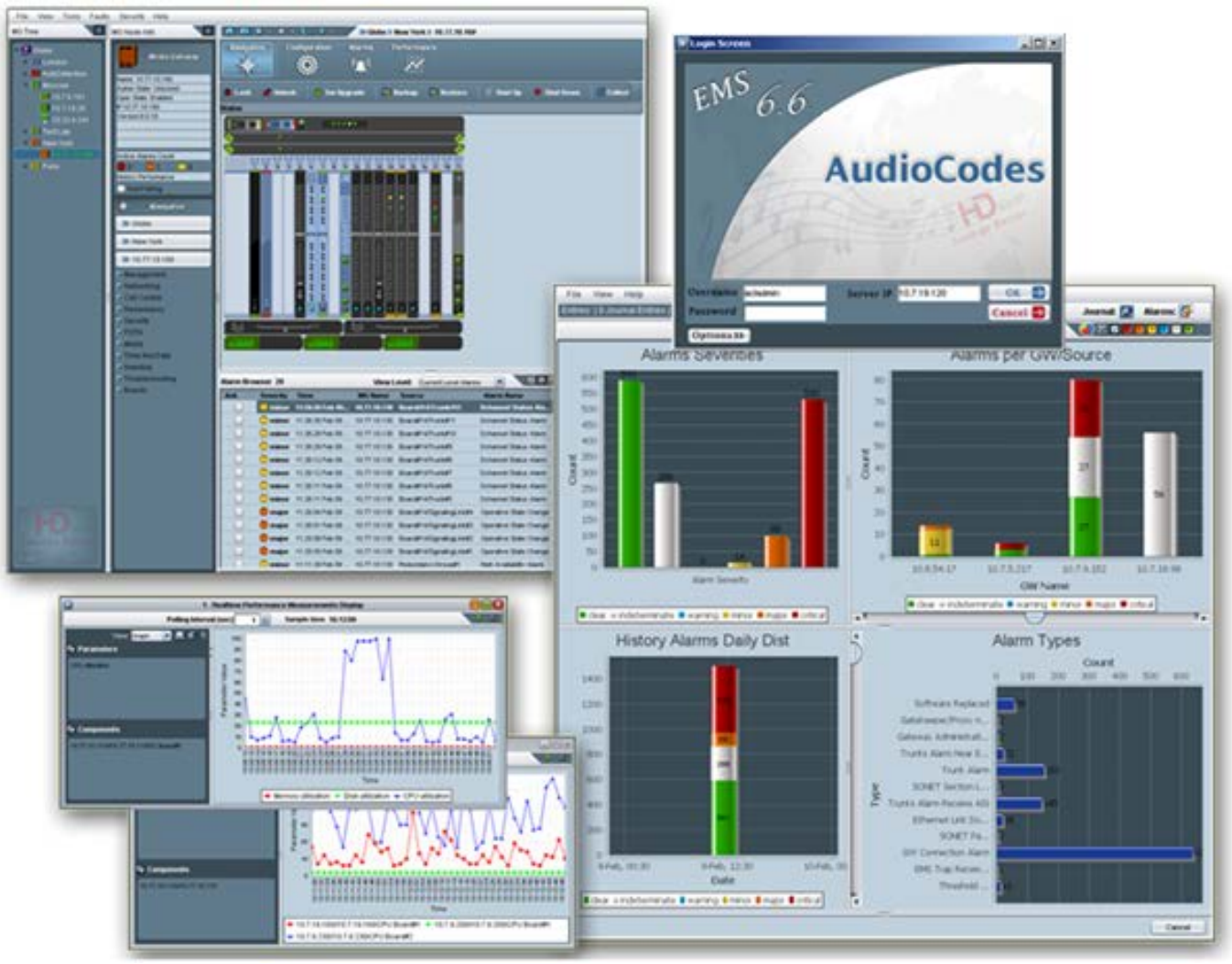
EMS for AudioCodes Media Gateways and Servers

EMS Element Management System

User's Manual

Version 6.6



AudioCodes

Table of Contents

List of Figures

List of Tables

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: March-23-2015

Note: The EMS supports the following products:

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

Trademarks

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
91022	Initial document release for Version 6.6.
91025	Correction for SEM monitored devices; the Mediant 3000 can only be monitored for SIP gateways.

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.

