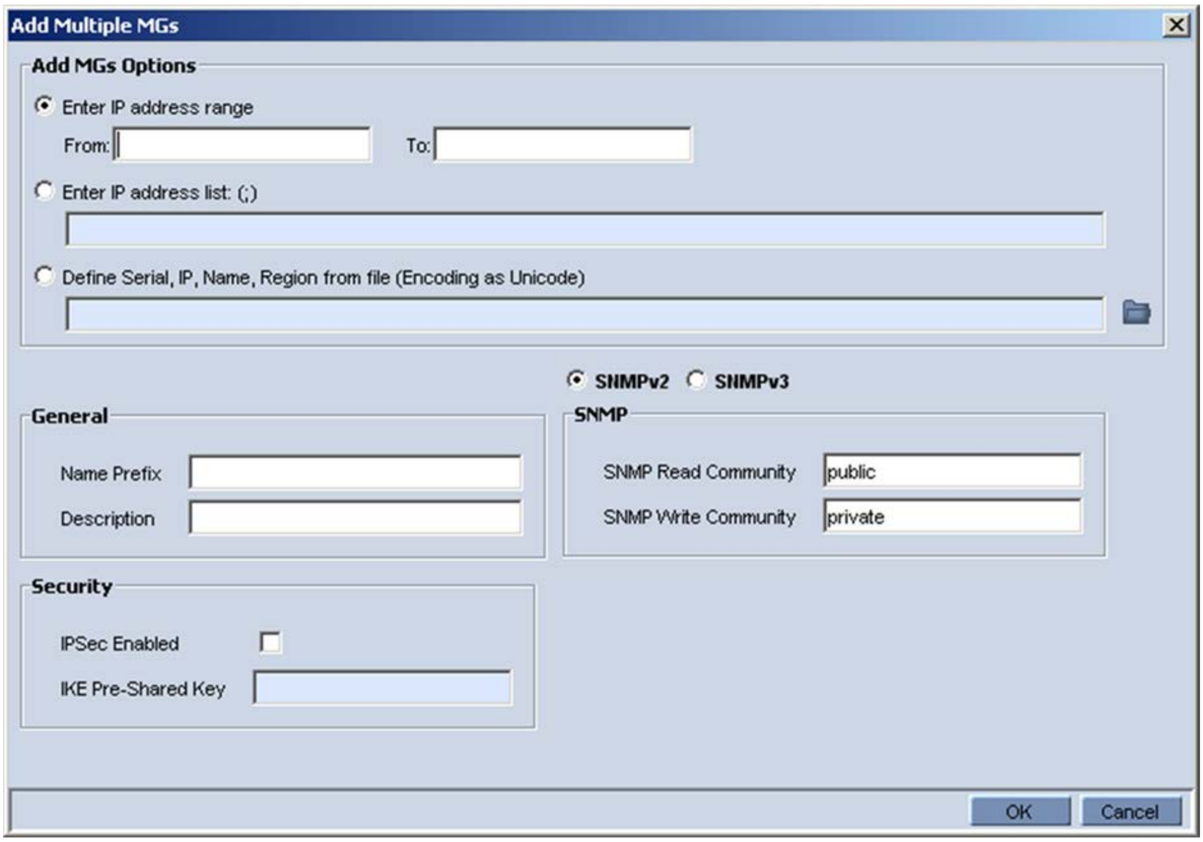
6.2.1 Defining Multiple Mediant 5000, Mediant 8000 Gateways

This section describes how to define multiple gateways.

➢ **To add a set of gateways simultaneously:**

1. Right-click the region in the MG Tree to which to add the multiple gateways and from the sub-menu, choose the option **Add MG** ; the 'Add Multiple MGs' screen appears:

Figure 6-5: Add Multiple MGs



Add Multiple MGs

Add MGs Options

● Enter IP address range

From: To:

○ Enter IP address list: (;)

○ Define Serial, IP, Name, Region from file (Encoding as Unicode)

● SNMPv2 ○ SNMPv3

General

Name Prefix

Description

SNMP

SNMP Read Community: public

SNMP Write Community: private

Security

IPSec Enabled □

IKE Pre-Shared Key

2. Check the 'Enter IP address range' check box, define the 'From' and 'To' fields and click **OK**. All devices in the defined range are added to the MG Tree with name combined as 'Name Prefix' + 'IP Address'.
3. Alternately, define multiple devices by checking check box 'Enter IP address list; in the field, define the IP addresses of the multiple gateways to be added, separating the IP address from each other with a semi colon.
4. Define the gateway name prefix as you would like it to be referenced in the EMS (a gateway's name comprises the prefix and IP address) and the gateway's SNMP Read and Write Community strings. If you're operating over a secured connection, check option 'Secured Connection Enabled' and enter the Pre-shared Key supplied by AudioCodes. The default Pre-shared Key is same for all media gateways and the EMS.

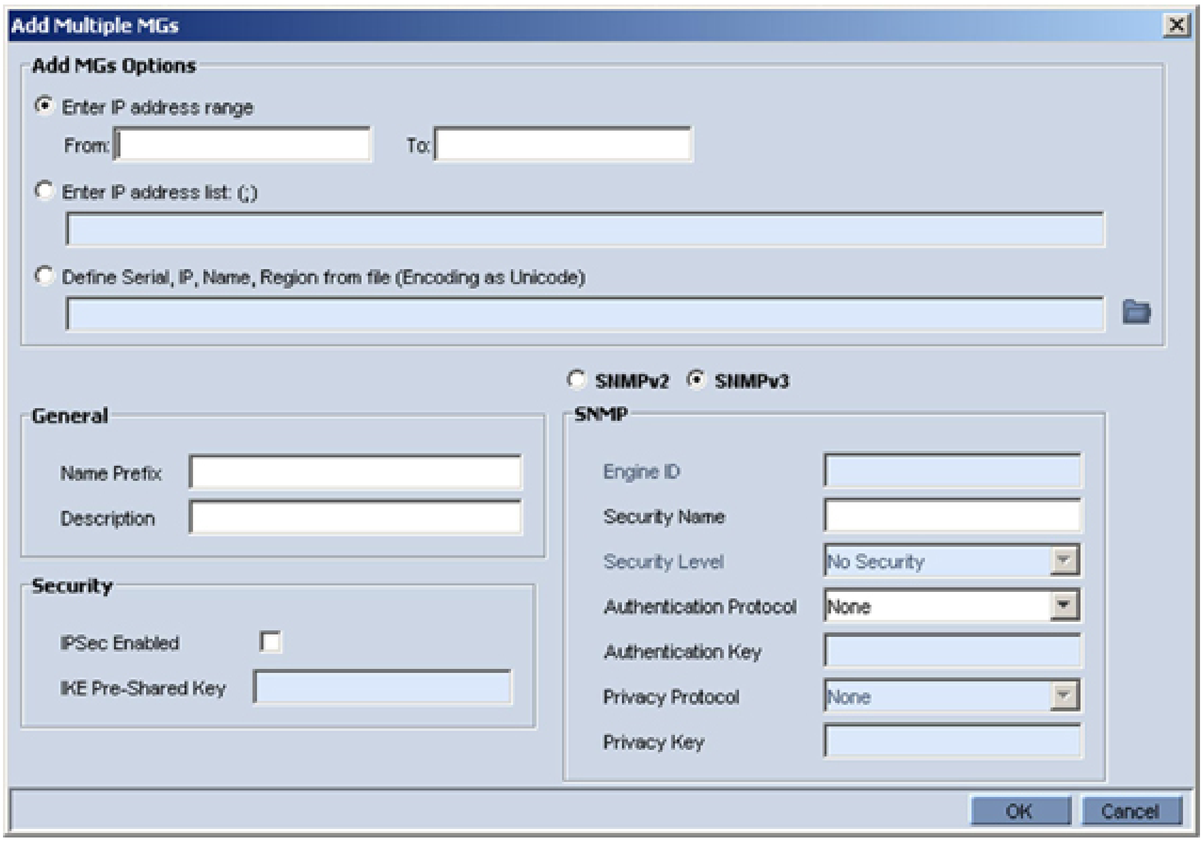
5. Verify that all the gateways are successfully defined in the EMS: Firstly, check the MGs List information; secondly, enter each gateway's status screen. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of the gateway, including its LEDs, must be displayed in the Status screen (refer to the figures displaying gateway status under 'MediaPack' on page 211). If you do not view a graphic representation of the gateway in the Status screen, see Section 'Troubleshooting' on page 385 to resolve the issue.
6. To change the default Telnet user name and password, right-click in the MGs Tree on each gateway and choose **Details**. Define the FTP and Telnet user and password to be used during the Software Upgrade procedure.
7. If you're operating over a secured connection over IPsec protocol, select the **IPsec Enabled** checkbox and enter the IPsec Pre-shared key defined in the media gateway.

Note: The IPSec and SNMP related security settings configured in this procedure should match the media gateway installation definitions. The Pre-shared Key string defined in the EMS and in the media gateway must be identical.

8. Configure SNMP between the EMS and the media gateway; select either the SNMPv2c (default) or SNMPv3 checkboxes.
9. If you are configuring SNMPv2c, enter values for the SNMP Read Community (default-public) and SNMP Write Community (default-private) fields.

If you selected SNMPv3, the following screen is displayed:

Figure 6-6: Add Multiple MGs-SNMPv3



● Enter IP address range
● SNMPv3
Security Level: No Security
Authentication Protocol: None
Privacy Protocol: None

10. Do the following:
    - In the 'Security Name' field, enter the Security name of the SNMPv3 user.
    - In the 'Authentication Protocol' field, from the drop-down list, select an authentication protocol. The corresponding security level is displayed in the **Security Level** field.
    - In the 'New Authentication Password' field, enter a new Authentication Password.
    - In the 'Privacy Protocol' field, from the drop-down list, select a Privacy Protocol.
    - In the 'New Privacy Password' field, enter a new Privacy Password.
11. Click **OK**; the requested gateway is added to the required region. Click **OK**; an Action Report is displayed, indicating the result of the add action for each gateway added.

Note: The last option of defining a Serial Number, IP and Name from the file is not supported for the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway.

6.3 Predefinition or Automatic Detection

This section describes the predefinition or automatic definition of the media gateway CPE devices.

6.3.1 Blades and CPE

EMS users can either predefine the VoIP equipment (CPE products) or let the EMS automatically detect it.

6.3.2 Automatic Detection

This section describes how to enable an automatic detection event (coldStart) to be sent to a configured SNMP Manager when a gateway device is connected to the power supply and the network at the customer's premises is rebooted and initialized.

When the MP is located inside the NAT network, it can connect to the Internet Public Network as long as the connection between the EMS server and the MP device is alive. This can be ensured by configuring the MP device to send coldStart and Keep Alive traps to the EMS server, which allows the EMS to perform SNMP SET and GET commands at any time. EMS recognizes the MP device according to the **sysDesc** field and MAC address on the device itself, and according to the entries in the EMS database and GWs tree. The MPs default name is composed of the router's IP address and port number. Sometimes the NAT changes the IP address and port for the MP devices. EMS recognizes these changes after the MP device is reset.

➢ **To set up automatic detection:**

1. Configure the following INI parameters on the media gateway device:

```
SNMPPort_0 = 161
SNMPManagerTrapPort_0 = 162
SNMPManagerIsUsed_0 = 1
SNMPManagerTrapSendingEnable_0 = 1
SNMPManagerTableIP_0 = 10.7.6.17
```

2. In the event that the media gateway is configured behind a NAT, you also need to configure the keep alive trap INI parameters on the media gateway as follows:

```
SendKeepAliveTrap = 1
KeepAliveTrapPort = 1161
NatBindingDefaultTimeout = 30
```

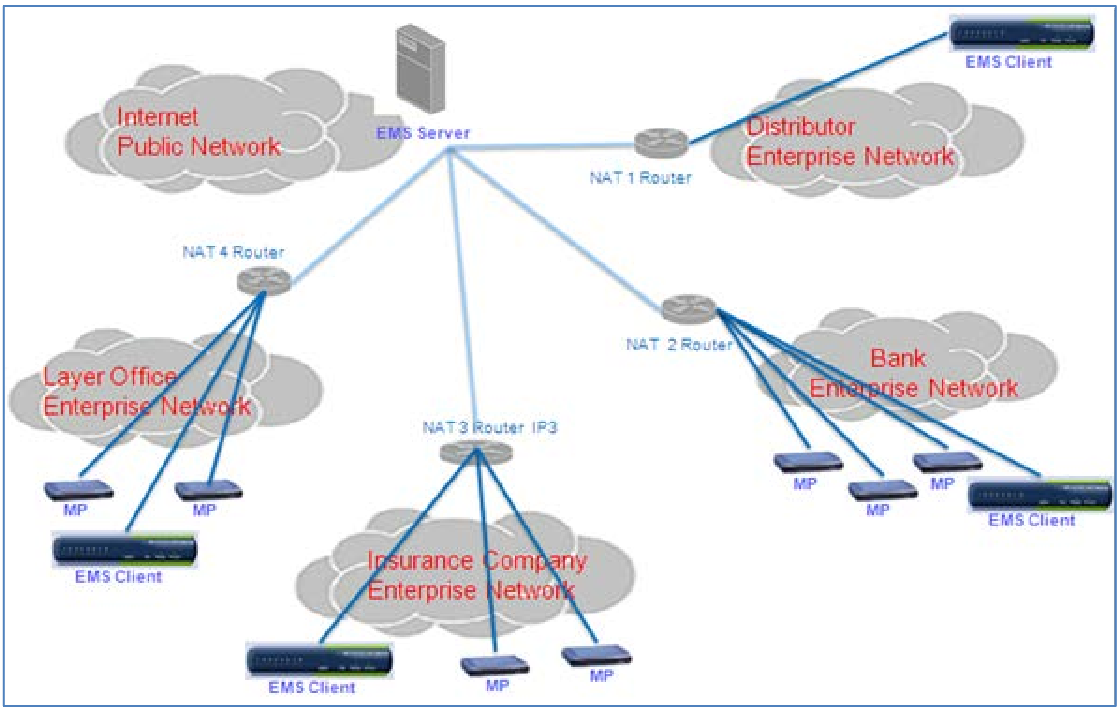
3. After the device is connected to the power supply and the network at the customer's premises, it performs a reboot and at the end of the initialization process, sends a coldStart trap event to the pre-provisioned 'SNMP Manager' name. When the coldStart trap is received, the EMS connects the device, verifies (from the version defined in the Software Manager) that it's AudioCodes' device, automatically defines a new Region named 'Auto Detection' and adds the device to this region. If the Region already exists, the device is simply added to it.

Note: Periodically check if Region 'Auto Detection' is created and move newly detected media gateways to the Regions appropriate to your network.

The figure below illustrates how MPs and EMS Clients and server can be located in the NAT Network:

- Each MP device in each LAN i.e. a Bank Enterprise Network connects to the Internet Public Network via a NAT IP address (configured in the **Applications** tab in the Network Parameters Provisioning screen).
- Connectivity between the EMS server and the MP device is maintained by configuring the MP device to coldStart and send Keep Alive traps.

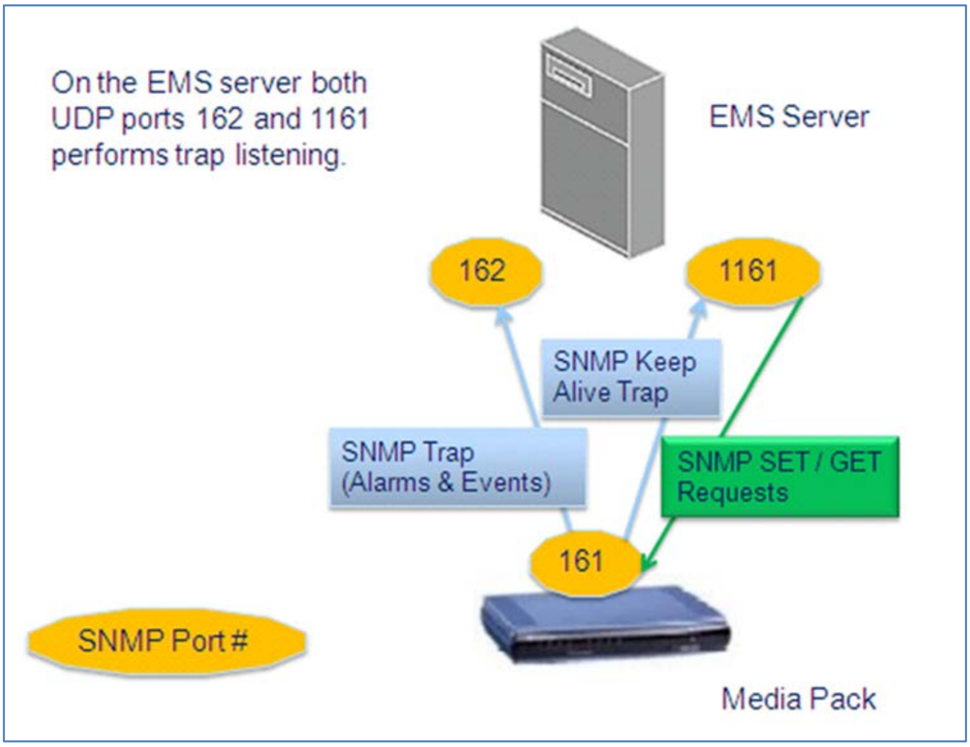
Figure 6-7: MP-NAT Configuration



The figure below describes how the EMS and the gateways manage SNMP connectivity:

- UDP ports 162 and 1161 on the EMS server are configured to listen for traps from the MP device. For example, the trap “an Ethernet link alarm indicates that the Redundant Link (Physical port #2) is down”.
- UDP port 1161 on the EMS server sends SNMP SET requests to the MP device. For example, in the EMS, the NAT Primary Server IP address is configured to 10.7.6.120.

Figure 6-8: Sending SNMP Traps to EMS Server (Behind a NAT)


On the EMS server both UDP ports 162 and 1161 performs trap listening.
EMS Server
162
1161
SNMP Keep Alive Trap
SNMP Trap (Alarms & Events)
SNMP SET / GET Requests
161
SNMP Port #
Media Pack

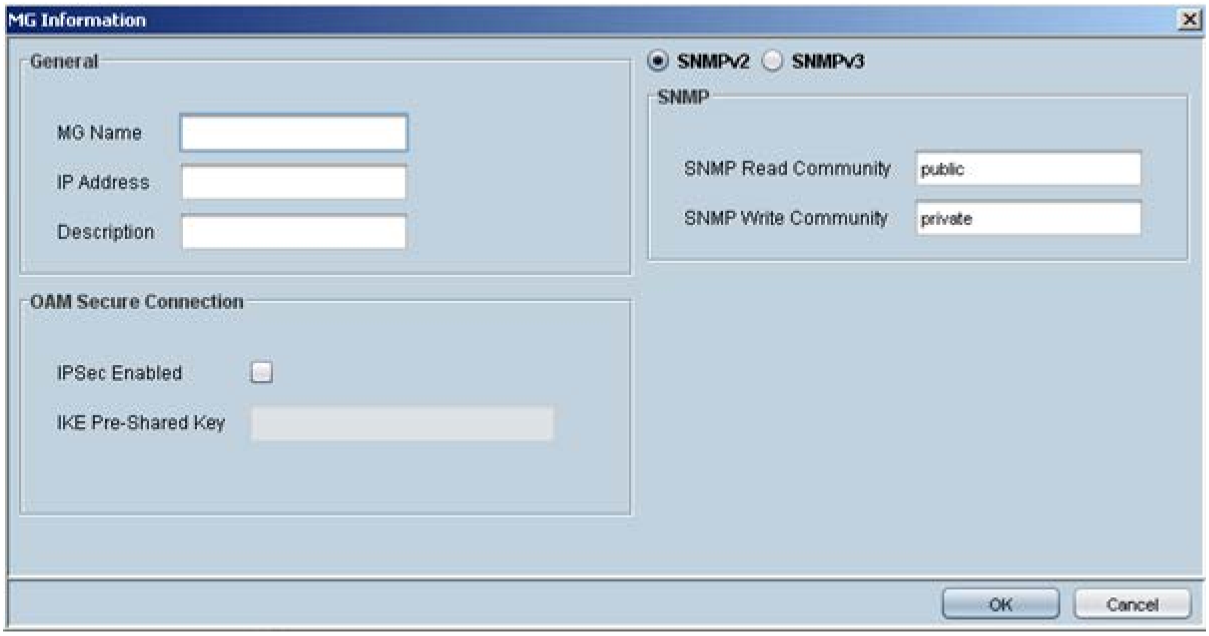
6.3.3 Defining a Single Blade or CPE

This section describes how to define a single blade or CPE.

➢ **To add a gateway:**

1. Right-click the region in the MG Tree to which to add multiple gateways and from the sub-menu, choose option **Add MG**.

Figure 6-9: MG Information - SNMP2



MG Information

General

MG Name:

IP Address:

Description:

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key:

● SNMPv2 ○ SNMPv3

SNMP

SNMP Read Community: public

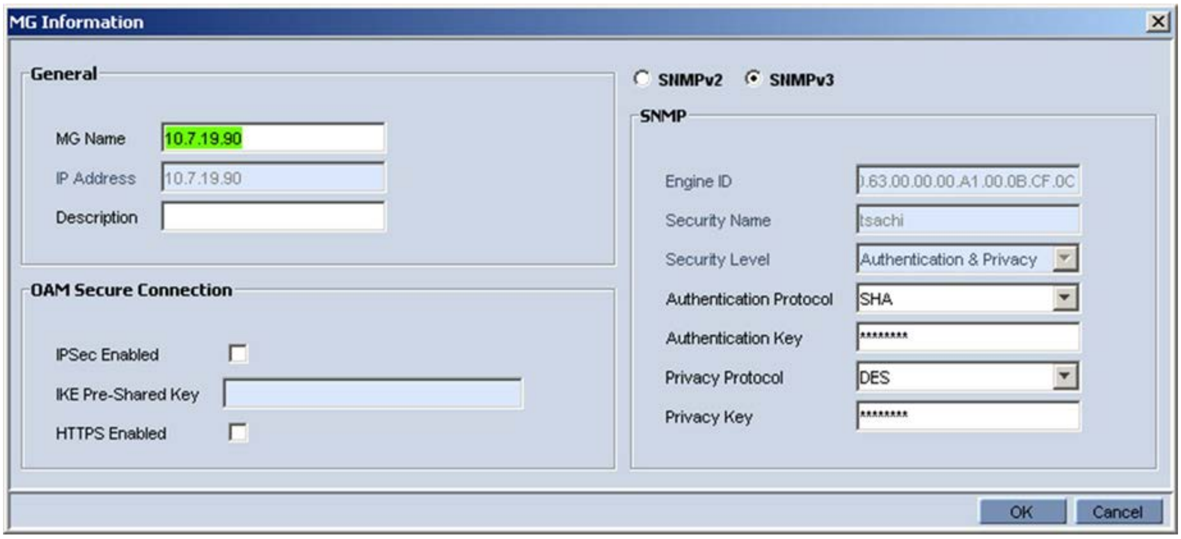
SNMP Write Community: private

2. Define the gateway name as you would like it to be referenced in the EMS Enter the gateway's IP Address, Description, and the gateway's SNMP Read and Write Community strings (if you are configuring SNMPv2) or Security fields if you are configuring SNMPv3, in which case proceed to the next step.
3. Do the following:
   a. In the 'Security Name' field, enter the Security name of the SNMPv3 user.
   b. In the 'Authentication Protocol' field, from the drop-down list, select an authentication protocol. The corresponding security level is displayed in the 'Security Level' field.
   c. In the 'New Authentication Password' field, enter a new Authentication Password.
   d. In the 'Privacy Protocol' field, select a Privacy Protocol from the drop-down list box.
   e. In the 'New Privacy Password' field, enter a new Privacy Password.

4. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of the gateway, including its LEDs, must be displayed in the EMS's Status screen. If you do not view a graphic representation of the gateway in the EMS's status screen, see Section 'Troubleshooting' on page 385 to resolve the issue.

   The gateway is added with HTTP communication enabled. To change the defaults, right-click the gateway in the MG Tree and choose **Details**; the MG Information screen opens (refer to the figure below).

Figure 6-10: MG Details



MG Information

○ SNMPv2 ● SNMPv3

General

MG Name: 10.7.19.90

IP Address: 10.7.19.90

Description:

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key:

HTTPS Enabled □

SNMP

Engine ID: .63.00.00.00.A1.00.0B.CF.0C

Security Name: tsachi

Security Level: Authentication & Privacy

Authentication Protocol: SHA

Authentication Key: ********

Privacy Protocol: DES

Privacy Key: ********

5. If you're operating over a secured connection over IPsec protocol, select the **IPsec Enabled** checkbox and enter the IPsec Pre-shared Key defined in the media gateway.

Note: The Pre-shared Key string defined in the EMS and in the media gateway must be identical.

6. Check the **HTTPS Enabled** option if required.
7. Click **OK**; the requested gateway is added to the required region.

Note: To perform changes in the EMS and MG connectivity related to the SNMP version, see Section 'Security Management' on page 333.

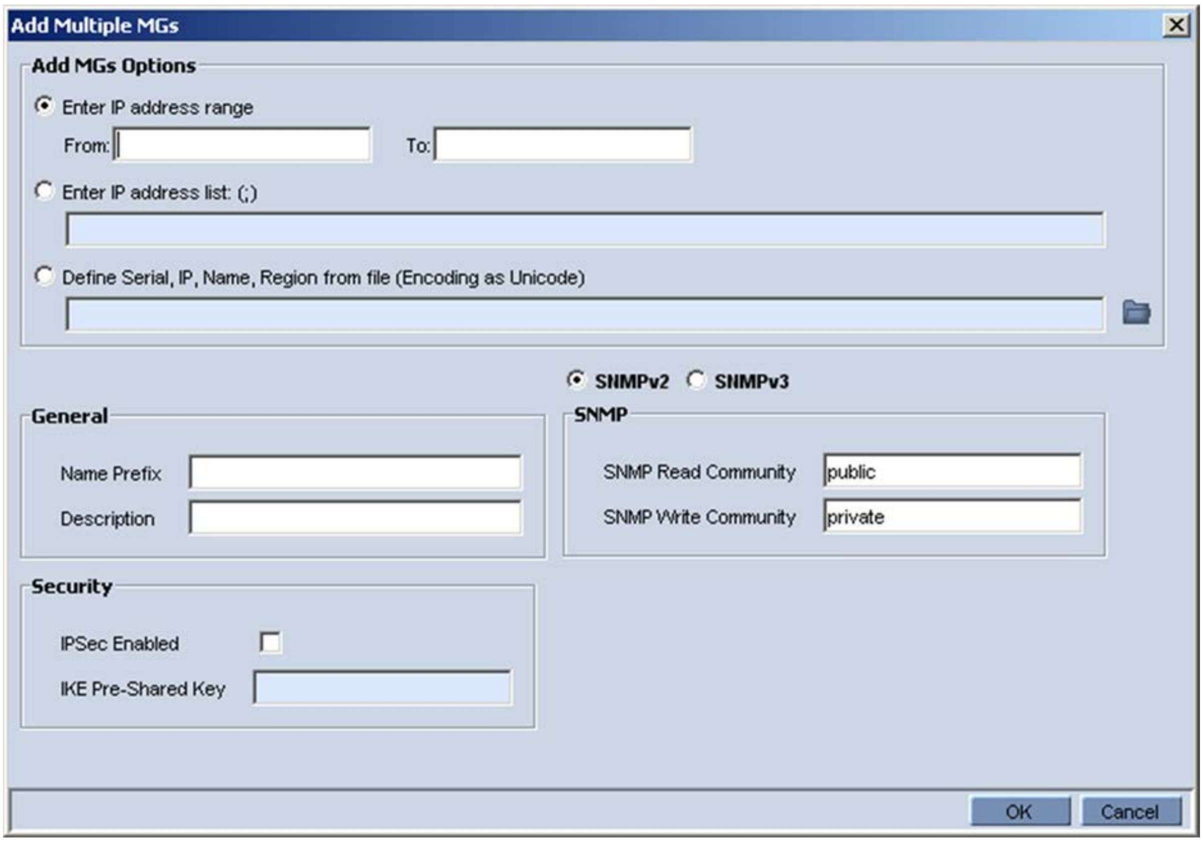
6.3.4 Defining Multiple Blades and CPEs

The EMS supports defining multiple devices (Multiple CPE devices) in a single screen on condition that all devices have identical SNMP Read and Write Community strings. The device hardware type is detected when connecting for the first time to the gateway.

➢ **To add multiple gateways:**

1. Right-click the region in the MG Tree to which to add multiple gateways and choose option **Add Multiple MGs** from the sub-menu.

Figure 6-11: Add Multiple MGs-SNMPv2


Add Multiple MGs

Add MGs Options

● Enter IP address range

From: To:

○ Enter IP address list: (;)

○ Define Serial, IP, Name, Region from file (Encoding as Unicode)

● SNMPv2 ○ SNMPv3

General

Name Prefix

Description

SNMP

SNMP Read Community: public

SNMP Write Community: private

Security

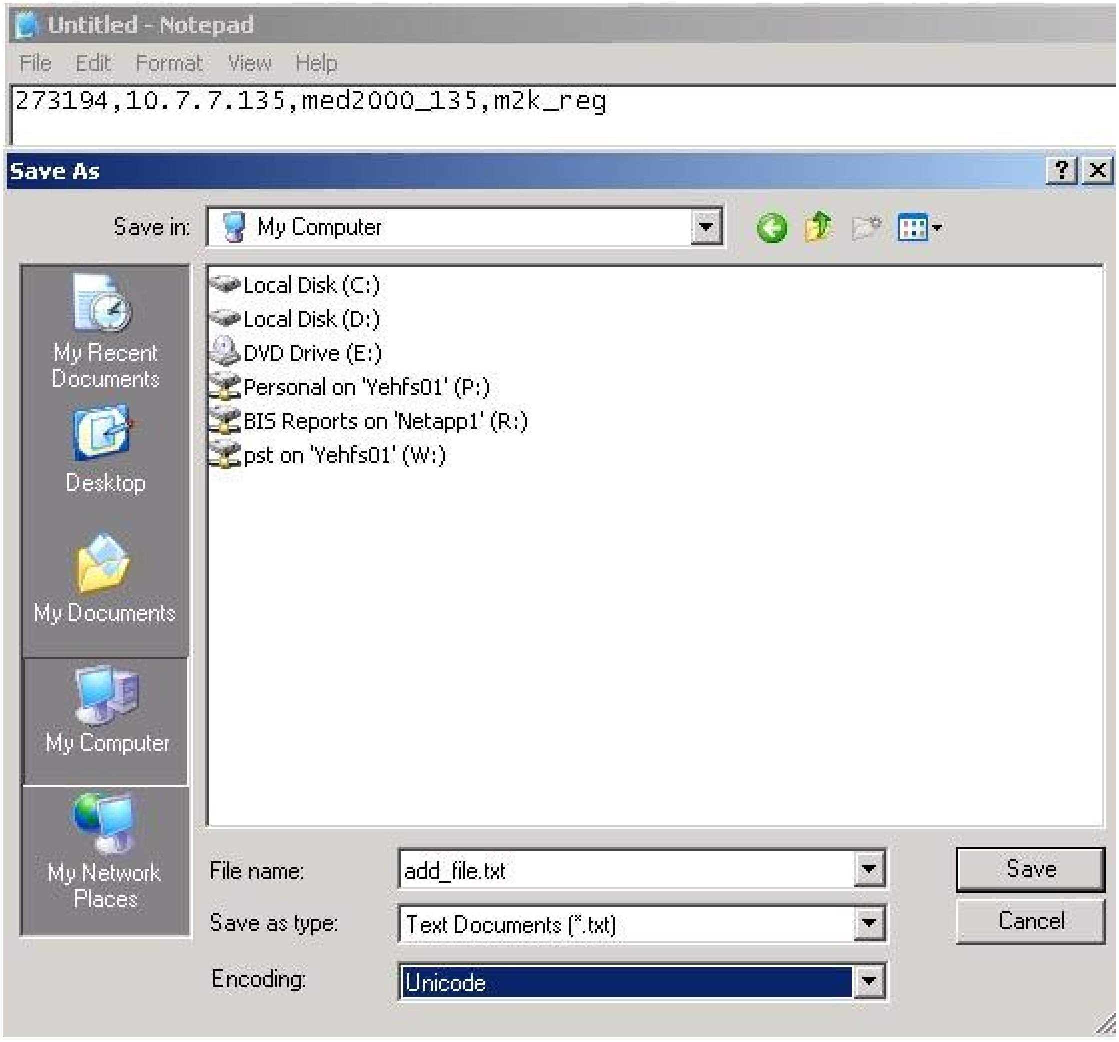
IPSec Enabled □

IKE Pre-Shared Key

2. Check the 'Enter IP address range' check box, define the 'From' and 'To' fields and click **OK**. All devices in the defined range are added to the MG Tree with name combined as 'Name Prefix' + 'IP Address'.
3. Alternately, define multiple devices by checking check box 'Enter IP address list. In the field, define the IP addresses of the multiple gateways to be added, separating the IP address from each other with a semi-colon.

4. Alternatively, define multiple devices by checking the check box 'Define Serial, IP, Name, Region from file', navigate to the prepared file and click **OK**. The figure below shows a gateway predefinition file. Each gateway must have a row in the predefinition file. If you don't know all the required information, use empty coma delimiters. The first field, Serial Number (or Mac), is optional; fields IP address, MG name and Region Name *must* be defined. The file must be saved in Unicode Encoding format before introducing it to the EMS client (refer to the example below).

Figure 6-12: Add File Unicode



```
273194,10.7.7.135,med2000_135,m2k_reg
```

Save in: My Computer

File name: add_file.txt

Save as type: Text Documents (*.txt)

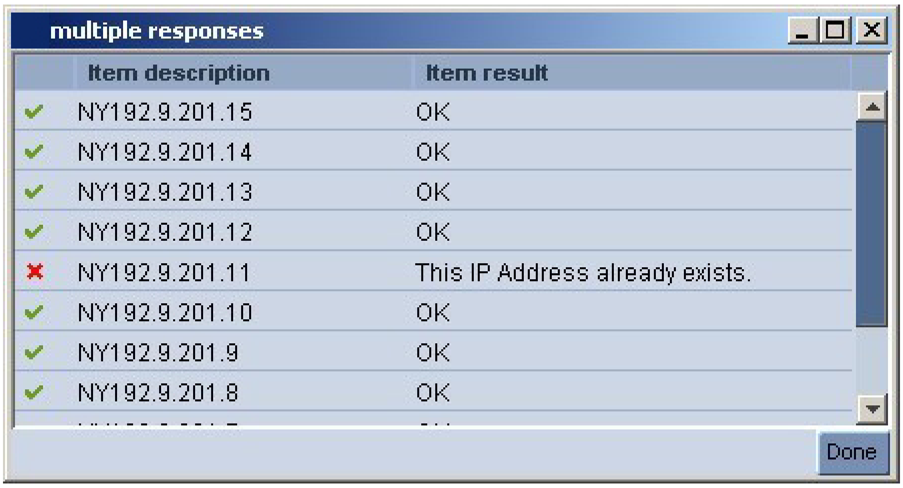
Encoding: Unicode

Note: *csv* file format enables you to define / edit the file in Excel. File previously saved from the EMS client or Server can be loaded.

5. Define the device's SNMP and IPsec related information as explained in the above Section 'Defining a Single Blade or CPE' on page 88.

6. Click **OK**; an Action Report is displayed, indicating the result of the add action for each gateway added.

Figure 6-13: Action Report for Adding Multiple Media Gateways Result



	Item description	Item result
✓	NY192.9.201.15	OK
✓	NY192.9.201.14	OK
✓	NY192.9.201.13	OK
✓	NY192.9.201.12	OK
✗	NY192.9.201.11	This IP Address already exists.
✓	NY192.9.201.10	OK
✓	NY192.9.201.9	OK
✓	NY192.9.201.8	OK

Notes:

- Gateways can be either connected or not connected to the network at the time of predefinition.
- To perform changes in the EMS and MG connectivity related to SNMP version: See Section 'Security Management' on page 333.

6.3.4.1 Gateways Connected to the Network

Verify that all gateways are successfully defined in the EMS by checking the MG Tree. If a gateway is up and running, a graphic representation of the gateway (including its LEDs), must be displayed in the Status screen.

If you encounter a pr oblem when defining your gateways, see Section 'Troubleshooting' on page 385 to resolve the issue (or contact AudioCodes).

6.3.4.2 Gateways not Connected to the Network

The EMS is capable of defining the gateway type before it is connected to the gateway for the first time. Until the first connection with the gateway is established, the EMS displays it in the MG Tree with an 'Unknown' sign ?.

If MediaPacks are NOT connected to the network, the operator can predefine the type and software version and also define first-time EMS connection behavior regarding the configuration data (see the next section for detailed information).

If you encounter problems when defining your devices, see Section 'Troubleshooting' on page 385 to resolve the issue (or contact AudioCodes).

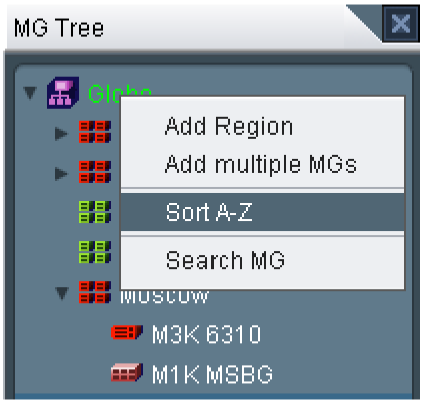
6.3.5 Sorting Regions and Gateways

The EMS supports sorting of the Regions (at the Globe level) and sorting of the gateways inside region (at Region level). Once user performs the sorting, the order of the gateways is saved for them for the next login session.

➢ **To sort regions / gateways:**

1. Right-click the Globe / Region in the MG Tree and from the sub-menu, choose the option **Sort A-Z**.

Figure 6-14: Sort Regions



6.4 First-Time Connection Problems

A gateway is indicated by ? in one of the following cases:

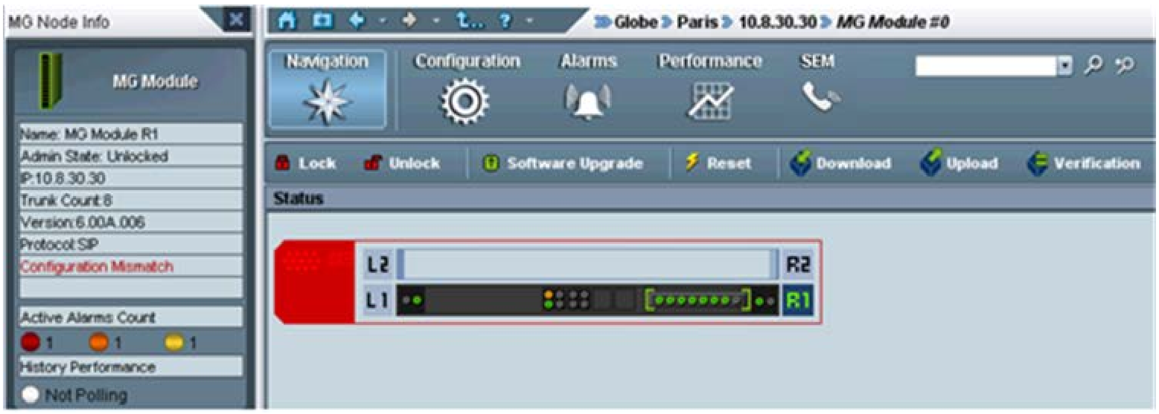
- **Unknown Hardware:** The Product Type, returned by the MIBII sysDescr value, is not recognized by the EMS. The gateway cannot be managed by the EMS.
- **Unknown Software**: The Software Version, returned by the MIBII sysDescr value, is not recognized by the EMS. Either add the specified version to the EMS Software Manager or download one of the existing software versions.

6.5 Mismatch Indications

Three types of mismatch between the database and gateway can occur. These mismatches can be detected when the device is connected for the first time, or during an automatic refresh performed by the EMS. Another important indication is Reset State (relevant for CPE products).

- **Hardware Type Mismatch:** If a hardware type mismatch occurs, the gateway is indicated by a red color in the MG Tree and a message box with a mismatch explanation is displayed instead of the status screen. Additionally, a hardware mismatch alarm is generated. This can occur when an operator defined the gateway as the 24-port gateway (for example) during the predefinition stage; however when connecting for the first time, the gateway type returned by the media gateway itself is the 8-port FXS gateway (for example). A hardware mismatch is the most severe of the three mismatch types.
- **Software Version Mismatch:** The Information pane displays information indicating a software version mismatch and a configuration mismatch alarm is generated. A software version mismatch can occur when the gateway returns a different software version to the software version that was configured by the operator. The EMS does not change the status of a gateway whose software version is mismatched.
- **Configuration Mismatch** (relevant for CPE products): The Information pane displays information indicating that the configuration in the device and the configuration saved in the database are mismatched (refer to the figure below) and a configuration mismatch alarm is generated. To solve the problem, either perform 'Configuration Download' (click the link in the Information pane; refer to the figure below) or 'Save' the actual device configuration in the EMS database (from the appropriate Parameters Provisioning screens).
- **Reset Needed** (relevant for CPE products): 'Reset Needed', displayed in the Information pane, indicates that configuration changes were loaded to the device; however, for these changes to take effect, the device must be reset. To start working with the updated configuration, perform a 'Reset' by clicking the Reset link in the Information pane (refer to the figure below).

Figure 6-15: Mediant 2000 Information pane Indicating Mismatch



MG Node Info

MG Module

Name: MG Module R1
Admin State: Unlocked
IP:10.8.30.30
Trunk Count:8
Version:6.00A.006
Protocol:SIP
Configuration Mismatch

Active Alarms Count
● 1 ● 1 ● 1
History Performance
○ Not Polling

Globe > Paris > 10.8.30.30 > MG Module #0

6.6 Moving a Gateway from Region to Region

This section describes how to move a gateway from region to region.

➢ To move a media gateway from one region to another:

1. Drag the device from its current Region and drop it into the destination region
2. Alternatively, right-click the gateway in the MG Tree and choose option **Move MG** from the pop-up menu; a list of regions pops up.
3. Select a region from the list and click **OK**; the gateway is moved.

6.7 Moving Multiple Gateways from Region to Region

The EMS supports moving multiple gateways in a single screen on condition that all devices are located in the same Region.

➢ To move multiple gateways from one region to another:

1. In the MGs Tree, right-click the Region to move from and choose option **Move Multiple MGs** from the sub-menu (refer to the figure below); the 'Multiple Move' screen is displayed (refer to the second figure below).

Figure 6-16: Moving Multiple MGs from Region to Region

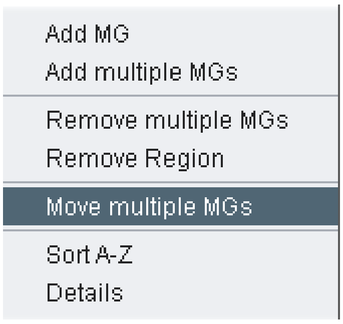
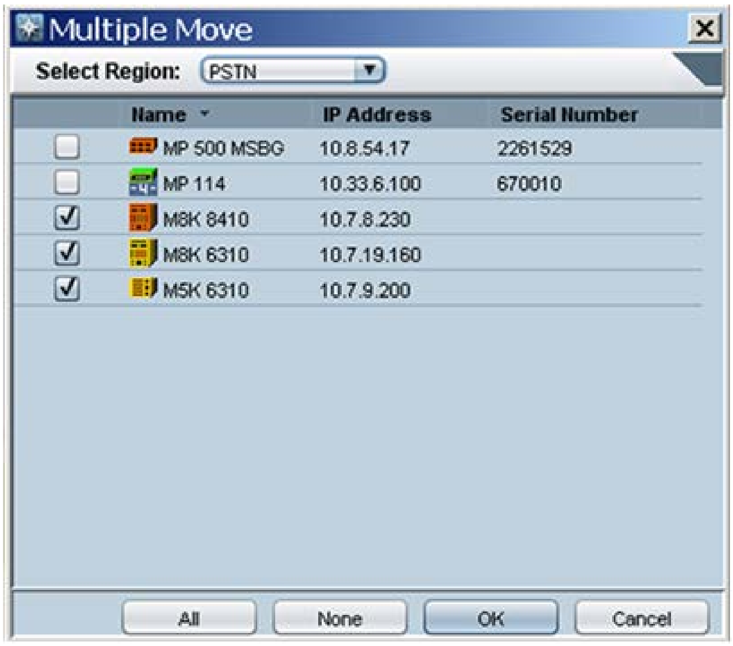


Figure 6-17: Multiple Move from Region to Region



Select Region: PSTN

	Name	IP Address	Serial Number
□	MP 500 MSBG	10.8.54.17	2261529
□	MP 114	10.33.6.100	670010
☑	M8K 8410	10.7.8.230	
☑	M8K 6310	10.7.19.160	
☑	M5K 6310	10.7.9.200	

2. In the 'Multiple Move' screen, select the gateways to move. To make your selection process quick and efficient, the screen provides you indications as to MG name, hardware type (icon), IP address and serial number.
3. From the 'Select Region' drop-down list, choose the name of the destination region to which to move the gateways.
4. Click **OK**; a Multiple Response screen opens, showing the results of the operation.

6.8 Removing a Gateway

This section describes how to remove a gateway.

➢ To remove a gateway:

- Right-click the gateway in the MG Tree and from the pop-up menu, choose option **Remove MG**; the gateway is removed.

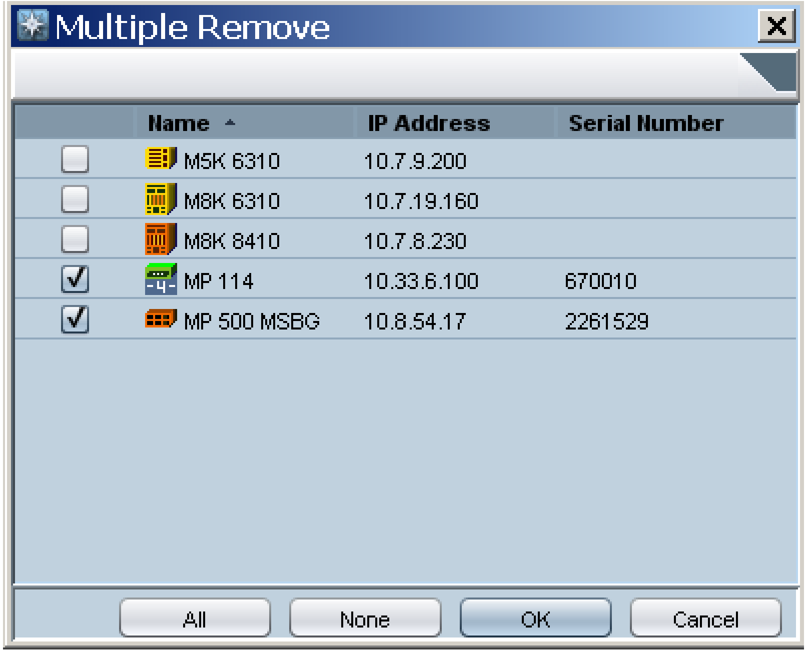
6.9 Removing Multiple Gateways

The EMS supports removing multiple gateways in a single screen (refer to the figure below), on the condition that all devices are located in the same Region. Note that the Mediant 5000 Media Gateway and the Mediant 8000 Media Gateway must be locked prior to removal.

➢ To remove multiple gateways:

1. Right-click the region in the MG Tree and choose option **Remove Multiple MGs** from the sub-menu; the 'Multiple Remove' screen is displayed:

Figure 6-18: Removing Multiple Media Gateways



Multiple Remove

	Name	IP Address	Serial Number
□	M5K 6310	10.7.9.200	
□	M8K 6310	10.7.19.160	
□	M8K 8410	10.7.8.230	
☑	MP 114	10.33.6.100	670010
☑	MP 500 MSBG	10.8.54.17	2261529

2. Check the check boxes adjacent to the IP addresses of the media gateways to be removed. To remove all media gateways listed, check all check boxes by clicking the **All** button, and click **OK**; an Action Report is displayed, indicating the result of the remove action for each gateway removed.

6.10 Searching for a Gateway

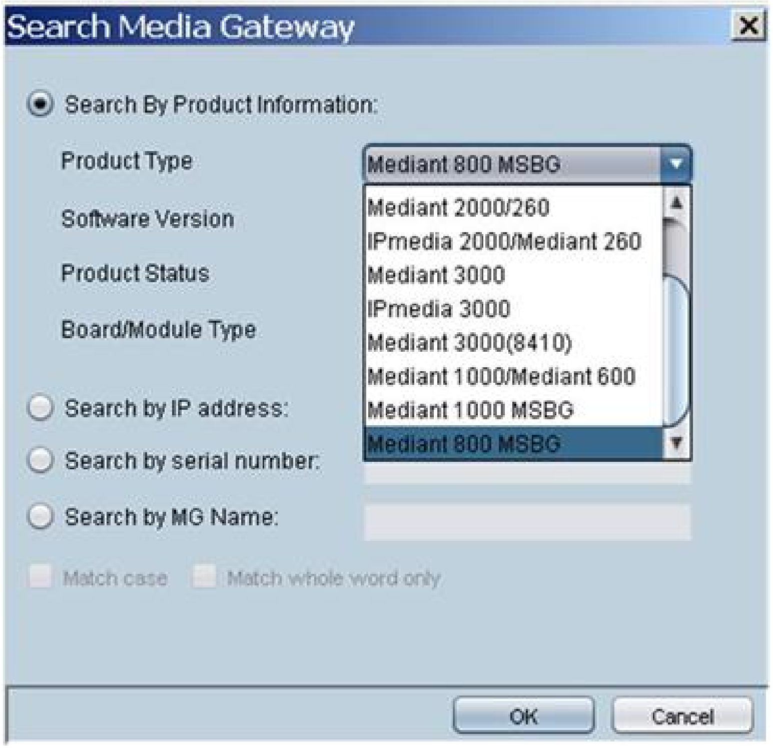
This section describes how to search for a media gateway.

➢ **To search for a media gateway:**

1. Open the Media Gateway dialog box and do one of the following:
   - In the MG Tree, right-click 'Globe' and select **Search MG**.

     -OR-
   - In the Tools menu, choose option **Search MG**); the 'Search MGs' screen is displayed (refer to the figure below).

Figure 6-19: Search MGs



Search Media Gateway

● Search By Product Information:

Product Type: Mediant 800 MSBG

Software Version

Product Status

Board/Module Type

○ Search by IP address:

○ Search by serial number:

○ Search by MG Name:

□ Match case □ Match whole word only

2. Search by Product Information: Enter the following media gateway information:
   a. **Product Type** - choose a product group
   b. **Software Version** - choose from the list of supported versions for the products you selected. You can choose to search for all versions.
   c. **Product Status** – choose from the list of gateway status options. You can choose to search for all options.
   d. **Module Type** – for Mediant 5000 / 8000 products, the user can search for TP1610, TP6310 or TP8410 boards, for modular devices, the user can search for Digital, Analog, BRI or IPmedia modules.
3. Click **OK**; if one media gateway is located, it is selected in the MG Tree and its Status screen is opened. If more than one appropriate media gateway is located, the Search Result screen is displayed.

4. **Search by IP Address**: Enter the media gateway's IP address and click **OK**; if the media gateway is located, it is selected in the MG Tree and its Status screen is opened.
5. **Search by Serial Number**: Enter the media gateway's Serial Number and click **OK**; if the media gateway is located, it is selected in the MG Tree and its Status screen is opened.
6. **Search by MG Name**: Enter the name of the media gateway you're trying to locate and click **OK**; if more than one appropriate media gateway is located, the Search Result screen is displayed.
7. In the Search Result screen, locate the media gateway in the list and double-click it; the media gateway is selected in the MG Tree and its Status screen is opened.

Note: You can enhance your search for a media gateway (especially when searching by name) by checking the 'Match case' and/or 'Match whole word only' check boxes.

When only the **Match Case** check box is selected, the EMS performs a search based on the case (upper/lower) of the letters entered by operators in the field 'Search by MG Name'.

When the '**Match whole word only** check box is selected, the EMS performs a search based only on the text entered by operators in the field 'Search by MG Name', *irrespective of upper and/or lower case*.

When both 'Match Case' and 'Match whole word only' are selected, the EMS performs a search based on the text that the operator entered in the field 'Search by MG Name' as well as on the letter case.

6.11 Saving the EMS Tree MGs Report in an External File

The MGs Report CSV file includes configuration and status data of all gateways that are defined on the EMS Server.

Note: In addition to the MGs Report file, a Topology file can also be generated, The Topology file is a user friendly snapshot of the MGs Report file and is automatically updated upon the addition /removal of a media gateway or upon updates to the media gateway properties such as name, IP address or region modification. For more information, refer to the *OAMP Integration Guide*.

➢ To save the MGs Report file:

1. In the Main menu, choose **File** > **MGs Report** action.
2. In the File Chooser, navigate to the desired location, select the file name and click **OK**.

The File is stored in the CSV format in the required location and includes the following field columns:

- Serial Number – relevant for CPE products (not relevant for the Mediant 5000 / 8000 Gateways).
- IP Address
- Node Name
- Region Name
- Description
- Product Type
- Software Version
- Connection Status – Connected / Not Connected – represent the ability of EMS application to communicate with MG
- Administrative State – Locked / Unlocked / Shutting Down
- Operational State – Enabled / Disabled
- Mismatch State – No Mismatch / SW Version Unsupported / SW Mismatch / HW Mismatch

- Last Change Time
- Performance Polling Status – Polling / Not Polling
- Performance Profile
- Protocol Type – MGCP / MEGACO / SIP – relevant for CPE devices. Not relevant for Mediant 5000 / 8000 Gateways.
- Master Profile

Note: The MGs Report file can be used as the input file to the EMS application during the 'Add Multiple MGs' command.

Reader's Notes

Part II

Status Monitoring and Navigation Concepts

This section describes the various status monitoring and navigation concepts.

7 Monitoring Multiple Media Gateways

This section describes how to monitor different media gateways. This section describes the read-only Status panes, enabling operators to monitor the media gateway and its components. After a status view is selected, it's automatically updated (refreshed) every 20 seconds.

Following are the EMS status components:

- 'Regions List' on page 105
- 'MGs List' on page 106

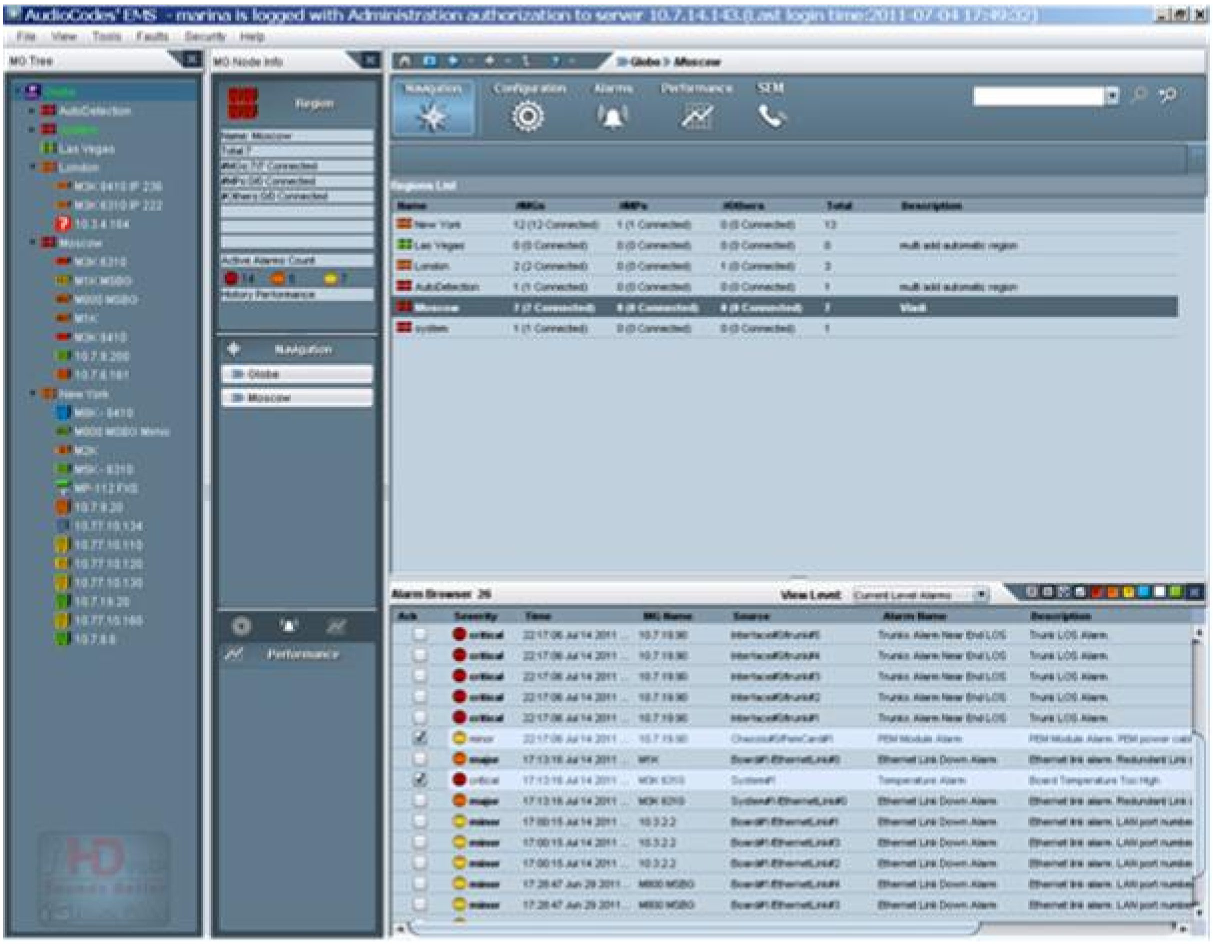
7.1 Regions List

This section describes the regions list.

➢ To access the Regions List:

- Click the root in the MG Tree (Globe); the Main Screen displays the Regions List pane, in which all defined regions are listed.

Figure 7-1: Regions List



AudioCodes' EMS - marina is logged with Administration authorization to server 10.7.14.143 (Last login time:2011-07-04 17:49:32)
File View Tools Faults Security Help
MG Tree
MG Node Info
Globe > Moscow
Navigation
Configuration
Alarms
Performance
SEM
Region
Navigation
Globe
Moscow
Performance

Regions List

Name	#MGs	#MPs	#Others	Total	Description
New York	12 (12 Connected)	1 (1 Connected)	0 (0 Connected)	13	
Las Vegas	0 (0 Connected)	0 (0 Connected)	0 (0 Connected)	0	mult add automatic region
London	2 (2 Connected)	0 (0 Connected)	1 (0 Connected)	3	
AutoDetection	1 (1 Connected)	0 (0 Connected)	0 (0 Connected)	1	mult add automatic region
Moscow	7 (7 Connected)	0 (0 Connected)	0 (0 Connected)	7	Vladi
system	1 (1 Connected)	0 (0 Connected)	0 (0 Connected)	1	

Alarm Browser 26 View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	critical	22:17:06 Jul 14 2011 ...	10.7.19.90	Interface#0/trunk#5	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	critical	22:17:06 Jul 14 2011 ...	10.7.19.90	Interface#0/trunk#4	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	critical	22:17:06 Jul 14 2011 ...	10.7.19.90	Interface#0/trunk#3	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	critical	22:17:06 Jul 14 2011 ...	10.7.19.90	Interface#0/trunk#2	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	critical	22:17:06 Jul 14 2011 ...	10.7.19.90	Interface#0/trunk#1	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☑	minor	22:17:06 Jul 14 2011 ...	10.7.19.90	Chassis#0/PemCard#1	PEM Module Alarm	PEM Module Alarm. PEM power cab
□	major	17:13:16 Jul 14 2011 ...	MTK	Board#1/EthernetLink#0	Ethernet Link Down Alarm	Ethernet link alarm. Redundant Link i
☑	critical	17:13:16 Jul 14 2011 ...	MGK 6310	System#1	Temperature Alarm	Board Temperature Too High
□	major	17:13:16 Jul 14 2011 ...	MGK 6310	System#1/EthernetLink#0	Ethernet Link Down Alarm	Ethernet link alarm. Redundant Link i
□	minor	17:00:15 Jul 14 2011 ...	10.3.2.2	Board#1/EthernetLink#1	Ethernet Link Down Alarm	Ethernet link alarm. LAN port numbe
□	minor	17:00:15 Jul 14 2011 ...	10.3.2.2	Board#1/EthernetLink#3	Ethernet Link Down Alarm	Ethernet link alarm. LAN port numbe
□	minor	17:00:15 Jul 14 2011 ...	10.3.2.2	Board#1/EthernetLink#2	Ethernet Link Down Alarm	Ethernet link alarm. LAN port numbe
□	minor	17:28:47 Jun 29 2011 ...	M800 MSBG	Board#1/EthernetLink#4	Ethernet Link Down Alarm	Ethernet link alarm. LAN port numbe
□	minor	17:28:47 Jun 29 2011 ...	M800 MSBG	Board#1/EthernetLink#3	Ethernet Link Down Alarm	Ethernet link alarm. LAN port numbe

The figure above displays the Regions List pane in the Main Screen. The Regions List pane lists and summarizes all regions and media gateways managed by the EMS.

For each region listed in the Regions List pane, the following information is displayed:

- Region name
- Number of digital gateways in the region (#MGs)
- Number of analog gateways in the region (#MPs)
- Number of Other (Unknown) gateways in the region
- Total Number of gateways in the region (digital and analog)
- Description

Each recognized gateway is given a Clear (**OK**) status; the EMS was able to connect to it and no hardware mismatch was found.

An unknown gateway is given a Clear (**OK)** status if the EMS has not connected to it yet and it has no mismatch.

The Region Status is defined according to the highest Gateway severity in each region. For example, when in a specific region there is a single Gateway with a major severity and several gateways with hundreds of clear severities, then this region is indicated with a major severity.

- Double-clicking on a region in the Regions List pane displays the MGs List for the gateways defined under that region (refer to the figure above); click the **Up** button in the MGs List pane to navigate up the hierarchy, back to the region level.

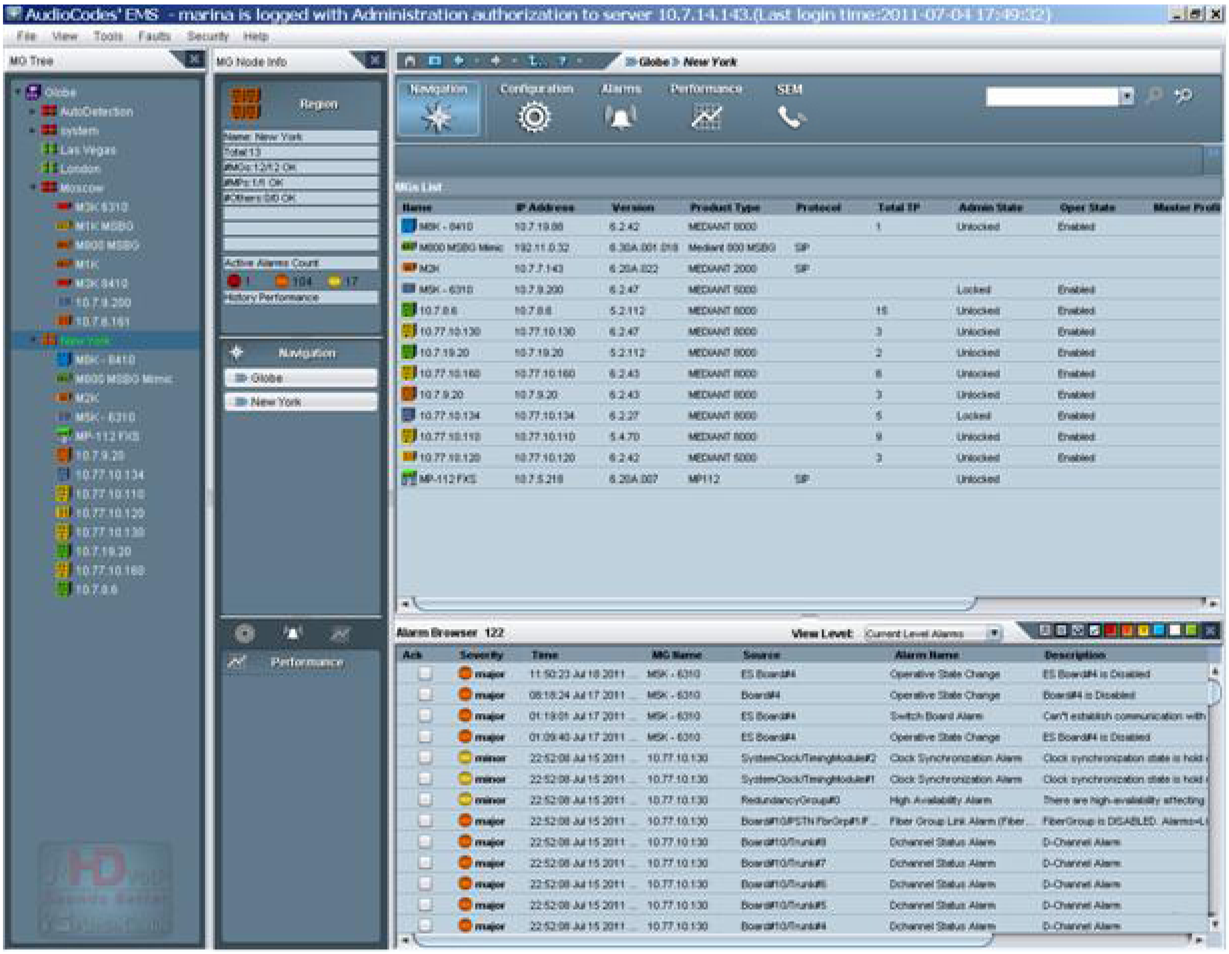
7.2 MGs List

This section describes the MGs list.

➢ To access the MGs List:

1. Click a region in the MG Tree; the MGs List pane is displayed in the Status pane of the main screen, listing all the gateways located under this region.
2. **Mediant 5000 Media Gateway and Mediant 8000 Media Gateway**: Click **Lock** or **Unlock** in the Actions bar.
3. **CPE and Blades**: Right-click the device to perform Software Download, Configuration Verification, Configuration Download, Network Configuration or Reset. Each of these actions can also be performed on a set of devices selected from the MGs List.
4. Double-click a device in the MGs List; the Main Screen displays the Status pane.
5. Click the **Up** button on the gateway level screens to return to the MGs List in the Main Screen.

Figure 7-2: MGs List



Name: New York
Total 13
#MGs:12/12 OK
#MPs:1/1 OK
#Others 0/0 OK
Active Alarms Count
1 104 17
History Performance

MGs List

Name	IP Address	Version	Product Type	Protocol	Total TP	Admin State	Oper State	Master Profi
MSK - 8410	10.7.19.88	6.2.42	MEDIANT 8000		1	Unlocked	Enabled	
M800 MSBG Mimic	192.11.0.32	6.30A.001.018	Mediant 800 MSBG	SIP				
M2K	10.7.7.143	6.20A.022	MEDIANT 2000	SIP				
MSK - 6310	10.7.9.200	6.2.47	MEDIANT 5000			Locked	Enabled	
10.7.8.6	10.7.8.6	5.2.112	MEDIANT 8000		15	Unlocked	Enabled	
10.77.10.130	10.77.10.130	6.2.47	MEDIANT 8000		3	Unlocked	Enabled	
10.7.19.20	10.7.19.20	5.2.112	MEDIANT 8000		2	Unlocked	Enabled	
10.77.10.160	10.77.10.160	6.2.43	MEDIANT 8000		6	Unlocked	Enabled	
10.7.9.20	10.7.9.20	6.2.43	MEDIANT 8000		3	Unlocked	Enabled	
10.77.10.134	10.77.10.134	6.2.27	MEDIANT 8000		5	Locked	Enabled	
10.77.10.110	10.77.10.110	5.4.70	MEDIANT 8000		9	Unlocked	Enabled	
10.77.10.120	10.77.10.120	6.2.42	MEDIANT 5000		3	Unlocked	Enabled	
MP-112 FXS	10.7.5.218	6.20A.007	MP112	SIP		Unlocked		

Alarm Browser 122 View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	major	11:50:23 Jul 18 2011 ...	MSK - 6310	ES Board#4	Operative State Change	ES Board#4 is Disabled
□	major	08:18:24 Jul 17 2011 ...	MSK - 6310	Board#4	Operative State Change	Board#4 is Disabled
□	major	01:19:01 Jul 17 2011 ...	MSK - 6310	ES Board#4	Switch Board Alarm	Can't establish communication with
□	major	01:09:40 Jul 17 2011 ...	MSK - 6310	ES Board#4	Operative State Change	ES Board#4 is Disabled
□	minor	22:52:08 Jul 15 2011 ...	10.77.10.130	SystemClock/TimingModule#2	Clock Synchronization Alarm	Clock synchronization state is hold
□	minor	22:52:08 Jul 15 2011 ...	10.77.10.130	SystemClock/TimingModule#1	Clock Synchronization Alarm	Clock synchronization state is hold
□	minor	22:52:08 Jul 15 2011 ...	10.77.10.130	RedundancyGroup#0	High Availability Alarm	There are high-availability affecting
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/PSTN FbrGrp#1/F...	Fiber Group Link Alarm (Fiber...	FiberGroup is DISABLED. Alarms=L
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/Trunk#8	Dchannel Status Alarm	D-Channel Alarm
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/Trunk#7	Dchannel Status Alarm	D-Channel Alarm
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/Trunk#6	Dchannel Status Alarm	D-Channel Alarm
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/Trunk#5	Dchannel Status Alarm	D-Channel Alarm
□	major	22:52:08 Jul 15 2011 ...	10.77.10.130	Board#10/Trunk#4	Dchannel Status Alarm	D-Channel Alarm

The above figure displays the MGs List in the Status pane. The MGs List lists and summarizes all gateways located in the selected region. For each gateway, the following information is displayed:

- Gateway name & status (status is indicated by the color coding)
- Gateway IP address
- SW Version
- Product Type
- Protocol (MGCP, MEGACO, SIP or None) - relevant to CPE products.
- Total TP - Total number of TP boards in the chassis (the accumulative number of active and redundant boards) - relevant to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway.
- Administrative State (Shut Down/Locked/Unlocked) - relevant to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway
- Operational State (Enabled/Disabled) - relevant to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway

- PM Profile. Indicates the name of the PM (Performance Monitoring) profile when a profile is attached to the device.
- PM Polling status (Polling / Not Polling). When the status is 'Polling', background PM data is collected from the device and stored in the EMS database according to parameters (duration, etc.) defined by the PM profile. When the status is 'Not Polling', no PM data is polled.
- Alarms associated with selected gateway/s in the MGs List.

7.3 Globe and Region – Graphical Summary View

➢ To view Globe and Region Graphical status summary:

- Click **Performance** icon and navigate to the Performance Monitoring Desktop. The graphical auto-refreshable summary screen is displayed. It consists of the following panes:
  - The upper pane summarizes the gateway severities as follows:
    - **Globe Level** - Alarm severity and connection status of all devices managed by the EMS server, categorized according to regions (each region is represented by a bar chart that is divided according to alarm severity and connection statuses).
    - **Region Level** - Alarm severity and connection status of all devices loaded to a specific region categorized according to the device product (each device product is represented by a bar chart that is divided according to alarm severity and connection statuses).

      In addition to the devices alarm severity, the device status is represented with the following states: Locked, Not Connected and Mismatch State.

      When devices cannot be categorized into one of the above states, they are collectively represented as a separate bar graph with the label 'Unknown'.
  - The lower pane consists of the following tabs:
    - Redundancy status of the TP boards (TP Boards tab): Distribution between the Active and Redundant boards for all the devices in the corresponding level (globe or region). This view consists of three pie charts; one each for the TP-1610, TP 6310 and TP-8410 boards respectively (in the Mediant 2000, 3000, Mediant 5000 or Mediant 8000 chassis). The TP boards are categorized according to one of the following protection types: Not Protected, Hot, Warm, and Redundant.
    - Interface types of the CPE devices (CPEs tab): Distribution of modules for the Mediant 600, Mediant 800, Mediant 800 MSBR, Mediant 1000 and Mediant 1000 MSBR 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.

The four example views are displayed below:

- Globe level – TPs
- Globe level – CPEs
- Region Level – TPs
- Region Level – CPEs

Figure 7-3: Globe Level - TPs

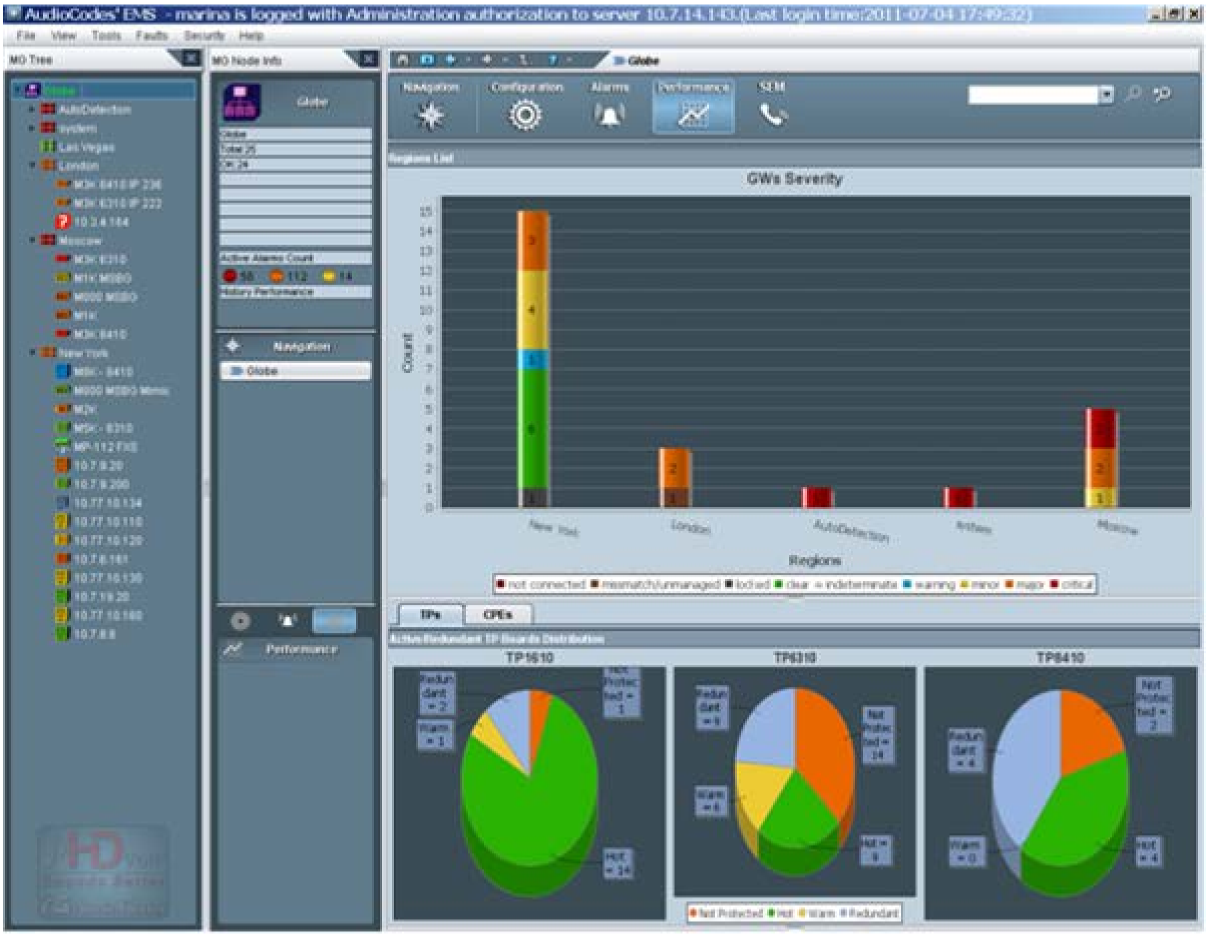


Figure 7-4: Globe Level – CPEs

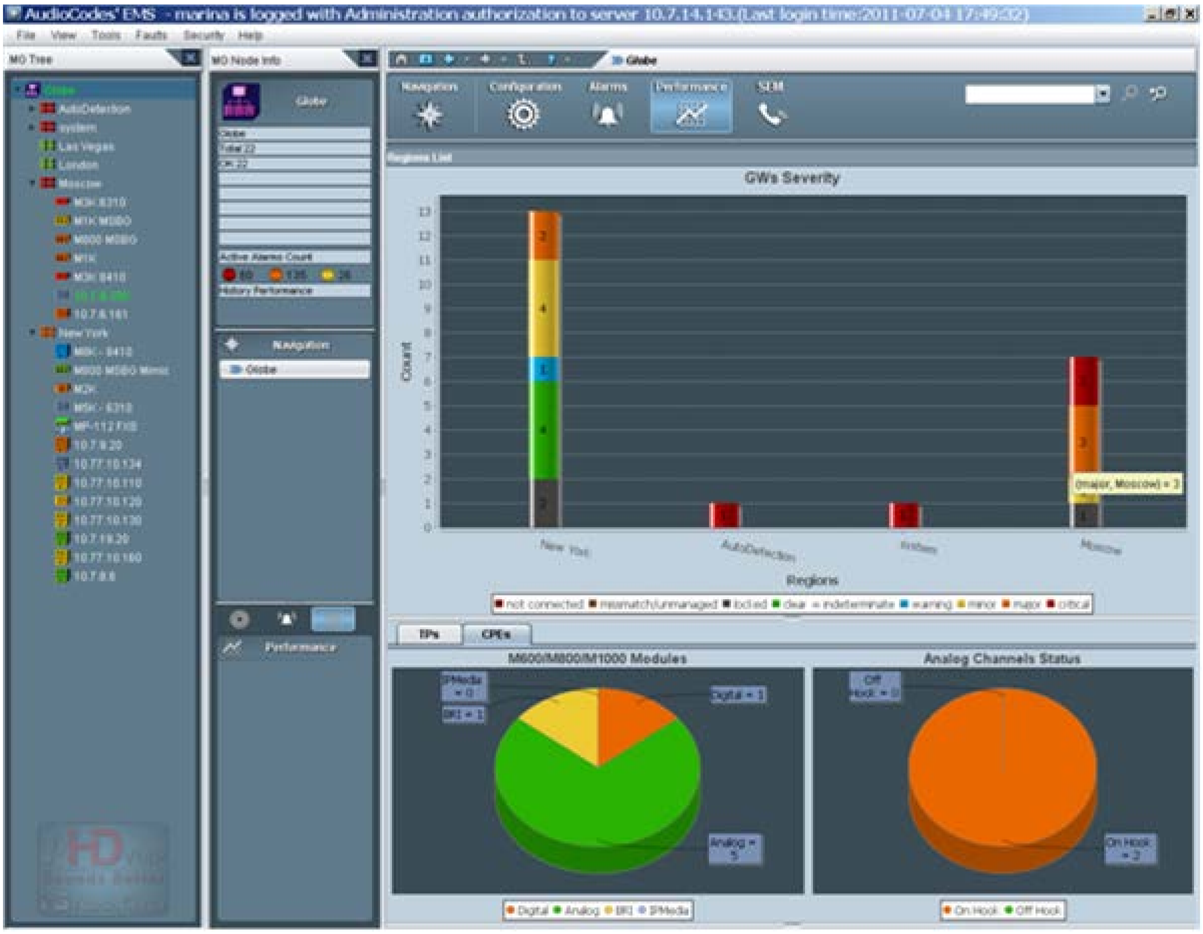


Figure 7-5: Region Level – TPs

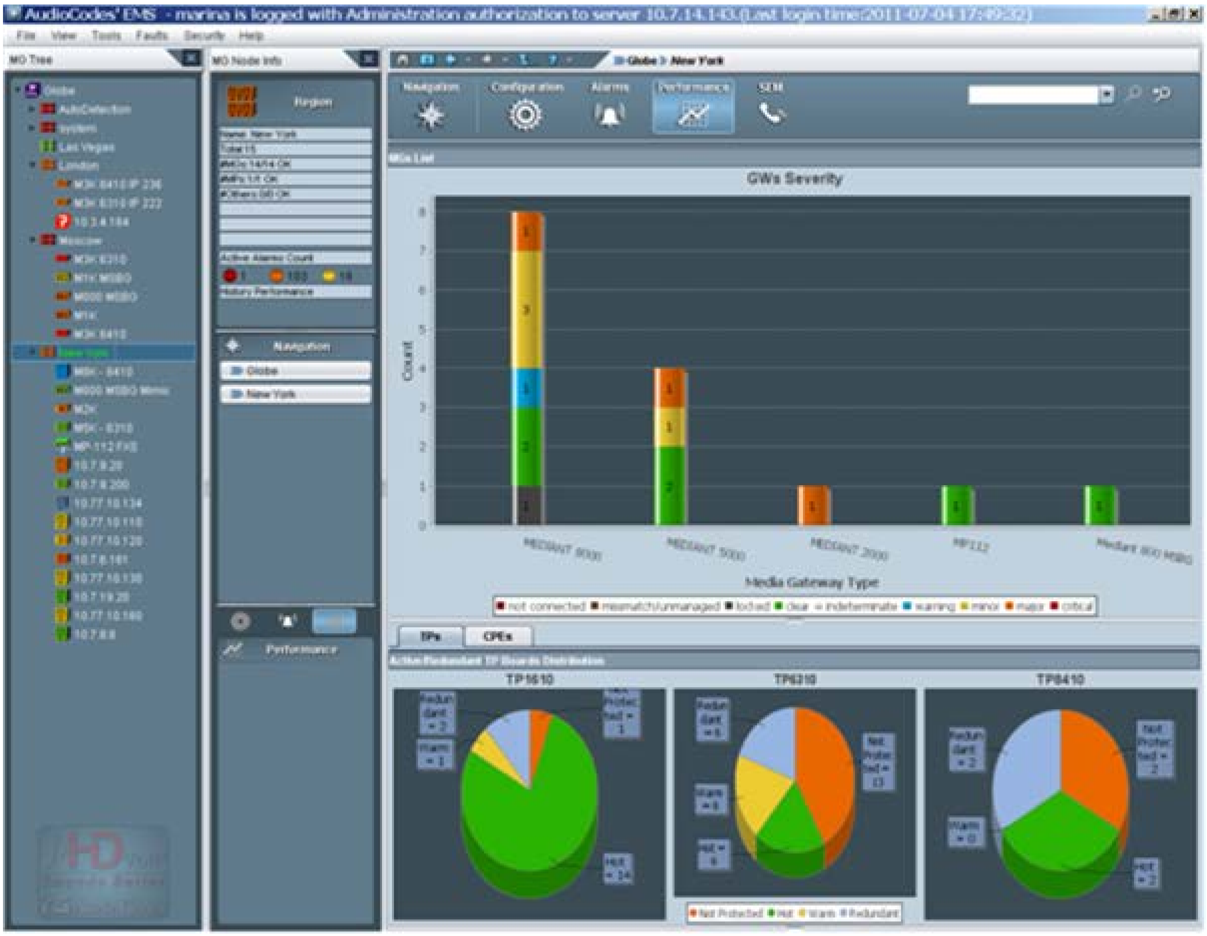
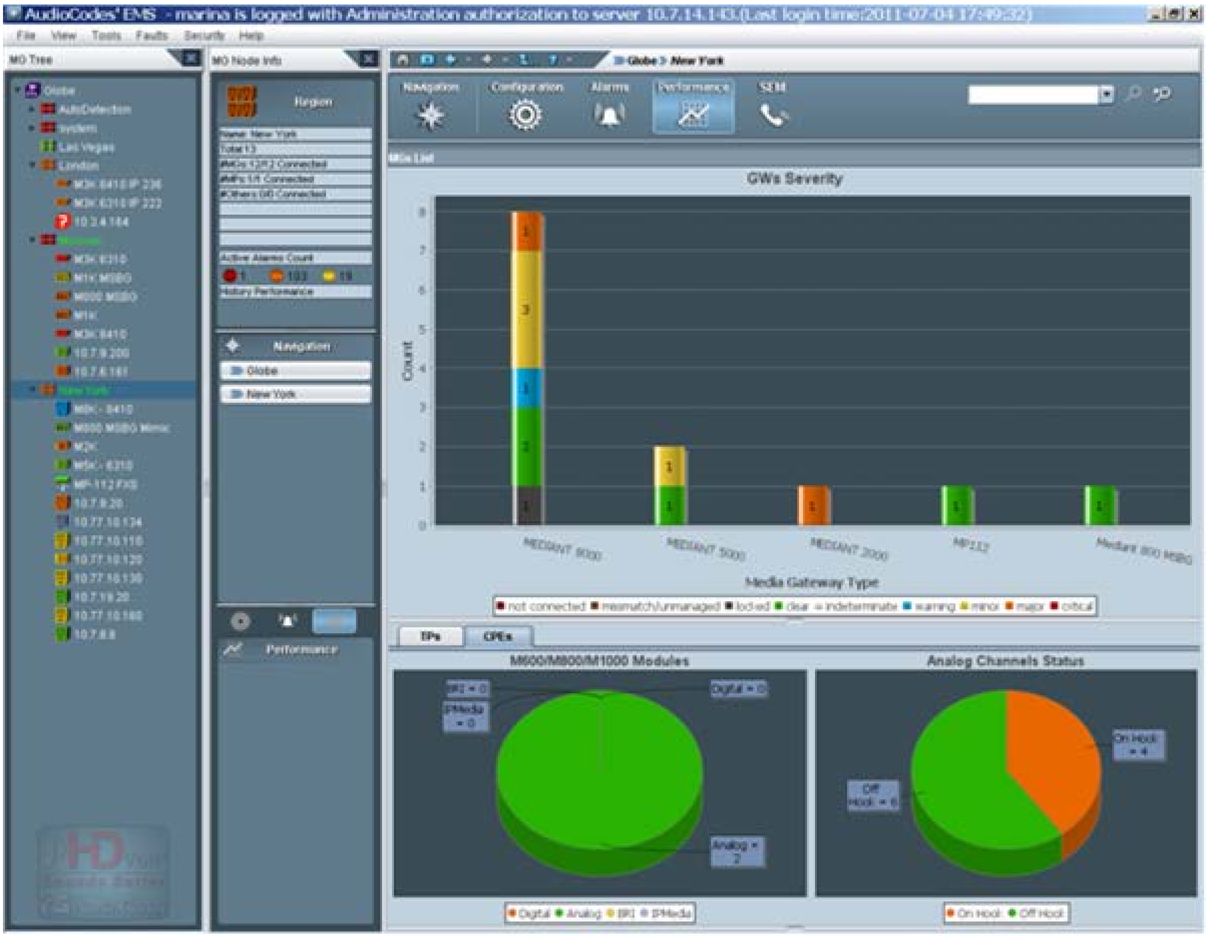


Figure 7-6: Region Level – CPEs



7.4 Media Gateway Level Status Pane

This section describes how to access the media gateway level status pane.

➢ To access a media gateway:

1. Do one of the following:
   - In the MG Tree, expand the region under which the media gateway is located and click the media gateway; a message appears indicating “Contacting Server. Please Wait;” a graphic representation of the MG is then displayed (refer to the figures below).

     -OR-
   - In the MGs List, double-click a media gateway; a message appears indicating “Contacting Server. Please Wait;” a graphic representation of the media gateway is then displayed (refer to the figures below).
2. Click the **Up** button in the board-level screens to navigate back up a level.

Reader's Notes

8 Mediant 5000 and Mediant 8000 Media Gateways

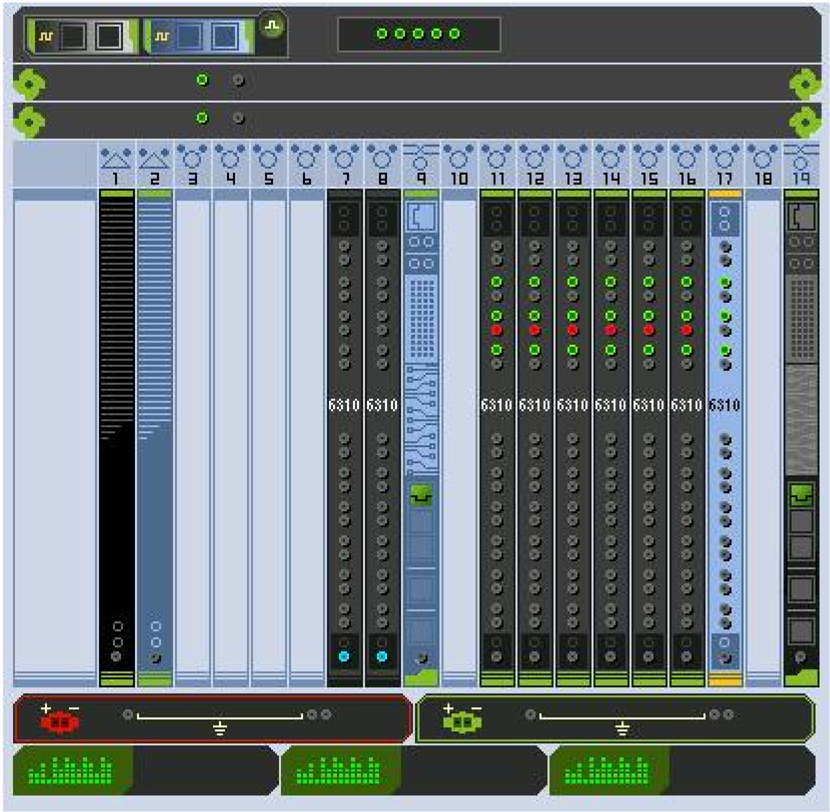
This section describes the elements of the Mediant 5000 Media Gateways, Mediant 8000 Media Gateways status panes.

8.1 Mediant 8000 Status Pane

The Status pane displayed in the main screen indicates the overall gateway status, as well as additional Info Panel information: Name, Administrative State (Shut Down/Locked/Unlocked), Operational State (Enabled/Disabled), gateway IP address and gateway software version.

The following VoIP boards populate the Mediant 8000 / TP-6310 and TP-8410.

Figure 8-1: Mediant 8000 Media Gateway 6310 Configuration Status Screen



Note: In the Mediant 8000, slots 3-8 and 10-18 inclusively are reserved for TP boards, slots 1-2 are reserved for the SC (System Controller) Boards, and slots 9 and 19 are reserved for the Ethernet Switch boards.

Statuses for the Mediant 8000 include the following:

- SAT card status :
  - Each SAT card is represented by a bar located in the MG Status screen near the corresponding SC board (refer to the figures above). The background of the SAT card represents SAT activity (black for active; pale blue for redundant). The overall status of the SAT card is represented by its border color (Gray = Locked; Red = Disabled; Green = Enabled; Orange = Major Severity).
  - The status of the Timing Module and External Interfaces is represented by corresponding icons in the SAT card status bar. Their color conventions are described below. Tooltips present users with relevant additional information.
  - The SAT card has the following color convention:

Table 8-1: SAT Card Status Color Convention

Color	Convention
Green	The SAT Card is locked to one of the external interfaces.
Blue	The SAT Card is in Hold Over state.
Yellow	The SAT Card is in Free Run state.
Red	SAT Card Error.

- The Timing module :
  - The Timing module summarizes the status of the clock reference source and the SAT card. The status of the Timing module is *Red*=Failed or *Green*=OK.
  - When you click this icon, the System Clock Parameters Provisioning screen for the current timing mode is displayed.
  - When you click this icon, the System Clock Parameters Provisioning screen for the current timing mode is displayed.
  - In the Standalone mode, the icon must be green.
  - For more information on the PSTN System Clock synchronization modes, navigate to the System Clock tab.

Note: When you navigate to the System Clock window, only events and alarms relevant to the System Clock are displayed in the Alarms Browser.

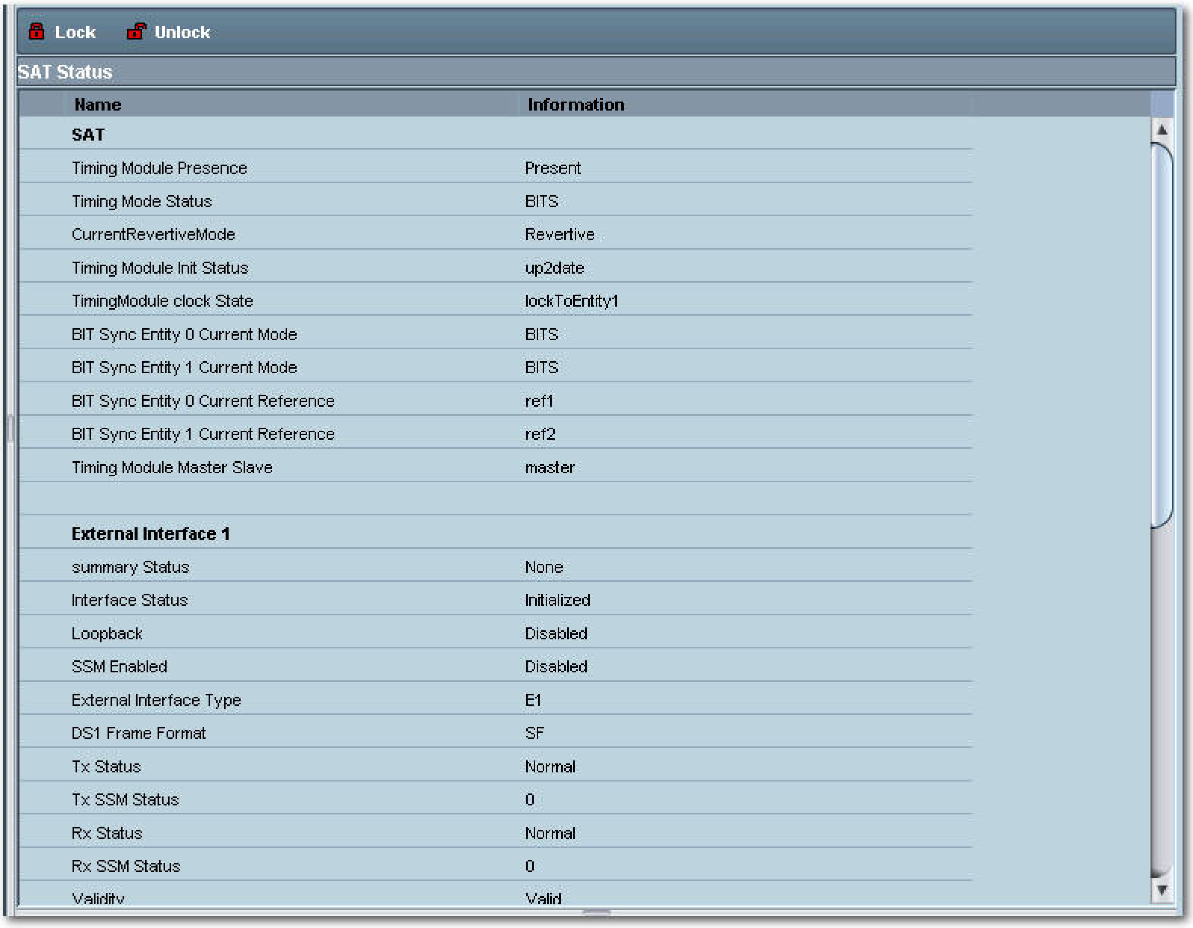
- External Interfaces have following color conventions:

Table 8-2: External Interface Color Convention

Color	Convention
Green with border	OK status and currently selected as the Clock source (as in the example).
Green	OK status.
Red	Failed (alarm) status.
Grey	Status Unknown.

- When a SAT card does not have a Timing Module, the status icon of the Timing Module is not displayed and External Interfaces are displayed as grey placeholders .
- To view additional information on the status of the Timing Module and External Interfaces, double-click the SAT bar; the screen shown below is displayed.

Figure 8-2: SAT Properties screen



SAT Status

Name	Information
SAT	
Timing Module Presence	Present
Timing Mode Status	BITS
CurrentRevertiveMode	Revertive
Timing Module Init Status	up2date
TimingModule clock State	lockToEntity1
BIT Sync Entity 0 Current Mode	BITS
BIT Sync Entity 1 Current Mode	BITS
BIT Sync Entity 0 Current Reference	ref1
BIT Sync Entity 1 Current Reference	ref2
Timing Module Master Slave	master
External Interface 1	
summary Status	None
Interface Status	Initialized
Loopback	Disabled
SSM Enabled	Disabled
External Interface Type	E1
DS1 Frame Format	SF
Tx Status	Normal
Tx SSM Status	0
Rx Status	Normal
Rx SSM Status	0
Validity	Valid

- Shelf LEDs :

  Five LEDs summarize the gateway's status (from top to bottom):

  - System: Red = System Error occurred; Green = OK
  - Critical: Red = Critical Error occurred; Green = OK
  - Major: Orange = Major Error occurred; Green = OK
  - Minor: Yellow = Minor Error occurred; Green = OK
  - Shelf: Red = Critical Error occurred; Orange = Major Error occurred; Green = OK; Gray = Off

- Fan status (in the Mediant 8000) :

  - Color convention: Red = Failed; Green = OK; Orange = Major Severity

- Fan status (in the Mediant 8000 6310)

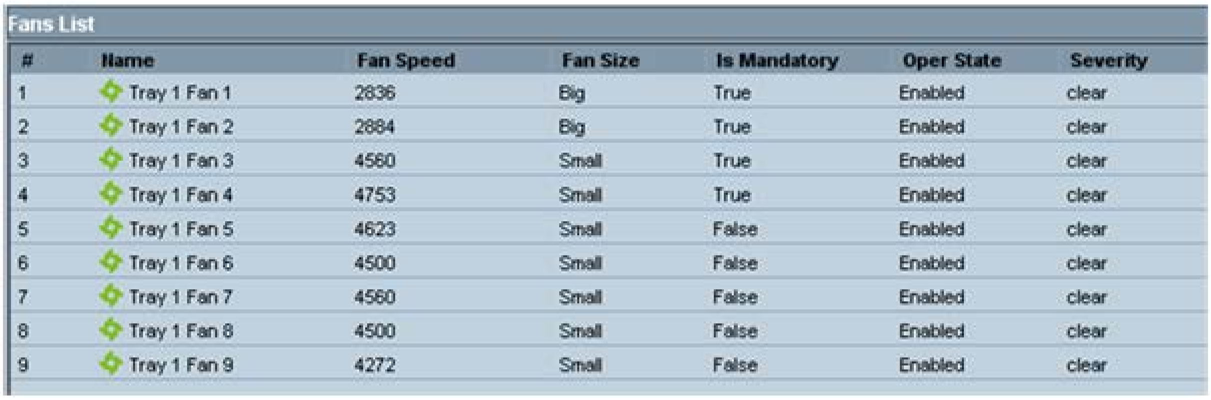
  Fans' two rows are read as follows:

  - Top Row: Upper Fan Tray
  - Bottom Row: Bottom Fan Tray
  - Double-click each fan tray to view fan status

  Color convention: Red = Failed; Green = OK

To view additional information on the status of the fans, double-click the Fan icon. The following status screen is displayed:

Figure 8-3: Mediant 8000 Fans List Information



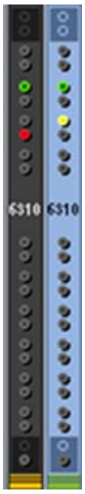
Fans List

#	Name	Fan Speed	Fan Size	Is Mandatory	Oper State	Severity
1	Tray 1 Fan 1	2836	Big	True	Enabled	clear
2	Tray 1 Fan 2	2884	Big	True	Enabled	clear
3	Tray 1 Fan 3	4560	Small	True	Enabled	clear
4	Tray 1 Fan 4	4753	Small	True	Enabled	clear
5	Tray 1 Fan 5	4623	Small	False	Enabled	clear
6	Tray 1 Fan 6	4500	Small	False	Enabled	clear
7	Tray 1 Fan 7	4560	Small	False	Enabled	clear
8	Tray 1 Fan 8	4500	Small	False	Enabled	clear
9	Tray 1 Fan 9	4272	Small	False	Enabled	clear

- VOP Boards status:

  The figures below display board status:

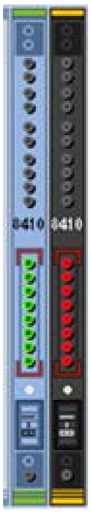
Figure 8-4: 6310 Board-Active and Redundant Status



- Background color: Dark Gray = Active board; Blue = Redundant board
- Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity, Yellow = Minor Severity, Blue = Warning Severity, White = Indeterminate Severity

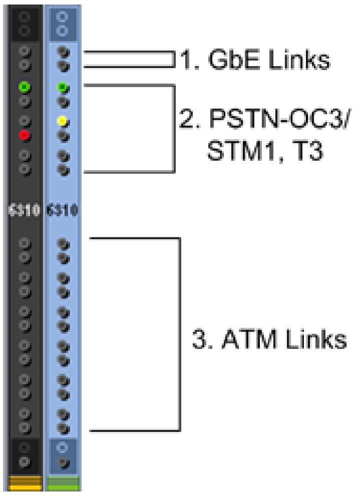
- TP Switchover: The active TP board, after switchover, is marked in a background black color without any LEDs, with a red or green frame around the board according to its Operational State (green = enabled boards, red = disabled boards). A redundant TP board, which becomes active after switchover, is marked in a background blue color, with LEDs for activated trunks.