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

1 Introducing the AudioCodes Element Management System

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

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

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

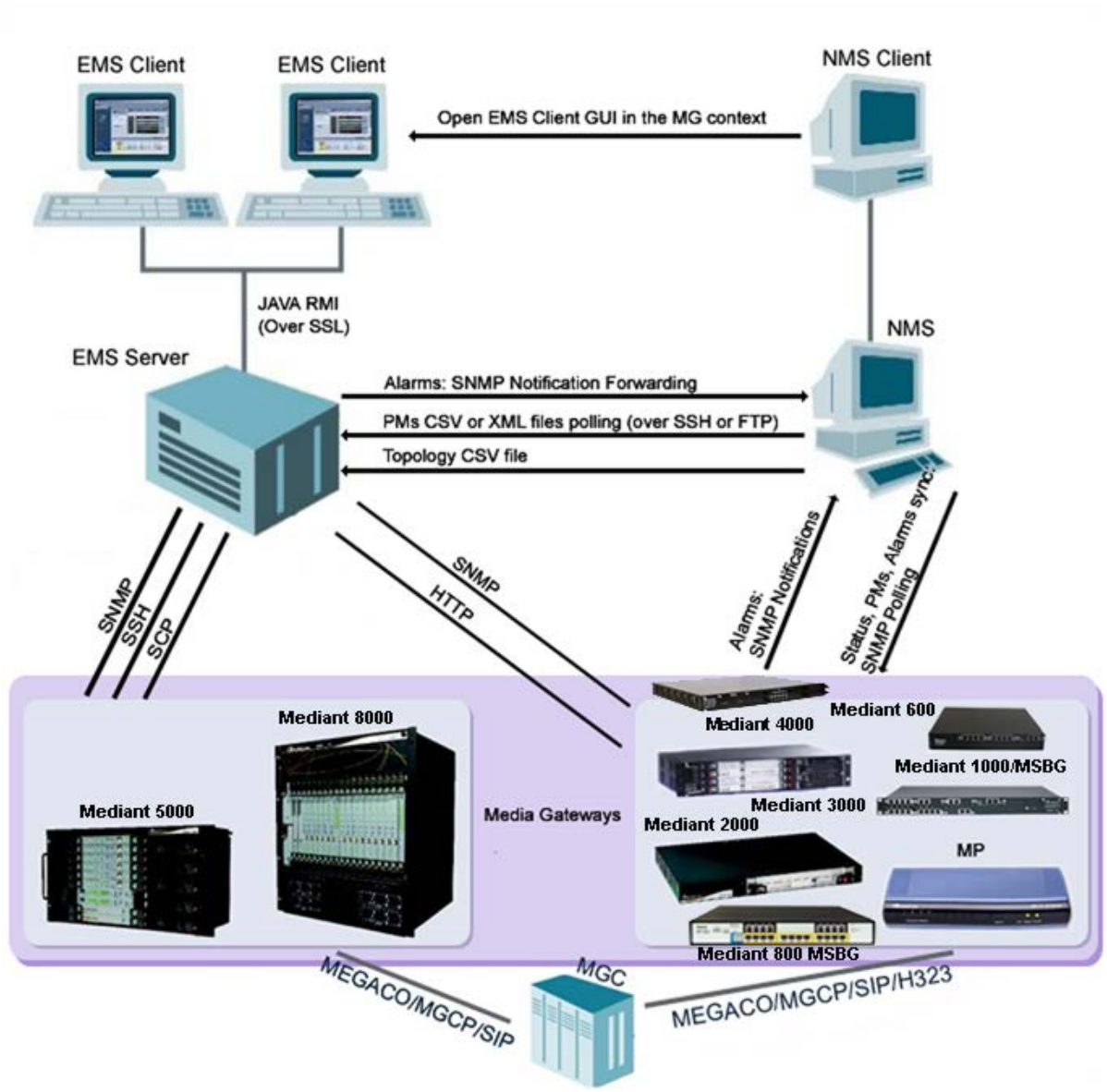
1.1 EMS within the Network

The Element Management System (EMS) is an advanced solution for standards-based management of media gateways within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM and P) of the AudioCodes' families of media gateways; the digital Mediant Series, Mediant 2600 E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant 5000 and Mediant 8000 media gateways; Mediant 800 MSBG, Mediant Analog and Digital Gateway and E-SBC; Mediant 850 MSBG, Mediant 600 and Mediant 1000 Analog and Digital Gateway and E-SBC; Mediant 1000 MSBG analog and digital gateway and analog MediaPack VoIP media gateways.

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

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.

1.2 Specifications

- Software Version Number: 6.6
- Release Date: Q4 2012
- 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.

1.3 Supported VoIP Equipment

This section provides a brief description of the different supported VoIP equipment.

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 800 MSBG  **Mediant 1000 MSBG** 	These Multi-Service Business Gateways (MSBG) are networking devices that combine multiple service functions such as a media gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server. 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

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
	as IP-PBX, Call Center, and Conferencing. (Refer to the product documentation for detailed information).
 **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 flexible, from a single trunk per module all the way to a single module with all 4 trunks) or as a purely analog configuration, supporting up to 24 analog ports (6 modules with 4 ports on each).
 **Mediant 1000 Gateway and E-SBC**	The Mediant 1000B Gateway and 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 provides SBC functionality as well as voice-over-IP (VoIP) media gateway 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, as well as flexible PSTN and legacy PBX connectivity.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 800 Gateway and E-SBC**	The Mediant 800 Gateway and 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 provides SBC functionality as well as voice-over-IP (VoIP) media gateway 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, as well as flexible PSTN and legacy PBX connectivity.
 **Mediant 850 MSBG**	The Mediant 850 Multi-Service Business Router (MSBR) is a networking device that combines 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 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, as well as flexible PSTN and legacy PBX connectivity.
 **Mediant 600 Media Gateway**	The Mediant 600 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**	The Mediant 2000 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 2600 E-SBC**	The Mediant 2600 Enterprise Session Border Controller (E-SBC), is a member of AudioCodes family of E-SBC products, 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 3000**	The Mediant 3000 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; Voice Coders: 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 fallback 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).
 **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; Voice Coders: include

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
	G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fallback 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).
 **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 4000 E-SBC Media Gateway**	AudioCodes' Mediant 4000 E-SBC (hereafter referred to as *device*) 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.

1.4 Managed Devices for All EMS Server Versions

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

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

1.5 SEM Monitored Devices

The following lists the devices monitored by the SEM:

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

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

1.6 EMS System Requirements

The table below describes the platform and software required to run the EMS.

Table 1-4: EMS- Minimal Platform Requirements

Resource	EMS Server			EMS Client
	Dedicated EMS Server – Solaris OS	**Dedicated EMS Server - Linux OS**	**VMware vSphere– Linux OS**	
Hardware	▪ Sun™ Fire™ V240[1] ▪ Sun™ Fire™ V215[1] ▪ Sun™ Netra™ T2000[2] ▪ Sun Netra T5220[1]	▪ HP DL360 G6		Monitor resolution: 1152*864 or higher
Operating System	Solaris™ 64-bit, version 10, Rev 7	Linux CentOS 64-bit, kernel version 5.3, Rev4	Linux CentOS 64-bit, kernel version 5.3 Rev4,	Windows™ 2000 / XP/ Vista/7
Memory	1 GB RAM	2 GB RAM	2 GB RAM	512 MB RAM
Disk space	▪ 73 GB for: ✓ Sun™ Fire™ V240 ✓ Sun™ Fire™ V215 ✓ Sun™ Netra™ T2000 ▪ 300 GB for: ✓ Sun Netra T5220	✓ 146 GB	Three configurations are available: ▪ Small – 60 GB ▪ Typical – 85 GB ▪ Large – 120 GB	300 MB
Processor	UltraSPARC IIIi 1-1.5 GHz	Intel Xeon E5504 (4M Cache, 2.00 GHz)	1 core not less than 2 GHz	600 MHz Pentium III or higher
Swap space	2 GB	4 GB	4 GB	1 GB
DVD-ROM	Local			

[1] Version 6.6 on Sun Solaris platforms is available for selected customers with approval from AudioCodes Product Management.

[2] Rev 7 is the recommended OS Revision for all Solaris Hardware platforms with the exception of the Sun™ Netra™ T2000 platform, which is released with OS Revision 6 only.

- The Network Bandwidth requirements per Media gateway are as follows:
  - 500 Kb/sec for faults, performance monitoring, provisioning and maintenance actions.
  - 20 Mb/sec for Mediant 5000 / 8000 Online Software Upgrade
- The working space requirements on the EMS server are as follows:
  - Solaris: Executable tcsh and X Server and Window Manager
  - Linux: Executable bash
- The EMS server works with the JDK version 1.6 (JDK 1.6 for Solaris™, JDK 1.6 for Linux™). The EMS client works with the JDK version 1.6 for Windows™.

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

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 253
- 'Configuration management' on page 73
- Accounting (managed by a higher-level management system such as an NMS)
- 'Performance Management' on page 295
- 'Security Management' on page 405

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 images and rebuilding 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*.

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.