Figure 8-5: 8410 Board-Active and Redundant Status



- Trunk (E1/T1) LED color convention: Red = Disabled; Green = Enabled; Gray = Locked

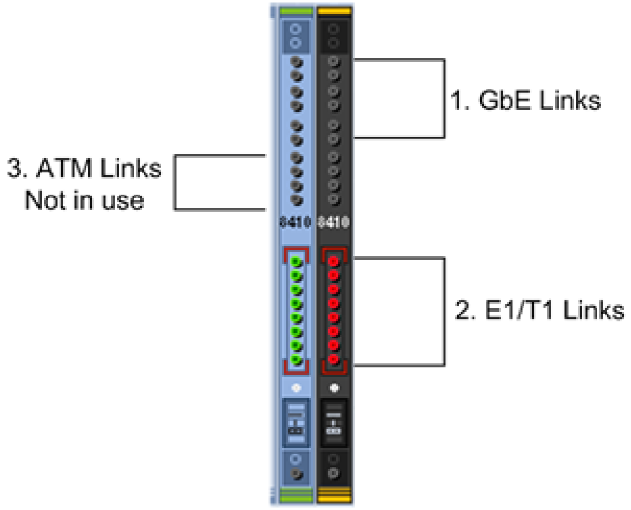
Figure 8-6: 6310-LED Status



Legend

- ♦ 1 = the first two LEDs represent the GbE (Gigabit Ethernet) status
- ♦ 2 = six LEDs representing PSTN Interface status (for OC3/STM1, four LEDs are relevant; for T3, all six LEDs are relevant)
- ♦ 3 = twelve LEDs representing ATM Interface status (not in use)

Figure 8-7: 8410-LED Status



Legend

- 1 = six LEDs representing the GbE (Gigabit Ethernet) status
- 2 = four LEDs representing ATM LEDs (not in use)
- 3 = eight LEDs representing E1/T1 LEDs

- ES Boards and Ports status:

  The figures below displays an ES Board Status screen

Figure 8-8: ES/6600 Board Status

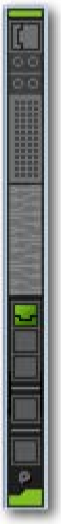
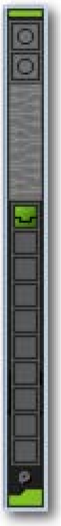
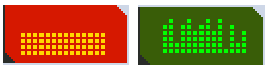


Figure 8-9:ES-2 Board Status



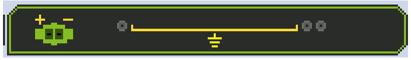
- ES boards can be displayed as follows:
  - Yellow = Minor Severity, due to unexpected ES alignment.
  - Blue = Warning Severity, due to the fact that some of the Uplinks are not connected.
  - Uplinks on the ES boards are displayed according to the Interface separation that was configured in the system (for more information, refer to the *Mediant 8000 IOM*). Ports properties can be viewed in the tool tip.
  - Color convention: Red = Disabled, Green = Enabled, yellow - Minor Alarm stating that certain port should not be used.
- Power Supplies Status:

Figure 8-10: Power Status



  - Color convention: Red = Failed; Green = OK
- PEM (Power Entry Module) status:

Figure 8-11: PEM Status



  - Color convention: Red = Failed; Green = OK
  - When the PEM is displayed in green, the tooltip 'PEM is OK, Power input is OK' appears.
  - When the PEM is displayed in red, the tooltip indicates the failure reason. The following reasons can be displayed: 'PEM is not responding', 'PEM is OK, power input is not detected', 'PEM is OK, power input polarity inversed'.

8.2 Mediant 5000 Status Pane

The Status pane displayed in the main screen indicates the overall gateway status, as well as additional Info Pane information: Name, Administrative State (Shut Down/Locked/Unlocked), Operational State (Enabled/Disabled), gateway IP address and gateway software version.

The following VoIP boards can populate the Mediant 5000 TP-6310 and TP-8410.

Figure 8-12: Mediant 5000 6310 Status Pane

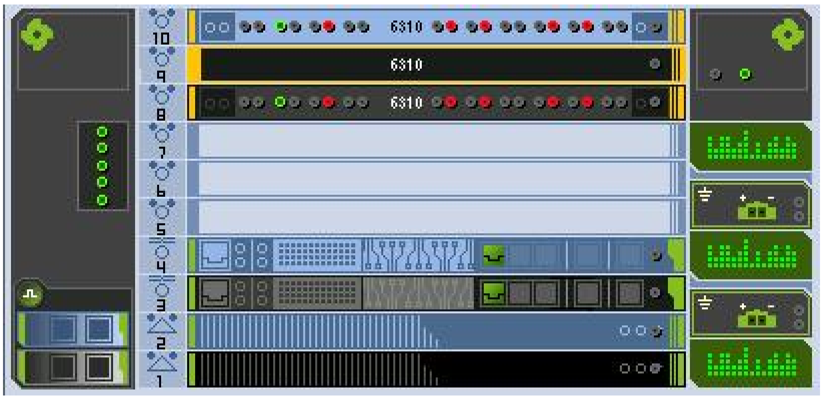
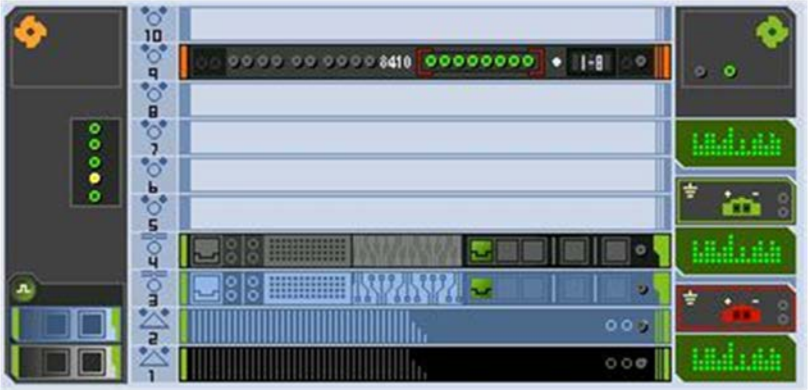


Figure 8-13: Mediant 5000 8410 Status Pane



Note: In the Mediant 5000, slots 5-10 inclusively are reserved for TP boards, slots 1-2 are reserved for the SC (System Controller) Boards, and slots 3-4 are reserved for the Ethernet Switch boards.

Statuses for the Mediant 5000 include the following:

- SAT Card status :
  - Each SAT card is represented by a bar located in the MG Status screen near the corresponding SC board (refer to the figures above). The background of the SAT card represents SAT activity (black for active; pale blue for redundant). The overall status of the SAT card is represented by its border color (Gray = Locked; Red = Disabled; Green = Enabled; Orange = Major Severity).
  - The status of the Timing module and External Interfaces is represented by corresponding icons in the SAT card status bar. Their color conventions are described below. Tooltips present users with relevant additional information.

  The SAT card has following color convention:

Table 8-3: SAT Card Status Color Convention

Color	Convention
Green	The SAT Card is locked to one of the external interfaces.
Blue	The SAT Card is in Hold Over state.
Yellow	The SAT Card is in Free Run state.
Red	SAT Card Error.

  - The status of the Timing module and External Interfaces is represented by corresponding icons in the SAT card status bar. Their color conventions are described below. Tooltips present users with relevant additional information.

- The Timing module has the following color convention:
  - The Timing module summarizes the status of the clock reference source and the SAT card. The status of the Timing module is *Red*=Failed or *Green*=OK.
  - When you click this icon, the System Clock Settings link is displayed in the Configuration pane. Click this link to display the current timing mode configuration.
  - In the Standalone mode, the icon must be *green*.

Note: When you navigate to the System Clock Settings window, only events and alarms relevant to the System Clock are displayed in the Alarms Browser.

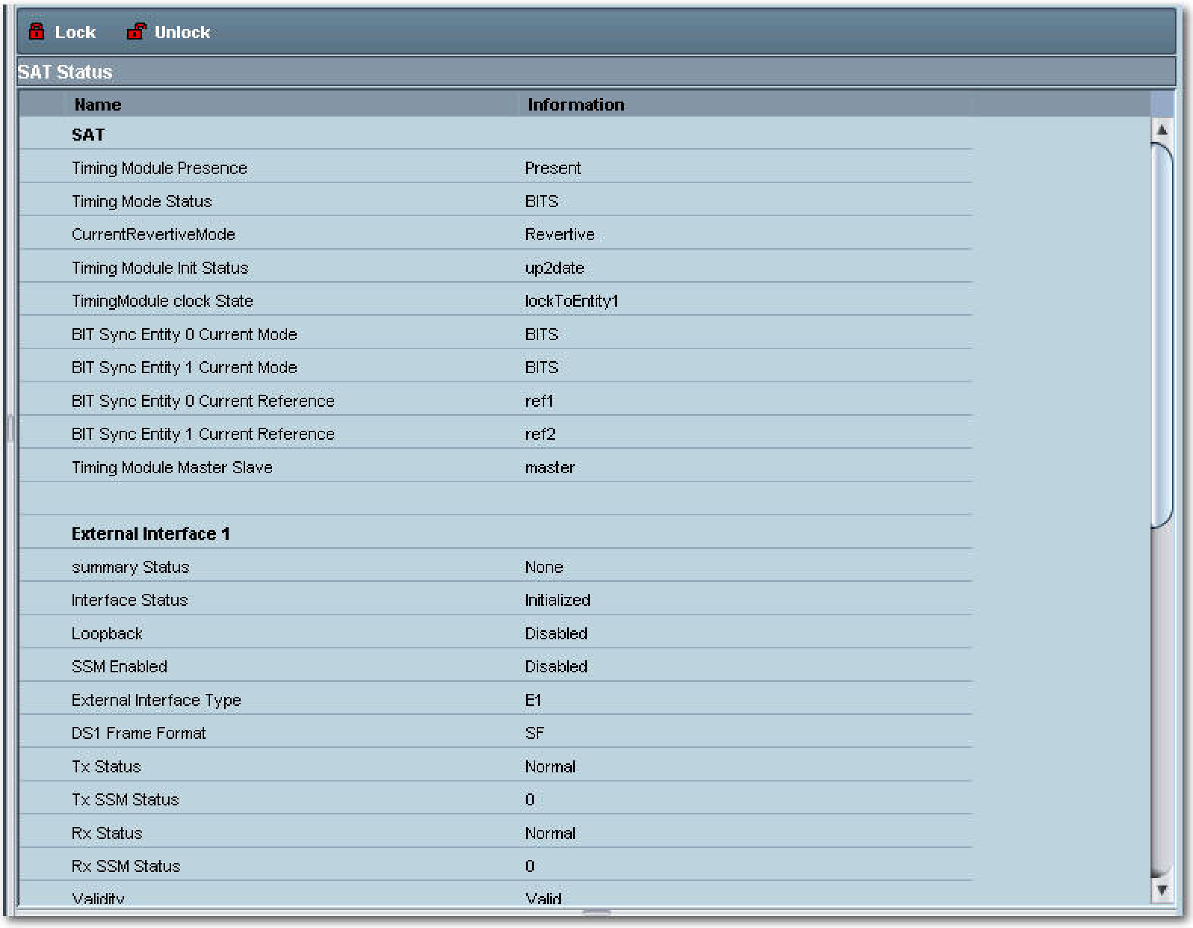
- External Interfaces have following color conventions:

Table 8-4: External Interface Color Convention

Color	Convention
Green with Border	OK status and currently selected as the Clock source (as in the example).
Green	OK status.
Red	Failed (alarm) status.
Grey	Status Unknown.

- When a SAT card does not have a Timing module, the status icon of the Timing Module is not displayed and External Interfaces are displayed as grey placeholders .
- To view additional information on the status of the Timing module and External Interfaces, double-click the SAT bar; the screen shown below is displayed.

Figure 8-14: SAT Properties Screen



SAT Status

Name	Information
SAT	
Timing Module Presence	Present
Timing Mode Status	BITS
CurrentRevertiveMode	Revertive
Timing Module Init Status	up2date
TimingModule clock State	lockToEntity1
BIT Sync Entity 0 Current Mode	BITS
BIT Sync Entity 1 Current Mode	BITS
BIT Sync Entity 0 Current Reference	ref1
BIT Sync Entity 1 Current Reference	ref2
Timing Module Master Slave	master
External Interface 1	
summary Status	None
Interface Status	Initialized
Loopback	Disabled
SSM Enabled	Disabled
External Interface Type	E1
DS1 Frame Format	SF
Tx Status	Normal
Tx SSM Status	0
Rx Status	Normal
Rx SSM Status	0
Validity	Valid

- Shelf LEDs :

  Five LEDs summarize the gateway's status (from top to bottom):

  - System: Red = System Error occurred; Green = OK
  - Critical: Red = Critical Error occurred; Green = OK
  - Major: Orange = Major Error occurred; Green = OK
  - Minor: Yellow = Minor Error occurred; Green = OK
  - Shelf: Red = Critical Error occurred; Orange = Major Error occurred; Green = OK; Gray = Off

- Fan status (in the Mediant 5000)

  Color convention: Red = Failed; Green = OK; Orange = Major Severity

- Fan status (in the Mediant 5000) :

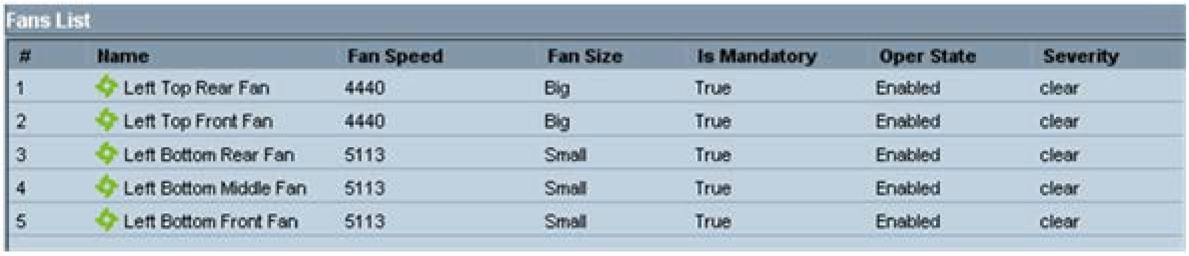
  Fans' two rows are read as follows:

  - Top Row: Upper Fan Tray
  - Bottom Row: Bottom Fan Tray
  - Double-click each fan tray to view fan status

  Color convention: Red = Failed; Green = OK

  To view additional information on the status of the fans, double-click the Fan icon. The following status screen is displayed:

Figure 8-15: Mediant 5000 Fans List Information



Fans List

#	Name	Fan Speed	Fan Size	Is Mandatory	Oper State	Severity
1	Left Top Rear Fan	4440	Big	True	Enabled	clear
2	Left Top Front Fan	4440	Big	True	Enabled	clear
3	Left Bottom Rear Fan	5113	Small	True	Enabled	clear
4	Left Bottom Middle Fan	5113	Small	True	Enabled	clear
5	Left Bottom Front Fan	5113	Small	True	Enabled	clear

- VOP Boards status:

  The figures below display board status:

  - TP-6310 Active and Redundant board:

Figure 8-16: 6310 Active Board Status

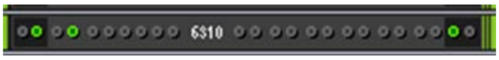
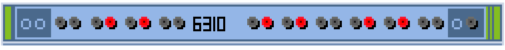


Figure 8-17: 6310 Redundant Board Status



- Background color: Dark Gray = Active board; Blue = Redundant board
- Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity, Yellow = Minor Severity, Blue = Warning Severity, White = Indeterminate Severity

  - TP Switchover: The active TP board, after switchover, is marked in a background black color without any LEDs, with a red or green frame around the board according to its Operational State (green = enabled boards, red = disabled boards). A redundant TP board, which becomes active after switchover, is marked in a background blue color, with LEDs for activated trunks.

- TP-8410 Active and Redundant board:

Figure 8-18: 8410 Active Board Status

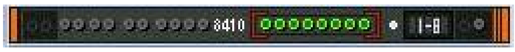
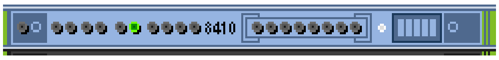


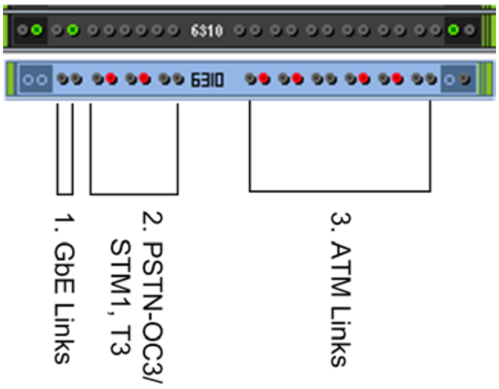
Figure 8-19: 8410 Redundant Board Status



  - Trunk (E1/T1) LED color convention: Red = Disabled; Green = Enabled; Gray = Locked

- LED Group status-TP-6310:

Figure 8-20: 6310 Board-LED Status

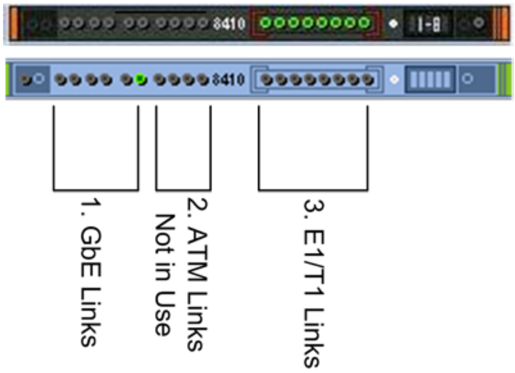


Legend

  - 1 = the first two LEDs represent the GbE (Gigabit Ethernet) status
  - 2 = six LEDs representing PSTN Interface status (for OC3/STM1, four LEDs are relevant; for T3, all six LEDs are relevant)
  - 3 = twelve LEDs representing ATM Interface status

- LED Group status-TP-8410

Figure 8-21: 8410 Board LED Status



Legend:

- 1. = six LEDs representing the GbE (Gigabit Ethernet) status
- 2.= four LEDs representing ATM LEDs which are not in use
- 3.= eight LEDs representing E1/T1 LEDs

- ES Boards and Ports status:

  The figure below displays an ES Board Status screen:

Figure 8-22: ES Board Status

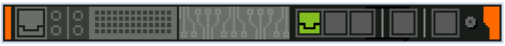
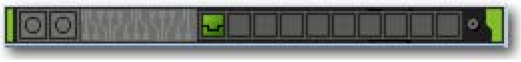


Figure 8-23: ES-2 Board Status

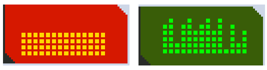


ES boards can be displayed as follows:

- Yellow = Minor Severity, due to unexpected ES alignment.
- Blue = Warning Severity, due to the fact that some of the Uplinks are not connected.
- Uplinks on the ES boards are displayed according to the Interface separation that was configured in the system (for more information, refer to the *Mediant 8000 IOM*). Ports properties can be viewed in the tool tip.
- Color convention: Red = Disabled, Green = Enabled, yellow - Minor Alarm stating that certain port should not be used.

- Power Supplies status:

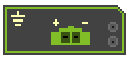
Figure 8-24: Power Supply Status



- Color convention: Red = Failed; Green = OK

- PEM (Power Entry Module) status:

Figure 8-25: PEM Status



- Color convention: Red = Failed; Green = OK
- When the PEM is displayed in green, the tooltip 'PEM is OK, Power input is OK' appears.
- When the PEM is displayed in red, the tooltip indicates reason of failure. The following reasons can be displayed: 'PEM is not responding', 'PEM is OK, power input is not detected', 'PEM is OK, power input polarity inversed'.

8.3 Provisioning Links

The Gateways' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and sub-links that are displayed in the Navigation pane.

The figure below shows the navigation hierarchy links used to provision the media gateway.

Figure 8-26: Media Gateway Level Navigation Buttons (Part 1)

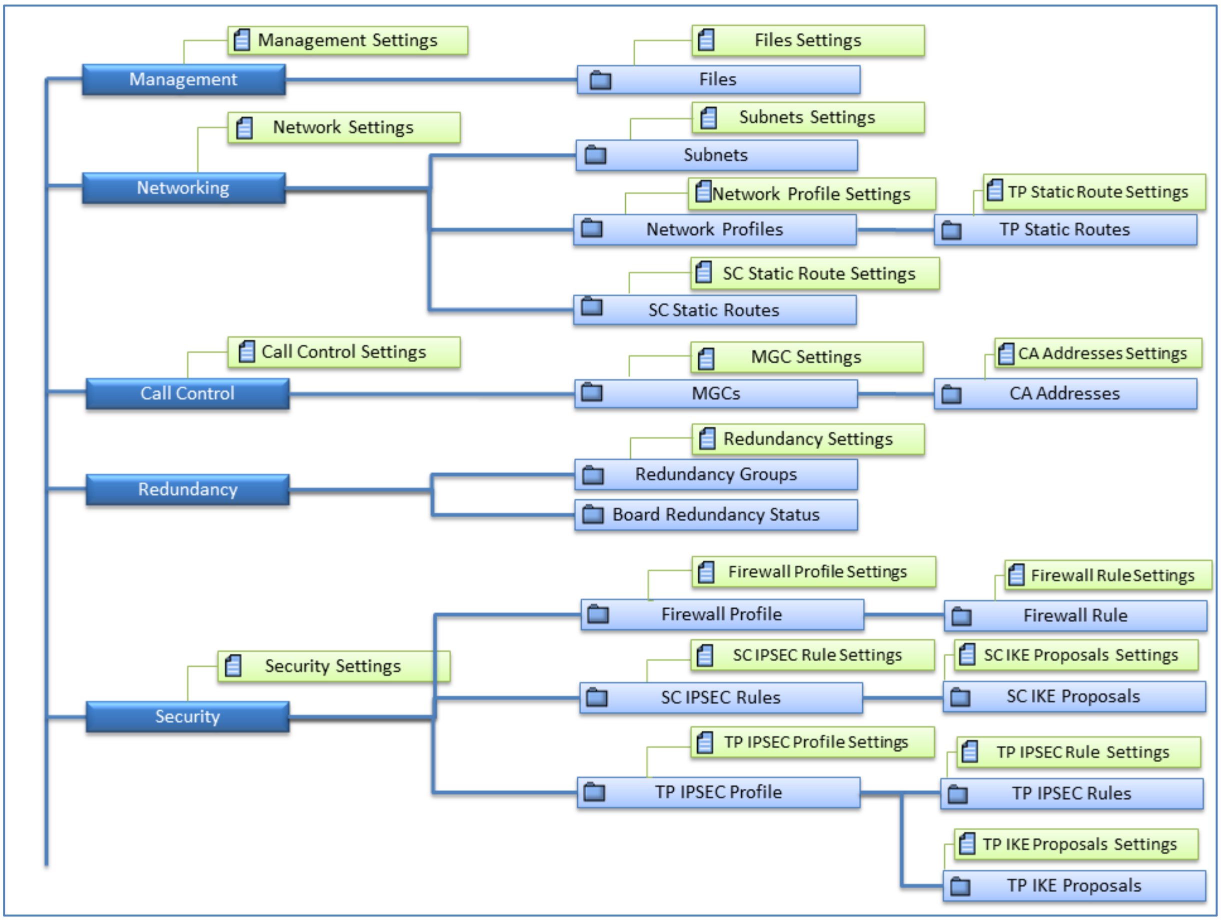
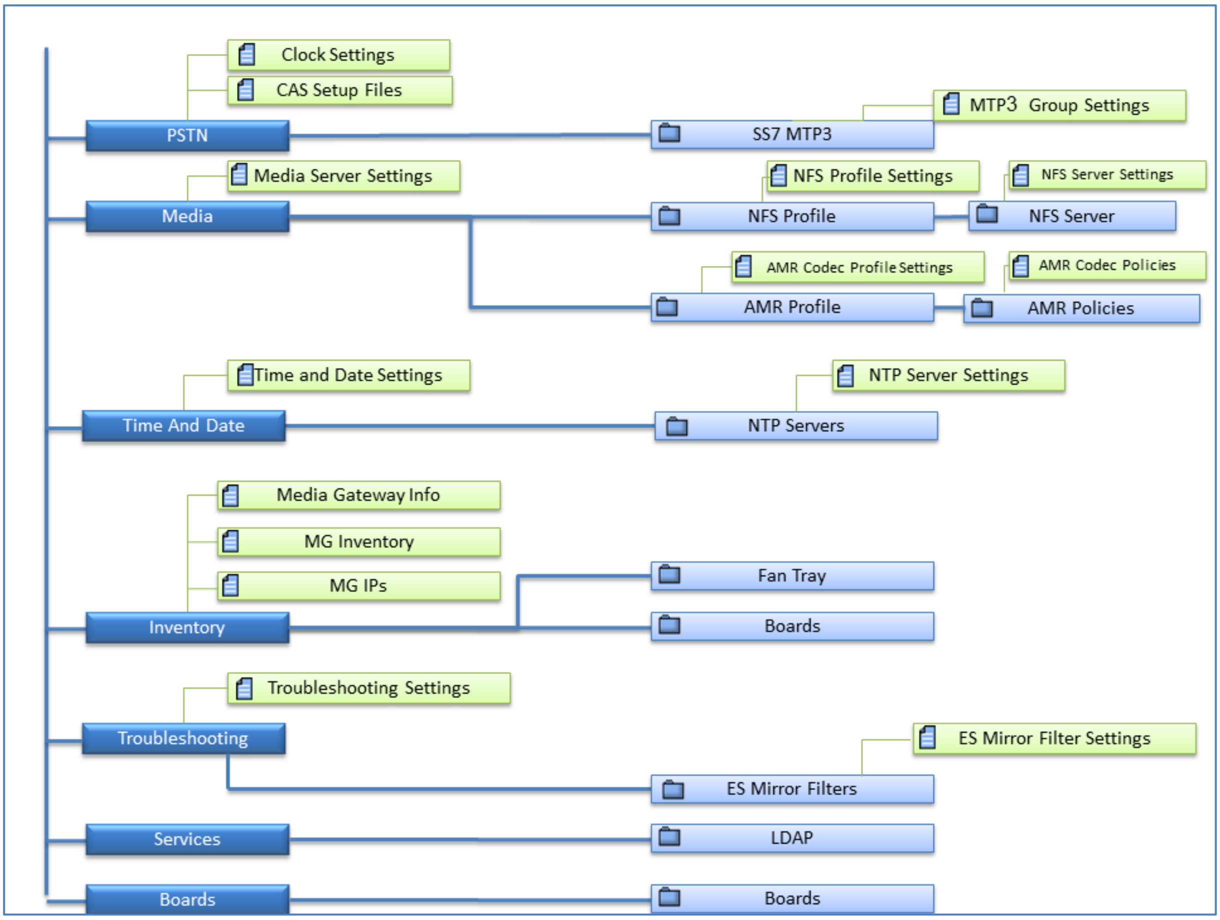


Figure 8-27: Media Gateway Level Navigation Buttons (Part 2)

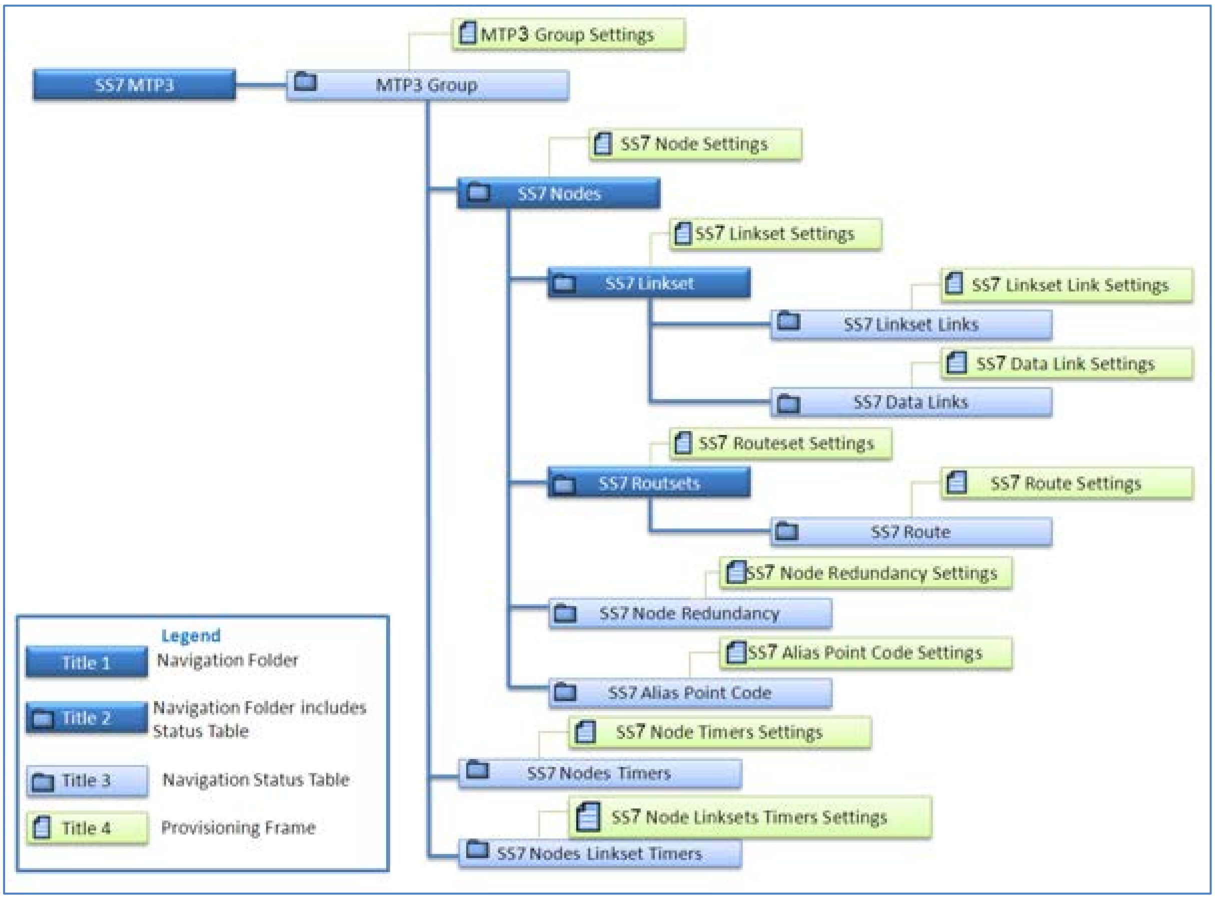


For more information, refer to the relevant *IOM Guide.*

8.3.1 MTP3 SS7 Provisioning

For SS7-level provisioning rules and configuration, refer to the *Mediant 5000 / 8000 IOM*. The figure below shows the MTP3 SS7 navigation hierarchy links:

Figure 8-28: SS7 MTP3 Navigation



8.3.2 V5.2 Provisioning (TP-8410)

For V5.2 applications, the following Settings Screens and actions are supported:

- **V5.2 Interfaces Table:** The user may define up to 31 different V5.2 interfaces that are indexed from 0 to 30. Each row in the table represents a V5.2 interface. The following actions (available from both the right-click menu and the Actions bar) are supported for each one of the V5.2 Interfaces: Add, Remove, Lock, Unlock, In Service, Offline, Protection Switchover, Properties.
- **V5.2 Links Table:** At least 2 V5.2 links (one primary and one secondary) must be configured before starting a V5.2 interface. There is a 1 to 1 mapping between V5.2 links and V5.2 interfaces configured with the V5.2 protocol type. The following actions (available from both the right-click menu and the Actions bar) are supported for each one of the V5.2 Links: Add, Remove, Lock, Unlock, Block, Unblock, Link ID Check, Properties.

For information on downloading and managing the V5.2 configuration file, see the 'Software Manager' on page 65.

Refer to the *Mediant 5000/8000 IOM Guide* to correctly provision and maintain the V5.2 solution.

8.4 Maintenance Actions

This section describes the Mediant 5000 and Mediant 8000 maintenance actions.

➢ To add a board to an empty slot in a gateway

- Right-click an empty slot to add a TP board to the gateway.

Table 8-5: Board Actions

Board Type	Add Board Action	Action Description
Empty Boards	Add TP-6310 OC-3 / STM-1 Board: ▪ Gateway ▪ SIP-Gateway ▪ Media-Server ▪ SIP-Media-Server	-
	Add TP-6310 T3 Board: ▪ Gateway ▪ SIP-Gateway ▪ Media-Server ▪ SIP-Media-Server	-
	Add TP-8410 Board: ▪ Gateway ▪ SIP-Gateway ▪ Media-Server ▪ SIP-Media-Server	-

8.4.1 Board Actions

- Right-click the board; a pop-up menu listing available Board Actions under three sub-menus is displayed: Configuration, Maintenance and Performance. Board actions are available in both the graphical and from the table view.
  Board actions are dependent on board type and state.

Table 8-6: Board Status Actions

Board Type	Action	Supported Maintenance Actions	Action Description
VoP BoardsTP-6310	DS1 Trunks List	-	Opens the list of all the DS1 Trunks of the VoP Board.
VoP BoardsTP-8410	DS1 Trunks List	-	Opens the list of all the DS1 Trunks of the VoP Board
	Trunks 1-8 Trunks 9-16 Trunks 17-24 Trunks 25 -31 Trunks 32-40 Trunks 41-42	-	Updates 8410 DS1 status panel on the status screen with the selected trunks leds

Table 8-7: Board Configuration Actions

Board Type	Action	Supported Maintenance Actions	Action Description
VoP Boards			

Table 8-8: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
VoIP Boards	Lock	Always	Caution: This action resets the board and drops all active calls on it.
	Unlock	Always	This action re-initializes the board.
	Remove	Board is Locked	Removes the board with its entire configuration from the chassis view.
	Move To Slot	Board is Locked	This action moves an existing TP board and its entire configuration to a free slot on the media gateway. This action may be used for system troubleshooting or due to changes in PSTN cabling. Note: you are prompted to select one of the empty boards in the system where you wish to remove an existing board.
	Make Board Redundant	Board is Locked	Defines the board to be redundant.
	Make Board Non-Redundant	Board is Locked & redundant	Defines the redundant board to be active.
	Switch Over	Board is unlocked and active	Performs a switchover action from a selected board to a predefined redundant board.
	Switch Back	Board is switched-over	Performs a switchback action from a selected redundant board to a previously failed active board.

Table 8-8: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
	License Update	Always	Updates the License Keys of the VoIP boards to enable a new set of features.
	Save INI File	Always	Saves a board INI file to an external location using one of the following options: ▪ INI file – includes only those parameters with changed values, (not including those with default values). ▪ Complete INI file– includes all parameters (including those with default values).
	Start Debug Recording	Board is unlocked and active	Starts debug recording according to previously defined rules for the VoP board.
	Stop Debug Recording	Board is unlocked and active	Stops debug recording.
ES Board	Lock	Always	
	Unlock	Always	Caution: This action might cause network connectivity problems. At least one ES board must stay unlocked.
	Align All Boards to me	Always	All boards will be aligned to use this ES board, where the target ES is not fully operational due to unconnected uplinks.
	Clear Severity	Always	When the ES alarm severity level is High (Warning or Major), it is manually cleared (note that this action is only relevant for the ES/6600 switch board).
	Enable Mirroring	Always	Enables mirroring of Ethernet ports.
	Disable Mirroring	Always	Disables mirroring of Ethernet ports
	Mirror to ES Eth. Port#23	Always	Defines mirroring destination to be at ES Eth. Port#23
	Mirror to Redundant SC Ethernet Port	Always	Defines mirroring destination to be Redundant SC Ethernet Port

Table 8-8: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
SC Board	Lock	On Redundant SC Board	Performs Lock of the SC Board
	Unlock	On Redundant SC Board	Performs Unlock of the SC Board
	Switch Over	When a redundant SC board is enabled	Performs a switchover from the active (selected) board to the redundant board.
	Clean Hard Disk Errors	Always	This action clears all the hard disk errors and sends corresponding 'Clear' Alarm.

Table 8-9: Board Performance Actions

Board Type	PM Action	Action Description
VoIP Boards SC Board ES Ports (RT related actions only)	Display Real-Time PMs	Opens a real-time graph for selected PM parameters
	Display Historical PMs	Opens a history PM table for selected parameters
	Configure MG Profile	Selects the PM parameters for background (history) sampling and creates a profile
	Attach MG Profile	Attaches the PM profile to the board
	Detach MG Profile	Detaches the PM profile from the board
	Stop Polling MG	Stops sampling Performance Monitoring data
	Start MG Polling	Starts sampling Performance Monitoring data
	Reset RT PM	Reset Real Time PM Counters. This action is available for VoP Boards only.

Note: All actions are available for the currently released version of the EMS. For previous versions, a partial subset of actions are available.

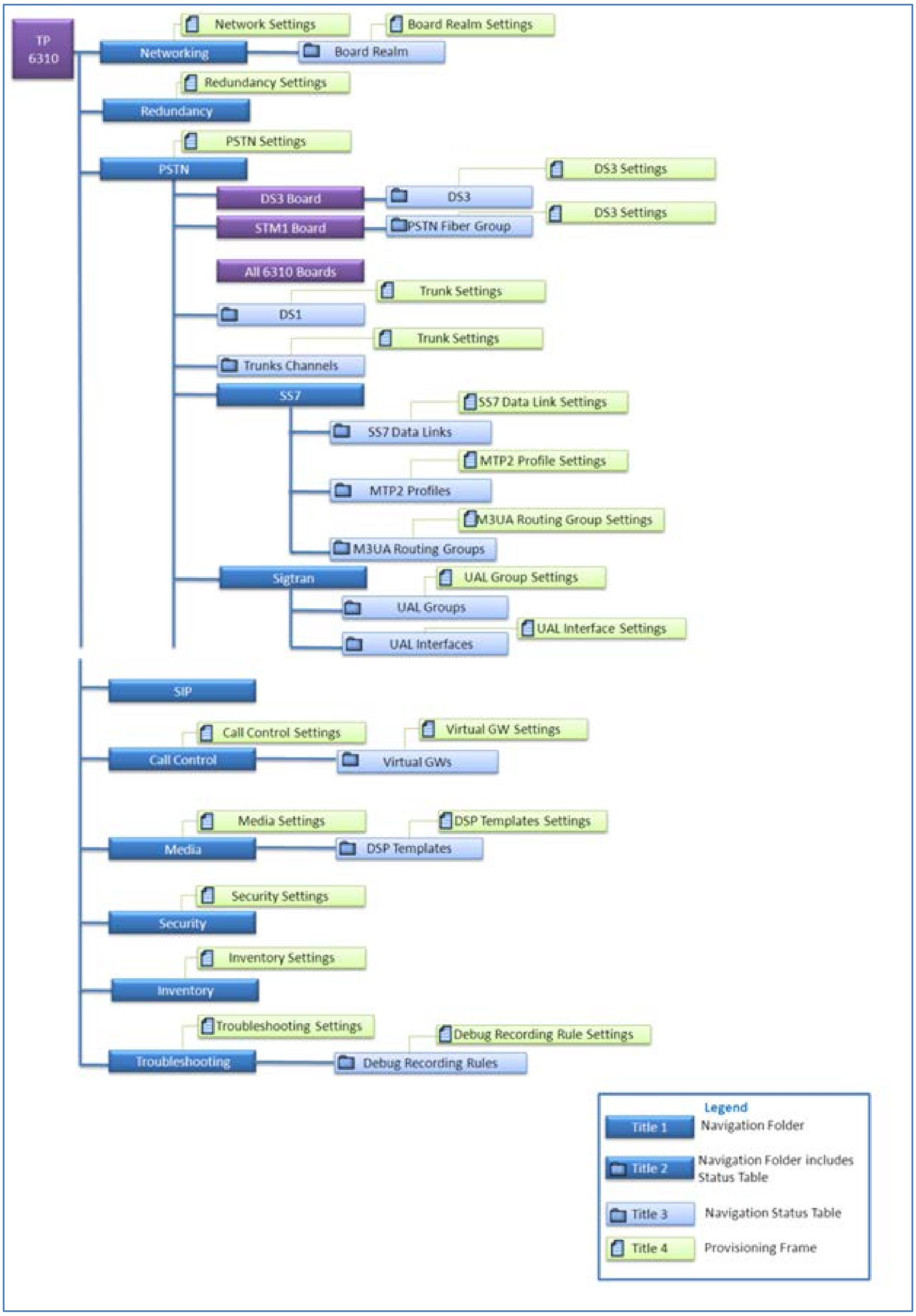
8.5 Accessing a TP-6310 Board

This section refers to the Mediant 5000 media gateways and Mediant 8000 media gateways.

The TP-6310 boards' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and sub-links that are displayed in the Navigation pane.

The figure below shows the navigation hierarchy links used to provision the TP-6310 media gateway board.

Figure 8-29: TP-6310 Board Level



For detailed information on the Status screens of the interfaces (PSTN Fiber Groups, DS3 status, DS1 status), see Section 'Accessing the Main Status Screens' on page 142.

8.5.1 Accessing the TP Board Level Provisioning Screen

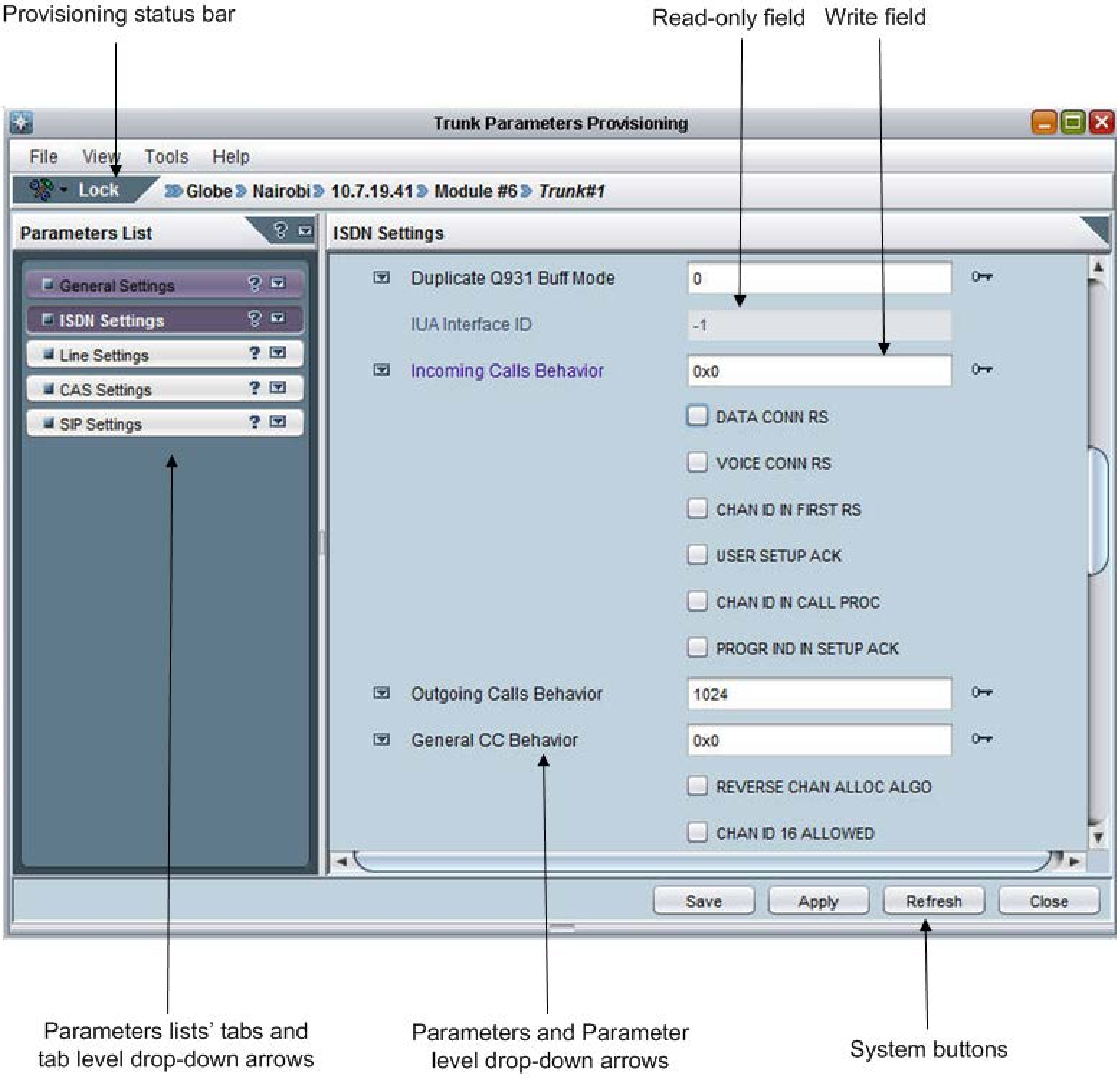
This section describes how to access the TP Board Level Provisioning Screen.

➢ **To access the TP-6310 'Board Provisioning Parameters' screen:**

1. In the graphic representation of the gateway in the 'MG Status' screen (shown in the figure 'MG Status Screen'), select the desired TP-6310 board.

2. In the Navigation pane, select the desired option and then in the 'Configuration' pane; click the desired option; the corresponding provisioning screen is displayed:

Figure 8-30: TP-6310 Board Provisioning Parameters



Provisioning status bar

Read-only field

Write field

Trunk Parameters Provisioning

Lock » Globe » Nairobi » 10.7.19.41 » Module #6 » Trunk#1

Parameters List

- General Settings
- ISDN Settings
- Line Settings
- CAS Settings
- SIP Settings

ISDN Settings

Duplicate Q931 Buff Mode	0
IUA Interface ID	-1
Incoming Calls Behavior	0x0
	□ DATA CONN RS
	□ VOICE CONN RS
	□ CHAN ID IN FIRST RS
	□ USER SETUP ACK
	□ CHAN ID IN CALL PROC
	□ PROGR IND IN SETUP ACK
Outgoing Calls Behavior	1024
General CC Behavior	0x0
	□ REVERSE CHAN ALLOC ALGO
	□ CHAN ID 16 ALLOWED

Parameters lists' tabs and tab level drop-down arrows

Parameters and Parameter level drop-down arrows

System buttons

For detailed information on provisioning the board parameters, refer to *EMS Parameter Guide for the Mediant 5000/8000*.

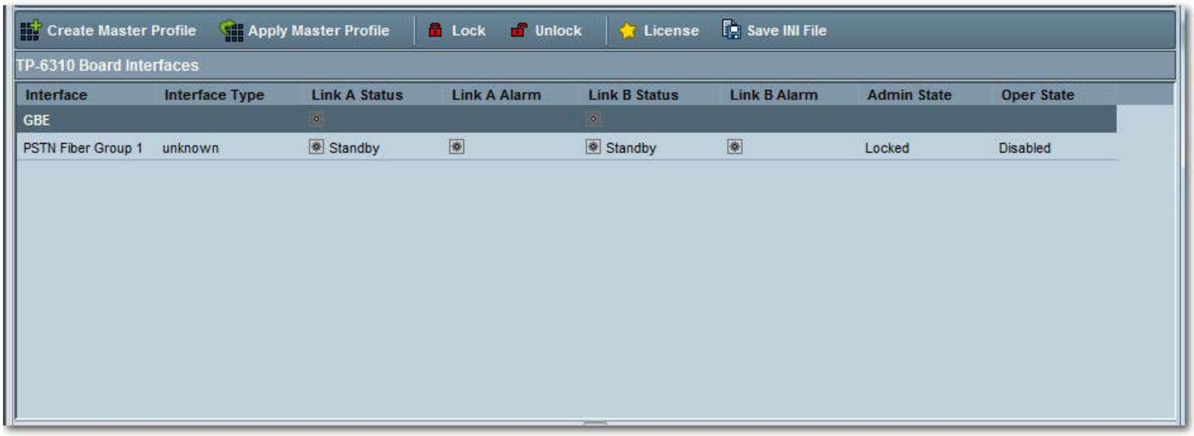
8.5.2 Accessing the PSTN Status Screens

This section describes how to access the PSTN Status screens.

➢ To access the TP-6310 Board Status Pane:

- In the 'MG Status' screen, select the specific TP-6310 STM1 board and in the Navigation pane, select **PSTN** ► **Fiber Group**. The 'TP-6310 Board Interfaces' screen is displayed (see the figure below), showing the fiber groups and interface type (STM1 or OC3).

Figure 8-31: TP-6310 STM1 Board Status Pane



TP-6310 Board Interfaces

Interface	Interface Type	Link A Status	Link A Alarm	Link B Status	Link B Alarm	Admin State	Oper State
GBE		●		●			
PSTN Fiber Group 1	unknown	● Standby	●	● Standby	●	Locked	Disabled

➢ To access the TP-6310 DS3 screen:

1. In the 'MG Status' screen, select the TP-6310 DS3 board and in the Navigation pane, select **PSTN** ► **DS3;** the DS3 Status screen is displayed (refer to the figure below), showing the status of the DS3 interfaces of the TP-6310 DS3 board.

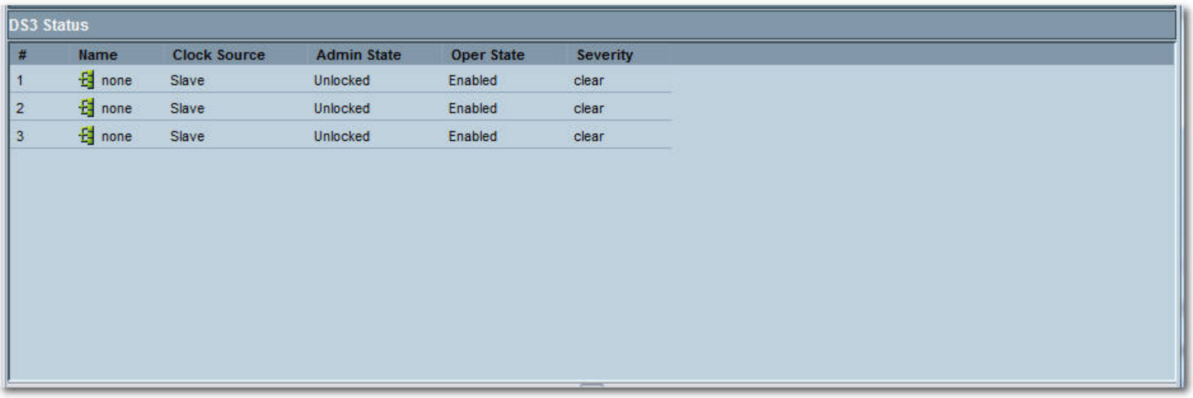
2. Double-click each DS3 interface to obtain the status of its DS1 interfaces.

3. Double-click the line that corresponds to the specific D3 interface to view the detailed list and status of T1 trunks corresponding to the specific D3 interface. Note that you can also view the DS1 Carriers List by selecting 'DS1' in the Navigation pane.

➤ To provision a DS3 Interface:

- Select the desired interface and then in the Configuration pane, click **DS3 Settings**.

Figure 8-32: TP-6310 DS3 Board Status Pane



DS3 Status

#	Name	Clock Source	Admin State	Oper State	Severity
1	none	Slave	Unlocked	Enabled	clear
2	none	Slave	Unlocked	Enabled	clear
3	none	Slave	Unlocked	Enabled	clear

➤ To access a PSTN Fiber Group:

- Double-click the row of PSTN Fiber Group 1 in the 'TP-6310 Board Interfaces' screen; the PSTN Fiber Group Status pane is displayed according to the interface type (refer to the figures 'PSTN Fiber Group (STM1 interface)' screen and the 'PSTN Fiber Group (OC3 interface)' screen below).

Figure 8-33: PSTN Fiber Group (SDH/STM1 Interface) Screen

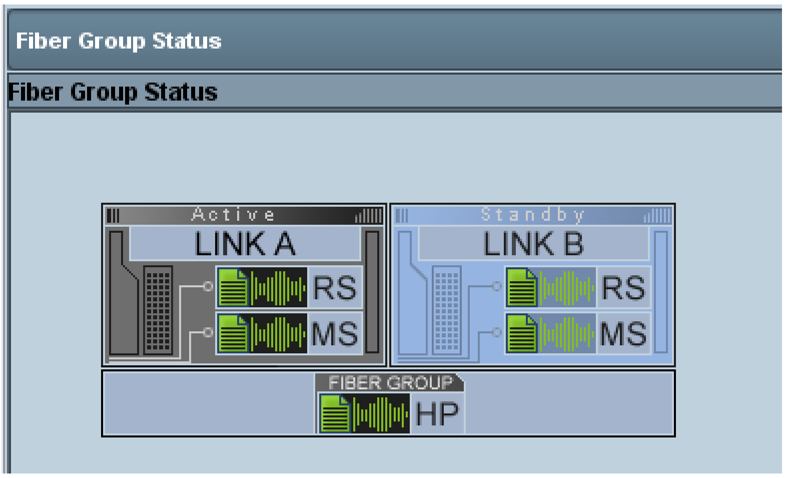
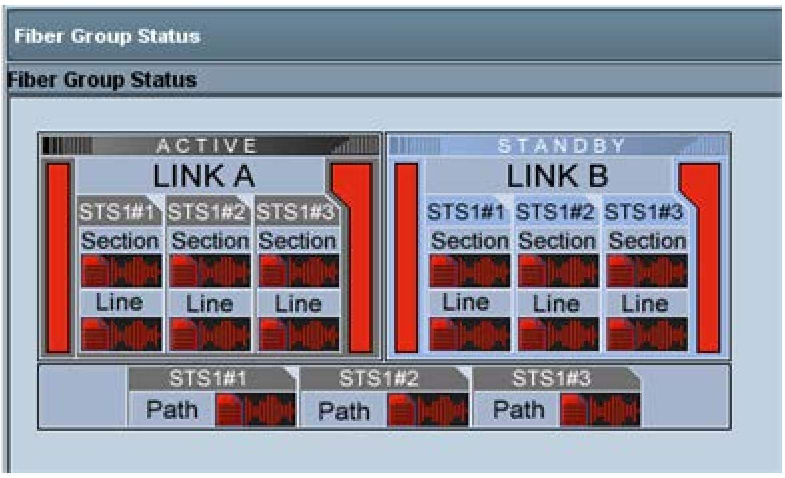


Figure 8-34: PSTN Fiber Group (Sonet OC3/STS Interface) Screen



➢ To provision the PSTN Fiber Group:

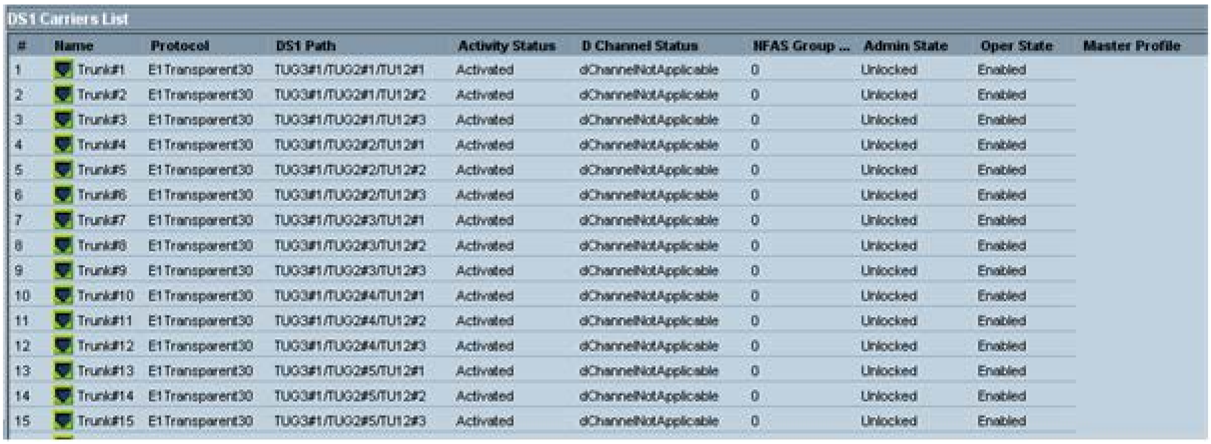
1. In the TP-6310 Status screen, select the desired PSTN Fiber Group, and then in the Configuration pane, click **Fiber Group Settings**; the Fiber Group Settings screen is displayed.

➢ To provision the DS1 Trunks:

1. In the Navigation pane, select **PSTN** ► **DS1 Trunks**; the DS1 Trunks list is displayed.

2. Select the desired trunk and in the Configuration pane, click **Trunk Settings**; the Trunk Settings screen is displayed.

Figure 8-35: DS1 Carriers List Screen



DS1 Carriers List

#	Name	Protocol	DS1 Path	Activity Status	D Channel Status	NFAS Group ...	Admin State	Oper State	Master Profile
1	Trunk#1	E1Transparent30	TUG3#1/TUG2#1/TU12#1	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
2	Trunk#2	E1Transparent30	TUG3#1/TUG2#1/TU12#2	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
3	Trunk#3	E1Transparent30	TUG3#1/TUG2#1/TU12#3	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
4	Trunk#4	E1Transparent30	TUG3#1/TUG2#2/TU12#1	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
5	Trunk#5	E1Transparent30	TUG3#1/TUG2#2/TU12#2	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
6	Trunk#6	E1Transparent30	TUG3#1/TUG2#2/TU12#3	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
7	Trunk#7	E1Transparent30	TUG3#1/TUG2#3/TU12#1	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
8	Trunk#8	E1Transparent30	TUG3#1/TUG2#3/TU12#2	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
9	Trunk#9	E1Transparent30	TUG3#1/TUG2#3/TU12#3	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
10	Trunk#10	E1Transparent30	TUG3#1/TUG2#4/TU12#1	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
11	Trunk#11	E1Transparent30	TUG3#1/TUG2#4/TU12#2	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
12	Trunk#12	E1Transparent30	TUG3#1/TUG2#4/TU12#3	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
13	Trunk#13	E1Transparent30	TUG3#1/TUG2#5/TU12#1	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
14	Trunk#14	E1Transparent30	TUG3#1/TUG2#5/TU12#2	Activated	dChannelNotApplicable	0	Unlocked	Enabled	
15	Trunk#15	E1Transparent30	TUG3#1/TUG2#5/TU12#3	Activated	dChannelNotApplicable	0	Unlocked	Enabled	

8.5.2.1 DS1 Trunks Actions

This section describes how to perform actions on DS1 trunks.

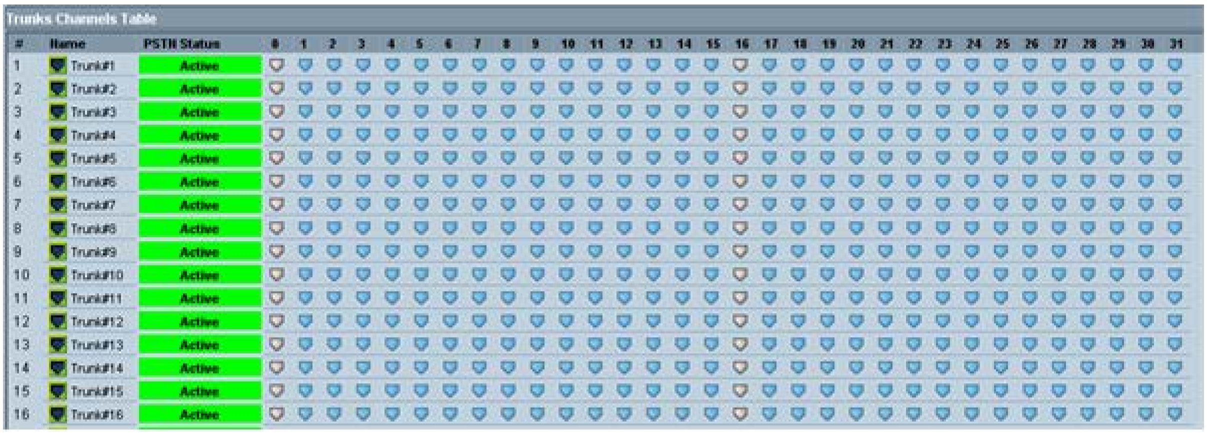
➢ **To access DS1 trunks:**

- Select multiple DS1 trunks and right-click; a popup menu listing available Configuration and Maintenance Trunk Actions is displayed. The following actions are available (note these options are also available from the Actions bar):
    - Configuration:
        - **Apply Profile** – allows applying a previously defined trunk profile to one or more selected trunks.
    - Maintenance:
        - **Lock** – take the trunk out-of-service and allow modification of its configuration (and specifically of Online configuration parameters); the synchronization with the remote PSTN side will be lost and corresponding voice and signaling traffic will be dropped; locked trunks will remain out-of-service even if the media gateway board is restarted (as a result of lock/unlock maintenance actions or board failure).
        - **Unlock** – Unlock the trunks
        - **Deactivate** – (can only be applied when trunks are in Unlock state)- When a trunk is deactivated, it is temporarily disabled from the PSTN network. An AIS alarm signal is sent from the media gateway board to the receiving end of the trunk and an RAI alarm signal is returned (displayed in the EMS Alarm Browser). Use this option for maintenance purposes. For example, the DS1 trunk for running maintenance tasks has SS7 links on it and therefore you cannot lock it and do not wish to deactivate SS7.
        - **Activate** – (can only be applied when trunks are in Unlock state)- Activate trunks after a trunk has been deactivated. When a trunk is activated, it is reconnected to the PSTN network and the relevant AIS alarm is cleared.
        - **Create Loopback** – This option is used to create remote loopback for DS1 lines.
        - **Remove Loopback** – This option is used to remove loopback for DS1 lines.

➢ To access the Trunks channels status of the STM1 board:

- In the Navigation pane, select **Trunks Channels**; the Trunks Channels table is displayed (refer to the figure below). For more information, see 'Trunks and Channels Status' on page 215.

Figure 8-36: Trunk Channels Status



Trunks Channels Table

#	Name	PSTN Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	Trunk#1	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
2	Trunk#2	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
3	Trunk#3	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
4	Trunk#4	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
5	Trunk#5	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
6	Trunk#6	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
7	Trunk#7	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
8	Trunk#8	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
9	Trunk#9	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
10	Trunk#10	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
11	Trunk#11	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
12	Trunk#12	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
13	Trunk#13	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
14	Trunk#14	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
15	Trunk#15	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
16	Trunk#16	Active	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▽	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼

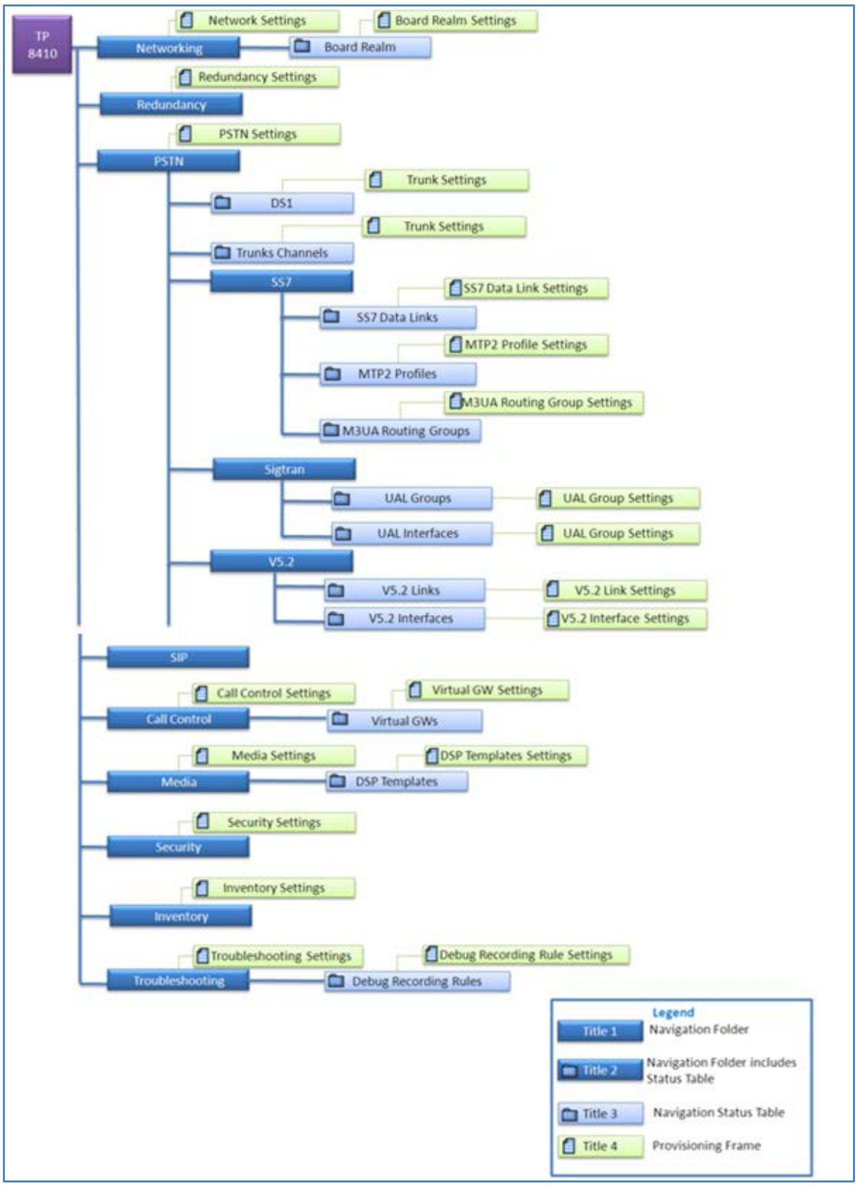
Note: The same actions as described for the 'DS1 Trunks Actions' above are available in the Channel right-click menu.

8.6 Accessing a TP-8410 in the Mediant 5000

The Gateways' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and sub-links that are displayed in the Navigation pane.

The figure below shows the navigation hierarchy links used to provision the TP-8410 board.

Figure 8-37: TP-8410 Board Hierarchy Links



8.7 SIP Provisioning of VoP Board (6310 and 8410)

The Gateways' SIP provisioning parameters are divided into groups / entities. Each group/entity is represented by links and sub-links that are displayed in the Navigation pane.

The figure below shows the navigation hierarchy links for the SIP board.

Figure 8-38: SIP General Hierarchy Links

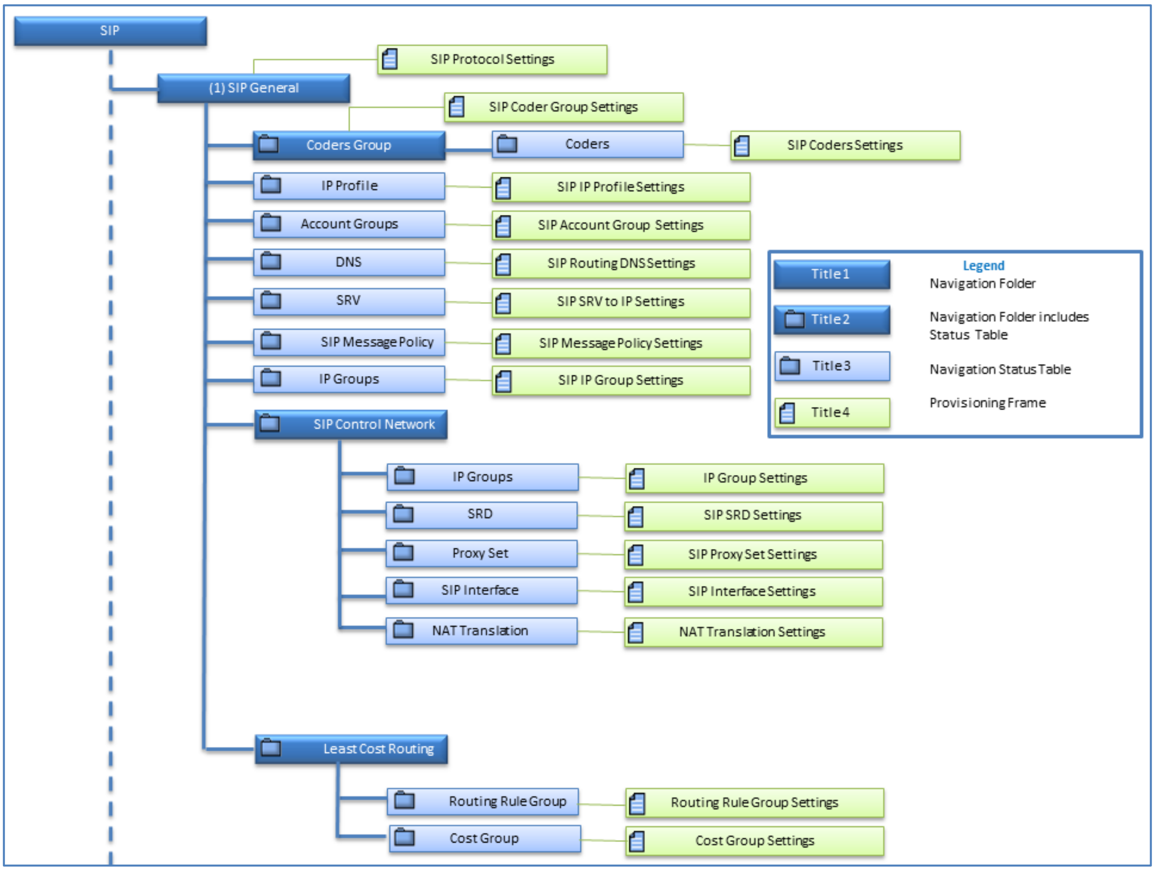


Figure 8-39: SIP GW/IP to IP Hierarchy Links

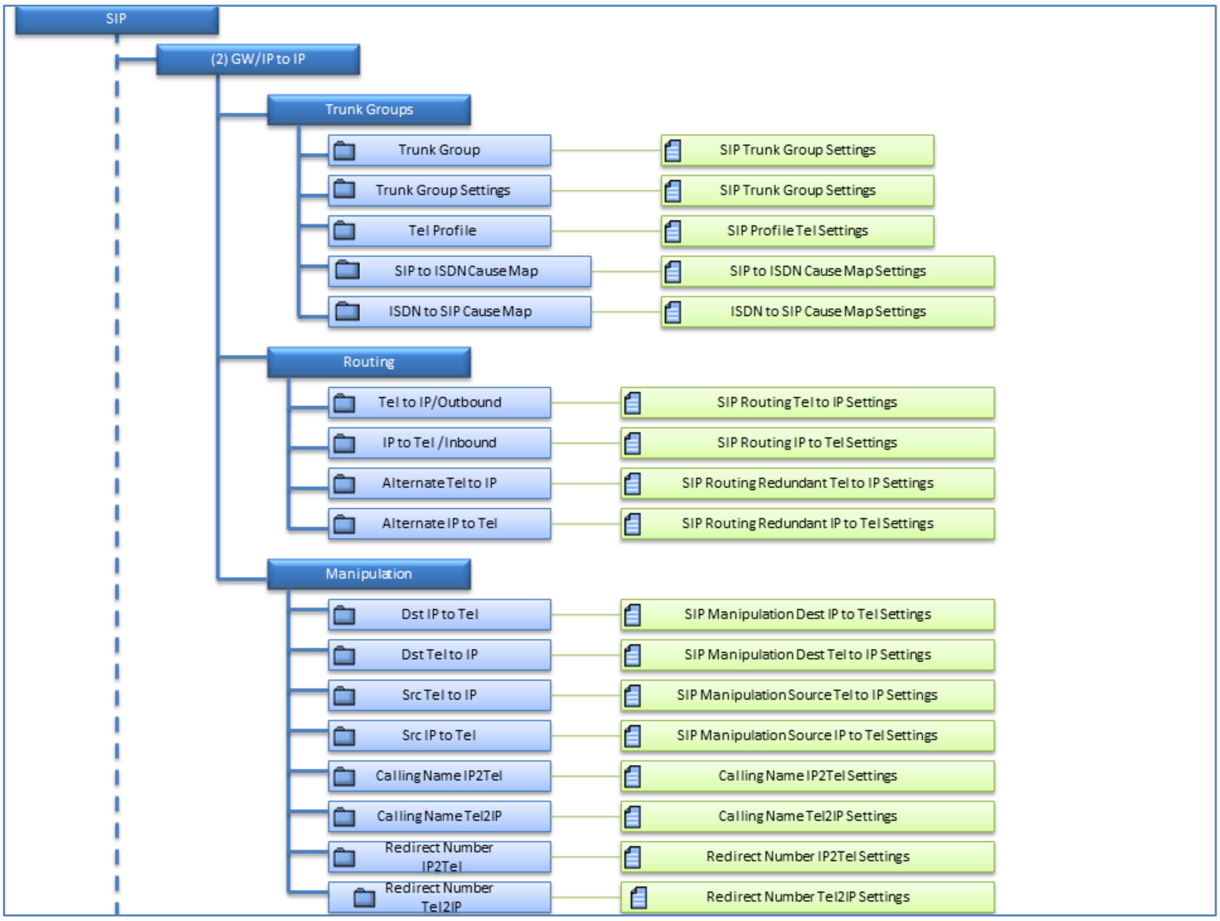

SIP
(2) GW/IP to IP
Trunk Groups
Trunk Group
SIP Trunk Group Settings
Trunk Group Settings
SIP Trunk Group Settings
Tel Profile
SIP Profile Tel Settings
SIP to ISDN Cause Map
SIP to ISDN Cause Map Settings
ISDN to SIP Cause Map
ISDN to SIP Cause Map Settings
Routing
Tel to IP/Outbound
SIP Routing Tel to IP Settings
IP to Tel /Inbound
SIP Routing IP to Tel Settings
Alternate Tel to IP
SIP Routing Redundant Tel to IP Settings
Alternate IP to Tel
SIP Routing Redundant IP to Tel Settings
Manipulation
Dst IP to Tel
SIP Manipulation Dest IP to Tel Settings
Dst Tel to IP
SIP Manipulation Dest Tel to IP Settings
Src Tel to IP
SIP Manipulation Source Tel to IP Settings
Src IP to Tel
SIP Manipulation Source IP to Tel Settings
Calling Name IP2Tel
Calling Name IP2Tel Settings
Calling Name Tel2IP
Calling Name Tel2IP Settings
Redirect Number IP2Tel
Redirect Number IP2Tel Settings
Redirect Number Tel2IP
Redirect Number Tel2IP Settings

Figure 8-40: SIP SBC Hierarchy Links

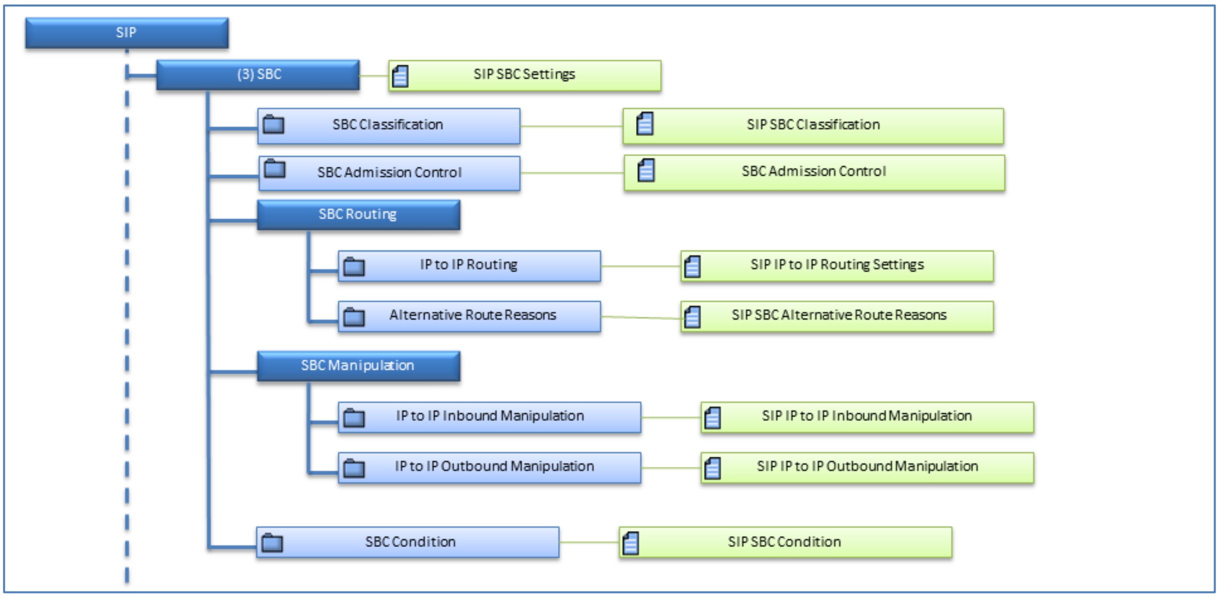
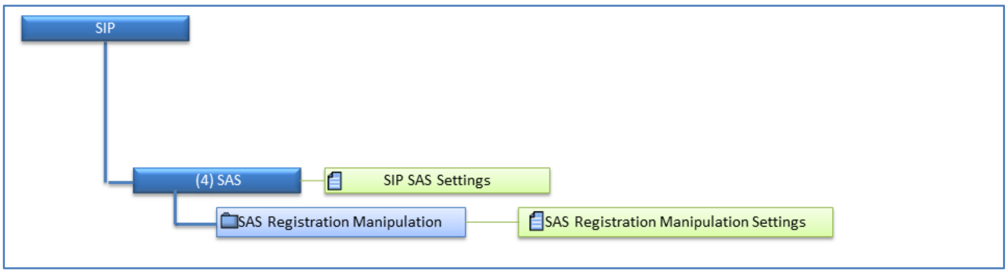

SIP
(3) SBC
SIP SBC Settings
SBC Classification
SIP SBC Classification
SBC Admission Control
SBC Admission Control
SBC Routing
IP to IP Routing
SIP IP to IP Routing Settings
Alternative Route Reasons
SIP SBC Alternative Route Reasons
SBC Manipulation
IP to IP Inbound Manipulation
SIP IP to IP Inbound Manipulation
IP to IP Outbound Manipulation
SIP IP to IP Outbound Manipulation
SBC Condition
SIP SBC Condition

Figure 8-41: SIP SAS Settings

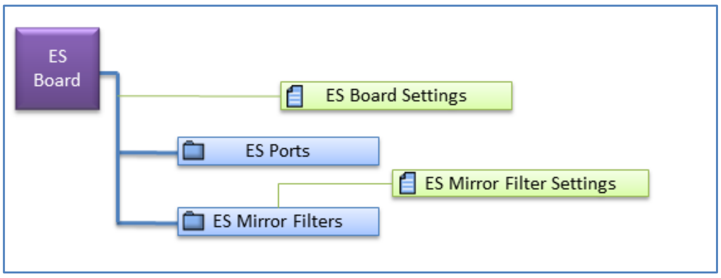

SIP
(4) SAS
SIP SAS Settings
SAS Registration Manipulation
SAS Registration Manipulation Settings

8.8 Ethernet Switch Board's

This section describes the Mediant 5000 and Mediant 8000 Ethernet switch boards' configuration screens and the link's status.

8.8.1 Navigation Hierarchy

Figure 8-42: ES Board Navigation Hierarchy



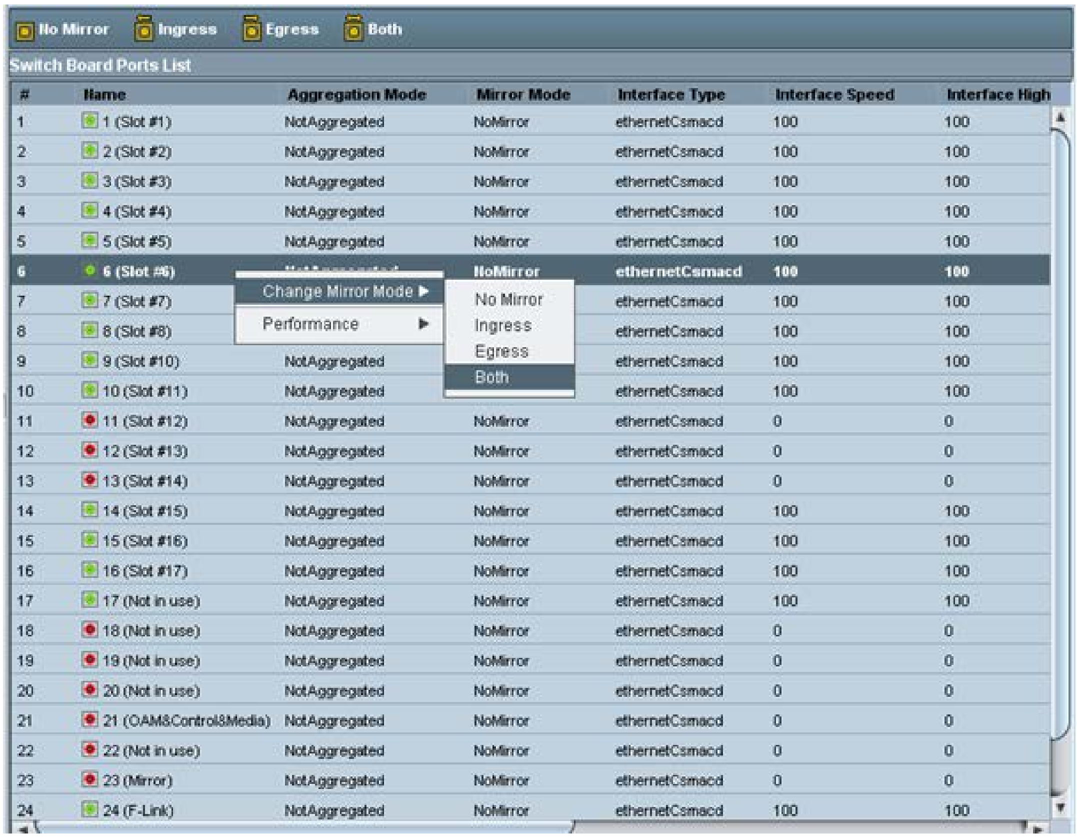
8.8.2 Links' Status

Ethernet Switch boards populate slots 3 and 4 in the Mediant 5000 Media Gateway and slots 9 and 19 in the Mediant 8000 Media Gateway Each contains a maximum of 26 links, of which 19 are used internally, two externally from/to the Gigabit Ethernet link, and five can be made available if a dedicated RTM is inserted behind the ES board.

➢ To determine the status of an Ethernet Switch board's link:

1. In the MG Tree, click a gateway containing the Ethernet Switch board whose link properties you want to determine.
2. Double-click the Ethernet Switch board; the Switch Links Status screen opens:

Figure 8-43: Switch Links Status Screen



#	Name	Aggregation Mode	Mirror Mode	Interface Type	Interface Speed	Interface High
1	🟩 1 (Slot #1)	NotAggregated	NoMirror	ethernetCsmacd	100	100
2	🟩 2 (Slot #2)	NotAggregated	NoMirror	ethernetCsmacd	100	100
3	🟩 3 (Slot #3)	NotAggregated	NoMirror	ethernetCsmacd	100	100
4	🟩 4 (Slot #4)	NotAggregated	NoMirror	ethernetCsmacd	100	100
5	🟩 5 (Slot #5)	NotAggregated	NoMirror	ethernetCsmacd	100	100
6	🟩 6 (Slot #6)	NotAggregated	NoMirror	ethernetCsmacd	100	100
7	🟩 7 (Slot #7)			ethernetCsmacd	100	100
8	🟩 8 (Slot #8)			ethernetCsmacd	100	100
9	🟩 9 (Slot #10)	NotAggregated		ethernetCsmacd	100	100
10	🟩 10 (Slot #11)	NotAggregated		ethernetCsmacd	100	100
11	🟥 11 (Slot #12)	NotAggregated	NoMirror	ethernetCsmacd	0	0
12	🟥 12 (Slot #13)	NotAggregated	NoMirror	ethernetCsmacd	0	0
13	🟥 13 (Slot #14)	NotAggregated	NoMirror	ethernetCsmacd	0	0
14	🟩 14 (Slot #15)	NotAggregated	NoMirror	ethernetCsmacd	100	100
15	🟩 15 (Slot #16)	NotAggregated	NoMirror	ethernetCsmacd	100	100
16	🟩 16 (Slot #17)	NotAggregated	NoMirror	ethernetCsmacd	100	100
17	🟩 17 (Not in use)	NotAggregated	NoMirror	ethernetCsmacd	100	100
18	🟥 18 (Not in use)	NotAggregated	NoMirror	ethernetCsmacd	0	0
19	🟥 19 (Not in use)	NotAggregated	NoMirror	ethernetCsmacd	0	0
20	🟥 20 (Not in use)	NotAggregated	NoMirror	ethernetCsmacd	0	0
21	🟥 21 (OAM&Control&Media)	NotAggregated	NoMirror	ethernetCsmacd	0	0
22	🟥 22 (Not in use)	NotAggregated	NoMirror	ethernetCsmacd	0	0
23	🟥 23 (Mirror)	NotAggregated	NoMirror	ethernetCsmacd	0	0
24	🟩 24 (F-Link)	NotAggregated	NoMirror	ethernetCsmacd	100	100

The figure above shows the status of each link in the Switch Links Status screen of the Mediant 8000 (the screen for the Mediant 5000 is similar), mapping which link is connected to each board. The mapping differs between the two gateways. The following information is displayed for each switch board link:

- Name and Status, where status can be one of the following:
  - Green - OK
  - Red - Failed
  - Yellow - Minor
  - Gray - Not connected
- Aggregation Mode, which can be 'Not Aggregated', 'Aggregated 2' or 'Aggregated 3'. This indicates that up to three up links can be aggregated together.
- Mirror Mode: No Mirror, Ingress, Egress, Both.
- Interface Type is always defined as EthernetCsmacd
- Interface speed: An estimate of the interface's current bandwidth, in bits per second.
- Interface High Speed: The current interface bandwidth (1 in units of megabits).
- Interface MTU: The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces used to transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface.

- Interface Mac Address
- Admin State: Locked or Unlocked
- Op State: Operational State, Enabled or Disabled
- Severity: Critical, Major, Minor, Warning, Clear or Indeterminate.

8.8.3 Ethernet Link Actions

This section describes how to perform Ethernet link actions.

➢ **To perform Ethernet link actions:**

- Select one or multiple Ethernet links and right-click; a popup menu listing available Ethernet Link Actions is displayed. Available actions are as follows:
    - Change Mirror Mode
        - No Mirror
        - Ingress
        - Egress
        - Both
    - Performance
        - Display Real Time PMs
        - Display Historical PMs

9 Mediant 9000

This section describes the Mediant 9000 status pane and provisioning.

9.1 Supported Configuration

The EMS supports the following product configuration:

- Standalone (Simplex) Mediant 9000
- High Availability-HA (1+ 1) Mediant 9000

9.2 Initial Configuration

Refer to the *Mediant 9000 SBC User's Manual* for the initial gateway configuration.

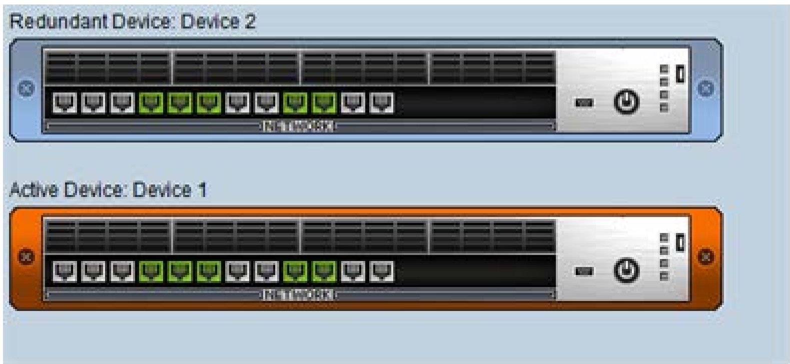
9.3 Status Pane

This Status pane provides the following information:

- Separate device statuses are displayed for the active device and redundant device.
- Mediant 9000 SBC device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figure below displays the Mediant 9000 SBC HA status pane.

Figure 9-1: Mediant 9000 SBC Status Pane

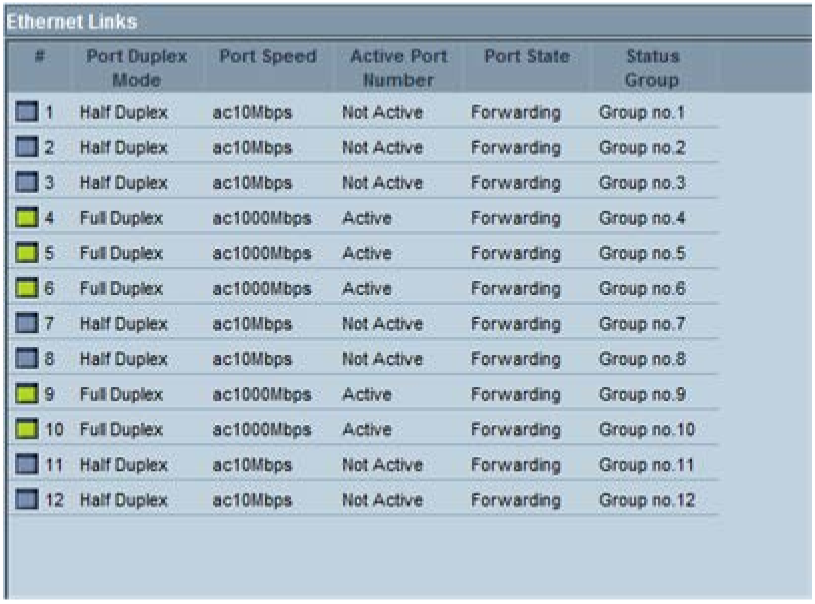


Gigabit Ethernet port status icons:

- 🟩 (green): Ethernet link is working
- ⬜ (gray): Ethernet link is not connected

Double-click these icons, and then in the Navigation pane, select **Ethernet Table**; the Ethernet Table screen is displayed.

Figure 9-2: Ethernet Table-Mediant 9000 SBC



Ethernet Links

#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Status Group
🟦 1	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.1
🟦 2	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.2
🟦 3	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.3
🟩 4	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.4
🟩 5	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.5
🟩 6	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.6
🟦 7	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.7
🟦 8	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.8
🟩 9	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.9
🟩 10	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.10
🟦 11	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.11
🟦 12	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.12

9.4 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The Mediant 9000 navigation hierarchy links are shown in the schema below.

Figure 9-3: Mediant 9000 and Software SBC (Part-1)

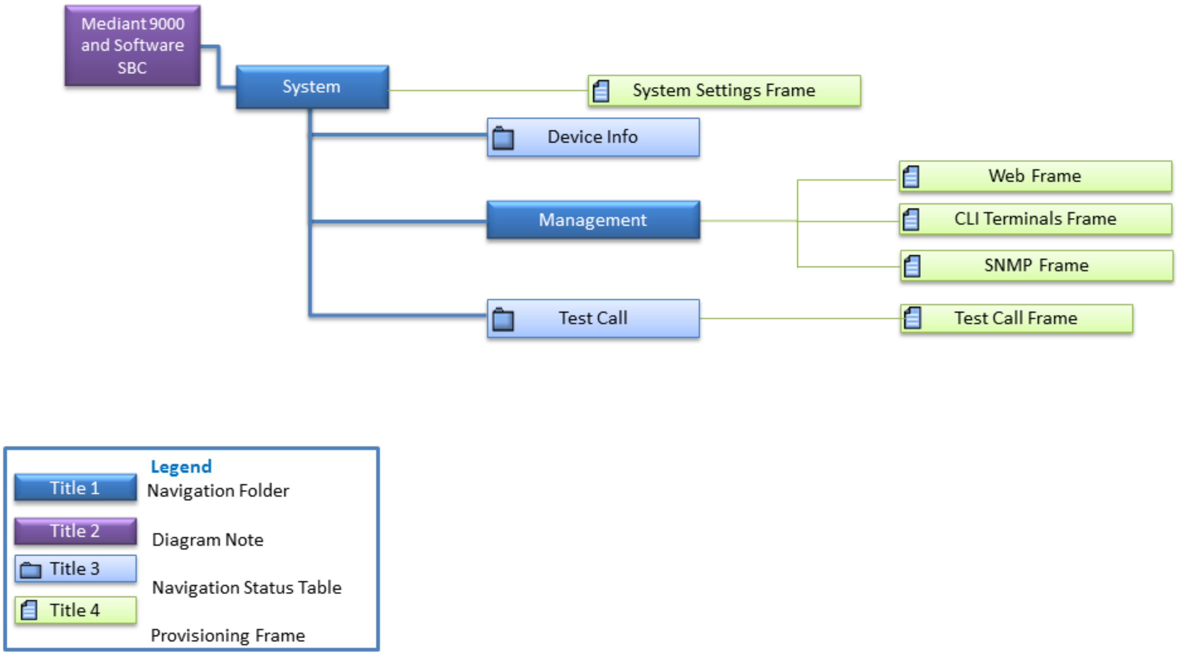


Figure 9-4: Mediant 9000 and Software SBC (Part-2)

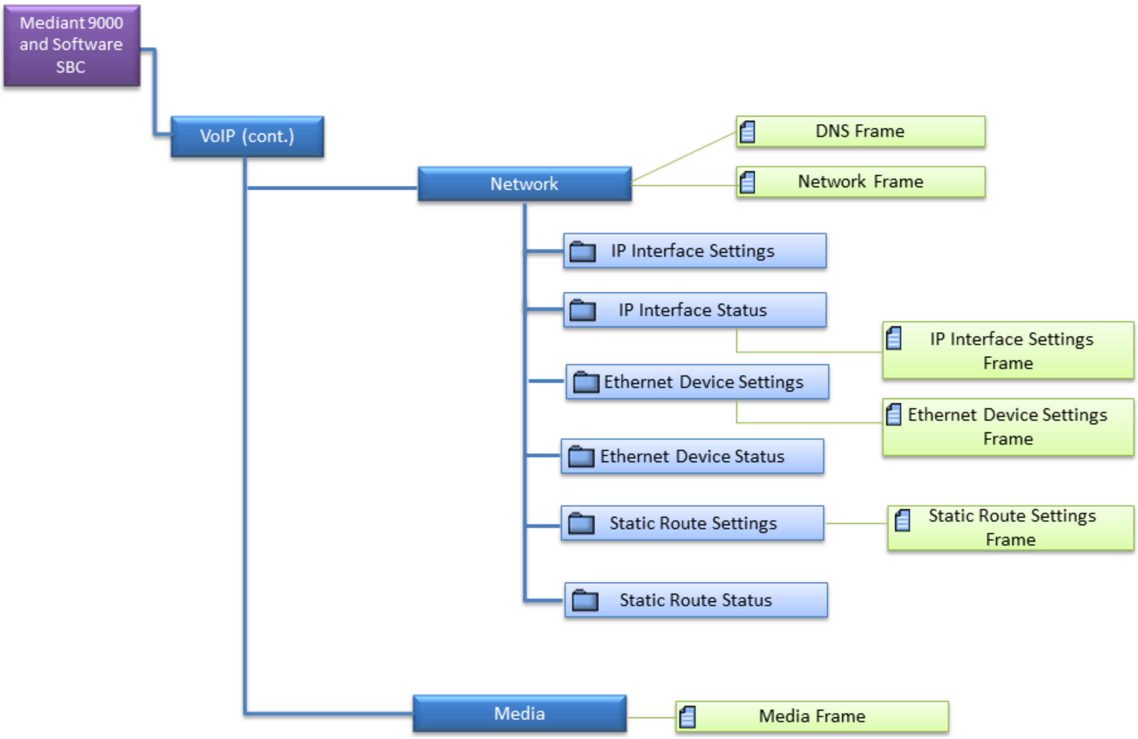


Figure 9-5: Mediant 9000 and Software SBC (Part-3)

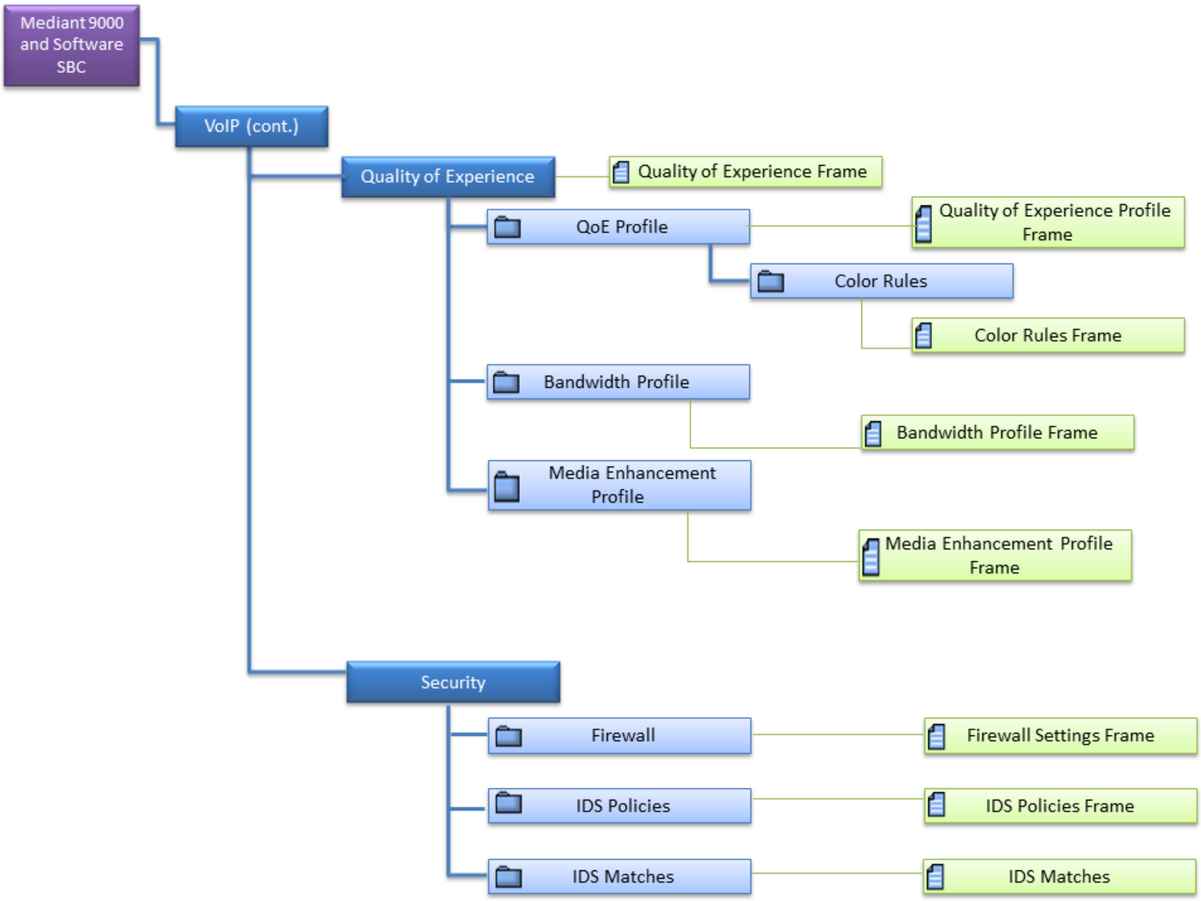


Figure 9-6: Mediant 9000 and Software SBC (Part-4)

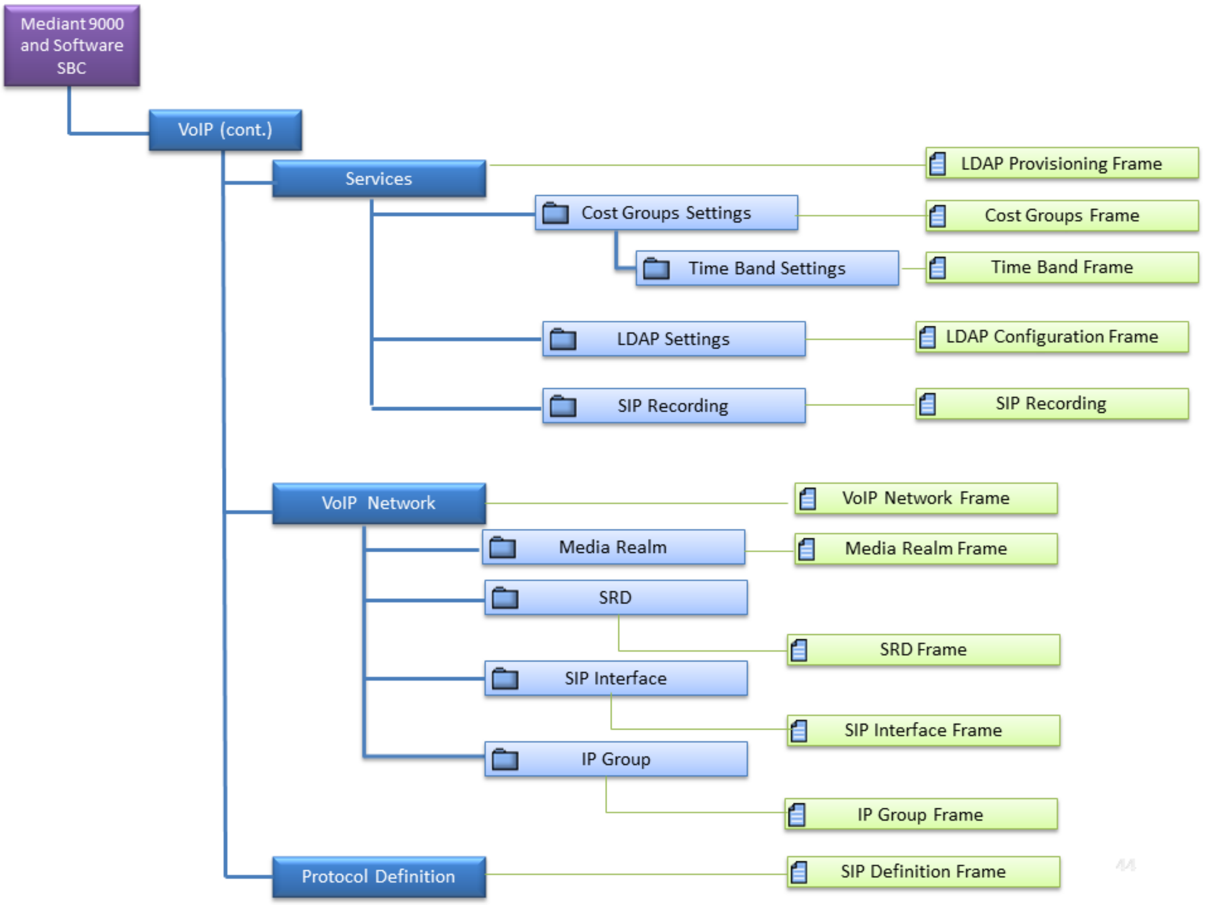


Figure 9-7: Mediant 9000 and Software SBC (Part-5)

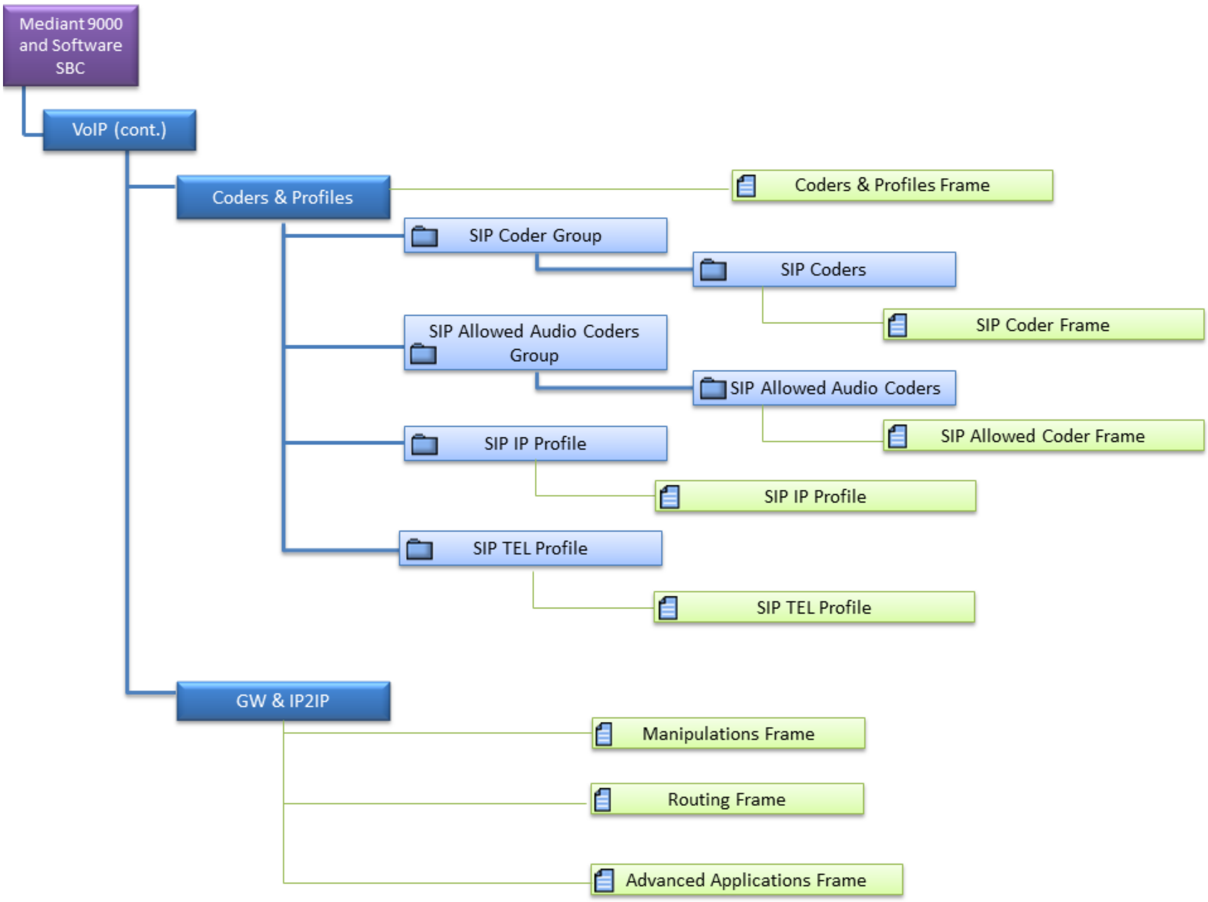
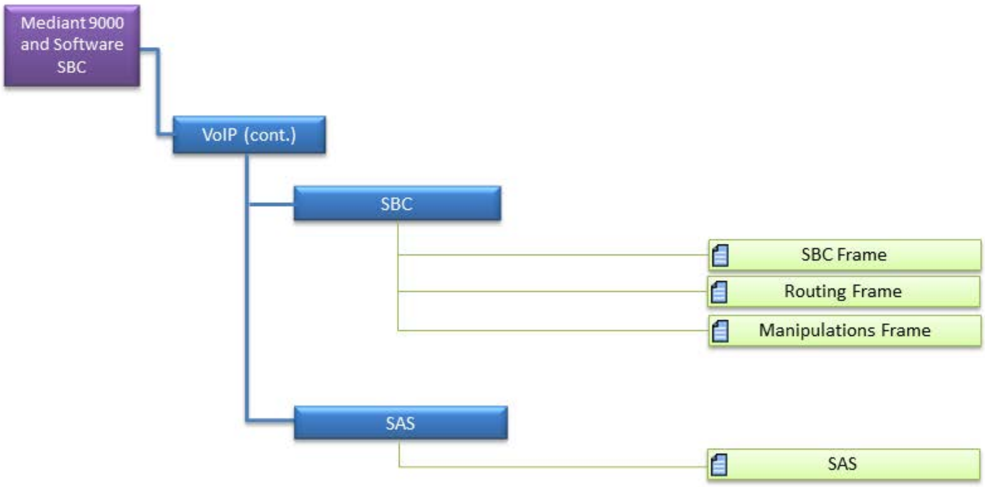


Figure 9-8: Mediant 9000 and Software SBC (Part-6)



9.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

10 Mediant Software SBC Products

This section describes the Mediant Software SBC products (Mediant SE SBC, Mediant SE-H SBC, Mediant VE SBC and Mediant VE-H SBC) status and provisioning.