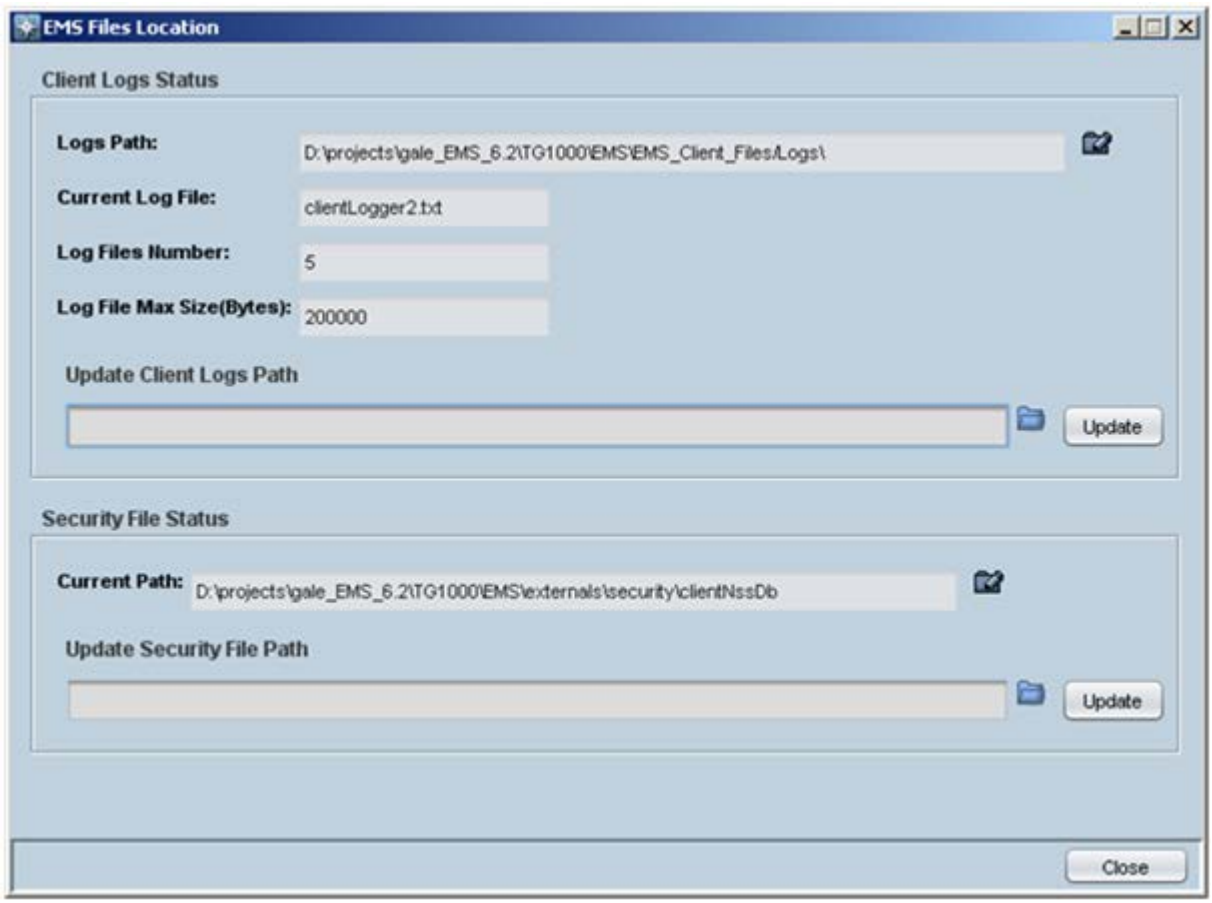
➢ **To install the EMS from the supplied DVD:**

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



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=no matter&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

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

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

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

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

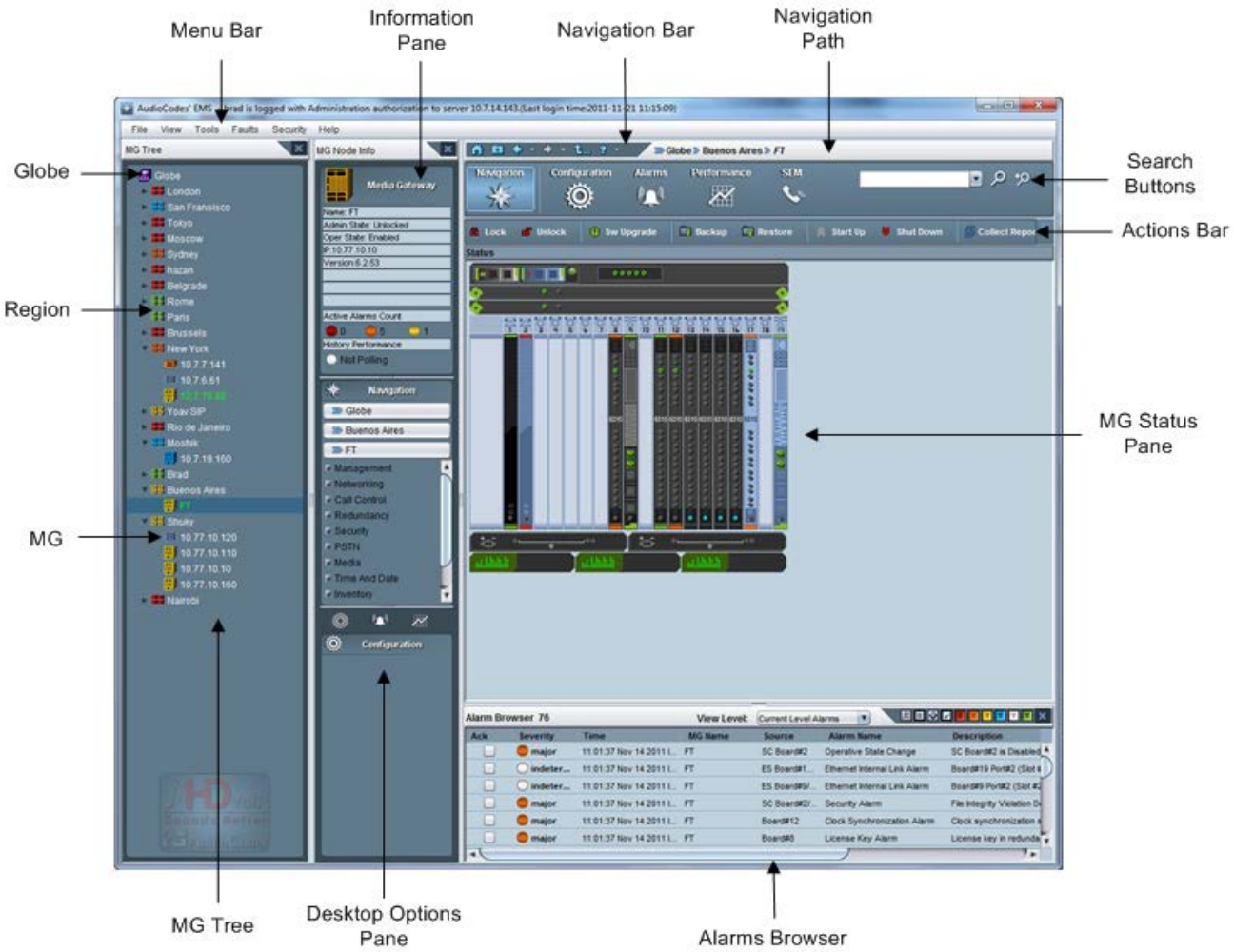
This subsection acquaints operators with the EMS. Read this section to quickly orient yourself to navigating in the EMS. The section explains the following:

- 'Navigating Down and Up System Hierarchy' on page 51.
- 'Selecting an Interface in the Context of an Element' on page 56 (and the concept of context-oriented screens).
- 'Using Color Coding to Assess Element Status' on page 58.

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 253.

- **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 295.

- **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 319.

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 136. 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 element 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.

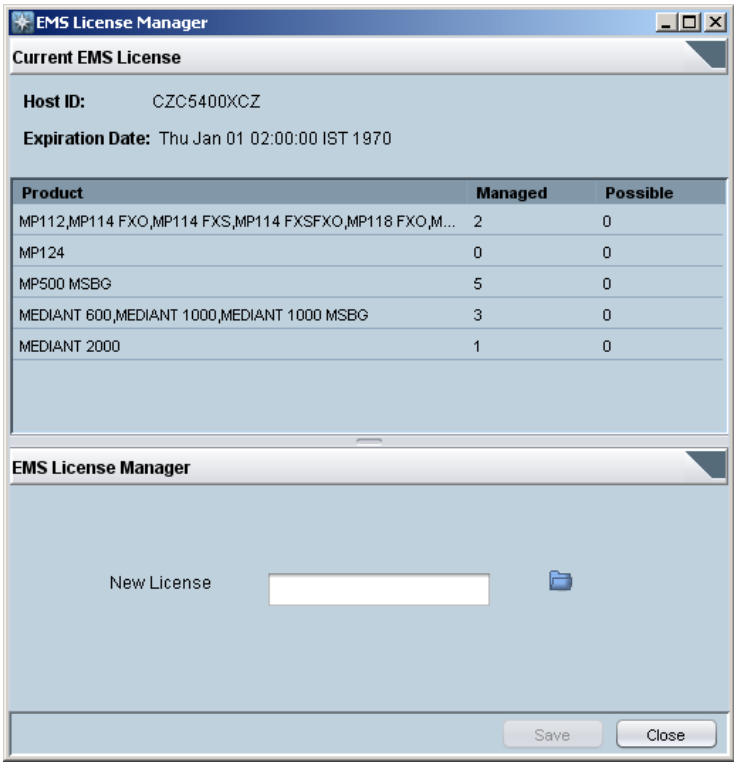
4.1 Viewing your Current License Key

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



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:

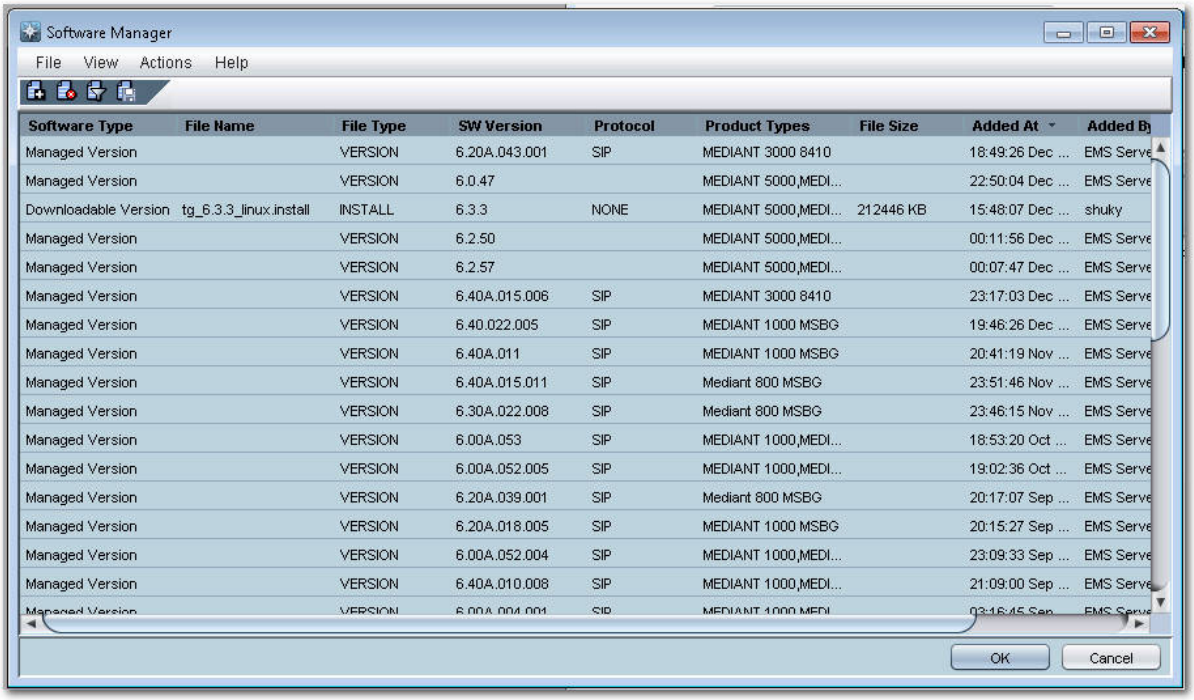
- **Software Type**

  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



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

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):

      MP-11x

      MP-124

      Mediant 600

      Mediant 800 MSBG

      Mediant 800 Gateway and E-SBC

      Mediant 850 MSBG

      Mediant 1000

      Mediant 1000 Gateway and E-SBC

      Mediant 1000 MSBG

      Mediant 2000

      Mediant 2600 E-SBC

      Mediant 3000

      Mediant 4000 E-SBC
    - Select a protocol from the list:

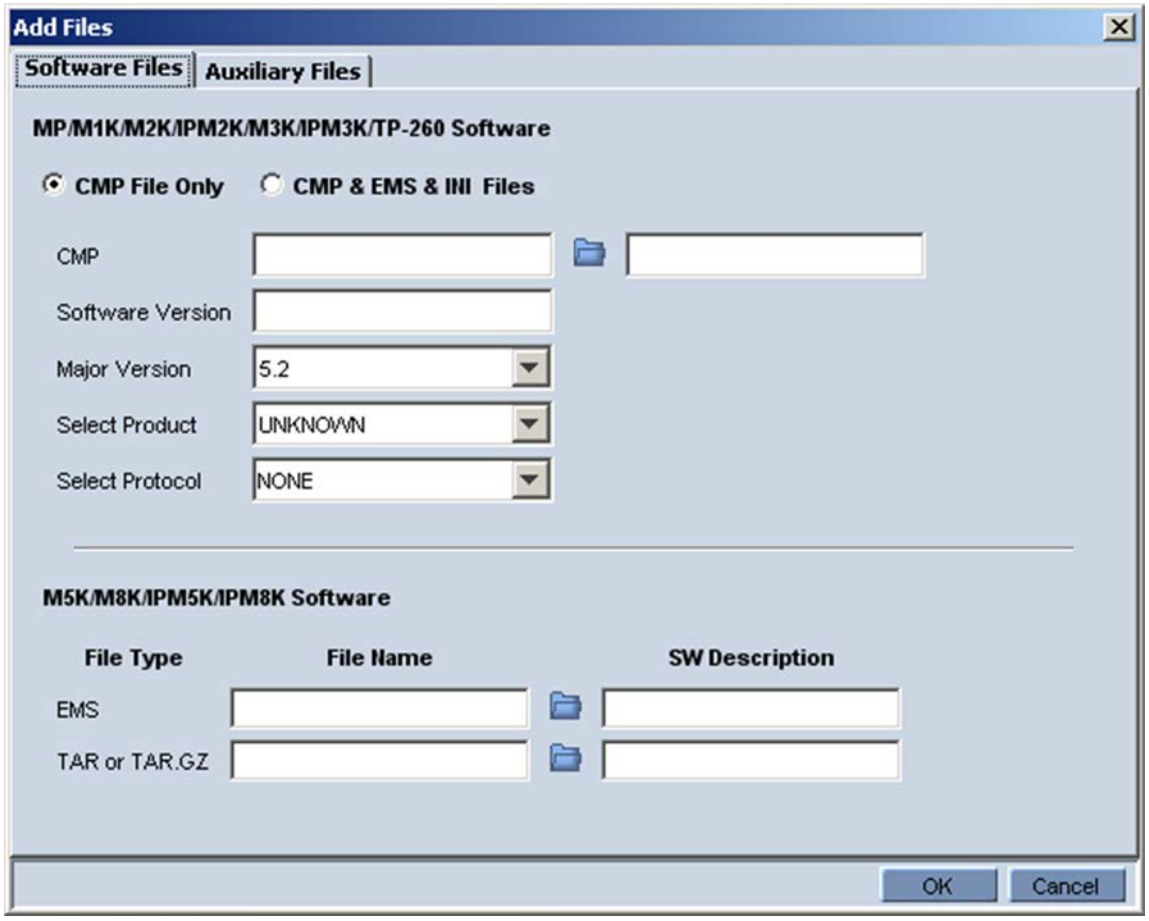
      MGCP

      MEGACO

      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



- 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

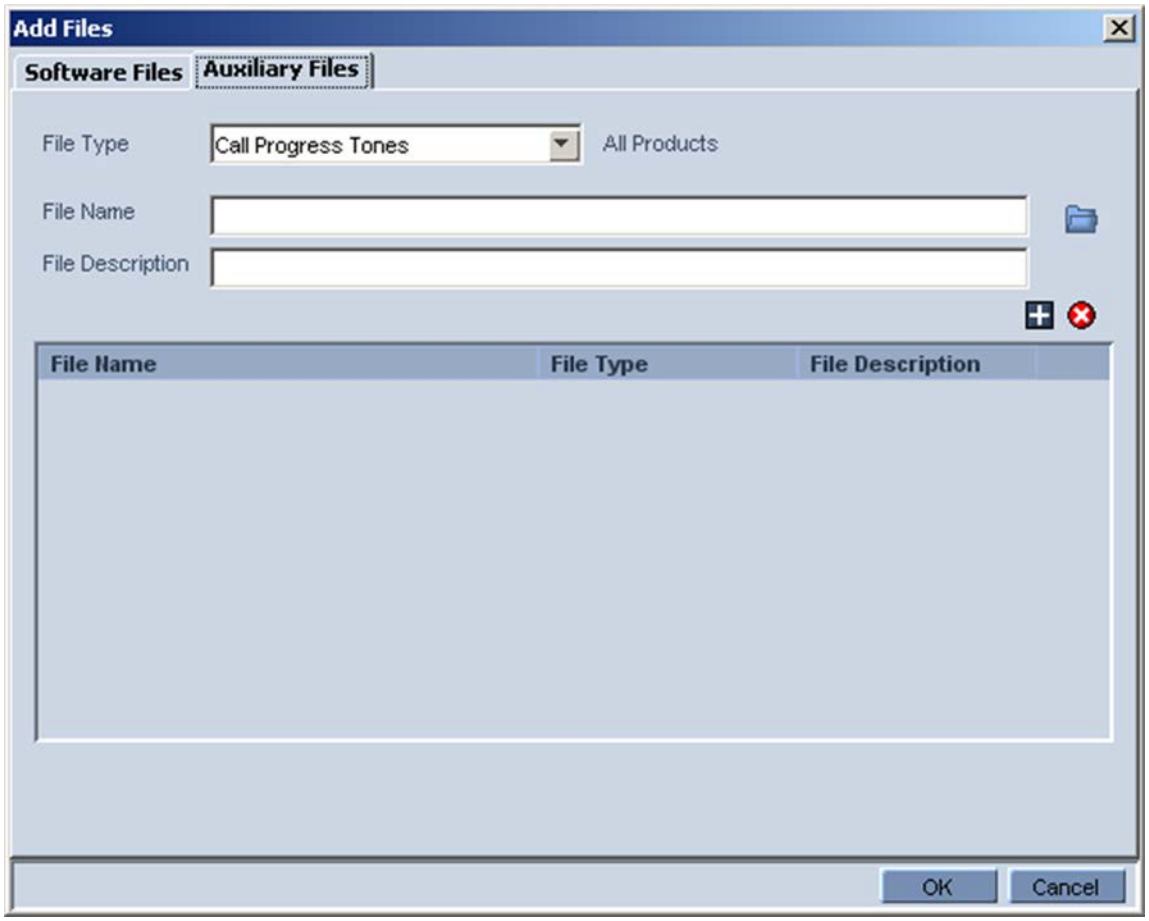


Table 5-1: Auxiliary Files

File Type	MediaPack (Analog Gateway)	Digital and Analog 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)	Digital and Analog 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	-	MSBG 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 235. 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 MSBG and Mediant 1000 MSBG 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
```

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