10.1 Supported Configuration

The EMS supports the following product configurations:

- Standalone (Simplex)
- High Availability-HA (1+ 1)

10.2 Initial Configuration

Refer to the *Mediant Software SBC User's Manual* for the initial gateway configuration.

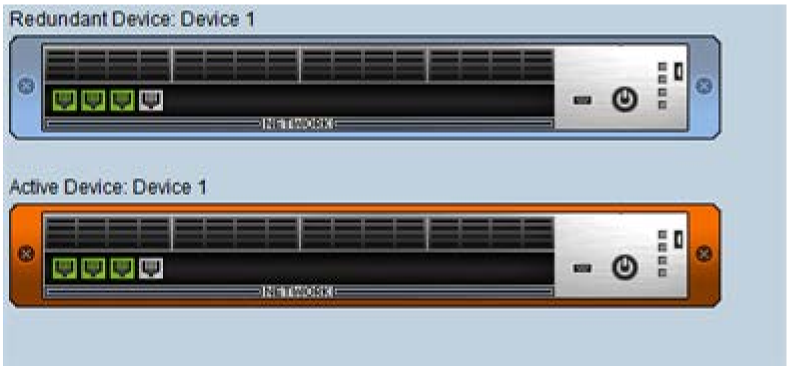
10.3 Status Pane

This Status pane provides the following information:

- Separate device statuses are displayed for the active device and redundant device.
- Mediant Software SBC device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figure below displays the Mediant Software SBC HA status pane.

Figure 10-1: Software SBC Status Pane

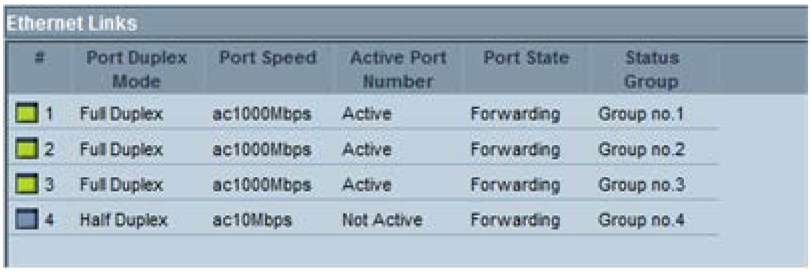


Gigabit Ethernet port status icons:

- 🟩 (green): Ethernet link is working
- ▨ (gray): Ethernet link is not connected

Click these icons, and then in the Navigation pane, select **Ethernet Table**; the Ethernet Table screen is displayed.

Figure 10-2: Ethernet Table-Software SBC



Ethernet Links

#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Status Group
🟩 1	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.1
🟩 2	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.2
🟩 3	Full Duplex	ac1000Mbps	Active	Forwarding	Group no.3
🟦 4	Half Duplex	ac10Mbps	Not Active	Forwarding	Group no.4

10.4 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The Mediant Software SBC product's navigation hierarchy links are described on page 162.

10.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

11 Mediant 4000

This section describes the Mediant 4000 status pane and provisioning.

11.1 Supported Configuration

The EMS supports the following product configuration:

- Standalone (Simplex) Mediant 4000
- High Availability-HA (1+ 1) Mediant 4000

11.2 Initial Configuration

Refer to the *Mediant 4000 SBC User's Manual* for the Gateway iinitial Configuration.

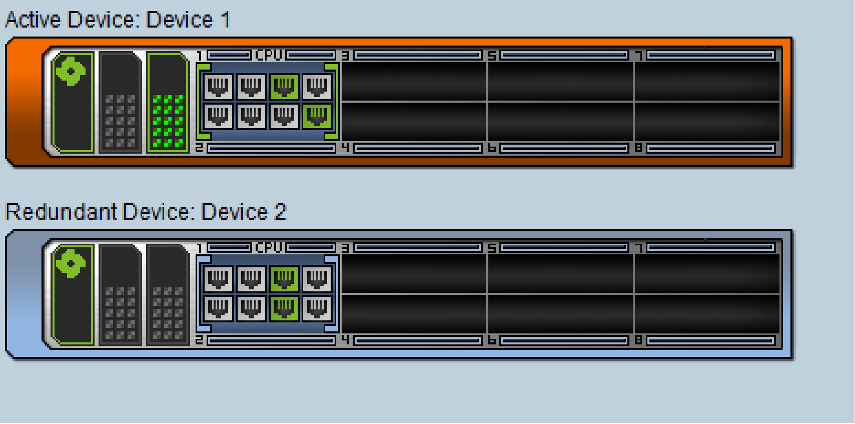
11.3 Status Pane

This Status pane provides the following information:

- Hardware components status support, including chassis LEDs, fan status and speed, power supplies and PEM status. Board temperature is indicated.
- Separate device statuses are displayed for the active device and redundant device.
- Mediant 4000 device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figure below displays the Mediant 4000 SBC HA status pane.

Figure 11-1: Mediant 4000 SBC HA Status Pane



- **CPU Module Status**

  The CPU module location is displayed in the EMS status screen.

- **Fan Tray status**

Color convention: Severity - indicates the fan tray's severity level. Green = Clear; White = Indeterminate; Blue = Warning; Yellow = Minor; Orange = Major; Red = Critical.

- **Fan status**

  The status of the 8 fans are read as follows:

  1. Bottom Front Fan
  2. Bottom Middle Fan
  3. Bottom Middle Fan
  4. Bottom Rear Fan
  5. Top Front Fan
  6. Top Middle Fan
  7. Top Middle Fan
  8. Top Rear Fan

  Color convention: Red = Failed; Green = OK

- **Power Supplies Status**

  There are 2 Power Supplies: PS Top and PS Bottom

  Color convention: Severity - indicates the power supply's severity level. Green = Clear; White = Indeterminate; Blue = Warning; Yellow = Minor; Orange = Major; Red = Critical.

  When a Manual or Automatic switchover or a software upgrade process occurs, users view a status screen indicating that the redundant board is now failed and notifying that the configuration should not be applied to the system. The figure below shows an example of this status screen and the warning notification.

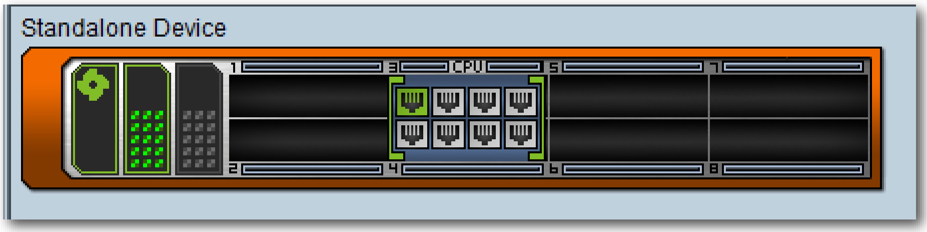
11.3.1 Hardware Component Status in Table View

This section describes the Hardware Component Status in Table View.

➢ To open the Hardware Component Status in Table View:

- Double-click the hardware component (not on the active TP itself as clicking on the active TP board opens the Trunk Tables Status table).

Figure 11-2: Mediant 4000 Hardware Components Status Pane



The device's Components Status pane graphically represents the status of each component using the same color conventions as those used in the Status pane, and displays additional information in the Information column. The following information is displayed:

- **Board status and information**
  - Board type
  - HA Status – active or redundant
  - Temperature, in Celsius (only for the TP board)
- **Fan Tray status and information**
  - Fan tray ID and version
  - Pre-provisioned speed
- **Fan status**

  The status of the 8 fans are read as follows:

  For each fan: Current speed, in revolutions per minute (rpm)
- **Power Supplies Status only**
- **PEM Status and information**

  There are 2 PEMs: PEM Top and PEM Bottom
  - Status: Color convention: Gray = Doesn't Exist; Red = Minor severity, power cable is missing; Green = Clear Severity
  - Information : PEM ID and version

11.4 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The figure below shows the navigation hierarchy links used to provision the Mediant 4000 SBC.

Figure 11-3: Navigation Hierarchy Links - Mediant 4000 (Part 1)

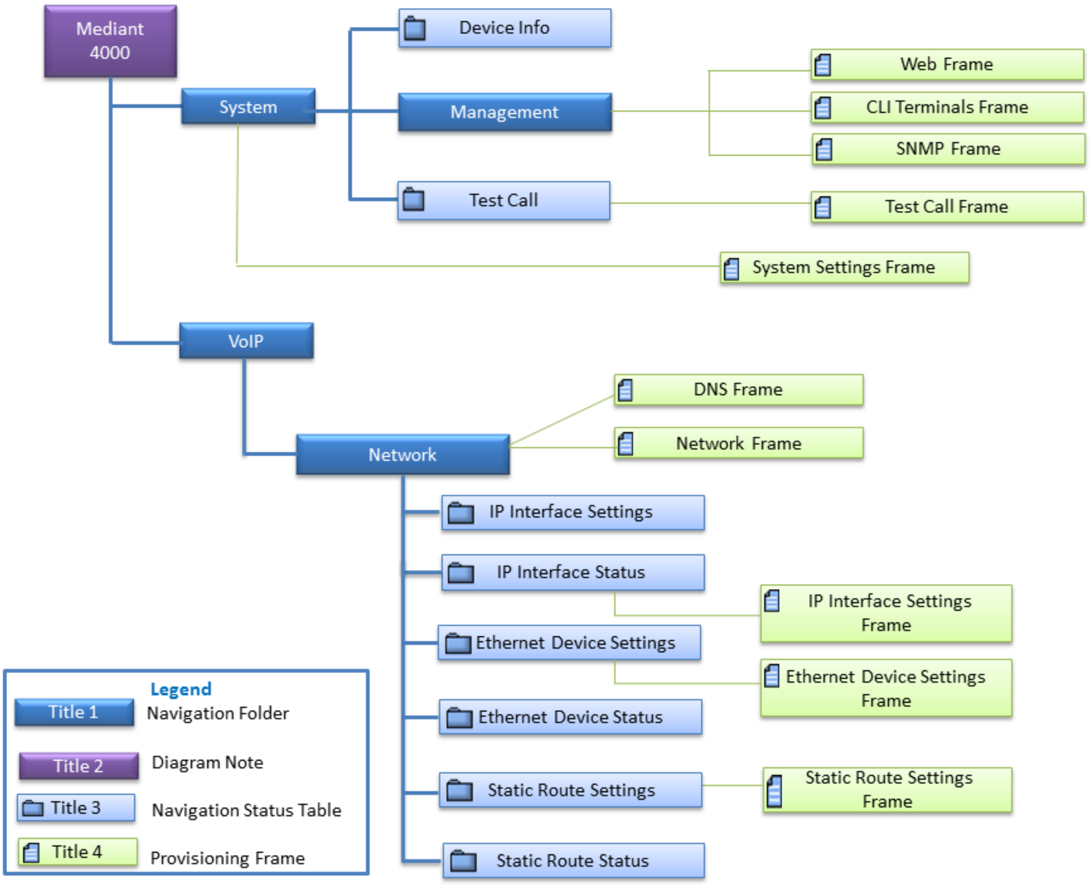


Figure 11-4: Navigation Hierarchy Links - Mediant 4000 (Part 2)

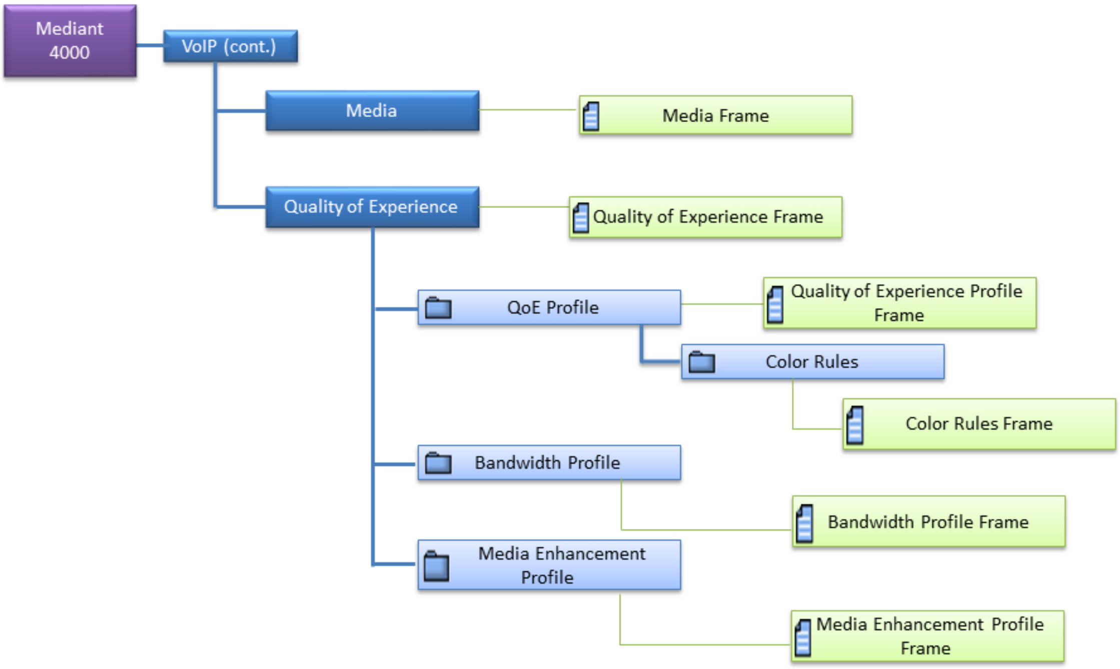


Figure 11-5: Navigation Hierarchy Links - Mediant 4000 (Part 3)

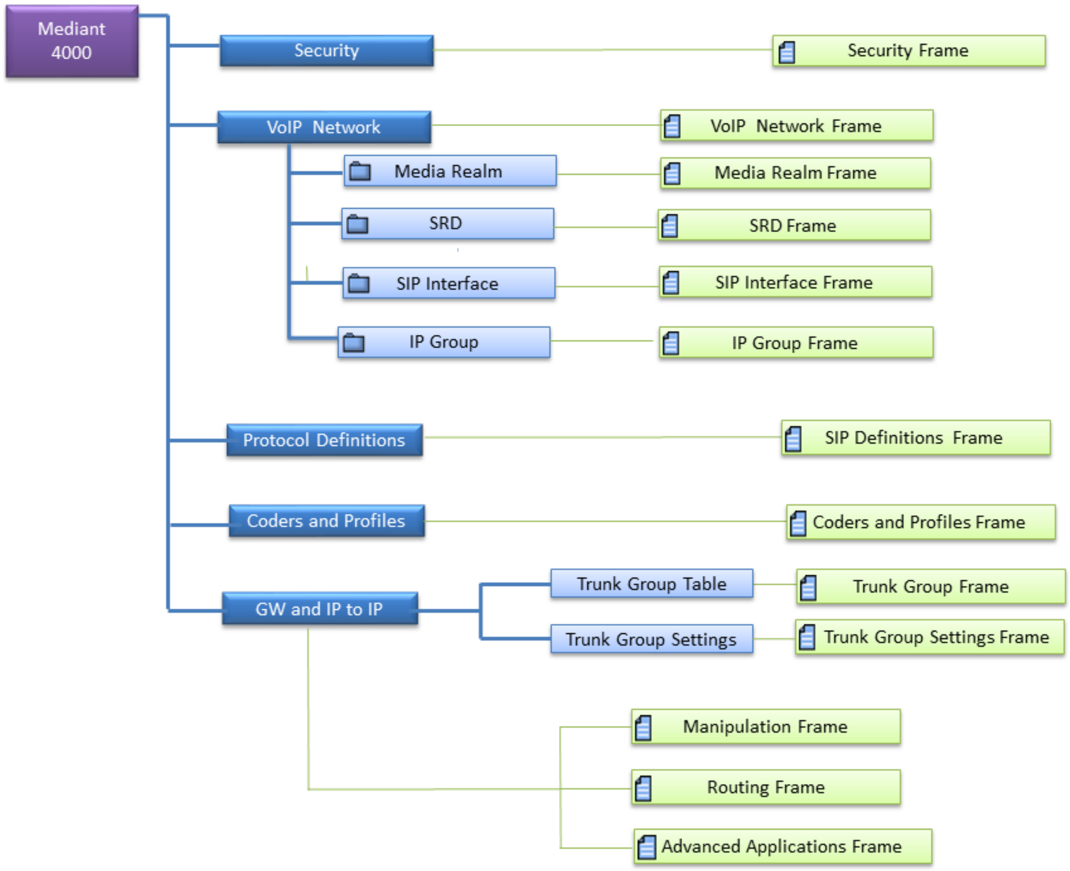
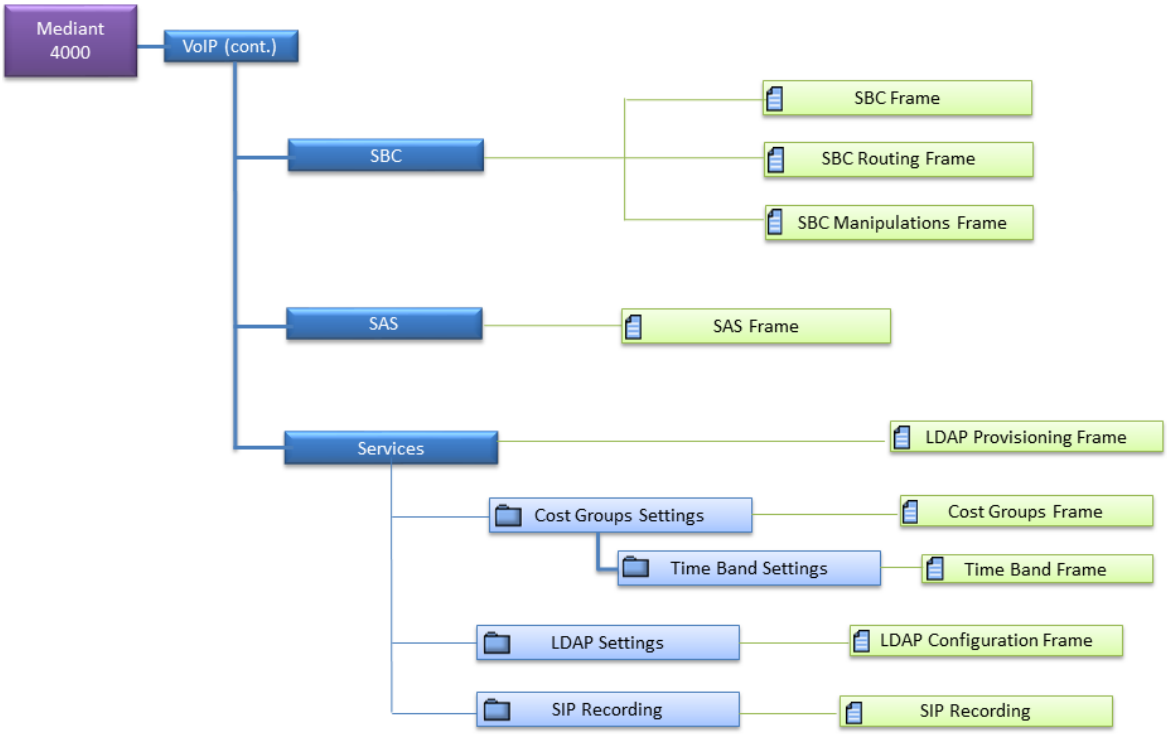


Figure 11-6: Navigation Hierarchy Links - Mediant 4000 (Part 4)



See Section 'Provisioning Concepts' on page 222 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

11.5 Executable Actions

The following maintenance actions are specific the Mediant 4000 Gateway:

- SwitchOver
- Reset Redundant Device

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

Reader's Notes

12 Mediant 3000

This section describes the Mediant 3000 status pane and provisioning.

12.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Mediant 3000 with TP-6310 boards
- Mediant 3000 with TP-8410 boards

12.2 Initial Configuration

Refer to the *Mediant 3000 User Manual* for the Gateway Initial Configuration.

12.3 Status Pane

EMS version 5.0 and above supports the Mediant 3000 Media Gateway: HA (1+ 1) and Simplex mode.

- Hardware components status support, including chassis LEDs, fan status and speed, power supplies and PEM status. Board temperature is indicated.
- TP-6310 or TP-8410 board active / redundant coloring is supported
- TP-6310 or TP-8410 and Alarm Card LEDs are supported
- Commands supported: Switchover; Reset whole chassis or each board (on TP board only).

The figures below display the Mediant 3000 HA status panes.

Figure 12-1: Mediant 3000 6310 Status Pane

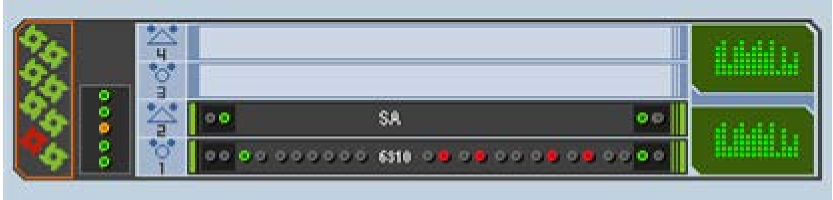
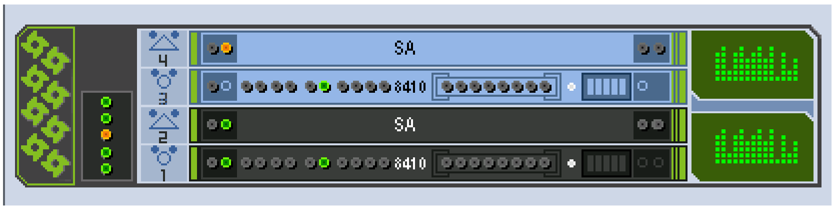


Figure 12-2: Mediant 3000 8410 Status Pane



12.3.1 High Availability (HA) (1+1) Mode

The Information pane indicates the Gateway's / Server's name, IP address, software version, and control protocol type. It also includes hardware, software or configuration mismatch if any problem is detected. “Reset Needed” indicates that the operator changed offline parameters and that to apply these parameters to the gateway/server, a Reset must be performed.

The Status screen representatively displays 4 boards: Alarm cards (slots 2 and 4) and the TP-6310 boards (slots 1 and 3). The Status screen also representatively displays the fan tray and fans status and the power supplies. If the connection to the active VoP module fails, the status of the gateway/server is indicated as failed.

The Mediant 3000 Status pane includes the following:

- **VoP Boards status**

  Background color: Dark Gray = Active board; Blue = Redundant board

  Upper and lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity

  The figures below display the TP-6310 board status Active/Redundant respectively.

Figure 12-3: 6310 Active Board Status

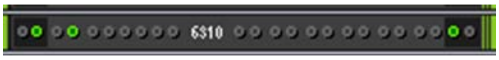
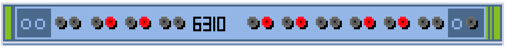


Figure 12-4: 6310 Redundant Board Status

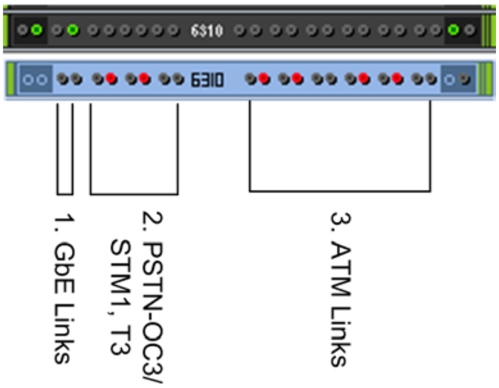


Background color: Dark Gray = Active board; Blue = Redundant board

Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity, Yellow = Minor Severity, Blue = Warning Severity, White = Indeterminate Severity

TP Switchover:
The active TP board, after switchover, is marked in a background black color without any LEDs, with a red or green frame around the board according to its Operational State (green = enabled boards, red = disabled boards). A redundant TP board, which becomes active after switchover, is marked in a background blue color, with LEDs for activated trunks.

Figure 12-5: 6310 Board-LED Status



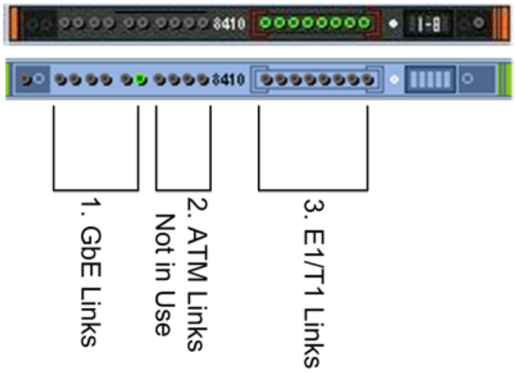
Legend

1 = the first two LEDs represent the GbE (Gigabit Ethernet) status

2 = six LEDs representing PSTN Interface status (for OC3/STM1, four LEDs are relevant; for T3, all six LEDs are relevant)

3 = twelve LEDs representing ATM Interface status (not in use)

Figure 12-6: 8410 Board LED Status



Legend

1. = six LEDs representing the GbE (Gigabit Ethernet) status

2.= four LEDs representing ATM LEDs which are not in use

3.= eight LEDs representing E1/T1 LEDs

Trunk (E1/T1) LED color convention: Red = Disabled; Green = Enabled; Gray = Locked

- **TP LEDs status**

  PSTN and ATM LEDs color convention:

  Rx /Tx LED: Red = Disabled, Green = Link OK, Yellow = Protection Link, Gray = No Link

  Alarm LED: Gray = Normal Link, Red = LOS, LOF, AIS, RDI

- **Alarm Card Status - each Alarm Card is represented as a board in the shelf**

  Background color: Dark Gray = Active board; Blue = Redundant board

  Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity

- **Fan Tray status**

  Color convention: Severity - indicates the fan tray's severity level. Green = Clear; White = Indeterminate; Blue = Warning; Yellow = Minor; Orange = Major; Red = Critical.

- **Shelf LEDs**

  Five LEDs summarize the Mediant 3000 status (from top to bottom):

  - System: Red = System Error occurred; Green = OK Off (currently unsupported)
  - Critical: Red = Critical Error occurred; Green = OK
  - Major: Orange = Major Error occurred; Green = OK
  - Minor: Orange = Minor Error occurred; Green = OK
  - Shelf: Red = Critical Error occurred; Orange = Major Error occurred; Green = OK; Gray = Off (currently unsupported)

- **Fan status**

  The status of the 8 fans are read as follows:

  - Bottom Front Fan
  - Bottom Middle Fan
  - Bottom Middle Fan
  - Bottom Rear Fan
  - Top Front Fan
  - Top Middle Fan
  - Top Middle Fan
  - Top Rear Fan

  Color convention: Red = Failed; Green = OK

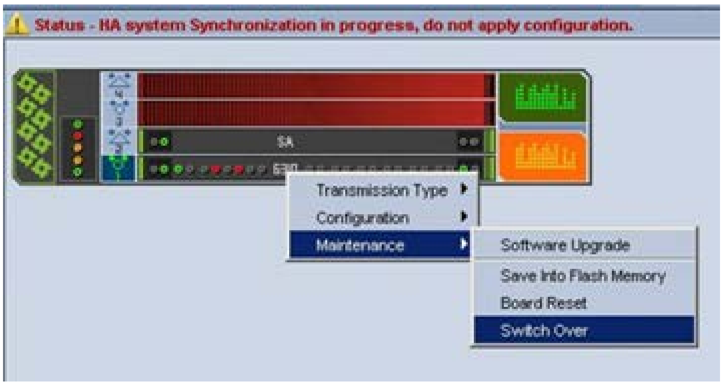
- **Power Supplies Status**

  There are 2 Power Supplies: PS Top and PS Bottom

  Color convention: Severity - indicates the power supply's severity level. Green = Clear; White = Indeterminate; Blue = Warning; Yellow = Minor; Orange = Major; Red = Critical.

When a Manual or Automatic switchover or a software upgrade process occurs, users view a status screen indicating that the redundant board is now failed and notifying that the configuration should not be applied to the system. The figure below shows an example of this status screen and the warning notification.

Figure 12-7: Status Screen Displaying Failed Redundant Boards and Warning Notification



Status - HA system Synchronization in progress, do not apply configuration.

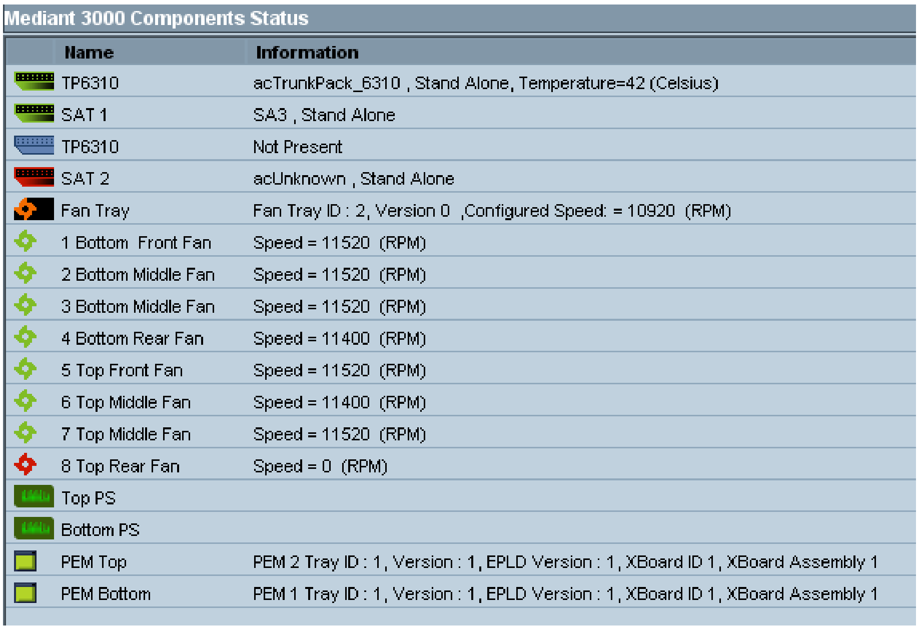
12.3.2 Hardware Component Status in Table View

This section describes the Hardware Component Status in Table View.

➢ To open the Hardware Component Status in Table View:

- Double-click the hardware component (not on the active TP itself as clicking on the active TP board opens the Trunk Tables Status table).

Figure 12-8: Mediant 3000 Hardware Components Status Pane



Mediant 3000 Components Status

	Name	Information
🟩	TP6310	acTrunkPack_6310 , Stand Alone, Temperature=42 (Celsius)
🟩	SAT 1	SA3 , Stand Alone
🟦	TP6310	Not Present
🟥	SAT 2	acUnknown , Stand Alone
🟧	Fan Tray	Fan Tray ID : 2, Version 0 ,Configured Speed: = 10920 (RPM)
🟩	1 Bottom Front Fan	Speed = 11520 (RPM)
🟩	2 Bottom Middle Fan	Speed = 11520 (RPM)
🟩	3 Bottom Middle Fan	Speed = 11520 (RPM)
🟩	4 Bottom Rear Fan	Speed = 11400 (RPM)
🟩	5 Top Front Fan	Speed = 11520 (RPM)
🟩	6 Top Middle Fan	Speed = 11400 (RPM)
🟩	7 Top Middle Fan	Speed = 11520 (RPM)
🟥	8 Top Rear Fan	Speed = 0 (RPM)
🟩	Top PS	
🟩	Bottom PS	
🟨	PEM Top	PEM 2 Tray ID : 1, Version : 1, EPLD Version : 1, XBoard ID 1, XBoard Assembly 1
🟨	PEM Bottom	PEM 1 Tray ID : 1, Version : 1, EPLD Version : 1, XBoard ID 1, XBoard Assembly 1

The device's Components Status pane graphically represents the status of each component using the same color conventions as those used in the Status pane, and presents additional information in the Information column. The following information is displayed:

- **Board status and information**
  - Board type (acMediant3000, or for Alarm Card – SA1, SA2, SA3)
  - HA Status – active or redundant
  - Temperature, in Celsius (only for the TP board)
- **Fan Tray status and information**
  - Fan tray ID and version
  - Pre-provisioned speed
- **Fan status**

  The status of the 8 fans are read as follows:

  For each fan: Current speed, in revolutions per minute (rpm)
- **Power Supplies Status only**
- **PEM Status and information**

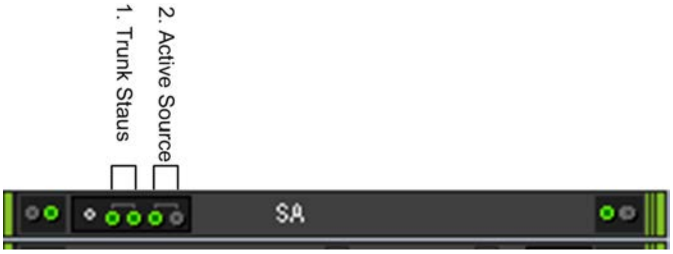
  There are 2 PEMs: PEM Top and PEM Bottom
  - Status: Color convention: Gray = Doesn't Exist; Red = Minor severity, power cable is missing; Green = Clear Severity
  - Information : PEM ID and version

12.3.3 Mediant 3000 TP-8410 SA BITS status

In the current EMS version, BITS status and provisioning is supported for the Mediant 3000 8410 configuration

The Mediant 3000 with TP-8410 boards which support an S A board with a BITs Timing module will have the following status screen:

Figure 12-9: Mediant 3000 SA Board Status

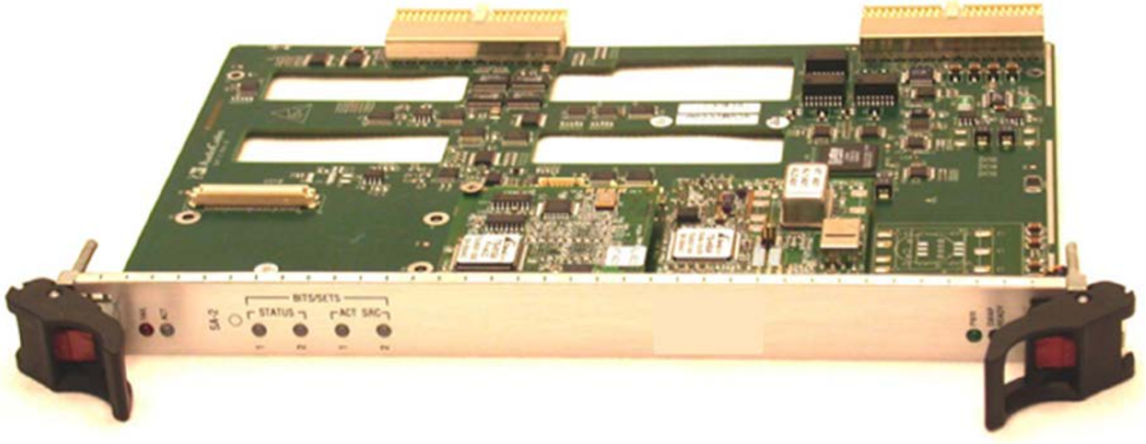


The LEDs are represented as follows:

- Trunk Status represents the status of Trunk A and Trunk B status correspondingly.
- Active Source displays which of the Trunks is the current active BITs clock source. In the figure above, Trunk A is the active clock source.

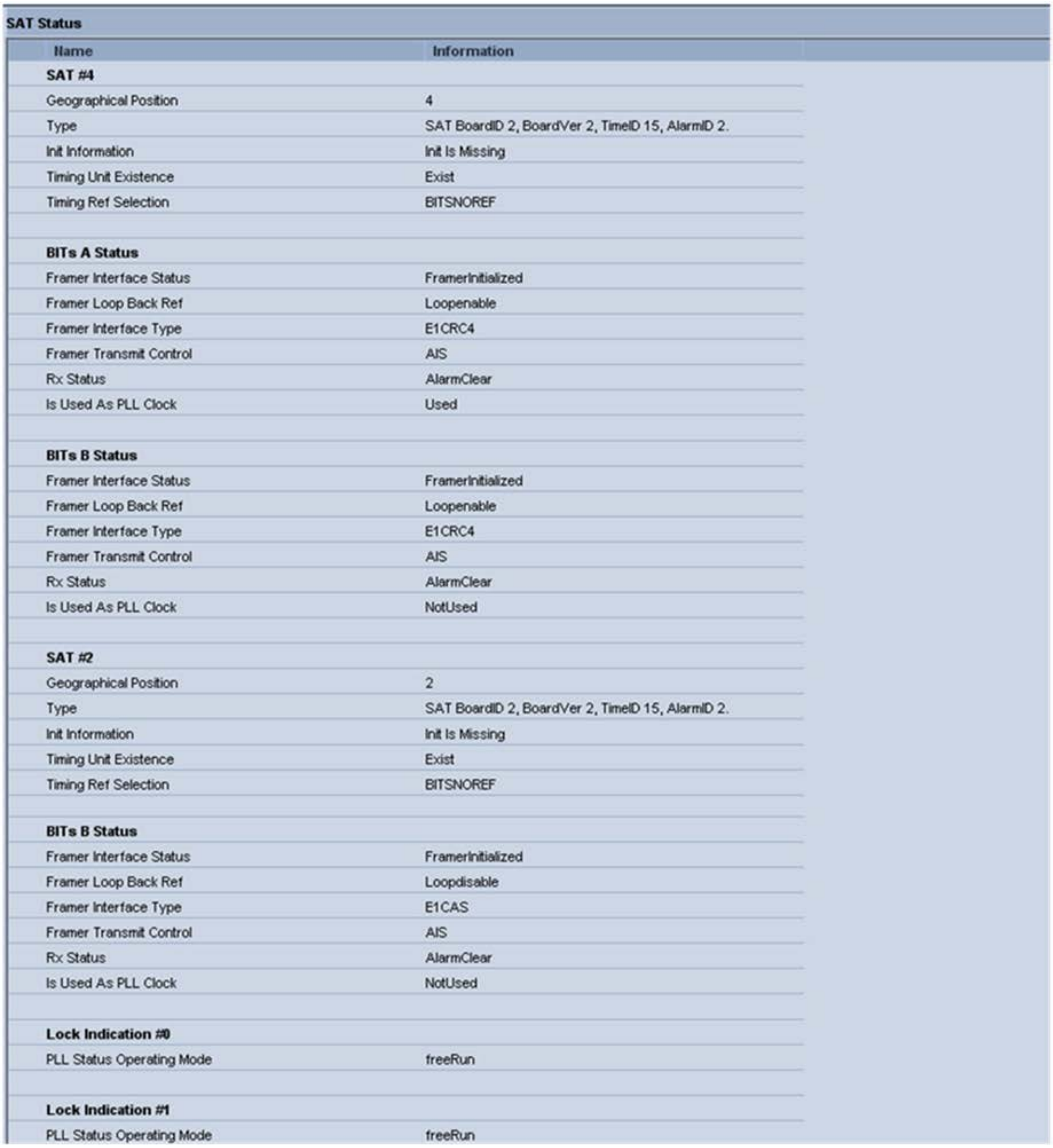
Green represents OK status, Red represents an a larm (problem), Grey -represents OFF

Figure 12-10: Mediant 3000 BITs Module



Double clicking the SA module drills down to status screen which includes additional information regarding both SA cards and BITS modules on each one of them, and PLL Lock indications.

Figure 12-11: Mediant 3000 SAT Status



SAT Status

Name	Information
SAT #4	
Geographical Position	4
Type	SAT BoardID 2, BoardVer 2, TimeID 15, AlarmID 2.
Init Information	Init Is Missing
Timing Unit Existence	Exist
Timing Ref Selection	BITSNOREF
BITs A Status	
Framer Interface Status	FramerInitialized
Framer Loop Back Ref	Loopenable
Framer Interface Type	E1CRC4
Framer Transmit Control	AIS
Rx Status	AlarmClear
Is Used As PLL Clock	Used
BITs B Status	
Framer Interface Status	FramerInitialized
Framer Loop Back Ref	Loopenable
Framer Interface Type	E1CRC4
Framer Transmit Control	AIS
Rx Status	AlarmClear
Is Used As PLL Clock	NotUsed
SAT #2	
Geographical Position	2
Type	SAT BoardID 2, BoardVer 2, TimeID 15, AlarmID 2.
Init Information	Init Is Missing
Timing Unit Existence	Exist
Timing Ref Selection	BITSNOREF
BITs B Status	
Framer Interface Status	FramerInitialized
Framer Loop Back Ref	Loopdisable
Framer Interface Type	E1CAS
Framer Transmit Control	AIS
Rx Status	AlarmClear
Is Used As PLL Clock	NotUsed
Lock Indication #0	
PLL Status Operating Mode	freeRun
Lock Indication #1	
PLL Status Operating Mode	freeRun

12.4 Physical and Logical Components Status and Provisioning

This section describes the Physical and Logical Components Status and Provisioning hierarchy.

12.4.1 Navigation Hierarchy

The gateways' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and s ub-links that are displayed in the Configuration pane.

The figures below shows the navigation hierarchy links used to provision the Mediant 3000-TP-8410 gateway.

Figure 12-12: Navigation Hierarchy Links-Mediant 3000-TP-8410 Part 1

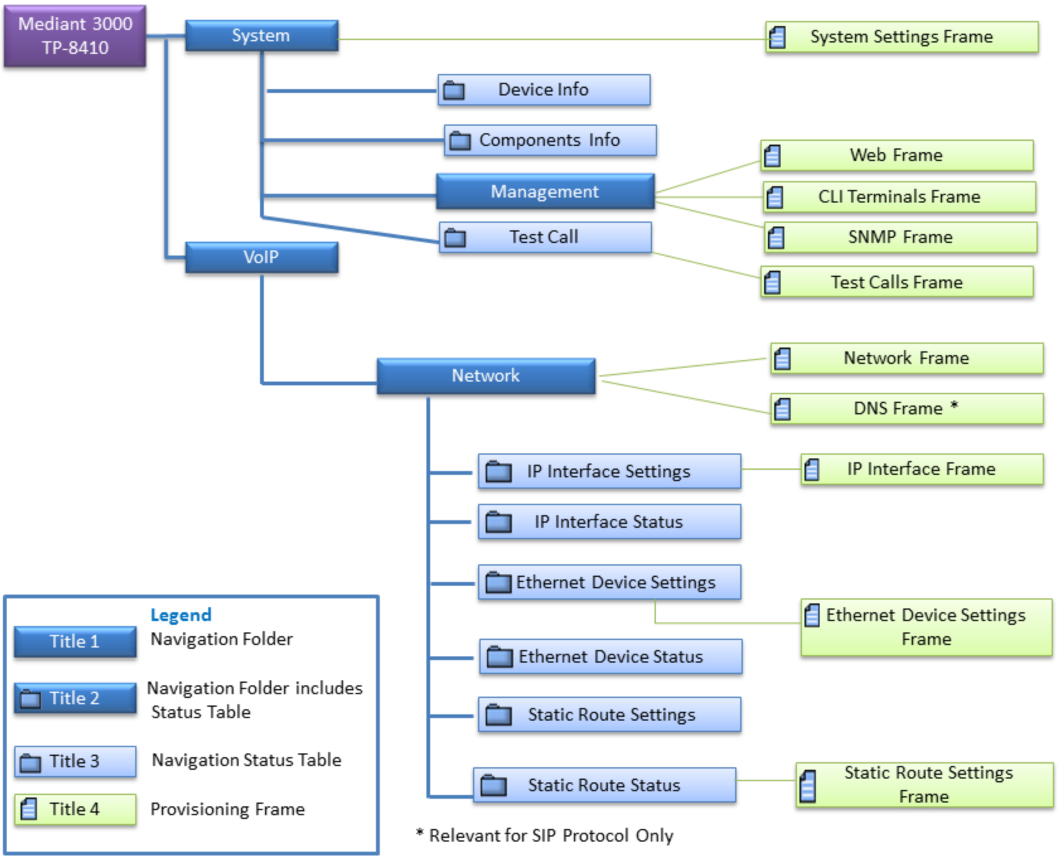


Figure 12-13: Navigation Hierarchy Links-Mediant 3000-TP-8410 Part 2

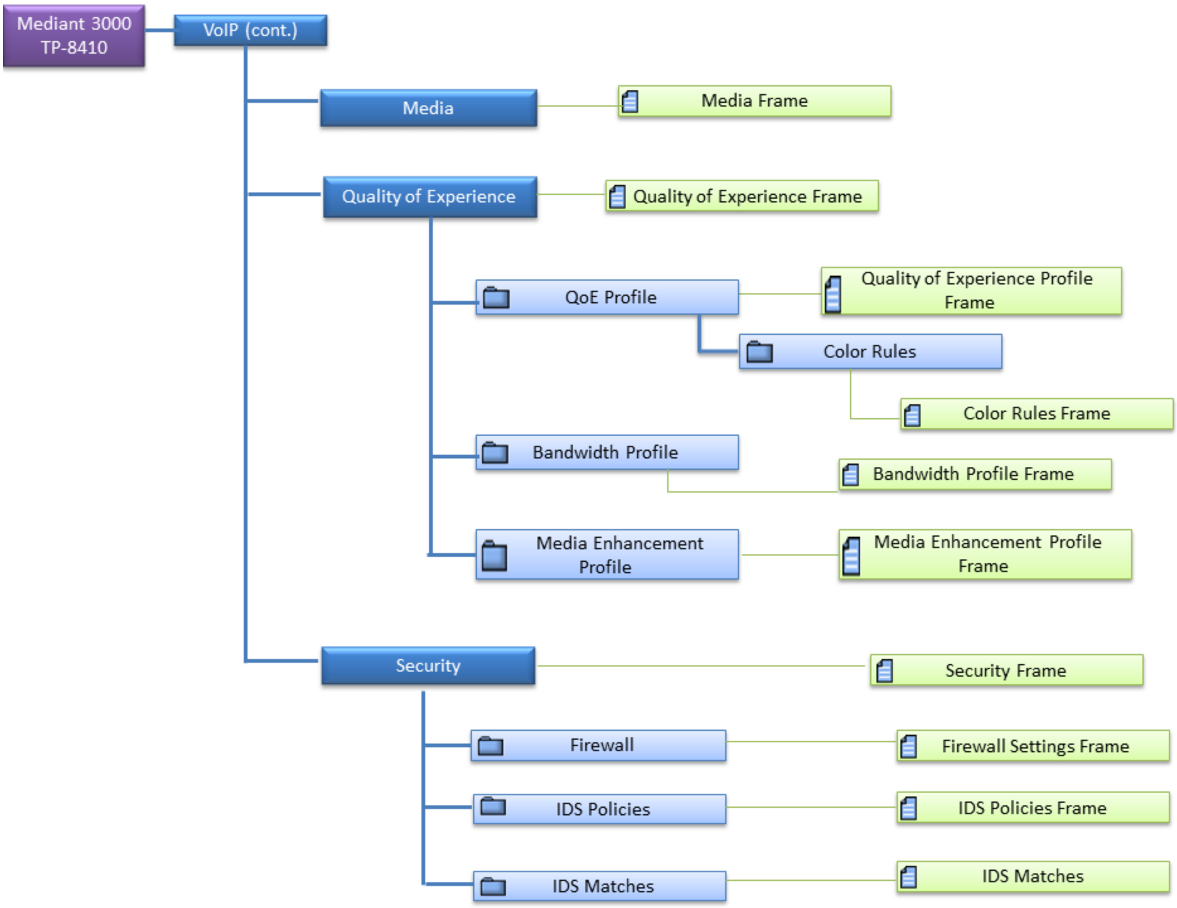
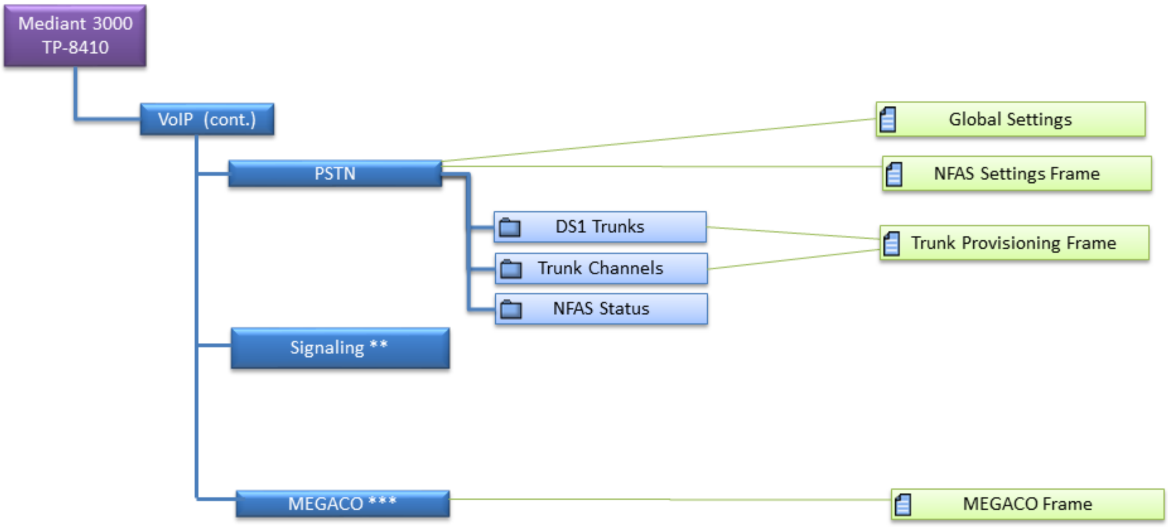


Figure 12-14: Navigation Hierarchy Links-Mediant 3000-TP-8410 Part 3



**Refer to Signaling Navigation Scheme for detailed lower levels

*** Relevant for MEGACO Protocol Only

Figure 12-15: Navigation Hierarchy Links-Mediant 3000-TP-6310 Part 1

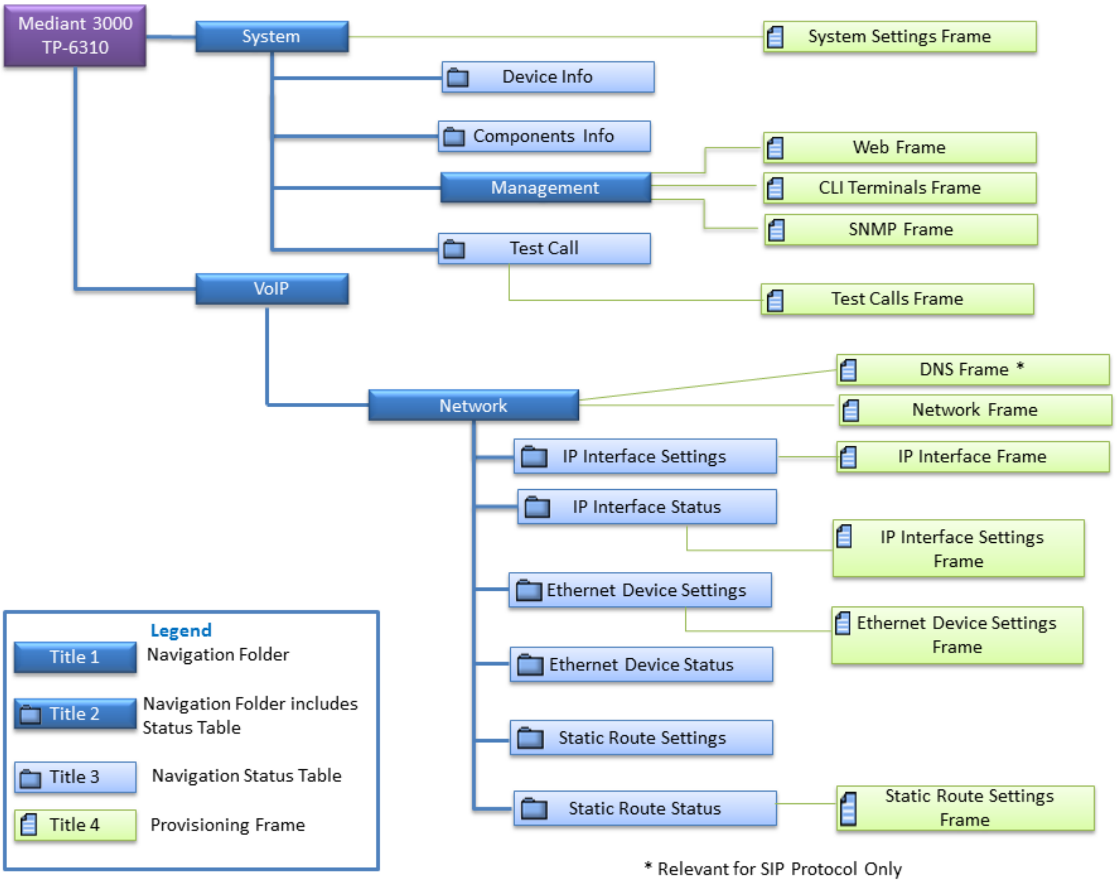


Figure 12-16: Navigation Hierarchy Links-Mediant 3000-TP-6310 Part 2

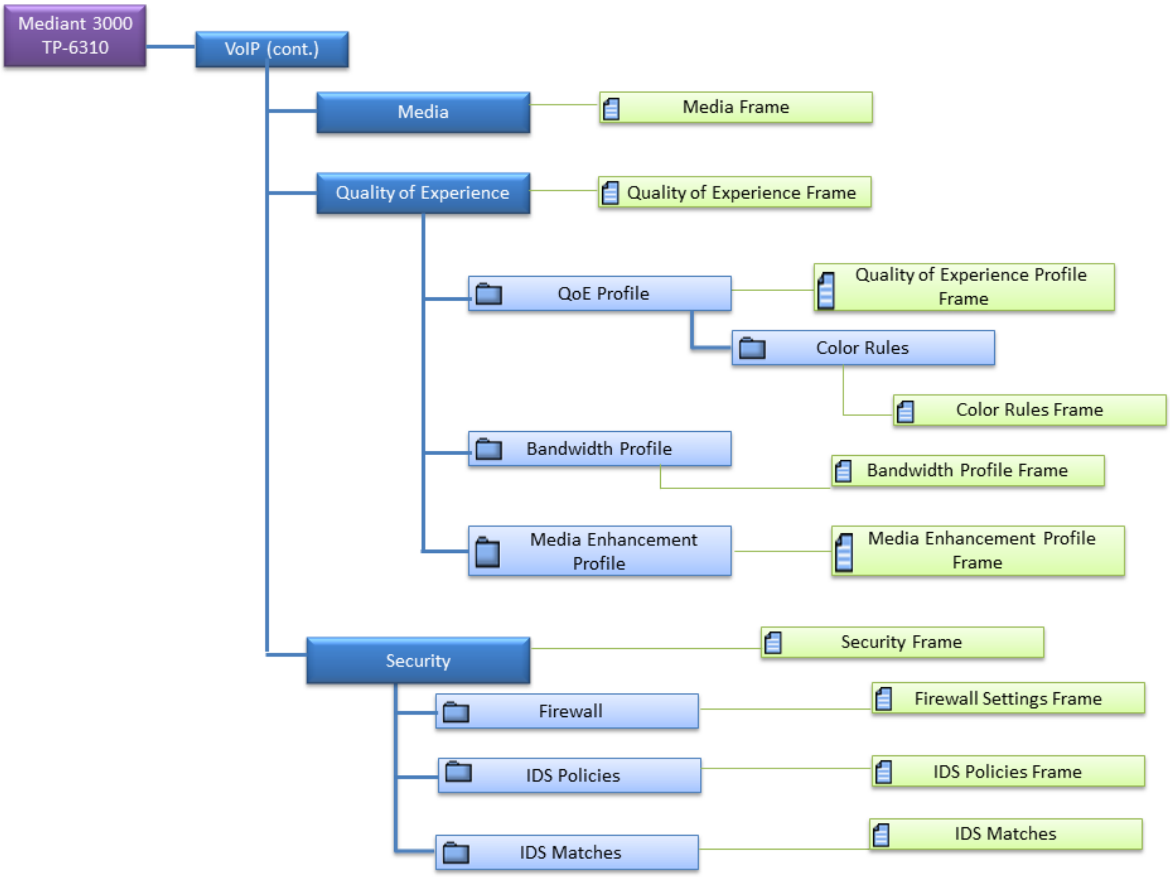


Figure 12-17: Navigation Hierarchy Links-Mediant 3000-TP-6310 Part 3

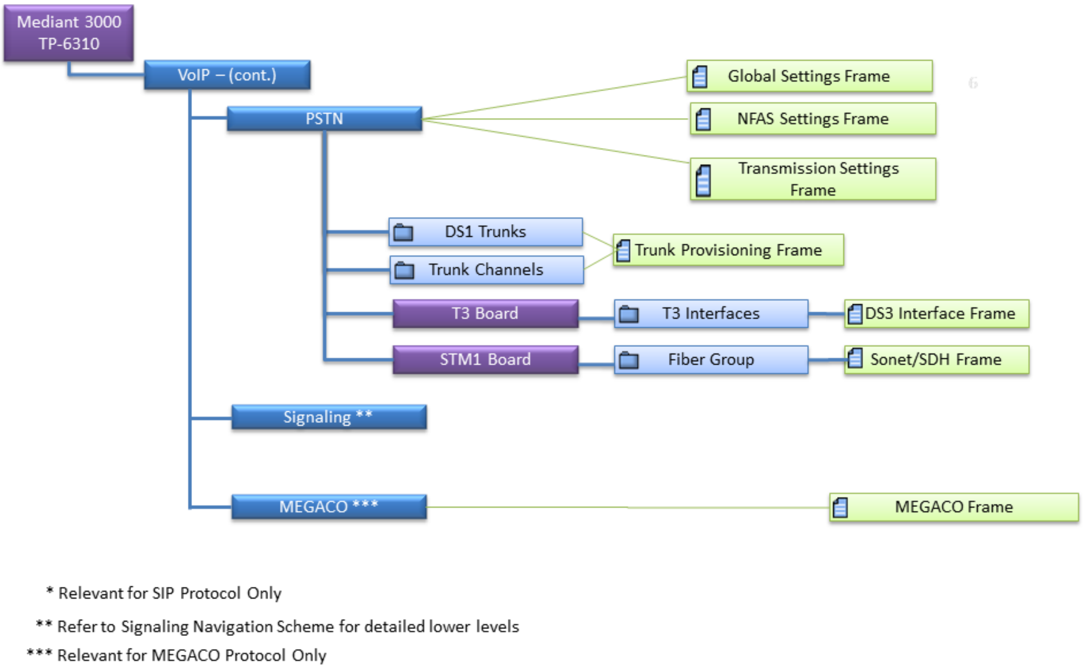


Figure 12-18: Navigation Hierarchy Links-Mediant 3000-TP-8410 and TP-6310 Part 1

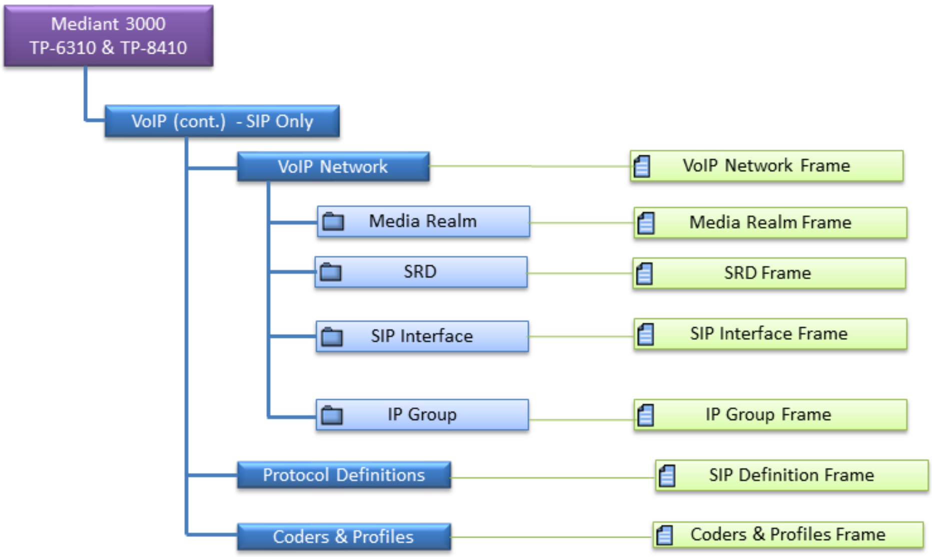


Figure 12-19: Navigation Hierarchy Links-Mediant 3000-TP-8410 and TP-6310 Part 2

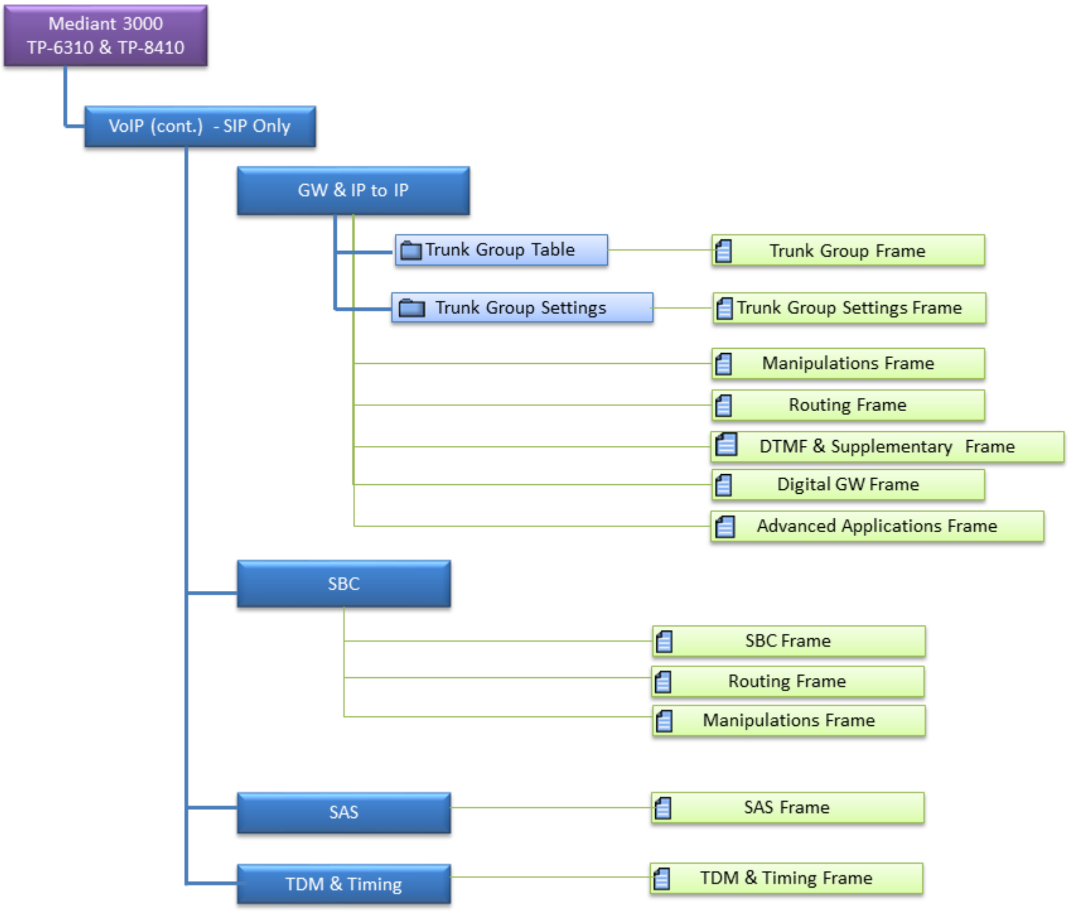
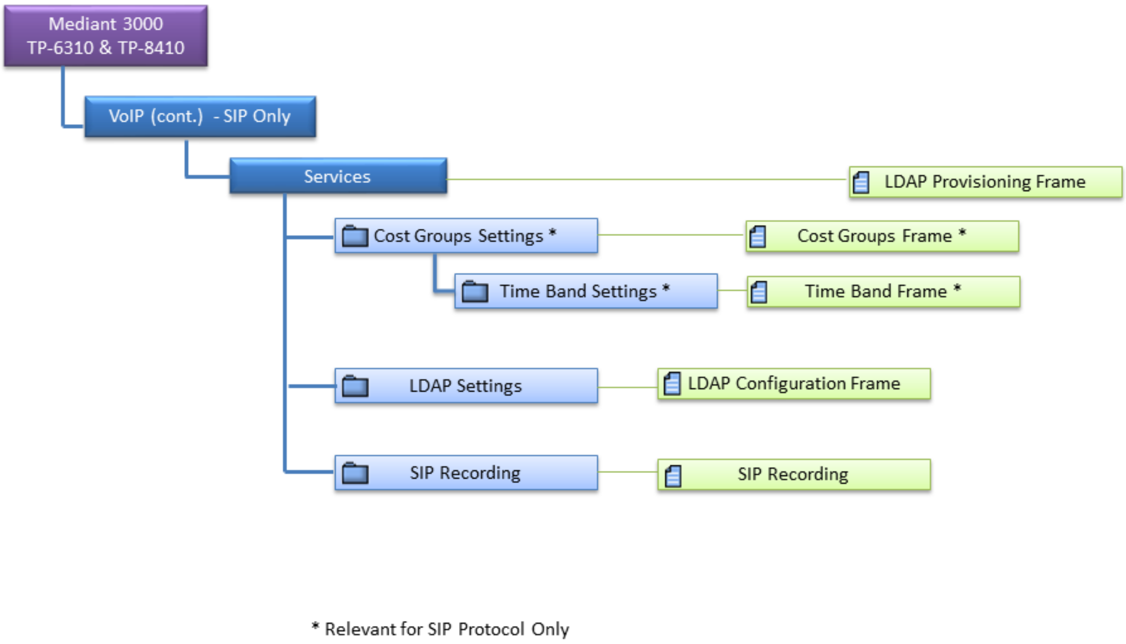


Figure 12-20: Navigation Hierarchy Links-Mediant 3000-TP-8410 and TP-6310 Part 3



See Section 'Provisioning Concepts' on page 222 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles.

Note: For SIP and SS7 MTP3 Navigation buttons, see Section 'Provisioning Concepts' on page 222.

12.4.1.1 Mediant 3000 8410 V5.2 Provisioning

For V5.2 applications, the following Provisioning screens and actions are supported:

- **V5.2 Interfaces Table**: The user may define up to 31 different V5.2 interfaces that are indexed from 0 to 30. Each row in the table represents a V5.2 interface. The following actions (activated from either the right-click menu or from the Actions bar) are supported for each one of the V5.2 Interfaces: Add, Remove, Lock, Unlock, In Service, Offline, Protection Switchover, Properties.
- **V5.2 Links Table:** At least 2 V5.2 links (one primary and one secondary) must be configured before starting a V5.2 interface. There is a 1 to 1 mapping between V5.2 links and V5.2 interfaces configured with the V5.2 protocol type. The following actions (activated from either the right-click menu or from the Actions bar) are supported for each one of the V5.2 Links: Add, Remove, Lock, Unlock, Block, Unblock, Link ID Check, Properties.

For information on downloading and managing the V5.2 configuration file, see Section 'Software Manager' on page 65.

To perform correct provisioning and maintenance of the V5.2 solution for the Mediant 3000, refer to the *Product Reference Manual for MGCP/Megaco (PSTN Chapter*).

12.4.2 SONET / SDH Interfaces

There are two SONET / SDH interfaces in the system. These interfaces act as Active / Standby, so from the provisioning perspective , users must configure one of them - and the configuration is transferred to the other. To provision a Fiber Group, select a row in the Fiber Group table and in the Configuration pane, click 'Fiber Group Settings'.

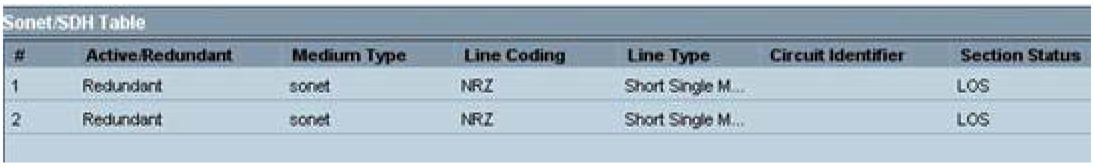
The Sonet OC3 interface on t he TP-6310 board supports mapping to three DS3 channels using STS1 (*DS3 Channelization-Asynchronous DS3*).

The Sonet interface on t he TP-6310 board supports mapping to OC3 using VT 1.5 mapping for North American T1 trunks.

The SDH interface on the TP-6310 board supports mapping to STM1 using VC12 for European E1 Trunks.

For more information, see 'Mediant 3000' on page 153 and refer to the *Mediant 5000/8000 IOM Guide*.

Figure 12-21: SONET / SDH Table



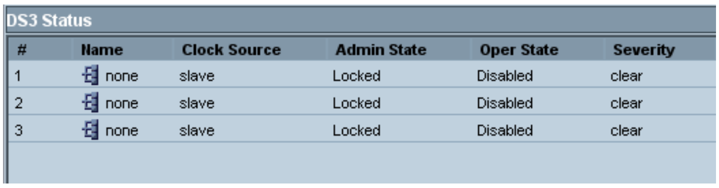
Sonet/SDH Table

#	Active/Redundant	Medium Type	Line Coding	Line Type	Circuit Identifier	Section Status
1	Redundant	sonet	NRZ	Short Single M...		LOS
2	Redundant	sonet	NRZ	Short Single M...		LOS

12.4.3 DS3 Interfaces

Three DS3 interfaces feature in the system. To provision a DS3 interface, select a row in the DS3 table and in the Configuration pane, click 'DS3 Settings'.

Figure 12-22: Provisioning a DS3 Interface



DS3 Status

#	Name	Clock Source	Admin State	Oper State	Severity
1	none	slave	Locked	Disabled	clear
2	none	slave	Locked	Disabled	clear
3	none	slave	Locked	Disabled	clear

12.4.4 DS1 Interfaces

DS1 Trunks and T runks Channels Status screens are described in 'MediaPack' on page 211.

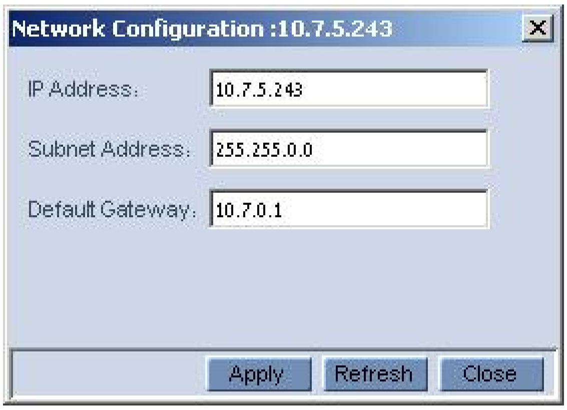
12.5 Executable Actions

The following right-click options are supported for the Mediant 3000:

12.5.1 Configuration Actions

- Network Configuration: Change the network configuration (IP Address, Subnet Mask and Default Gateway); send the changes to the device and save the settings in the EMS database. This action is not supported for the HA configuration.

Figure 12-23: Changing a Mediant 3000 Gateways' Network Configuration



Network Configuration :10.7.5.243

IP Address: 10.7.5.243

Subnet Address: 255.255.0.0

Default Gateway: 10.7.0.1

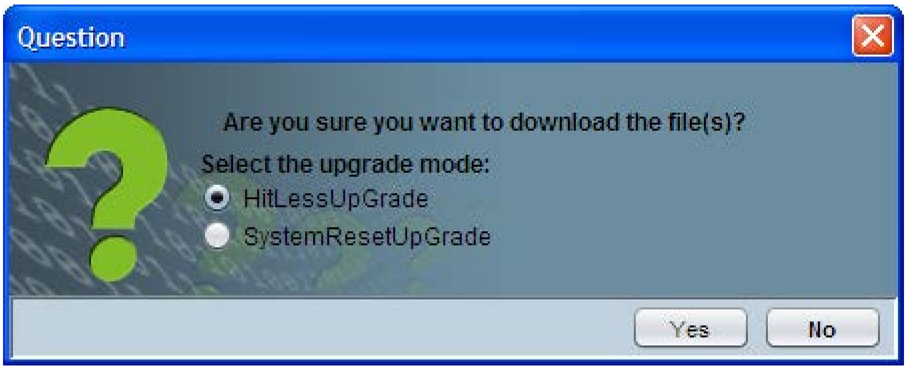
Note: Reconfiguring the network parameters might cause a loss of connection with the device. Make sure that the IP address you reconfigure is distinct from those of other devices in the tree.

12.5.2 Software Upgrade

- Software Upgrade performs loading software or regional files.

  Note, that when loading a new software file, Hitless Software Upgrade is supported. EMS checks if according to 'From' and 'To' versions, there is a possibility to perform hitless software upgrade, and provides an EMS user with appropriate questionnaire.

Figure 12-24: Hitless Upgrade Prompt



Question

Are you sure you want to download the file(s)?

Select the upgrade mode:

● HitLessUpGrade

○ SystemResetUpGrade

12.5.3 Switchover

- Switchover: Each TP board can be switched over by right-clicking on it. If a switchover is in progress, the configuration cannot be applied. A warning icon and a message are viewed at the top of the Status pane:

  '⚠ HA system switch-over in progress; do not apply the configuration.

12.5.4 Reset MG / TP Board

Reset MG: Resets the entire chassis. Click the **Reset' link** in the Info Pane or choose the right-click **Reset** action. To confirm the action, click **OK**; the gateway is reset.

To Reset each individual TP Boards, select the Reset option by right clicking on each TP Board.

For more details on the Maintenance Actions supported by digital gateways, refer 'Executable Actions on MediaPacks' on page 214.

Reader's Notes

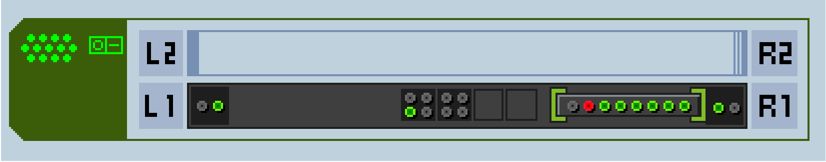
13 Mediant 2000

This section describes the Mediant 2000 status pane and provisioning.

13.1 Status Pane

The figure below shows the 16-trunk media gateway Status pane. The Status pane for the 1, 2, 4 and 8-trunk media gateways are identical; only the number of trunks differs.

Figure 13-1: Mediant 2000 Status Pane



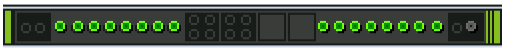
The Mediant 2000 Status pane graphically represents the status of the one or two-module gateway. If one of the modules fails, the status of the Mediant 2000 is indicated as failed. The Mediant 2000 Status pane indicates trunk status: Green for enabled, red for disabled and gray for locked (manually out of service) mode.

The Mediant 2000 Status pane includes the following:

- **VoP Boards status**
  - Background color: Dark Gray = Active board; Blue = Redundant board
  - Upper and lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity

  The figures below displays board status: TP-1610 Active board status:

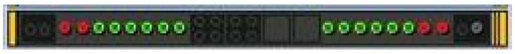
Figure 13-2: TP-1610 Active



- Background color: Dark Gray = Active board; Blue = Redundant board
- Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity, Yellow = Minor Severity, Blue = Warning Severity, White = Indeterminate Severity

- TP Switchover: The active TP board, after switchover, is marked in a background black color without any LEDs, with a red or green frame around the board according to its Operational State (green = enabled boards, red = disabled boards). A redundant TP board, which becomes active after switchover, is marked in a background blue color, with LEDs for activated trunks.

Figure 13-3: 1610 Board Status

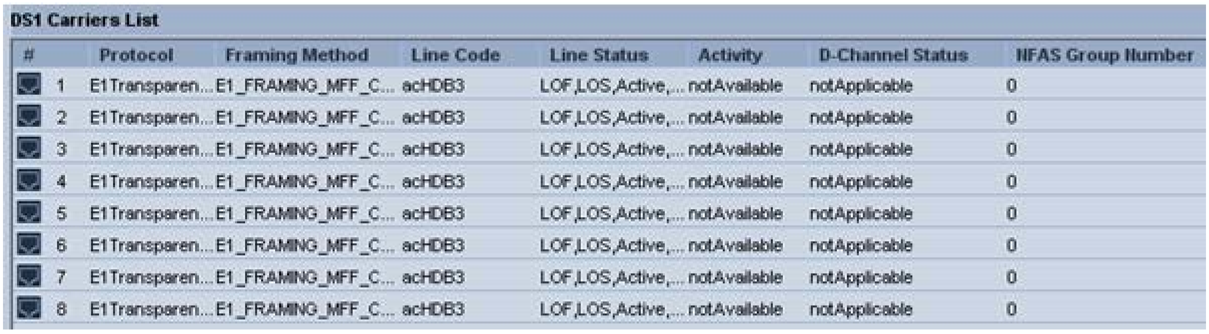


- All the TP-1610 LEDS above represent 16 E1/T1 interfaces: 8 in each TPM

TP LEDs status

- PSTN and ATM LEDs color convention:
- Rx /Tx LED: Red = Disabled, Green = Link OK, Yellow = Protection Link, Gray = No Link
- Alarm LED: Gray = Normal Link, Red = LOS, LOF, AIS, RDI

Figure 13-4: Trunk List for Mediant 2000 Module #1 or 2



DS1 Carriers List

#	Protocol	Framing Method	Line Code	Line Status	Activity	D-Channel Status	NFAS Group Number
1	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
2	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
3	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
4	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
5	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
6	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
7	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
8	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0

- The MG Node Info pane indicates the media gateway's name, IP address, software version, trunks count and control protocol type. It also includes hardware, software or configuration mismatch if any problem is detected. “Reset Needed” indicates that the operator changed offline parameters and that to apply these parameters to the media gateway, a Reset must be performed.
- The DS1 Trunks and Trunks Channels Status screens are described in 'DS1 Interfaces' on page 186.

13.2 Provisioning

The Gateways' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and s ub-links that are displayed in the Configuration pane.

The figure below shows the navigation hierarchy links used to provision the Mediant 2000 Media Gateway.

Figure 13-5: Navigation Hierarchy Links- Mediant 2000 (Part 1)

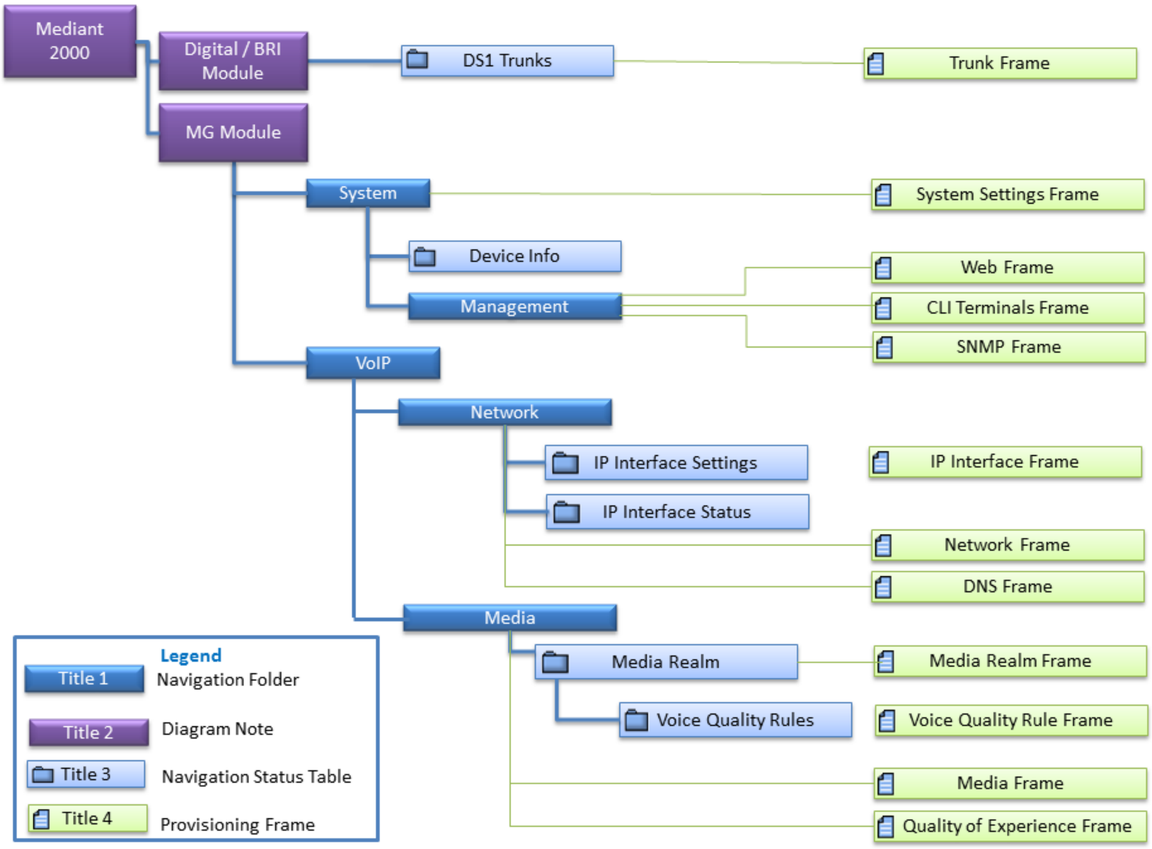


Figure 13-6: Navigation Hierarchy Links-Mediant 2000 (Part 2)

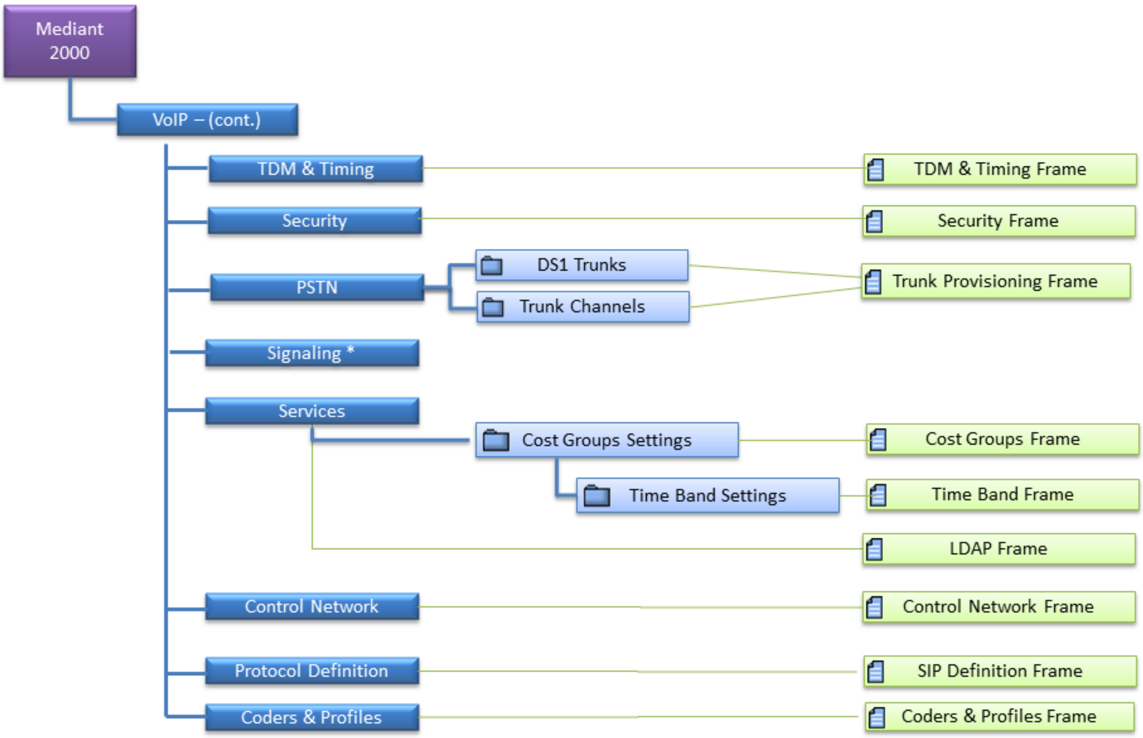
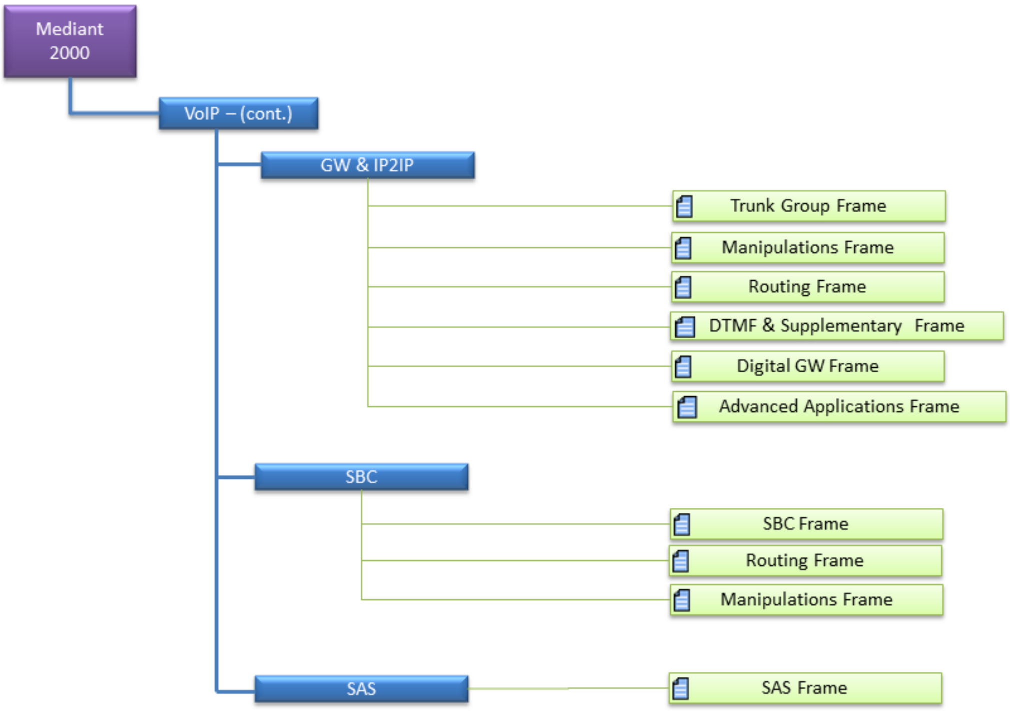


Figure 13-7: Navigation Hierarchy Links-Mediant 2000 (Part 3)



See Section 'Provisioning Concepts' on page 222 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles.

13.3 Executable Actions

All the maintenance actions for the Mediant 2000 are performed separately for each module.

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

Reader's Notes

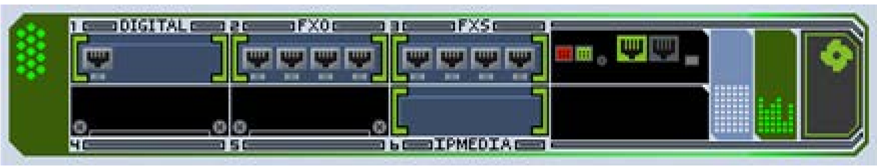
14 Mediant 600 and Mediant 1000

This section describes the Mediant 1000 and Mediant 600 status panes and provisioning.

14.1 Mediant 1000 Status Pane

The figure below displays the Mediant 1000 status pane.

Figure 14-1: Mediant 1000 Media Gateway Status



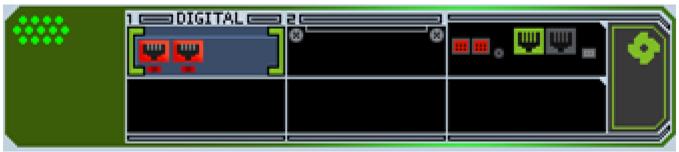
Note the following:

- To define new modules, physically insert them and reset the gateway. It's not necessary to perform an 'Insert Module' action.
- The Status pane represents the Mediant 1000 Analog and Digital Modules status. For each module, its number and type (Digital, FXS, FXO, BRI or IPmedia) and status are displayed. Additionally, the status of its trunks (digital) or lines (analog) is displayed. Green = enabled, red = disabled and gray = locked.
- Double-clicking the digital module opens the Trunks screen where users can view, and perform maintenance actions on one or more trunks.
- For provisioning a trunk, select a trunk and in the Configuration pane, click **Trunk Provisioning**.
- Fan and power supply status is displayed according to the following color convention: *Green* = enabled, *red* = disabled and *gray* = doesn't exist.
- DS1 Trunks and Trunks Channels Status screens are described in 'DS1 Interfaces' on page 186.

14.2 Mediant 600 Status Pane

The Mediant 600 status pane is illustrated below.

Figure 14-2: Mediant 600 Status Pane



14.3 Provisioning

The gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and sub-links that are displayed in the Configuration pane.

The figure below shows the navigation hierarchy links used to provision the E-SBC and MSBR series gateways.

Figure 14-3: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 1)

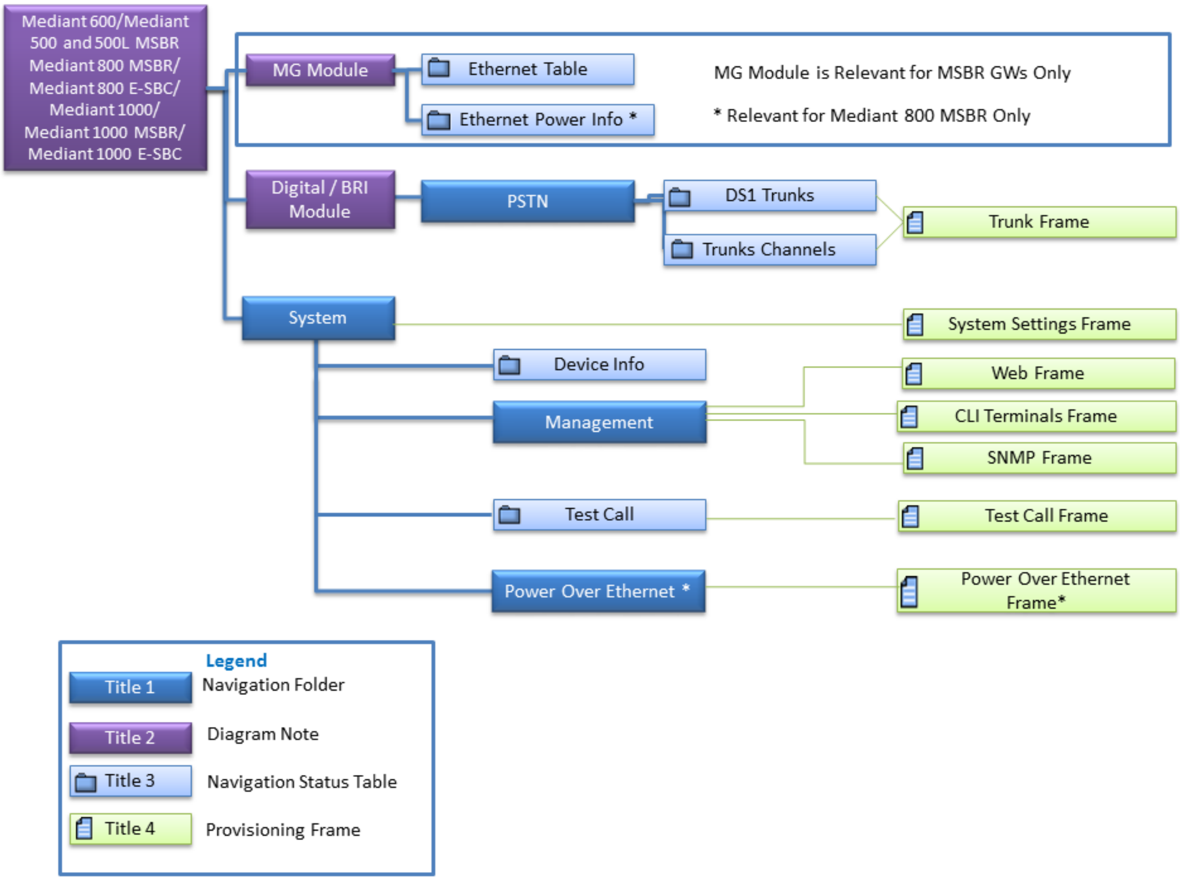


Figure 14-4: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 2)

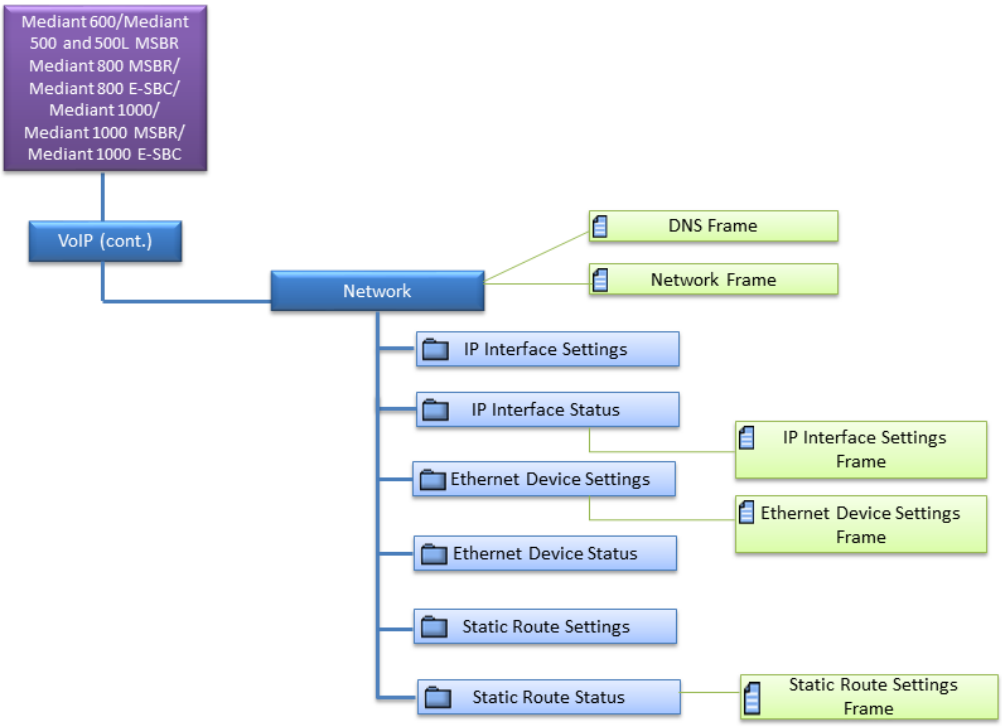

Mediant 600/Mediant 500 and 500L MSBR Mediant 800 MSBR/ Mediant 800 E-SBC/ Mediant 1000/ Mediant 1000 MSBR/ Mediant 1000 E-SBC
VoIP (cont.)
Network
DNS Frame
Network Frame
IP Interface Settings
IP Interface Status
IP Interface Settings Frame
Ethernet Device Settings
Ethernet Device Settings Frame
Ethernet Device Status
Static Route Settings
Static Route Status
Static Route Settings Frame

Figure 14-5: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 3)

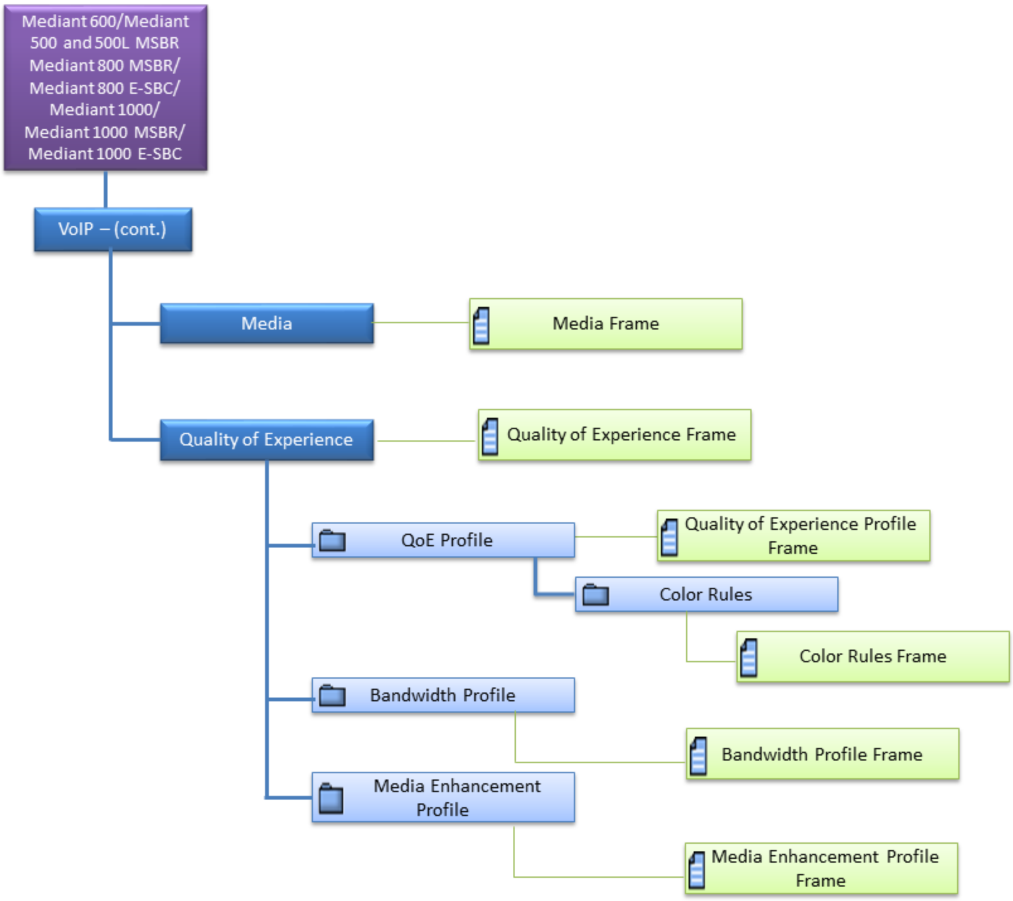

Mediant 600/Mediant 500 and 500L MSBR Mediant 800 MSBR/ Mediant 800 E-SBC/ Mediant 1000/ Mediant 1000 MSBR/ Mediant 1000 E-SBC
VoIP – (cont.)
Media
Media Frame
Quality of Experience
Quality of Experience Frame
QoE Profile
Quality of Experience Profile Frame
Color Rules
Color Rules Frame
Bandwidth Profile
Bandwidth Profile Frame
Media Enhancement Profile
Media Enhancement Profile Frame

Figure 14-6: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 4)

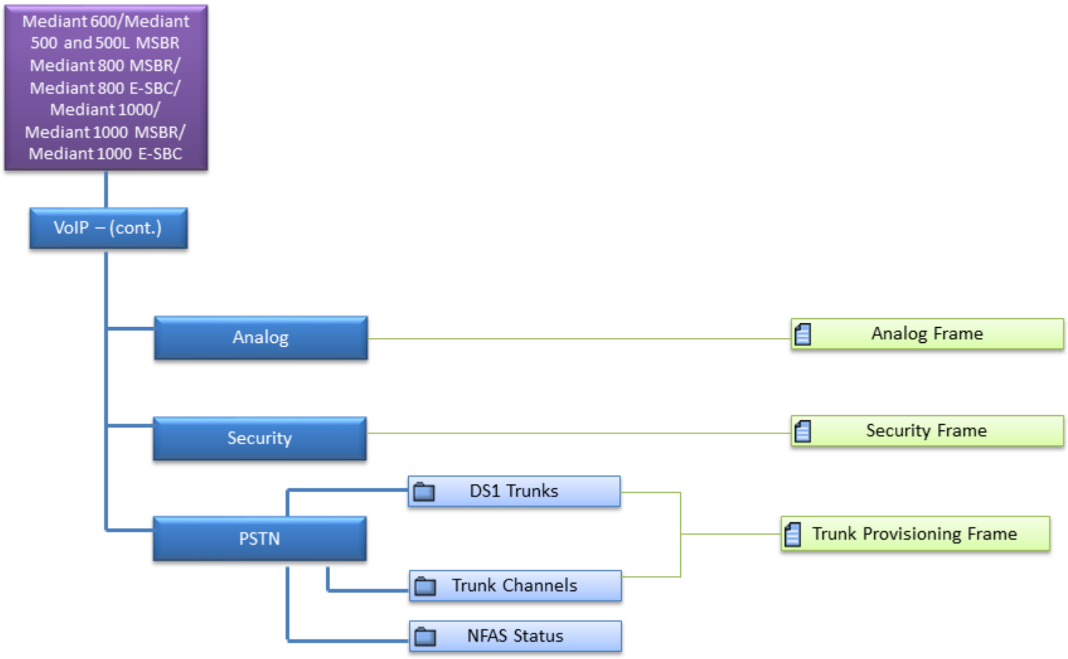

Mediant 600/Mediant 500 and 500L MSBR Mediant 800 MSBR/ Mediant 800 E-SBC/ Mediant 1000/ Mediant 1000 MSBR/ Mediant 1000 E-SBC
VoIP – (cont.)
Analog
Analog Frame
Security
Security Frame
DS1 Trunks
PSTN
Trunk Provisioning Frame
Trunk Channels
NFAS Status

Figure 14-7: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 5)

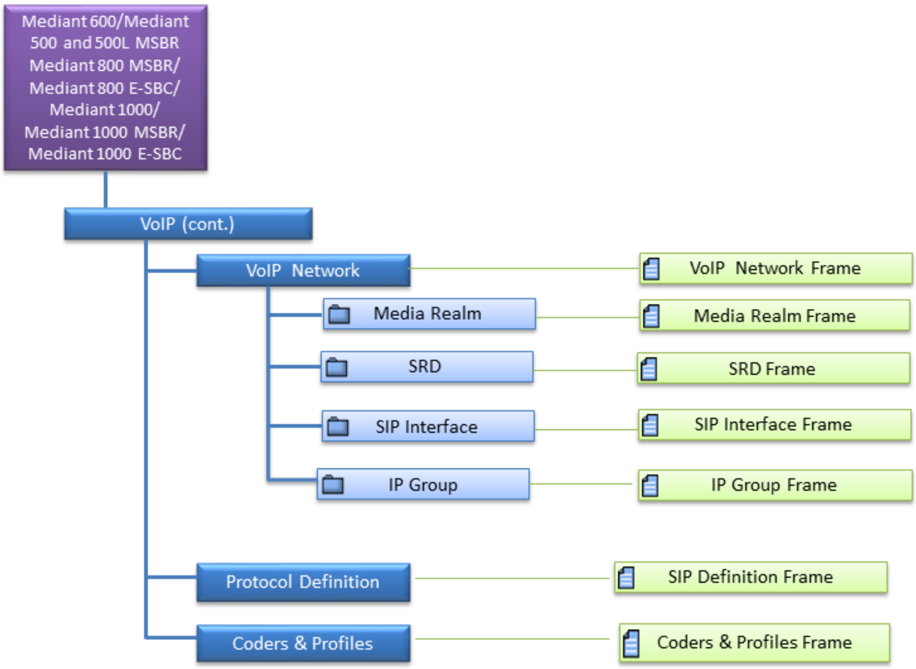


Figure 14-8: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 6)

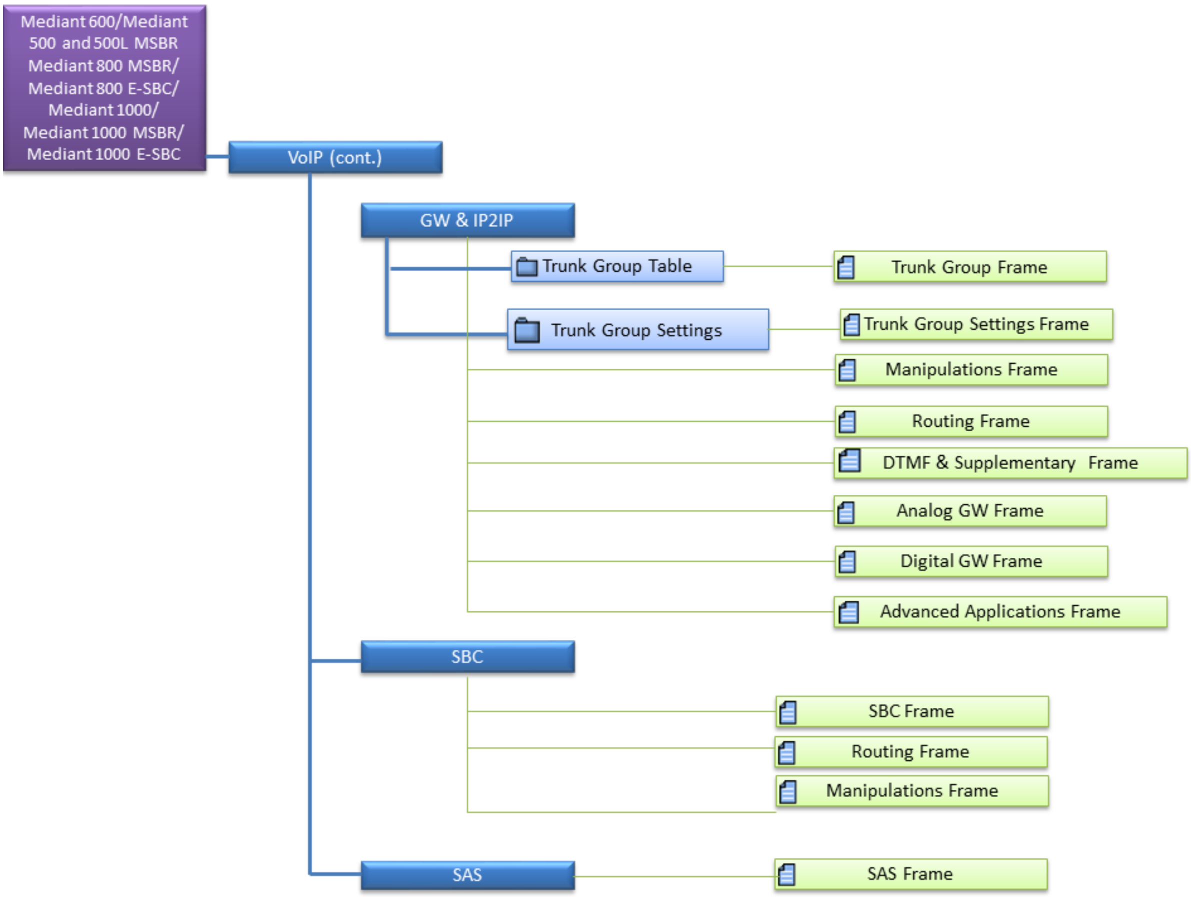
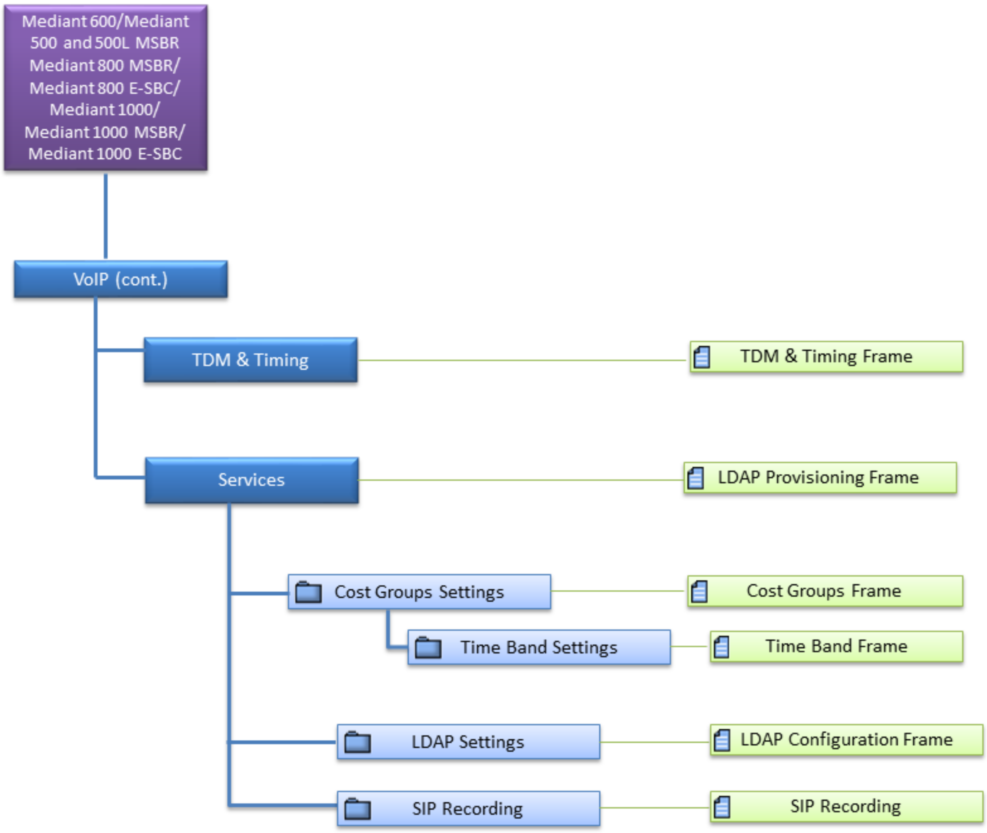

Mediant 600/Mediant 500 and 500L MSBR Mediant 800 MSBR/ Mediant 800 E-SBC/ Mediant 1000/ Mediant 1000 MSBR/ Mediant 1000 E-SBC
VoIP (cont.)
GW & IP2IP
Trunk Group Table
Trunk Group Frame
Trunk Group Settings
Trunk Group Settings Frame
Manipulations Frame
Routing Frame
DTMF & Supplementary Frame
Analog GW Frame
Digital GW Frame
Advanced Applications Frame
SBC
SBC Frame
Routing Frame
Manipulations Frame
SAS
SAS Frame

Figure 14-9: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 E-SBC and MSBR Devices (Part 7)



See Section 'Provisioning Concepts' on page 222 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

14.4 Executable Actions

The following maintenance actions are specific for the Mediant 1000 Gateway:

Insert Module: When reinserting a previously removed module into the chassis (in the event that you performed a Remove Module' action and you wish to insert the new module in the same slot), right-click and choose option 'Insert Module' from the popup menu, insert the missing board and reset the gateway.

Remove Module: Before removing the existing module, right-click it, select option **Remove Module**, remove the module physically, and reset the gateway.

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

Reader's Notes

15 Mediant E-SBC Products

This section describes the Mediant 800 E-SBC status pane and provisioning.

15.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Standalone (Simplex) Mediant 500 E-SBC
- High Availability-HA (1+ 1) Mediant 500 E-SBC
- Standalone (Simplex) Mediant 800B Gateway and E-SBC
- High Availability-HA (1+ 1) Mediant 800B Gateway and E-SBC
- Standalone (Simplex) Mediant 1000B Gateway and E-SBC

15.2 Initial Configuration

Refer to the relevant User's Manual for the initial gateway configuration.

15.3 Status Pane

This Status pane provides the following information:

- Hardware components status support, including chassis LEDs, fan status and speed, power supplies and PEM status. Board temperature is indicated.
- Separate device statuses are displayed for the active device and redundant device.
- Device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figures below display the Mediant 500 E-SBC and Mediant 800B Gateway and E-SBC HA status pane.

Mediant 1000B Gateway and E-SBC Status Pane

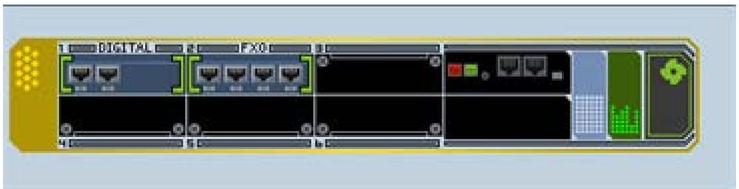


Figure 15-1: Mediant 800B Gateway and E-SBC HA Status Pane

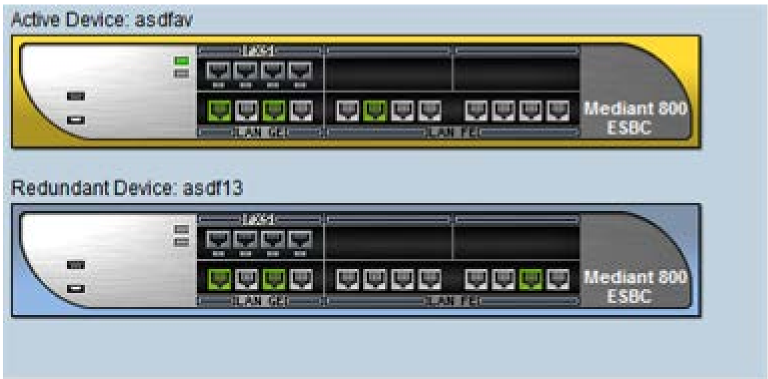
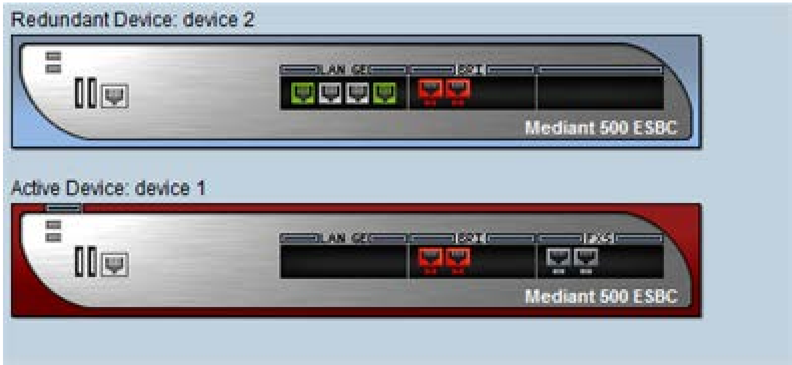


Figure 15-2: Mediant 500 Gateway and E-SBC Status Pane

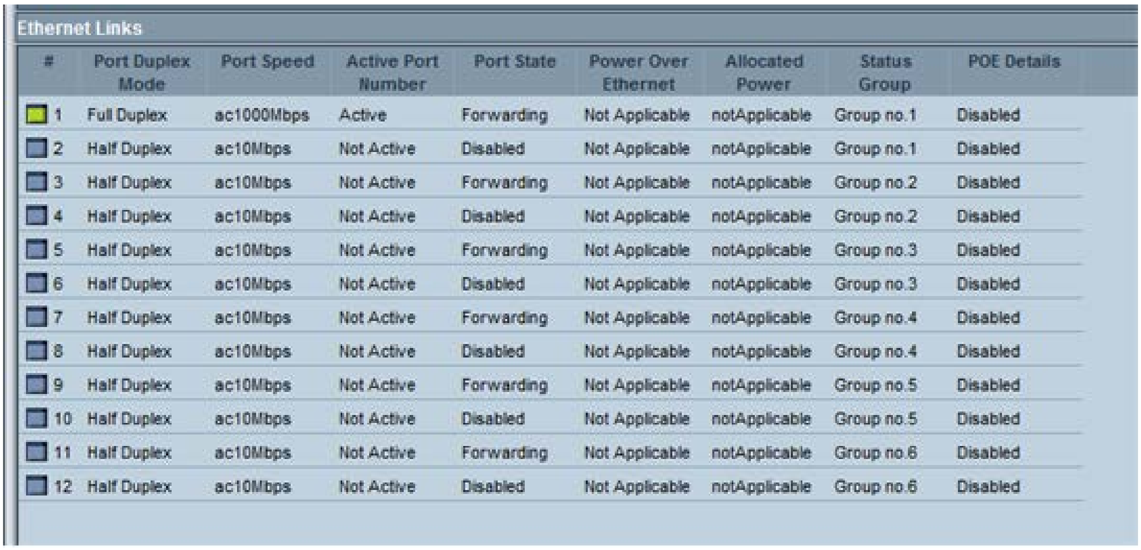


Double-click an FXO link to open the FXO Line Test Table.

Double-click an FXS link to open the FXS Line Test Table.

Double-click one of the Ethernet ports (to display the detailed status for each port) and then in the Navigation pane, select **Ethernet Table**; the Ethernet Links Table screen is displayed:

Figure 15-3: Mediant 800B E-SBC and Gateway Ethernet Links

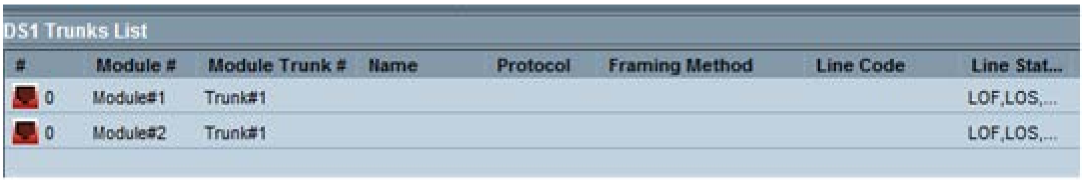


Ethernet Links

	#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Power Over Ethernet	Allocated Power	Status Group	POE Details
🟩	1	Full Duplex	ac1000Mbps	Active	Forwarding	Not Applicable	notApplicable	Group no.1	Disabled
🟦	2	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.1	Disabled
🟦	3	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	Group no.2	Disabled
🟦	4	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.2	Disabled
🟦	5	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	Group no.3	Disabled
🟦	6	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.3	Disabled
🟦	7	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	Group no.4	Disabled
🟦	8	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.4	Disabled
🟦	9	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	Group no.5	Disabled
🟦	10	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.5	Disabled
🟦	11	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	Group no.6	Disabled
🟦	12	Half Duplex	ac10Mbps	Not Active	Disabled	Not Applicable	notApplicable	Group no.6	Disabled

Double-click an E1/T1 trunk to open the DS1 Trunks List

Figure 15-4: Mediant 800B E-SBC and Gateway DS1 Trunks List



DS1 Trunks List

#	Module #	Module Trunk #	Name	Protocol	Framing Method	Line Code	Line Stat...
0	Module#1	Trunk#1					LOF,LOS,...
0	Module#2	Trunk#1					LOF,LOS,...

15.4 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The E-SBC product's navigation hierarchy links are described on page 196.

15.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

Reader's Notes

16 Mediant MSBR Products

This section describes the Mediant 800 MSBR status pane and provisioning.

16.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Standalone (Simplex) Mediant 1000B MSBR, Mediant 800B MSBR, Mediant 500 MSBR and Mediant 500L MSBR.

16.2 Initial Configuration

Refer to the relevant User's Manual for the initial gateway configuration.

16.3 Status Pane

This pane provides the following information:

- Hardware components status support, including chassis LEDs, fan status and speed, power supplies and PEM status. Board temperature is indicated.
- Device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figures below displays the MSBR status panes.

Figure 16-1: Mediant 500 MSBR Status Pane

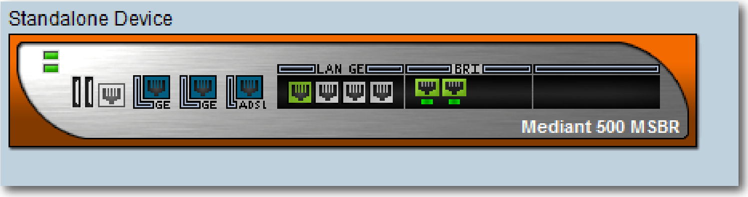


Figure 16-2: Mediant 500L MSBR Status Pane

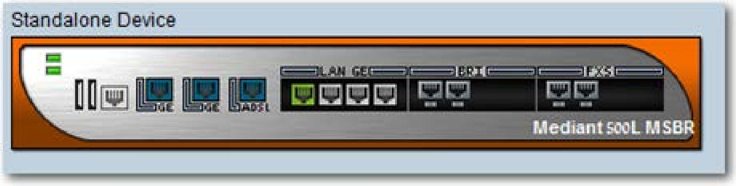


Figure 16-3: Mediant 800B MSBR Status Pane

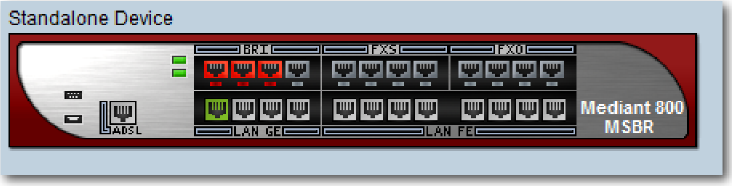
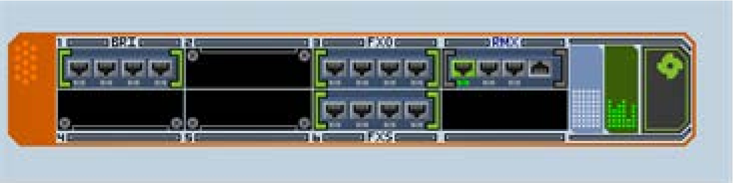


Figure 16-4: Mediant 1000B MSBR Status Pane



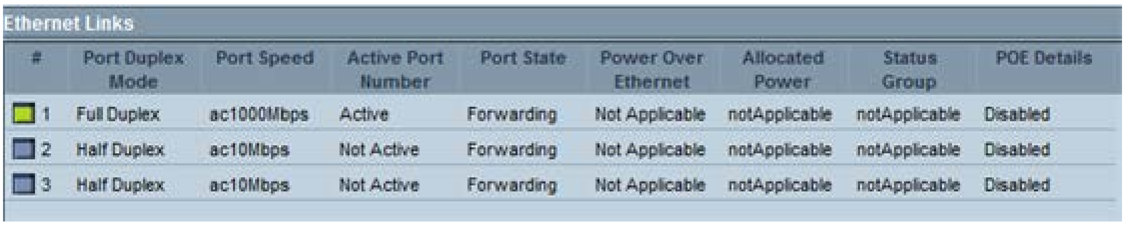
The Status pane displays MediaPacks and their LEDs, which indicate channel status (green- for off-hook and gray- for on-hook) for FXS and FXO ports in the upper row of ports, and Ethernet ports LEDs in the bottom row of ports.

Double-click an FXO link to open the FXO Line Test Table.

Double-click an FXS link to open the FXS Line Test Table.

Double-click one of the Ethernet ports (to display the detailed status for each port) and then in the Navigation pane, select **Ethernet Table**; the Ethernet Links Table screen is displayed:

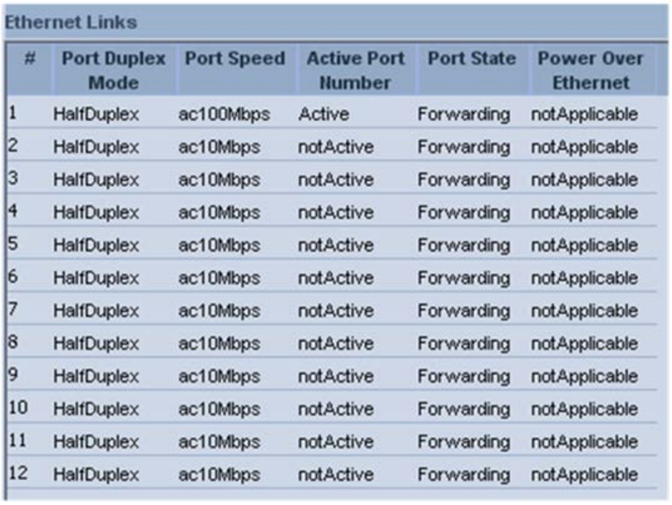
Figure 16-5: Mediant 1000B MSBR Ethernet Links



Ethernet Links

#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Power Over Ethernet	Allocated Power	Status Group	POE Details
🟩 1	Full Duplex	ac1000Mbps	Active	Forwarding	Not Applicable	notApplicable	notApplicable	Disabled
🟦 2	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	notApplicable	Disabled
🟦 3	Half Duplex	ac10Mbps	Not Active	Forwarding	Not Applicable	notApplicable	notApplicable	Disabled

Figure 16-6: Mediant 800 MSBR Ethernet Links

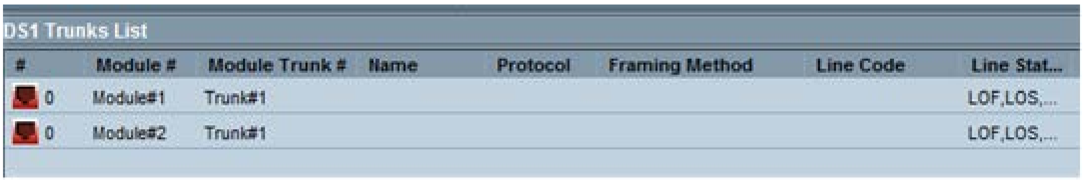


Ethernet Links

#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Power Over Ethernet
1	HalfDuplex	ac100Mbps	Active	Forwarding	notApplicable
2	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
3	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
4	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
5	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
6	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
7	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
8	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
9	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
10	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
11	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
12	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable

Double-click an E1/T1 trunk to open the DS1 Trunks List

Figure 16-7: Mediant 800 MSBR DS1 Trunks List



DS1 Trunks List

#	Module #	Module Trunk #	Name	Protocol	Framing Method	Line Code	Line Stat...
🟥 0	Module#1	Trunk#1					LOF,LOS,...
🟥 0	Module#2	Trunk#1					LOF,LOS,...

The Information pane indicates the media gateway's name, IP address, software version, trunks count and control protocol type. It also includes hardware, software or configuration mismatch information, In case any problem is detected. 'Reset Needed' indicates that the operator has changed offline parameters and that a reset must be performed to apply these parameters to the media gateway.

Note: MSBR Data Routing is not provisioned via the EMS application and therefore, the relevant INI file should be downloaded to the device. For more information, refer to the relevant User's Manual.

16.4 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The MSBR product's navigation hierarchy links are described on page 196.

16.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

Reader's Notes

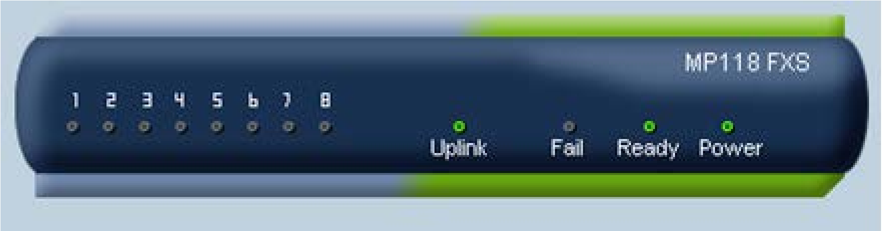
17 MediaPack

This section describes the MediaPack status pane and provisioning.

17.1 Status Pane

The figure below shows the 2-channel media gateway Status pane. The Status pane for the 4-channel, 8-channel, 24-channel media gateways are identical (except for the number of channels).

Figure 17-1: MediaPack Status Pane



The Status pane r epresents MediaPacks and t heir LEDs indicating channel status (green- for off-hook and gray- for on-hook), LAN and Ready LEDs (refer to the table below). Data and Control LEDs are not represented and are always colored in *gray*.

Table 17-1: MediaPack Status LEDs

LED	Type	Color	State	Definition	EMS Representation
Ready	Device Status	Green	ON	Device powered, self-test OK	Ready LED is *green*
		Orange	Blinking	Software loading/Initialization	Ready LED is *green*
		Red	ON	Malfunction	The entire MP is *red*
LAN	Ethernet Link Status	Green	ON	Valid connection to 10/100 Base-T hub/switch	LAN LED is *green*
		Red	ON	Malfunction	The entire MP is *red*
		Red	Blinking	MediaPack is receiving data packets	LAN LED is *green*
		Blank		No traffic	LAN LED is *green*
Channels	Telephone Interface	Green	ON	The phone is off-hooked (FXS); the FXO off-hooks the line towards the PBX.	Channel LED is *green*
		Green	Blinking	There's an incoming call, before answering	Channel LED is *green*

Table 17-1: MediaPack Status LEDs

LED	Type	Color	State	Definition	EMS Representation
		Red	ON	Line malfunction	Not supported
		Blank	-	Normal on-hook position	Channel LED is *gray*

The Information pane indicates the media gateway's name, IP address, software version, trunks count and control protocol type. It also includes hardware, software or configuration mismatch information, in case any problem is detected. 'Reset Needed' indicates that the operator changed offline parameters and t hat a r eset must be performed to apply these parameters to the media gateway.

17.2 Line Test

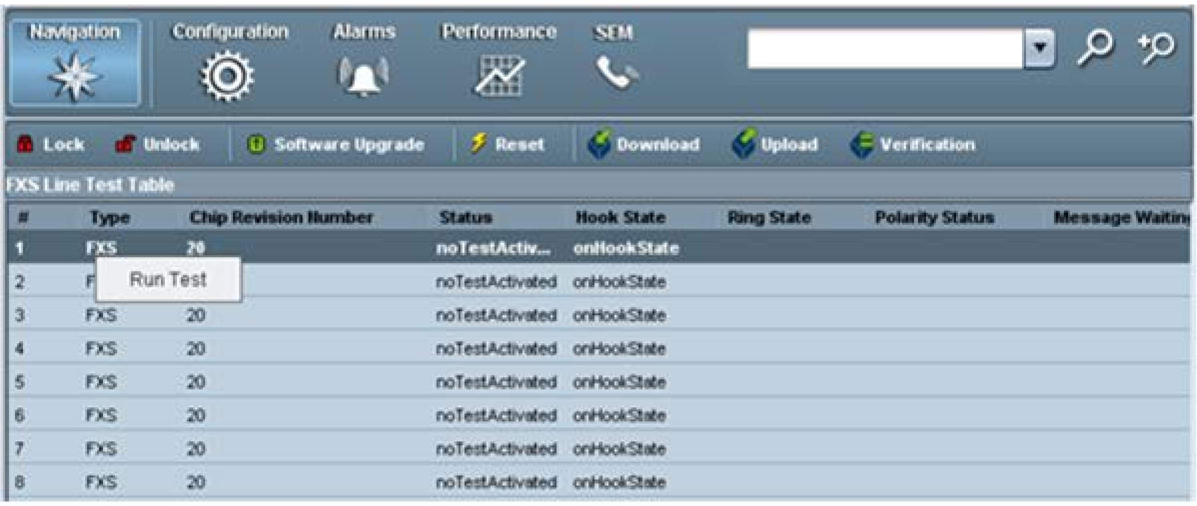
The MediaPack media gateway supports Line Testing.

➢ To review the last test result or run a test:

1. Double-click the MediaPack Status screen.
2. Select the line/s on which to run the test.
3. Right-click and choose option **RunTest** from the popup menu.

Note that the test will stop phone calls on the selected lines.

Figure 17-2: MediaPack Line Test



FXS Line Test Table

#	Type	Chip Revision Number	Status	Hook State	Ring State	Polarity Status	Message Waitin
1	FXS	20	noTestActiv...	onHookState			
2	F		noTestActivated	onHookState			
3	FXS	20	noTestActivated	onHookState			
4	FXS	20	noTestActivated	onHookState			
5	FXS	20	noTestActivated	onHookState			
6	FXS	20	noTestActivated	onHookState			
7	FXS	20	noTestActivated	onHookState			
8	FXS	20	noTestActivated	onHookState			

17.3 Provisioning

The Gateways' provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The figure below shows the navigation hierarchy links used to provision the MediaPack.

Figure 17-3: Navigation Hierarchy Links-MediaPack

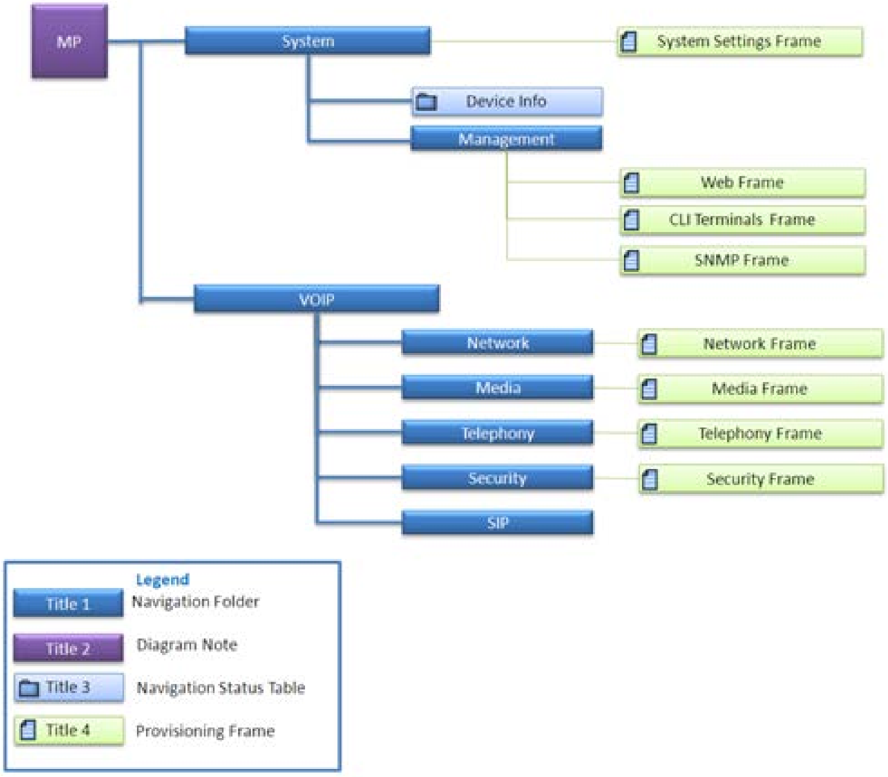
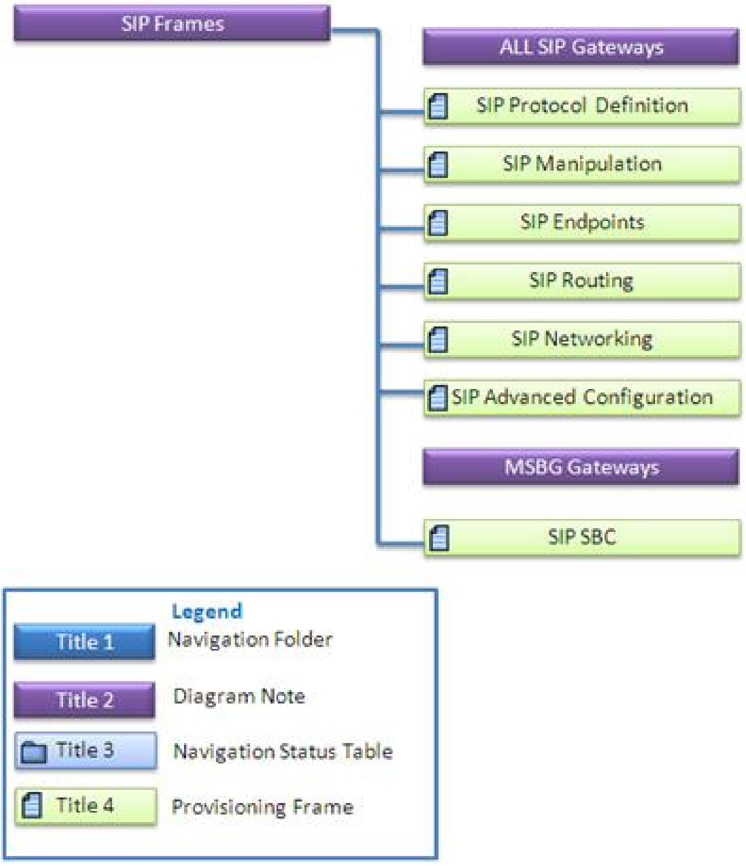


Figure 17-4: MediaPack-Hierarchy Links (Part 2)



See Section 'Provisioning Concepts' on page 222 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles on provisioning parameters.

17.4 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 225.

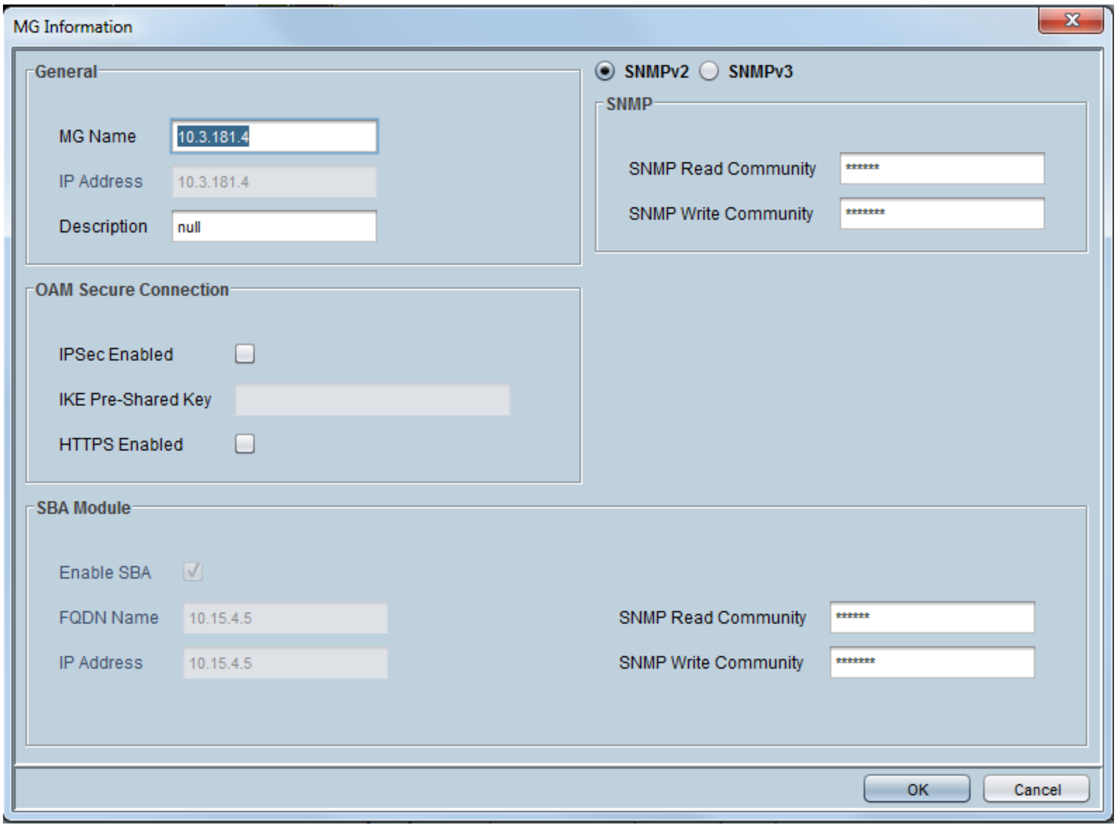
18 SBA

When you add the SBA to the EMS, you need to enable the module and configure the IP address of the SBA Management Interface, which you can then later access when you click the 'SBA Home Page' link on the SBA status screen (see Section 18.1.1 on page 218).

➢ To add the SBA module:

1. In the Navigation pane, right-click the Mediant 1000B or Mediant 800B gateway with the resident OSN SBA module.

Figure 18-1: MG Details-Adding SBA



MG Information

General

MG Name 10.3.181.4

IP Address 10.3.181.4

Description null

● SNMPv2 ○ SNMPv3

SNMP

SNMP Read Community ******

SNMP Write Community *******

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key

HTTPS Enabled □

SBA Module

Enable SBA ☑

FQDN Name 10.15.4.5

IP Address 10.15.4.5

SNMP Read Community ******

SNMP Write Community *******

2. In the SBA Module pane, select the 'Enable SBA' check box and then enter the FQDN Name and IP address of the SBA Management Interface (the IP address that you configured when setting up the SBA).

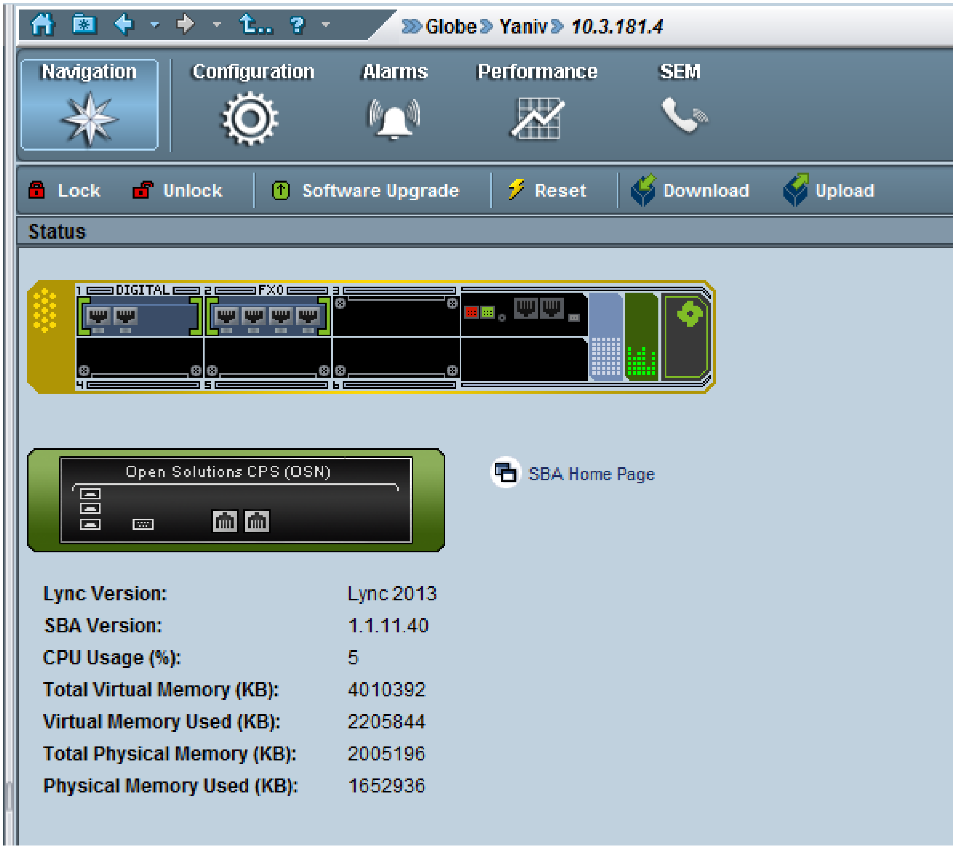
Note:

- If you wish the SBA device to report SNMP info and traps to the EMS, then you must configure the EMS as an external trap manager and start the SNMP service on the SBA (for more information, refer to the section 'Step 17 (Optional) SNMP Setup' in the *Mediant 1000B SBA for Microsoft Lync 2010 and 2013 Installation and Maintenance Guide* or in the *Mediant 800B SBA for Microsoft Lync 2010 and 2013 Installation and Maintenance Guide.*
- The same community string values configured in the MG information screen above must be entered in the SNMP configuration on the SBA device.
- The gateway must be configured for SNMPv2 only.

18.1 SBA Status Pane

This section describes the SBA status pane. The SBA OSN module is resident on the Mediant 800B and Mediant 1000B chassis (version 6.6). The status pane includes the details of the Lync version,e.g., Lync 2013 and the SBA Management Interface version, e.g., version 1.1.11.40. In addition, you can view the OSN host CPU resource utilization details, such as 'Total Virtual Memory' update in real time.

Figure 18-2: SBA Status Screen

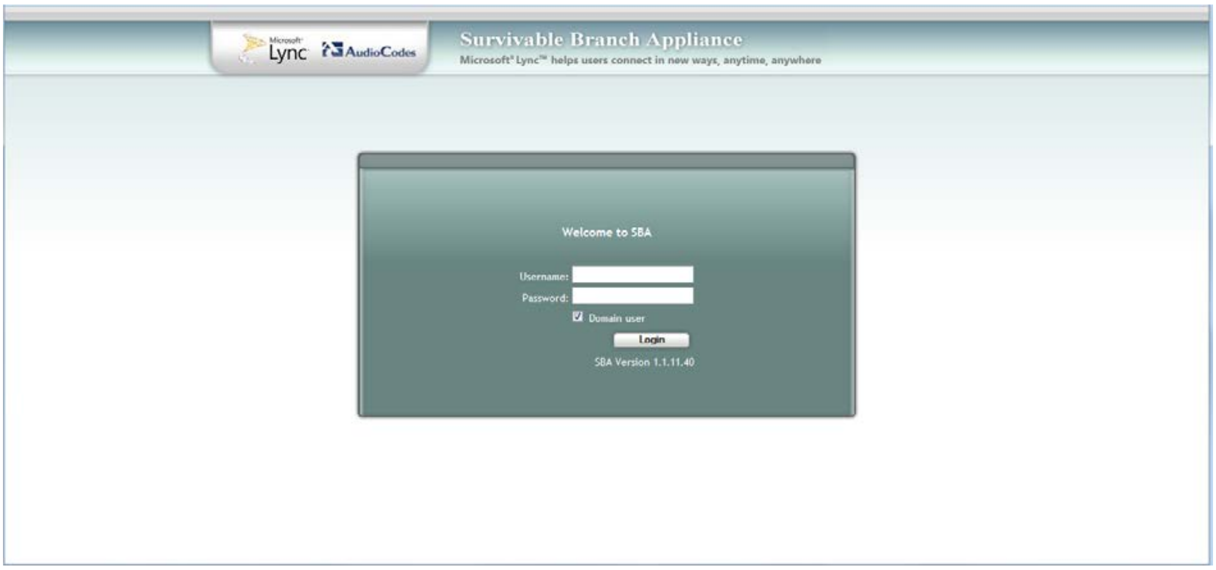


Lync Version:	Lync 2013
SBA Version:	1.1.11.40
CPU Usage (%):	5
Total Virtual Memory (KB):	4010392
Virtual Memory Used (KB):	2205844
Total Physical Memory (KB):	2005196
Physical Memory Used (KB):	1652936

18.1.1 SBA Management Interface Link

The SBA Status screen includes a l ink to the SBA Management Interface Login screen, which opens automatically when you click on the 'SBA Home Page' link (see example login screen in the figure below):

Figure 18-3: SBA Management Interface Login Screen



Survivable Branch Appliance

Microsoft® Lync™ helps users connect in new ways, anytime, anywhere

Welcome to SBA

Username:

Password:

☑ Domain user

Login

SBA Version 1.1.11.40

19 Trunks and Channels Status

All the Digital Gateways have common DS1 Trunks and Trunk Channel Status screens.

19.1 DS1 Trunks Status and Provisioning

The Trunk List displays basic information (status and configuration) on the trunks contained in the gateway/server. Double-clicking a t runk opens this trunk's provisioning screen.

Note that most Trunk provisioning parameters require that a Trunk Lock / Unlock be performed before / after configuring each of the trunks. When performing a Lock action, all active calls are dropped and users cannot originate new calls. This mode is 'Out Of Service' mode.

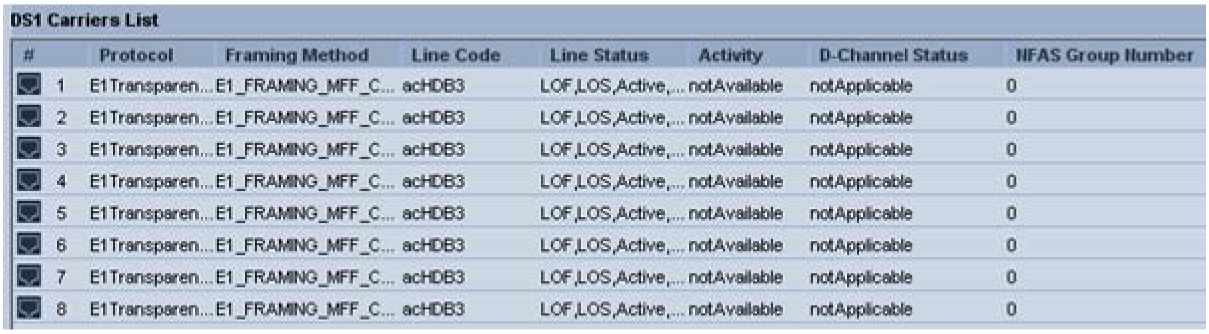
When performing a deactivate action on a trunk, all active calls are dropped and users cannot originate new calls. Configuration changes cannot be performed, only maintenance actions. You may wish to deactivate a trunk when trunk channels have SS7 links and therefore you cannot lock the trunk nor do you wish to deactivate SS7. See Trunks Channel status (section below) to determine whether a trunk channels has SS7 links.

When changing 'Trunk Protocol Type' from 'None' to any other protocol, the Gateway must be r eset. You're not required to reset the gateway when making subsequent changes to 'Trunk Protocol Type'. After the Gateway is reset, the trunks are automatically set to the Unlock state.

Table 19-1: DS1 Trunk Alarm Status

Trunk Color	Trunk Alarm Status
⬜	Locked
🟥	Unlocked and Disabled or Critical Alarm (Unlocked and Enabled)
🟧	Major Alarm (Unlocked and Enabled)
🟨	Minor Alarm (Unlocked and Enabled)
🟦	Warning (Unlocked and Enabled)
	Indeterminate (Unlocked and Enabled)
🟩	Clear, OK (Unlocked and Enabled)

Figure 19-1: Trunk List for Mediant 2000 Module #1 or 2



DS1 Carriers List

#	Protocol	Framing Method	Line Code	Line Status	Activity	D-Channel Status	NFAS Group Number
1	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
2	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
3	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
4	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
5	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
6	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
7	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0
8	E1Transparen...	E1_FRAMING_MFF_C...	acHDB3	LOF,LOS,Active,...	notAvailable	notApplicable	0

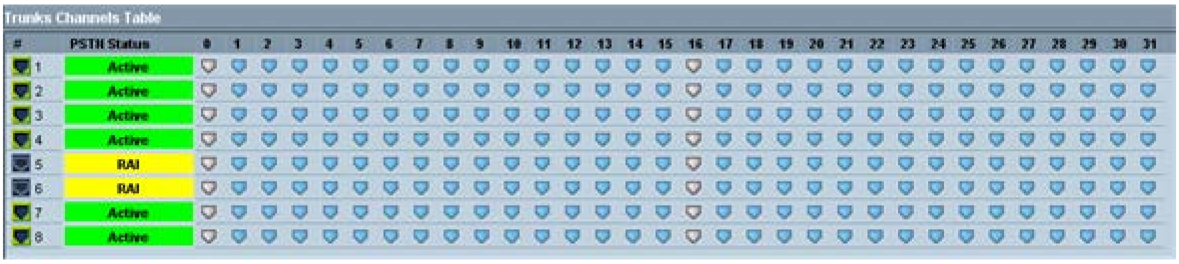
19.2 Trunk Channel Call Status

The Trunks Channel Status screen enables the user to view the status of each one of the channels of each Trunk of the TP board. View the trunks channels by selecting the **Trunks Channel** button at the top of the screen. The following color convention is used to display a trunk channels' call status:

Table 19-2: Trunk Channel Call Status

Channel Color	Channel Call Status
🟩	Active
🟦	Inactive
⬜	Non-Voice
🟪	SS7
🔷	ISDN Signaling (D-channel)
🟨	CAS Blocked

Figure 19-2: Trunk Channel Status



Trunks Channels Table

#	PSTN Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
2	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
3	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
4	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
5	RAI	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
6	RAI	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
7	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
8	Active	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

20 Mediant 2000 and Mediant 3000 SIP and SS7 Navigation Concepts

SIP and SS7 Provisioning Concepts are common for the Mediant 2000 and Mediant 3000 product family.

See Section 'Provisioning Concepts' on page 222 for information on the parameter provisioning types, how to work with table status columns and how to create and apply profiles.

20.1 SS7 Provisioning Navigation Buttons

For SS7-level provisioning rules and configuration, refer to the *MGCP Megaco Mediant 2000 and Mediant 3000 User manual* or the *Product Reference Manual for SIP Gateways*.

The figure below displays the MTP3 SS7 navigation hierarchy links used to provision the Mediant 2000 and Mediant 3000:

Figure 20-1: SS7 Hierarchy Levels-Mediant 3000 and Mediant 2000

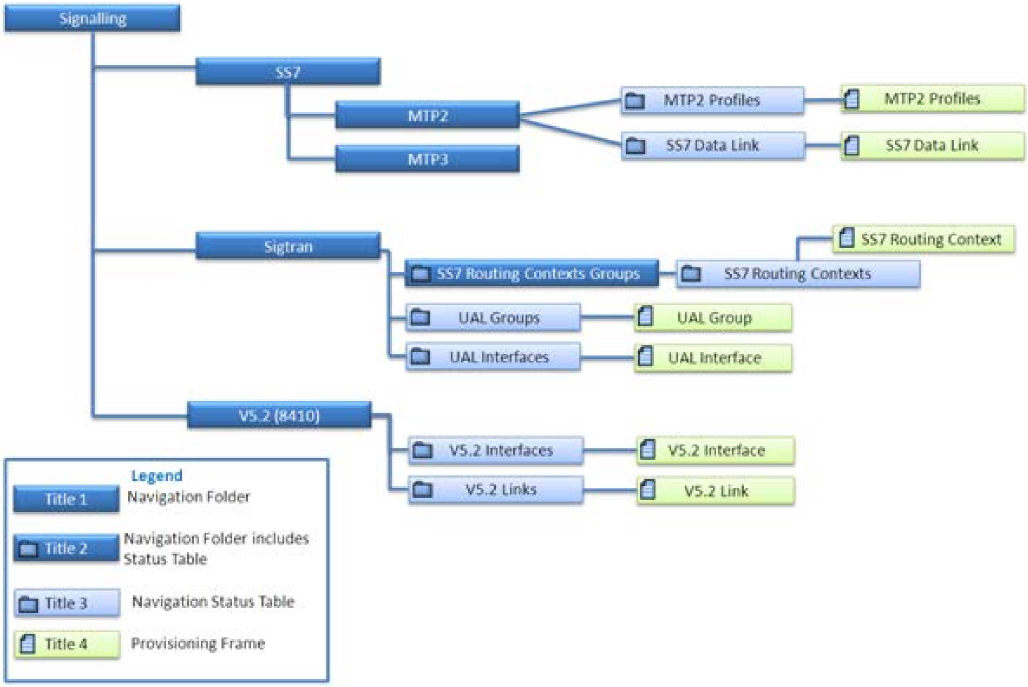
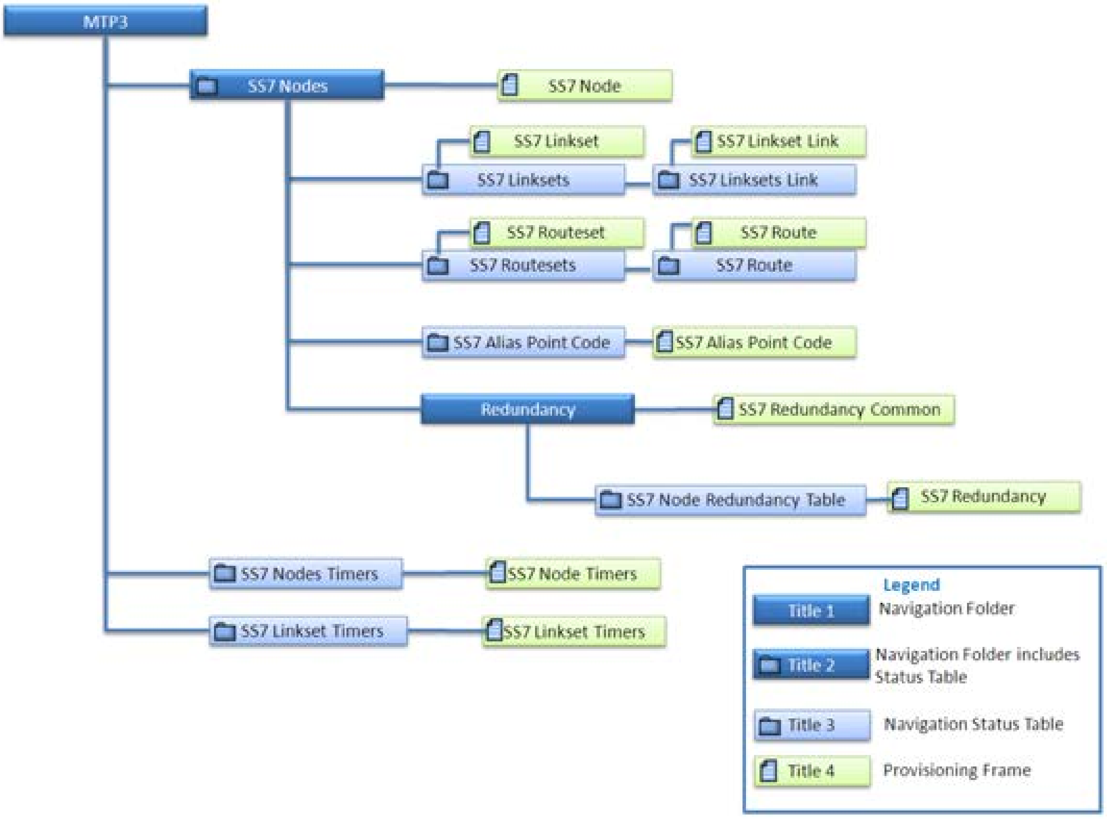


Figure 20-2: MTP3 Hierarchy Levels-Mediant 3000 and Mediant 2000



Part III

Actions and Provisioning

This section describes the EMS GUI actions and parameter provisioning for the specific media gateways.

.

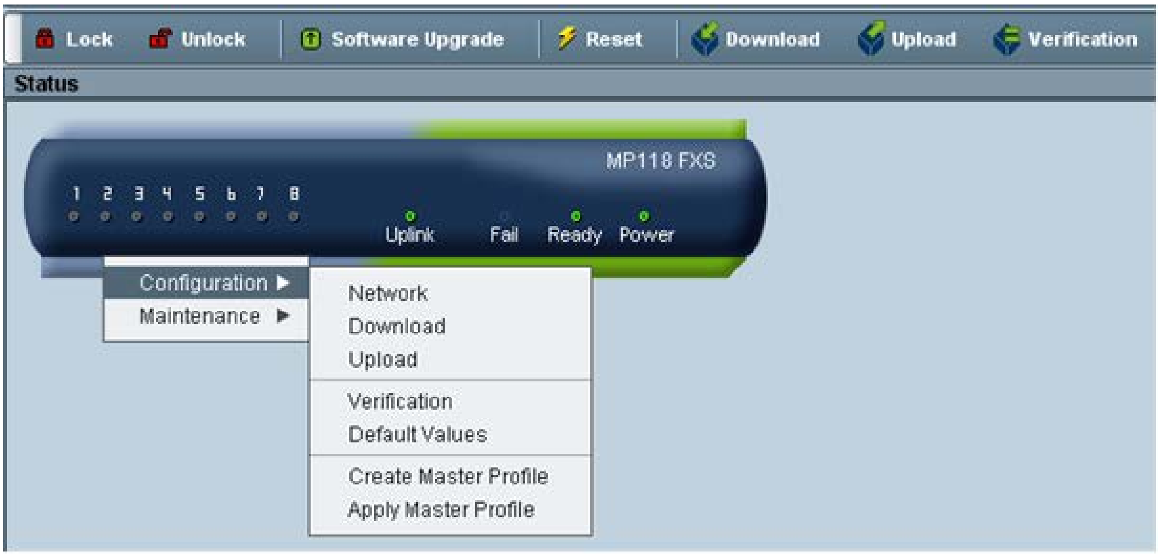
21 CPE Configuration and Maintenance Actions

This section describes the CPE Configuration and Maintenance actions.

21.1 Configuration Actions

All the actions described in this section are supported by right-clicking the gateway and selecting the Configuration Menu or by clicking the appropriate button in the Actions bar. The Actions bar includes a s ubset of the most commonly performed actions and may differ according to the relevant media gateway type and version.

Figure 21-1: Configuration Actions menu

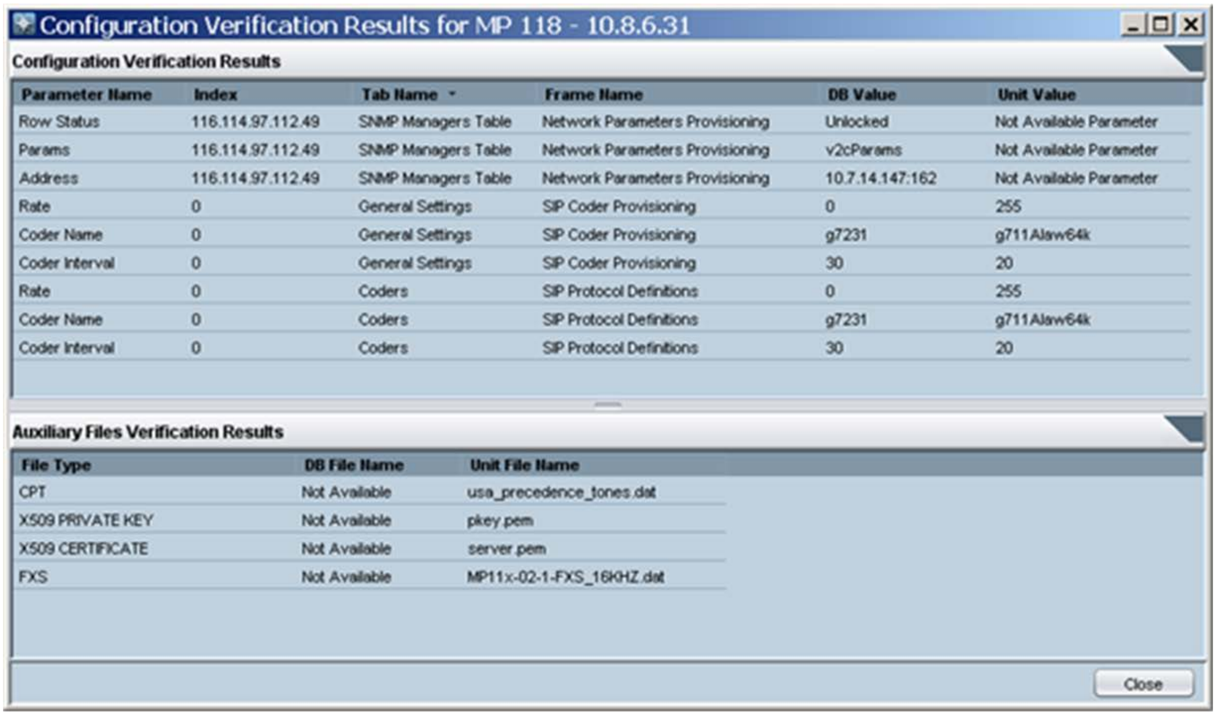


- **Network:** This operation allows modification of the Gateway IP address, Default GW and Subnet Mask.
- **Download**: This operation loads the entire configuration saved in the EMS Database to the media gateway. In addition to provisioned configuration parameters, the user can load Auxiliary files previously loaded to the same Gateway and saved in the EMS Database.

  Note, it is recommended to first perform the Verification action to ensure that only the required configuration is loaded to the gateway.
- **Upload**: Reads the entire current configuration of the media gateway and saves it in the EMS database. Upload does not perform Auxiliary files upload and save into the EMS database.

  Note: It is recommended to first perform the Verification action to ensure that only the required configuration is saved in the EMS database,.
- **Verification**: Compares the entire configuration saved in the EMS to the current configuration of the media gateway (provisioning parameters and auxiliary files). In the case of a mismatch, users can perform a Configuration Download, or Upload the media gateway configuration into the EMS database.

Figure 21-2: Configuration Verification Results



Configuration Verification Results for MP 118 - 10.8.6.31

Configuration Verification Results

Parameter Name	Index	Tab Name	Frame Name	DB Value	Unit Value
Row Status	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	Unlocked	Not Available Parameter
Params	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	v2cParams	Not Available Parameter
Address	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	10.7.14.147:162	Not Available Parameter
Rate	0	General Settings	SIP Coder Provisioning	0	255
Coder Name	0	General Settings	SIP Coder Provisioning	g7231	g711Alaw64k
Coder Interval	0	General Settings	SIP Coder Provisioning	30	20
Rate	0	Coders	SIP Protocol Definitions	0	255
Coder Name	0	Coders	SIP Protocol Definitions	g7231	g711Alaw64k
Coder Interval	0	Coders	SIP Protocol Definitions	30	20

Auxiliary Files Verification Results

File Type	DB File Name	Unit File Name
CPT	Not Available	usa_precedence_tones.dat
X509 PRIVATE KEY	Not Available	pkey.pem
X509 CERTIFICATE	Not Available	server.pem
FXS	Not Available	MP11x-02-1-FXS_16KHZ.dat

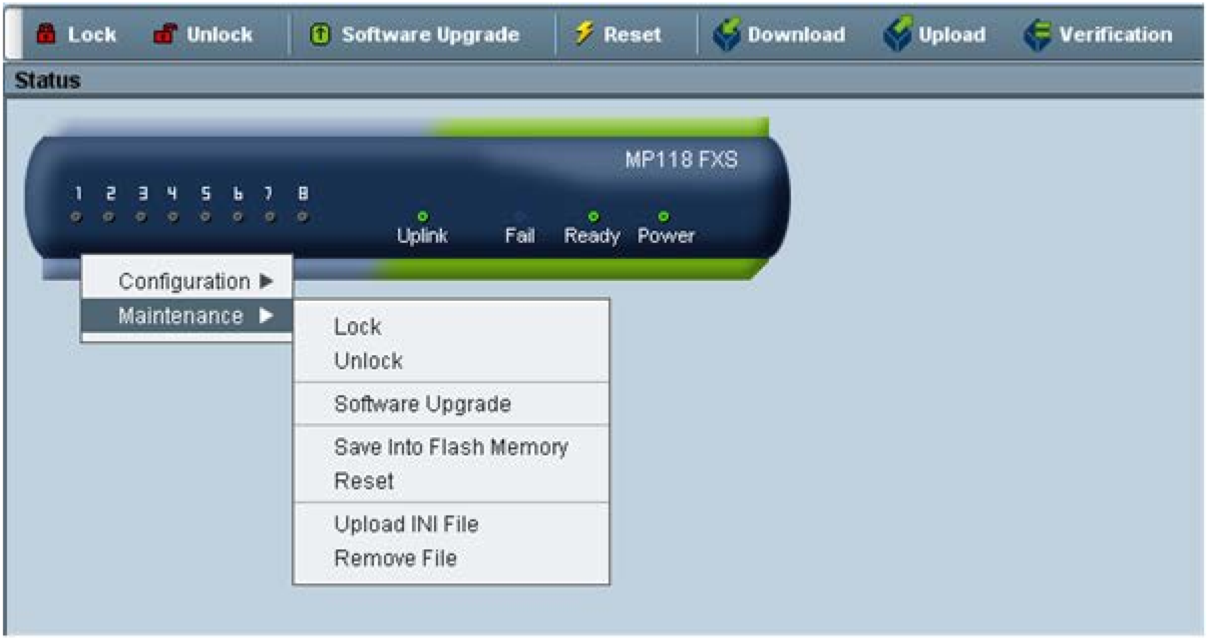
- **Default Values**: Removes all user-defined configurations and restores the media gateway to its factory defaults.

  Note: EMS does not remove the user-defined configuration from the Database. Use the Verification action to review the differences. In case of a mismatch, users can perform a Configuration Download, or Upload the media gateway configuration into the EMS database.

21.2 Maintenance Actions

All the below actions are supported via the gateway right-click option and selection of the Maintenance Menu or by clicking the appropriate icon on the Actions bar. The Actions bar includes a subset of the most commonly performed actions and may differ according to the media gateway type and version.

Figure 21-3: Maintenance Actions menu



- **Lock / Unlock**: Locking / Unlocking of the media gateway. Locking the media gateway, stops call control functionality and enters the gateway to the maintenance state. Unlock returns it to service.
- **Software Upgrade**: Loading a software or regional auxiliary file.
- **Save Into Flash Memory**: Saves the entire media gateway configuration in flash memory so that after reset Configuration Download is not required.
- **Reset**: Select Info Panel or right-click 'Reset' action. To confirm the action, click **OK**; the media gateway is reset.
- **Upload INI File**: This option is defined for debug purposes. The INI file received from gateway is used to assist AudioCodes FAE to perform problem debugging.
- **Remove File**: removed auxiliary file/s from the gateway. When this option is selected, the user is prompted with a list of all the files used by a specific gateway. The user can then select the files they wish to remove.

All the actions below are supported via Trunk and Channel right-click menus.

- **Lock/Unlock Trunk/s** – **Lock** – take the trunk out-of-service and allow modification of its configuration (and specifically of Online configuration parameters); the synchronization with the remote PSTN side will be lost and corresponding voice and signaling traffic will be dropped; locked trunks will remain out-of-service even if the media gateway board is restarted (as a result of lock/unlock maintenance actions or board failure).

> **Note:** If the trunk type is changed from 'Null' or from 'E1' based to 'T1' based (or vice versa), the media gateway must be reset at the end of the provisioning action, or else the Lock / Unlock action on the trunk fails.

- **Activate / Deactivate Trunk/s**
  - **Activate** (can only be applied when trunks are in Unlock state)- Activate trunks after a trunk has been deactivated. When a trunk is activated, it is reconnected to the PSTN network and the relevant AIS alarm is cleared.
  - **Deactivate** (can only be applied when trunks are in Unlock state)- When a trunk is deactivated, it is temporarily disabled from the PSTN network. An AIS alarm signal is sent from the media gateway board to the receiving end of the trunk and an RAI alarm signal is returned to the media gateway (displayed in the EMS Alarm Browser). Use this option for maintenance purposes. For example, the DS1 trunk that you wish to run maintenance tasks has SS7 links on it and therefore you cannot lock it and do not wish to deactivate SS7.

  The following action is specific to the Channel right-click menu:

- **Reset B-channel** – This option restarts a B-channel. If a call is in progress while the B-channel is being restarted, the call is stopped. A B-channel restart does not affect the configuration of the device. B-channel restart can only be done if the D-channel of the trunk to which it belongs is synchronized (see 'D-Channel Status' alarm).

21.3 Performing Actions on Multiple Gateways

This section describes how to perform actions on multiple gateways.

➢ **To perform an action on multiple gateways:**

1. In the MGs Tree Status screen, select the Region under which the media gateways are located.
2. Select one or more media gateways using the CTRL or Shift keys, or by using the mouse. Verify that all media gateways you intend to perform the action on are selected.
3. Right-click and choose the required action option from the pop-up; an Action Result table is displayed showing progress and action results. Note that for specific media gateway types and software versions, some actions in the right-click pop-up menu may be disabled. This implies that in the selected set of media gateways, there are one or more media gateways which cannot support the action that is disabled in the pop-up.

Reader's Notes

22 Provisioning Concepts

This section describes the EMS provisioning concepts.

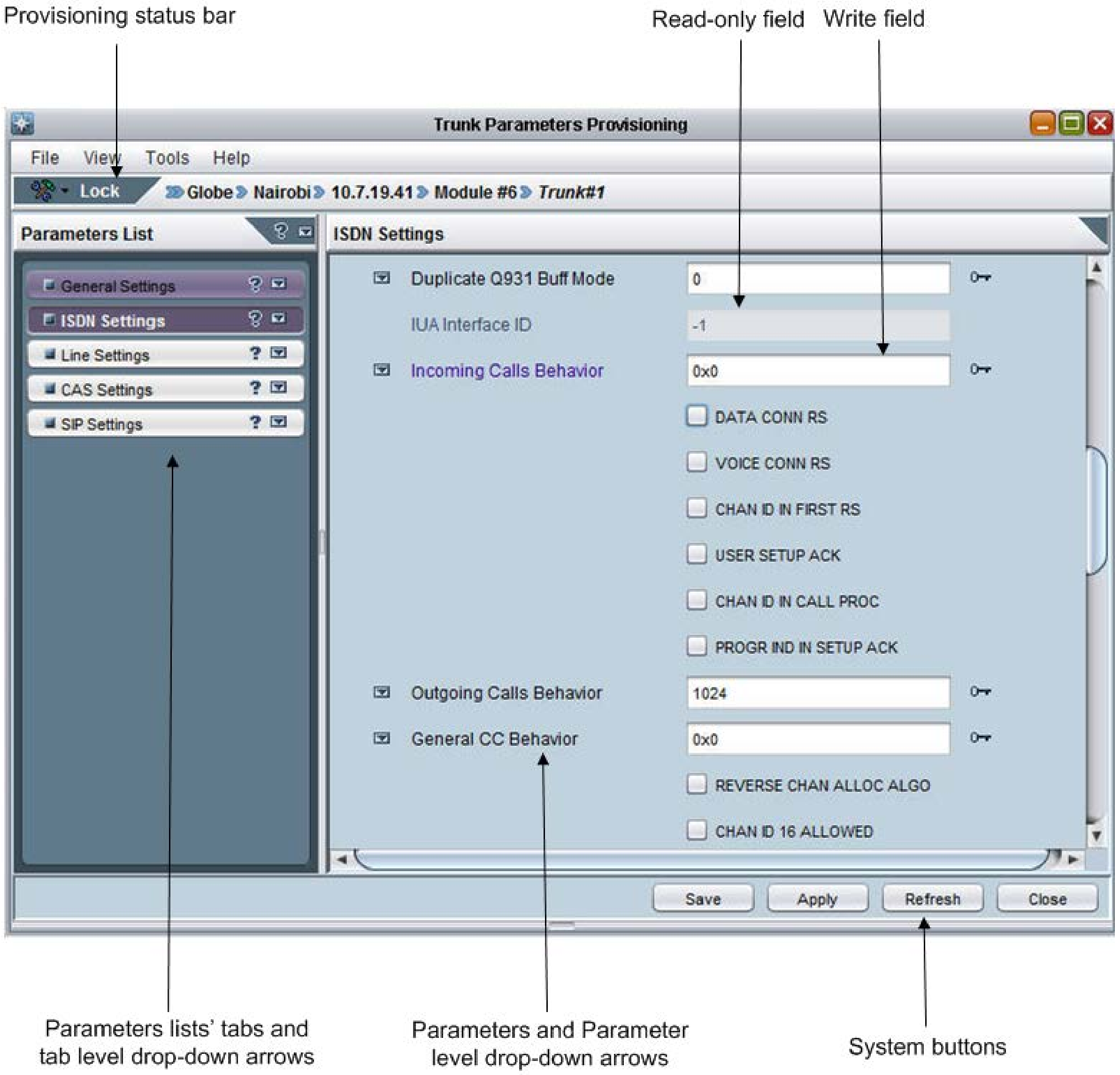
22.1 Working with the EMS's Provisioning Screens

All screens in the EMS that enable operators to provision the media gateways, boards and trunks, in the context of these entities' interfaces, described in this section, are configured according to the same principle.

The provisioning screens are easily and intuitively reached by navigating down (or up as the case may be) the hierarchy links in the Navigation or Configuration pane to select the entity to be provisioned. The next step is to select the desired configuration option in the Configuration pane; the corresponding provisioning screen for this specific entity is displayed.

An example TP board provisioning screen is displayed in the figure below.

Figure 22-1: TP-6310 Board Provisioning Parameters



Duplicate Q931 Buff Mode: 0

IUA Interface ID: -1

Incoming Calls Behavior: 0x0

□ DATA CONN RS

□ VOICE CONN RS

□ CHAN ID IN FIRST RS

□ USER SETUP ACK

□ CHAN ID IN CALL PROC

□ PROGR IND IN SETUP ACK

Outgoing Calls Behavior: 1024

General CC Behavior: 0x0

□ REVERSE CHAN ALLOC ALGO

□ CHAN ID 16 ALLOWED

The Board Provisioning screen displayed in the figure contains the following:

- **Provisioning Status Bar**
  Includes the path of the EMS-managed entity, as well as its Administrative State (Locked/Unlocked) and its Operational State (Enabled/Disabled). The Administrative State of the board can be changed using the Administrative State drop-down arrow.

  For the CPE products, Reset State is displayed. The Reset State of the board can be changed using the Reset State drop-down arrow.

- **Parameters List**

  The Parameters List is in the pane on the left side of the Provisioning screen. The Parameters List categorizes are color-coded for quick operator assessment.

The table below decodes the colors of the category buttons.

Table 22-1: Provisioning Parameters in the Board Provisioning Screen – Color Codes

Color	Meaning
Red	Data error as a result of an operator's modification or a data error produced by the media gateway.
Violet	▪ The list item was modified and all data in it is valid. In case of the CPE products, the button was modified and saved in the database; however, not yet loaded to the VoIP device.
Blue	List item is not modified and all data in it is valid
Bold	Currently viewed list item
Orange (for CPE products only).	The value from the VoIP device is different to the value in the database (can be seen when the Unit Value arrow button is clicked)

- **Provisioning Parameters Button**

  Each Provisioning Parameters button lists all parameters under that category.

  After modifying a parameter, the parameter's name color is changed to violet, and the modified category button's color is changed to violet.

  If a provisioned parameter is invalid, the invalid parameter is colored in red and a tool tip with the corrective instructions appears. The category button name is colored in red as well.

  If a parameter is not editable (read-only), its value and name are grayed (disabled).

- **Drop-down Arrows**

  A drop-down arrow is adjacent to each provisioning parameters category button, and to each parameter in that category.

  Each drop-down combo lists two actions that operators can optionally perform (for each individual parameter and for each provisioning parameters category:

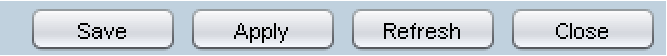
  - Undo modification/s
  - Factory default value - displays the values that the media gateway is initiated with prior to its release.

  Unit Value (exists for CPE products) – displays actual gateway values read from the gateway during the last Refresh or when the screen is opened. In case of a mismatch between the gateway's actual value and the value saved in the database, the parameter and tab name are colored in orange. To synchronize the gateway and the database, either 'Save' the media gateway's value in the database, or 'Apply' the database value to the gateway.

- **System Buttons**

  At the bottom of the Board Parameters Provisioning screen are the following system buttons (refer to the figure below and to the figure above):

Figure 22-2: System Buttons in Board Parameters Provisioning Screen



Save - Save your changes in the EMS database (Applicable only for the CPE products).

Apply - Load your changes to the gateway, and in addition for the CPE products, saves your changes to the EMS Database.

Refresh - Read the current gateway setting (replace your changes with the current data). For low density gateways, reads the current value from the EMS Database.

Cancel - Cancel your changes and close the screen.

- **Working with tables in Provisioning Screens**

  Table information is sometimes displayed as a tab in the provisioning screens. Note the following when working with tables:

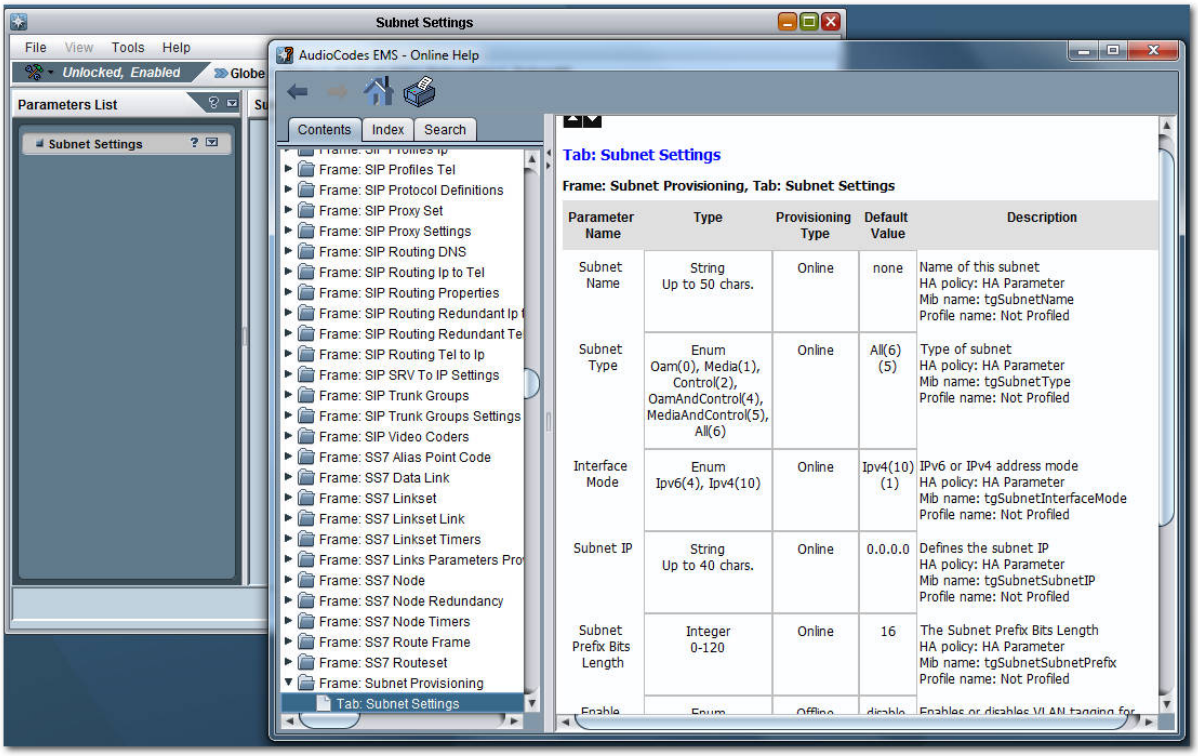
  - Right-clicking on a table row and choosing an Add / Remove / Lock / Unlock action does not then require clicking the **Apply** button; the action is executed immediately. Pressing CTRL-A enables you to select all rows in the configuration table at the same time.
  - When you finish editing a cell in a row, you must click **Enter** to finish editing.
  - After finishing defining table data, you must click the **Apply** button. After your change is applied, a Lock/Unlock action on table rows is required.

- **Online Help and Tooltip**

  During the provisioning process, it's important to understand the meaning of each one of the parameters. Integrated context-sensitive online help is accessed by clicking on the ? mark in the relevant tab to browse to the online help focused on the specified parameters. Online help includes parameter name, type, its range, default value, and most importantly the parameter description (including its MIB name, INI file name and EMS Profile name).

In addition, when the user turns the mouse over the provisioning parameter, the parameter range is displayed in the tooltip.

Figure 22-3: Online Help


Subnet Settings
File
View
Tools
Help
Unlocked, Enabled
Globe
Parameters List
Subnet Settings
AudioCodes EMS - Online Help
Contents
Index
Search
Frame: SIP Profiles Ip
Frame: SIP Profiles Tel
Frame: SIP Protocol Definitions
Frame: SIP Proxy Set
Frame: SIP Proxy Settings
Frame: SIP Routing DNS
Frame: SIP Routing Ip to Tel
Frame: SIP Routing Properties
Frame: SIP Routing Redundant Ip t
Frame: SIP Routing Redundant Te
Frame: SIP Routing Tel to Ip
Frame: SIP SRV To IP Settings
Frame: SIP Trunk Groups
Frame: SIP Trunk Groups Settings
Frame: SIP Video Coders
Frame: SS7 Alias Point Code
Frame: SS7 Data Link
Frame: SS7 Linkset
Frame: SS7 Linkset Link
Frame: SS7 Linkset Timers
Frame: SS7 Links Parameters Pro
Frame: SS7 Node
Frame: SS7 Node Redundancy
Frame: SS7 Node Timers
Frame: SS7 Route Frame
Frame: SS7 Routeset
Frame: Subnet Provisioning
Tab: Subnet Settings

Tab: Subnet Settings

Frame: Subnet Provisioning, Tab: Subnet Settings

Parameter Name	Type	Provisioning Type	Default Value	Description
Subnet Name	String Up to 50 chars.	Online	none	Name of this subnet HA policy: HA Parameter Mib name: tgSubnetName Profile name: Not Profiled
Subnet Type	Enum Oam(0), Media(1), Control(2), OamAndControl(4), MediaAndControl(5), All(6)	Online	All(6) (5)	Type of subnet HA policy: HA Parameter Mib name: tgSubnetType Profile name: Not Profiled
Interface Mode	Enum Ipv6(4), Ipv4(10)	Online	Ipv4(10) (1)	IPv6 or IPv4 address mode HA policy: HA Parameter Mib name: tgSubnetInterfaceMode Profile name: Not Profiled
Subnet IP	String Up to 40 chars.	Online	0.0.0.0	Defines the subnet IP HA policy: HA Parameter Mib name: tgSubnetSubnetIP Profile name: Not Profiled
Subnet Prefix Bits Length	Integer 0-120	Online	16	The Subnet Prefix Bits Length HA policy: HA Parameter Mib name: tgSubnetSubnetPrefix Profile name: Not Profiled
Enable	Enum	Offline	disable	Enables or disables VLAN tagging for

22.1.1 Provisioning Procedure for Mediant 5000 and Mediant 8000

This section covers the Mediant 5000 Media Gateway and Mediant 8000 Media Gateways.

➢ **To provision a M ediant 5000 Media Gateway and Mediant 8000 M edia Gateway, follow these procedures:**

1. Navigate to the element/entity you wish to provision, select it (for a gateway, select it in the MGs List under the region; for a board, select it in the graphic representation of the gateway; and for a trunk, select it in the Trunk List.
2. In the Navigation pane, select the desired provisioning option or in the corresponding list screen, select a row.
3. In the Configuration pane (located below the Navigation pane), select the desired provisioning option; the corresponding provisioning screen for the selected element is displayed.
4. Modify the required parameters using the interface-context buttons.
5. Change the managed element/entity to the **Locked** Administrative State (refer to the bullet 'Provisioning Status Bar', above).
6. Click the **Apply** system button; your changes are loaded to the gateway.
7. Change the managed element/entity to the **Unlocked** Administrative State (refer to the bullet 'Provisioning Status Bar', above) to return it to service.
8. Click the **OK** or **Cancel** button to exit the provisioning screen.

Note:

- After a successful **Apply**, all parameters and tabs previously colored in purple will return to their normal colors (black).
- If you make a mistake in the provisioning process, the system notifies you and prompts you for the corrective action.

22.1.2 Provisioning Procedure for CPE Products

This section describes the provisioning procedure for CPE products.

➤ **To provision these VoIP devices, follow these procedures:**

1. Navigate to the element/entity you wish to provision, select it (for a gateway, select it in the MGs List under the region; for a board, select it in the graphic representation of the gateway; and for a trunk, select it in the Trunk List).
2. In the Configuration pane (located below the Navigation pane), select the desired provisioning option; the corresponding parameters provisioning screen for that element is displayed.
3. If the device is currently not connected to the network, its Parameters Provisioning screen title bar will include a suffix indicating 'Offline'.
4. Modification of single parameters: Modify the required parameters using the interface-context buttons.
5. Modification of table parameters: Some provisioning screens include Tables.
   a. **Add Row**: To define a new row in the table, right-click the table tab and select the option **Add Row**.
   b. **Modify Row Data**: To modify a row's data, double-click the relevant cell, change the data and exit the cell by clicking on any object in the screen. Verify that the cell is not in focus.
   c. **Lock / Unlock Row**: To make a row operational, unlock it by clicking **Unlock** in the Actions bar or by right-clicking and choosing option **Unlock** from the row menu.
   d. **Remove Row**: To remove a row, right-click the row and choose the option **Remove**.
   e. Note that all the right-click actions are sent immediately to the device, The **Apply** button only applies parameter changes.
6. Click the **Apply** system button; your changes are loaded to the device and saved in the database.
7. When working in Offline mode, save your changes in the EMS database by clicking **Save**. After the device is connected to the network, click **Configuration Download** in the Info pane to load all changes previously saved in the EMS database to the device.
8. If Reset State is marked as **Reset Needed**, reset the gateway by clicking **Reset** in the Actions bar to return it to service (or clicking **Board Reset** if you are provisioning a board).
9. Click the **OK** or **Cancel** button to exit the provisioning screen.

Note:

- After a successful **Apply**, all parameters and tabs previously colored in purple will return to their normal colors (black).
- If you make a mistake in the provisioning process, the system notifies you and prompts you for the corrective action.

22.2 Parameters Provisioning Types

The EMS features the following provisioning parameter types:

- Instant (changes are applied to the media gateway after Clicking **Apply/OK**).
- Online (the modified entity must be locked prior to applying the changes)
- Offline (the modified entity must be locked prior to applying the changes and the physical component (board or media gateway) must be locked.

An icon indicating parameter-provisioning *type* is placed adjacent to the field and only applies to *modifiable parameters*. Each parameter displayed in a provisioning parameters screen is indicated as one of the following types (refer to the table below):

Table 22-2: Indication Mapping Summary

Parameter Provisioning Type	Indication / Gateway Type	Description
Instant	No indication	Click Apply, OK button to load changes to the media gateway.
Online	🔑	Lock / Unlock modified entity (trunk, for example)
Offline	🔐 Trunking Gateway	Lock/Unlock the physical entity within/under which the managed entity is located, and the managed entity itself
	⚡ CPE products	Reset the module (TPM). In the Mediant 2000, there can be two TPMs in the case of a 16-trunk configuration)

- **Online** - To configure an 'Online' mode parameter (indicated in the EMS by the icon 🔑 adjacent to the parameter), you need to lock *only the entity containing the parameter*. *You do not need to lock the board/media gateway* containing the entity. The mode is called 'Online' because the parameter can be configured without resetting any board in the media gateway.
- **Offline -** To configure an 'Offline' mode parameter (indicated in the EMS by the icon 🔐 adjacent to the parameter), you need to lock the board/media gateway containing the entity as well as the entity to configure the entity's parameter. The mode is called 'Offline' because all calls active on the board/media gateway containing the entity's parameter are dropped when you lock the board/media gateway and entity to configure the parameter.
- **Instant -** An 'Instant' mode parameter can be configured on the fly; the configuration takes effect immediately. No icon is displayed adjacent to the parameter in the EMS GUI. No locking or unlocking of the entity or of the board/media gateway is required to perform the configuration.

22.3 Parameters HA Type

This sign is used for Mediant 5000 and Mediant 8000 gateways.

The EMS features three provisioning parameter types:

- Instant (changes are applied to the media gateway after clicking **Apply/OK**).
- Online (the modified entity must be locked prior to applying the changes)
- Offline (the modified entity must be locked prior to applying the changes and the physical component (board or media gateway) must be locked.

An icon indicating parameter-provisioning type is placed adjacent to the field and only applies to modifiable parameters. Each parameter displayed in a provisioning parameters screen is indicated as one of the following types (refer to the table below):

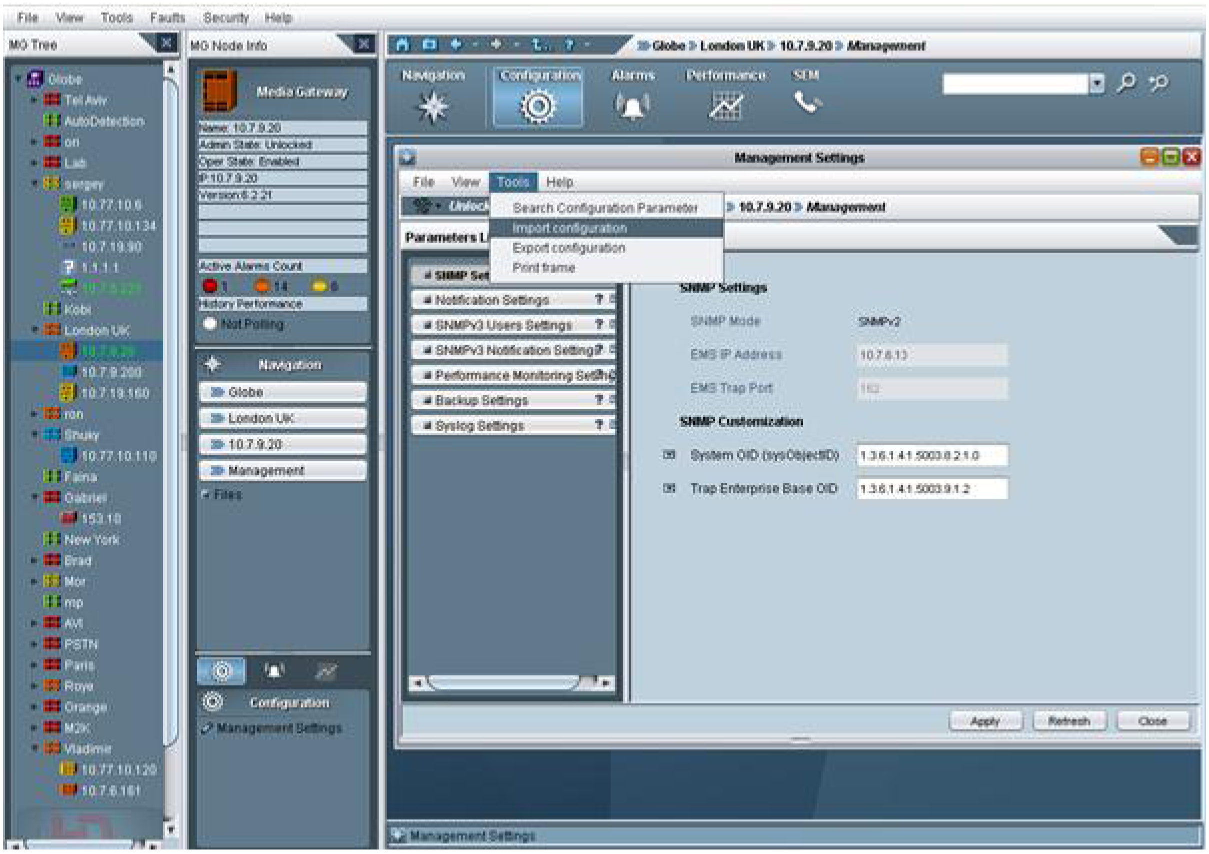
Table 22-3: Indication Mapping Summary-Parameters HA Type

Parameter Provisioning Type	Indication	Description
No Affect on HA	No indication	Modification of this parameter will not affect High Availability Feature
Affects HA	HA✗	Modification of these parameters will affect HA of the TP board. For more information, refer to Redundancy provisioning Frame to review affected boards.
Partially Affects HA	HA✓✗	Modification of these parameters might affect HA of the TP board. For more information, refer to Redundancy provisioning Frame to review affected boards.

22.4 Exporting, Importing an Entity Configuration as a File

This section describes Exporting, Importing an Entity Configuration as a File.

Figure 22-4: Importing an Entity Configuration



Name: 10.7.9.20
Admin State: Unlocked
Oper State: Enabled
IP:10.7.9.20
Version:6.2.21

SNMP Settings

SNMP Mode: SNMPv2
EMS IP Address: 10.7.6.13
EMS Trap Port: 162

SNMP Customization

System OID (sysObjectID): 1.3.6.1.4.1.5003.8.2.1.0
Trap Enterprise Base OID: 1.3.6.1.4.1.5003.9.1.2

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

Operators can then 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, 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 file is imported, operators can view the imported parameter configurations in the provisioning screen and decide whether to apply the configurations to the entity (by clicking the **Apply** button).

After operator has imported the entity configuration file into the EMS, it is suggested to use profiles to spread the configuration over the different entities of the objects managed by same EMS.

➢ To export an entity's parameters provisioning screen as a file:

1. Open the parameters provisioning screen of the entity to be exported.
2. In the Tools menu, choose the option **Export Configuration**; the 'Select File' screen opens (refer to the figure below).
3. Select the folder where you want the configuration file to be saved, define the 'File Name' field and click **OK**; a file with the suffix *.xml* is created.

➢ To import the .xml file into an entity:

1. Open the parameters provisioning screen of the entity into which you want to import the *xml* file.
2. In the Tools menu, choose the option **Import Configuration**; the 'Select File' screen opens (refer to the figure above).
3. Navigate to the saved *xml* configuration file and double-click it; the entity's provisioning screen now displays the parameter configurations retrieved from the *xml* file; parameter configurations that differ from the previous configuration are colored in purple.

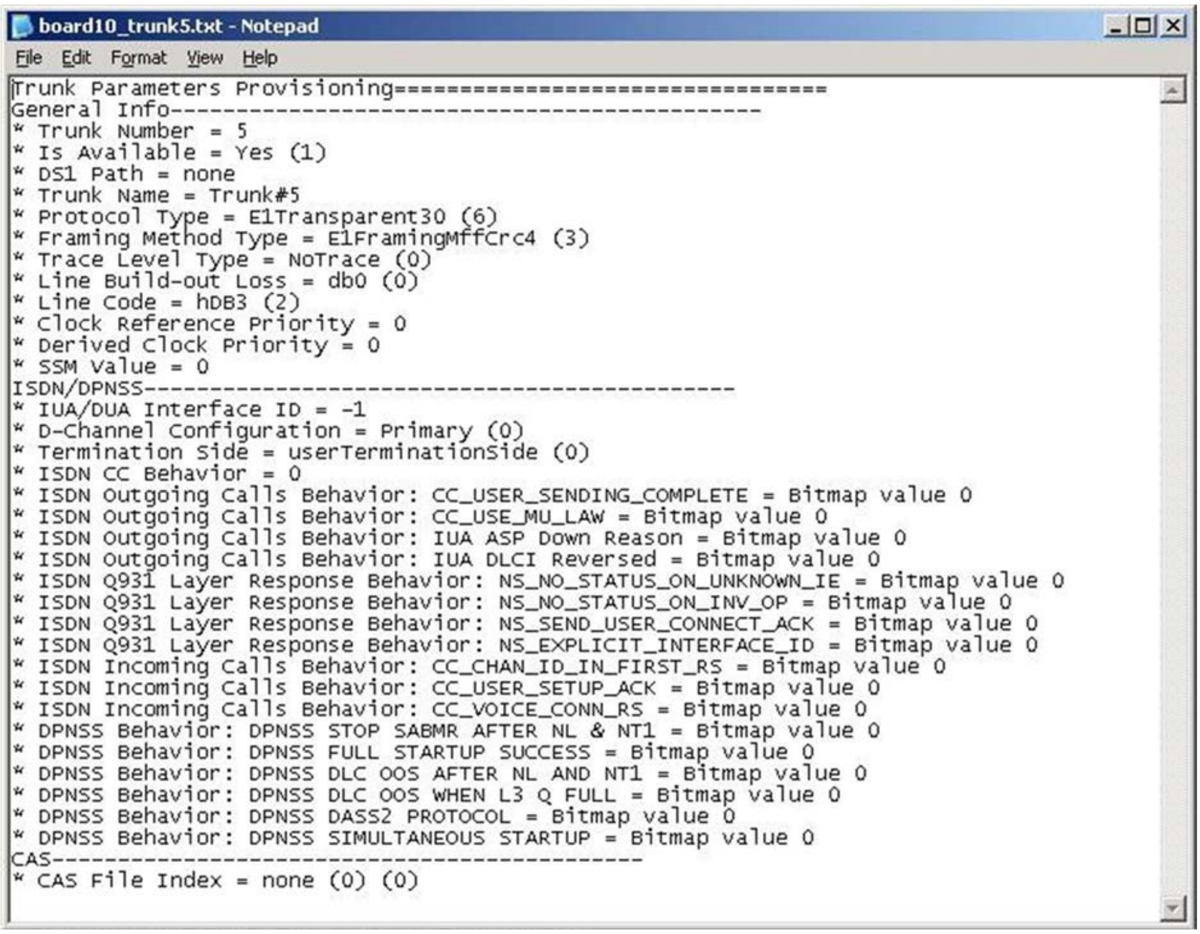
22.5 Printing an Entity's Configuration as a File

The EMS enables operators to export an entire entity's parameters provisioning screen as a printable and easily readable file. The file is in readable *txt* format. An example of a Trunk Level configuration is displayed in the figure below.

➢ To print an entity's parameters provisioning screen as a file:

1. Open the parameters provisioning screen of the entity to be exported.
2. In the 'Tools' menu, choose option **Print Frame**; the 'Select File' screen opens.
3. Select the folder where you want the configuration file to be saved, define the field 'File Name' and click **OK**; a file with the suffix *.txt* is created.

Figure 22-5: Trunk Print Format



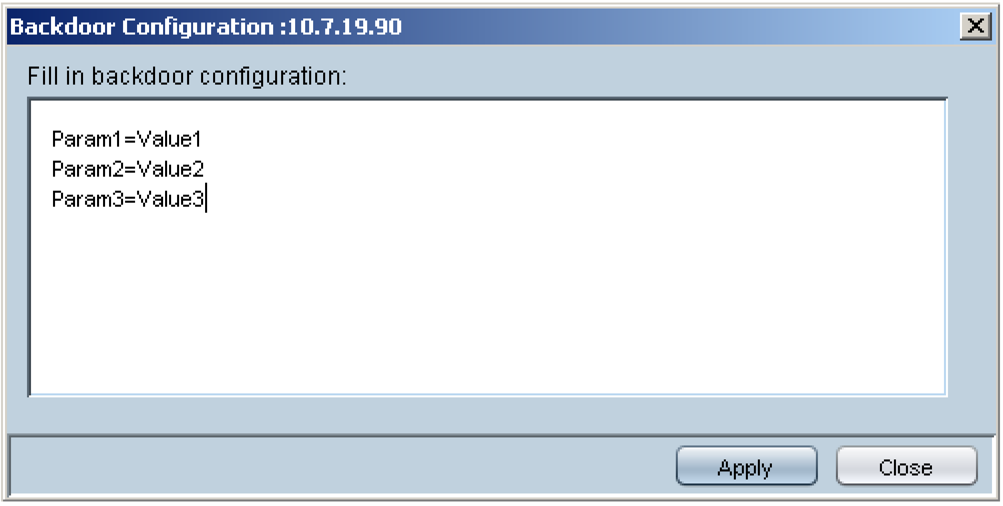
```
Trunk Parameters Provisioning=================================
General Info--------------------------------------------------
* Trunk Number = 5
* Is Available = Yes (1)
* DS1 Path = none
* Trunk Name = Trunk#5
* Protocol Type = E1Transparent30 (6)
* Framing Method Type = E1FramingMffCrc4 (3)
* Trace Level Type = NoTrace (0)
* Line Build-out Loss = db0 (0)
* Line Code = hDB3 (2)
* Clock Reference Priority = 0
* Derived Clock Priority = 0
* SSM Value = 0
ISDN/DPNSS----------------------------------------------------
* IUA/DUA Interface ID = -1
* D-Channel Configuration = Primary (0)
* Termination Side = userTerminationSide (0)
* ISDN CC Behavior = 0
* ISDN Outgoing Calls Behavior: CC_USER_SENDING_COMPLETE = Bitmap value 0
* ISDN Outgoing Calls Behavior: CC_USE_MU_LAW = Bitmap value 0
* ISDN Outgoing Calls Behavior: IUA ASP Down Reason = Bitmap value 0
* ISDN Outgoing Calls Behavior: IUA DLCI Reversed = Bitmap value 0
* ISDN Q931 Layer Response Behavior: NS_NO_STATUS_ON_UNKNOWN_IE = Bitmap value 0
* ISDN Q931 Layer Response Behavior: NS_NO_STATUS_ON_INV_OP = Bitmap value 0
* ISDN Q931 Layer Response Behavior: NS_SEND_USER_CONNECT_ACK = Bitmap value 0
* ISDN Q931 Layer Response Behavior: NS_EXPLICIT_INTERFACE_ID = Bitmap value 0
* ISDN Incoming Calls Behavior: CC_CHAN_ID_IN_FIRST_RS = Bitmap value 0
* ISDN Incoming Calls Behavior: CC_USER_SETUP_ACK = Bitmap value 0
* ISDN Incoming Calls Behavior: CC_VOICE_CONN_RS = Bitmap value 0
* DPNSS Behavior: DPNSS STOP SABMR AFTER NL & NT1 = Bitmap value 0
* DPNSS Behavior: DPNSS FULL STARTUP SUCCESS = Bitmap value 0
* DPNSS Behavior: DPNSS DLC OOS AFTER NL AND NT1 = Bitmap value 0
* DPNSS Behavior: DPNSS DLC OOS WHEN L3 Q FULL = Bitmap value 0
* DPNSS Behavior: DPNSS DASS2 PROTOCOL = Bitmap value 0
* DPNSS Behavior: DPNSS SIMULTANEOUS STARTUP = Bitmap value 0
CAS-----------------------------------------------
* CAS File Index = none (0) (0)
```

22.6 Backdoor Configuration for CPE Products

In very rare circumstances, the EMS application may not include specific provisioning parameters or tables which are supported via the gateway INI file provisioning. In these cases, the user should use the Backdoor Configuration screen and inform an AudioCodes FAE engineer to open a trouble ticket in reference to the missing parameter.

To open the Backdoor parameters configuration screen, select **Tools > Configuration Backdoor** option in any provisioning screen of the required gateway. Each one of the parameters or table rows should be inserted as a separate row in the screen. It should be added exactly as it is defined in the INI file.

Figure 22-6: Backdoor Configuration



Backdoor Configuration :10.7.19.90

Fill in backdoor configuration:

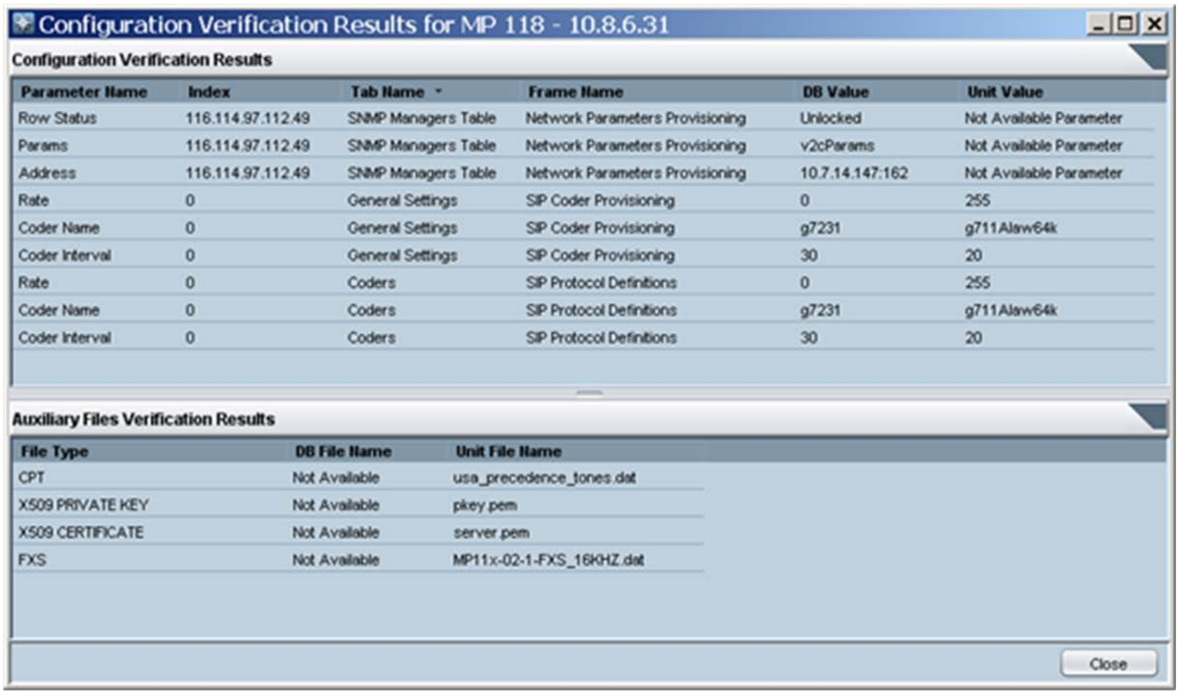
```
Param1=Value1
Param2=Value2
Param3=Value3
```

Notes: Backdoor parameters are downloaded directly to the gateway and are not saved in the EMS Database, and therefore they are not downloaded as part of the Configuration Download and are not tested as part of the Upload and Verification commands.

22.7 Configuration Verification, Download for CPE Products

Configuration Verification is a process of verifying that the configuration saved in the EMS database tallies with the actual media gateway configuration. In the event of inconsistencies, Operators are notified of the mismatch, which they can then fix by working with the EMS's parameter provisioning screens. The Configuration Verification Results screen (refer to the figure below) displays all EMS-saved configuration parameters that are discrepant with the actual media gateway configuration parameters. The names of discrepant parameters are listed under the 'Parameter Name' column, adjacent to which are the 'Screen Name' and 'Tab Name' columns.

Figure 22-7: Configuration Verification Results



Configuration Verification Results for MP 118 - 10.8.6.31

Configuration Verification Results

Parameter Name	Index	Tab Name	Frame Name	DB Value	Unit Value
Row Status	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	Unlocked	Not Available Parameter
Params	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	v2cParams	Not Available Parameter
Address	116.114.97.112.49	SNMP Managers Table	Network Parameters Provisioning	10.7.14.147:162	Not Available Parameter
Rate	0	General Settings	SIP Coder Provisioning	0	255
Coder Name	0	General Settings	SIP Coder Provisioning	g7231	g711Alaw64k
Coder Interval	0	General Settings	SIP Coder Provisioning	30	20
Rate	0	Coders	SIP Protocol Definitions	0	255
Coder Name	0	Coders	SIP Protocol Definitions	g7231	g711Alaw64k
Coder Interval	0	Coders	SIP Protocol Definitions	30	20

Auxiliary Files Verification Results

File Type	DB File Name	Unit File Name
CPT	Not Available	usa_precedence_tones.dat
X509 PRIVATE KEY	Not Available	pkey.pem
X509 CERTIFICATE	Not Available	server.pem
FXS	Not Available	MP11x-02-1-FXS_16KHZ.dat

Configuration Download is the process of loading configuration changes (performed by the operator) to the managed media gateway .

Each download action can be performed by clicking the **Configuration Download** link in the Information Pane, or from the MGs List.

From the MGs List, each of the actions can be performed for a single media gateway , or for a set of selected media gateways.

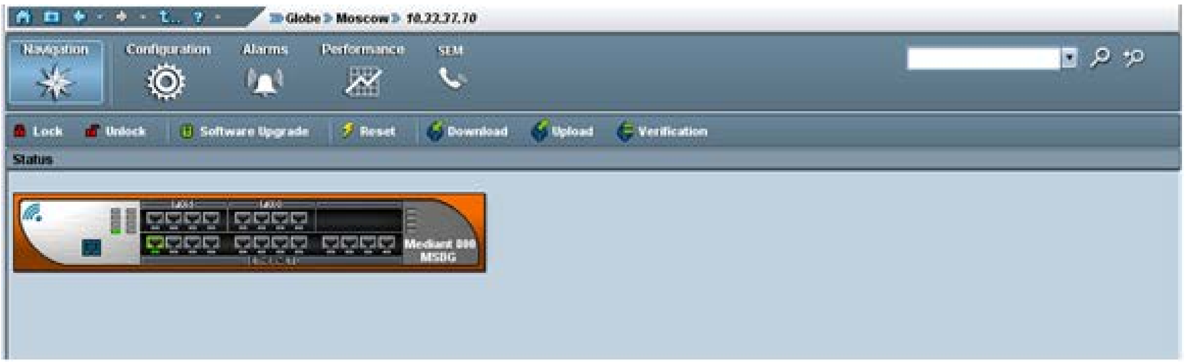
22.8 Searching for a Provisioned Parameter

The EMS parameter search 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.

➢ To perform a Basic Search:

1. Type the required string or its substring, or alternatively select one of the previously searched strings. Click the 'Search' button.

Figure 22-8: Parameter Search Drop-down list

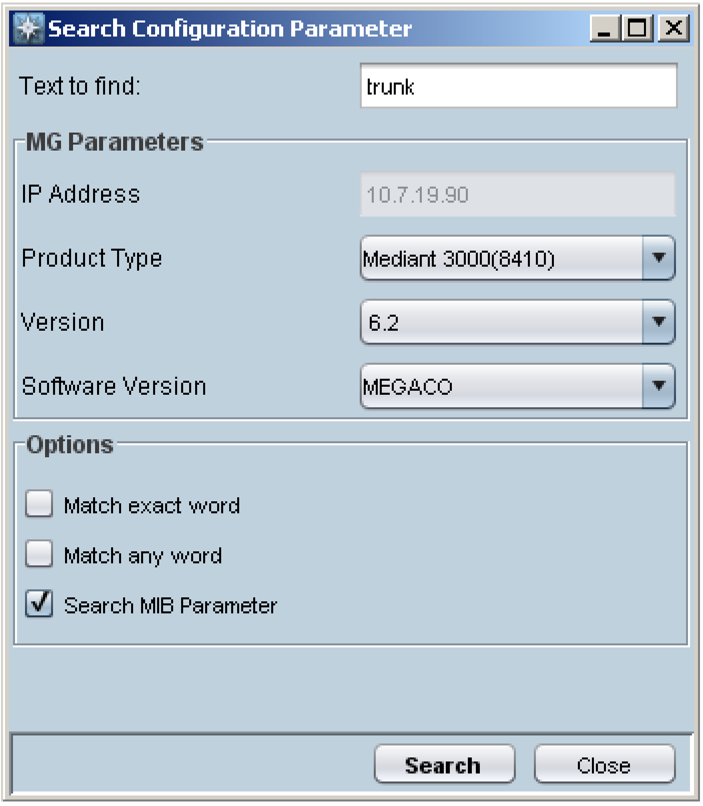


➢ To perform an Advanced Search:

1. Click the **Advanced Search** button the Advanced Search Configuration parameter dialog screen is displayed (as below).
2. Enter the Parameter Name (or part thereof).
3. Choose the Product Type and Software Version from these two fields' drop-down lists.
4. Enhance your search for a provisioned parameter (if you need to) by checking the **Match case** and/or **Match whole word only** check boxes. For example, if you only recall part of the parameter name, for example “IP”, you can verify the **Match case** check box and the 'Match whole word only' check box.
5. Click the **Search** button; the Search Result screen opens, displaying a list of parameters addressing the criteria you defined previously in the Search Provisioned Parameter screen, with Tab Name and Screen Name columns indicating location. Use the information under the Tab Name and the Frame Name to help you navigate efficiently and quickly to the EMS screen (frame) in which the parameter (whose configured value you need to view and/or reconfigure) is displayed.

Notes: Provisioning parameters differ from platform to platform and version to version and from product to product, therefore it's very important to define the exact product and version.

Figure 22-9: Advanced Search Configuration Parameter Dialog



Text to find: trunk

MG Parameters

IP Address: 10.7.19.90

Product Type: Mediant 3000(8410)

Version: 6.2

Software Version: MEGACO

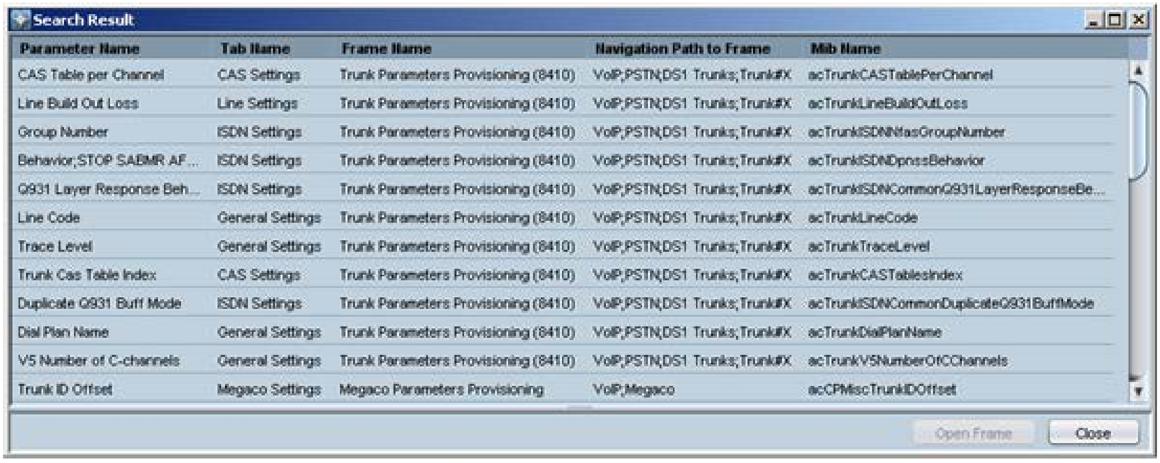
Options

☐ Match exact word

☐ Match any word

☑ Search MIB Parameter

Figure 22-10: Advanced Search Configuration Results Dialog



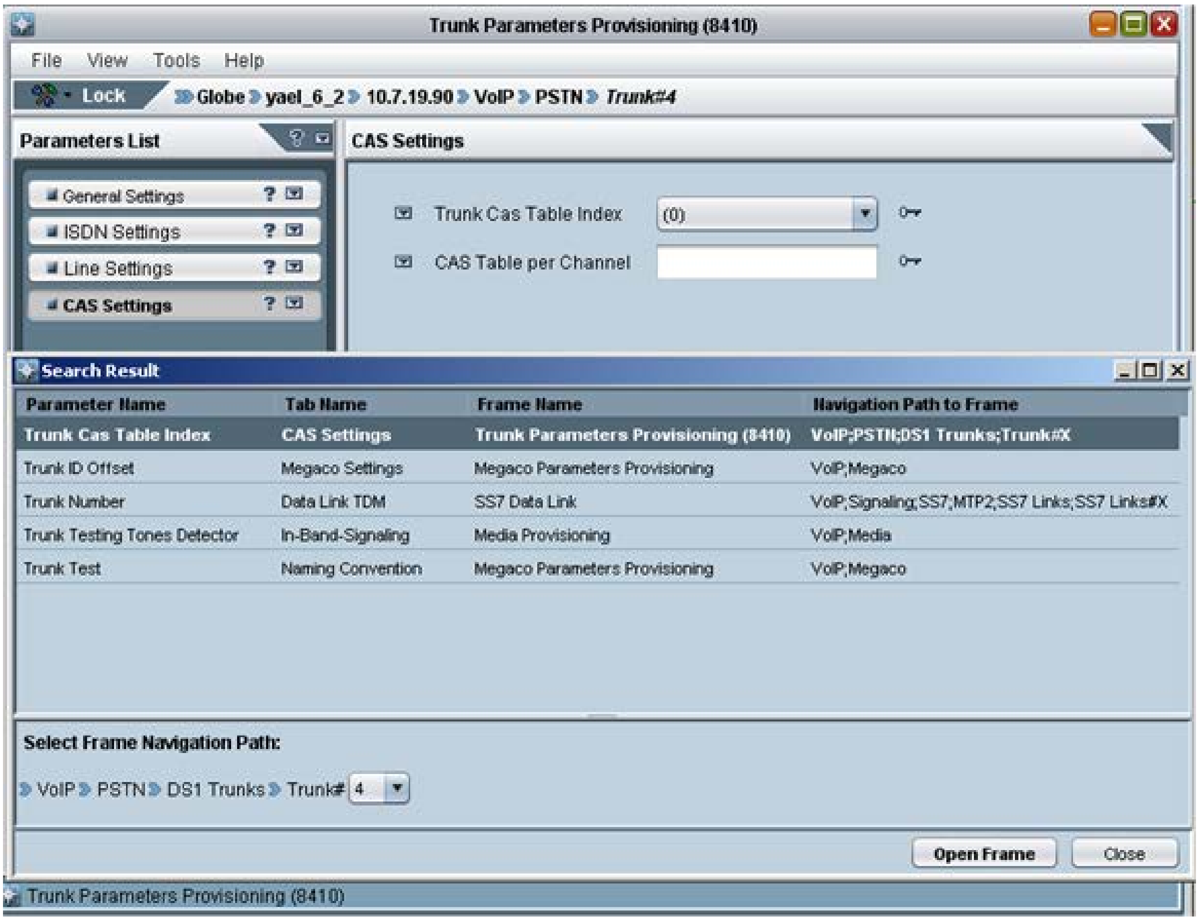
Parameter Name	Tab Name	Frame Name	Navigation Path to Frame	Mib Name
CAS Table per Channel	CAS Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkCASTablePerChannel
Line Build Out Loss	Line Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkLineBuildOutLoss
Group Number	ISDN Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkISDNNfasGroupNumber
Behavior;STOP SABMR AF...	ISDN Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkISDNDpnssBehavior
Q931 Layer Response Beh...	ISDN Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkISDNCommonQ931LayerResponseBe...
Line Code	General Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkLineCode
Trace Level	General Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkTraceLevel
Trunk Cas Table Index	CAS Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkCASTablesIndex
Duplicate Q931 Buff Mode	ISDN Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkISDNCommonDuplicateQ931BuffMode
Dial Plan Name	General Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkDialPlanName
V5 Number of C-channels	General Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkV5NumberOfCChannels
Trunk ID Offset	Megaco Settings	Megaco Parameters Provisioning	VoIP;Megaco	acCPMiscTrunkIDOffset

➢ Navigating to the searched entity:

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

  For example, for specific trunk parameters, in the Navigation path frame, a drop-down list enables you to select a specific board number and trunk number. You can then open the specific provisioning frame for the selected board and trunk.

Figure 22-11: Advanced Search Results screen and related Provisioning screen



Trunk Cas Table Index (0)

CAS Table per Channel

Parameter Name	Tab Name	Frame Name	Navigation Path to Frame
Trunk Cas Table Index	CAS Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X
Trunk ID Offset	Megaco Settings	Megaco Parameters Provisioning	VoIP;Megaco
Trunk Number	Data Link TDM	SS7 Data Link	VoIP;Signaling;SS7;MTP2;SS7 Links;SS7 Links#X
Trunk Testing Tones Detector	In-Band-Signaling	Media Provisioning	VoIP;Media
Trunk Test	Naming Convention	Megaco Parameters Provisioning	VoIP;Megaco

Select Frame Navigation Path:

VoIP › PSTN › DS1 Trunks › Trunk# 4

The context sensitive search options are always visible in the right-hand corner of the EMS toolbar. In addition, the Advanced Search Configuration dialog can be displayed from the EMS Tools menu.

Reader's Notes

23 Gateway Installation, Software Upgrade and Regional Files Distribution

Software can be loaded to a gateway to update the current software version and to provide the appropriate regional files.

During the software upgrade process, the gateway configuration is saved.

For the Mediant 5000 media gateway / Mediant 8000 Media Gateway, online software upgrade is supported (the gateway continues its operation uninterruptedly during the software upgrade).

Software loading involves two procedures:

- Introduce new files to the EMS by adding files to the Software Manager.
- Load the required file/s to the gateway.

23.1 Software Manager

See Section 'Software Manager' on page 65.

23.2 Software Upgrade for CPE and Blades

This section describes the software upgrade for CPEs and blades.

➢ **To load software to CPE and blades, follow these procedures:**

1. Either select the media gateway to which to load files in the MG Tree and choose **Software Upgrade** from the Info pane, or select multiple devices in the Regions table and choose **Software Upgrade** from the right-click pop-up menu.
2. Select the set of files to load to the device/s. Since the Software Manager is context sensitive, only the files available for the selected media gateway are displayed.
3. Wait for the operation result prompt; in both cases, the EMS opens the Software Manager with a subset of software files which can be loaded to the selected entities.

Notes:

- In the event that multiple gateways are selected and the gateways are of different types, the Software Manager only includes files that can be loaded to all the gateways together (it might be an empty list).
- Each time a new *cmp* file is downloaded, the device's flash memory is cleaned and Regional files must be loaded again (even if they were not changed).
- Overall size of the file loaded to the MediaPack should not exceed 7 MB.

The software distribution process is performed via HTTP. The default password received by the VoIP device at AudioCodes is used to connect the HTTP server.

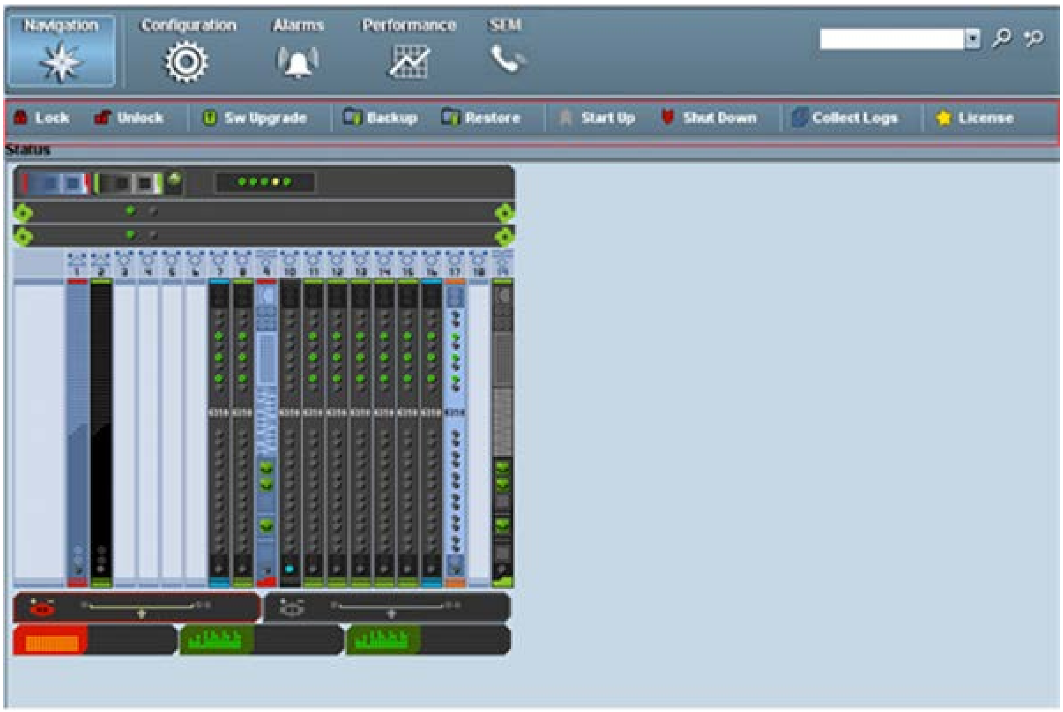
23.3 Mediant 5000/Mediant 8000 Maintenance Actions

This section refers to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway. Before performing an Online Software Upgrade, refer to the *Mediant 5000* and *Mediant 8000 IOM* for detailed information on s ite preparation and the Online Software Upgrade process.

➢ To perform maintenance actions:

1. In the MG Tree, select the gateway on which maintenance action is required.
2. In the Actions bar, click the relevant maintenance action. For example, **Lock** to lock the gateway.

Figure 23-1: Maintenance Actions Icon and Popup Menu



3. For the 'Sw Upgrade' pop-up menu option: In the 'Software Manager' screen, select the *tar* or *tar.gz* file to load to the device and click **OK**; the Software Upgrade Wizard opens and guides you through the process.

The software distribution process is performed via FTP and Telnet. The EMS server implements the FTP client. The Mediant 5000 Media Gateway and Mediant 8000 Media Gateway have an FTP server.

23.3.1 Locking and / Unlocking the Gateway

The **Operational State** of the MO cannot be altered. Instead you can alter the **Administrative State** of the MO by performing a lock or unlock action. If the action succeeds, the **Operational State** is changed to the corresponding value as soon as the factual operability is updated.

It may take some time for the operability state of an MO to change – e.g., it takes a few minutes for a Media Gateway board to complete an unlock action. In the intermediate state, the **Administrative State** of the corresponding MO is unlocked, but the **Operational State** of the MO is disabled. As soon as the Media Gateway board returns to service its **Operational State** is enabled.

Notes: It may take some time for the operability state of an MO to change – e.g., it takes a few minutes for a Media Gateway board to complete an unlock action. In the intermediate state, the **Administrative State** of the corresponding MO is unlocked, but the **Operational State** of the MO is disabled. As soon as the Media Gateway board returns to service its **Operational State** is enabled.

23.3.2 License Key Update

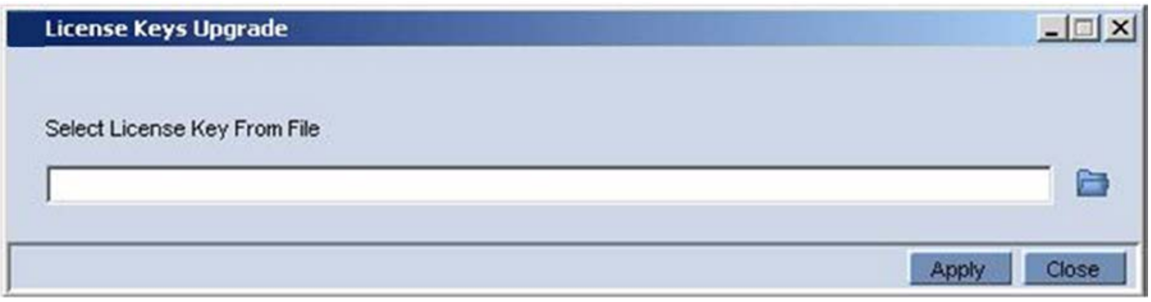
You can update the License Key for multiple TP boards managed in the same Gateway using a single file which includes all the corresponding Keys.

➢ **To update the License Key:**

1. In the Gateway status screen, select the Maintenance Icon drop down menu action **License Key Update**.

   The License Keys Upgrade dialog opens.

Figure 23-2: License Keys Upgrade



2. Select an appropriate file and click the **Apply** button.

   The Mediant 5000 / 8000 updates all the boards with the new License Keys.

23.3.3 Online Software Upgrade Wizard

An Online Software Upgrade is performed when the gateway is up and running. The procedure upgrades the software on all gateway components, including:

- System Controller boards
- Media Gateway boards
- Ethernet Switch boards

The gateway's configuration is preserved throughout the upgrade. Impact on service is minimized.

After upgrading each major system component (e.g., the SC or gateway board) the process pauses and allows you to verify the basic functionality of the upgraded component. At these 'stop points', you can decide whether to proceed with the upgrade or initiate a roll-back. Roll-back enables you to return the gateway to the pre-upgrade software version and configuration in the event of a problem.

The gateway continues its uninterrupted operation during the software upgrade of the SC and ES boards. However, certain calls can be affected when upgrading gateway boards, depending on the upgrade mode used. To minimize impact on gateway service, boards are upgraded one at a time.

The Online Software Upgrade Wizard GUI includes 'Wizard Stages' screen section and a 'Summary Table' screen section. The Summary Table includes a summary of the Request / Response messages exchanged between the EMS server and each of the System Controller boards during the upgrade process. This screen can be used for debugging and to obtain additional information on the process. The Summary Table is saved in the EMS Client Logs files folder as a csv file.

The EMS's Online Software Upgrade Wizard guides users through these steps:

1. **Welcome screen**

   The Welcome Questionnaire includes basic questions regarding the software upgrade process. In this screen, configure the following parameters:

   - VoIP Board Upgrade Mechanism – preferred upgrade mechanism used for upgrading the gateway boards. The following options are available:
     - **Hitless Upgrade** – Gateway boards are upgraded via a switchover between normal and redundant boards of board activity; all established calls are preserved.
     - **Graceful Shutdown** – Gateway boards are upgraded sequentially; the mechanism minimizes the number of calls impacted.
   - **VoIP Board Upgrade Mode** – different levels of user involvement when upgrading boards; the following options are available:
     - **Non-Interactive** - the upgrade process moves to the next gateway board without involvement on the part of the user; the user is informed when all boards complete the upgrade.
     - **Pause after the first gateway board** - allows a pause after the first board is upgraded so that the user can test the system and ensure that the upgrade to the board was successful before upgrading the remaining boards

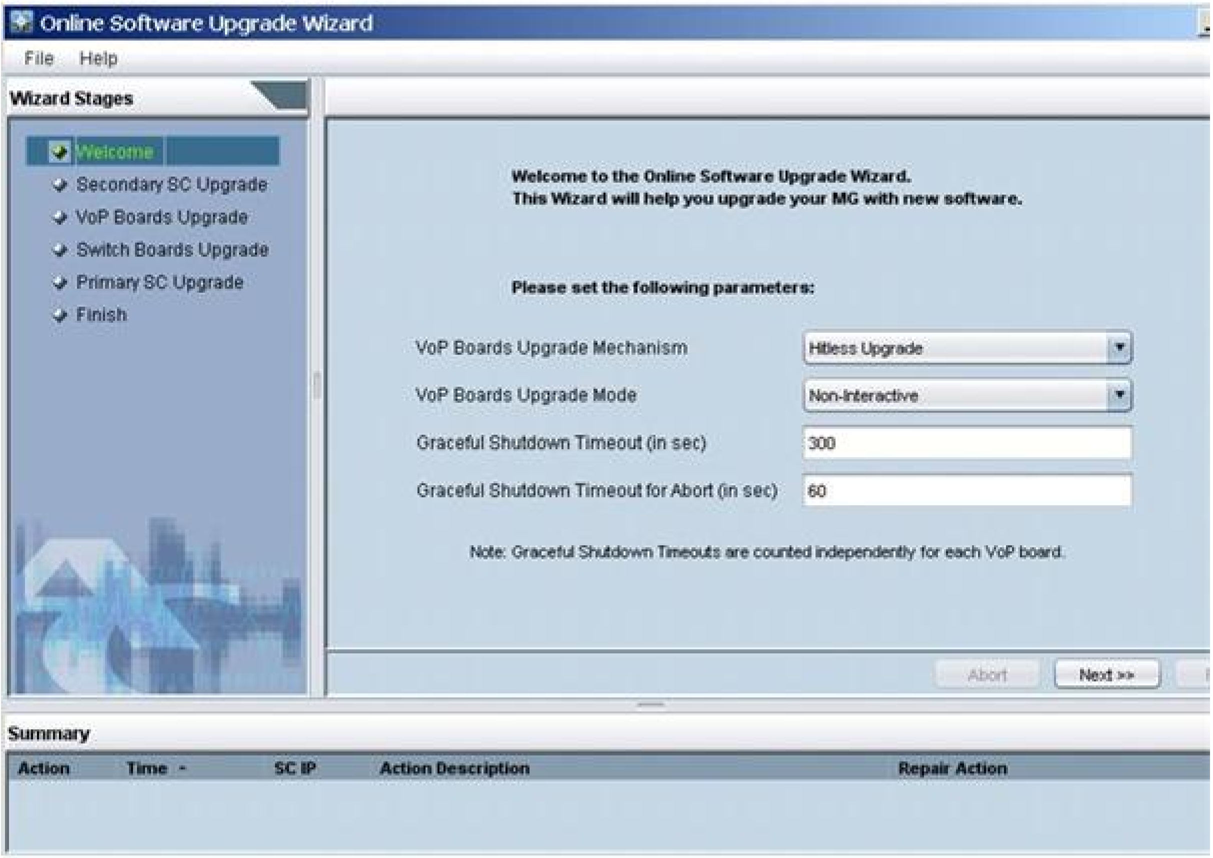
    - **Pause after each gateway board** - allows a pause after each board is upgraded. The user controls the start time of each board upgrade. This option further minimizes the number of calls impacted by the upgrade.

- **Graceful Shutdown Period (sec)** – the period of time allowed for calls to end before each board is upgraded. Inapplicable when a board is upgraded with the Hitless Upgrade option. During the time period, the board accepts no new calls. At the end of the time period, all remaining calls are dropped.
- **Graceful Shutdown Period for Abort (sec)** – the time period used during a rollback sequence after the user clicks the **Abort** button.

Notes:

- Set parameter 'Graceful Shutdown Period' to 0 since it directly impacts the total time of the upgrade process and new calls are not established on the specific board during this time.
- Even though you choose 'Hitless Upgrade' as the upgrade mechanism, some boards may be upgraded with the Graceful Shutdown mechanism). Therefore set a proper value for the Graceful Shutdown Period and estimate the worst-case required upgrade maintenance time.
- The rollback sequence always uses the 'Graceful Shutdown' mechanism, so always set a proper value for the Graceful Shutdown Period for the 'Abort' parameter.

Figure 23-3: Welcome to the Online Software Upgrade Wizard



Welcome to the Online Software Upgrade Wizard.
This Wizard will help you upgrade your MG with new software.

Please set the following parameters:

VoP Boards Upgrade Mechanism: Hitless Upgrade
VoP Boards Upgrade Mode: Non-Interactive
Graceful Shutdown Timeout (in sec): 300
Graceful Shutdown Timeout for Abort (in sec): 60

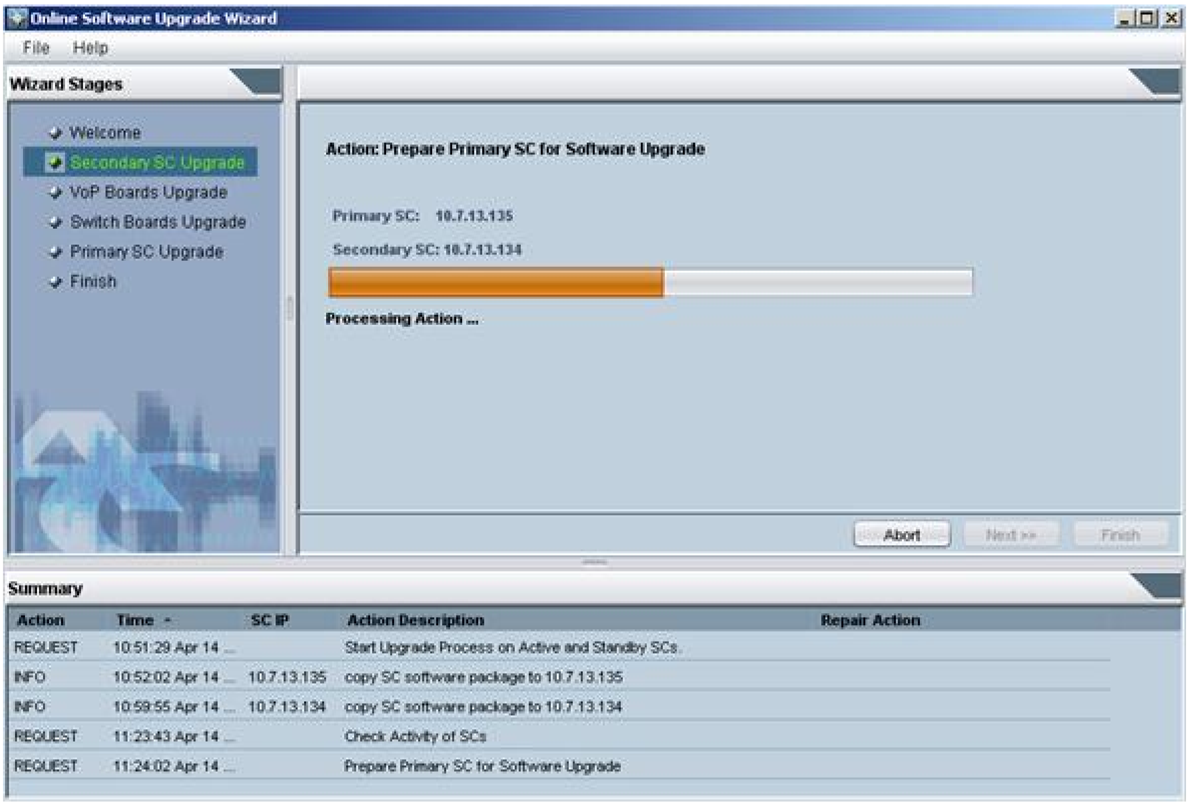
Note: Graceful Shutdown Timeouts are counted independently for each VoP board.

2. Secondary SC Update

In the first stage, the secondary System Controller's software is upgraded. Thereafter, the secondary SC actually manages the upgrade process of the TP boards (refer to the figure below).

After the secondary System Controller's software is updated, the primary System Controller is taken down and an activity switchover to the secondary System Controller is performed.

Figure 23-4: Software Upgrade in Process, Managed by the System Controller



Action: Prepare Primary SC for Software Upgrade

Primary SC: 10.7.13.135

Secondary SC: 10.7.13.134

Processing Action ...

Action	Time	SC IP	Action Description	Repair Action
REQUEST	10:51:29 Apr 14 ...		Start Upgrade Process on Active and Standby SCs.	
INFO	10:52:02 Apr 14 ...	10.7.13.135	copy SC software package to 10.7.13.135	
INFO	10:59:55 Apr 14 ...	10.7.13.134	copy SC software package to 10.7.13.134	
REQUEST	11:23:43 Apr 14 ...		Check Activity of SCs	
REQUEST	11:24:02 Apr 14 ...		Prepare Primary SC for Software Upgrade	

3. VoP Boards Update

Note that at this stage of the software upgrade, active calls are dropped. The secondary SC upgrades all VoP boards in the system, shutting down one at a time after a predefined graceful shutdown period.

4. ES Boards Update

Ethernet Switch boards are upgraded one by one.

5. Primary SC Upgrade

After the secondary SC and all TP boards are updated, the primary SC is upgraded to the new version.

6. Finish

23.3.3.1 Rollback

At any time during an upgrade process, users can perform a rollback to the previous software configuration by clicking the 'Abort' button in the Online Software Upgrade Wizard. A rollback may or may not affect media gateway service. It depends on how far the upgrade has progressed by the time the rollback is performed. A rollback is not service-affecting (i.e., it can be performed without impacting the calls serviced by the media gateway) until the final phase of the 'Secondary SC Upgrade' stage - up to the point that the primary Shelf Controller is shut down and an activity switchover to the secondary Shelf Controller is performed. After this point, rollback will be s ervice-affecting and will cause a reset of all TP boards.

If an upgrade fails, the EMS informs users of the failure and enables a rollback to be performed.

23.3.3.2 Troubleshooting

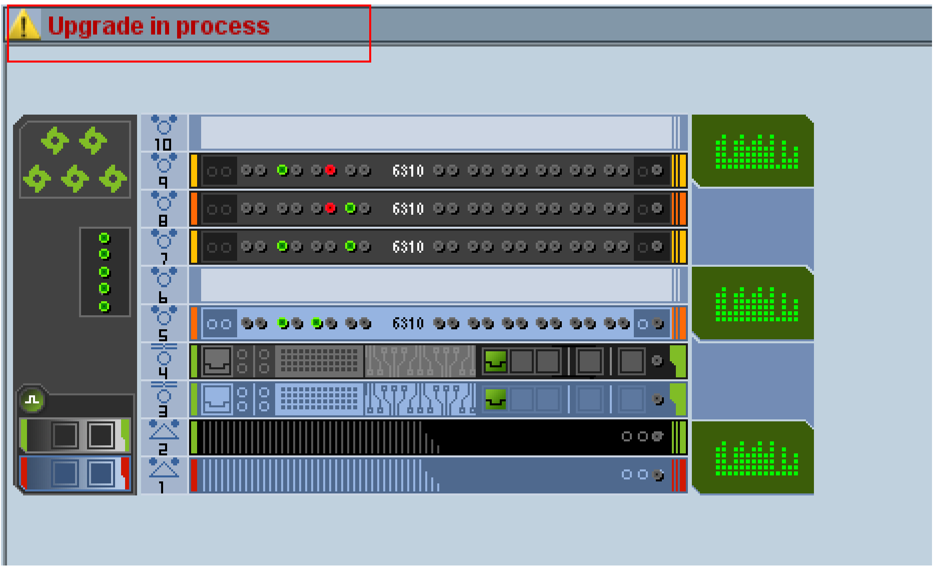
If you experience an unexpected network or software problem during online software upgrade (e.g., if the PC, on which the EMS client runs, crashes or the network connection to the media gateway is lost) you have several options to continue the upgrade session from the same stage. If your network fails, a 'Connect' button appears in the Upgrade Wizard; if the Upgrade Wizard was closed, try reopen it. If the upgrade process is at a point where it can resume, a message is displayed; you can continue by clicking the 'Next' button. In any other case, you'd have the option to rollback from this point.

If there's a disconnection from the network during rollback, you can choose to reconnect or skip. If you skip a failed SC, you'll roll back to a simplex state, and you must manually replace the failed SC.

Notes: After performing an online software upgrade, the Performance Monitoring Data Collector is stopped by the EMS application. To resume data collection, perform the action 'Start Polling MG'.

During the upgrade process, an indicator is displayed in the main status screen (refer to the figure below). If you close the Upgrade Wizard during the upgrade process and the indicator is still displayed, reopen the Wizard and continue, or roll back. The device is vulnerable during an upgrade and it is not recommended to leave it unnecessarily in this state.

Figure 23-5: Upgrade Indicator



23.3.4 Backing Up and Restoring the Media Gateway

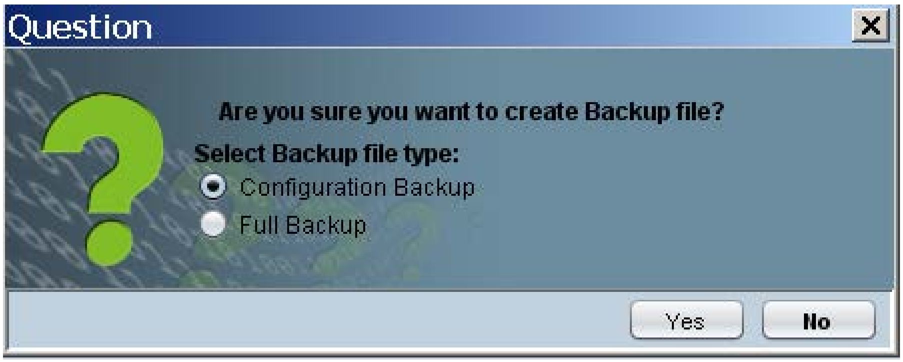
This section describes how to backup and restore the media gateway.

➢ **To back up the gateway :**

1. From the 'Maintenance Actions' popup menu, select **Back Up**.
2. Click **OK**.

   Note that you cannot start up an already started gateway.
3. Select whether you wish to create **Configuration Backup** or **Full Backup**.
   - **Configuration Backup** – contains configuration data and auxiliary files.
   - **Full Backup** – contains software binaries in addition to the configuration data.
4. Click **Yes** to confirm the Configuration Backup.

Figure 23-6: Create Backup File Prompt



Question

Are you sure you want to create Backup file?

Select Backup file type:

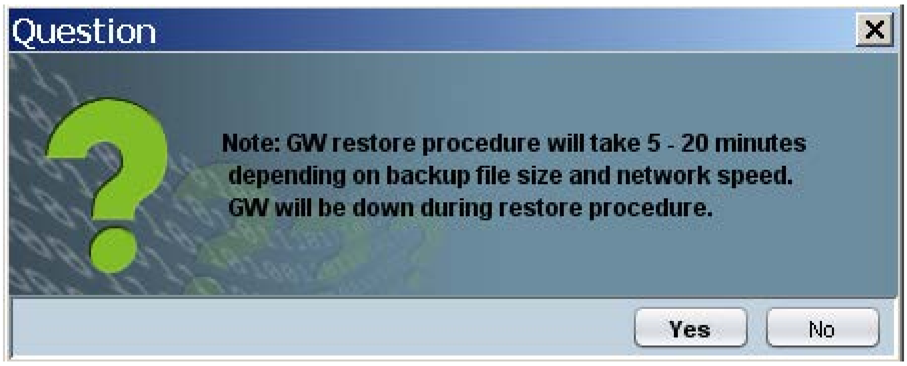
● Configuration Backup

○ Full Backup

➢ To restore the gateway:

1. Lock the media gateway.
2. From the 'Maintenance Actions' pop-up menu, select the **Restore** option. The user is prompted with the Note below.

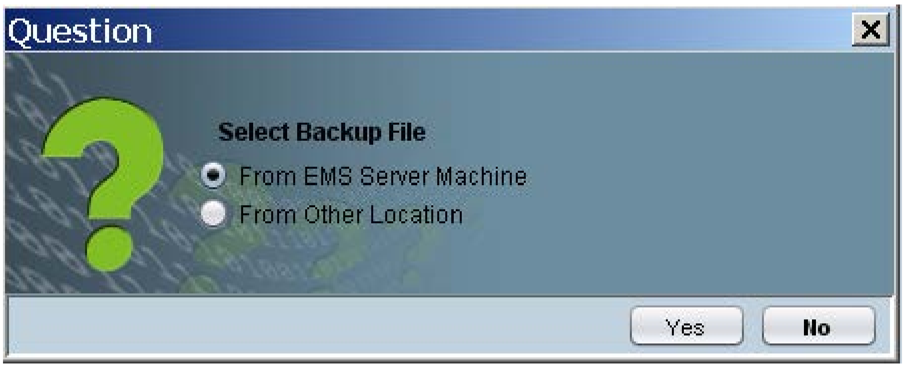
Figure 23-7: Restore Media Gateway Note



Note: GW restore procedure will take 5 - 20 minutes depending on backup file size and network speed. GW will be down during restore procedure.

3. Select the backup file you wish to restore: it can be either selected from the EMS server machine, or from any other location, which can be accessed via the network.

Figure 23-8: Select Backup File Prompt



Select Backup File

● From EMS Server Machine

○ From Other Location

Upon selecting the backup file, EMS will transfer it to both SCs and run the restore procedure.

23.4 Mediant 5000, Mediant 8000 Startup and Shutdown

This section refers to the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway.

➢ To reset the gateway software:

- In the Actions bar, select **Start Up** (if you haven't started up yet) or 'Shut Down' (if you previously started up but now want to shut down).

  Note that you cannot start up an already started gateway.

23.5 Collecting Log Files

This section describes how to collect log files.

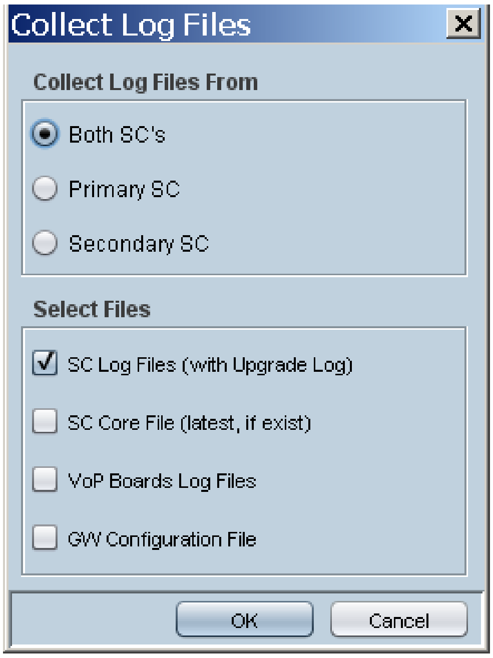
➢ To collect MG logs:

1. In the Actions bar, select **Collect Log Files** menu.
2. Select the SCs and Logs you wish to collect (see figure below), and clicking **OK** button.

The Log c ollection process is started, and the user is displayed with the waiting indicator. Upon log collection finish, the user is prompted with the file chooser to select a location for log file placement. The entire report is packaged as a TAR file, named according to following convention:

```
<GW_Name>_<GW_Global_IP>_report.tar
```

Figure 23-9: Collecting Log Files



Collect Log Files

Collect Log Files From

● Both SC's

○ Primary SC

○ Secondary SC

Select Files

☑ SC Log Files (with Upgrade Log)

☐ SC Core File (latest, if exist)

☐ VoP Boards Log Files

☐ GW Configuration File

23.6 Backup Files

This section describes how to backup gateway configurations.

23.6.1 Mediant 5000 and Mediant 8000 Gateways

EMS can collect backup files (.bk files) that were created and locally stored on the media gateway and store them on t he EMS server machine, thereby enabling a centralized backup files location for all managed gateways.

Upon file collection from the media gateway, an acEMSMGBackupEvent is generated and can be displayed in the Alarm Browser with file details.

File name convention:

<MG_Name>_<MG_OAM_IP_Address>_<m/p>_<backup_file_number>_<backup_date>.bk.

Where <m/p> is a manual or periodic backup.

For example: GW13_10.7.19.100_m_Backup0244-Oct-29-2007.bk

media gateway backup files are located in the EMS Server machine under ACEMS/NBIF/mgBackup folder. File can be accessed and transferred using SSH, and SFTP.

Note: For Mediant 5000 and Mediant 8000 devices, the EMS periodically checks each of the media gateways and when a new backup file is created on the gateway, copies the file to the EMS server database. You can define different backup file creation rules for each gateway.

23.6.2 CPE Devices

The EMS automatically backs up device configurations to *ini* files (device configuration is not saved to the EMS database). The *ini* files are updated according to the backup settings.

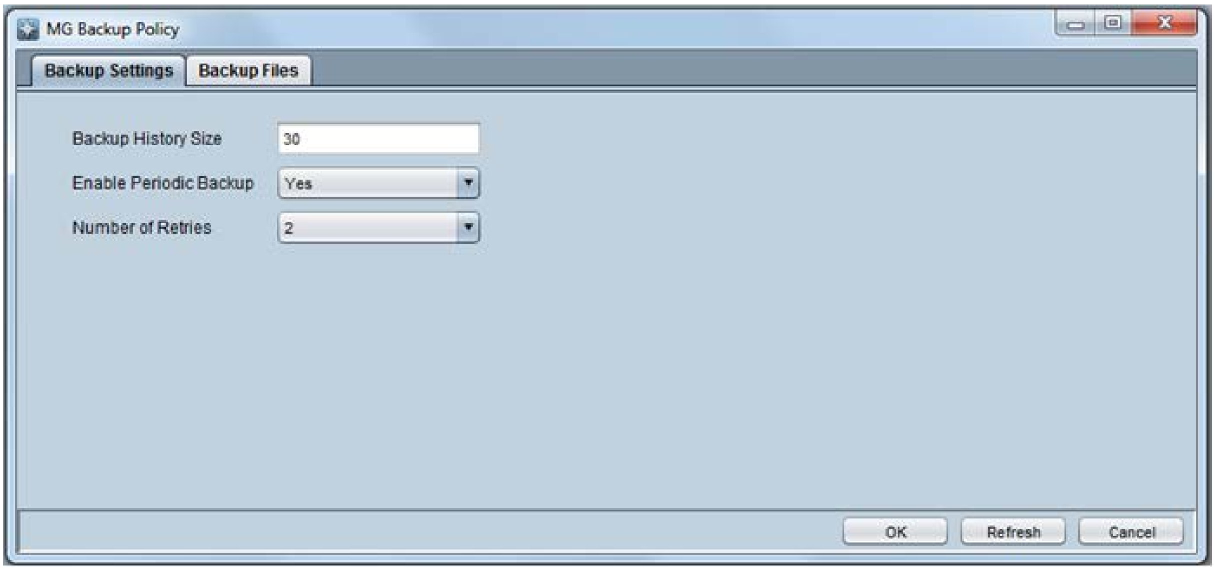
23.6.3 Setting up and Viewing Backup Files

This section describes how to setup and view the collection of the backup files for the Mediant 5000 and Mediant 8000 gateways and for CPE devices.

➢ **To setup the collection of the backup files :**

1. From the EMS menu, choose **Tools** > **MG Backup Settings**; the MG Backup Policy **Backup Settings** tab is displayed:

Figure 23-10: Backup Settings



MG Backup Policy

Backup Settings | Backup Files

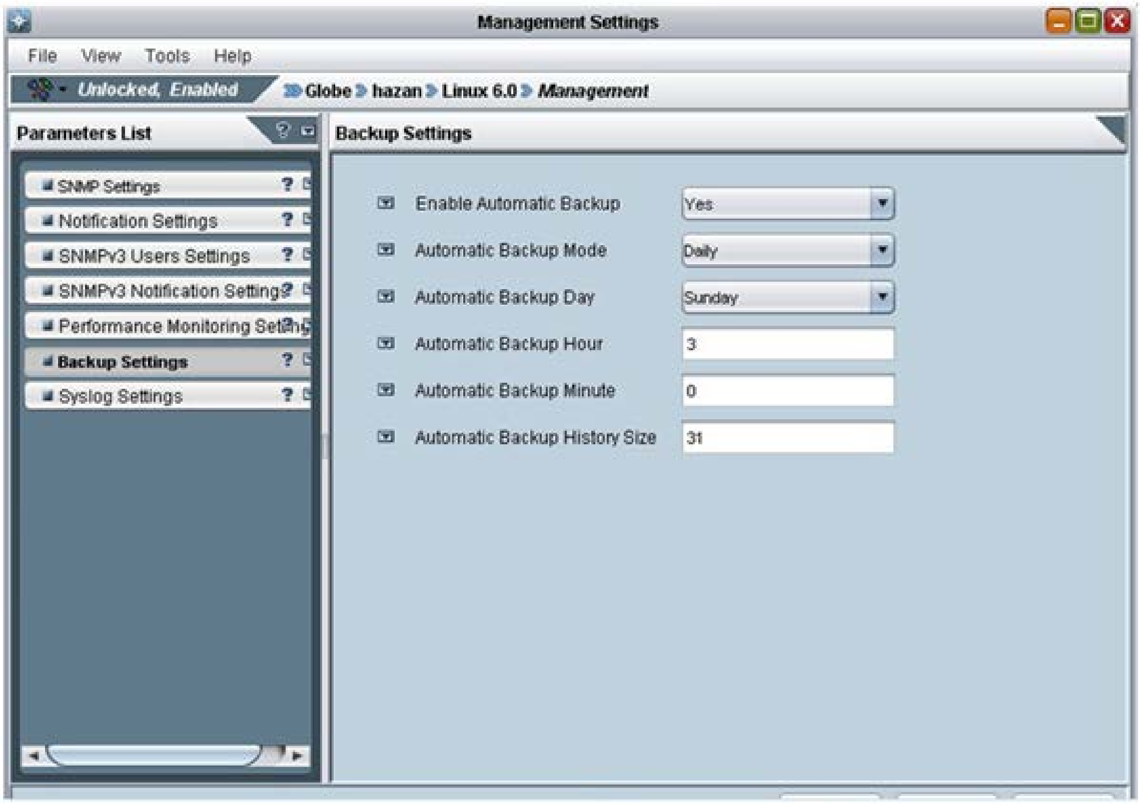
Backup History Size: 30

Enable Periodic Backup: Yes

Number of Retries: 2

2. Set the Backup History Size. This parameter determines the number of latest backup files that will be stored for each one of the managed GWs. Default value 30.
3. Enable or disable Periodic Backup collection.
4. Define the number of retries that must be made on each connection to the media gateway. Default-2.
5. (Mediant 5000 and Mediant 8000 gateways only) To provision backup creation policy for each individual media gateways, open the media gateway Provisioning Frame, Automatic Backup Tab. For more information, refer to the *Mediant 5000 / Mediant 8000 IOM Guide*.

Figure 23-11: Automatic Backup Setup



Enable Automatic Backup: Yes

Automatic Backup Mode: Daily

Automatic Backup Day: Sunday

Automatic Backup Hour: 3

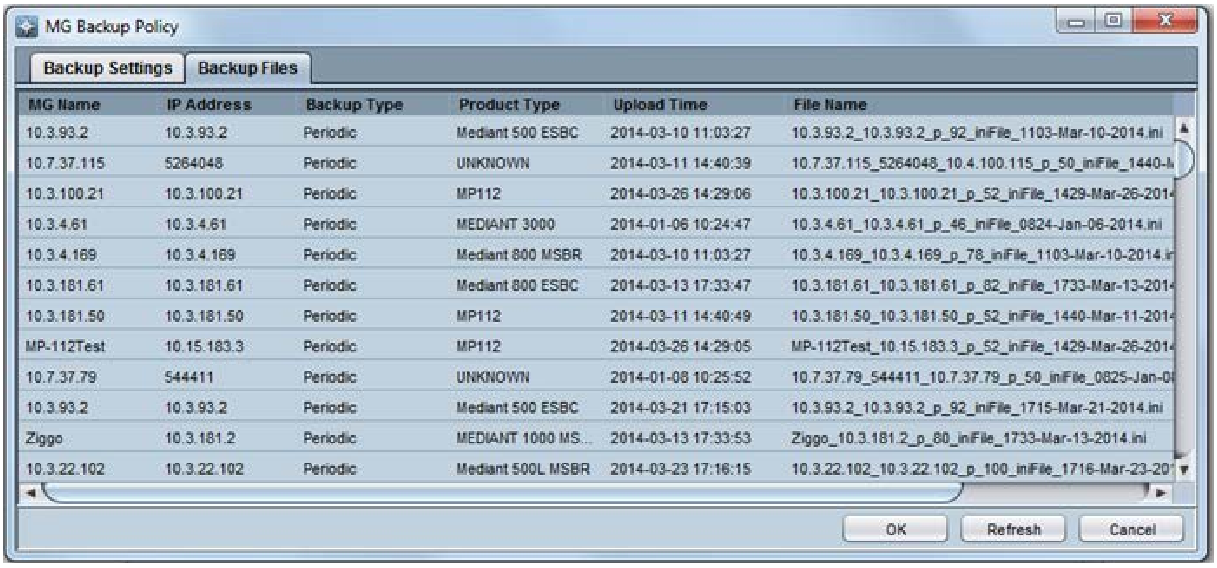
Automatic Backup Minute: 0

Automatic Backup History Size: 31

➢ To view backup files,

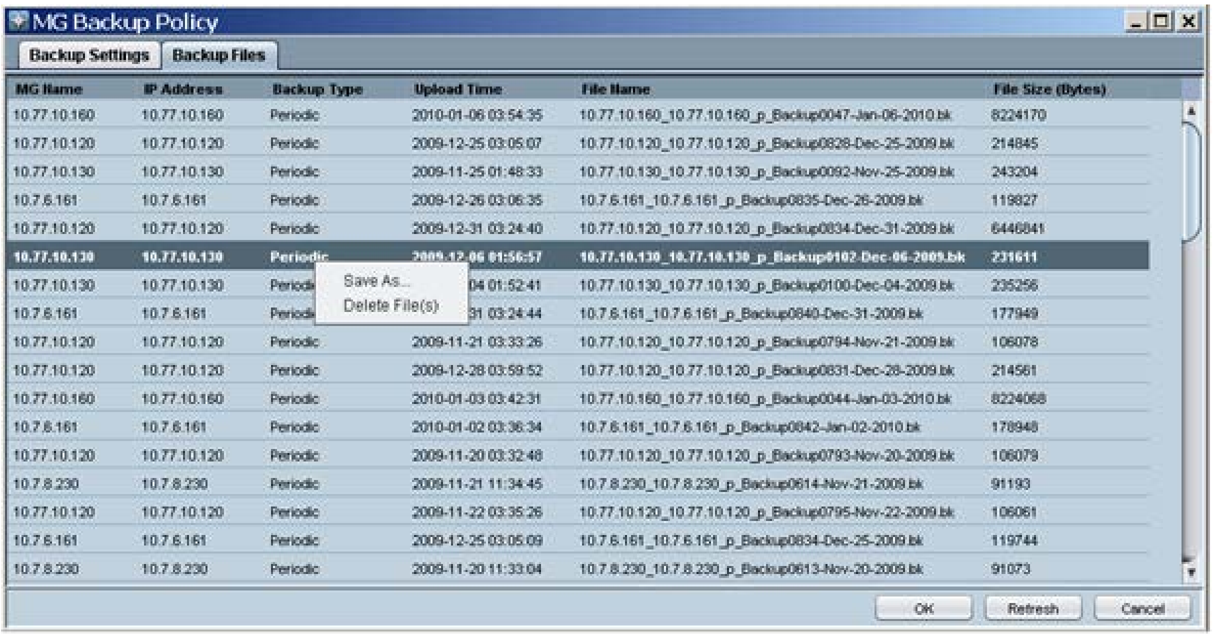
- From the EMS menu, choose **Tools** > **Backup Files**; the MG Backup Policy **Backup Files** tab is displayed with a listing of the device backup files (*INI* files for CPE devices and *.bk* files for the Mediant 5000 and Mediant 8000 devices).

Figure 23-12: Backup Files-CPE INI Files



MG Name	IP Address	Backup Type	Product Type	Upload Time	File Name
10.3.93.2	10.3.93.2	Periodic	Mediant 500 ESBC	2014-03-10 11:03:27	10.3.93.2_10.3.93.2_p_92_iniFile_1103-Mar-10-2014.ini
10.7.37.115	5264048	Periodic	UNKNOWN	2014-03-11 14:40:39	10.7.37.115_5264048_10.4.100.115_p_50_iniFile_1440-M
10.3.100.21	10.3.100.21	Periodic	MP112	2014-03-26 14:29:06	10.3.100.21_10.3.100.21_p_52_iniFile_1429-Mar-26-201
10.3.4.61	10.3.4.61	Periodic	MEDIANT 3000	2014-01-06 10:24:47	10.3.4.61_10.3.4.61_p_46_iniFile_0824-Jan-06-2014.ini
10.3.4.169	10.3.4.169	Periodic	Mediant 800 MSBR	2014-03-10 11:03:27	10.3.4.169_10.3.4.169_p_78_iniFile_1103-Mar-10-2014.i
10.3.181.61	10.3.181.61	Periodic	Mediant 800 ESBC	2014-03-13 17:33:47	10.3.181.61_10.3.181.61_p_82_iniFile_1733-Mar-13-201
10.3.181.50	10.3.181.50	Periodic	MP112	2014-03-11 14:40:49	10.3.181.50_10.3.181.50_p_52_iniFile_1440-Mar-11-201
MP-112Test	10.15.183.3	Periodic	MP112	2014-03-26 14:29:05	MP-112Test_10.15.183.3_p_52_iniFile_1429-Mar-26-201
10.7.37.79	544411	Periodic	UNKNOWN	2014-01-08 10:25:52	10.7.37.79_544411_10.7.37.79_p_50_iniFile_0825-Jan-0
10.3.93.2	10.3.93.2	Periodic	Mediant 500 ESBC	2014-03-21 17:15:03	10.3.93.2_10.3.93.2_p_92_iniFile_1715-Mar-21-2014.ini
Ziggo	10.3.181.2	Periodic	MEDIANT 1000 MS...	2014-03-13 17:33:53	Ziggo_10.3.181.2_p_80_iniFile_1733-Mar-13-2014.ini
10.3.22.102	10.3.22.102	Periodic	Mediant 500L MSBR	2014-03-23 17:16:15	10.3.22.102_10.3.22.102_p_100_iniFile_1716-Mar-23-20

Figure 23-13: Backup Files-Mediant 5000/Mediant 8000



MG Name	IP Address	Backup Type	Upload Time	File Name	File Size (Bytes)
10.77.10.160	10.77.10.160	Periodic	2010-01-06 03:54:35	10.77.10.160_10.77.10.160_p_Backup0047-Jan-06-2010.bk	8224170
10.77.10.120	10.77.10.120	Periodic	2009-12-25 03:05:07	10.77.10.120_10.77.10.120_p_Backup0828-Dec-25-2009.bk	214845
10.77.10.130	10.77.10.130	Periodic	2009-11-25 01:48:33	10.77.10.130_10.77.10.130_p_Backup0092-Nov-25-2009.bk	243204
10.7.6.161	10.7.6.161	Periodic	2009-12-26 03:06:35	10.7.6.161_10.7.6.161_p_Backup0835-Dec-26-2009.bk	119827
10.77.10.120	10.77.10.120	Periodic	2009-12-31 03:24:40	10.77.10.120_10.77.10.120_p_Backup0834-Dec-31-2009.bk	6446841
10.77.10.130	10.77.10.130	Periodic	2009-12-06 01:56:57	10.77.10.130_10.77.10.130_p_Backup0102-Dec-06-2009.bk	231611
10.77.10.130	10.77.10.130	Periodi	04 01:52:41	10.77.10.130_10.77.10.130_p_Backup0100-Dec-04-2009.bk	235256
10.7.6.161	10.7.6.161	Periodi	31 03:24:44	10.7.6.161_10.7.6.161_p_Backup0840-Dec-31-2009.bk	177949
10.77.10.120	10.77.10.120	Periodic	2009-11-21 03:33:26	10.77.10.120_10.77.10.120_p_Backup0794-Nov-21-2009.bk	106078
10.77.10.120	10.77.10.120	Periodic	2009-12-28 03:59:52	10.77.10.120_10.77.10.120_p_Backup0831-Dec-28-2009.bk	214561
10.77.10.160	10.77.10.160	Periodic	2010-01-03 03:42:31	10.77.10.160_10.77.10.160_p_Backup0044-Jan-03-2010.bk	8224068
10.7.6.161	10.7.6.161	Periodic	2010-01-02 03:36:34	10.7.6.161_10.7.6.161_p_Backup0842-Jan-02-2010.bk	178948
10.77.10.120	10.77.10.120	Periodic	2009-11-20 03:32:48	10.77.10.120_10.77.10.120_p_Backup0793-Nov-20-2009.bk	106079
10.7.8.230	10.7.8.230	Periodic	2009-11-21 11:34:45	10.7.8.230_10.7.8.230_p_Backup0614-Nov-21-2009.bk	91193
10.77.10.120	10.77.10.120	Periodic	2009-11-22 03:35:26	10.77.10.120_10.77.10.120_p_Backup0795-Nov-22-2009.bk	106061
10.7.6.161	10.7.6.161	Periodic	2009-12-25 03:05:09	10.7.6.161_10.7.6.161_p_Backup0834-Dec-25-2009.bk	119744
10.7.8.230	10.7.8.230	Periodic	2009-11-20 11:33:04	10.7.8.230_10.7.8.230_p_Backup0613-Nov-20-2009.bk	91073

Part IV

Fault and Performance Management

This section describes fault and performance management.

24 Introduction

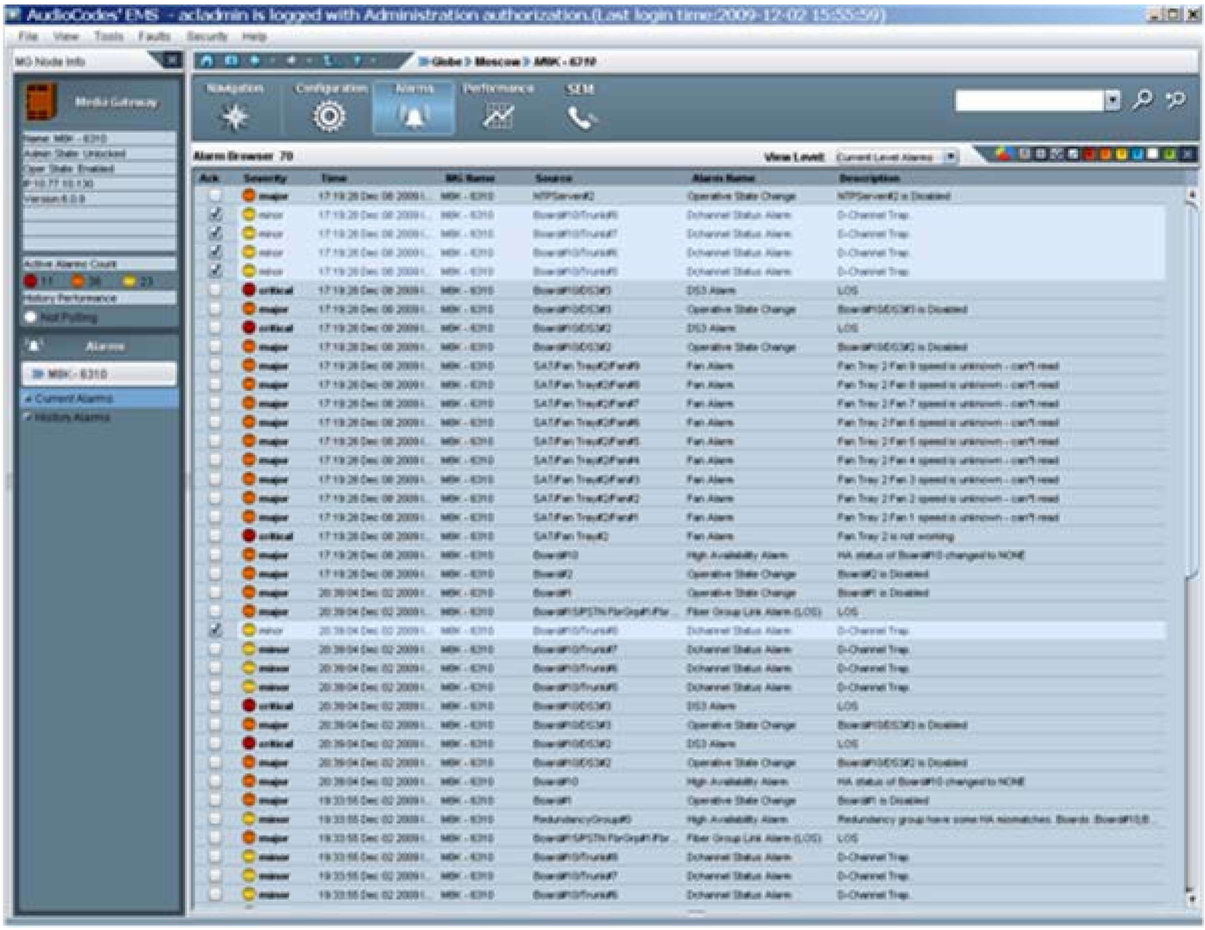
After service is provisioned for a s ubscriber under a given QoS level, the service provider must ensure that the purchased level of service is delivered. In the domain of the EMS, this process involves high-level fault and performance management of the managed entities. This section describes the fault management functionality of the EMS.

High-level fault management involves monitoring managed entities to detect malfunction, preempt failures, and detect faults. After faults are discovered, the operator must troubleshoot, repair, and restore the entity as quickly as possible. Fault management ensures that service remains available.

Technicians can use various EMS tools to perform a pinpoint diagnosis. EMS provides one or more fault screens that contain detailed information on eac h alarm or event generated by the entities in its domain. An alarm is a specific problem indicator with predefined actions that trigger the alarm. Events are typically service provider-set thresholds that, if exceeded, send a message that appears in the alarm screen along with faults. A common use of the event mechanism is to detect degrading transmission facilities to alert operations personnel to a problem before it affects customers.

You can view a combined table with all the alarms, events and journal records to correlate user activities with system behavior and responses. The combined view is opened from the Alarms Browser, Alarm History and Journal Frames. A unified Advanced Filter allows you to view the filter according to Time interval, GW Gateway IP address, User name or Action Type, Alarm Name, Source or Free text in Description Fields.

Figure 24-1: Alarm Browser in Main Screen



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-02 15:55:59)

Globe > Moscow > MSK - 6310

MG Node Info

Media Gateway

Name: MSK - 6310
Admin State: Unlocked
Oper State: Enabled
IP:10.77.10.130
Version:6.0.9

Active Alarms Count
● 11 ● 36 ● 23

History Performance
Not Polling

Alarm Browser 70

View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	NTPServer#2	Operative State Change	NTPServer#2 is Disabled
☑	minor	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/Trunk#8	D-channel Status Alarm	D-Channel Trap
☑	minor	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/Trunk#7	D-channel Status Alarm	D-Channel Trap
☑	minor	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/Trunk#6	D-channel Status Alarm	D-Channel Trap
☑	minor	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/Trunk#5	D-channel Status Alarm	D-Channel Trap
☐	critical	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/DS3#3	DS3 Alarm	LOS
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/DS3#3	Operative State Change	Board#1/DS3#3 is Disabled
☐	critical	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/DS3#2	DS3 Alarm	LOS
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#1/DS3#2	Operative State Change	Board#1/DS3#2 is Disabled
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#9	Fan Alarm	Fan Tray 2 Fan 9 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#8	Fan Alarm	Fan Tray 2 Fan 8 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#7	Fan Alarm	Fan Tray 2 Fan 7 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#6	Fan Alarm	Fan Tray 2 Fan 6 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#5	Fan Alarm	Fan Tray 2 Fan 5 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#4	Fan Alarm	Fan Tray 2 Fan 4 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#3	Fan Alarm	Fan Tray 2 Fan 3 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#2	Fan Alarm	Fan Tray 2 Fan 2 speed is unknown - can't read
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2/Fan#1	Fan Alarm	Fan Tray 2 Fan 1 speed is unknown - can't read
☐	critical	17:19:28 Dec 08 2009 I...	MSK - 6310	SAT/Fan Tray#2	Fan Alarm	Fan Tray 2 is not working
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#10	High Availability Alarm	HA status of Board#10 changed to NONE
☐	major	17:19:28 Dec 08 2009 I...	MSK - 6310	Board#2	Operative State Change	Board#2 is Disabled
☐	major	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1	Operative State Change	Board#1 is Disabled
☐	major	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/SPSTN FbrGrp#1/Fbr...	Fiber Group Link Alarm (LOS)	LOS
☑	minor	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#8	D-channel Status Alarm	D-Channel Trap
☐	minor	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#7	D-channel Status Alarm	D-Channel Trap
☐	minor	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#6	D-channel Status Alarm	D-Channel Trap
☐	minor	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#5	D-channel Status Alarm	D-Channel Trap
☐	critical	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/DS3#3	DS3 Alarm	LOS
☐	major	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/DS3#3	Operative State Change	Board#1/DS3#3 is Disabled
☐	critical	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/DS3#2	DS3 Alarm	LOS
☐	major	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#1/DS3#2	Operative State Change	Board#1/DS3#2 is Disabled
☐	major	20:39:04 Dec 02 2009 I...	MSK - 6310	Board#10	High Availability Alarm	HA status of Board#10 changed to NONE
☐	major	19:33:55 Dec 02 2009 I...	MSK - 6310	Board#1	Operative State Change	Board#1 is Disabled
☐	minor	19:33:55 Dec 02 2009 I...	MSK - 6310	RedundancyGroup#0	High Availability Alarm	Redundancy group have some HA mismatches. Boards: Board#1(B...
☐	major	19:33:55 Dec 02 2009 I...	MSK - 6310	Board#1/SPSTN FbrGrp#1/Fbr...	Fiber Group Link Alarm (LOS)	LOS
☐	minor	19:33:55 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#8	D-channel Status Alarm	D-Channel Trap
☐	minor	19:33:55 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#7	D-channel Status Alarm	D-Channel Trap
☐	minor	19:33:55 Dec 02 2009 I...	MSK - 6310	Board#1/Trunk#6	D-channel Status Alarm	D-Channel Trap

25 Alarm Browser

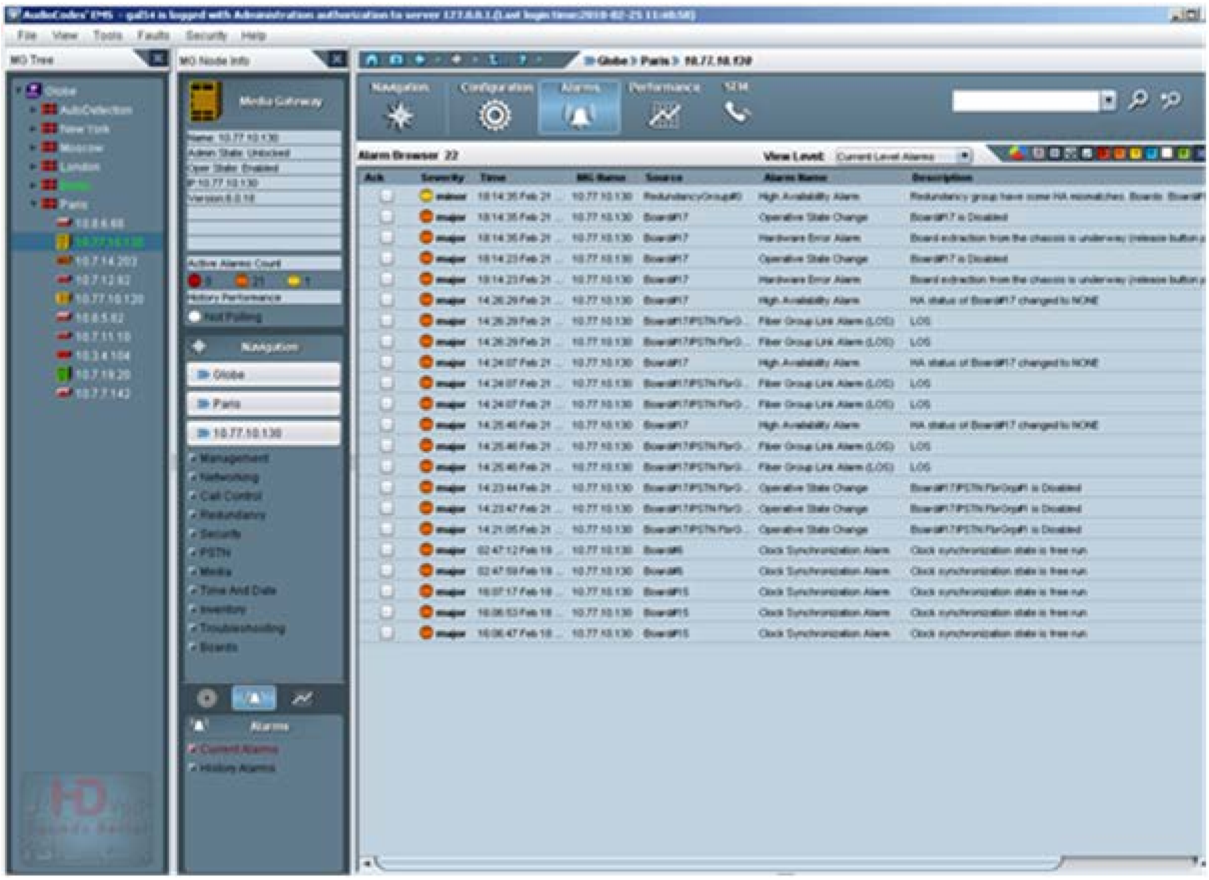
The EMS's fault management functionality manages and displays all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system.

The EMS can typically process 30 alarms/events per second continuously. When an alarm is received, it is parsed, stored in the database and immediately displayed in the GUI's Alarm Browser. The Alarm Browser displays *current active* system faults at the top of the alarms list, allowing Operators to identify equipment and facilities most recently affected.

The EMS utilizes the ability to synchronize with media gateways on missed alarms which could occur due to Network Connectivity or other problems. EMS will retrieve these missed alarms and add them to the Alarm Browser / History windows. Upon alarms retrieval, depending on the trap forwarding rules, alarms will also be forwarded.

The Alarm Browser is context-based so that (for example) only alarms of the media gateway selected in the MGs List will be displayed in the Alarm Browser or (as another example) only alarms of the TP board selected in the graphic representation of the media gateway will be displayed in the Alarm Browser. The Alarms module displays the Current and History Alarms view. Additionally users can filter the Alarms view in the Navigation and Configuration modes to current, node or regional alarms,. The figure below displays the Alarms module for the Moscow region-context alarms displayed in the Alarm Browser.

Figure 25-1: Alarms Browser Mediant 8000



Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	minor	18:14:35 Feb 21 ...	10.77.10.130	RedundancyGroup#0	High Availability Alarm	Redundancy group have some HA mismatches. Boards: Board#
□	major	18:14:35 Feb 21 ...	10.77.10.130	Board#17	Operative State Change	Board#17 is Disabled
□	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
□	major	18:14:23 Feb 21 ...	10.77.10.130	Board#17	Operative State Change	Board#17 is Disabled
□	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
□	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
□	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:26:29 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
□	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:24:07 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17	High Availability Alarm	HA status of Board#17 changed to NONE
□	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:25:46 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Fiber Group Link Alarm (LOS)	LOS
□	major	14:23:44 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
□	major	14:23:47 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
□	major	14:21:05 Feb 21 ...	10.77.10.130	Board#17/PSTN FbrG...	Operative State Change	Board#17/PSTN FbrGrp#1 is Disabled
□	major	02:47:12 Feb 18 ...	10.77.10.130	Board#8	Clock Synchronization Alarm	Clock synchronization state is free run
□	major	02:47:59 Feb 18 ...	10.77.10.130	Board#8	Clock Synchronization Alarm	Clock synchronization state is free run
□	major	16:07:17 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run
□	major	16:08:53 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run
□	major	16:06:47 Feb 18 ...	10.77.10.130	Board#15	Clock Synchronization Alarm	Clock synchronization state is free run

The number of alarms currently displayed in the Alarms Browser is indicated adjacent to the pane title bar. For each alarm, the following alarm details are displayed in the Alarm Browser pane:

- **Ack** - a check box in the left column of the Alarm Browser indicates if an alarm has been Acknowledged (checked) or Unacknowledged (unchecked). After an alarm is acknowledged, the entire row displaying the alarm and its details becomes gray (disabled).
- **Severity** - indicates the alarm's severity level. green=Clear; white=Indeterminate; blue=Warning; yellow=Minor; orange=Major; red=Critical.
- **Time** (Day of the Week, Month, Date in the Month, Hours:Minutes:Seconds, Time Zone, Year). Note that the Time value presented in the Alarm Browser is based on the time in EMS Server Time Zone, adjusted to the local time of the EMS client (according to the workstation machine's clock definition). To update the Time Zone, refer to the *EMS Server IOM Manual.*
- **MG Name**
- **Source** - the source of the alarm; the failed entity that generated the alarm (in format Board#1/Trunk#2, etc.)
- **Alarm/Event Nam**e (short description of the alarm)
- **Events** are indicated by the label [Event] which makes it easy for the user to sort between alarms and events.
- **Description** (elaborated alarm details)

Notes: By default, alarms are listed in the Alarm Browser in chronological order. The most recently received alarms appear at the **top** of the list, with the oldest alarms at the **bottom**.

25.1 Filtering Alarms

The Alarm Browser lists all the currently active alarms in the EMS for a c ontext selected in the Navigation module. When selecting the root (Globe) of the managed media gateways in the MG Tree, the Alarm Browser displays all alarms for all EMS -managed elements (as shown in the figure below).

When selecting a region in the MG Tree, for example, the Alarm Browser displays all alarms for all media gateways under that region.

Available contexts are as follows:

- **Globe** - all alarms in the entire system.
- **Region** - alarms of all nodes located under the region.
- **Media gateway** - all the alarms of the media gateway
- **TP Board and its subcomponents** (Trunk, SS7, MTP2), SAT, Ethernet Switch and System Controller boards - all the alarms of the selected entity.

Additionally, operators can filter alarms according to Ack status and/or severity (using the Alarm Browser's toolbar buttons).

Table 25-1: Alarm Browser Buttons

Alarm Severity Filtration Toolbar	Purpose (When Clicking on a Button on the Toolbar)
✎	Opens the Actions Journal. For more information, see Section Viewing Operator Actions in the Actions Journal on page 266.
🔇	Enables Audio Indication on receipt of alarm. For more information, see Audio Indication on Receipt of Alarms.
⏸	Pauses Alarms / Events auto refresh.
e	Filters the active Alarm Browser window by only displaying alarms (events are not displayed)
✓	Filters the active Alarm Browser window by displaying only Unacknowledged Alarms (acknowledged alarms are not displayed)
🟥	Filters the active Alarm Browser window by displaying Critical Alarms.
🟧	Filters the active Alarm Browser window by displaying Major Alarms.
🟨	Filters the active Alarm Browser window by displaying Minor Alarms.
🟦	Filters the active Alarm Browser window by displaying Warning Alarms
⬜	Filters the active Alarm Browser window by displaying Info Alarms.
🟩	Filters the active Alarm Browser window by displaying Clear Alarms.

Alarm Severity Filtration Toolbar	Purpose (When Clicking on a Button on the Toolbar)
☒	Close Alarm Browser

Notes: By default, all Alarm Severity Filtration buttons are selected, meaning that both acknowledged and unacknowledged alarms of all severities are displayed by default. After clicking a button, the arrow (↓) ceases to be displayed on that button, meaning that alarms have been filtered for that severity level.

25.2 Acknowledging an Alarm

Operators should acknowledge an alarm to inform other operators that the acknowledged alarm has been handled and troubleshooted by someone, and to communicate to other operators that it is no longer an active system alarm.

➢ **To acknowledge an alarm, do one of the following:**

- Right-click the alarm row in the Alarm Browser and select the option **Acknowledge** in the pop-up (multiple rows can be selected to be acknowledged in this way).

  -OR-

- Check the check box under the column Ack adjacent to the alarm you need to acknowledge.

25.3 Alarms and Event Clearing

The Alarm Browser for each media gateway is cleared from all the current alarms and events upon system GW startup (cold start event).

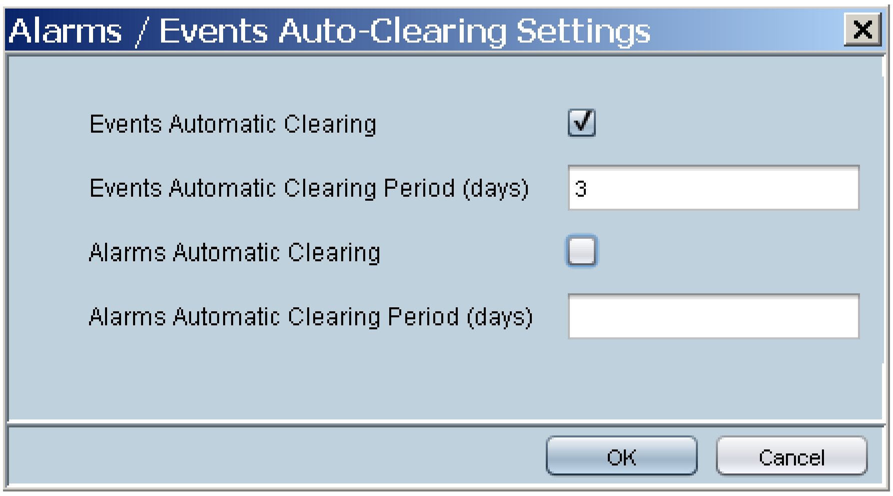
Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) when a Clear alarm is generated by the same entity (source) and same media gateway that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature prevents irrelevant alarms from congesting the Alarms Browser. Operators view the list of only the currently active alarms.

Events are informative messages (usually not severe) which are not automatically cleared by the EMS application. The EMS performs automatic events clearing three days after the event has been received.

In addition, the user can enable or disable events and/or alarms automatic clearing, as well as define the period after which each one of these notifications must be removed from the Active Alarms browser.

To change Alarms / Events clearing rules and times, select the Faults -> Automatic Clearing menu. The Alarms / Events Auto-Clearing Settings screen is displayed.

Figure 25-2: Alarm and Event Auto-Clearing Settings



Alarms / Events Auto-Clearing Settings

Events Automatic Clearing ☑

Events Automatic Clearing Period (days) 3

Alarms Automatic Clearing ☐

Alarms Automatic Clearing Period (days)

The default application settings ensures that events are cleared by the EMS application after three days, while alarms are not cleared (only by the Gateway itself). If the user wishes the EMS to perform automatic alarms clearing, they should select the checkbox in the above screen and define the clearing period (default is 30 days).

When the EMS application performs Events/Alarms Automatic Clearing, it moves the cleared Events/Alarms to the Alarm History view with the text indication 'Automatic Cleared'.

25.4 Changing the Alarms Browser Views

This section describes how to change the Alarms Browser Views.

25.4.1 Alarms View Level

Each user can select what alarms filtering level s/he wishes to apply in his/her Alarm Browser. The following options are supported:

- **Current Level Alarms (default)** - users view alarms filtered according to the context they're viewing in the status pane
- **Node Level Alarms** – users always view all alarms received from the node they're viewing, regardless of the lower level context (board, trunk) they've accessed.
- **Region Level Alarms** – users will view all alarms at region level, regardless of the node or lower level context they've accessed.
- **All Alarms** - users view all alarms at the globe level, regardless of the context.

25.4.2 Alarm Browser Columns View

You can select viewed columns in the Alarm Browser and Alarms History window. For example, you can add a new column to view the 'Source Description' field (implemented for Mediant 5000 / 8000 GWs). The 'Source Description' field includes the object name as it defined by the user in the 'Name' field in each one of the Provisioning Screens. Users can also decide to reduce the number of viewed columns. You can view all the available and currently viewed columns by right-clicking on the Alarms Browser and Alarms History table's title bars.

Figure 25-3: Alarm Browser Column View

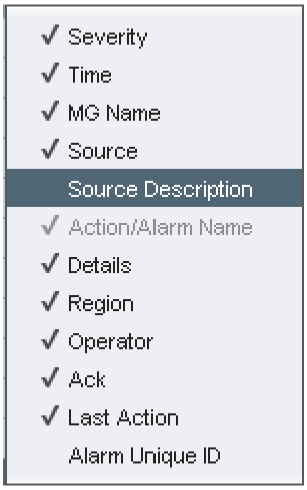
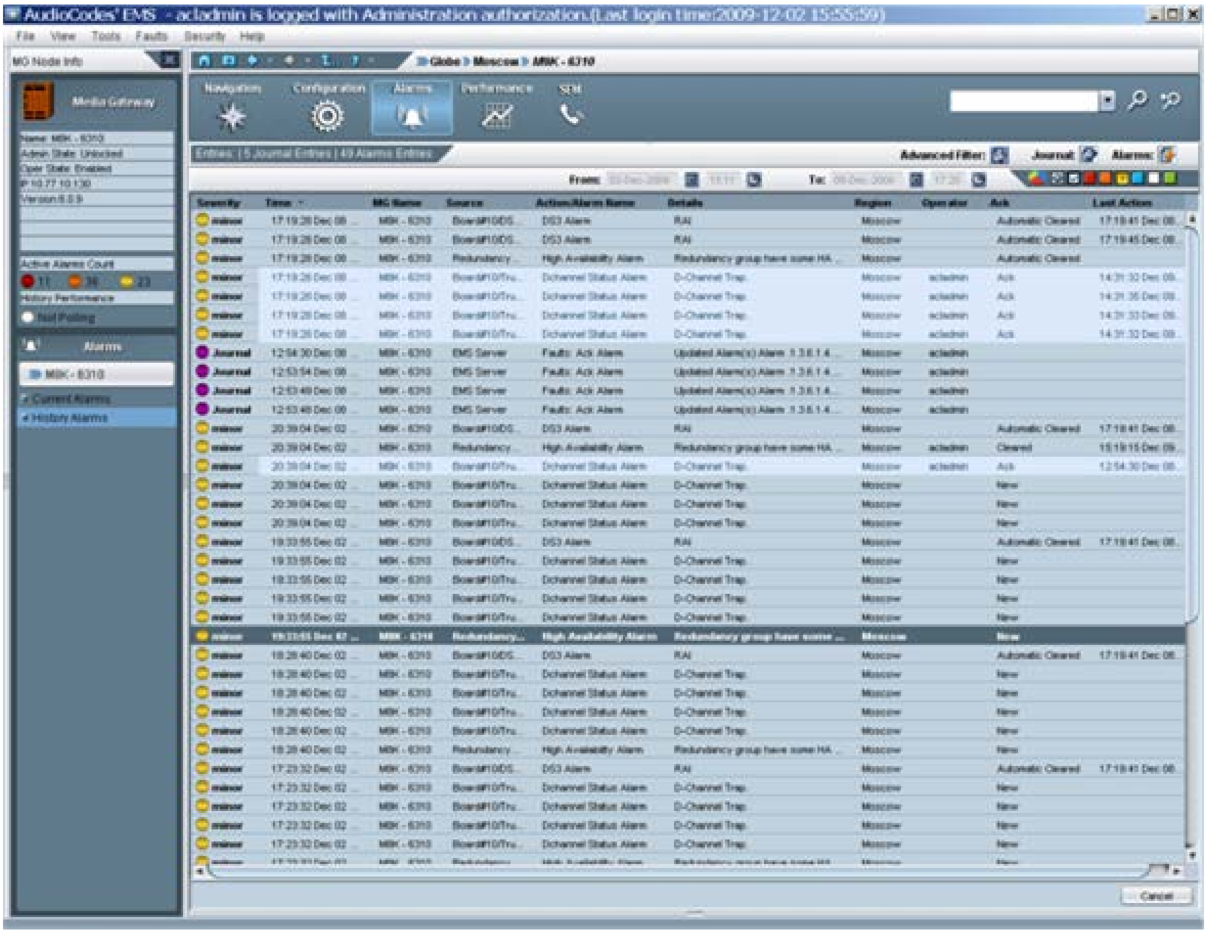


Figure 25-4: Alarm History



Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator	Ack	Last Action
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:45 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		Automatic Cleared	
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow	acladmin	Ack	14:31:32 Dec 09...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow	acladmin	Ack	14:31:35 Dec 09...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow	acladmin	Ack	14:31:33 Dec 09...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow	acladmin	Ack	14:31:32 Dec 09...
Journal	12:54:30 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:54 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:49 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:48 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	20:39:04 Dec 02 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow	acladmin	Cleared	15:19:15 Dec 09...
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow	acladmin	Ack	12:54:30 Dec 08...
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Redundancy...	High Availability Alarm	Redundancy group have some ...	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/Tru...	Dchannel Status Alarm	D-Channel Trap.	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	

25.5 Open Alarms History

To review the Alarm History records for the selected context, in the Alarms pane, click **History Alarms**. For the specifications and features pertaining to the Alarm History, see Section 'Alarms History' on page 276.

25.6 Open Journal

To review Journal records for the selected context, click **Journal** on the Alarm Browser tool bar. For the specifications and f eatures pertaining to the Journal, see Section 'Viewing Operator Actions in the Actions Journal' on page 373.

25.7 Audio Indication on Receipt of Alarms

Each time a new alarm answering context selection criteria is received and displayed in the Alarm Browser, a bell sound is played by EMS application.

➢ To enable the bell sound:

- Click the button **Alarm Sound Disabled** on the Alarm Browser toolbar.

25.8 Pause Alarms Auto Refreshing

This section describes how to pause alarm auto refreshing.

➢ To stop alarms auto refreshing:

- Click the **Pause** button on the Alarm Browser toolbar; Alarms received by the EMS while Alarm Browser refreshing is paused are saved in the database and displayed to operators after re-clicking (de-selecting) the **Pause** button.

  While the **Pause** button is clicked, the alarm browser presentation is paused as well.

25.9 Alarms and Events Filtering & Sorting

Alarms and Events can be displayed as separate graphic entities in the Alarm Browser and History screens. You can easily sort between alarms and events or filter events from the Alarm Browser and Alarm History windows.

➢ To filter events in the Alarm and Alarm History Browser windows:

- In the Alarms Browser toolbar, click the **Filter Events** icon. All events are removed from the Alarm Browser display.

➢ To sort between Alarms and Events in the Alarm and Alarm History Browser windows:

- In the Alarms Browser toolbar, click the 'Alarm Name' field. All events are sorted to the top of the Alarm Browser view. Each event is displayed in the following format:

  [Event]

25.10 Closing the Alarm Browser Pane

This section describes how to close the Alarm Browser pane.

➢ To close the Alarm Browser pane:

- Click the **x** button.

➢ To reopen the Alarm Browser pane

- Open the View menu in the menu bar of the main screen, and choose option **View Alarm Browser**.

26 Alarms History

All alarms received by the EMS are archived in a database. Extensive information related to the alarm is saved, together with the alarm itself: Region and media gateway location, physical attributes of failed entity.

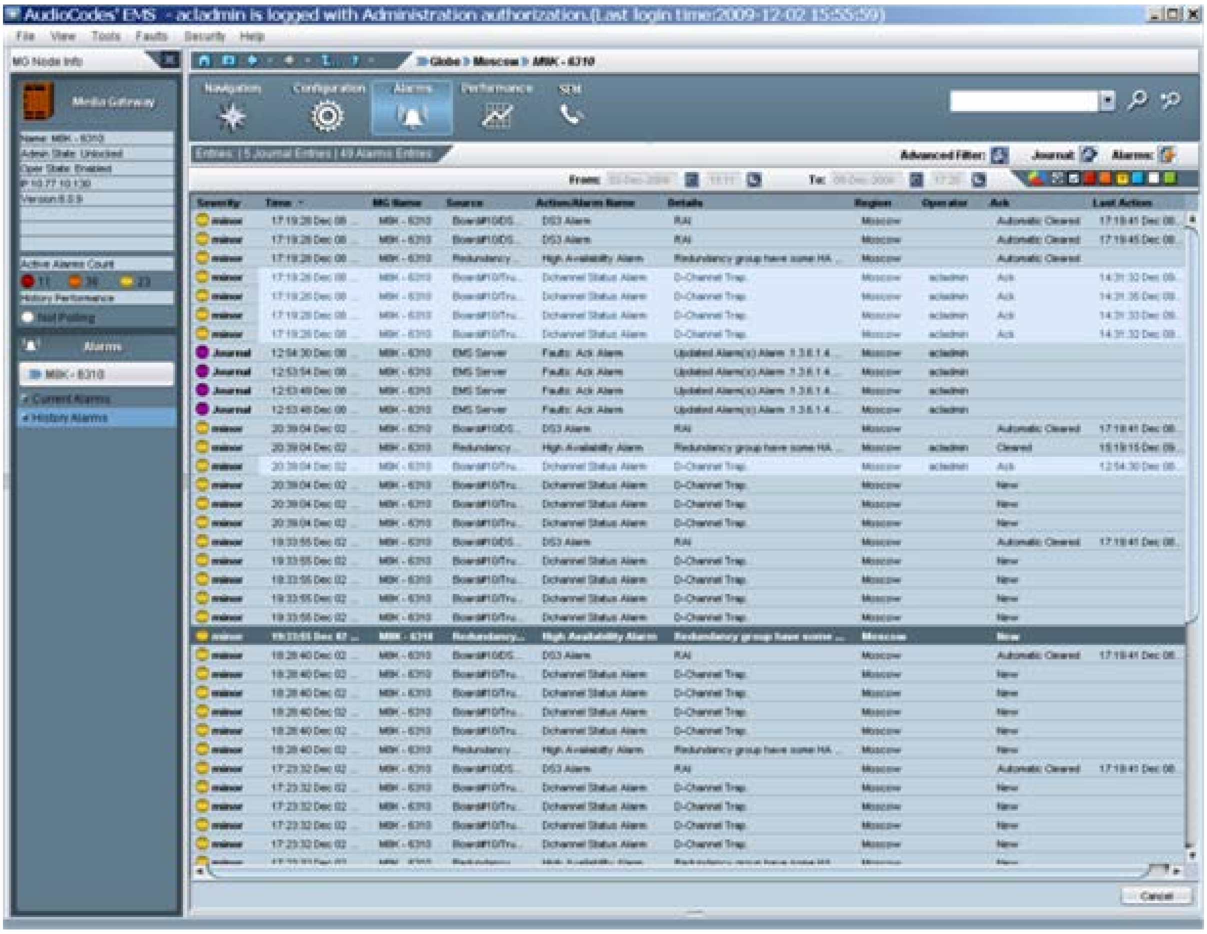
Open the Alarms History screen from the Alarms module by clicking the 'History Alarms' option. The Alarms History screen is context-sensitive like the Alarm Browser; the context is displayed in the title of the screen.

The EMS's Alarms History screen (refer to the figure below) provides operators with a view of the alarms' history over an extended period of time. EMS operators can time-filter alarms according to a time definition so that they are operator-organized and viewed according to operator requirements.

The EMS database stores history alarms for six months, depending on the available disk space. When 80% of the EMS server disk space is full, the EMS removes 20% of the oldest alarms. Alternatively, if the number of alarms exceeds 10 million, the EMS removes 1 million of the oldest alarms.

The Alarms History screen informs operators of the actions performed on each alarm, including the alarm's current state, the last action performed on t he alarm and t he name of the operator who performed the last action for the alarm.

Figure 26-1: Alarms History



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-02 15:55:59)

Name: MBK - 6310
Admin State: Unlocked
Oper State: Enabled
IP 10.77.10.130
Version 6.0.9

Active Alarms Count
● 11 ● 34 ● 23

History Performance
Not Polling

Entries: | 5 Journal Entries | 49 Alarms Entries

From: 03-Dec-2008 11:11 To: 09-Dec-2008 17:20

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator	Ack	Last Action
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:45 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		Automatic Cleared	
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow	acladmin	Ack	14:31:32 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow	acladmin	Ack	14:31:35 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow	acladmin	Ack	14:31:33 Dec 08...
minor	17:19:28 Dec 08 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow	acladmin	Ack	14:31:32 Dec 08...
Journal	12:54:30 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:54 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:48 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
Journal	12:53:48 Dec 08 ...	MBK - 6310	EMS Server	Faults: Ack Alarm	Updated Alarm(s) Alarm 1.3.6.1.4 ...	Moscow	acladmin		
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	20:39:04 Dec 02 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow	acladmin	Cleared	15:19:15 Dec 09...
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow	acladmin	Ack	12:54:30 Dec 08...
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	20:39:04 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	19:33:55 Dec 02 ...	MBK - 6310	Redundancy...	High Availability Alarm	Redundancy group have some ...	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	18:28:40 Dec 02 ...	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DS...	DS3 Alarm	RAI	Moscow		Automatic Cleared	17:19:41 Dec 08...
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	17:23:32 Dec 02 ...	MBK - 6310	Board#1/DTru...	Dchannel Status Alarm	D-Channel Trap	Moscow		New	
minor	[illegible]	MBK - 6310	Redundancy ...	High Availability Alarm	Redundancy group have some HA ...	Moscow		New	

The Time Filtering fields enable filtering alarms along the parameters of date and time. They're located adjacent to the filter buttons on the Alarms History screen's top bar, to their left. The date and time parameters both have a ' From' and 'To' (). This filter feature functions similarly to the other Alarms Browser filters. See the two figures below. The screen is a read-only screen. To refresh, choose the View menu's Refresh option, as the screen is not refreshed automatically.

To print alarm history, open the frame via Faults -> Alarm History menu, and then select the **File > Print option**.

27 Alarm Reports Graphical Display

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 and according to the user filters applied on this data.

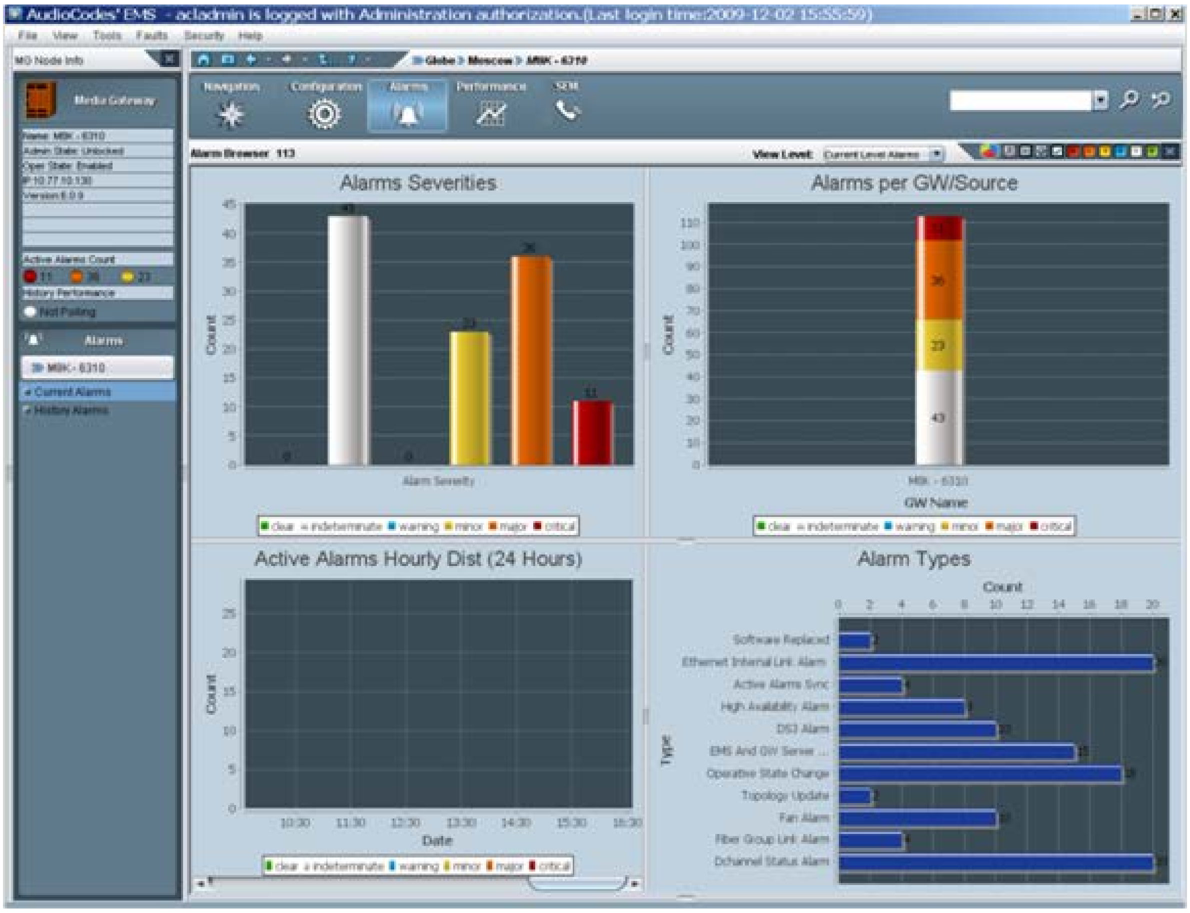
The following graphs are displayed:

- Alarms Severity distribution: displays the number of Critical, Major, Minor, Warning, Indeterminate and Clear alarms.
- Alarms Severities distribution over time: for Active alarms hourly – during the last 24 hours; for History alarms daily – during the time that the history data was viewed.
- Alarms Severities distribution per Gateway (when in the Region view) or in the selected context.
- Alarm Types distribution for the selected context. For example, the number of Security alarms, Power Supply alarms or Ethernet Switch alarms is displayed.

When you move the mouse over each one of the graph items, a tooltip is displayed with detailed information of the graph type and number of alarms in the view. You can view either a list of Current Alarms or a list of History Alarms.

The following screen illustrates the Current Alarms graph for the media gateway:

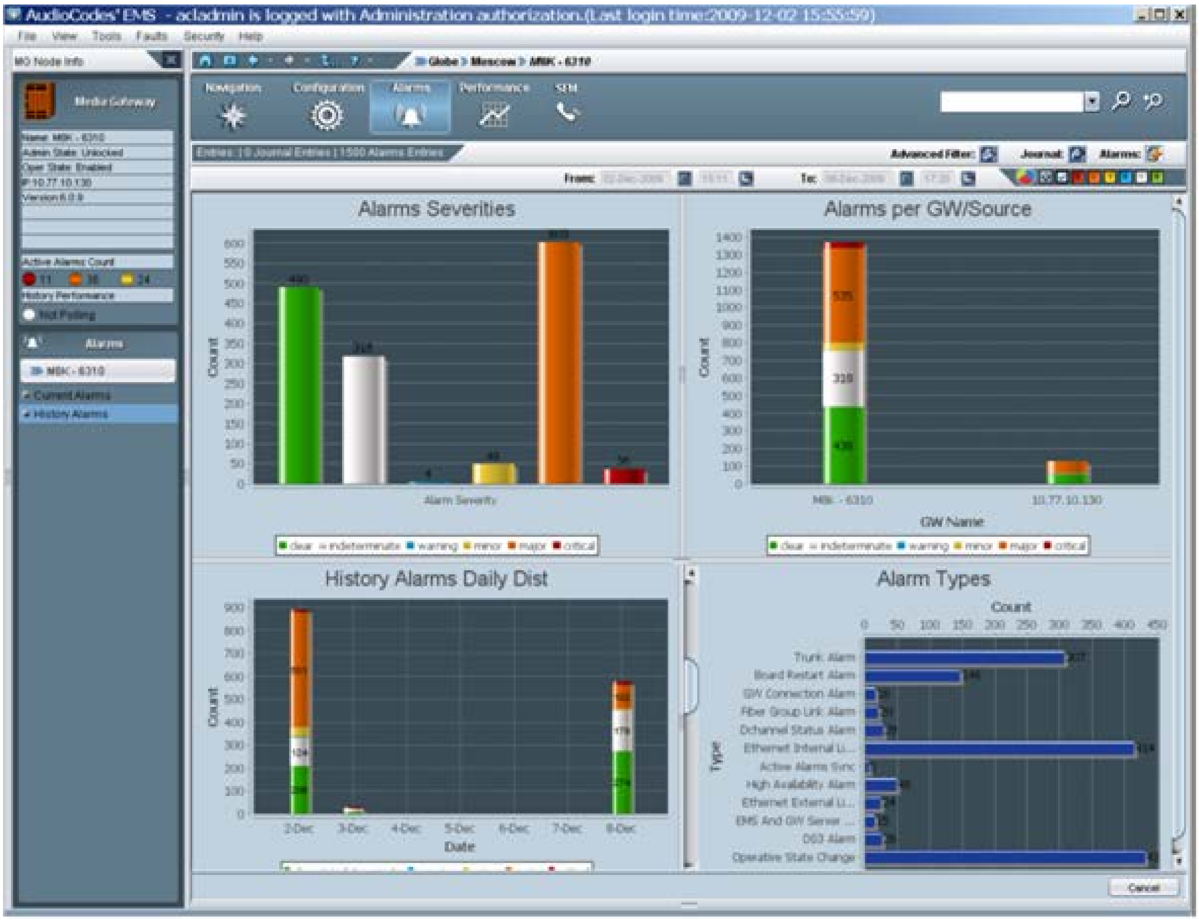
Figure 27-1: Current Alarms Graph



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-02 15:55:59)

The following screen illustrates the History Alarms graph for the media gateway:

Figure 27-2: History Alarms Graph



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-02 15:55:59)

Name: MBK - 6310
Admin State: Unlocked
Oper State: Enabled
IP 10.77.10.130
Version 6.0.9

Entries: 10 Journal Entries | 1500 Alarms Entries

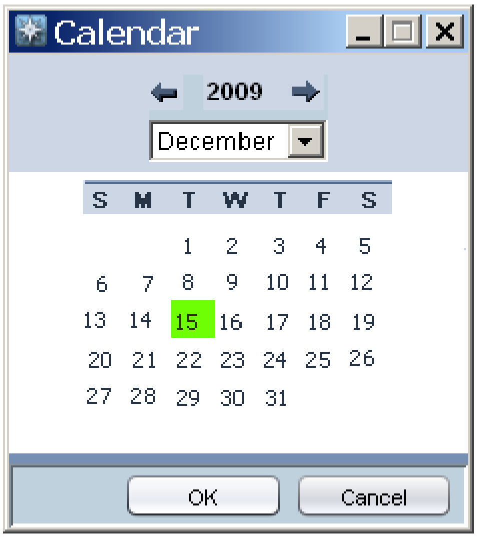
28 Using Alarm Filters

This section describes how to use the alarm filters.

28.1 Using Time Filters

The Time Filtering fields enable filtering alarms along the parameters of date and time. They're located adjacent to the severity filter buttons on the Alarms History screen's upper bar, to their left. The date and time parameters both have a 'From' and 'To'. This filter feature functions similarly to the other Alarms Browser filters. See the two figures below. To refresh (after defining a time filter), choose the View menu's Refresh option, as the screen is not refreshed automatically.

Figure 28-1: Alarms History Screen: Defining Time Filtration using Calendar

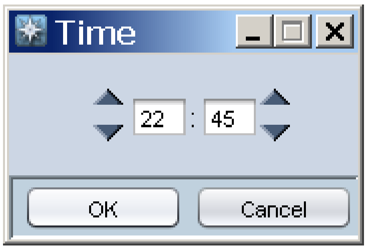


2009

December

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Figure 28-2: Alarms History Screen: Defining Time Filtration using Hour & Minutes



22 : 45

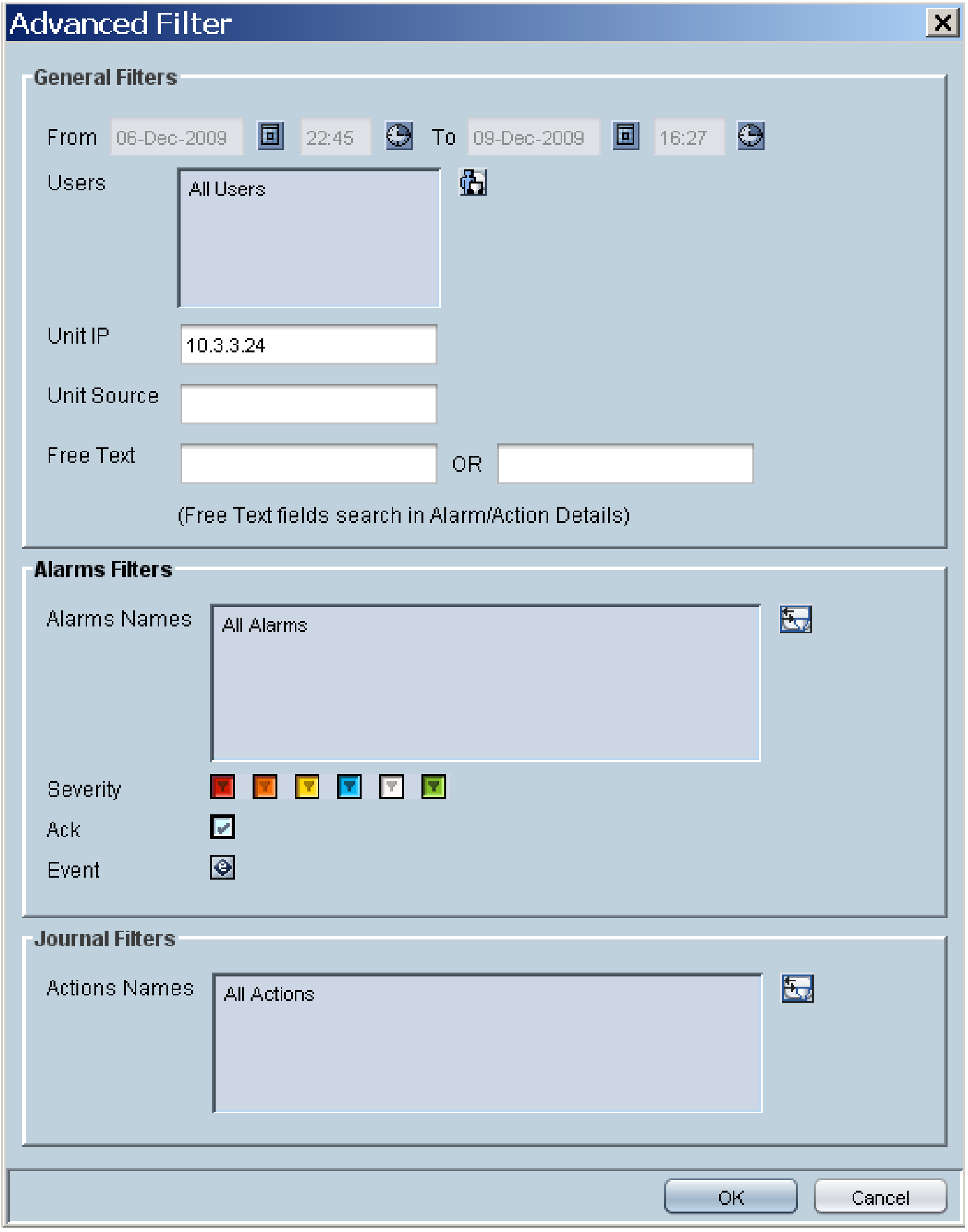
28.2 Using Advanced Filters

You can use the 'Advanced Filter' screen to define queries to search for EMS and media gateway alarms that were raised during a specific period. The filter also enables you to filter the severity of the raised alarms. In addition, you can define a query to search for events raised during a specific period, such as configuration updates to parameters and software downloads from the EMS to a media gateway.

The Advanced Filter menu is available from the History Alarms screen or from the Journal screens.

In each screen, click the **Advanced Filter** icon; the Advanced Filter screen is displayed.

Figure 28-3: Advanced Filter



Advanced Filter

General Filters

From 06-Dec-2009 22:45 To 09-Dec-2009 16:27

Users: All Users

Unit IP: 10.3.3.24

Unit Source:

Free Text: OR

(Free Text fields search in Alarm/Action Details)

Alarms Filters

Alarms Names: All Alarms

Severity

Ack ☑

Event

Journal Filters

Actions Names: All Actions

- **General Filters**

  To configure general filters, click the General Filters icon in the General Filters pane. You can configure the following filters:

  - Date and Time Filter
  - Users Filter. An operator can select a user or a set of users whose actions the operator needs to view.
  - Unit IP
  - Unit Source
  - Free Text 1 (searched in the Details filed)

- **Alarms Filters**

  To configure alarm filters, click the Alarms Filters icon in the Alarms Filters pane. You can configure the following filters:

  - Includes the lists of Alarms / Events per MG type.
  - Alarm Severity
  - Alarm Ack Status
  - Events

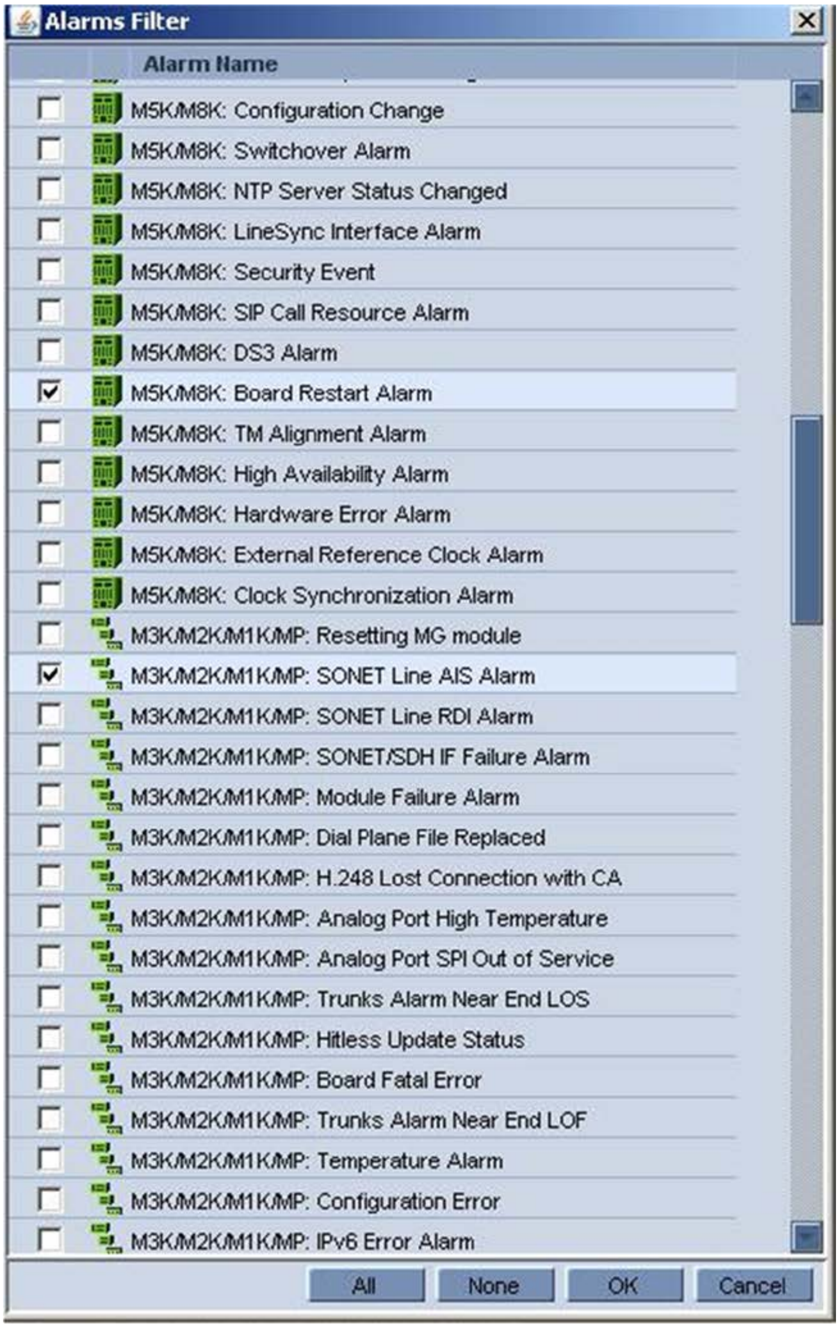
- **Journal Filters**

  To configure journal filters, click the Journal Filters icon in the Journal Filters pane. You can configure the following filters:

  - Actions Filter (all user actions are classified according to EMS functionality):
    - Fault Management Actions (acknowledge, delete, prioritize alarms, change trap configuration)
    - Configuration Management Actions (add, remove, update managed object, software upgrade, etc.)
    - Performance Management (start, stop polling, create, attach, detach PM profile)
    - Security Management Actions (add, remove, update operator info, login, logout)

The following screen displays an example of the Alarms Filter screen:

Figure 28-4: Alarms Filter



Alarm Name

- □ M5K/M8K: Configuration Change
- □ M5K/M8K: Switchover Alarm
- □ M5K/M8K: NTP Server Status Changed
- □ M5K/M8K: LineSync Interface Alarm
- □ M5K/M8K: Security Event
- □ M5K/M8K: SIP Call Resource Alarm
- □ M5K/M8K: DS3 Alarm
- ☑ M5K/M8K: Board Restart Alarm
- □ M5K/M8K: TM Alignment Alarm
- □ M5K/M8K: High Availability Alarm
- □ M5K/M8K: Hardware Error Alarm
- □ M5K/M8K: External Reference Clock Alarm
- □ M5K/M8K: Clock Synchronization Alarm
- □ M3K/M2K/M1K/MP: Resetting MG module
- ☑ M3K/M2K/M1K/MP: SONET Line AIS Alarm
- □ M3K/M2K/M1K/MP: SONET Line RDI Alarm
- □ M3K/M2K/M1K/MP: SONET/SDH IF Failure Alarm
- □ M3K/M2K/M1K/MP: Module Failure Alarm
- □ M3K/M2K/M1K/MP: Dial Plane File Replaced
- □ M3K/M2K/M1K/MP: H.248 Lost Connection with CA
- □ M3K/M2K/M1K/MP: Analog Port High Temperature
- □ M3K/M2K/M1K/MP: Analog Port SPI Out of Service
- □ M3K/M2K/M1K/MP: Trunks Alarm Near End LOS
- □ M3K/M2K/M1K/MP: Hitless Update Status
- □ M3K/M2K/M1K/MP: Board Fatal Error
- □ M3K/M2K/M1K/MP: Trunks Alarm Near End LOF
- □ M3K/M2K/M1K/MP: Temperature Alarm
- □ M3K/M2K/M1K/MP: Configuration Error
- □ M3K/M2K/M1K/MP: IPv6 Error Alarm

29 Defining Complex Queries using a Combination of Filters

Using a combination of filtering options, users can easily create complex queries.

29.1 Example of Filter Use

To find all the critical and major alarms and parameters that were modified in October 2008 in Board#8 of a s pecific gateway, apply the following filters in the 'Advanced Alarm Filter' screen:

- **Date & Time**: Define 'From date' as 'October 1, 2008' and 'To date' as 'November 1, 2008'.
- **Unit IP** - Define the gateway IP address or open the Journal in the appropriate context from the Alarm Browser for the parameter to automatically be defined.
- **Unit Source** - Define 'Board#8' in the field 'Unit Source' or open the Journal in the appropriate context from the Alarm Browser for the parameter to automatically be defined.
- **Alarm Filters**: leave Critical & Major severities selected and remove Events selection.
- In the 'Journal Actions' screen, select the checkbox **Configuration: Update**.

Reader's Notes

30 Viewing, Interpreting an Alarm's Details

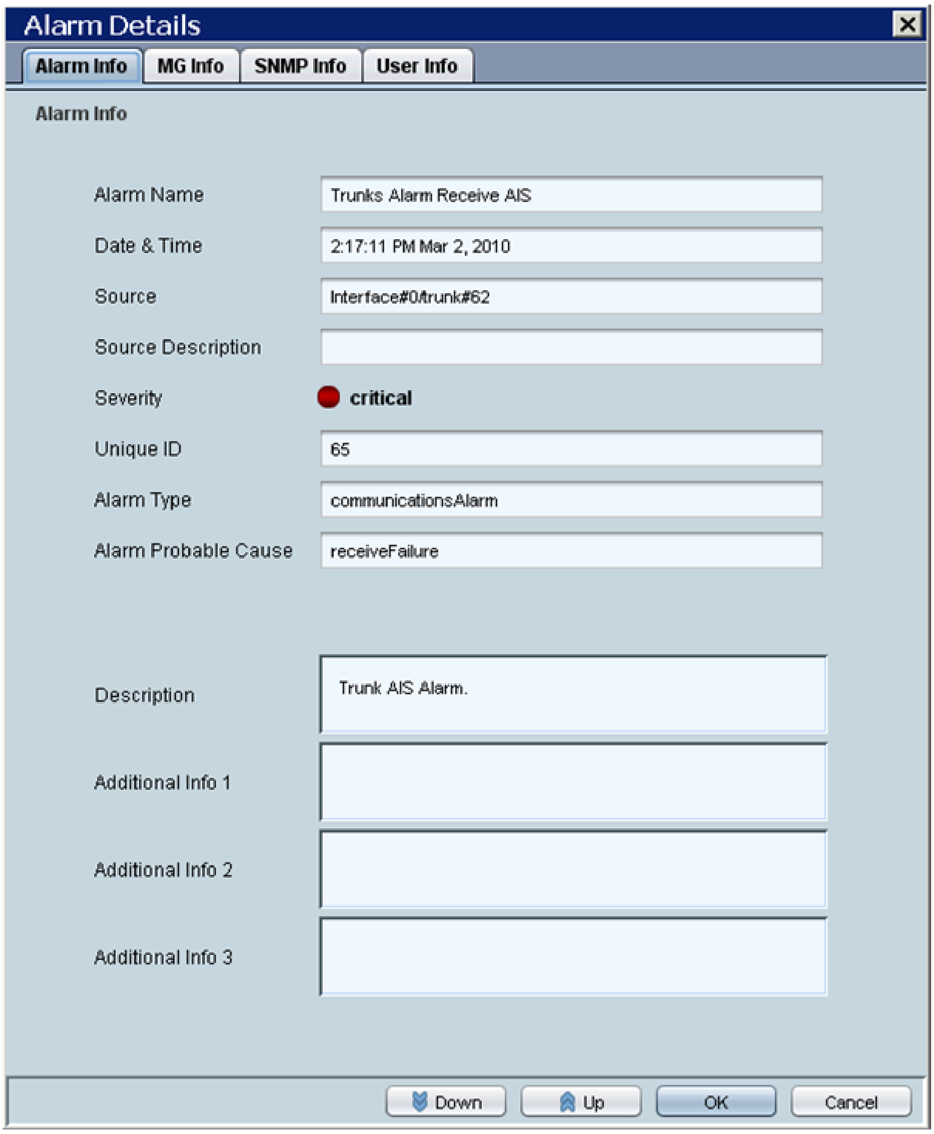
This section describes how to view and interpret an Alarm's Details.

➢ **To view/interpret an alarm's details, do one of the following:**

- Double-click the row of the alarm listed in the Alarm Browser or in the Alarms History, whose details you need to view/interpret.

  -OR-
- Right-click the row of the alarm listed in the Alarm Browser and select the option **Alarm Details** from the pop-up menu. The Alarm Details screen opens.

Figure 30-1: Alarm Details



Alarm Info

Alarm Name	Trunks Alarm Receive AIS
Date & Time	2:17:11 PM Mar 2, 2010
Source	Interface#0/trunk#62
Source Description	
Severity	● critical
Unique ID	65
Alarm Type	communicationsAlarm
Alarm Probable Cause	receiveFailure
Description	Trunk AIS Alarm.
Additional Info 1	
Additional Info 2	
Additional Info 3	

The Alarm Details screen features the following tabs:

- **Alarm Info** (includes all the information provided by the alarm; refer to its details below).
- **MG Info** (includes details regarding the location - region - of the media gateway, and the precise source of the alarm; refer to its details below).
- **SNMP Info** (includes SNMP-related information such as Trap OID, etc.; refer to its details below).
- **User Info** (includes user-specific information such as alarm status and identifying data fields that users can define to use as future reference when searching; refer to its details below).

30.1 Alarm Info Tab

The Alarm Info tab features the following fields:

- Title

  The name of the alarm, provided in the Alarm Browser.
- Date & Time

  Date and Time when the alarm was received by the EMS.
- Source

  The exact alarm source, in format, for example, “Board#3/Trunk#7”.
- Severity

  Alarm Severity as displayed in Alarm Browser pane, according to- ITU X.733 standard
- Unique ID

  Alarm Unique ID provided by the media gateway for alarm clearing and correlation purposes.
- Alarm Type

  The alarm type can be one of the following:
  - Communication (inter-process communication alarm)
  - Quality of Service (indicates degradation in service performance)
  - Processing Error (used for internal software errors)
  - Equipment Alarm (indicates a hardware failure)
  - Environmental alarm (used to indicate environmental errors such as temperature, power, etc.)

Notes: The parameter 'Alarm Type' is based on ITU X.733, X736 standards.

- Probable Cause

  The probable cause of the alarm. The probable cause can be one of the following:

  - Degraded Signal for Trunk Alarm
  - Communications Protocol Error for a V5.2 Alarm
  - Underlying Resource Unavailable for a Change in a Managed Entity's Administrative State or Operational State
  - Configuration Or Customization Error for Configuration Error Alarm
  - Heating Vent Cooling System Problem for Fan or Temperature Alarm
  - Temperature Unacceptable for Temperature Alarm
  - Power Problem for Voltage Alarm

Notes: he parameter 'Alarm Type' is based on ITU X.733, X736 standards.

- Description

  Textual description of the alarm, received as part of the alarm information

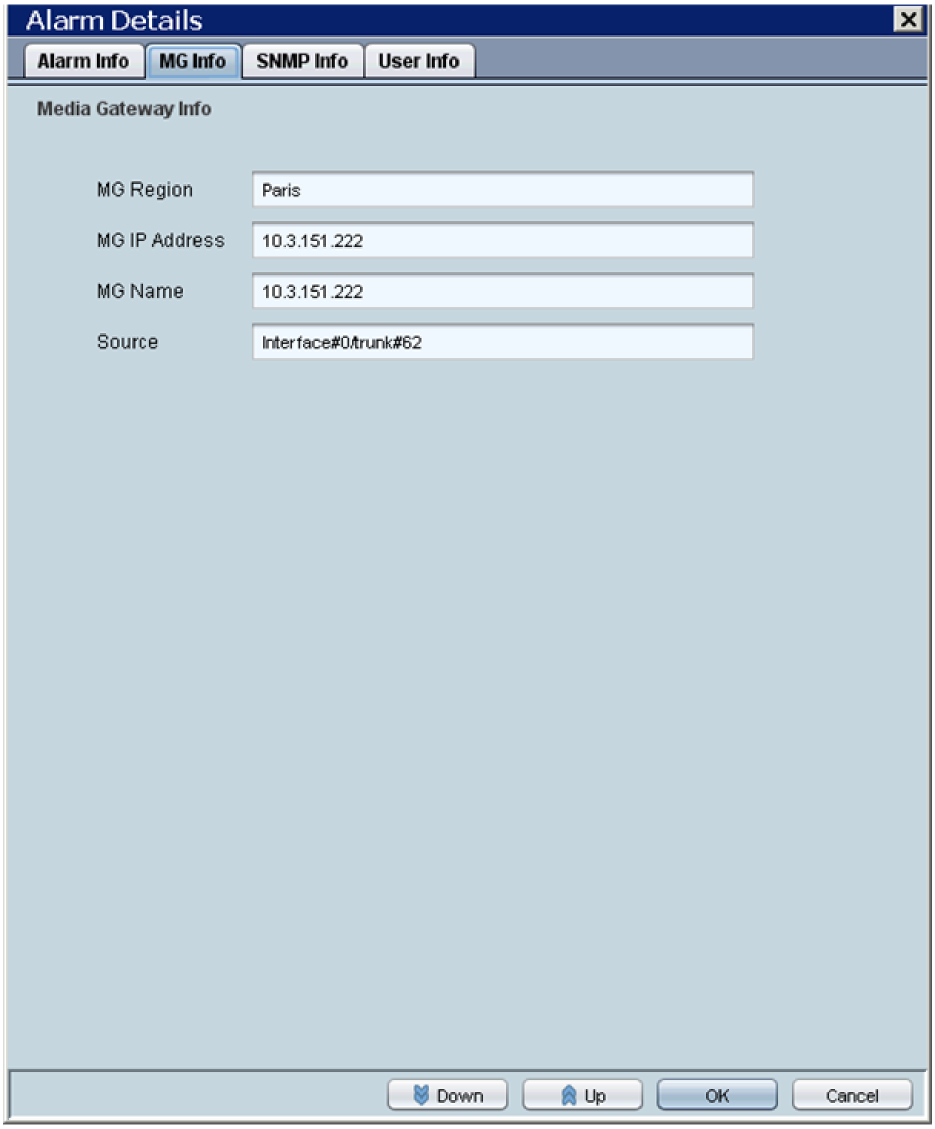
- Additional Info 1-3

  These three fields are provided as part of the alarm information, supplying additional information on the alarm.

30.2 Alarm Details - Tab MG Info

This section describes the MG Info tab.

Figure 30-2: Alarm Details-MG Info



Media Gateway Info

MG Region: Paris

MG IP Address: 10.3.151.222

MG Name: 10.3.151.222

Source: Interface#0/trunk#62

The **MG Info** tab features the following fields:

- MG Region

  The name of the region in which the media gateway is located.

- MG IP Address

  The IP address of the media gateway that originated the alarm.

- MG Name

  Name of the media gateway that originated the alarm.

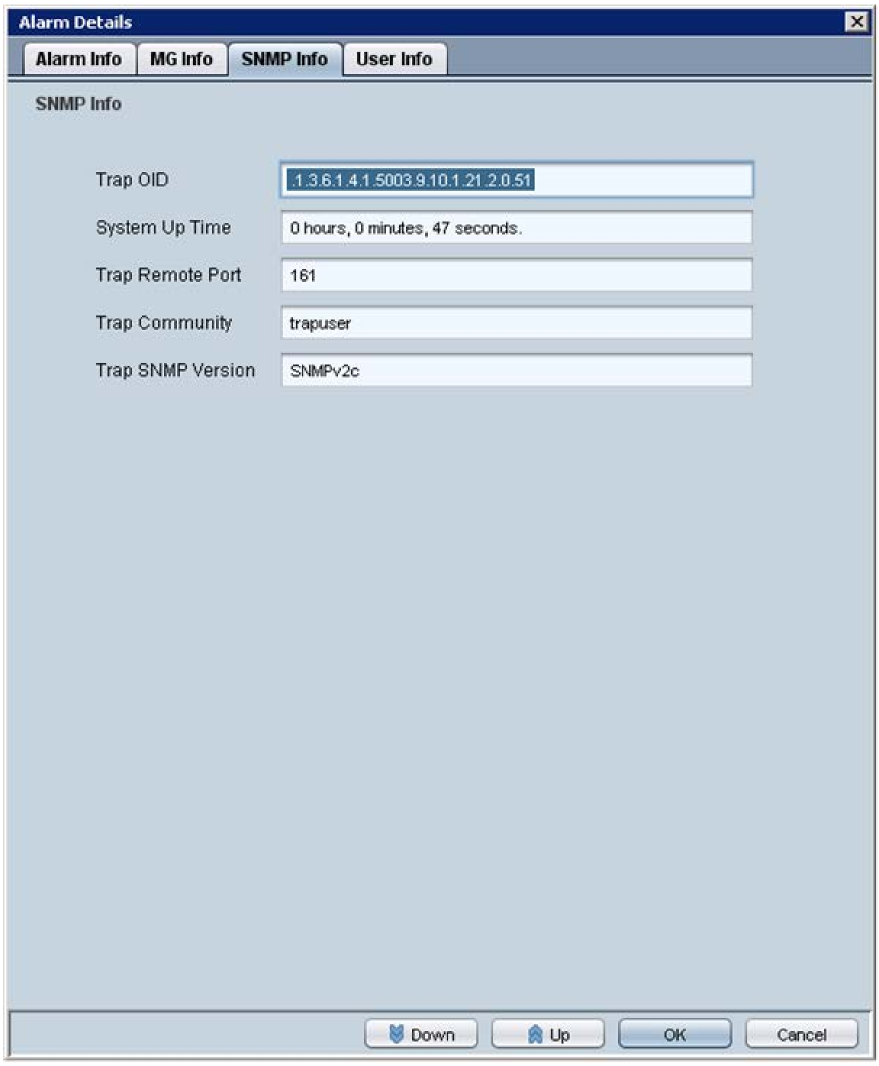
- Source

  The exact alarm source, in format 'board#3/trunk#7'

30.3 Alarm Details > Tab SNMP Info

This section describes the SNMP Info tab.

Figure 30-3: Alarm Details-SNMP Info



SNMP Info

Trap OID: .1.3.6.1.4.1.5003.9.10.1.21.2.0.51

System Up Time: 0 hours, 0 minutes, 47 seconds.

Trap Remote Port: 161

Trap Community: trapuser

Trap SNMP Version: SNMPv2c

The **SNMP Info** tab features the following fields:

- Trap OID

  Trap Object Identifier, as defined in the MIB.

- System Up Time

  The time elapsed since the last system reset.

- Trap Remote Port

  The EMS UDP remote port at which the trap was received.

- Trap Community

  Trap Community String received as part of the Notification message

- Trap SNMP Version

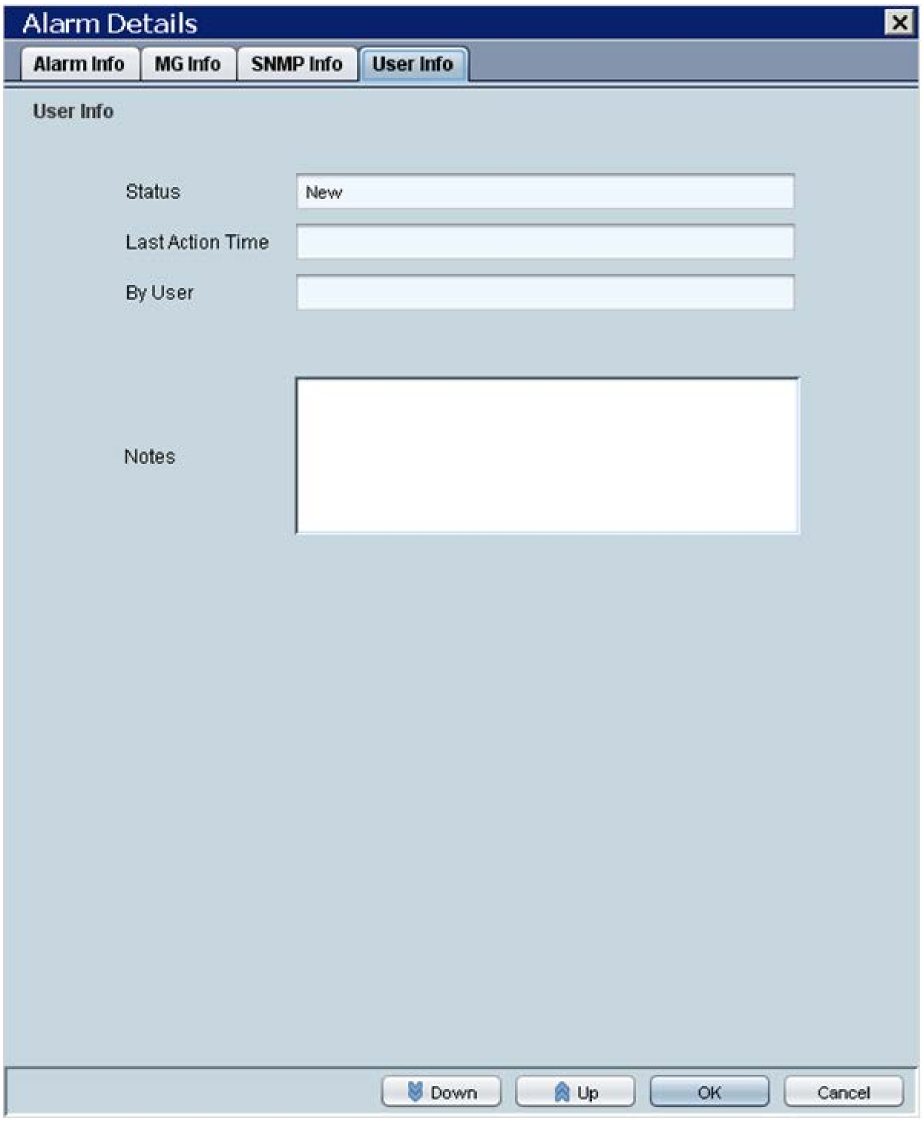
  The SNMP version of the Agent that sent the trap. The SNMP version can be one of the following:

  - SNMPv1
  - SNMPv2c
  - SNMPv3

30.4 Alarm Details > Tab User Info

This section describes the User Info tab.

Figure 30-4: Alarm Details-User Info



User Info

Status: New

Last Action Time:

By User:

Notes:

The **User Info** tab features the following fields:

- Status

  Either:

  - New (the alarm has recently been received by the EMS and currently Active.
  - Ack (the alarm was manually acknowledged by a user. Refer to the other User Info fields.
  - Cleared (the alarm was manually cleared (deleted) by a user. Refer to the other User Info fields.
  - Automatic Cleared (a clear alarm was received by the EMS from the media gateway; the alarm condition no longer exists.
  - ColdStart Cleared (The media gateway generated a cold start event and all the old alarms are cleared by this action.
- Last Action

  The time an action was performed on the alarm.
- By User

  The name of the user who performed the last action on the alarm.
- Notes

  Define this field for you to use as future reference when searching.

➢ To print an alarm's details:

- Right-click any of the tabs of the Alarm Details screen, and select the **Print** option.

Reader's Notes

31 Trap Forwarding

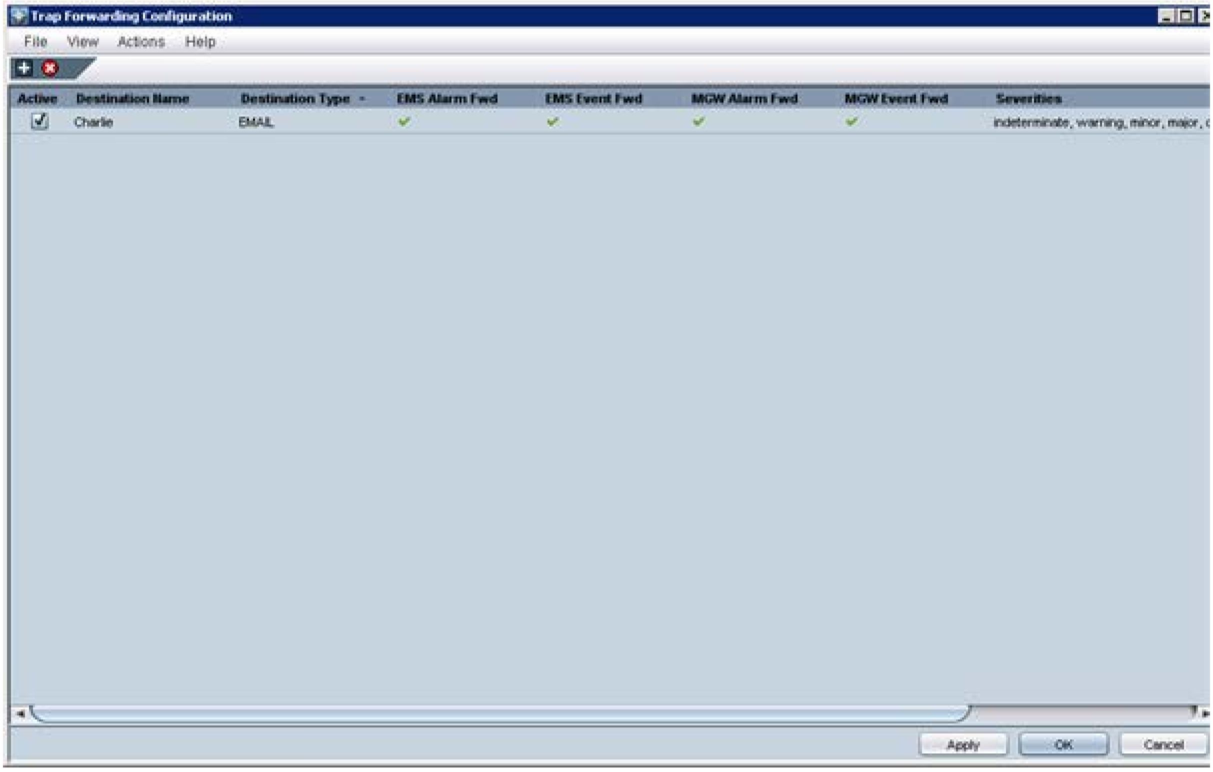
All the alarms and events issues by media gateways are send as SNMP Notifications. EMS can forward alarms and events in the following formats:

- SNMP Notifications
- SMS
- Mail
- Syslog

Multiple Trap forwarding destinations are supported. Each line in the Trap Forwarding Table defines a specific destination. The SNMP forwarding option is usually used for EMS – NMS integration. For more information regarding SNMP Notifications forwarding, refer to the *OAM Integration Guide*.

The section below describes how to configure Mail, SMS and Syslog trap forwarding options.

Figure 31-1: Trap Forwarding Summary-Mail



Active	Destination Name	Destination Type	EMS Alarm Fwd	EMS Event Fwd	MGW Alarm Fwd	MGW Event Fwd	Severities
☑	Charlie	EMAIL	✓	✓	✓	✓	indeterminate, warning, minor, major, c

31.1 Trap Forwarding in Mail Format

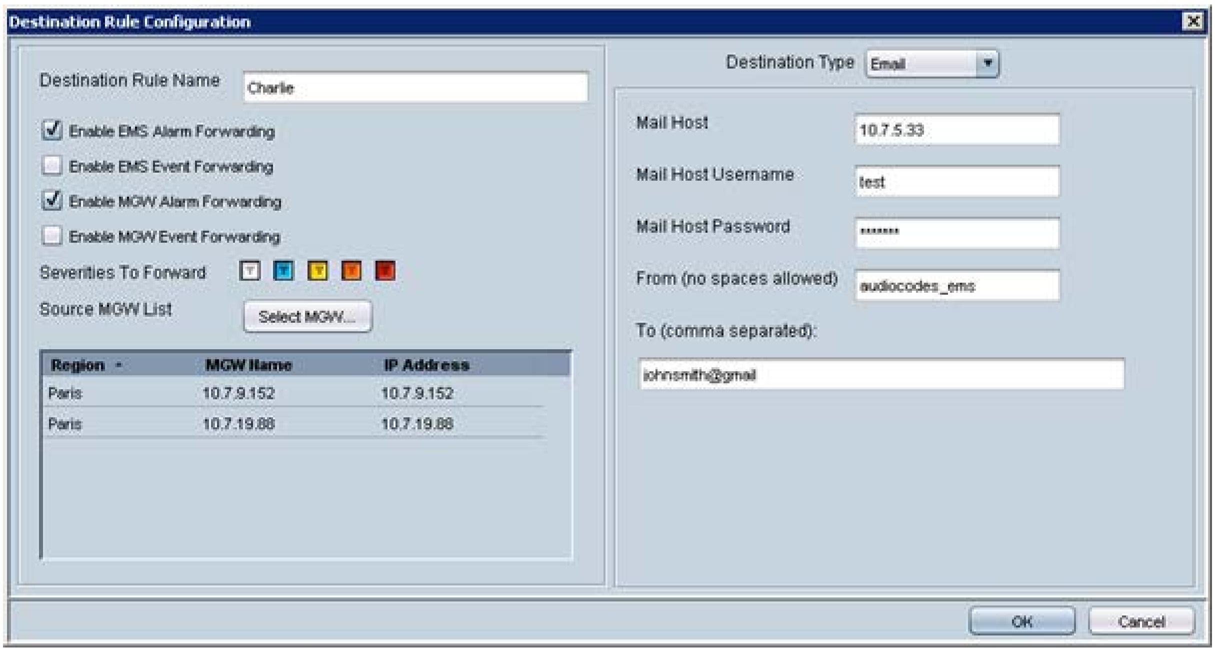
This option describes how to forward traps from EMS to a mail server host in e-mail format.

➢ To forward traps in mail format:

1. Open the **Faults >Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Email**.
4. In the left-hand pane, provision the following parameters:
   - 'Destination Rule Name' as you wish it to appear in the summary screen.
   - Select the subset of alarms and events that must be forwarded to the NMS from the following subset (by default, all the alarms and events are selected):
     - ♦ EMS Alarms Forwarding
     - ♦ EMS Events Forwarding
     - ♦ MGW Alarms Forwarding
     - ♦ MGW Events Forwarding
     - ♦ Select the subset of 'Severities To Forward': severities that you wish to receive in the NMS application (by default, all the severities are selected). Note: CLEAR alarms for selected subset of the alarms are always forwarded.
     - ♦ Select the media gateways from which you wish to forward alarms and events.

5. In the right-hand pane, provision the following parameters:
   - In the 'Mail Host IP Address' field, enter the **Mail Host IP address**.
   - In the 'Mail Host Username' field, enter the **mail host username**.
   - In the 'Mail Host Password' field, enter the **mail host password**.
   - In the 'From' field, enter the the **e-mail address** the recipient will see when the mail arrives.
   - In the 'To' field, enter the **list of email addresses** (coma separated) to which you wish to send mail.

Figure 31-2: Trap Forwarding-Email



Destination Rule Configuration

Destination Rule Name: Charlie

☑ Enable EMS Alarm Forwarding

□ Enable EMS Event Forwarding

☑ Enable MGW Alarm Forwarding

□ Enable MGW Event Forwarding

Severities To Forward

Source MGW List

Region	MGW Name	IP Address
Paris	10.7.9.152	10.7.9.152
Paris	10.7.19.88	10.7.19.88

Destination Type: Email

Mail Host: 10.7.5.33

Mail Host Username: test

Mail Host Password: ********

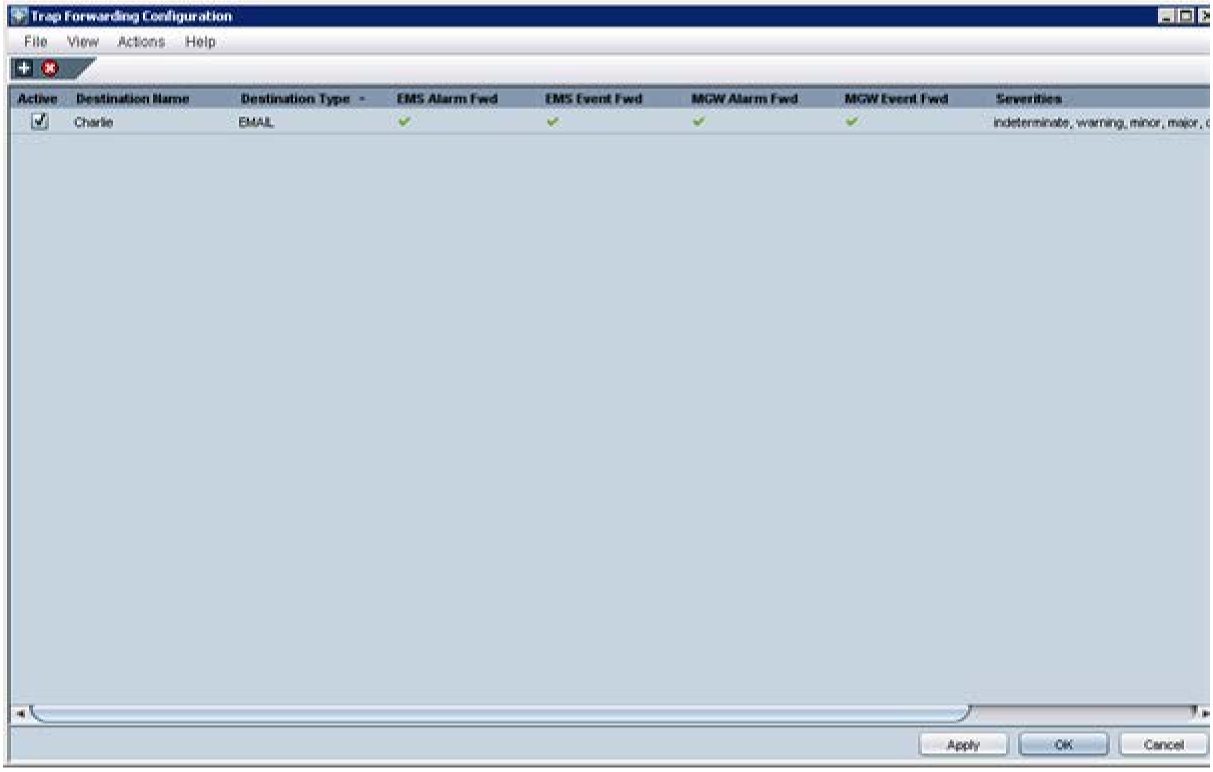
From (no spaces allowed): audiocodes_ems

To (comma separated): iohnsmith@gmail

6. Click **OK**.

Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 31-3: Trap Forwarding Summary-Mail



Active	Destination Name	Destination Type	EMS Alarm Fwd	EMS Event Fwd	MGW Alarm Fwd	MGW Event Fwd	Severities
☑	Charlie	EMAIL	✓	✓	✓	✓	indeterminate, warning, minor, major, c

EMAIL traps are forwarded to specified destinations in the following format:

```
EMAIL format
Title: New <Alarm/Event> <Alarm Name>, received from <Node Name>
with Severity <Severity>
Message body: will include all the fields we have today in Alarm
Item
```

31.2 Trap Forwarding in Mail2SMS Format

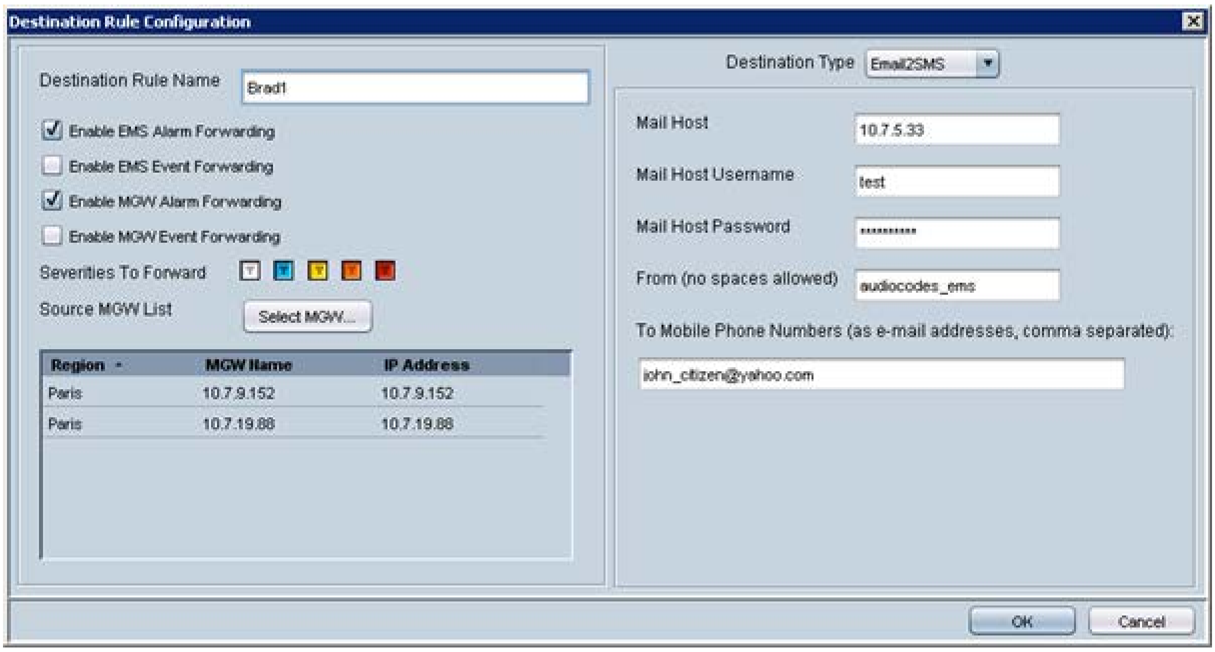
This option describes how to forward traps from EMS to a mail server host in mail2SMS format.

➢ To forward traps in mail2SMS format:

1. Open the **Faults >Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Mail2SMS**.
4. In the left-hand pane, provision the following parameters:
    - 'Destination Rule Name' as you wish it to appear in the summary screen.
    - Select the subset of alarms and events that must be forwarded to the NMS from the following subset (by default, all the alarms and events are selected):
    - EMS Alarms Forwarding
    - EMS Events Forwarding
    - MGW Alarms Forwarding
    - MGW Events Forwarding
        - ♦ Select the subset of 'Severities To Forward'; severities that you wish to receive in the NMS application (by default, all the severities are selected). Note: CLEAR alarms for selected subset of the alarms are always forwarded.
        - ♦ Select the media gateways from which you wish to forward alarms and events.
5. In the right-hand pane, provision the following parameters:
    - In the 'Mail Host IP Address' field, enter the **Mail Host IP address**.
    - In the 'Mail Host Username' field, enter the **mail host username**.
    - In the 'Mail Host Password' field, enter the **mail host password**.
    - In the 'From' field, enter the e-mail address the recipient will see when the mail arrives.

- In the 'To Mobile Numbers' field, enter the **list of Email addresses** (comma separated) to whose corresponding mobile numbers you wish to send mail.

Figure 31-4: Trap Forwarding-SMS



Destination Rule Configuration

Destination Rule Name: Brad1

☑ Enable EMS Alarm Forwarding

□ Enable EMS Event Forwarding

☑ Enable MGW Alarm Forwarding

□ Enable MGW Event Forwarding

Severities To Forward

Source MGW List

Region	MGW Name	IP Address
Paris	10.7.9.152	10.7.9.152
Paris	10.7.19.88	10.7.19.88

Destination Type: Email2SMS

Mail Host: 10.7.5.33

Mail Host Username: test

Mail Host Password: **********

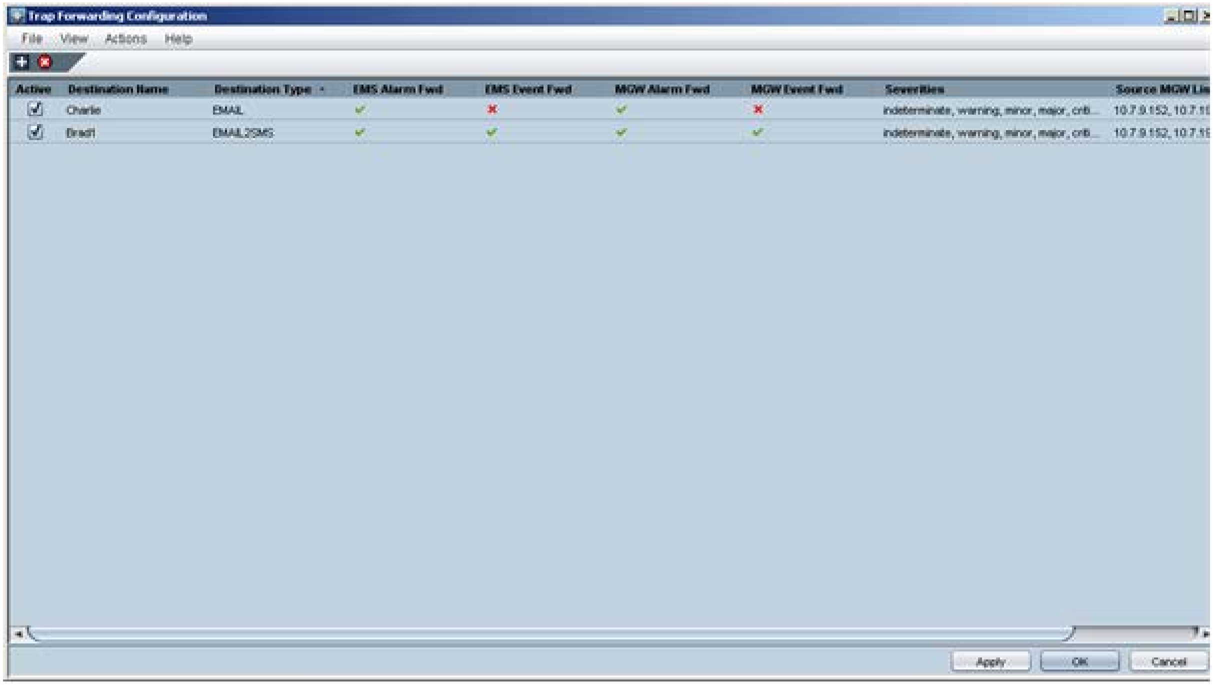
From (no spaces allowed): audiocodes_ems

To Mobile Phone Numbers (as e-mail addresses, comma separated): iohn_citizen@yahoo.com

6. Click **OK.**

   Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 31-5: Trap Forwarding Summary-Mail2SMS



Trap Forwarding Configuration

Active	Destination Name	Destination Type	EMS Alarm Fwd	EMS Event Fwd	MGW Alarm Fwd	MGW Event Fwd	Severities	Source MGW Lis
☑	Charlie	EMAIL	✓	✗	✓	✗	indeterminate, warning, minor, major, criti...	10.7.9.152, 10.7.1
☑	Brad1	EMAIL2SMS	✓	✓	✓	✓	indeterminate, warning, minor, major, criti...	10.7.9.152, 10.7.1

Notes: CLEAR alarms for selected subset of the alarms are always forwarded.

- Select the media gateways from which you wish to forward alarms and events.

31.3 Trap Forwarding in Syslog Format

This option describes how to forward traps from EMS to a syslog server host in syslog format.

➢ **To forward traps in syslog format:**

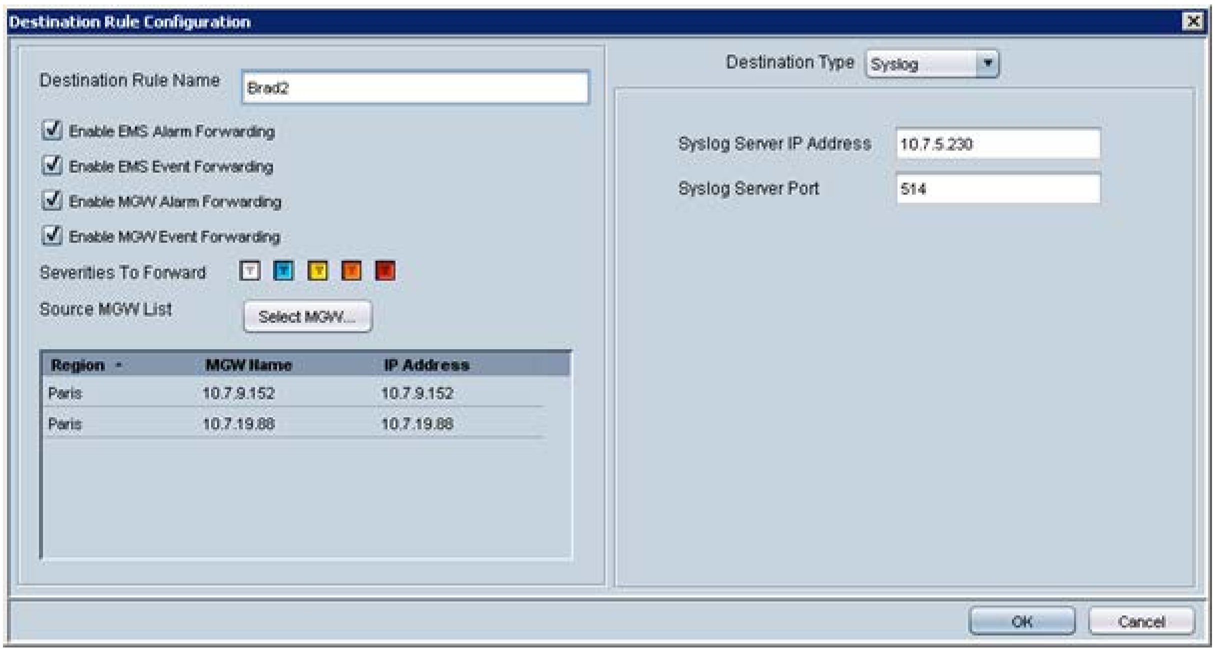
1. Open the **Faults** > **Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Syslog**.
4. In the left-hand pane, provision the following parameters:
   - 'Destination Rule Name' as you wish it to appear in the summary screen.
   - Select the subset of alarms and events that must be forwarded to the NMS from the following subset (by default, all the alarms and events are selected):
     - ♦ EMS Alarms Forwarding
     - ♦ EMS Events Forwarding
     - ♦ MGW Alarms Forwarding
     - ♦ MGW Events Forwarding
   - Select the subset of 'Severities To Forward'; severities that you wish to receive in the NMS application (by default, all the severities are selected).

Note: CLEAR alarms for selected subset of the alarms are always forwarded.

Select the media gateways from which you wish to forward alarms and events.

5. In the right-hand pane, provision the following parameters:
   - Enter the Syslog Server IP Address.
   - Enter the Syslog Server Port.

Figure 31-6: Trap Forwarding-Syslog



Destination Rule Configuration

Destination Rule Name: Brad2

☑ Enable EMS Alarm Forwarding
☑ Enable EMS Event Forwarding
☑ Enable MGW Alarm Forwarding
☑ Enable MGW Event Forwarding

Severities To Forward

Source MGW List

Region	MGW Name	IP Address
Paris	10.7.9.152	10.7.9.152
Paris	10.7.19.88	10.7.19.88

Destination Type: Syslog

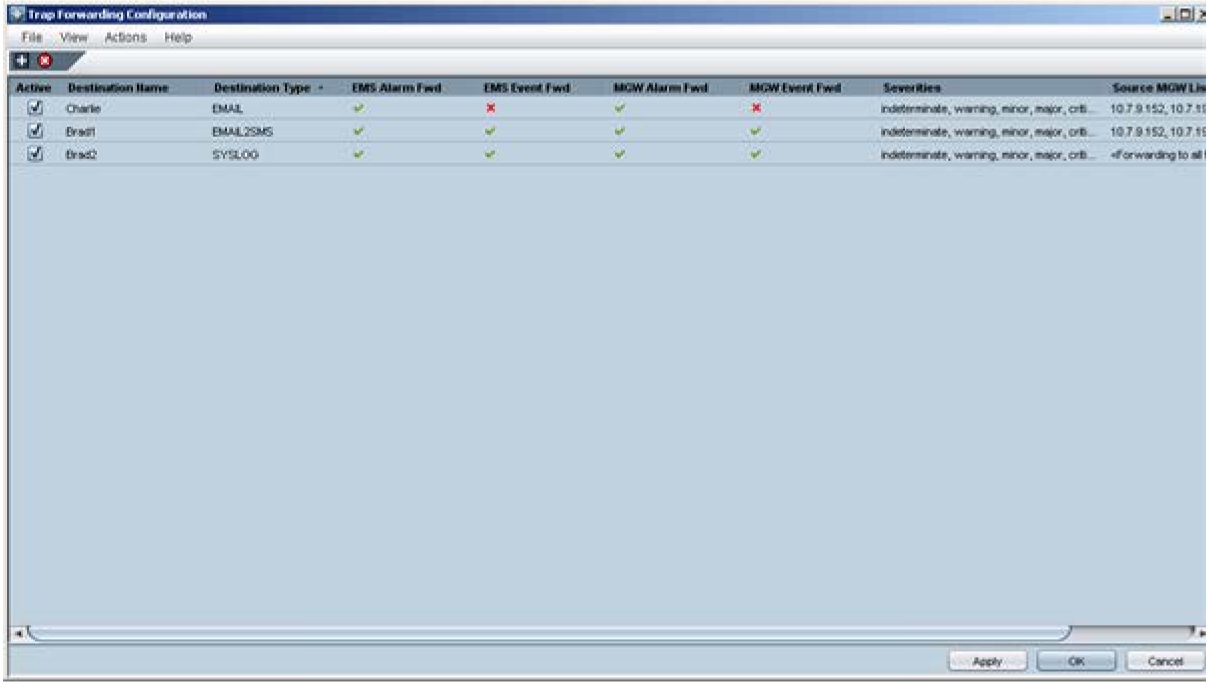
Syslog Server IP Address: 10.7.5.230

Syslog Server Port: 514

6. Click **OK.**

Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 31-7: Trap Forwarding Configuration Summary-Syslog



Trap Forwarding Configuration

Active	Destination Name	Destination Type	EMS Alarm Fwd	EMS Event Fwd	MGW Alarm Fwd	MGW Event Fwd	Severities	Source MGW Lis
☑	Charlie	EMAIL	✓	✗	✓	✗	indeterminate, warning, minor, major, criti...	10.7.9.152, 10.7.1
☑	Brad1	EMAIL2SMS	✓	✓	✓	✓	indeterminate, warning, minor, major, criti...	10.7.9.152, 10.7.1
☑	Brad2	SYSLOG	✓	✓	✓	✓	indeterminate, warning, minor, major, criti...	<Forwarding to all

Since syslog has a well-defined message format structure (defined by RFC 3164), the severity levels in EMS are adjusted to the severity levels of the syslog protocol. The following table describes the severity levels mapping:

Table 31-1: EMS and Syslog Severity Mapping

EMS Severity	Syslog Severity
Critical	Alert
Major	Critical
Minor	Error
Warning	Warning
Indeterminate	Informational
Clear	Notice

The message part of the syslog protocol will contain the following structure:

```
Title: <Alarm/Event> <Alarm Name>, received from <Node Name, Node IP>
with Severity <Severity>.
Description: <Source>, <Description>
```

Reader's Notes

32 Saving Alarms in a .csv File

Viewed alarms can be saved in a *.csv file (Comma Separated 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.

➢ To save 'Alarm Browser' alarms in a *.csv file:

- Open the 'Faults' menu and choose option **Save Alarms** in the EMS main screen; Alarms viewed in the Alarm Browser screens are saved (apply appropriate filters before saving alarms).

➢ To save 'Alarms History' alarms in a *.csv file:

- Open the 'Faults' menu and choose option **Save Alarms** in the Alarms History screen.

  The result is one of the following:

  - When the number of alarms is less than 1500, the alarms viewed in the Alarms History screen are saved in the location chosen by the user (apply appropriate filters before saving alarms)
  - When the number of alarms is 1500 (the maximum that can be displayed in the Alarm History screen), the EMS assumes that the actual number of alarms answering the selecting criteria is greater than 1500. Users are prompted whether to save all available alarms or only those alarms that they're currently viewing. If the user chooses to save all alarms, the EMS creates a .csv file in the EMS server machine installation folder, under directory '/ACEMS/NBIF/alarms'. The file name is alarm_result_<date_time>, where <date_time> is the query date and time. The maximum file size is 65000 lines (due to an Excel™ limitation). If the user chooses to save only the viewed alarms, the file chooser is opened and the file is saved in the location chosen by the user.

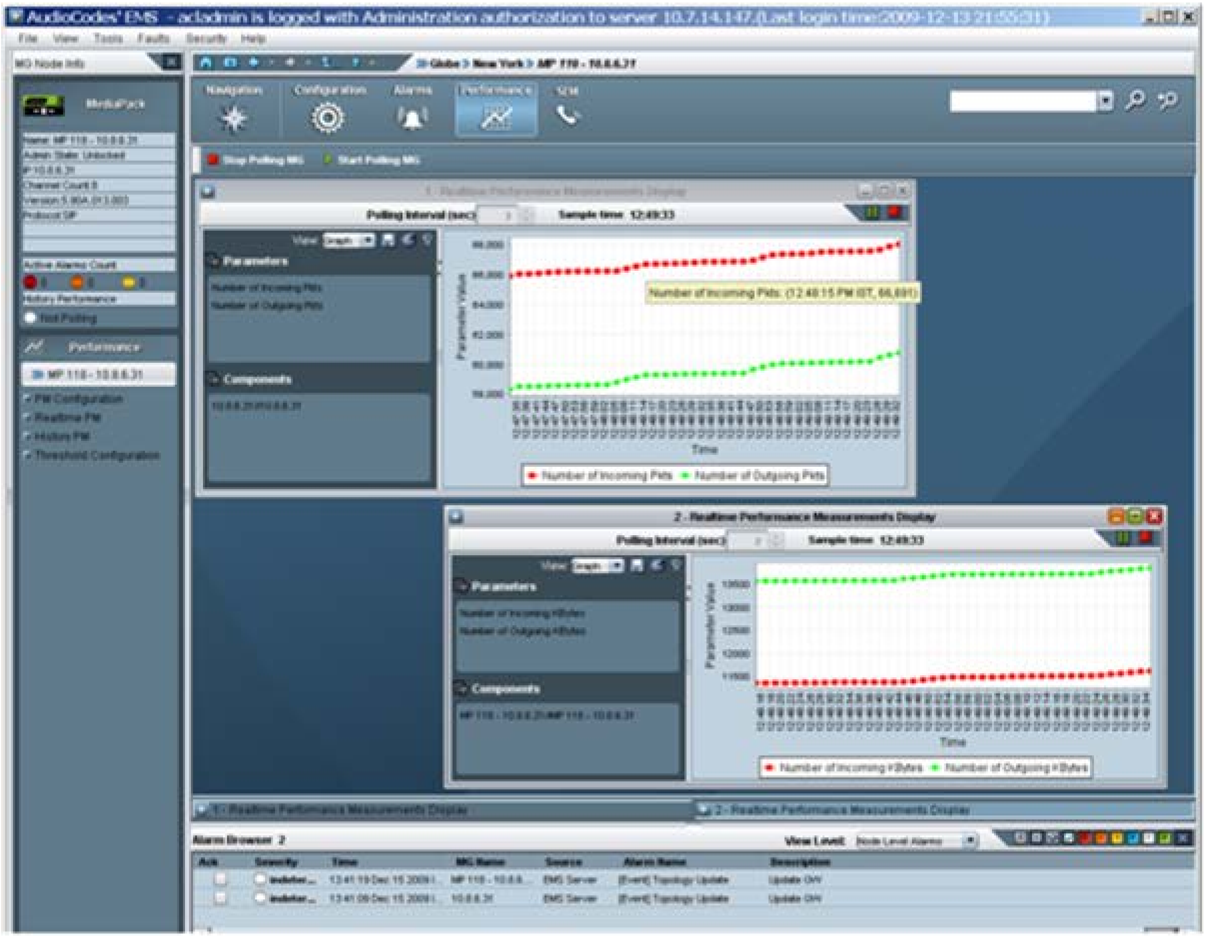
Reader's Notes

33 Performance Management

After service is provisioned for a s ubscriber 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. This section describes the performance management functionality of the EMS.

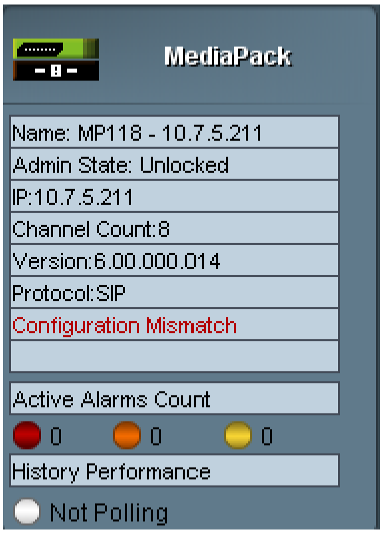
The EMS's Performance Management is composed of real-time and hi storical data monitoring. Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. Historical data can be used for long-term network analysis and planning. For the exact list of all the Performance Monitoring parameters supported for each one of the Gateways, refer to the relevant product *OAM Guide*.

Figure 33-1: Performance Desktop



Notes: The history performance monitoring icon in displayed in the Info pane. The color of the icon (adjacent to 'History Performance') indicates whether background monitoring is running for a specific device. Green indicates that it is running; gray indicates that it is not running. All the performance monitoring menus are displayed on the Performance desktop for the selected gateway / managed object.

Figure 33-2: Performance Monitoring Icon in the Info Pane



MediaPack

Name: MP118 - 10.7.5.211
Admin State: Unlocked
IP:10.7.5.211
Channel Count:8
Version:6.00.000.014
Protocol:SIP
Configuration Mismatch

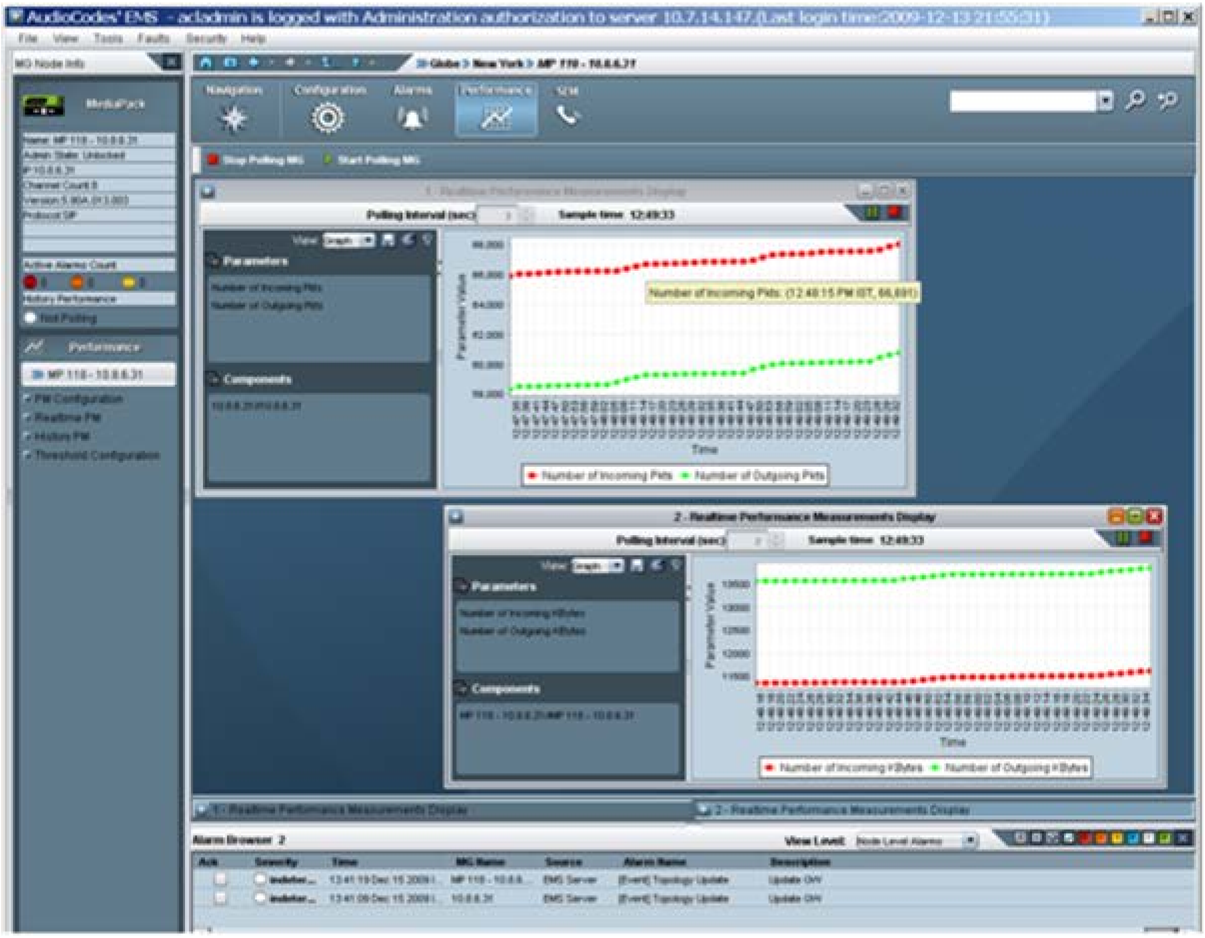
Active Alarms Count
● 0 ● 0 ● 0

History Performance
○ Not Polling

33.1 Real-Time Performance Monitoring

Real-time performance monitoring provides EMS users with the ability to perform high-frequency polling of various system parameters.

Figure 33-3: Real-time PMs



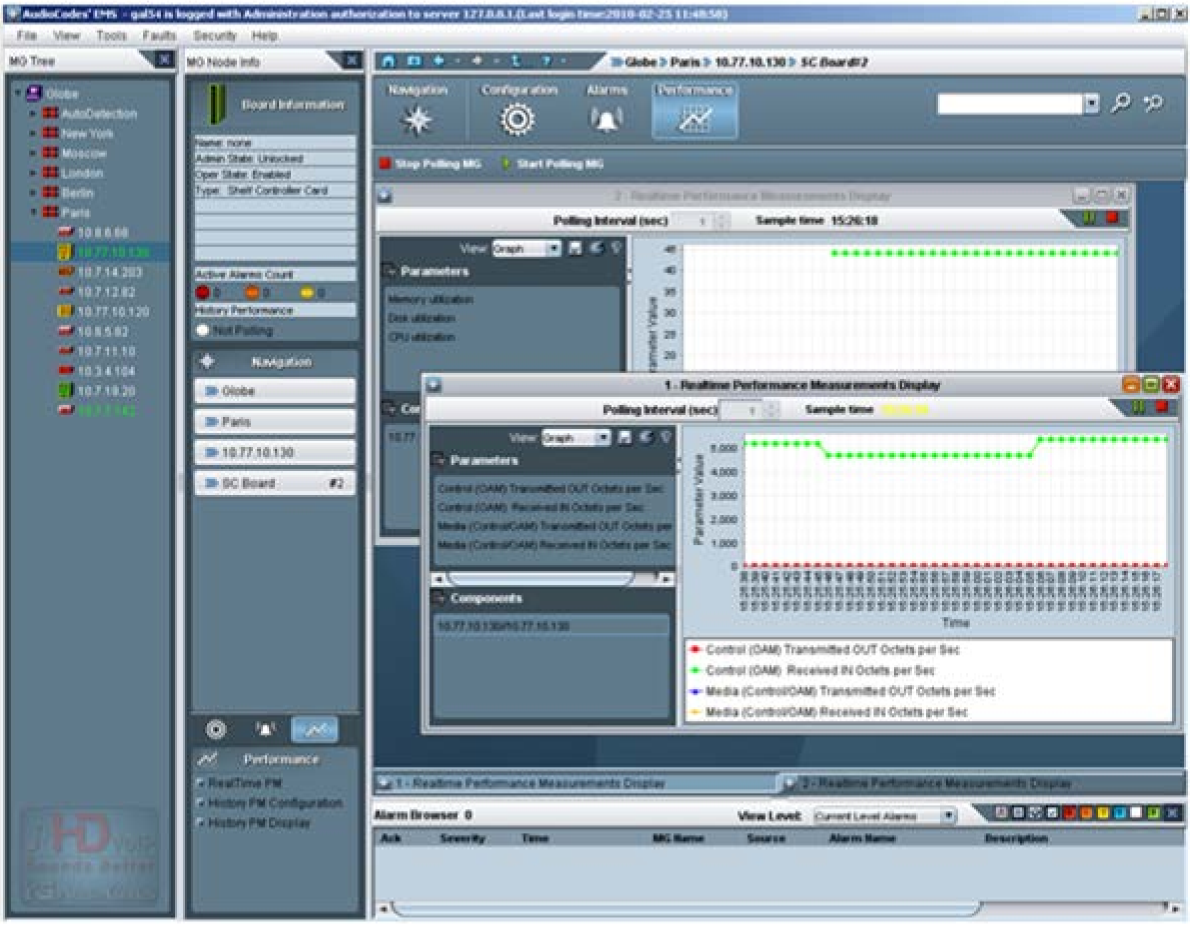
➢ To select an entity to poll:

1. Select the relevant media gateway entity for which you wish to display Real Time PMs. For example, select the media gateway board, and then in the Desktop toolbar, click **Performance**.

   The EMS application automatically displays a pre-defined real-time graph showing the progress of key parameters. The user 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.

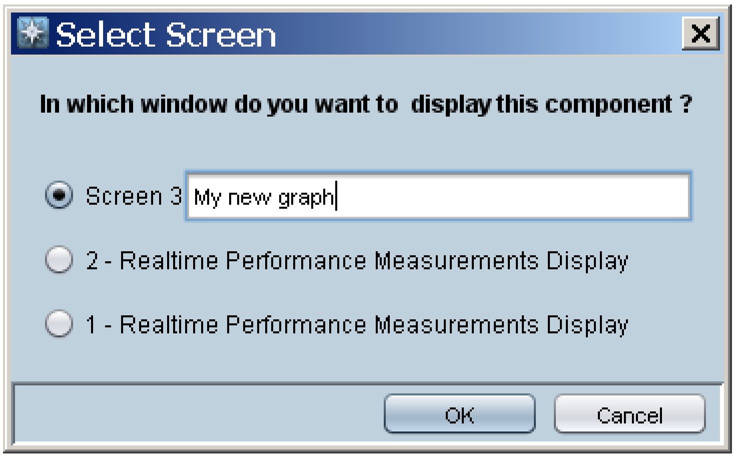
2. To define additional real-time performance monitoring windows, in the Performance pane, select **RealTime PM**.

Figure 33-4: Select Real-time Polling Entity



3. Select the frame you prefer (a new frame or an already existing frame) to view the performance graph (refer to the figure below) and click **OK**. Note that when choosing to open real-time monitoring graphs in the new frame, you can enter your own frame title.

Figure 33-5: Selecting the Frame to Display the Graph of the Entity's Performance



Select Screen

In which window do you want to display this component ?

● Screen 3 My new graph

○ 2 - Realtime Performance Measurements Display

○ 1 - Realtime Performance Measurements Display

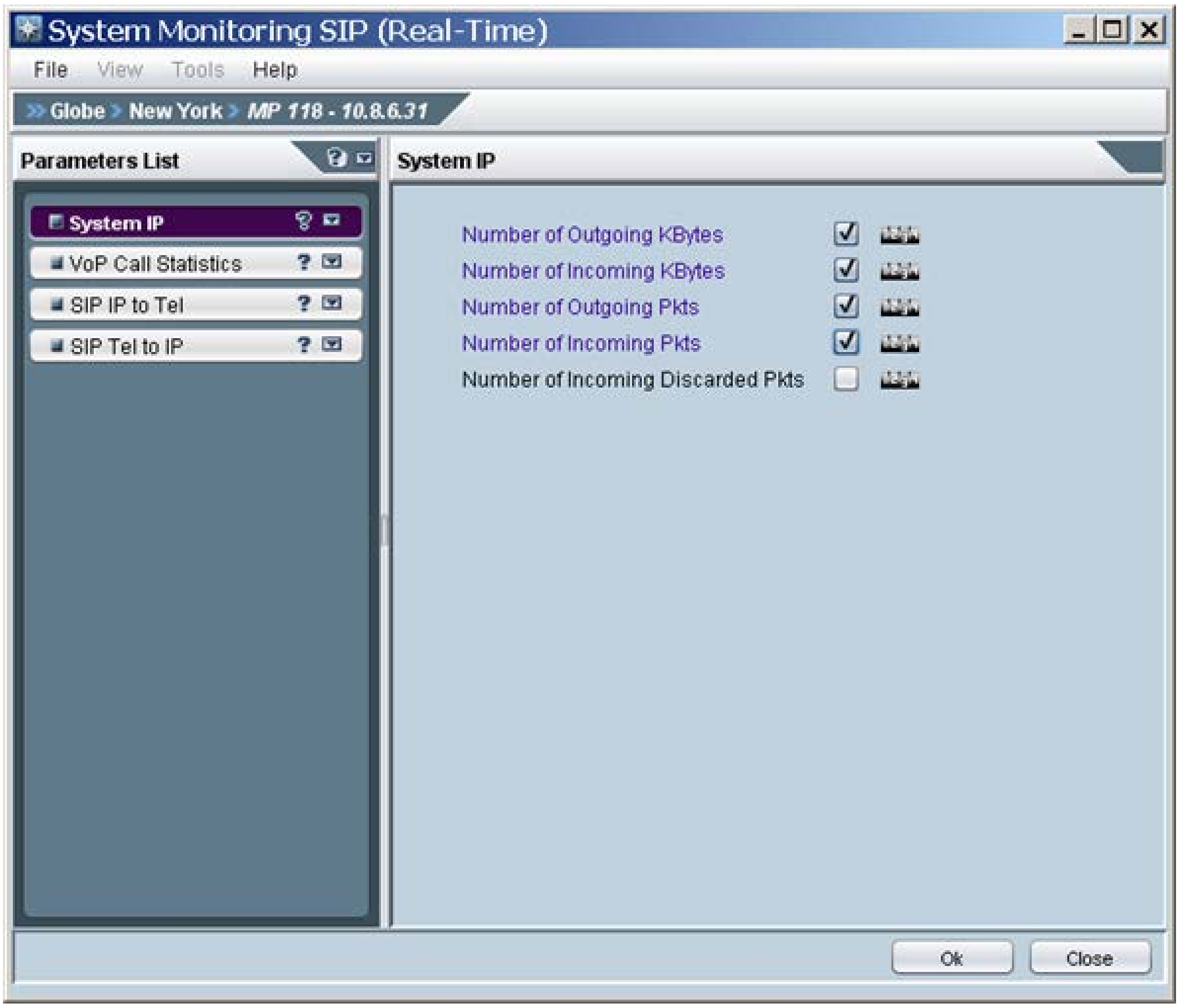
Users can open up to five separate real-time graphs in the same client application. There are two graph types that operators can use: Line Graph and Table View. In most cases, Line Graph is recommended when only a few parameters are compared. Table View is recommended when extensive data is displayed and analyzed.

In each Line Graph, you can simultaneously view up to 10 parameters of the same entity (media gateway, board and trunk) or compare the same parameters over different entities (different boards / trunks of the same or different gateways). In each Table Graph, you can simultaneously view up to 50 parameters of up to 50 entities (Table 50X50).

After opening the real-time frame, you can continue selecting entities to add to it. After all entities are selected, select the parameter to poll by clicking the button 'Parameters Filter' on the top left side of the real-time frame . Only parameters available for that entity type are displayed for selection.

The performance-monitoring feature supports two parameter types: Gauges and Counters. Gauges are indicated by and Counters are indicated by .

Figure 33-6: Parameter Type - Counters



Number of Outgoing KBytes ☑

Number of Incoming KBytes ☑

Number of Outgoing Pkts ☑

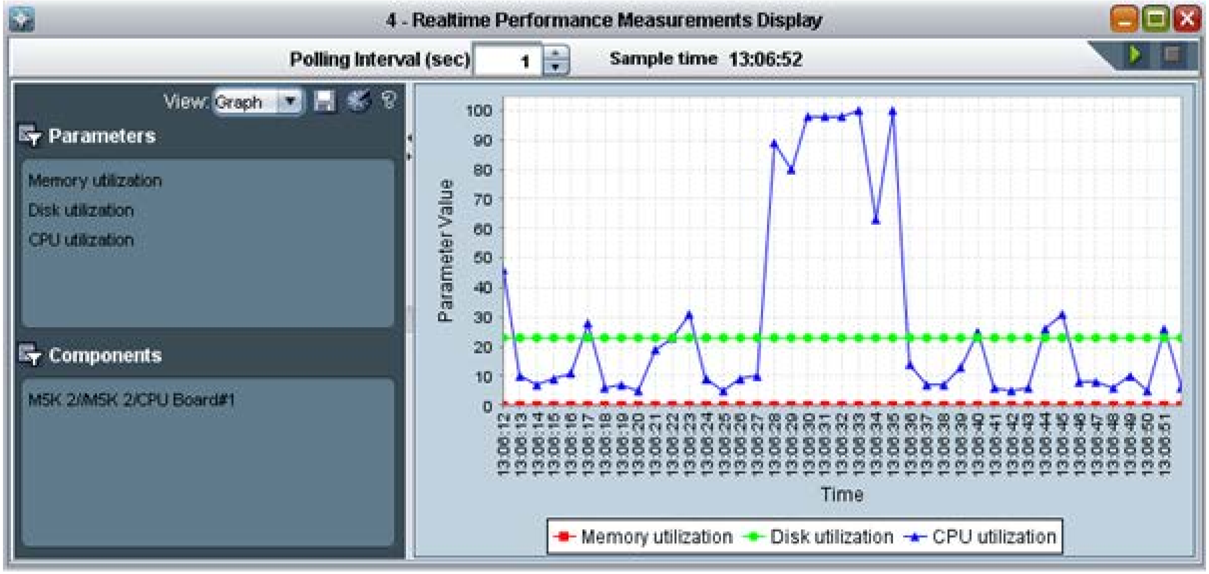
Number of Incoming Pkts ☑

Number of Incoming Discarded Pkts ☐

In the screen 'Real-Time Performance Measurements Display' (refer to the figures below), choose the type of view (Graph or Table). Choose the Polling Interval you require from the drop-down under the title bar and click the Start button ▶ to start polling; a real-time graph or table is displayed. You can pause the polling by clicking the pause button ⏸ and restart it again by clicking the Start button. To stop polling, click the Stop button ■. You can view a color legend (below the graph) for entities / parameters. You can choose to save the graph as an image by clicking the Save button in the left pane 💾. Historical data of the selected components and parameters can be viewed by clicking the 'History' button and then defining the History View. To view the Online Help, click the Help button ?.

In addition, you can apply Parameters or Components filters by clicking the filter button.

Figure 33-7: Graph Comparing CPU, Disk and Memory Utilization of SC Boards in Media Gateways



4 - Realtime Performance Measurements Display

Polling Interval (sec) 1

Sample time 13:06:52

View: Graph

Parameters

- Memory utilization
- Disk utilization
- CPU utilization

Components

- M5K 2/M5K 2/CPU Board#1

In the screen 'Real-Time Performance Measurements Display' (refer to the figures below), choose the 'Polling Interval you require from the drop-down under the title bar and click the Start button ▶ to start polling; a real-time graph is displayed. At the bottom of the graph you can view a color legend for entities / parameters.

➢ To add / remove parameters / entities from the real-time graph or to change the polling interval:

- Stop the current graph, perform the required configuration changes and then restart the polling.

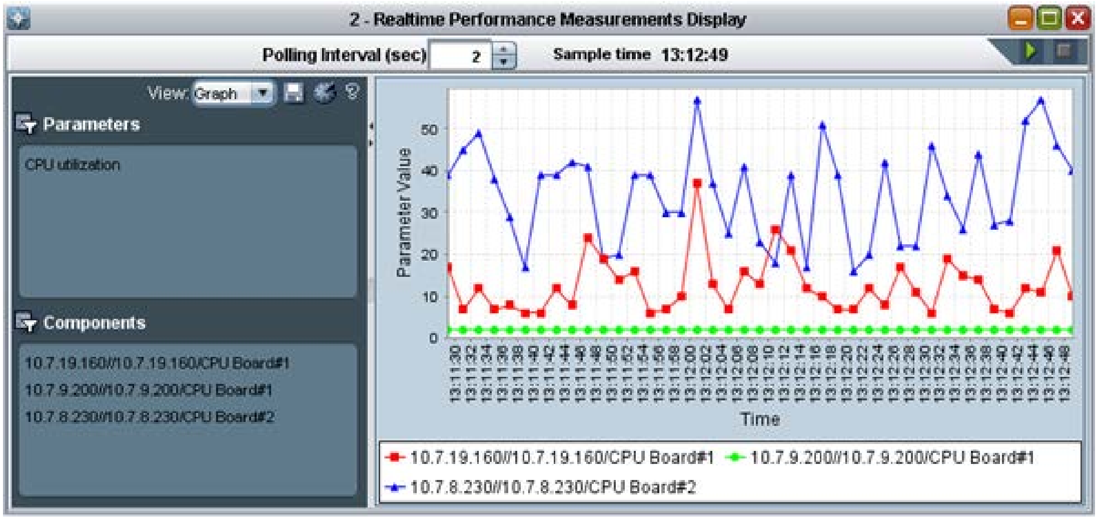
  At each stage, you can position your cursor over the nodes in the graph and view - in the tool tip - the precise information you require (the exact value of the parameter at the monitored point in time).

  The figures below show graphs depicting the following examples:

  Compare CPU utilization of System Controller boards in the Mediant 5000 and Mediant 8000 (refer to the figure below):

  - Compare CPU utilization of System Controller boards in the gateways.

Figure 33-8: Graph Comparing CPU Utilization of SC Boards in Media Gateways



2 - Realtime Performance Measurements Display

Polling Interval (sec) 2

Sample time 13:12:49

View: Graph

Parameters

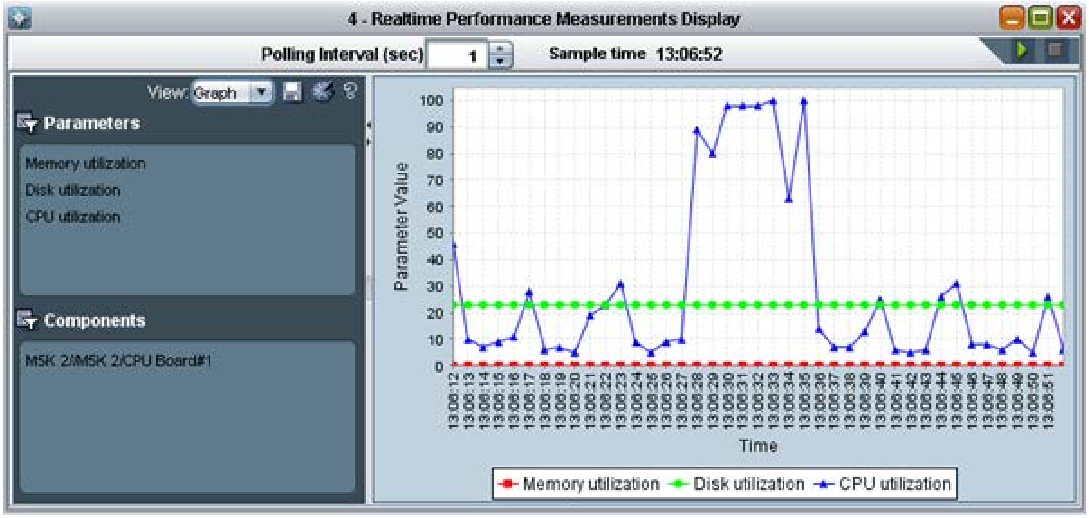
CPU utilization

Components

10.7.19.160//10.7.19.160/CPU Board#1
10.7.9.200//10.7.9.200/CPU Board#1
10.7.8.230//10.7.8.230/CPU Board#2

- View CPU, Memory and Disk utilization of the System Controller board #1 in the Mediant 5000 Media Gateway.

Figure 33-9: View CPU, Memory and Disk Utilization of Mediant 5000 SC Board 1



4 - Realtime Performance Measurements Display

Polling Interval (sec) 1

Sample time 13:06:52

View: Graph

Parameters

Memory utilization
Disk utilization
CPU utilization

Components

M5K 2//M5K 2/CPU Board#1

33.2 Background (History) Performance Monitoring

There are two main functions of the history data monitoring: Configure the EMS to collect the data and to view the collected data. Both options are available by clicking PM icon below.

This section describes the following:

- Defining Performance Monitoring Profiles

Notes: Before collecting History Performance measurements, you must define a PM profile. For more information, see 'Configuring Background Monitoring' on page 315 below.

- Exporting Background Monitoring Data as a file
- Viewing Historical Data

33.2.1 Configuring Background Monitoring

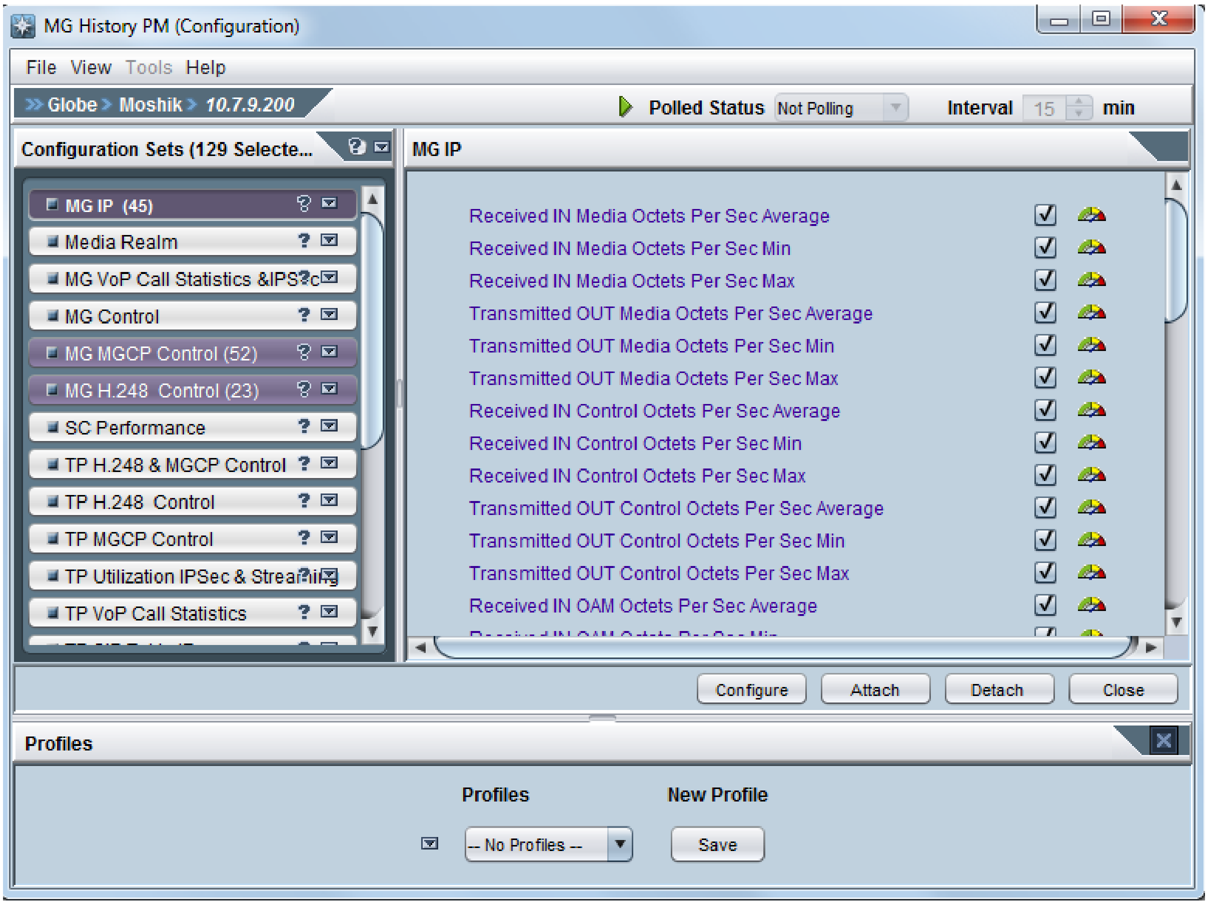
This section describes how to define a performance management profile. This procedure must be performed before you can view historical data.

➢ **To collect historical performance data:**

1. Select the relevant MO entity for which you wish to display Historical PMs. For example, select the media gateway board, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, click **History PM Configuration**.

   Note that each gateway and control protocol features a different set of available parameters. The figure below shows the gateway background monitoring provisioning parameters.

Figure 33-10: MG History PMs-Mediant 5000/Mediant 8000



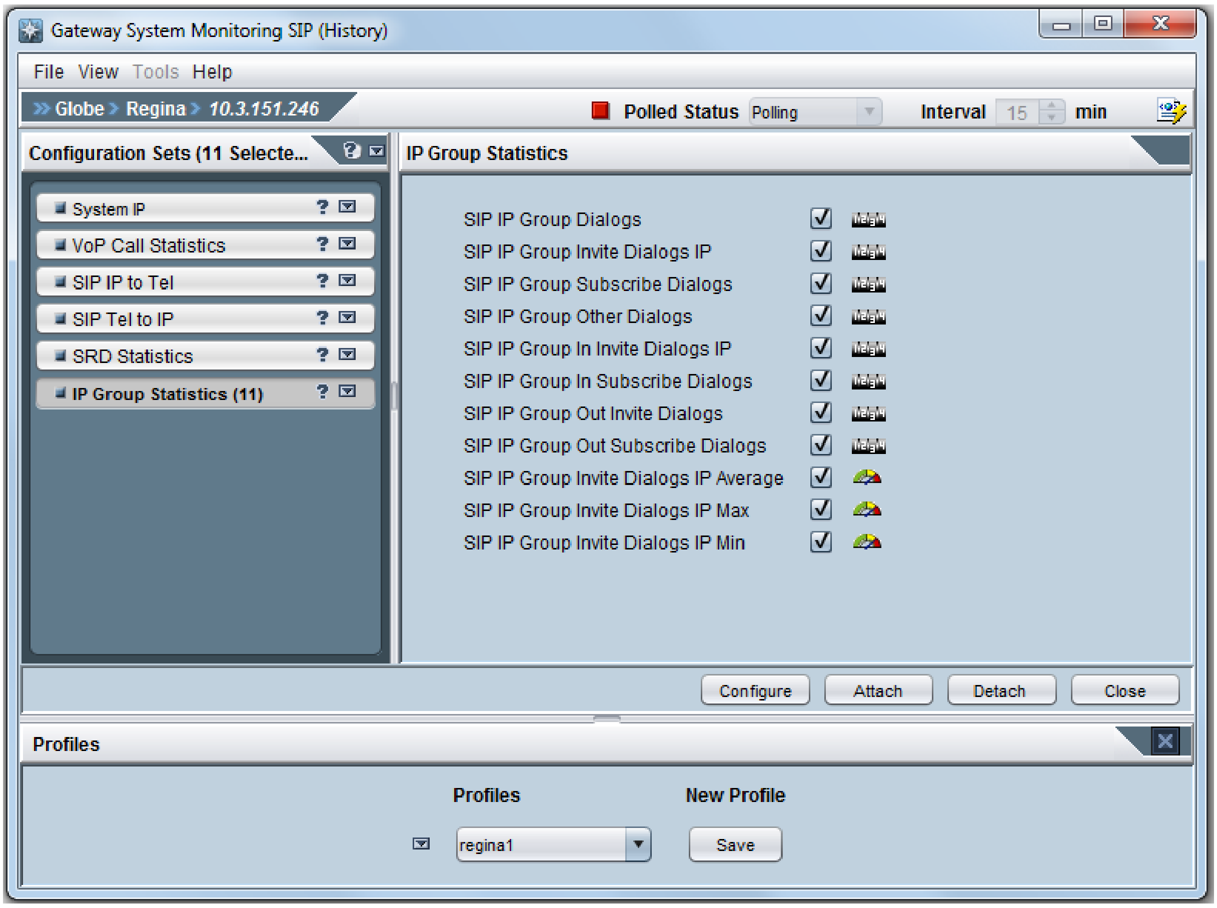
Polled Status: Not Polling
Interval: 15 min

Configuration Sets (129 Selecte...
- MG IP (45)
- Media Realm
- MG VoP Call Statistics &IPSec
- MG Control
- MG MGCP Control (52)
- MG H.248 Control (23)
- SC Performance
- TP H.248 & MGCP Control
- TP H.248 Control
- TP MGCP Control
- TP Utilization IPSec & Streaming
- TP VoP Call Statistics

MG IP
- Received IN Media Octets Per Sec Average ☑
- Received IN Media Octets Per Sec Min ☑
- Received IN Media Octets Per Sec Max ☑
- Transmitted OUT Media Octets Per Sec Average ☑
- Transmitted OUT Media Octets Per Sec Min ☑
- Transmitted OUT Media Octets Per Sec Max ☑
- Received IN Control Octets Per Sec Average ☑
- Received IN Control Octets Per Sec Min ☑
- Received IN Control Octets Per Sec Max ☑
- Transmitted OUT Control Octets Per Sec Average ☑
- Transmitted OUT Control Octets Per Sec Min ☑
- Transmitted OUT Control Octets Per Sec Max ☑
- Received IN OAM Octets Per Sec Average ☑

Profiles: -- No Profiles --
New Profile: Save

Figure 33-11: Gateway System Monitoring SIP (History)



SIP IP Group Dialogs ☑
SIP IP Group Invite Dialogs IP ☑
SIP IP Group Subscribe Dialogs ☑
SIP IP Group Other Dialogs ☑
SIP IP Group In Invite Dialogs IP ☑
SIP IP Group In Subscribe Dialogs ☑
SIP IP Group Out Invite Dialogs ☑
SIP IP Group Out Subscribe Dialogs ☑
SIP IP Group Invite Dialogs IP Average ☑
SIP IP Group Invite Dialogs IP Max ☑
SIP IP Group Invite Dialogs IP Min ☑

3. Select the parameters whose data you need to collect as part of background monitoring. Save these parameters as a PM profile or alternatively select a profile from the already available previously defined profiles.
4. Click the **Attach** button. Note that the parameters of all media gateway entities are polled. For example, trunk performance parameters are polled for all trunks of the selected media gateway. Note too that the same background configuration screen opens from every media gateway entity.
5. Select the Time Interval according to which to perform the polling (the default interval is 15 minutes) and click the polling state menu item **Start** option. Verify that the polling status has changed to **Polled**.
6. To change the polling interval or the PM profile, or to stop polling, click the **polling state** button.

33.2.2 Exporting Background Monitoring Data as a File

In addition to storing PM background monitoring data in the EMS server database, an *xml* or *csv* file can be created per time interval (starting from the Mediant 5000 Media Gateway and Mediant 8000 Media Gateway, versions 3.2).

The file is created at the end of the PM polling interval in accordance with a user-defined PM profile, and stored in the EMS server under directory 'Pmfiles'.

Users can choose whether or not to receive a trap when each file is created. The trap name is acEMSPmFileGenerate. The trap contains information as to the file name and the time it was created.

File name - the file name contains the gateway name in the EMS, the gateway's IP address and the time stamp of the performance data collection.

File location – performance monitoring files are located in the EMS Server machine at the following location:

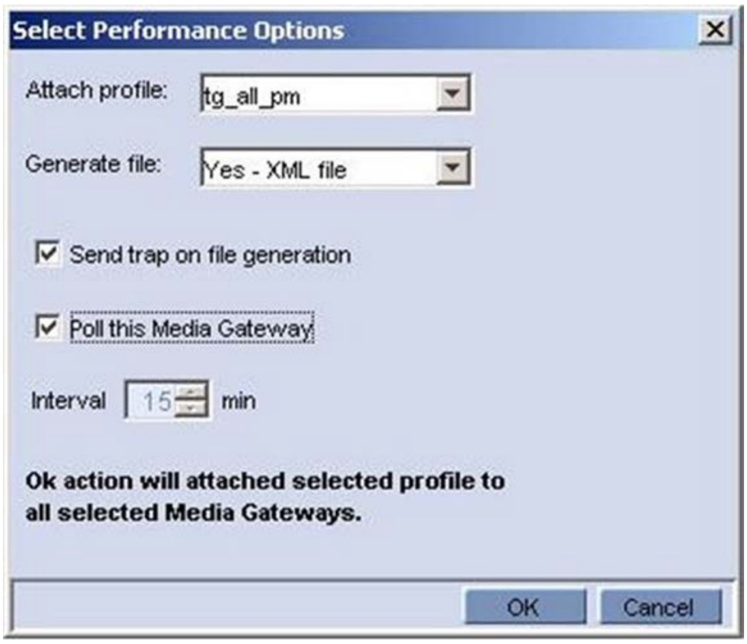
```
ACEMS/NBIF/pmFiles
```

Users should forward the trap to the NMS (Network Management System) (see Section 'Trap Forwarding to NB IF' on page 294).

➢ To enable a file to be created:

1. Select the option **Configure PM Profile** in the 'Performance Monitoring' menu.
2. Click the button '**Configure'**.
3. Continue (if needs be) to select a profile.
4. Select the file type – *csv* or *xml.*
5. Select the checkbox **Send trap on file generation** to receive a trap when each file is created.
6. Select **Poll this Media Gateway.**

Figure 33-12: Background Monitoring - Generate File Options



Select Performance Options

Attach profile: tg_all_pm

Generate file: Yes - XML file

☑ Send trap on file generation

☑ Poll this Media Gateway

Interval 15 min

Ok action will attached selected profile to all selected Media Gateways.

> **Notes:** A performance data file cannot be created unless the media gateway is polled (see section 'Configuring Background Monitoring' on page 315.

- The PM file icon is displayed in the 'Configure PM Profile' frame tool bar:

  xml file

  xml file with trap generation after creation

  csv file

  csv file with trap generation after creation

- Retrieve the PM file from the FTP server with the NMS / OSS system. In the event of EMS server machine hardening, use a secure FTP.
- The EMS keeps PM files for 24 hours (up to 96 files per gateway).

An unknown value can be received from the gateway if the TP board is locked or for some other reason information is not received from the TP board.

For exact CSV and XML files format, refer to the *OAM Integration Guide*.

33.2.3 Viewing Historical Data

This section describes how to view historical data.

➢ **To view collected (historical) data:**

1. Select the relevant MO entity for which you wish to display Historical PMs. For example, select the media gateway board, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, select **History PM Display**.
3. Continue (if required) to select entities to be added to the same screen. All entities must be of the same type (trunks, or System Controller boards, or gateways of the same control protocol type). After all entities are selected, select the parameter to view by clicking the **Parameters Filter** button; only parameters available for that entity type are displayed for selection. Note that you can select up to 15 parameters. Note that the number of entities you can select is unlimited.
4. Select the Time Interval according to which you need to review data and click **Refresh**; after data is displayed, you can save it as a *csv* file by clicking the **Save** icon.

   Historical data comprises two tables: The uppermost table displaying detailed data (in user-defined intervals) and the table below it displaying summarized data.

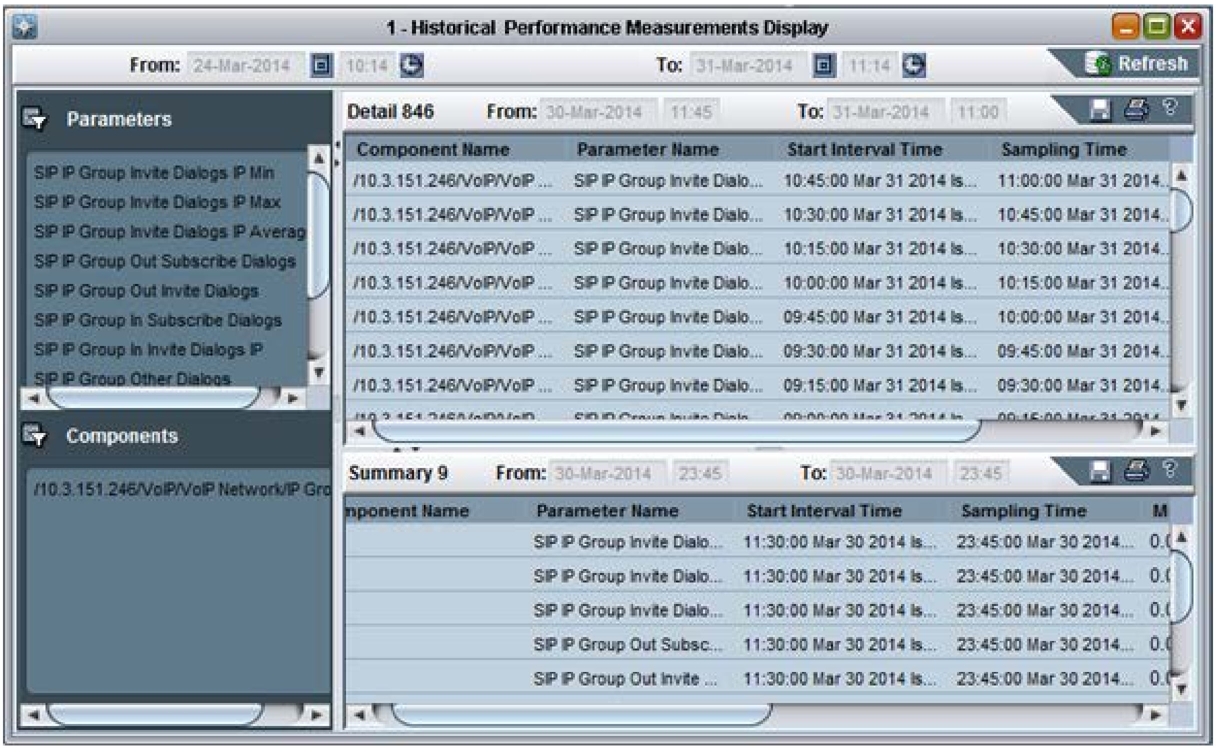
   Each time a sample is taken from the gateway, it is stored in the detailed table, where the entity name and index, parameter name, start, stop polling time and parameter value are specified.

   After every 24 hours of sampled data, the detailed table is summarized. For each entity and parameter, the following data is collected:

   - **Start Interval Time**-The time when the polling was started.
   - **Samling Time**-The time at the end of the sampling period
   - **Min Value**, **Avg Value** and **Max Value**-The minium, average and maximum sampling values respectively collected during the sampling period
   - **Min Value Time** and **Max Value Time**-The respective times when the minimum value and the maximum values were recorded during the sampling period. For example, if the Start Interval Time was 14:15:00 and the Sampling Time was 14:30:00, the Min. Value Time occurred at 14:25:00 and the Max. Value Time occurred at 14:28:00.

Detailed data is stored for a period of 7 days (in intervals of 15 minutes). Summary data is stored for 30 days (in intervals of 24 hours). Data storage time is dependent on available disk space.

Figure 33-13: Performance Monitoring - Historical Data



1 - Historical Performance Measurements Display

From: 24-Mar-2014 10:14 To: 31-Mar-2014 11:14 Refresh

Parameters

- SIP IP Group Invite Dialogs IP Min
- SIP IP Group Invite Dialogs IP Max
- SIP IP Group Invite Dialogs IP Averag
- SIP IP Group Out Subscribe Dialogs
- SIP IP Group Out Invite Dialogs
- SIP IP Group In Subscribe Dialogs
- SIP IP Group In Invite Dialogs IP
- SIP IP Group Other Dialogs

Components

- /10.3.151.246/VoIP/VoIP Network/IP Gro

Detail 846 From: 30-Mar-2014 11:45 To: 31-Mar-2014 11:00

Component Name	Parameter Name	Start Interval Time	Sampling Time
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:45:00 Mar 31 2014 Is...	11:00:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:30:00 Mar 31 2014 Is...	10:45:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:15:00 Mar 31 2014 Is...	10:30:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:00:00 Mar 31 2014 Is...	10:15:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:45:00 Mar 31 2014 Is...	10:00:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:30:00 Mar 31 2014 Is...	09:45:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:15:00 Mar 31 2014 Is...	09:30:00 Mar 31 2014...

Summary 9 From: 30-Mar-2014 23:45 To: 30-Mar-2014 23:45

nponent Name	Parameter Name	Start Interval Time	Sampling Time	M
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Out Subsc...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Out Invite ...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(

It's possible to save selected data by clicking **Save** button 💾 on the right size of the History Data display. Data is saved in .csv file format.

33.2.4 Prinitng Historical Data PM Reports

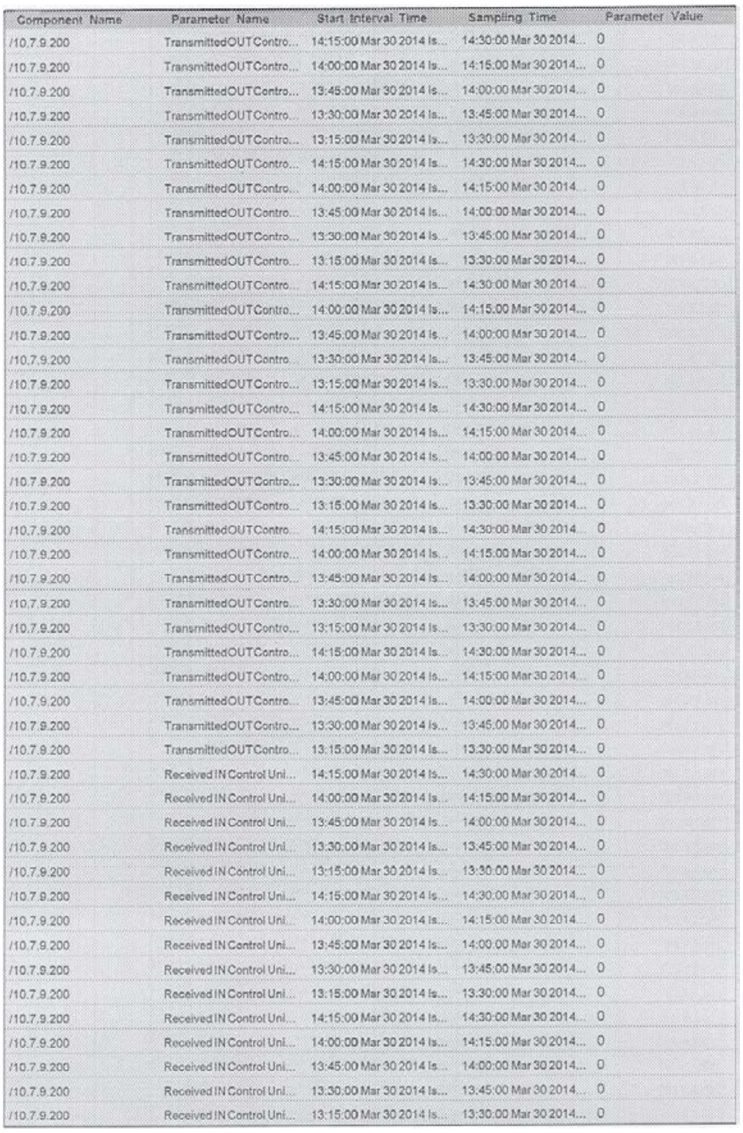
Once you view the sample polled data, you can also print the displayed data by clicking the **Print** icon.

➢ To print historical data PM reports:

- In the Historical Performance Measurements Display, click the **Print** icon 🖶; the Print dialog is displayed.

  An example of the printed output is displayed below:

Figure 33-14: Historical Data PM Report



Component Name	Parameter Name	Start Interval Time	Sampling Time	Parameter Value
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControlUni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0

33.3 Performance Monitoring Threshold Alarm

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

The user can define High and Low threshold for any history PMs; an alarm is generated when the predefined High Threshold value is exceeded. The alarm is cleared when the PMs value passes below the predefined Low Threshold value.

For example: once 'Lifetime in Seconds (Max)' has exceeded the user defined **Lifetime High Threshold**, a Threshold exceed alarm is generated.

33.3.1 Configuring Performance Monitoring Threshold Values for CPE Products

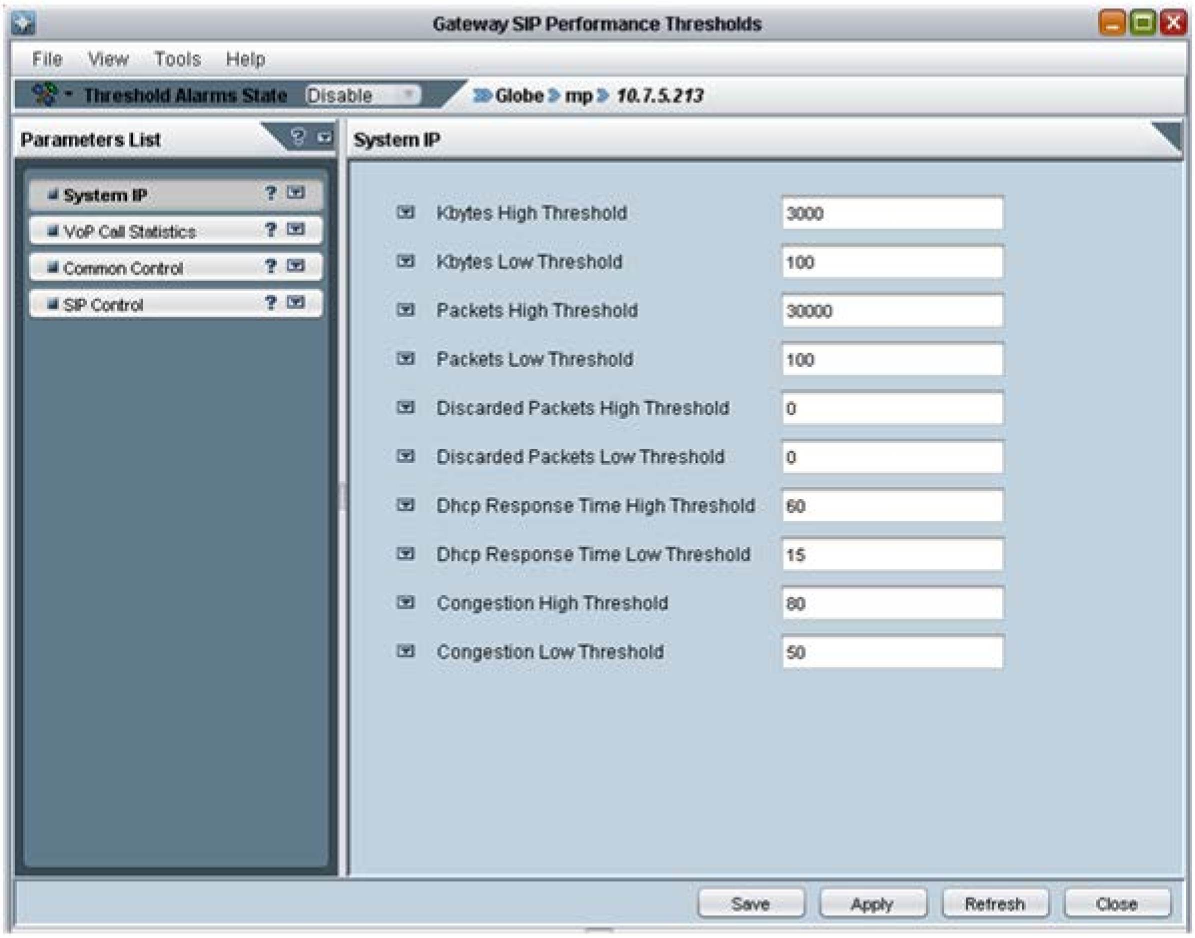
This section describes how to configure performance monitoring thresholds for CPE Products.

➢ **To provision the gateway to issue a Threshold Crossing Alarm:**

1. Select the Media Gateway for which you wish to display Historical PMs, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, click **Threshold Configuration**; the Gateway Performance Thresholds provisioning screen opens.

   The provisioning screen differs between gateway types and control protocols. The following screen displays an example of the MediaPack Performance Monitoring screen.

Figure 33-15: MediaPack Performance Thresholds



Threshold Alarms State: Disable

System IP

Kbytes High Threshold	3000
Kbytes Low Threshold	100
Packets High Threshold	30000
Packets Low Threshold	100
Discarded Packets High Threshold	0
Discarded Packets Low Threshold	0
Dhcp Response Time High Threshold	60
Dhcp Response Time Low Threshold	15
Congestion High Threshold	80
Congestion Low Threshold	50

3. To provision the required threshold parameters, click **Apply**.

   If the 'Threshold Alarms State' parameter is Disabled, select the **Enable** option from the drop-down menu adjacent to the Maintenance icon.

   The gateway sends a Threshold Cross Alarm when a pre-defined threshold is crossed and a corresponding clear alarm when the measured value returns to normal.

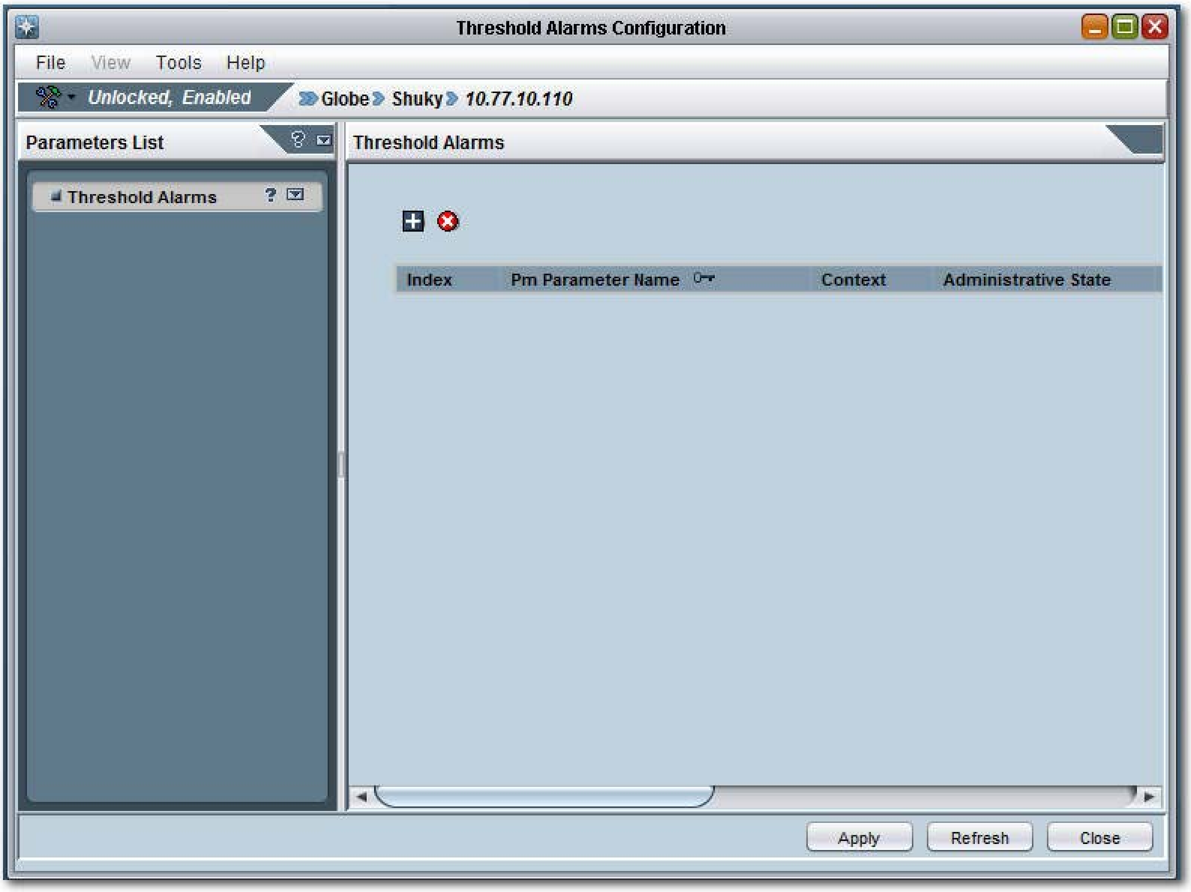
33.3.2 Configuring Performance Monitoring Threshold Values for Mediant 5000 / Mediant 8000 Media Gateways.

The feature is applicable for History PMs only, for both Counters and G auge PM types. Up to 100 entries can be configured in the PM thresholds table.

➢ **To provision the gateway to issue a Threshold Crossing Alarm:**

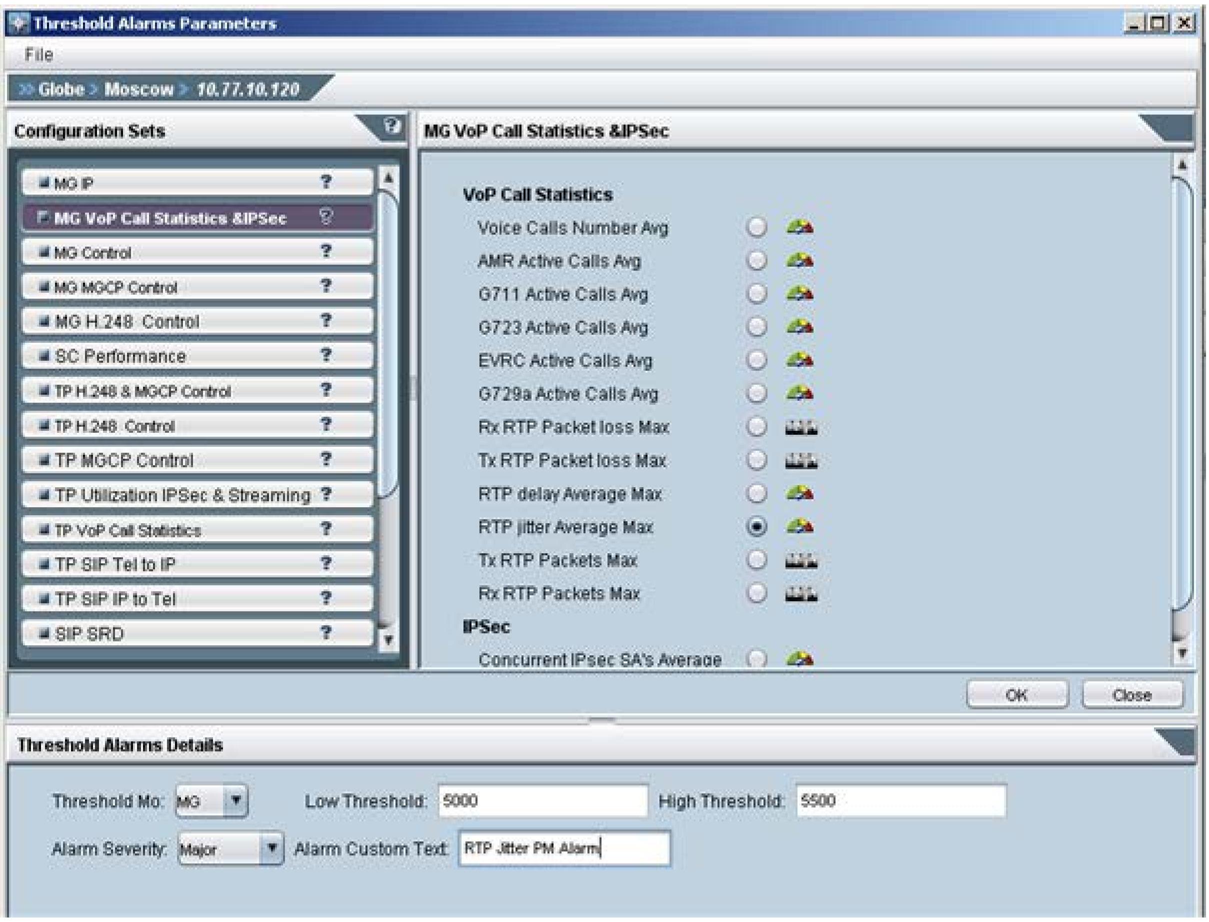
1. Select the relevant MO entity for which you wish to display Historical PMs. For example, select the media gateway board, and then in the Desktop toolbar, click **Performance**.
2. Click **Threshold Alarms** in the Performance pane; the Threshold Alarms Configuration frame is displayed.

Figure 33-16: Threshold Alarms Configuration Frame



3. Click the ➕ button to define a new threshold; the Threshold Alarm Parameters Frame is displayed.
4. Select one parameter at a time. Repeat this process as desired until the maximal threshold table size (100) is reached. For each parameter, in the Threshold Alarms Details pane, the user can define alarm severity, alarm customized text, and the low and high thresholds. For Board level parameters, it's possible to define threshold per board with different parameters.

Figure 33-17: Threshold Alarms Parameters-MG VoP Statistics and IPSec



VoP Call Statistics

- ○ Voice Calls Number Avg
- ○ AMR Active Calls Avg
- ○ G711 Active Calls Avg
- ○ G723 Active Calls Avg
- ○ EVRC Active Calls Avg
- ○ G729a Active Calls Avg
- ○ Rx RTP Packet loss Max
- ○ Tx RTP Packet loss Max
- ○ RTP delay Average Max
- ● RTP jitter Average Max
- ○ Tx RTP Packets Max
- ○ Rx RTP Packets Max

IPSec

- ○ Concurrent IPsec SA's Average

Threshold Mo: MG

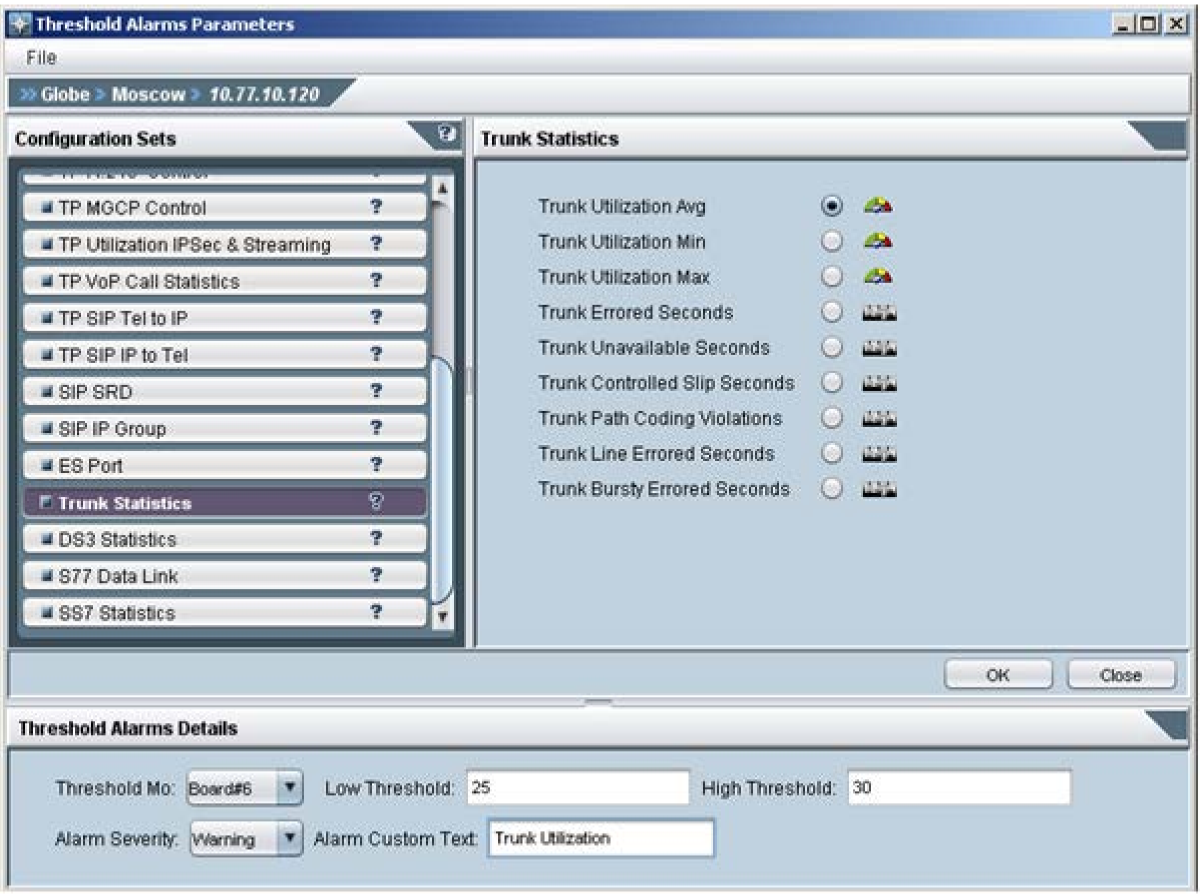
Low Threshold: 5000

High Threshold: 5500

Alarm Severity: Major

Alarm Custom Text: RTP Jitter PM Alarm

Figure 33-18: Threshold Alarms Parameters-Trunk Statistics



Trunk Statistics

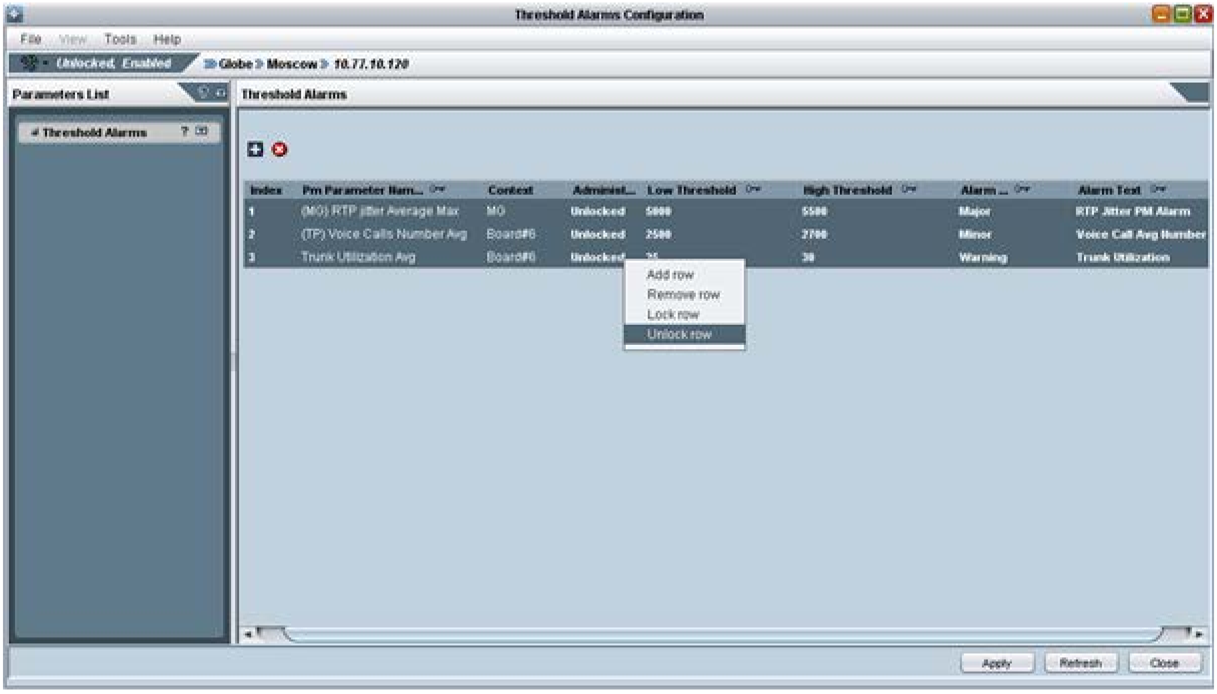
- Trunk Utilization Avg ●
- Trunk Utilization Min ○
- Trunk Utilization Max ○
- Trunk Errored Seconds ○
- Trunk Unavailable Seconds ○
- Trunk Controlled Slip Seconds ○
- Trunk Path Coding Violations ○
- Trunk Line Errored Seconds ○
- Trunk Bursty Errored Seconds ○

Threshold Mo: Board#6 Low Threshold: 25 High Threshold: 30

Alarm Severity: Warning Alarm Custom Text: Trunk Utilization

5. When all the required thresholds are defined, the user should perform **Unlock** to unlock all the rows in the Thresholds table. Once all the entries are Unlocked, the Gateway starts to collect measurements.

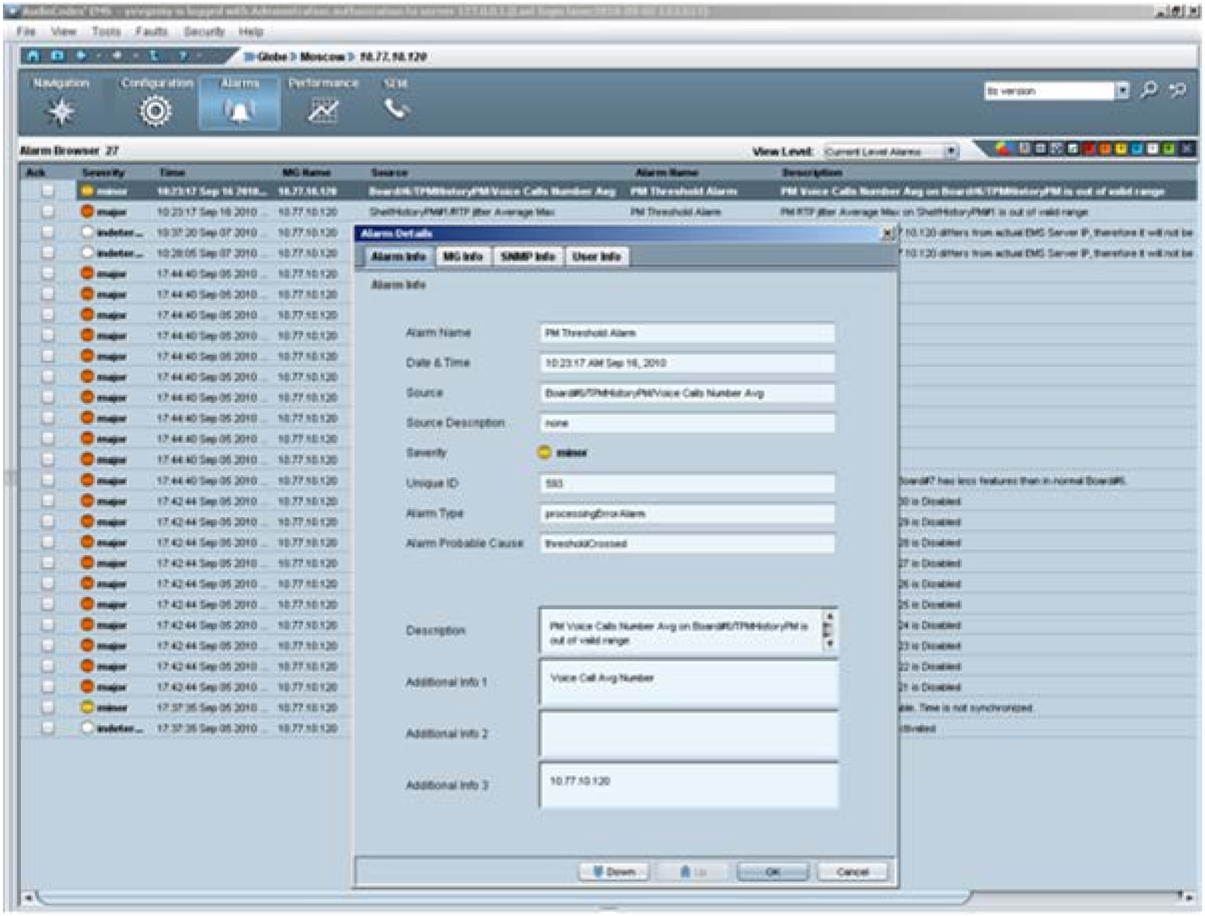
Figure 33-19: Threshold Alarms Configuration



Index	Pm Parameter Nam...	Context	Administ...	Low Threshold	High Threshold	Alarm ...	Alarm Text
1	(MG) RTP jitter Average Max	MG	Unlocked	5000	5500	Major	RTP Jitter PM Alarm
2	(TP) Voice Calls Number Avg	Board#6	Unlocked	2500	2700	Minor	Voice Call Avg Number
3	Trunk Utilization Avg	Board#6	Unlocked	25	30	Warning	Trunk Utilization

6. When the threshold value is crossed, the gateway generates a Threshold alarm with all the required information. See the example below.

Figure 33-20: Threshold Alarm Details



Alarm Details

Alarm Info | MG Info | SNMP Info | User Info

Alarm Info

Alarm Name: PM Threshold Alarm

Date & Time: 10:23:17 AM Sep 16, 2010

Source: Board#6/TPMHistoryPM/Voice Calls Number Avg

Source Description: none

Severity: minor

Unique ID: 593

Alarm Type: processingErrorAlarm

Alarm Probable Cause: thresholdCrossed

Description: PM Voice Calls Number Avg on Board#6/TPMHistoryPM is out of valid range

Additional Info 1: Voice Call Avg Number

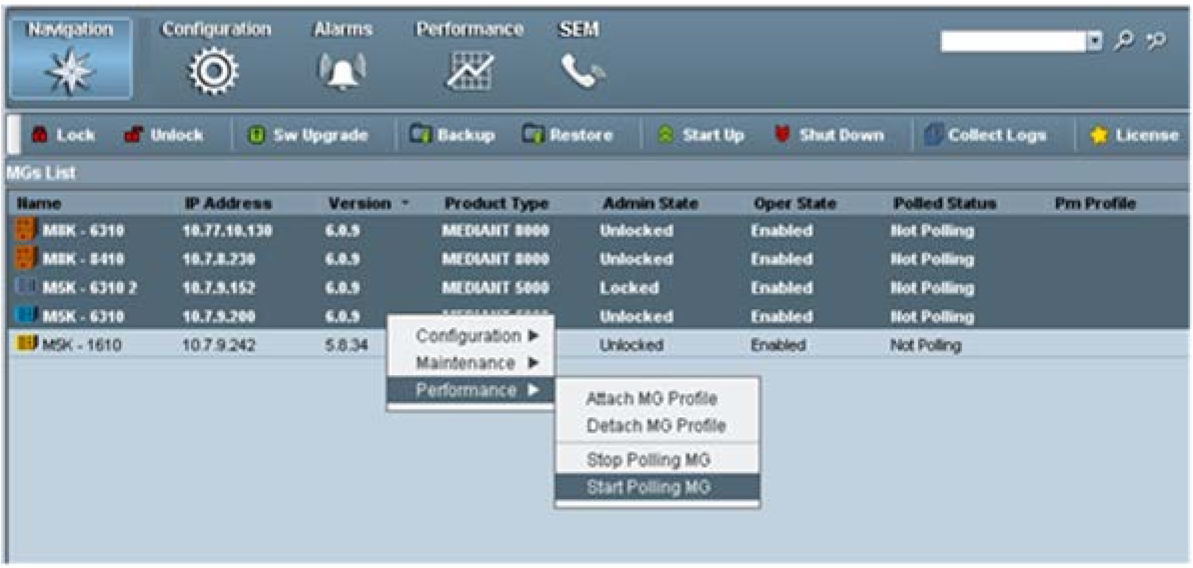
Additional Info 2:

Additional Info 3: 10.77.10.120

33.4 Performance Monitoring Actions on Multiple Media Gateways

This section describes performance monitoring actions on multiple media gateways.

Figure 33-21: Performance Monitoring Actions on Multiple Media Gateways



Name	IP Address	Version	Product Type	Admin State	Oper State	Polled Status	Pm Profile
M8K - 6310	10.77.10.130	6.0.9	MEDIANT 8000	Unlocked	Enabled	Not Polling	
M8K - 8410	10.7.8.230	6.0.9	MEDIANT 8000	Unlocked	Enabled	Not Polling	
M5K - 6310 2	10.7.9.152	6.0.9	MEDIANT 5000	Locked	Enabled	Not Polling	
M5K - 6310	10.7.9.200	6.0.9	MEDIANT 5000	Unlocked	Enabled	Not Polling	
M5K - 1610	10.7.9.242	5.8.34		Unlocked	Enabled	Not Polling	

Users can perform following actions on multiple gateways:

- Attach / Detach Profile
- Start / Stop Polling

Notes: For 'Display Real-Time and Historical PMs' and for 'Attach / Detach Profile', all the gateways you select must be of the same type, for example, either MediaPacks, or Mediant 2000 Media Gateways, or Mediant 5000 Media Gateways.

Reader's Notes

Part V

Security Management

This section describes the security features implemented on the EMS.

34 Overview

EMS Security Management features:

- Network Communication Security (see Section 'Network Communication Security' on page 334).
- EMS Application Security
- Local EMS Users Authentication and Authorization
- Centralized EMS Users Authentication and Authorization via Radius Server
- EMS User Activities Journal
- EMS Server Machine (including UNIX and Oracle related items) (refer to the *EMS Server IO&M Manual*):
- Oracle Database Hardening and recent security patch installation.
- File Integrity Checking - The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported via EMS Security Events.
- Intrusion Detection System - The Intrusion Detection tool scans predefined 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.

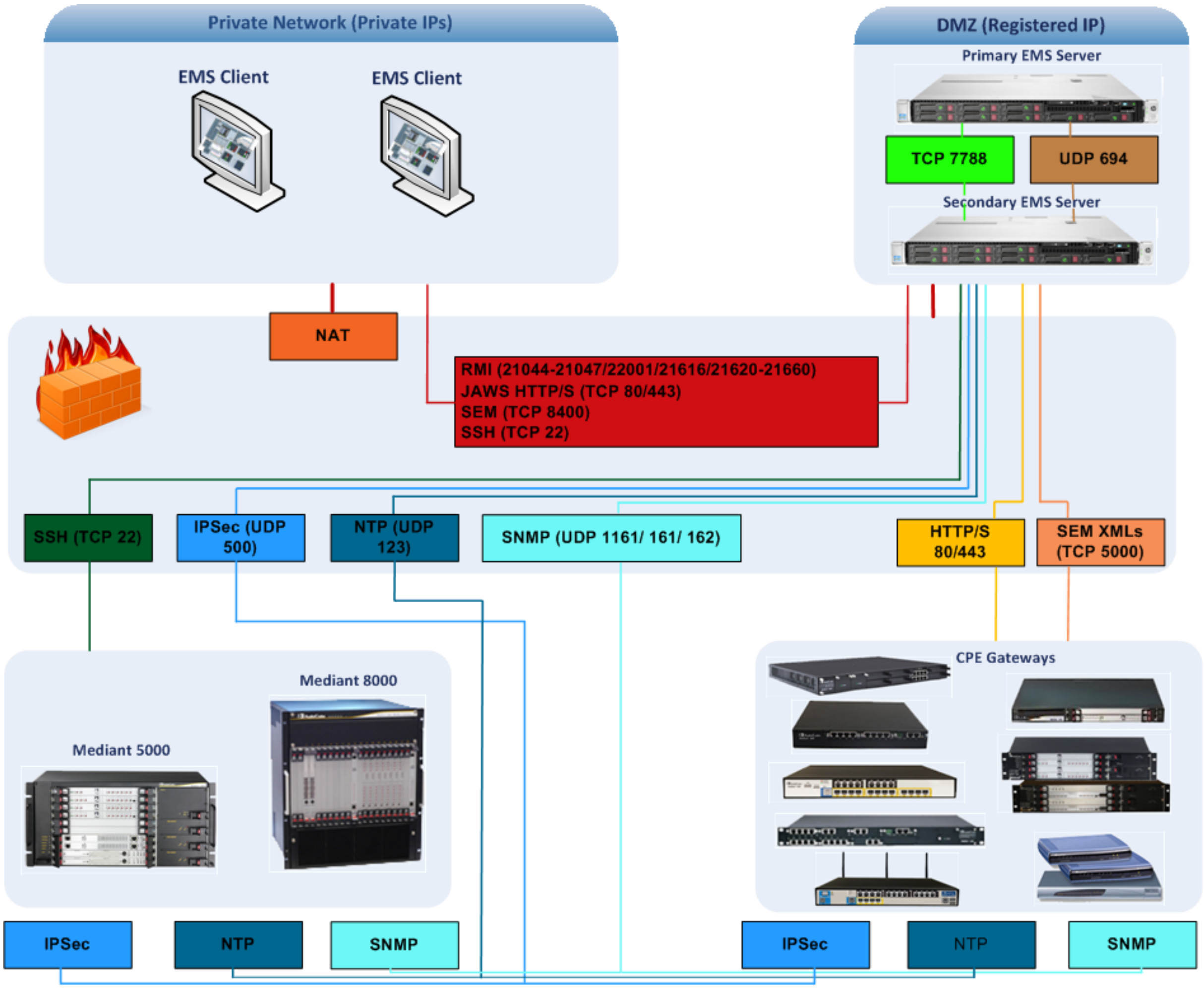
Reader's Notes

35 Network Communication Security

When installing the EMS server, you need to configure its network and open the ports required for the EMS client-server and the EMS server-media gateway communication. For more information, refer to the *EMS Server Installation and Maintenance Manual.*

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 the EMS client, server and managed media gateways (see the figure below).

Figure 35-1: EMS Firewall Configuration Schema



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).

EMS server communications with the media gateways is performed over the protocols described in the subsections below.

35.1 SNMP Management

The SNMP protocol is used for provisioning, maintenance actions, fault and performance management between the EMS Manager and i ts agents (AudioCodes media gateways).

The SNMPv3 protocol provides more sophisticated security mechanisms than SNMPv2c. It implements a user-based security model (USM), allowing both authentication and encryption of the requests sent between the EMS Manager and their agents, as well as user-based access control.

35.2 Mediant 5000 and Mediant 8000 Security Management

EMS <-> media gateway communication is performed using SNMP, Telnet and FTP protocols, which can be secured in the following ways:

- SNMP: use SNMPv3 instead of SNMPv2c.
- Telnet & FTP: use SSH and SCP. Telnet and FTP are used for installation and upgrading software. By default EMS runs this connectivity in the secure mode using SSH and SCP. In addition, SSH and SCP communications can be secured by running them over IPsec protocol.
- Overall communication: SNMPv2c, Telnet & FTP over IPsec.

➢ **To configure EMS-gateway secure communication:**

1. Right-click the media gateway you wish to provision in the MG Tree and choose **Details**; the MG Information screen opens (see the figure below).
2. Choose to work with either SNMPv2c or SNMPv3:

   For SNMPv2c, do the following:

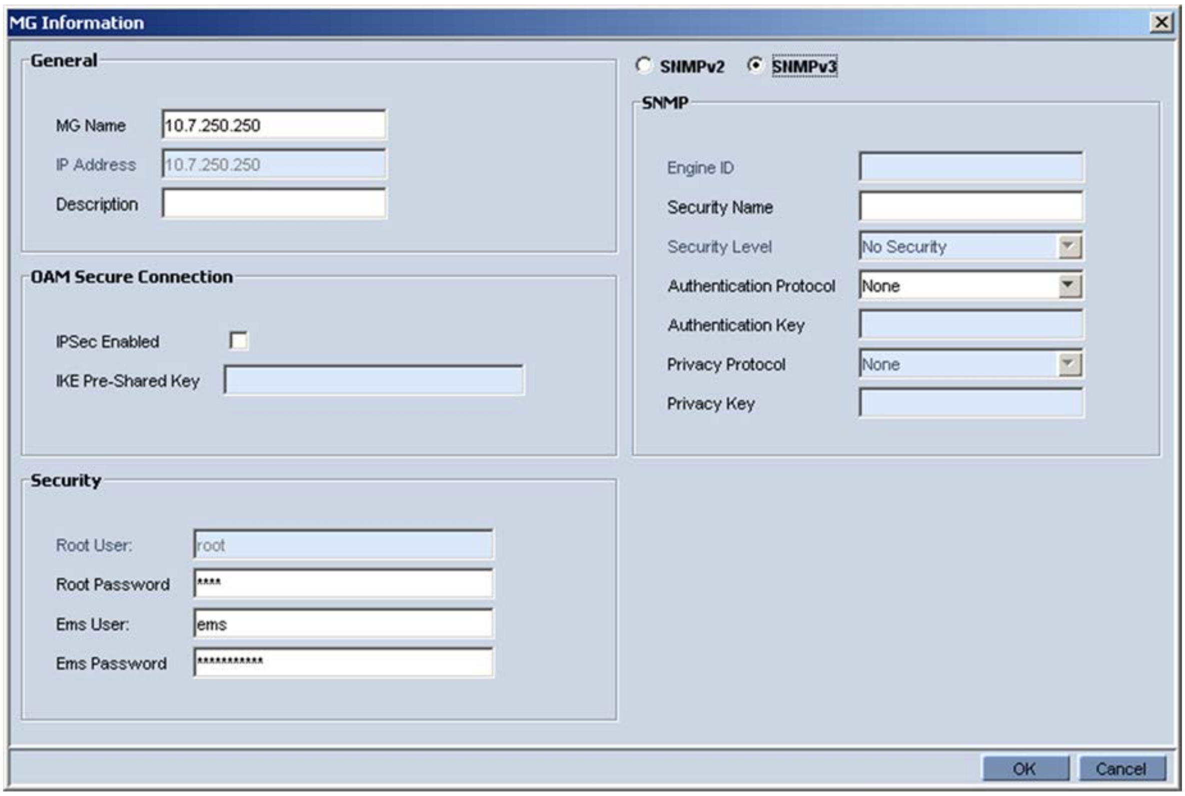
   - It is recommended to select the **IPSec Enabled** checkbox and enter the 'Pre-shared Key' string. This configuration can be performed either during the gateway definition stage or later. The Pre-shared Key string defined in the EMS and in the media gateway must be identical.

   For SNMPv3, do the following:

   - It is recommended to select the **IPSec Enabled** checkbox and enter the 'Pre-shared Key' string. This configuration can be performed either during the gateway definition stage or later. The Pre-shared Key string defined in the EMS and in the media gateway must be identical.
   - In the 'Security Name' field, enter the Security name of the SNMPv3 user.
   - In the 'Authentication Protocol' field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the 'Security Level' field;

- In the 'New Authentication Password' field, enter a new Authentication Password; In the 'Privacy Protocol' field, select a Privacy Protocol from the drop-down list box;
- In the 'New Privacy Password' field, enter a new Privacy Password.

Figure 35-2: MG Information - Secured Connection Enabled



MG Information

General

MG Name: 10.7.250.250

IP Address: 10.7.250.250

Description:

OAM Secure Connection

IPSec Enabled: □

IKE Pre-Shared Key:

Security

Root User: root

Root Password: ****

Ems User: ems

Ems Password: ***********

○ SNMPv2 ● SNMPv3

SNMP

Engine ID:

Security Name:

Security Level: No Security

Authentication Protocol: None

Authentication Key:

Privacy Protocol: None

Privacy Key:

35.3 CPE Security Management

- EMS < > MG communication is performed using SNMP and HTTP protocols, which can be secured in the following way:
  - SNMP: use SNMPv3 instead of SNMPv2c. SNMP is used for provisioning, maintenance actions and fault and performance management.
  - HTTP: use HTTPS instead of HTTP. HTTP is used for installation and upgrading software, and for downloading auxiliary files.
  - Overall communication: SNMP & HTTP over IPsec.

35.3.1 Configuring SNMP

This section describes the SNMP Security Management features for CPE Gateways.

➢ **To configure MG and EMS to work over SNMPv3:**

1. Right-click the media gateway you wish to provision in the MG Tree and choose **Details**; the MG Information screen opens (see the figure below).
2. In the 'Security Name' field, enter the Security name of the SNMPv3 user.
3. In the 'Authentication Protocol' field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the Security Level field.
4. In the 'New Authentication Password' field, enter a new Authentication Password; In the Privacy Protocol field, select a Privacy Protocol from the drop-down list box;
5. In the 'New Privacy Password' field, enter a new Privacy Password.

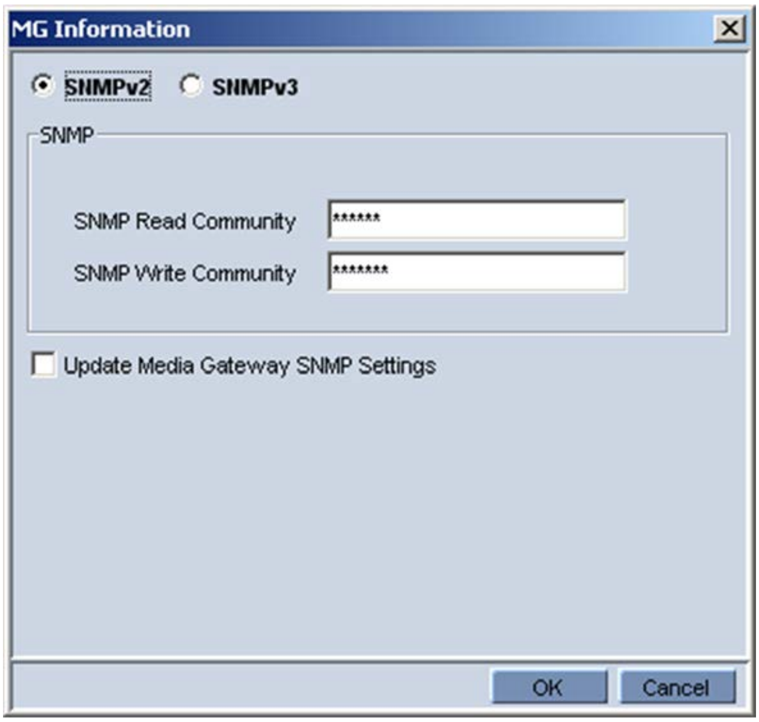
➢ **To switch MG & EMS communication from one SNMP version to another via EMS:**

1. In the Region Status screen, select one or more CPEs (multiple selections are relevant when all the gateways are updated to the same community strings / passwords).
2. Right-click **Configuration** ▶ **SNMP Configuration** option. The MG Information screen is displayed.
3. To switch from a SNMPv2 user to a SNMP v3 user, click the SNMPv3 button and enter the required SNMPv3 fields as described above.
4. To switch from an SNMP v3 user to a SNMP v2 user, click the SNMPv2 button and fill in the SNMP community strings.
5. Select the **Update Media Gateway SNMP Settings** checkbox.

   EMS updates the EMS database and the media gateway. If you do not check this option, any changes performed in the MG Information screen are only updated to the EMS database.

Note: When you switch from a SNMPv2 to a SNMPv3 user and select the **Update Media Gateway SNMP Settings** checkbox, the EMS logs into the media gateway using the SNMPv2 user privileges. SNMPv3 user privileges are used the next time you connect to the media gateway. Sometimes this operation might take up to 3 minutes.

Figure 35-3: MG Information-New SNMPv3 User



● SNMPv2 ○ SNMPv3

SNMP Read Community: ******

SNMP Write Community: *******

□ Update Media Gateway SNMP Settings

➢ To Modify SNMPv2 community strings or SNMP v3 User Passwords in MG & EMS via EMS:

1. From the Region Status screen, select CPE/s (multiple selections are relevant when all the gateways are updated to the same community strings / passwords). Right-click **Configuration** ► **SNMP Configuration** option.
2. Update SNMPv2 community strings / or SNMPv3 Users passwords.
3. Select the Update SNMP Settings in media gateway checkbox.

35.3.2 Defining (Cloning) SNMPv3 Users

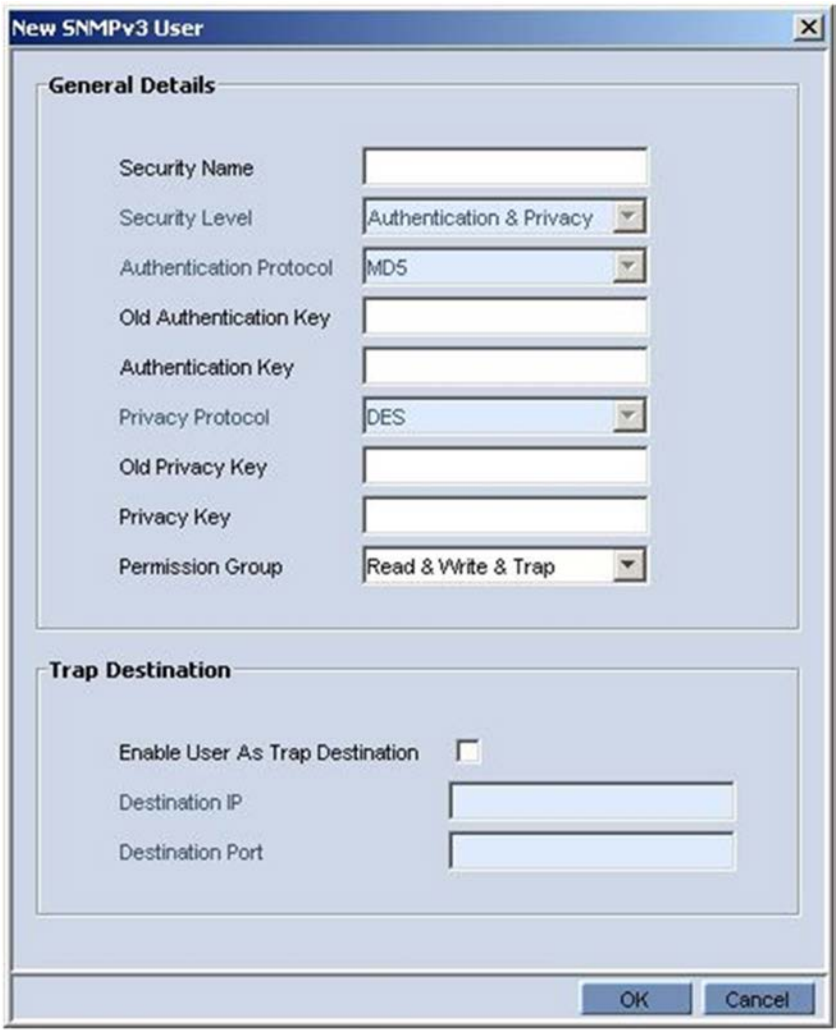
According to the SNMPv3 standard, SNMPv3 users on the SNMP Agent (on the media gateway) cannot be directly added via the SNMP protocol e.g. SNMP Manager (EMS). Instead new users must be def ined via User Cloning. The SNMP Manager then creates a new user according to the original user permission levels.

➢ **To clone SNMPv3 Users:**

1. In the Desktop toolbar, click **Configuration** and in the Configuration pane, click **Network Frame**; The Network Parameters Provisioning screen is displayed.
2. Select the **SNMPv3 Users** tab and select the user you wish to clone permission levels.
3. Click **+** button; the New SNMPv3 User window is opened.
4. Provide a new user name, old passwords of the user you clone permissions from and new user passwords.
5. Select a User permission group.
6. If the new user wishes to receive traps to the predefined destination, check the **Enable User as Trap Destination** option to provision Trap destination IP and Port. EMS adds this new user to the SNMP Trap Managers Table. It is also possible to define an additional trap destination after a new user is defined.

The new user is added to the SNMPv3 Users table.

Figure 35-4: MG Information Screen-New SNMPv3 User



New SNMPv3 User

General Details

Security Name

Security Level: Authentication & Privacy

Authentication Protocol: MD5

Old Authentication Key

Authentication Key

Privacy Protocol: DES

Old Privacy Key

Privacy Key

Permission Group: Read & Write & Trap

Trap Destination

Enable User As Trap Destination □

Destination IP

Destination Port

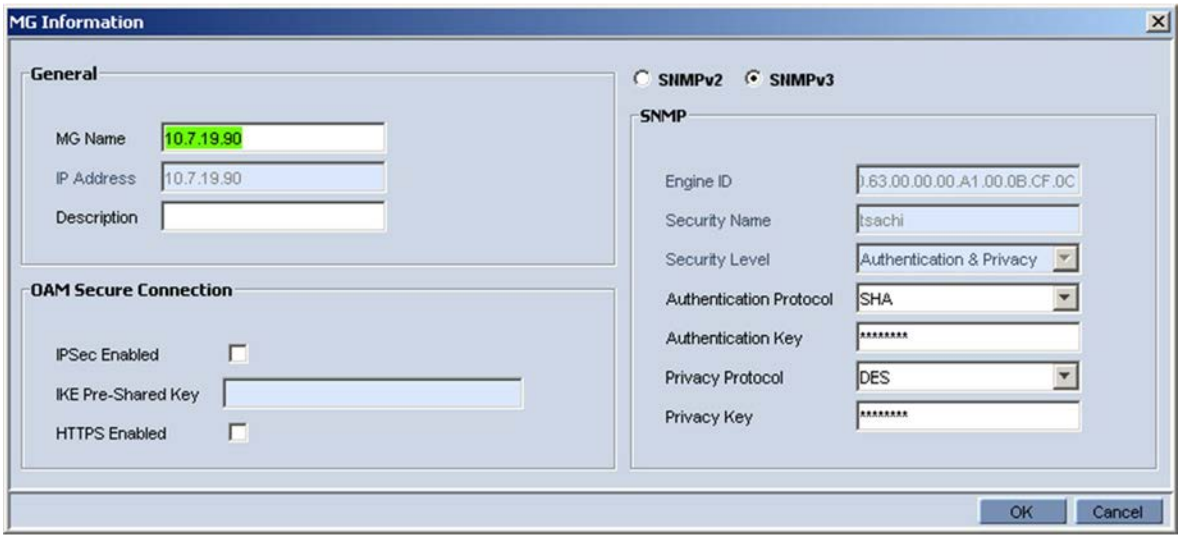
35.3.3 Configuring HTTPS

This section describes how to configure the media gateway and the EMS to communicate via the HTTPS protocol.

➢ To configure MG & EMS to work over HTTPS:

1. Right-click the media gateway you wish to provision in the MG Tree and choose **Details**; the MG Information screen opens (see the figure below).

Figure 35-5: Securing Communication



MG Information

General

MG Name: 10.7.19.90

IP Address: 10.7.19.90

Description:

OAM Secure Connection

IPSec Enabled ☐

IKE Pre-Shared Key:

HTTPS Enabled ☐

○ SNMPv2 ● SNMPv3

SNMP

Engine ID:).63.00.00.00.A1.00.0B.CF.0C

Security Name: tsachi

Security Level: Authentication & Privacy

Authentication Protocol: SHA

Authentication Key: ********

Privacy Protocol: DES

Privacy Key: ********

2. Select the 'HTTPS Enabled' check box.

35.3.4 Configuring Media Gateway Web Server and SSH Server User Passwords

This section describes how to configure the media gateway Web Server and SSH Server user passwords via the EMS Software Manager. By default, this feature is disabled from the EMS application (SNMP), to enable it, a standalone INI file containing the following parameter must be downloaded to the CPE via the EMS Software Manager:

```
WEBPasswordControlViaSNMP = 1
```

The example above assumes that the default user name and password are **Admin / Admin** and the required user name and password are **Test / Test12345**.

➢ **To Update the media gateway Web Server and SSH user passwords via EMS:**

1. In the Desktop toolbar, click **Configuration** and in the Configuration pane, select **Info and Security**; the Info & Security Parameters Provisioning screen is displayed.
2. Select the **Web Access Settings** tab.
3. In the administrator row, enter User name: **Admin/Admin/Test (Current User Name / Current User Password / New User Name)**.
4. Click **Apply**; **t**he User Name is modified. Current User name is **Test**.
5. In the administration row, enter User code (Password): **Test/Admin/Test12345** (Current User Name/Current User Password /New Password).
6. Click **Apply**.

   The Password for User Test is changed to **/Test12345**.

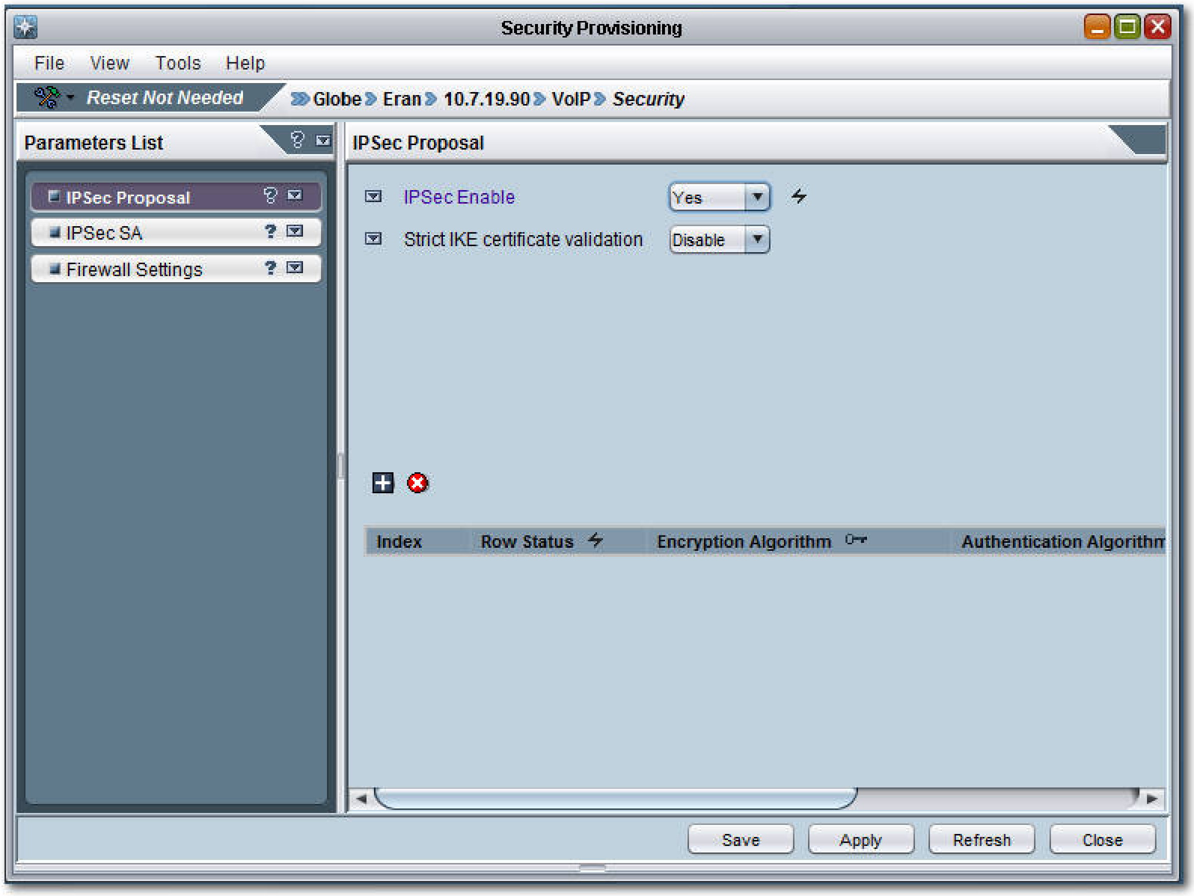
35.3.5 Configuring IPsec

This section describes how to configure IPsec.

➤ To configure MG & EMS to work over IPsec:

1. In the Navigation pane, select **VoIP** ▶ **Security** and in the Configuration pane, select **Security**. The Security Provisioning screen is displayed.

Figure 35-6:Security Provisioning



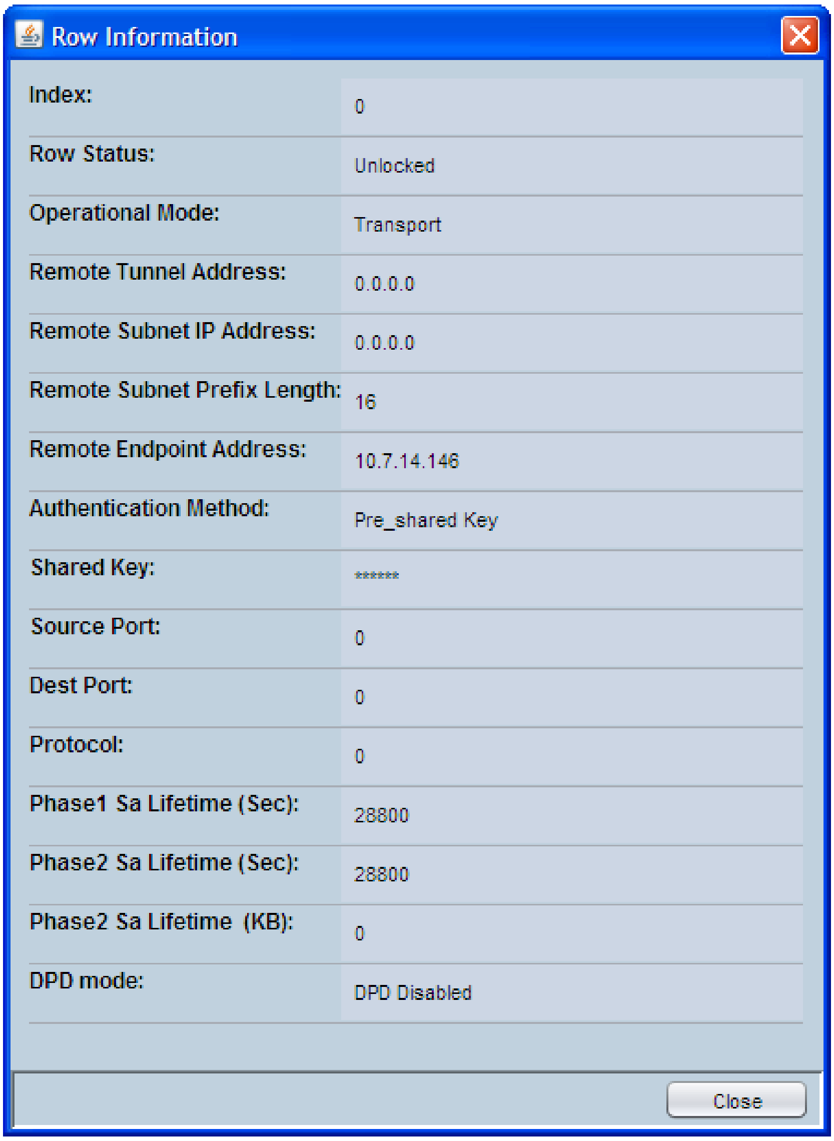
IPSec Enable: Yes

Strict IKE certificate validation: Disable

2. In the **IPSec Proposal** tab, set parameter 'IPSec Enable' to **Yes**.
3. Configure IPsec SA and IPsec Proposal tables according to the examples in the figures below.
4. Reset the media gateway (with burn).

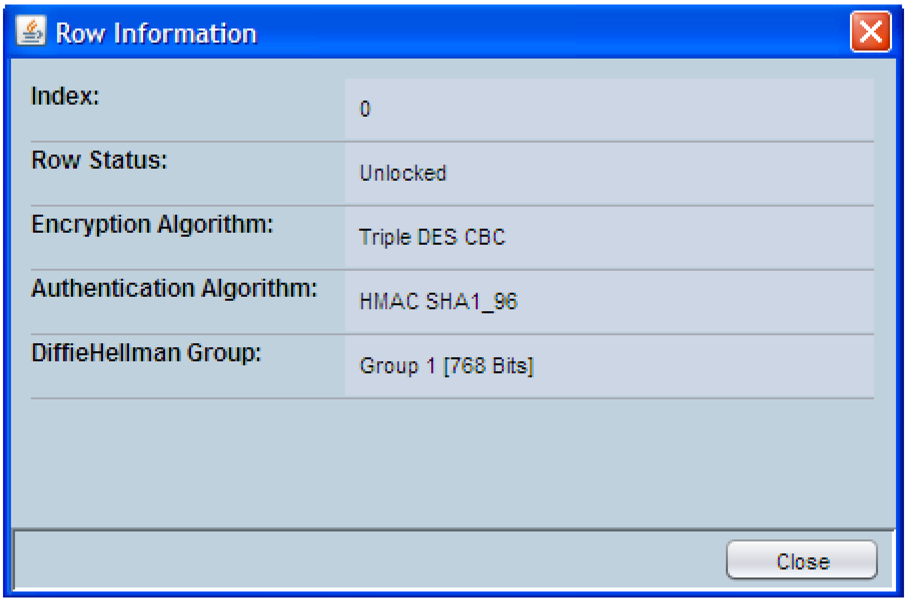
Note: You must configure the IPsec and IKE parameters exactly as shown in the figures below:

Figure 35-7: IPsec SA Configuration



Index:	0
Row Status:	Unlocked
Operational Mode:	Transport
Remote Tunnel Address:	0.0.0.0
Remote Subnet IP Address:	0.0.0.0
Remote Subnet Prefix Length:	16
Remote Endpoint Address:	10.7.14.146
Authentication Method:	Pre_shared Key
Shared Key:	******
Source Port:	0
Dest Port:	0
Protocol:	0
Phase1 Sa Lifetime (Sec):	28800
Phase2 Sa Lifetime (Sec):	28800
Phase2 Sa Lifetime (KB):	0
DPD mode:	DPD Disabled

Figure 35-8: IPsec Proposal Configuration

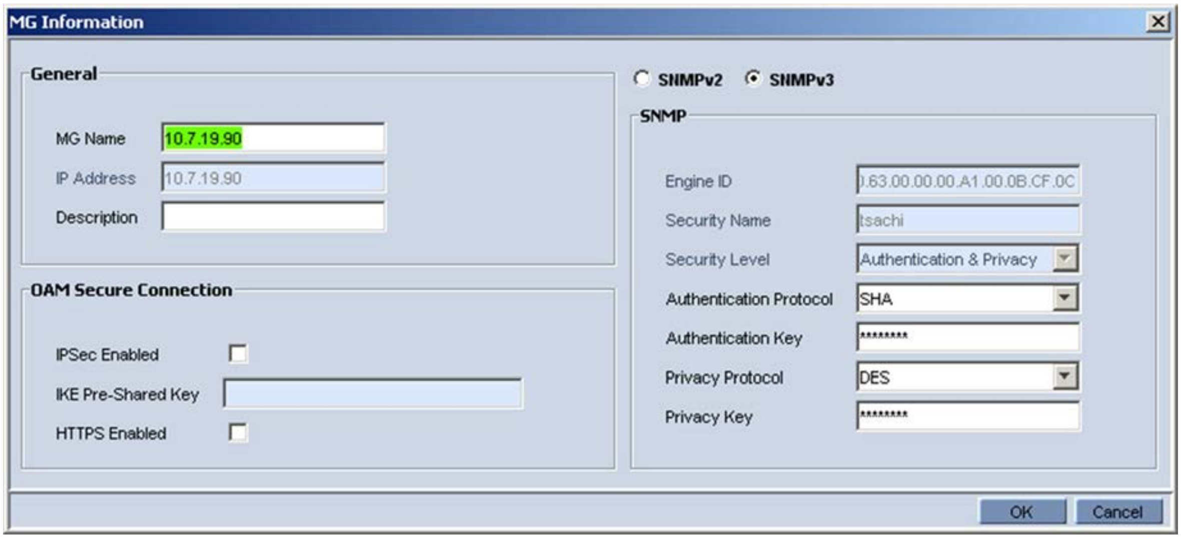


Row Information

Index:	0
Row Status:	Unlocked
Encryption Algorithm:	Triple DES CBC
Authentication Algorithm:	HMAC SHA1_96
DiffieHellman Group:	Group 1 [768 Bits]

5. Open the screen 'MG Information' (right-click the device in the **MGs List** and choose **Details**).

Figure 35-9: Securing Communication



MG Information

General

MG Name: 10.7.19.90

IP Address: 10.7.19.90

Description:

OAM Secure Connection

IPSec Enabled □

IKE Pre-Shared Key:

HTTPS Enabled □

○ SNMPv2 ● SNMPv3

SNMP

Engine ID:).63.00.00.00.A1.00.0B.CF.0C

Security Name: tsachi

Security Level: Authentication & Privacy

Authentication Protocol: SHA

Authentication Key: ********

Privacy Protocol: DES

Privacy Key: ********

6. Select the **IPSec Enabled** checkbox and enter the 'IKE Pre-shared Key' string (see the figure below). This configuration can be performed either during the media gateway definition stage or later.

Note: The IKE Pre-shared key string defined in the EMS and in the media gateway (see step 3 above) must be identical.

7. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of it, including its LEDs, must be displayed in the EMS's Status screen (see the figures of the status panes). If you do not view a graphic representation of the gateway in the Status screen (see Section 'Troubleshooting' on page 385 to resolve the issue).

35.3.6 Generating X.509 CSR and Self-Signed Certificate via EMS

A Certificate Signing Request (CSR) is a message sent from an applicant to a Certificate Authority (CA) to apply for a digital identity certificate. The CSR contains information identifying the applicant and the Public Key. The corresponding Private Key is not included in the CSR; however, is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proof of identity required by the Certificate Authority, and the Certificate Authority may contact the applicant for further information.

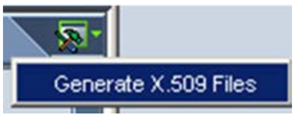
If the request is successful, the Certificate Authority will send back an identity certificate that has been digitally signed with the Private Key of the Certificate Authority. This certificate file, together with the certificate of the CA itself, must be added to the media gateway Auxiliary Files repository and configured in the Security Settings screen for the media gateway. You must also configure the Trusted Root Certificate file on the media gateway, depending on the identity of the CA who signed the certificate of the other participant (e.g. of the CA who issued the certificate for the Softswitch that communicates with the media gateway via SIP/TLS protocol).

Note: Never send the Private Key file to anybody. It contains the most sensitive security data and should never be disclosed. Use CSR instead as described below.

➢ **To generate a X.509 CSR and Self-Signed Certificate via EMS:**

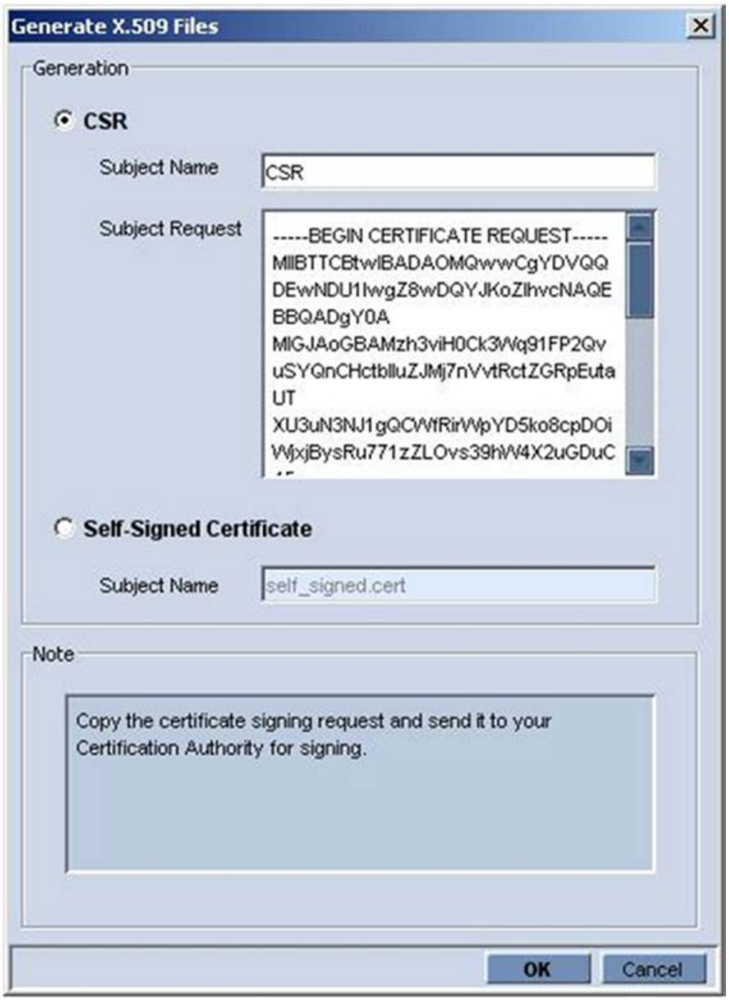
1. In the Info and Security Parameters Provisioning screen ► **General Settings** Tab, click the drop-down menu on the Maintenance icon in the top right-hand corner of the screen and click the **Generate X.509 Files** button.

Figure 35-10: Maintenance Action: Generate X.509 Files



The Generate X.509 Files dialog is displayed.

Figure 35-11: Generating a CSR Request



Subject Name: CSR

Subject Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTTCBtwIBADAOMQwwCgYDVQQ
DEwNDU1IwgZ8wDQYJKoZIhvcNAQE
BBQADgY0A
MIGJAoGBAMzh3viH0Ck3Wq91FP2Qv
uSYQnCHctblluZJMj7nVvtRctZGRpEuta
UT
XU3uN3NJ1gQCWfRirWpYD5ko8cpDOi
WjxjBysRu771zZLOvs39hW4X2uGDuC
```

○ Self-Signed Certificate

Subject Name: self_signed.cert

Copy the certificate signing request and send it to your Certification Authority for signing.

2. Click **OK**.
3. Click the **CSR** button.
4. Select a Private Key to apply to the Certificate Signing Request.
5. In the 'Subject' field, enter a brief description of the Certificate Signing Request.
6. Click **OK**.

   The CSR file is generated and the **Save As** dialog is displayed.
7. Enter the name of the CSR file and choose a folder on your computer where you wish to save it.
8. Send the CSR file to the Certificate Authority.

35.3.7 Adding Certificates to the Software Manager

After successfully generating the CSR and submitting it to the CA, you receive a digitally signed X.509 Certificate file from the CA. You should also have a certificate of the CA itself (for verification purposes) and a certificate of Trusted Root (depending on the PKI scheme that is implemented). All these files must be added t o the Software Manager prior to configuring them in the media gateway. For more information, see 'Software Manager' on page 65.

35.3.8 Activating the new X.509 Certificates on the Media Gateway

Once certificate files have been added to the Software Manager, do the following to activate the new X.509 configuration on the media gateway:

- Apply the new X.509 configuration to the media gateway boards by performing the Software Upgrade action and selecting the previously added files. Click **Apply** to download them to the media gateway.

For more information, see the relevant media gateway User Guide.

Reader's Notes

36 EMS Application Security

EMS Operator's Authentication and Authorization can be performed using either local EMS users management tools, or by using a centralized database. These options are described as follows:

- **Local User Management:**

  By default, the EMS application manages its users in the local EMS server where the EMS user and password are saved in the EMS database (see Section 36.3 on page 357).

- **Centralized User Management via an external database:**

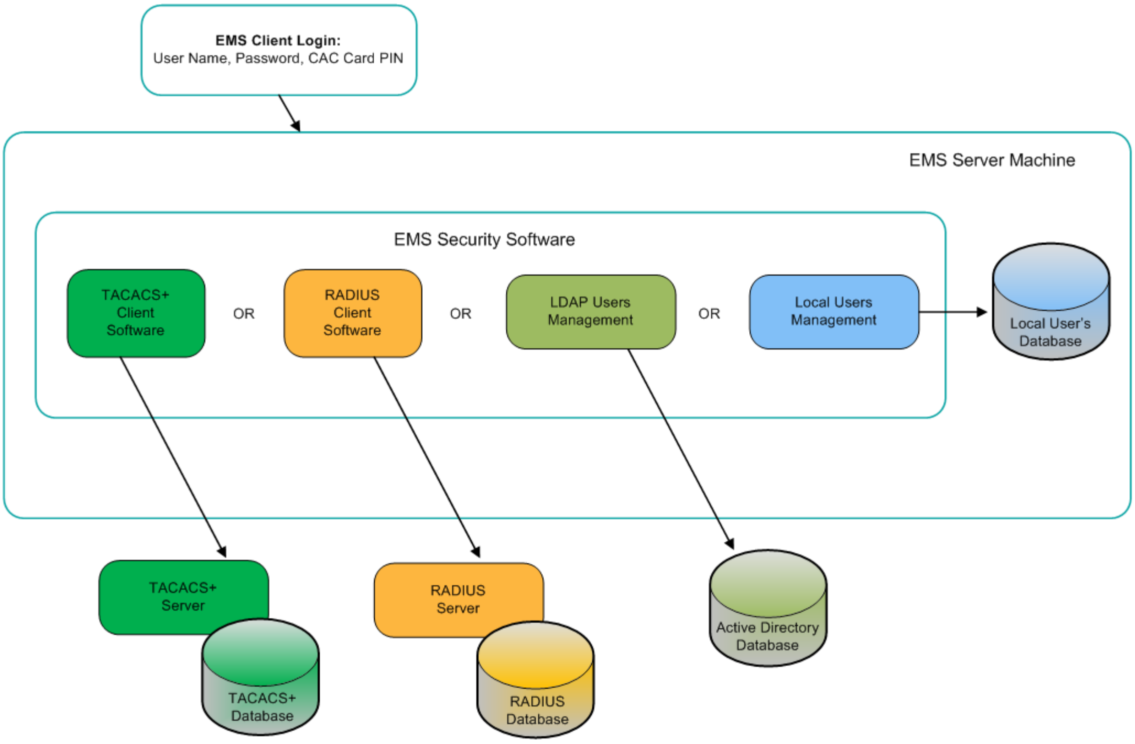
  When you choose these options, numerous usernames, passwords and access level attributes are stored externally on these platforms. In this case, the EMS server doesn’t store the username and password (these users are not displayed in the EMS users list) and instead forwards them to the pre-configured external user database.

  The following external user databases are supported:

  - Remote Authentication Dial-In User Service (RADIUS) (see Section 36.2.1 on page 353).
  - Terminal Access Controller Access-Control System Plus (TACACS+) (see Section 36.2.2 on page 355).
  - Lightweight Directory Access Protocol (LDAP) server (see Section 36.2.3 on page 356).

The figure below shows the different user management options.

Figure 36-1: Centralized User Management



Users can identify themselves with a Login user name and Password or by using Common Access Card (CAC) card (see below).

36.1 CAC Card

The CAC is a U nited 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 CAC is used as a g eneral identification card as well as for authentication to enable access to DoD computers, networks, and specific DoD facilities. It also serves as an identification card under the Geneva Conventions. The CAC enables the encryption and cryptographic signing, thereby facilitating the use of PKI authentication tools, and establishing an authoritative process for the use of identity credentials.

DoD PCs have a smartcard reader device installed, which is accompanied by the corresponding software kit that provides PKCS#11 compliant access to the smartcard reader. 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.

User who have CAC card, should select the option checkbox 'CAC PIN Number' in the Login screen 'Options' menu. When selected, a field to enter the CAC PIN number to login to the EMS client is displayed. You can use this option as an a lternative to entering the EMS username and password.

36.2 Centralized EMS Users Authentication and Authorization

Customers may select an option for EMS Application Users Authentication and Authorization using centralized Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) servers. For detailed information in reference to RADIUS or TACACS+ servers provisioning in the EMS, refer to Section 'Security' in the *EMS OAM Integration Guide*.

36.2.1 RADIUS Server

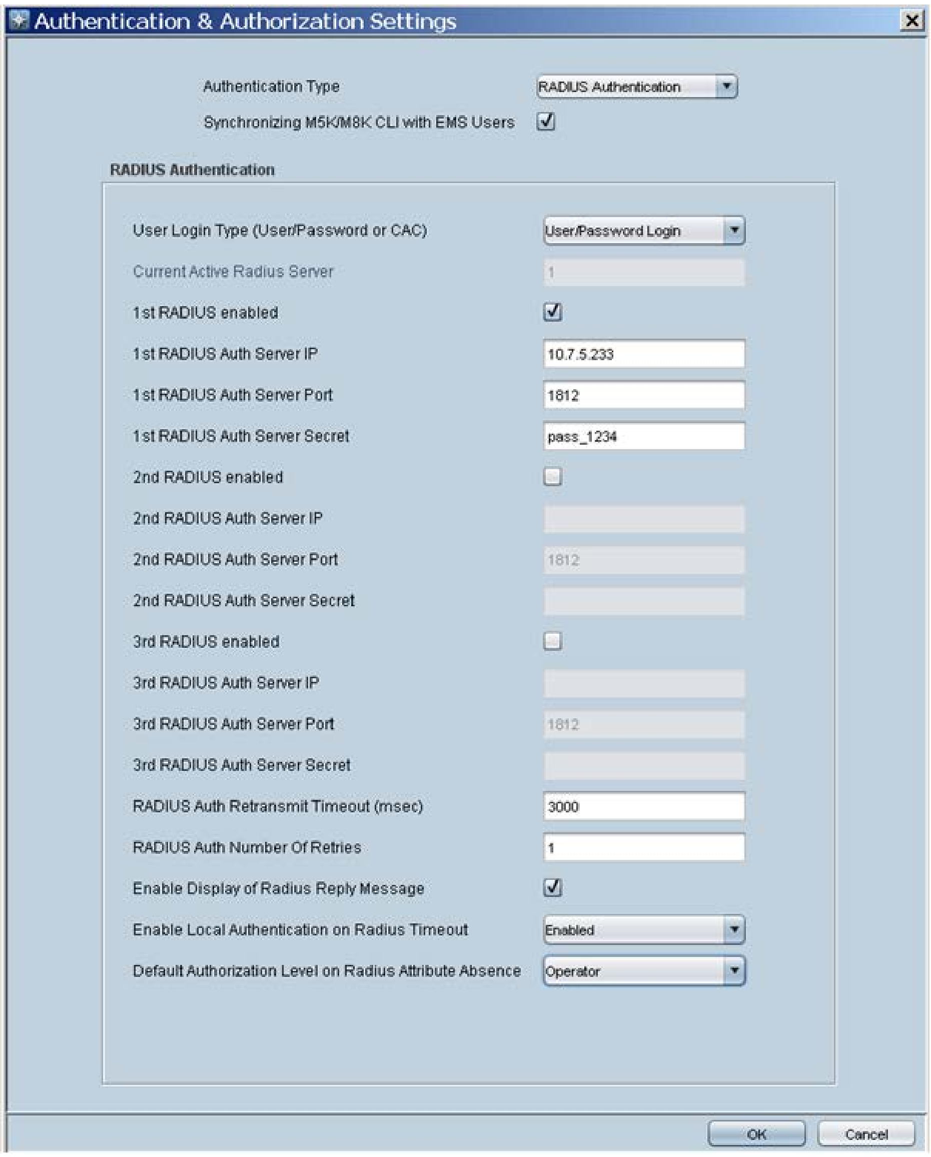
This section describes how to configure centralized EMS users Authentication and Authorization using a RADIUS server.

Note: There is a fallback option to save the user and password locally in the event that these servers do not respond ('Enable Local Authentication on Radius Timeout').

➢ To configure using a RADIUS server.

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the RADIUS Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **RADIUS Authentication**.

Figure 36-2: RADIUS Authentication and Authorization



Authentication Type	RADIUS Authentication
Synchronizing M5K/M8K CLI with EMS Users	☑

RADIUS Authentication

User Login Type (User/Password or CAC)	User/Password Login
Current Active Radius Server	1
1st RADIUS enabled	☑
1st RADIUS Auth Server IP	10.7.5.233
1st RADIUS Auth Server Port	1812
1st RADIUS Auth Server Secret	pass_1234
2nd RADIUS enabled	□
2nd RADIUS Auth Server IP	
2nd RADIUS Auth Server Port	1812
2nd RADIUS Auth Server Secret	
3rd RADIUS enabled	□
3rd RADIUS Auth Server IP	
3rd RADIUS Auth Server Port	1812
3rd RADIUS Auth Server Secret	
RADIUS Auth Retransmit Timeout (msec)	3000
RADIUS Auth Number Of Retries	1
Enable Display of Radius Reply Message	☑
Enable Local Authentication on Radius Timeout	Enabled
Default Authorization Level on Radius Attribute Absence	Operator

3. Configure parameters as shown in the screen above.

36.2.2 TACACS+ Server

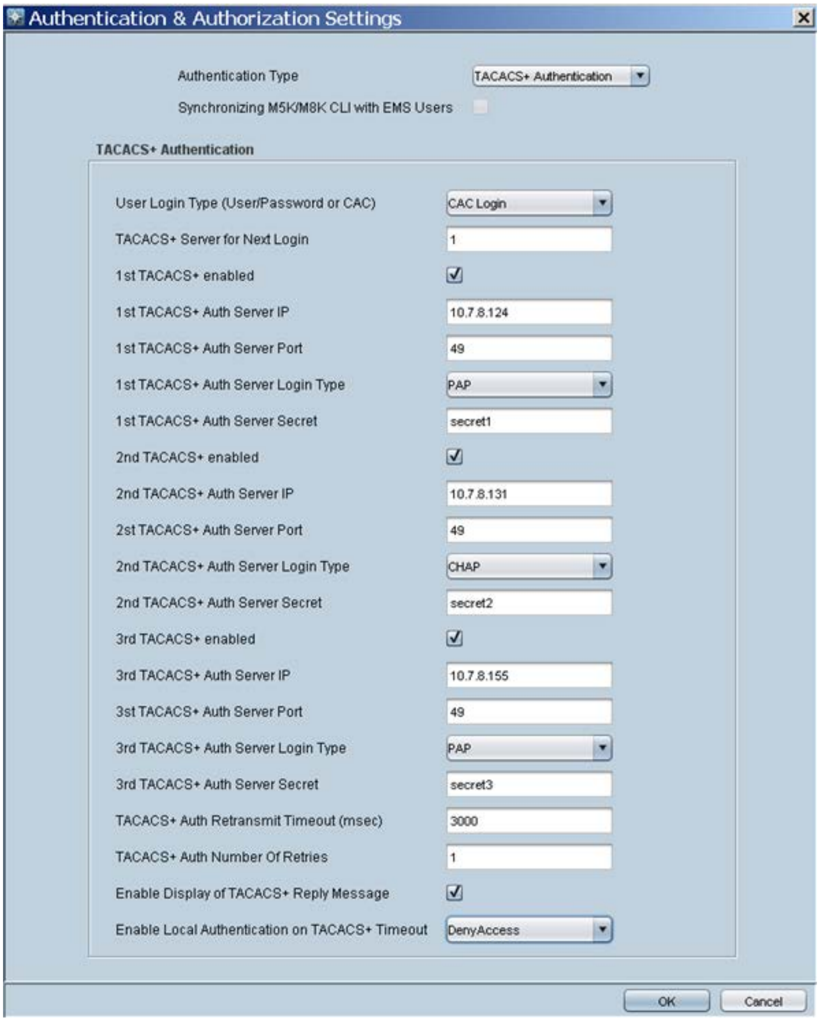
This section describes how to configure centralized EMS users Authentication and Authorization using a TACACS+ server.

Note: There is a fallback option to save the user and password locally in the event that these servers do not respond ('Enable Local Authentication on TACACS+ Timeout').

➢ To configure using a TACACS+ server.

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the TACACS+ Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **TACACS+ Authentication**.

Figure 36-3: TACACS Authentication and Authorization



Authentication & Authorization Settings

Authentication Type	TACACS+ Authentication
Synchronizing M5K/M8K CLI with EMS Users	□

TACACS+ Authentication

User Login Type (User/Password or CAC)	CAC Login
TACACS+ Server for Next Login	1
1st TACACS+ enabled	☑
1st TACACS+ Auth Server IP	10.7.8.124
1st TACACS+ Auth Server Port	49
1st TACACS+ Auth Server Login Type	PAP
1st TACACS+ Auth Server Secret	secret1
2nd TACACS+ enabled	☑
2nd TACACS+ Auth Server IP	10.7.8.131
2st TACACS+ Auth Server Port	49
2nd TACACS+ Auth Server Login Type	CHAP
2nd TACACS+ Auth Server Secret	secret2
3rd TACACS+ enabled	☑
3rd TACACS+ Auth Server IP	10.7.8.155
3st TACACS+ Auth Server Port	49
3rd TACACS+ Auth Server Login Type	PAP
3rd TACACS+ Auth Server Secret	secret3
TACACS+ Auth Retransmit Timeout (msec)	3000
TACACS+ Auth Number Of Retries	1
Enable Display of TACACS+ Reply Message	☑
Enable Local Authentication on TACACS+ Timeout	DenyAccess

3. Configure parameters as shown in the screen above.

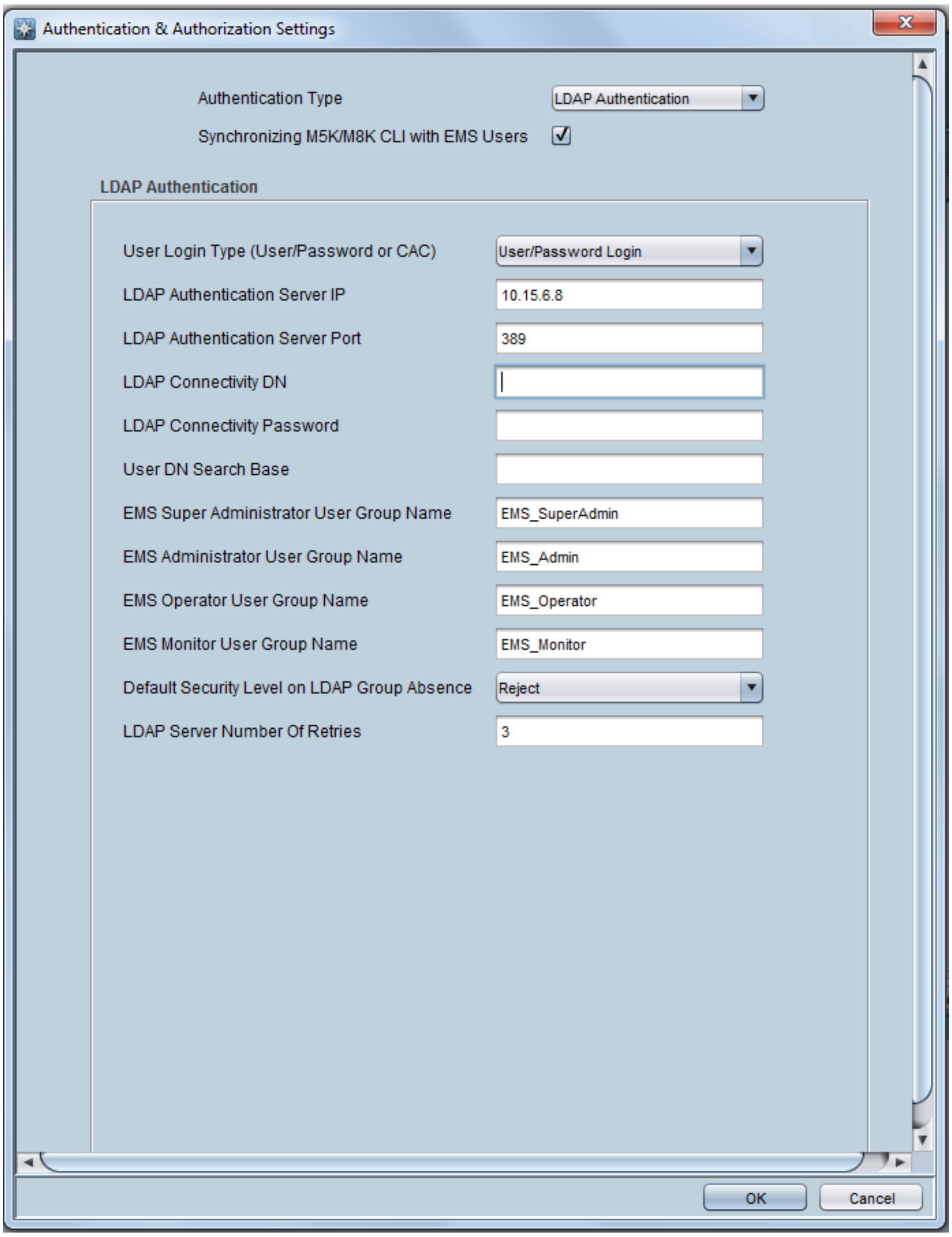
36.2.3 LDAP Server

This section describes how to configure centralized EMS users Authentication and Authorization using an LDAP server.

➢ To configure using an LDAP server.

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the LDAP Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **LDAP Authentication**.

Figure 36-4: LDAP Authentication and Authorization



Authentication & Authorization Settings

Authentication Type: LDAP Authentication

Synchronizing M5K/M8K CLI with EMS Users ☑

LDAP Authentication

User Login Type (User/Password or CAC)	User/Password Login
LDAP Authentication Server IP	10.15.6.8
LDAP Authentication Server Port	389
LDAP Connectivity DN	
LDAP Connectivity Password	
User DN Search Base	
EMS Super Administrator User Group Name	EMS_SuperAdmin
EMS Administrator User Group Name	EMS_Admin
EMS Operator User Group Name	EMS_Operator
EMS Monitor User Group Name	EMS_Monitor
Default Security Level on LDAP Group Absence	Reject
LDAP Server Number Of Retries	3

3. Configure the LDAP Authentication Server IP.
4. Configure other parameters as required.

36.3 Local Users Management in the EMS Application

This section describes how to provision and operate EMS users stored locally in the EMS application. All the user operations can be performed by the user with the Administrator security level.

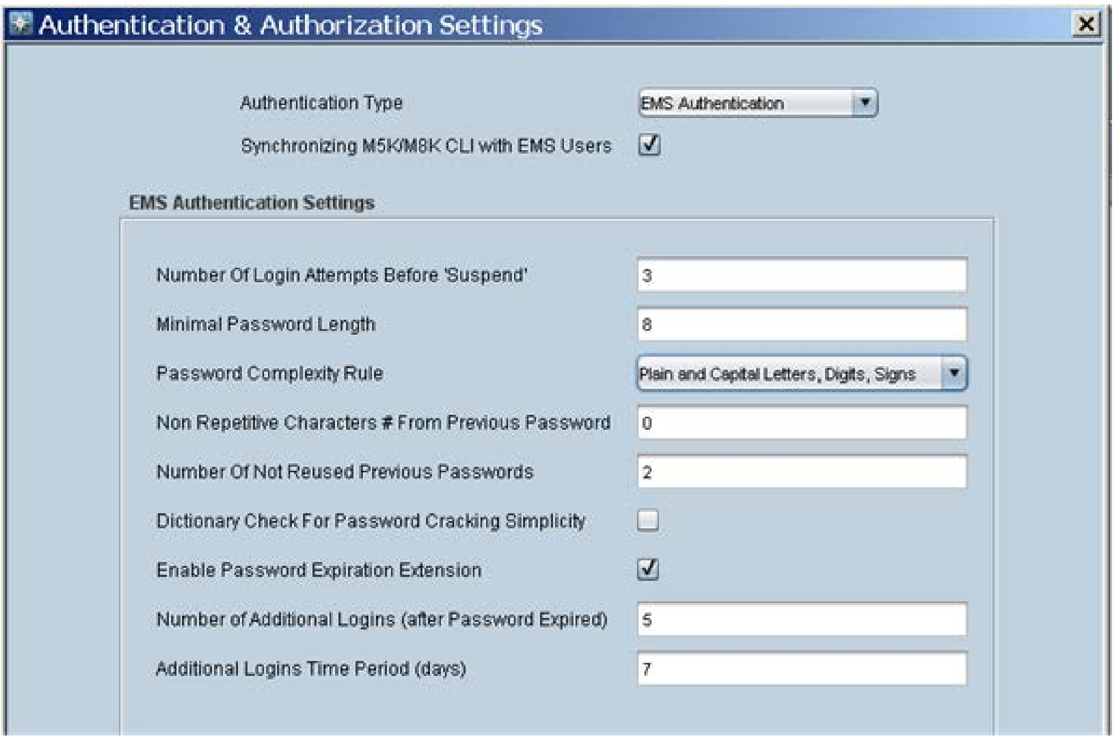
The local EMS's users management feature enables the operator with the Administrator security level to exert control over other operators' access to system resources. This ensures that sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be d isrupted by inexpert operators. In addition, the Administrator can set different user permissions for different regions. This feature has been implemented for Enterprise and Service provider environments who need to allow specific users to view only a subset of the sites, as well as to provide them with different security level per sites (regions).

User management is performed in the Security Menu, 'Users List' window. This window lists local EMS users and enables you to perform user management actions such as adding or removing a user. The EMS's user management feature enables the operator with the Administrator security level to exert control over other operators' access to system resources. In this way, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators.

➢ To manage EMS users using EMS:

1. In the Main EMS menu, choose **Security** ► **Authentication and Authorization**.
2. From the 'Authentication Type' drop-down list, select **EMS Authentication**.

Figure 36-5: EMS Authentication Settings



Authentication Type: EMS Authentication

Synchronizing M5K/M8K CLI with EMS Users: ☑

EMS Authentication Settings

Number Of Login Attempts Before 'Suspend': 3

Minimal Password Length: 8

Password Complexity Rule: Plain and Capital Letters, Digits, Signs

Non Repetitive Characters # From Previous Password: 0

Number Of Not Reused Previous Passwords: 2

Dictionary Check For Password Cracking Simplicity: □

Enable Password Expiration Extension: ☑

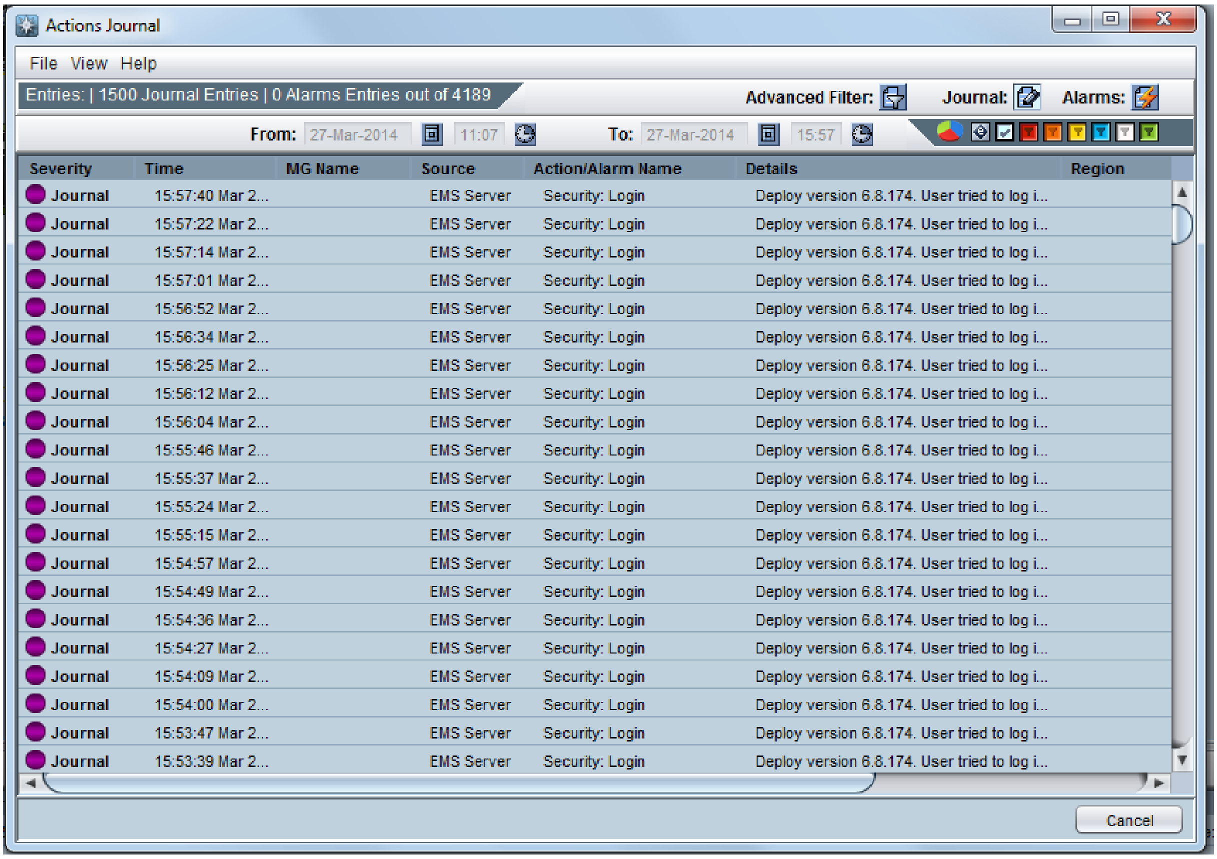
Number of Additional Logins (after Password Expired): 5

Additional Logins Time Period (days): 7

36.3.1 Actions Journal-Security Items

The Actions Journal displays all logged operator actions, enabling the Administrator to verify appropriate operator access to system resources and providing the Administrator with the means to retroactively analyze actions previously carried out by operators. The Actions Journal screen is context sensitive and therefore when accessed from the Security menu, option 'Actions Journal', displays all login related events. For more information, see Chapter 37 on page 373.

Figure 36-6: Actions Journal-Security Items



Entries: | 1500 Journal Entries | 0 Alarms Entries out of 4189

From: 27-Mar-2014 11:07 To: 27-Mar-2014 15:57

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region
Journal	15:57:40 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:22 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:14 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:01 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:52 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:34 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:25 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:12 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:04 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:46 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:37 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:24 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:15 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:57 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:49 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:36 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:27 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:09 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:00 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:53:47 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:53:39 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	

36.3.2 Synchronizing EMS and Mediant 5000 / 8000 CLI users

When selecting this option, EMS automatically updates each one of the managed Gateways with the entire user's list defined in EMS, and synchronizes this list upon user addition, removal, password change or for any other changes in user details. For more information, refer to the relevant *IOM Guide*.

➢ To synchronize EMS and Mediant 5000 / 8000 CLI users:

- In the Authorization and Authentication Settings window, select the **Synchronizing M5K/M8K Users CLI with EMS Users** checkbox.

36.3.3 Provisioning Password Aging Rules

This section describes the EMS user password aging rules. Some of the rules are configured per EMS application and are applicable for all the users. Another subset of settings can be configured for each user. For more information on the user specific configuration, see the 'User Details Screen' descriptions.

The provisioning rules below are applicable for the entire EMS application and all its users.

➢ To provision password aging rules:

- In the Authorization and Authentication Settings window, set the following parameters:
  - Number of Login Attempts before the EMS application suspends the user

    Once the number of login attempts as defined by this parameter is reached, the user is blocked from logging into EMS and can only be unblocked by the Administrator. Default-3 attempts.
  - Minimal Password Length: Default= 8 characters. The maximum supported value is 30 characters.
  - Password Complexity Rule- the following options are supported:
    - No complexity rules are applied (default)
    - Use Plain or Capital letters, Digits and Special Characters
    - Use Plain and Capital letters, Digits and Special Characters
  - Non Repetitive Characters # From Previous Password: Default=0, where all the characters can be reused for more than one password. The maximum supported value is 10.
  - Number of Not Reused Previous Passwords: Default=5. Possible values are 0-10.
  - Dictionary Check For Password Cracking Simplicity: when this option is enabled, the EMS server performs a password weakness check on the EMS user password. By default, this feature is disabled.

Note: All the parameters provisioned in this window are applicable for all the users and all the gateways in the EMS application.

36.3.4 Provisioning Password Expiration Extension Period

This section describes how to provision the password expiration extension period.

➢ **To provision password expiration extension period:**

1. In the Authorization and Authentication Settings window, select the **Enable Password Expiration Extension** checkbox, and set the following parameters:
2. **Number of Additional Logins** – defines the number of logins user can perform after his password already expired. Valid range: 1-10. Default: disabled.
3. **Additional Logins time period (days)** – defines the period (in days) during which user can perform the defined above number of additional logins. Valid range: 1-60. Default: disabled.

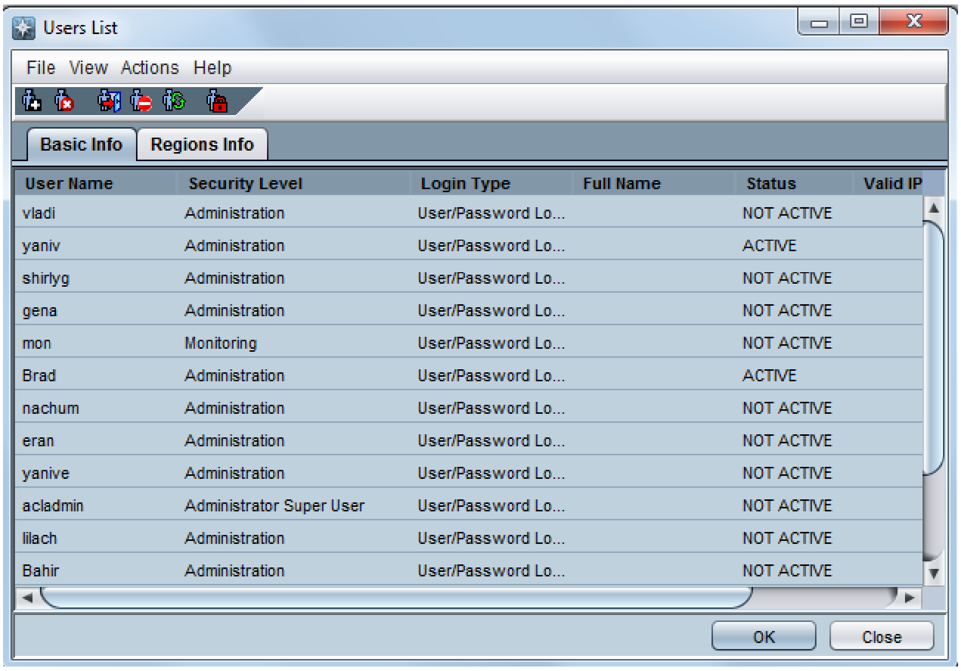
36.4 Managing the Users List

This section describes how to access the EMS Users list. User security level can be defined either per entire application or per Region.

➢ **To open the Users List:**

- In the EMS Main menu, choose **Security** ▶ **Users List** ; the Users List screen opens:

Figure 36-7: Users List



User Name	Security Level	Login Type	Full Name	Status	Valid IP
vladi	Administration	User/Password Lo...		NOT ACTIVE	
yaniv	Administration	User/Password Lo...		ACTIVE	
shirlyg	Administration	User/Password Lo...		NOT ACTIVE	
gena	Administration	User/Password Lo...		NOT ACTIVE	
mon	Monitoring	User/Password Lo...		NOT ACTIVE	
Brad	Administration	User/Password Lo...		ACTIVE	
nachum	Administration	User/Password Lo...		NOT ACTIVE	
eran	Administration	User/Password Lo...		NOT ACTIVE	
yanive	Administration	User/Password Lo...		NOT ACTIVE	
acladmin	Administrator Super User	User/Password Lo...		NOT ACTIVE	
lilach	Administration	User/Password Lo...		NOT ACTIVE	
Bahir	Administration	User/Password Lo...		NOT ACTIVE	

The EMS application supports 25 concurrent (active) EMS users. In the Users List screen (displayed in the above figure) you can do the following:

- View the list of operators defined in the EMS system
- View each user's status:
  - ACTIVE (the user is currently connected to the EMS application)
  - NOT ACTIVE (the user is not connected to the EMS application)
  - SUSPENDED (the user was suspended by the Administrator; double-click the row of the user for more details).
  - AUTOMATICALLY SUSPENDED (the user was automatically suspended by the EMS system. This occurs when a user exceeds the maximum number of allowed login attempts (3). An operator with Administration security level is automatically released from suspension after 1 hour. An operator with Monitoring or Operation security level will require manual release by the Administrator).
- View Login type:
  - **User / Password User** – the user should identify themselves by typing user / password in the Login Frame.
  - **CAC User** – the user should identify themselves using the CAC card and typing the CAC card PIN code in the Login Frame.
- View list of IP addresses from which the user can login.
- View and define user permissions per Region in the 'Regions Info' Tab.

Note: A user can open only one active session at a time. If a user is in Active state, this user cannot open a second instance of the application.

36.4.1 Adding an Operator

This section describes how to add an EMS Operator.

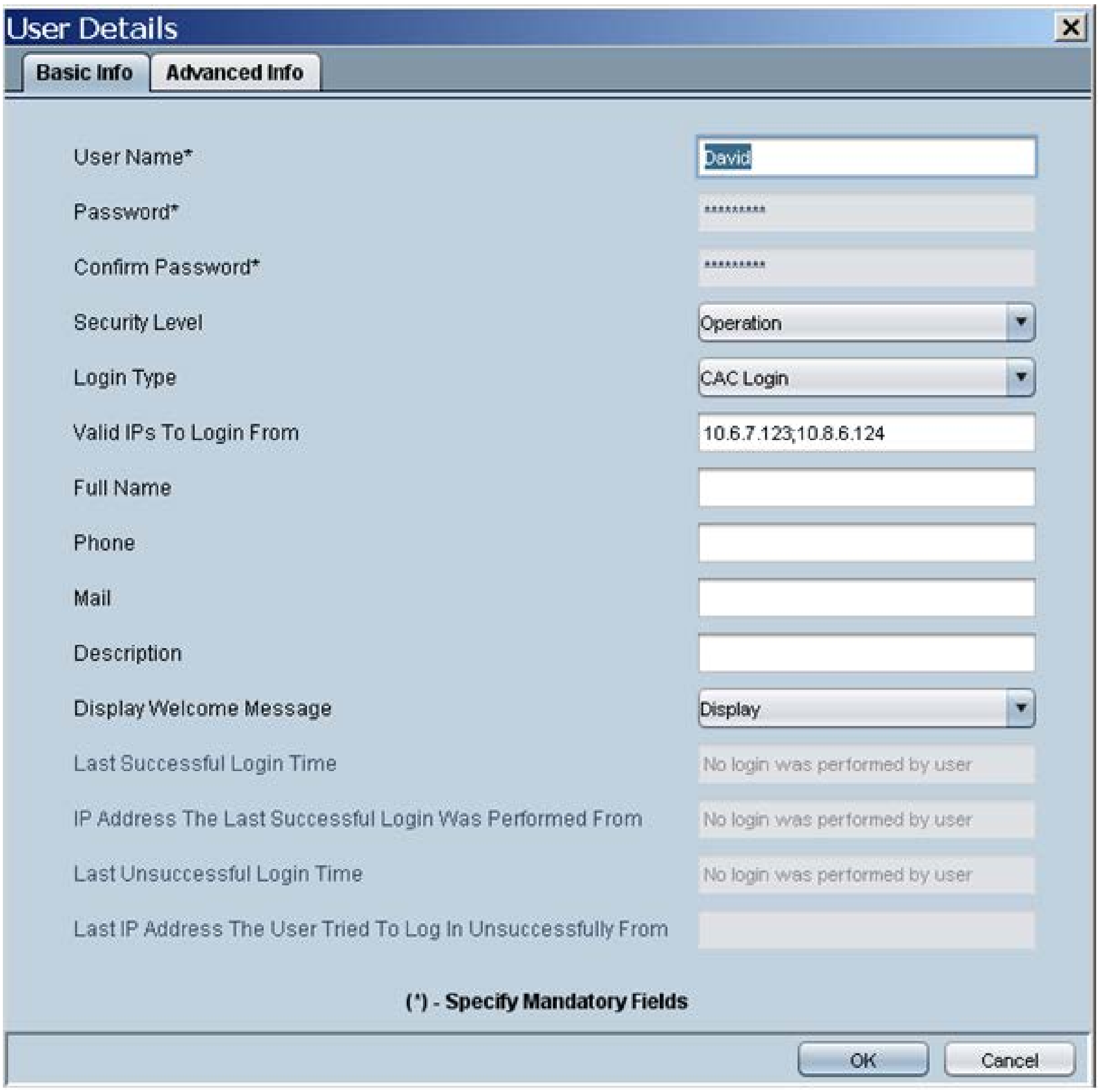
➢ **To add an operator, do one of the following:**

- In the menu bar, choose **Actions > Add User**.

  -OR-

- Click the button **Add User** on the Users List toolbar; the User Details screen opens.

Figure 36-8: User Details screen - Basic Info



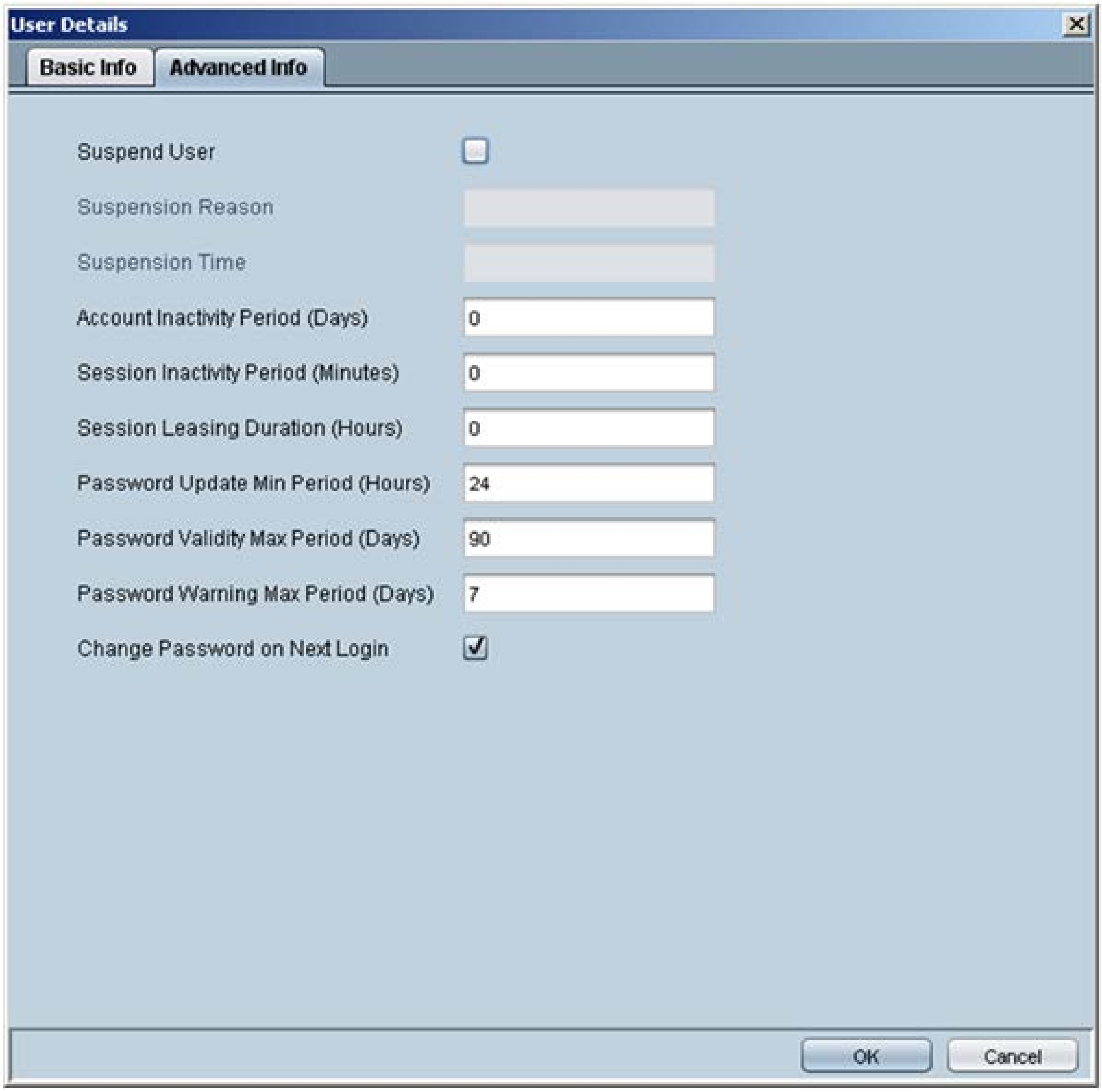
User Details

Basic Info | Advanced Info

User Name*	David
Password*	*********
Confirm Password*	*********
Security Level	Operation
Login Type	CAC Login
Valid IPs To Login From	10.6.7.123;10.8.6.124
Full Name	
Phone	
Mail	
Description	
Display Welcome Message	Display
Last Successful Login Time	No login was performed by user
IP Address The Last Successful Login Was Performed From	No login was performed by user
Last Unsuccessful Login Time	No login was performed by user
Last IP Address The User Tried To Log In Unsuccessfully From	

(*) - Specify Mandatory Fields

Figure 36-9: User Details screen - Advanced Info



Suspend User	□
Suspension Reason	
Suspension Time	
Account Inactivity Period (Days)	0
Session Inactivity Period (Minutes)	0
Session Leasing Duration (Hours)	0
Password Update Min Period (Hours)	24
Password Validity Max Period (Days)	90
Password Warning Max Period (Days)	7
Change Password on Next Login	☑

- The User Details screen (displayed in the figure above) enables you to add an operator to the list of operators displayed in the Users List screen (see Section 'Security Management' on page 333, specifically, to the figure 'Users List').
- Mandatory fields in the User Details screen are Login Name and Password. The other fields in the screen are optional.
- Click **OK** at the bottom of the screen to send your changes to the server.

Parameters that can be defined during an 'Add User' operation or modified thereafter are divided into two screens: Basic and Advanced Info.

36.4.1.1 Basic Info

- Changing a user's password: To modify a user's password, change the 'Password' and 'Confirm Password' fields. Both fields should have the same values.
- Security Level: EMS operators can be assigned one of the following security levels:
  - Not visible – this level is relevant only when defining different security levels per Region. When some Regions are defined as 'Not Visible' for the specific user, they will not be able to see these Regions and their devices in the EMS Tree.
  - Monitoring (viewing only)
  - Operation (viewing and all system provisioning operations on media gateways)
  - Administration (viewing, all system provisioning operations on media gateways, and operator security management described in this section).
  - Administrator Super User (viewing, all system provisioning operations on media gateways, operator security management described in this section and Administration users manipulations i.e. adding and removing administrators). This is the highest level of security.
- Login Type
  - User / Password Login – the default
  - CAC Login
- Valid IPs to Log In From: the following formats of IP addresses and / or ranges from which the operator is allowed to log into the EMS application are supported (should be separated by ;). The user will be allowed to perform the login when one of the following rules matches the User IP:
  - List of specific IPs: IP1;IP2;IP3;IP4
  - List of IPs ranges: IP1-IP2; IP3-IP4 (ranges are limited to IP Group D).
  - List of Networks: Network1/Mask;Network2/Mask

  For example, the following set will be valid: 10.7.6.20; 10.7.6.21; 10.7.6.30-10.7.6.40; 10.7.16.0/20
- Full Name: The user's full name
- Phone: The user's phone number
- Mail: The user's mail address
- Pager: The user's pager
- Description: A description of the user's position, function and responsibilities in the enterprise.

36.4.1.2 Login Information

- Display Welcome Message

  In cases where the Welcome Message Option in the Help -> Welcome Message screen is set to 'Optional' or 'Disable', the Administrator can Enable / Disable the Welcome Message for each one of the specific users. A summary of the different definitions is summarized in the table below.

Table 36-1: Welcome Message Options

Welcome Message Options	Don't Display	Display	Display without Login Information
Mandatory	Welcome Message	Welcome Message + Login Information	Welcome Message
Optional	X	Welcome Message + Login Information	Welcome Message
Disable	X	Login Information	X

- Last Login Time and client workstation IP Addresses of the latest Successful and Unsuccessful Login attempts are displayed.

36.4.1.3 Advanced Info

Suspend Information

- User suspension information: Suspension Status, Suspension Reason and Suspension Time.

Account / Session Security Settings

- **Account Inactivity Period (Days)**: User accounts are suspended in case the user did not login to the EMS application during a specified period of time (according to the parameter Account Inactivity Period). Default value= 0 where this feature is disabled and User Accounts are never suspended due to account inactivity. Maximal available value is 10.000 days.
- **Session Inactivity Period (Minutes)**: After the defined period of time (according to parameter Session Inactivity Period (minutes), the operator is notified that the session is 'Locked' and is prompted to enter their password to re-enter the EMS application. When set to the default configuration (0), no session inactivity timeout is applied. The Session inactivity period is a security mechanism designed to prevent unauthorized users from using the application while the authorized user is away from their computer.
- **Session Leasing Duration (Hours)**: After the defined period of time, the user is notified that the session is finished and is prompted to enter their password to work with the EMS. When defined as '0' (default configuration), no leasing time is applied. Leasing time is a security mechanism to permit the operator to log in to a time duration that is equivalent to one shift (i.e., 8 hours).

Password Settings

- **Password Update Minimum Period (Hours)**: A user password cannot be changed more than once within the time specified by this parameter. Default-24 hours.
- **Password Validity Maximum Period (Days)**: A user password must be changed within a specific number of days since the last password change as defined by this parameter. Default-90 days.
- **Password Warning Max Period (Days)**: The user receives a warning message a specified number of days prior to the password expiration date. Default-7 days.
- **Force Password Change on the next login**: A user password must be changed on the next Login attempt, before the previously defined password expiration time has expired. Active users are not required to Logout the application until their session has ended.

36.4.1.4 Regions Info

- The **Regions Info** tab includes the currently defined regions in the EMS and the security level for each region. The security level can be defined per region only for users with the 'Basic' security permissions 'Operator' or 'Monitoring'. For each one of the regions, the administrator can choose one of the following permissions:
  - Operator
  - Monitoring
  - Not visible
- The Region security level cannot be set to a higher security level than the 'Basic' user security level. For example, if the 'Basic' security level is set to 'Monitoring', it cannot be set to 'Operator' in any of the regions.

Note: For the 'Super-Admin' & 'Admin' levels, there is no option to define the security level per region, since these users are system level users.

- **Global Users Permissions:**

  Users with 'Super Administrator' or 'Administrator' permissions can perform the following EMS actions:

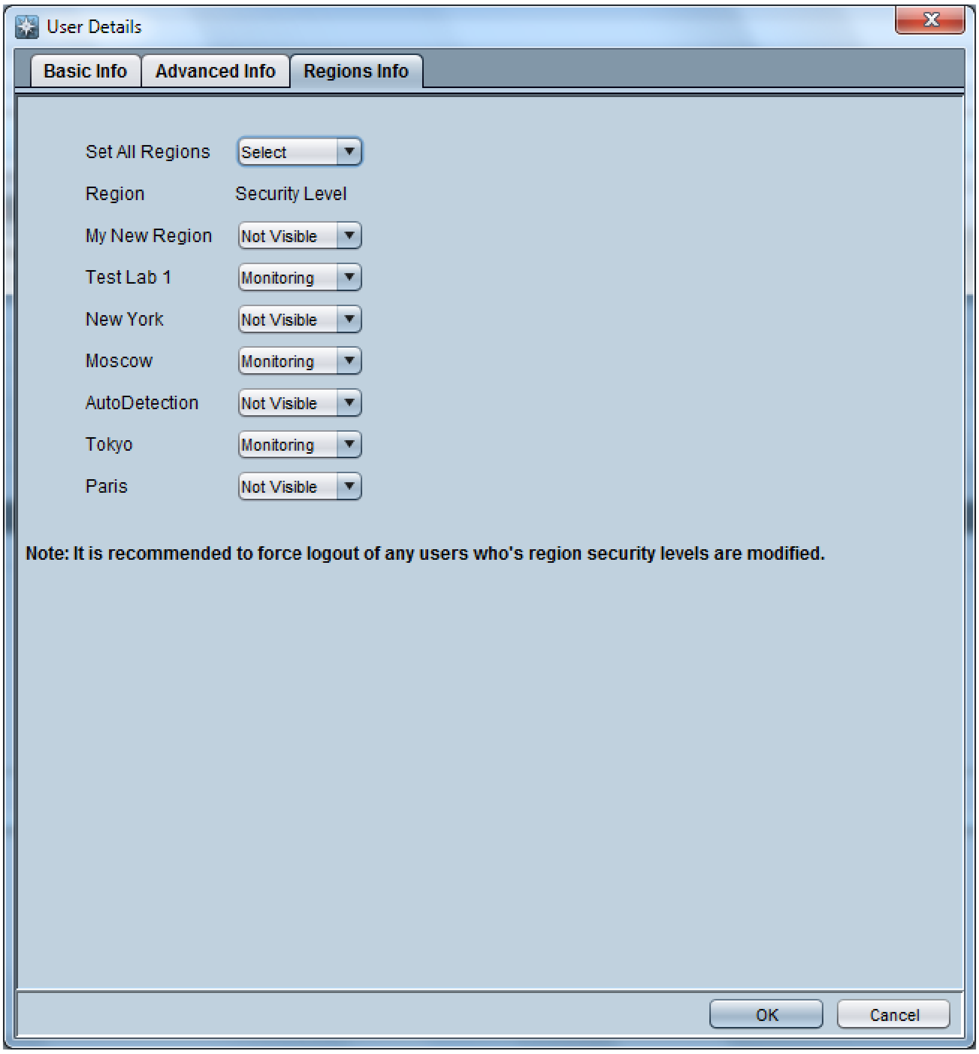
  - Users Management – view, define, edit users and user permissions. Perform actions related to the Users.
  - View Users Actions Journal
  - Perform Software and / or Auxiliary Files definition in the Software Manager (while the download to the gateway can be performed also by Regional Users)
  - Add / Remove Region (Gateway), Move Gateway from one Region to Another.
  - Provision Trap Forwarding Rules

Note: These actions are not supported at the Regions level.

- **Regional Users Permissions:**
  - Regional level users can be set with different permissions in different regions. The regional user can be set with the following permissions:
  - Operator (read-write) - Perform any actions and/or provisioning changes on all the relevant gateways, alarms actions, performance monitoring profiles/rules definition.
  - Monitoring (read-only) – View all the data without option to perform any modifications.
  - Not Visible – A user defined as 'Not Visible' for a specific region does not see this region displayed in the EMS.

  You can also use the 'Set All Regions' option to replicate an identical permission for all the regions in a single click.

Figure 36-10: User Details - Regions Info



Set All Regions	Select
Region	Security Level
My New Region	Not Visible
Test Lab 1	Monitoring
New York	Not Visible
Moscow	Monitoring
AutoDetection	Not Visible
Tokyo	Monitoring
Paris	Not Visible

Note: It is recommended to force logout of any users who's region security levels are modified.

36.4.2 Modifying Operator Details

This section describes how to modify EMS Operator details.

➢ **To modify operator details:**

1. Double-click the name of the operator listed in the left column under Login; the User Details screen opens.

   The User Details screen is identical to that displayed in the figure 'Adding an Operator' (see Section 'Adding an Operator' on page 361) with the difference that fields are configured and the first field Login Name is disabled (read-only and non-configurable).

   The field 'Security Level' enables the Administrators to set access rights for each operator: Administrator Super User, Administration, Operation and Monitoring.

   If the user is an active user (logged in), changing the security level automatically logs the user out.

2. Click **OK** to send the modified user data to the server.

36.4.2.1 Removing an Operator

This section describes how to remove an EMS Operator.

➢ **To remove an operator:**

1. In the Users List screen, select the row of the operator to remove. Multiple rows can be selected to be removed.
2. Click the **Remove User** button or open the 'Action' menu and choose option **Remove User**. All selected rows are removed from the User Security Management screen.
3. Click **OK** to send your changes to the server.

⚠ **Note:** At least one user with the security level of Administrator Super User should always be defined in the EMS system. Attempted removal of the last user with the security level of Administrator Super User will fail.

36.4.2.2 Forcing the Logout of a Currently Active Operator

This section describes how to force the logout of a currently active Operator.

➢ **To force the logout of a currently active operator:**

1. In the 'Users List' screen, select the row of the operator who is to be logged out. Multiple users can be selected for logout.
2. Click the icon **Logout User** or open the 'Actions' menu and choose option **Logout User**; all selected rows now indicate 'NOT ACTIVE'.
3. Click **OK** to send your changes to the server.

36.4.2.3 Suspending an Operator

This section describes how to suspend an EMS operator.

➢ **To suspend an operator:**

1. In the 'Users List' screen, select the row of the operator who is to be suspended. Multiple users can be selected for suspension.
2. Click the icon **Suspend User** or open the 'Actions' menu and choose option **Suspend User** or double-click the user's row and select the check box **Suspended**; all selected rows now indicate 'SUSPENDED'.
3. Open the 'User Details' screen (double-click the row of the user) and enter the reason for the suspension of that user in the field 'Suspension Reason'.
4. Click **OK** to send your changes to the server.

   All active users are automatically logged out before suspension

Note: A user with the security level of Administrator or Administrator Super User cannot be suspended.

36.4.2.4 Releasing an Operator from Suspension

This section describes how to release an EMS operator from suspension.

➢ **To release an operator from suspension:**

1. In the Users List screen, select the row of the (suspended) operator who is to be released from suspension. Multiple users can be selected for release from suspension.
2. Click the icon **Release User from Suspension** or open the 'Actions' menu and choose option **Release User from Suspension**, or double-click the user's row and clear the checkbox **Suspended**; all selected rows now indicate 'NOT ACTIVE'.
3. Click **OK** to send your changes to the server.

36.4.2.5 Canceling Changes Made to the Users List

This section describes how to cancel changes made to the users list.

➢ **To cancel changes made to the Users List screen:**

- Click the **Cancel** button (not the **OK** button); all changes you made are canceled.

36.4.2.6 Changing an Operator's Password

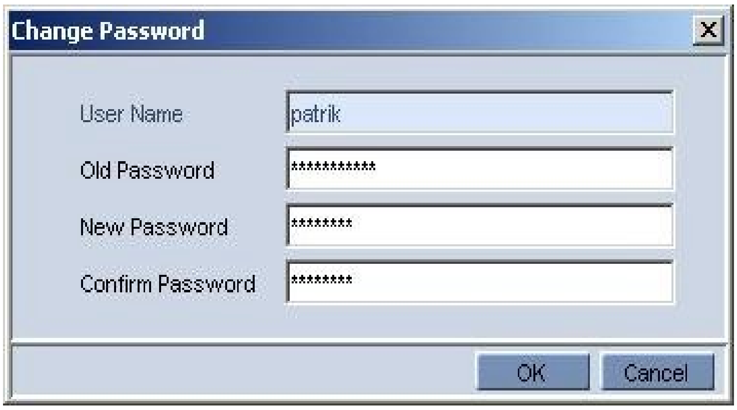
The following describes the conditions for changing an EMS operator's password:

Password management rules are defined both per EMS application and per specific operator. These rules are configured by the EMS Administrator.

➢ **To change an operator's password:**

1. Operators can change their own password. In the 'Security' menu, choose option **Change Password**; the 'Change Password' screen opens (see the figure below).

Figure 36-11: Change Password



Change Password

User Name: patrik

Old Password: ***********

New Password: ********

Confirm Password: ********

2. Change the password previously defined in the Password field.

Reader's Notes

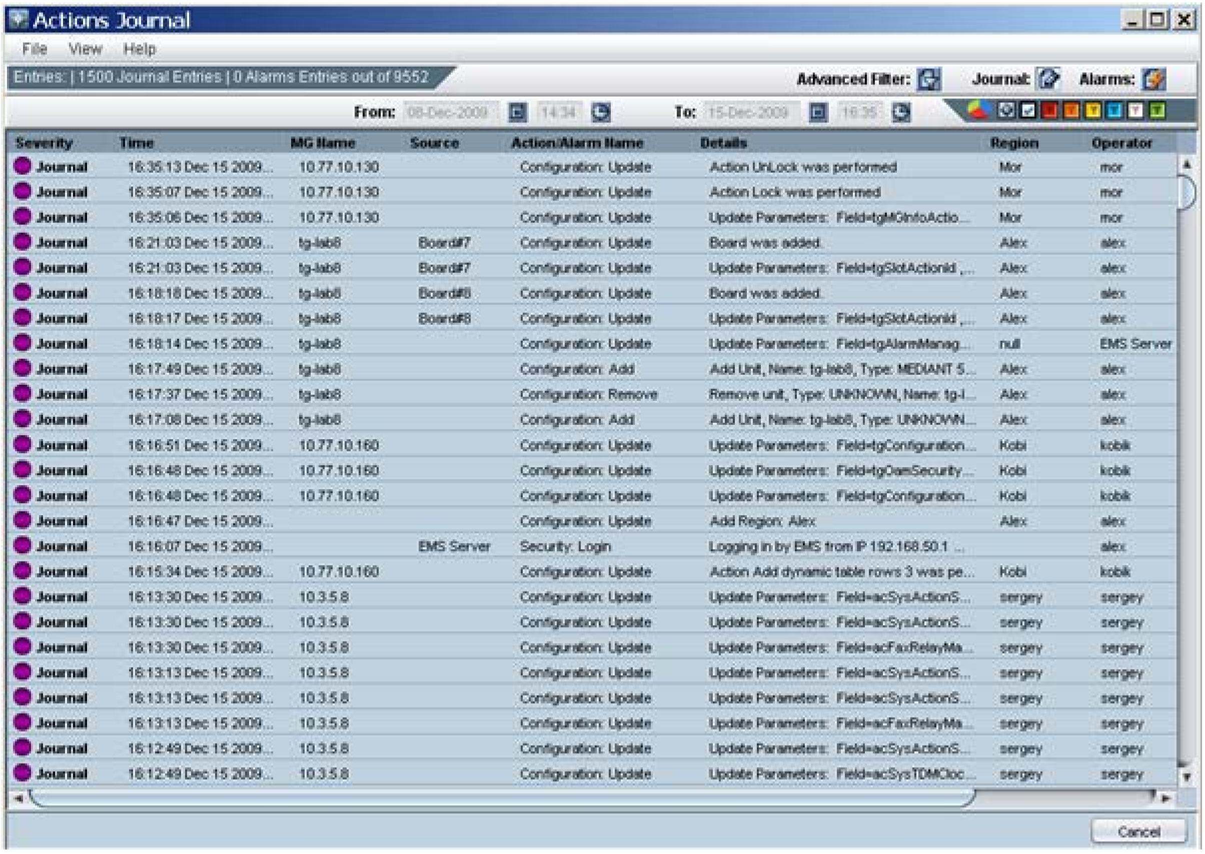
37 Viewing Operator Actions in the Actions Journal

This section describes how to view operator actions in the actions journal.

➢ **To view the Actions Journal:**

- In the EMS Main menu, choose **Security** ▸ **Actions Journal**; the Actions Journal screen is displayed.

Figure 37-1: Alarms Journal



Entries: | 1500 Journal Entries | 0 Alarms Entries out of 9552

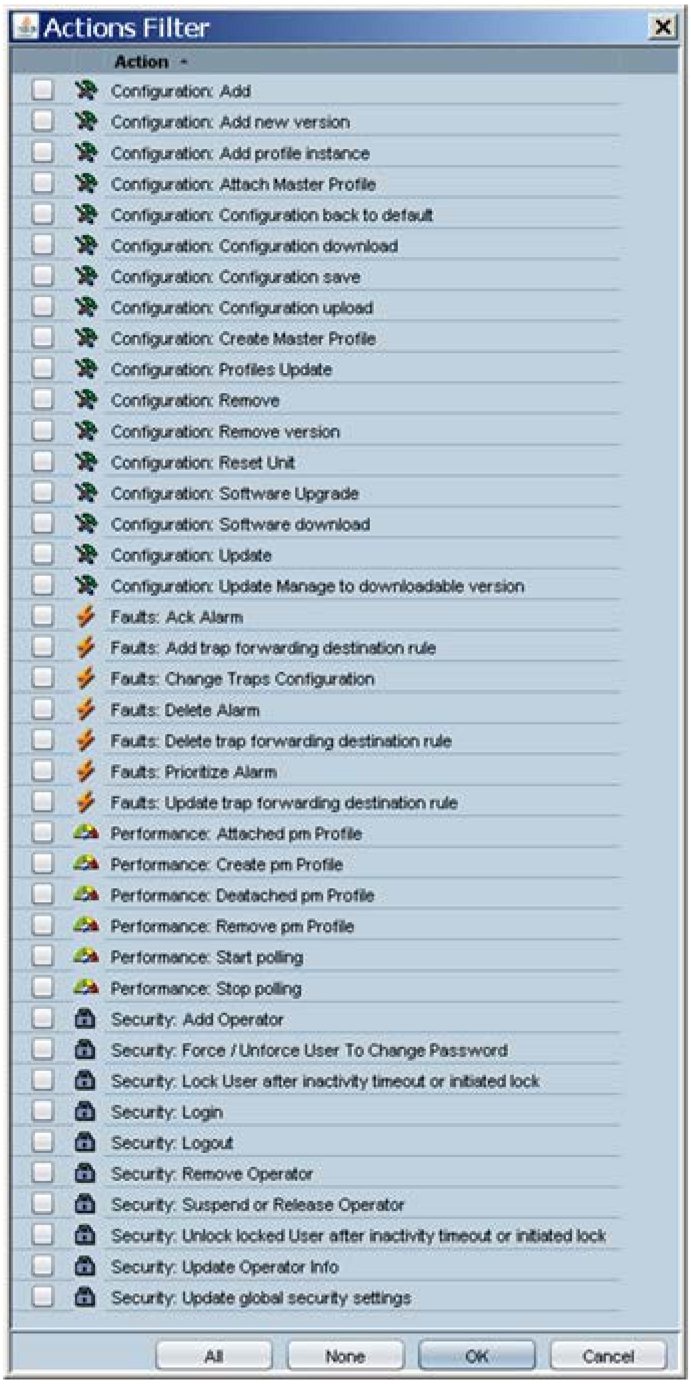
From: 08-Dec-2009 14:34 To: 15-Dec-2009 16:35

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=tgMGInfoActio...	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=tgSlotActionId ,...	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=tgSlotActionId ,...	Alex	alex
Journal	16:18:14 Dec 15 2009...	tg-lab8		Configuration: Update	Update Parameters: Field=tgAlarmManag...	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=tgConfiguration...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=tgOamSecurity...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=tgConfiguration...	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

- The Actions Journal screen enables the operator to track all actions performed by all users on all MGs in all Regions.
- The Actions Journal can be opened either by opening menu **Security** > **Actions Journal**, or by clicking the icon **Journal** on the Alarm Browser tool bar. When opening the Journal from the Alarm Browser, it's opened in the context of the Alarm Browser (Status screen).
- In addition to a context filter, available from the Alarm Browser tool bar, operators filter according to Users, Date and Time, and Action Type.
- The Actions Journal screen is read-only and non-configurable.
- Data displayed in the Actions Journal can be saved in a *csv* file.

- Following are columns displayed in the Actions Journal:
  - **Time** - date & time of the action
  - **MG Name** - the name of the MG on which the action was performed.
  - **Source** - managed object on which the action was performed, for example, 'Board#8'
  - **Action** - Action type, one of the values from the list displayed in the figure below.

Figure 37-2: Journal Actions



Actions Filter

Action

- ☐ Configuration: Add
- ☐ Configuration: Add new version
- ☐ Configuration: Add profile instance
- ☐ Configuration: Attach Master Profile
- ☐ Configuration: Configuration back to default
- ☐ Configuration: Configuration download
- ☐ Configuration: Configuration save
- ☐ Configuration: Configuration upload
- ☐ Configuration: Create Master Profile
- ☐ Configuration: Profiles Update
- ☐ Configuration: Remove
- ☐ Configuration: Remove version
- ☐ Configuration: Reset Unit
- ☐ Configuration: Software Upgrade
- ☐ Configuration: Software download
- ☐ Configuration: Update
- ☐ Configuration: Update Manage to downloadable version
- ☐ Faults: Ack Alarm
- ☐ Faults: Add trap forwarding destination rule
- ☐ Faults: Change Traps Configuration
- ☐ Faults: Delete Alarm
- ☐ Faults: Delete trap forwarding destination rule
- ☐ Faults: Prioritize Alarm
- ☐ Faults: Update trap forwarding destination rule
- ☐ Performance: Attached pm Profile
- ☐ Performance: Create pm Profile
- ☐ Performance: Deatached pm Profile
- ☐ Performance: Remove pm Profile
- ☐ Performance: Start polling
- ☐ Performance: Stop polling
- ☐ Security: Add Operator
- ☐ Security: Force / Unforce User To Change Password
- ☐ Security: Lock User after inactivity timeout or initiated lock
- ☐ Security: Login
- ☐ Security: Logout
- ☐ Security: Remove Operator
- ☐ Security: Suspend or Release Operator
- ☐ Security: Unlock locked User after inactivity timeout or initiated lock
- ☐ Security: Update Operator Info
- ☐ Security: Update global security settings

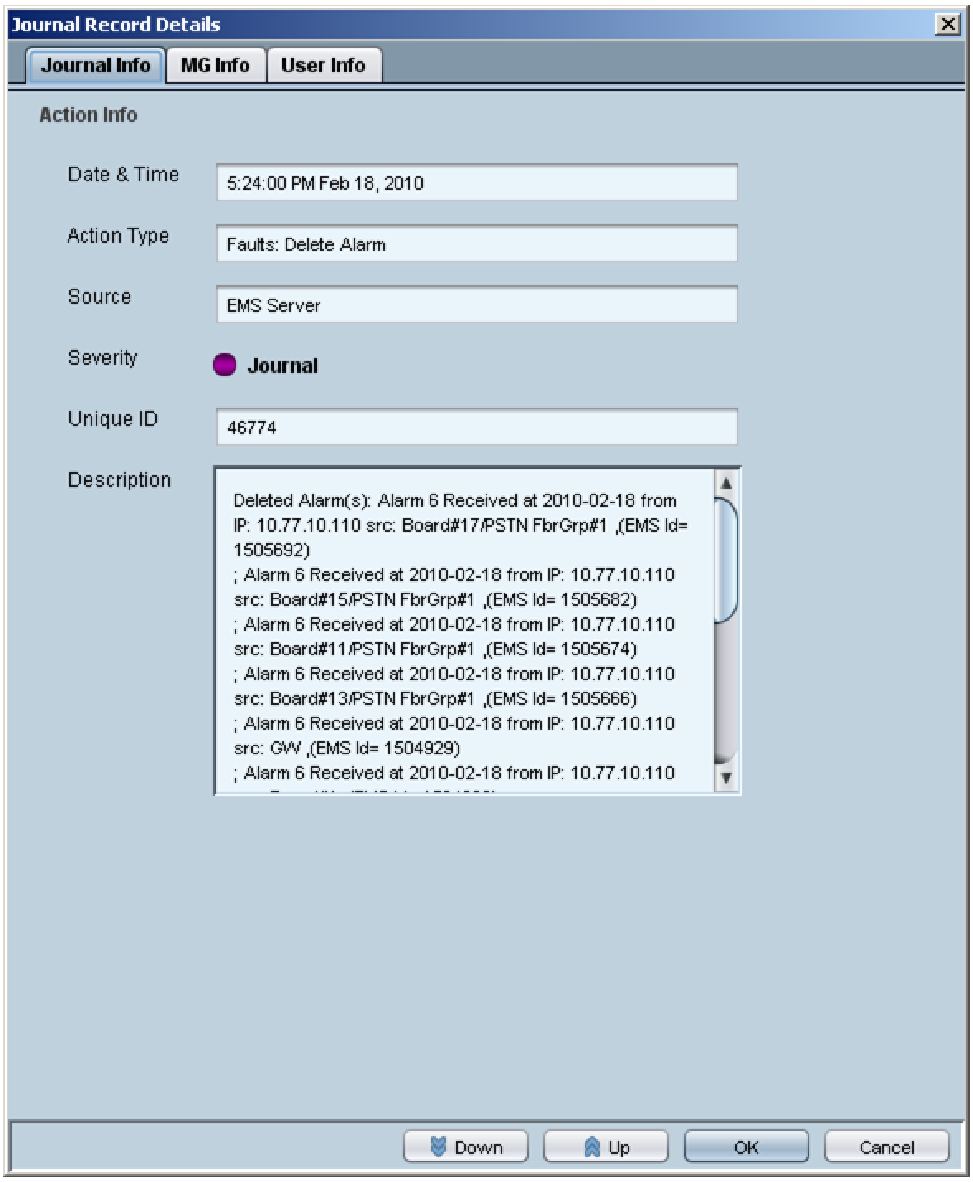
- **Details** - a precisely detailed description of the action, for example, parameter names and values for a Configuration Update action.
- **Operator** - the name of the operator who performed the action.
- **Region** - the region in which the gateway resides.

37.1 Viewing 'Journal Record Details

Users can view more details by double-clicking a row containing a Journal record and opening the 'Journal Record Details' screen. The following information is displayed in the screen:

- Journal Info

Figure 37-3: Journal Record Details - Journal Information



Action Info

Date & Time: 5:24:00 PM Feb 18, 2010

Action Type: Faults: Delete Alarm

Source: EMS Server

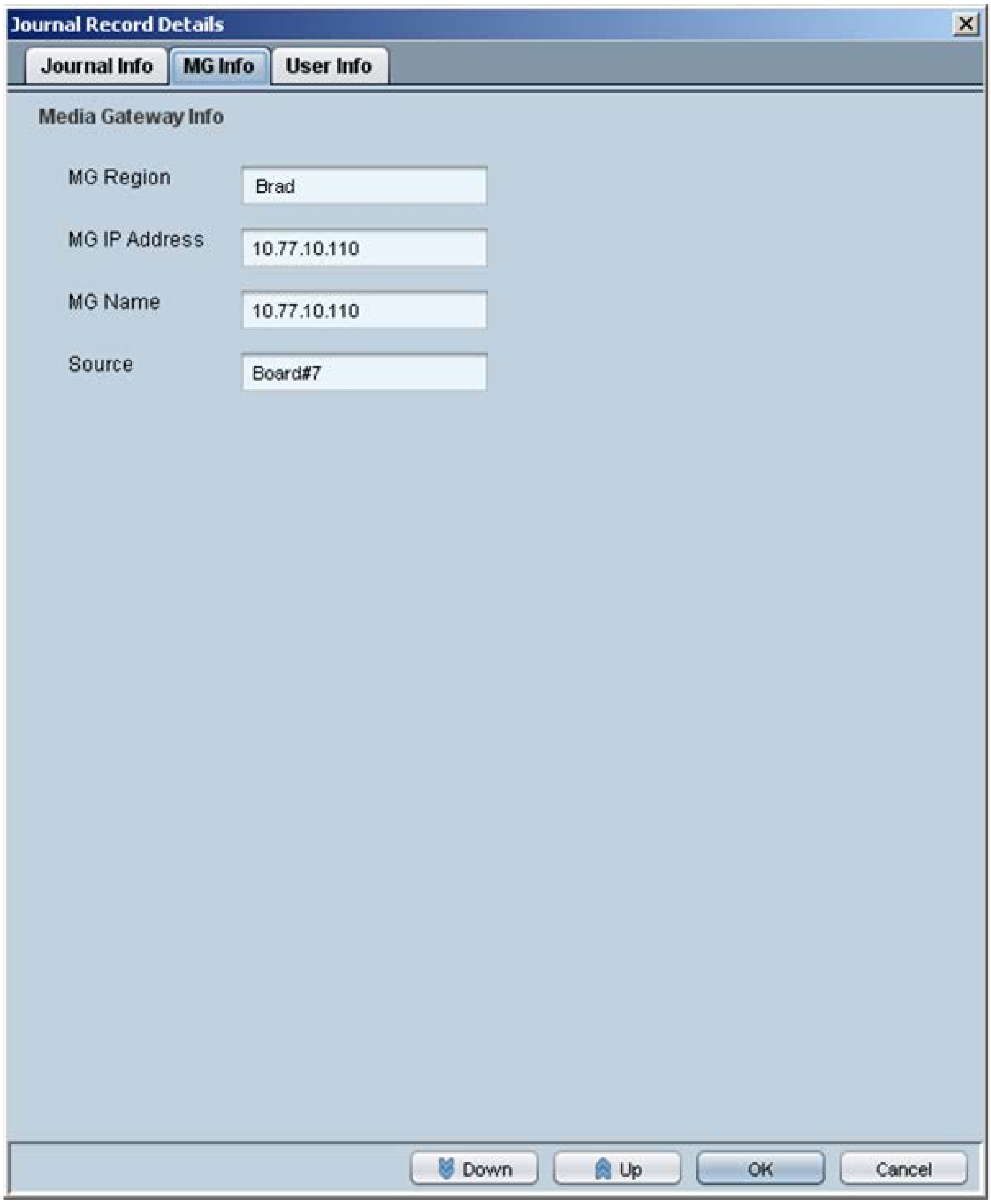
Severity: ● Journal

Unique ID: 46774

Description: Deleted Alarm(s): Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#17/PSTN FbrGrp#1 ,(EMS Id= 1505692)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#15/PSTN FbrGrp#1 ,(EMS Id= 1505682)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#11/PSTN FbrGrp#1 ,(EMS Id= 1505674)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#13/PSTN FbrGrp#1 ,(EMS Id= 1505666)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: GW ,(EMS Id= 1504929)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110

- MG Info

Figure 37-4: Journal Record Details - Media Gateway Information



MG Region: Brad

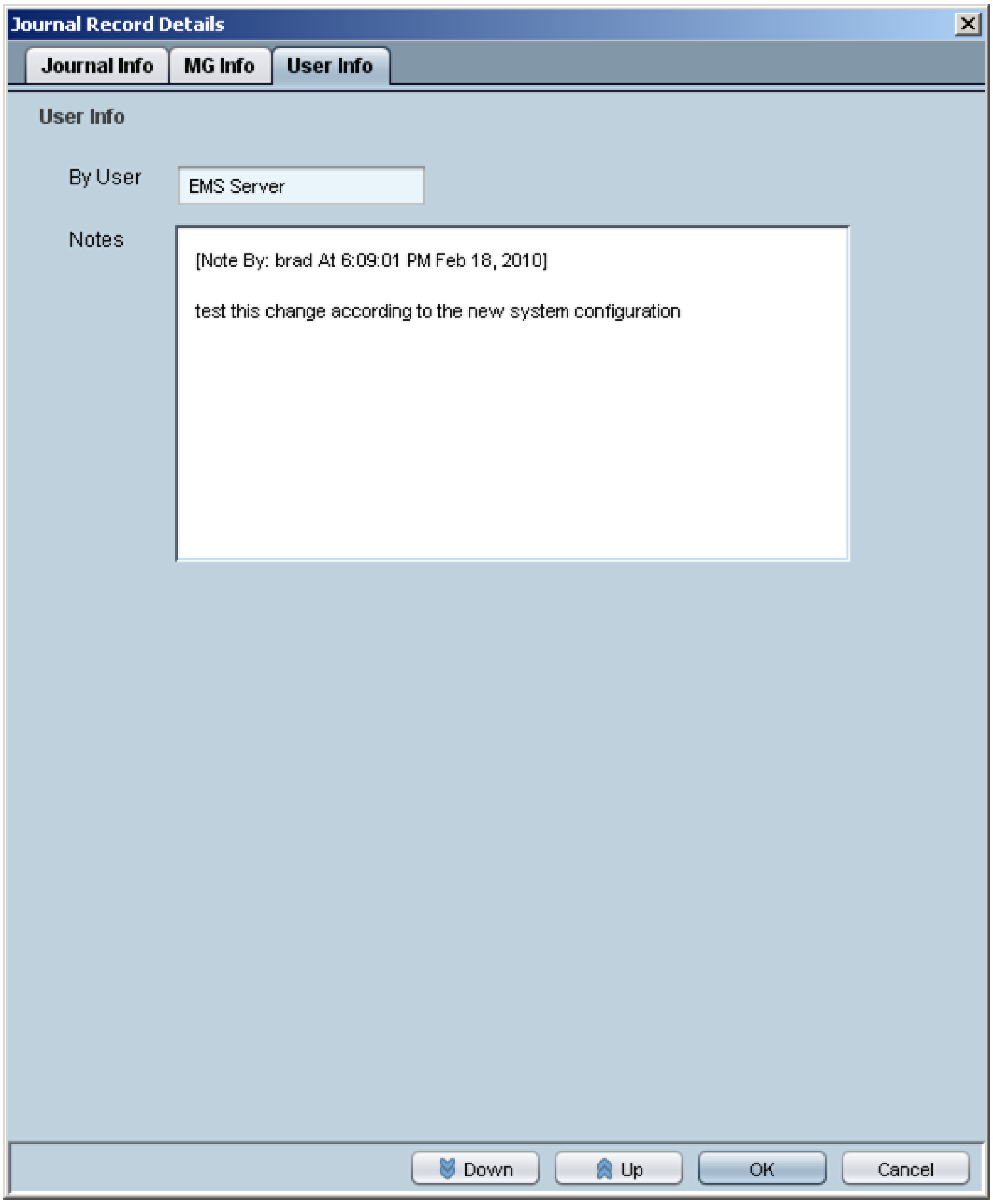
MG IP Address: 10.77.10.110

MG Name: 10.77.10.110

Source: Board#7

- User Info

Figure 37-5: Journal Record Details - User Info



By User: EMS Server

Notes:

[Note By: brad At 6:09:01 PM Feb 18, 2010]

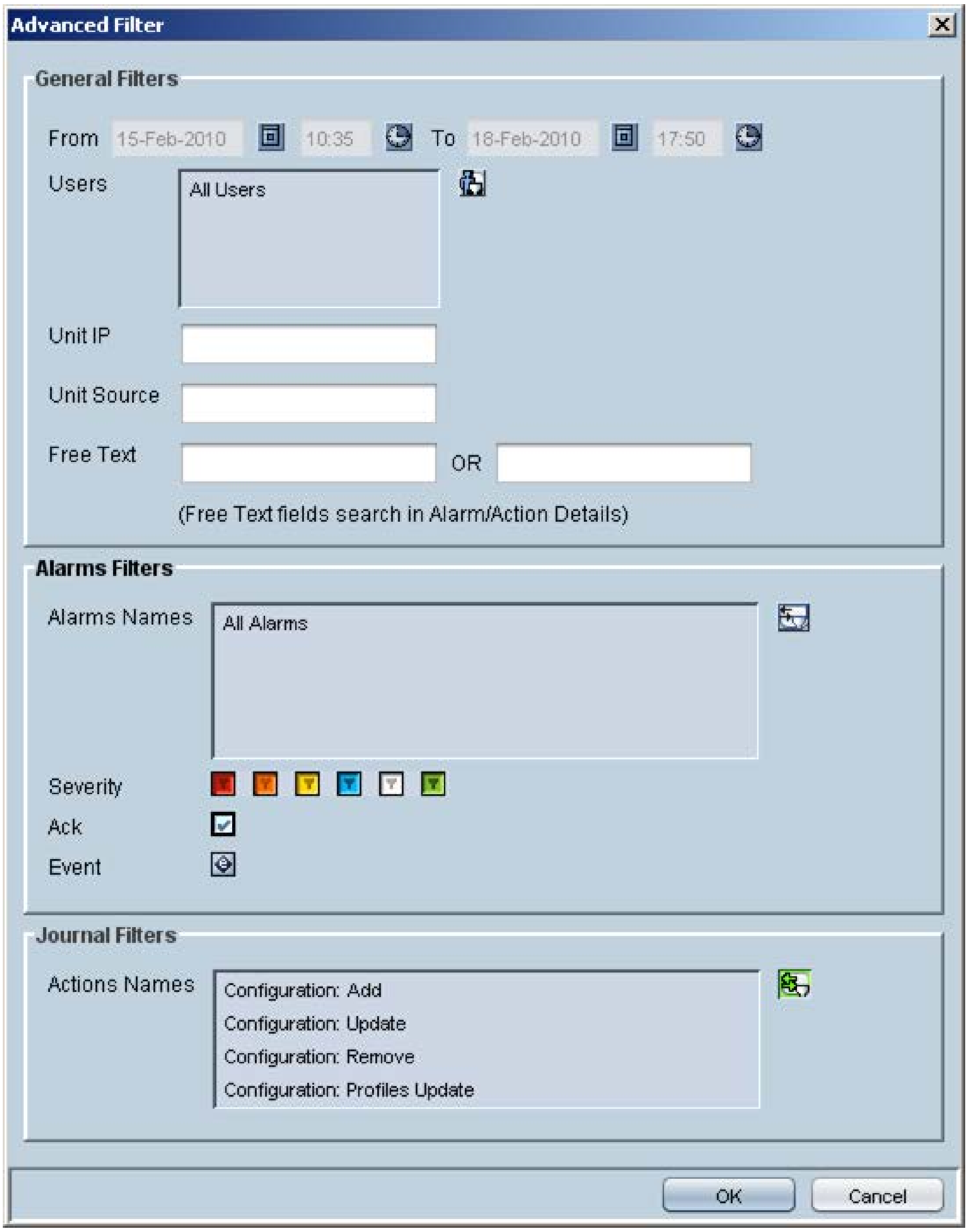
test this change according to the new system configuration

Users can insert data to be saved, together with the journal record in the Journal.

37.2 Filters Supported in the Actions Journal

The Actions Journal supports an Advanced Filter comprising the filters shown in the figure and described below. All filters can be applied simultaneously.

Figure 37-6: Filters



Advanced Filter

General Filters

From 15-Feb-2010 10:35 To 18-Feb-2010 17:50

Users: All Users

Unit IP

Unit Source

Free Text OR

(Free Text fields search in Alarm/Action Details)

Alarms Filters

Alarms Names: All Alarms

Severity

Ack ☑

Event

Journal Filters

Actions Names:
Configuration: Add
Configuration: Update
Configuration: Remove
Configuration: Profiles Update

- **General Filters**
  - Date and Time Filter
  - Users Filter. An operator can select a user or a set of users whose actions the operator needs to view.
  - Unit IP
  - Unit Source
  - Free Text 1 (searched in the Details filed)
  - Free Text 2 (searched in the Details filed)
- **Alarms Filters** (See Section 'Fault Management' on page 267)
- **Journal Filters**
  - Actions Filter (all user actions are classified according to EMS functionality):
    - Fault Management Actions (acknowledge, delete, prioritize alarms, change trap configuration)
    - Configuration Management Actions (add, remove, update managed object, software upgrade, etc.)
    - Performance Management (start, stop polling, create, attach, detach PM profile)
    - Security Management Actions (add, remove, update operator info, login, logout)

37.2.1 Example of Filter Use

This section describes how to find all parameters that were modified in September 2006 in Board#8 of a specific gateway. Apply the filters below in the 'Advanced Alarm Filter' screen:

➢ To apply the filters:

1. In the 'Date & Time' field, define 'From date' as 'September 1, 2006' and 'To date' as 'September 30 2006'.
2. In the 'Unit IP' field, define the gateway IP address or open the Journal in the appropriate context from the Alarm Browser for the parameter to automatically be defined.
3. In the 'Unit Source' field, define 'Board#8' in the field 'Unit Source' or open the Journal in the appropriate context from the Alarm Browser for the parameter to automatically be defined.
4. In the 'Journal Actions' screen, select the checkbox **Configuration: Update**.
5. Click **OK**; your Journal is filtered with all records answering your search criteria.

37.3 Saving the Data in the Actions Journal as a csv File

The results displayed in the Actions Journal can be saved as a *csv* file.

➢ **To save the data in the Actions Journal as a csv file:**

1. Apply any filters you may require.
2. Open the menu 'Security' and choose '**Save Records** as'; the 'Select File' screen opens.
3. Select a file name and location and click **OK**; your data is saved in the *csv* file, together with the filter applied (if any).

38 EMS Application Welcome Message

The Welcome Screen is displayed to the user upon successful Login information validation and is composed of Administrator defined textual message and previous Successful and Unsuccessful Login Information including Date, Time, and Login Machine IP.

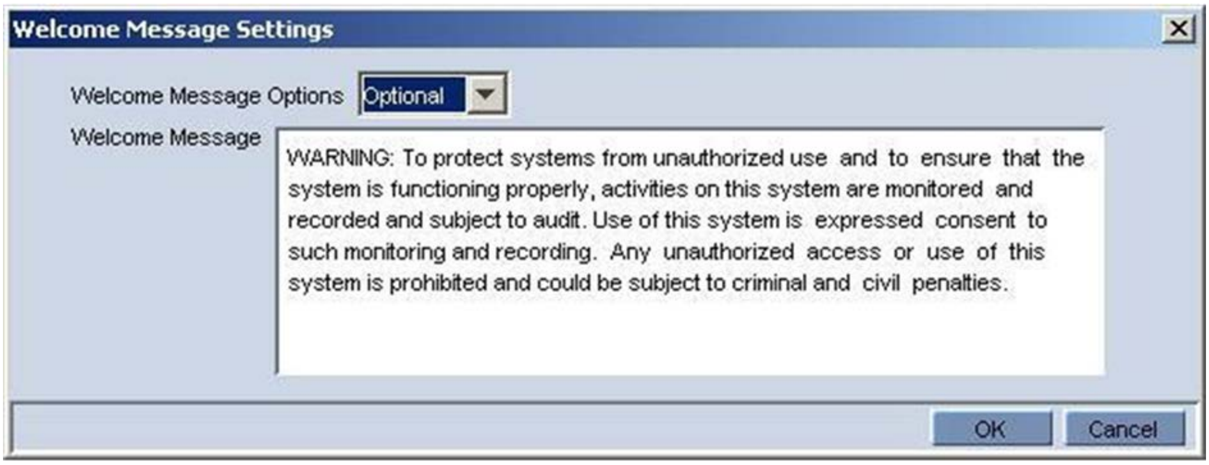
The Administrator can set a w elcome message note using the Help -> Advisory Message menu.

The Administrator can define one of the following three Welcome Message Options:

- **Mandatory** – the Welcome Message is always displayed. The Administrator can define per user if the Login Info part is displayed.
- **Optional (default)** – the Welcome Message is displayed according to definition in the Users table in the field 'Display Welcome Message'. The user can disable the Welcome Message or Login Information parts and thereby disable the entire Welcome Message starting next session.
- **Disable** – the Welcome Message is displayed with only the Login Information pane. The user can disable the Login Information part (by selecting the 'Do Not Display Login Information on the next Login' button) and thereby disable the entire Welcome Message starting next session.

  Any changes made to the Welcome Message are stored in the Actions Journal.

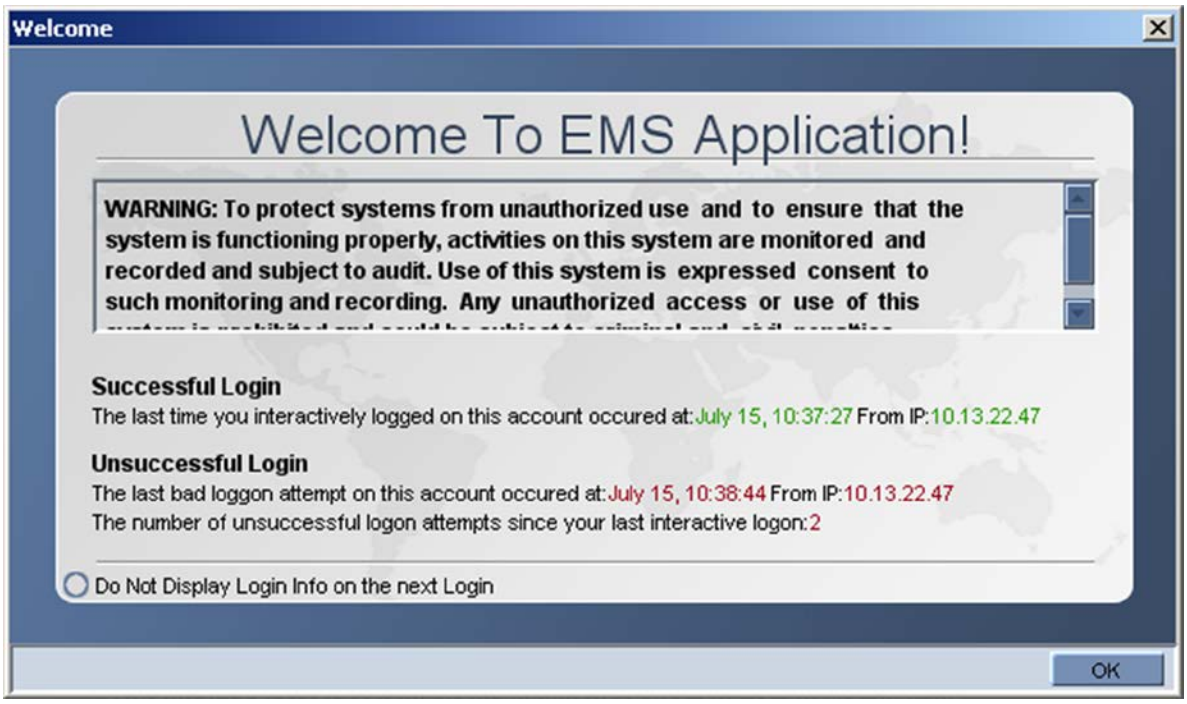
Figure 38-1: Welcome Message Settings



Welcome Message Options: Optional

WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.

Figure 38-2: Welcome Message with Login Information



Welcome To EMS Application!

WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this

Successful Login

The last time you interactively logged on this account occured at:July 15, 10:37:27 From IP:10.13.22.47

Unsuccessful Login

The last bad loggon attempt on this account occured at:July 15, 10:38:44 From IP:10.13.22.47

The number of unsuccessful logon attempts since your last interactive logon:2

○ Do Not Display Login Info on the next Login

Part VII

Troubleshooting

This section describes the various EMS troubleshooting scenarios.

39 Failure to Connect to a Media Gateway - all Media Gateways

This section describes the various scenarios that may cause a failure to connect to a media gateway.

Failure to connect to a gateway can occur in one of the following circumstances:

- When attempting to connect to a gateway for the first time
- When attempting to connect to a gateway after already having established a connection but in the interim the gateway's operation was interrupted due to an electricity surge (for example).

There are three EMS GUI indications as to a first-time connection failure:

1. Notification of the failure to connect appears in the EMS's Status pane: “*Cannot establish connection*”.
2. One of the following two question marks ❔ ❓ is displayed under the Region instead of the gateway icon, shown in the figure 'Failure to Connect to a media gateway IP Address', below.
3. When selecting the Region (London, in this example), then in the Status pane under MGs List a question mark appears and **UNKNOWN** appears under the column Product Type.

Five possible reasons for a first-time connection failure are as follows:

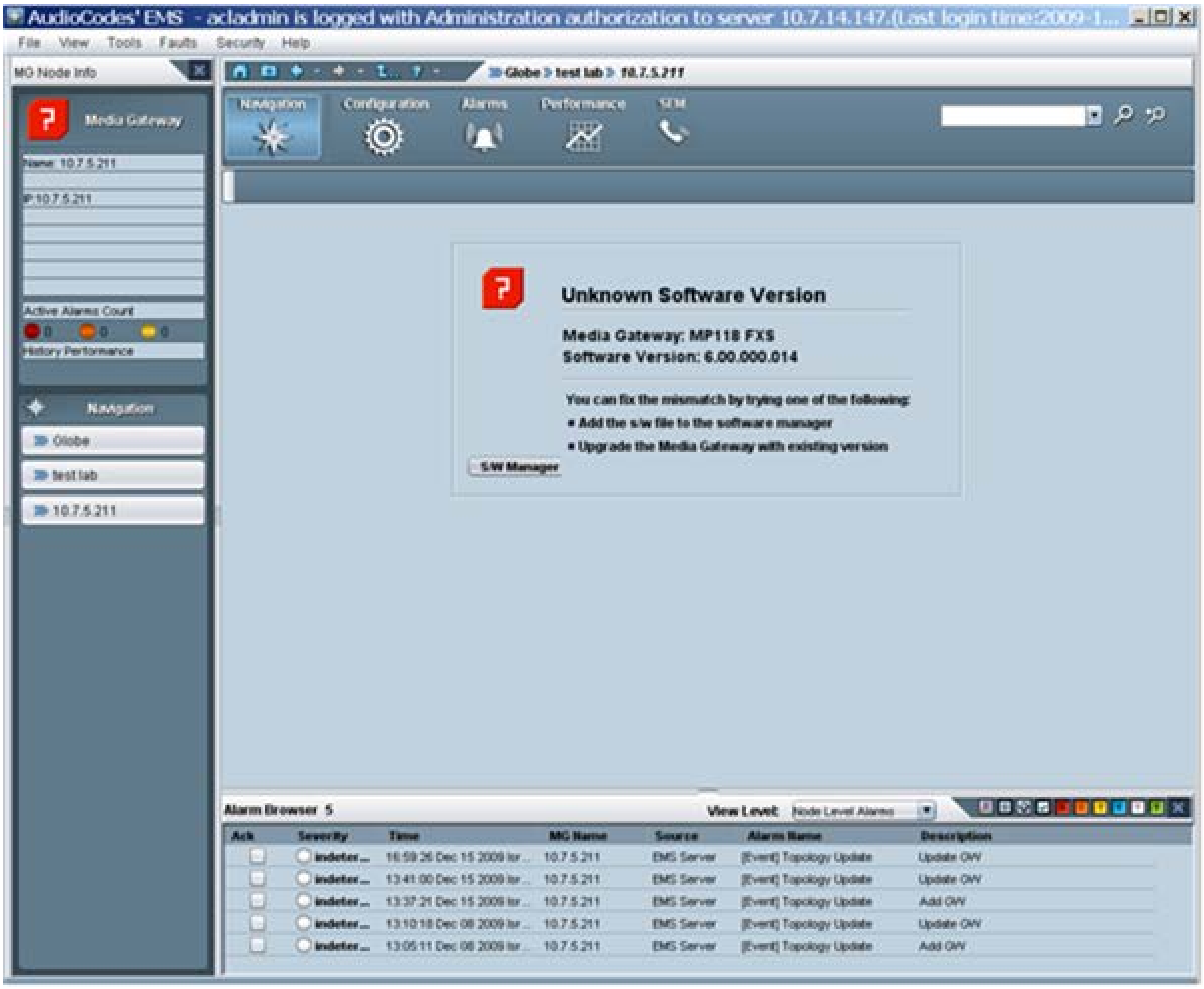
1. You've incorrectly defined the IP address of the media gateway you're attempting to connect to (in the MG Information screen; see the figure 'Incorrectly Defined MG Information Screen', below).
2. An operational problem exists in the system (lack of communication with the server, for example).
3. A network problem prevents the EMS server from connecting to the media gateway. Ping the media gateway's IP address to verify that it exists.
4. The community string is incorrect.
5. Unrecognized software version.

The table below summarizes possible first-time connection problem scenarios, the verification test that operators should perform in each scenario, and how to fix the problem.

Table 39-1: Possible First-Time Connection Problems: How to Verify Them, How to Fix Them

Possible Problem	How to Verify It	How to Fix It
Wrong media gateway IP Address defined in EMS	In the MG Tree, right-click the gateway and choose option **Details**; verify that the gateway IP address is correct.	- Delete the gateway (right-click the question-mark icon and choose the option **Remove MG**). - Add a new gateway (see Section 'Defining VoIP Devices, Managing the MG Tree' on page 77). Define the MG Information fields ensuring that the IP address for the gateway you're attempting to add (connect to for the first time) is the correct one, and that all other fields are correctly defined.
Incorrect MG SNMPv2 Read Community String defined in the EMS, or incorrect SNMPv3 info	In the MG Tree, right-click the gateway and choose option **Details**; verify that the SNMP Read and Write Community Strings are defined correctly , or when working with SNMPv3, all the SNMPv3 parameters match the Gateway definition.	Note that the factory default values for SNMP community strings are: read=public, write=private. Contact your system integrator to verify correct values.
The media gateway is not connected to the Network	In the cmd window (**Start > Run**), ping the gateway to verify that it is responding.	If the gateway isn't responding to the ping, check if there is a network problem or if the gateway is not operating.
The media gateway version is not defined in the EMS Software Manager	A message notifying you that the current gateway version is not supported by the EMS will be displayed in the status screen.	Operators can either add the missing software version to the Software Manager or load the software to the gateway of one of the EMS-supported versions.
The media gateway type is not supported by the EMS	In the 'MGs List' pane, an entry under the Product Type column is identified as UNKNOWN_XXX (where XXX is the product description returned by the gateway).	Contact Customer Support.

Figure 39-1: Incorrectly Defined MG Information Screen


AudioCodes' EMS - acladmin is logged with Administration authorization to server 10.7.14.147.(Last login time:2009-1...
File View Tools Faults Security Help
MG Node Info
Media Gateway
Globe > test lab > 10.7.5.211
Navigation Configuration Alarms Performance SEM
Active Alarms Count
History Performance
Navigation
Globe
test lab
10.7.5.211
S/W Manager
View Level: Node Level Alarms

Name: 10.7.5.211

IP 10.7.5.211

Unknown Software Version

Media Gateway: MP118 FXS

Software Version: 6.00.000.014

You can fix the mismatch by trying one of the following:

- Add the s/w file to the software manager
- Upgrade the Media Gateway with existing version

Alarm Browser 5

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	○ indeter...	16:59:26 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:41:00 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:37:21 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Add GW
□	○ indeter...	13:10:18 Dec 08 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:05:11 Dec 08 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Add GW

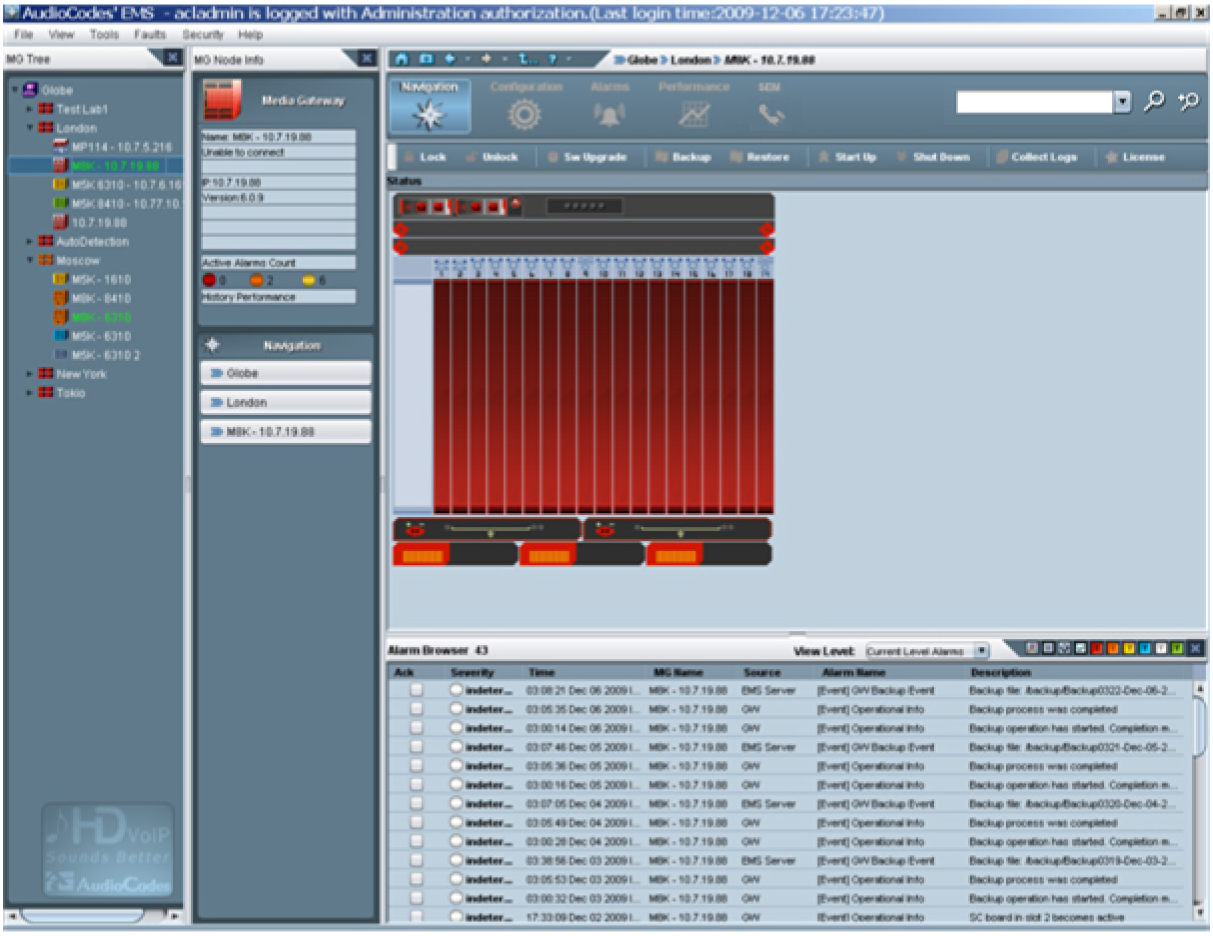
39.1 Failure to Reconnect to a Previously-Connected Media Gateway whose Operation was Interrupted

This section describes the various scenarios that may cause a failure to reconnect to a previously-connected media gateway whose operation was interrupted.

There are three EMS GUI indications as to a failure to reconnect to a gateway that was previously connected but whose operation has been subsequently interrupted:

- A red icon of a gateway is displayed under the Region and in the Status pane (when the Region is selected).
- A media gateway color-coded red is displayed in the Status pane (after double-clicking the icon color-coded red in the MGs List).
- The Status pane's navigation buttons are disabled, shown in the figure below.

Figure 39-2: Failure to Reconnect to a Media Gateway Whose Operation was Interrupted



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-06 17:23:47)

Name: M8K - 10.7.19.88
Unable to connect
IP:10.7.19.88
Version:6.0.9
Active Alarms Count
● 0 ● 2 ● 6
History Performance

Alarm Browser 43 View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	○ indeter...	03:08:21 Dec 06 2009 I...	M8K - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0322-Dec-06-2...
□	○ indeter...	03:05:35 Dec 06 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	○ indeter...	03:00:14 Dec 06 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	○ indeter...	03:07:46 Dec 05 2009 I...	M8K - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0321-Dec-05-2...
□	○ indeter...	03:05:36 Dec 05 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	○ indeter...	03:00:16 Dec 05 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	○ indeter...	03:07:05 Dec 04 2009 I...	M8K - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0320-Dec-04-2...
□	○ indeter...	03:05:49 Dec 04 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	○ indeter...	03:00:28 Dec 04 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	○ indeter...	03:38:56 Dec 03 2009 I...	M8K - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0319-Dec-03-2...
□	○ indeter...	03:05:53 Dec 03 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	○ indeter...	03:00:32 Dec 03 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	○ indeter...	17:33:09 Dec 02 2009 I...	M8K - 10.7.19.88	GW	[Event] Operational Info	SC board in slot 2 becomes active

The table below summarizes possible reconnection (following disconnection) problem scenarios, the verification test that operators should perform in each scenario, and how to fix the problem.

Table 39-2: Possible Reconnection Problems: How to Verify Them, How to Fix Them

Possible Problem	How to Verify It	How to Fix It
Network Problems	Network problems can occasionally interrupt valid and quick EMS Client / EMS Server / media gateway communication.	Refresh by pressing F5 or View > Refresh. If the EMS cannot reestablish connection with the media gateway, ping the media gateway from the EMS client or EMS server.
Invalid modification of Community Strings	If you changed the Read Community String (SNMPv2) or SNMPv3 parameters to an invalid value, the EMS will not be able to connect to the media gateway again. (SNMP error 22 – Timeout) will be constantly received.	Verify in the EMS's Users Journal that the media gateway Community Strings (SNMPv2) or SNMPv3 parameters were changed. Verify that the media gateway is up and running and you're able to connect it via PING and MIB Browser. Fix the community string problem
MG has failed and is not responding	The media gateway is not responding to ping requests.	Refer to the sections on troubleshooting the media gateway.

Note:

- A media gateway (that was previously connected but whose operation has been interrupted) is **automatically reconnected** by the system when its operation resumes.
- There is no need to attempt to *manually* add a new media gateway, as was the case with a first-time connection failure.

39.2 Information Required when Contacting Technical Support

- When contacting AudioCodes Technical Support (refer to the title page or last page of this manual for detailed contact information), send the following information:
  - A description of the system configuration - including the number and type of media gateway boards, network configuration, signaling protocols being used, exact software version, and the S/N of the failed module.
  - A detailed description of the problem, including screen shots when applicable.
  - Any information obtained from the troubleshooting process, suspected components, captured network traces, etc.
  - Information on any changes recently made to the system and its environment, i.e., to the system configuration, networking changes, etc.
  - EMS server machine – the output of the Collect Log commands from the EMS Server Manager.
- EMS Client Logs is located at the following path:

  <EMS Server installation folder>\EMS_Client_Files\Logs

40 Index

AudioCodes™ Element Management System (EMS)

User's Manual

AudioCodes

www.audiocodes.com