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**.

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 region to another and how to remove it from the EMS.

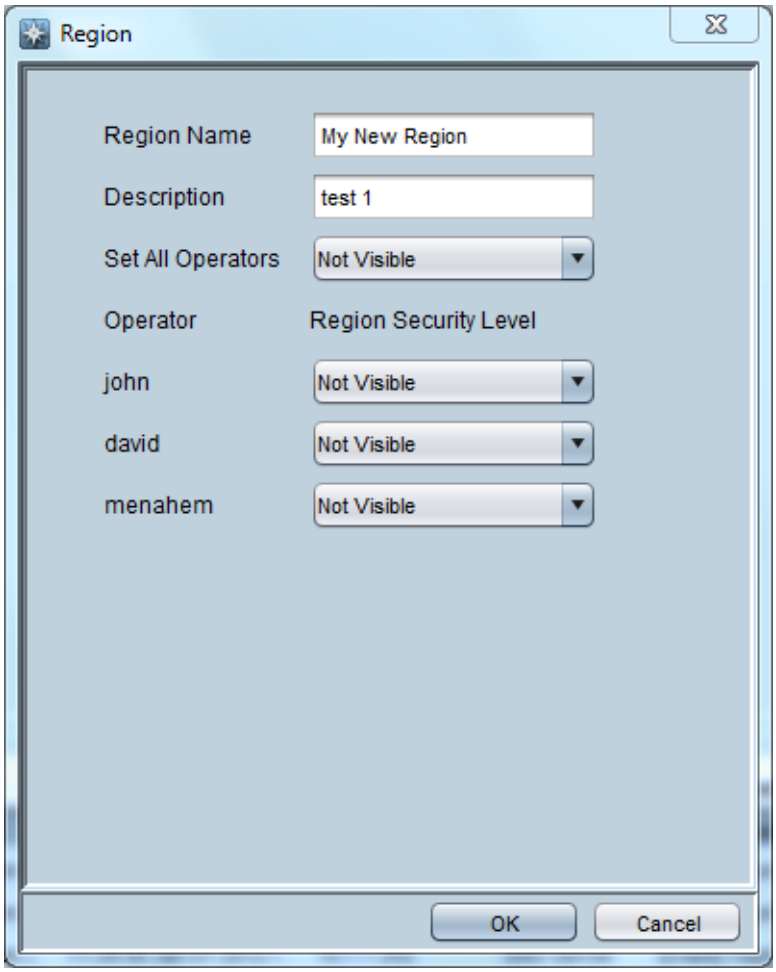
6.1 Configuring a Region

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



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

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.

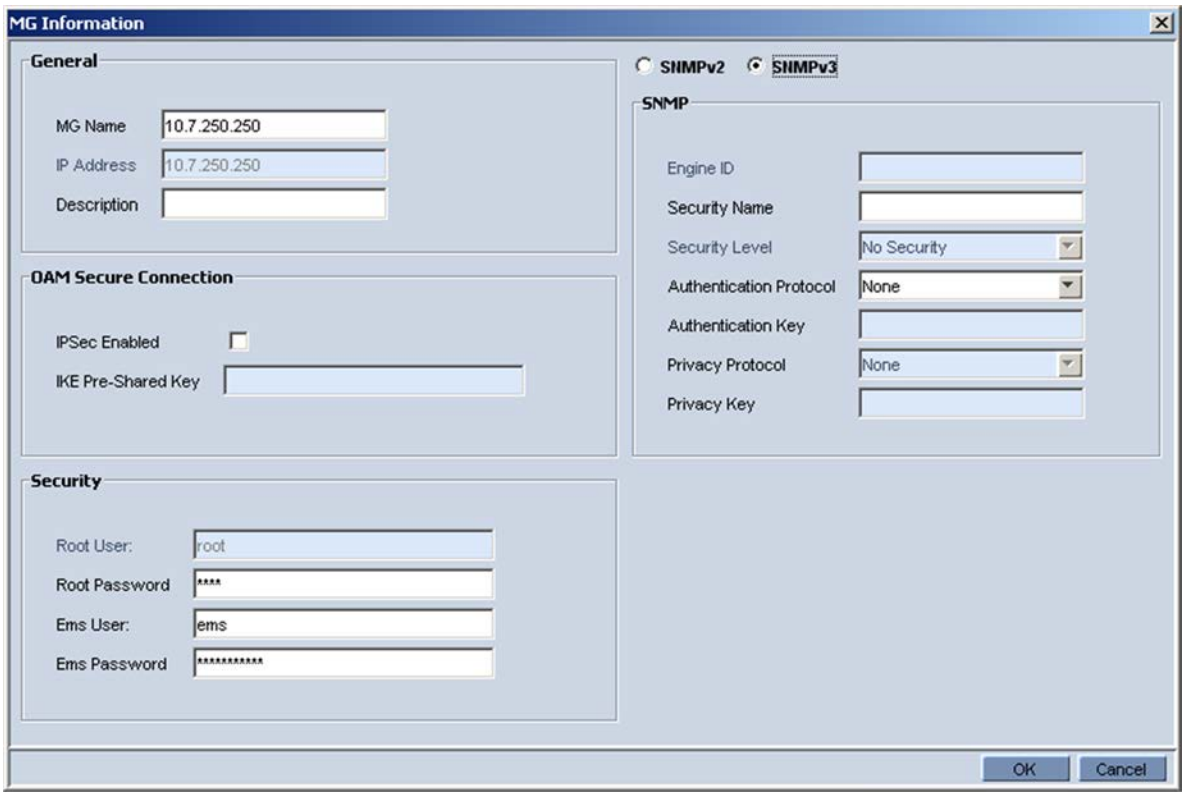
If you selected SNMPv3, the following screen is displayed:

Figure 6-3: MG Information- SNMP3

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 453 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



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.

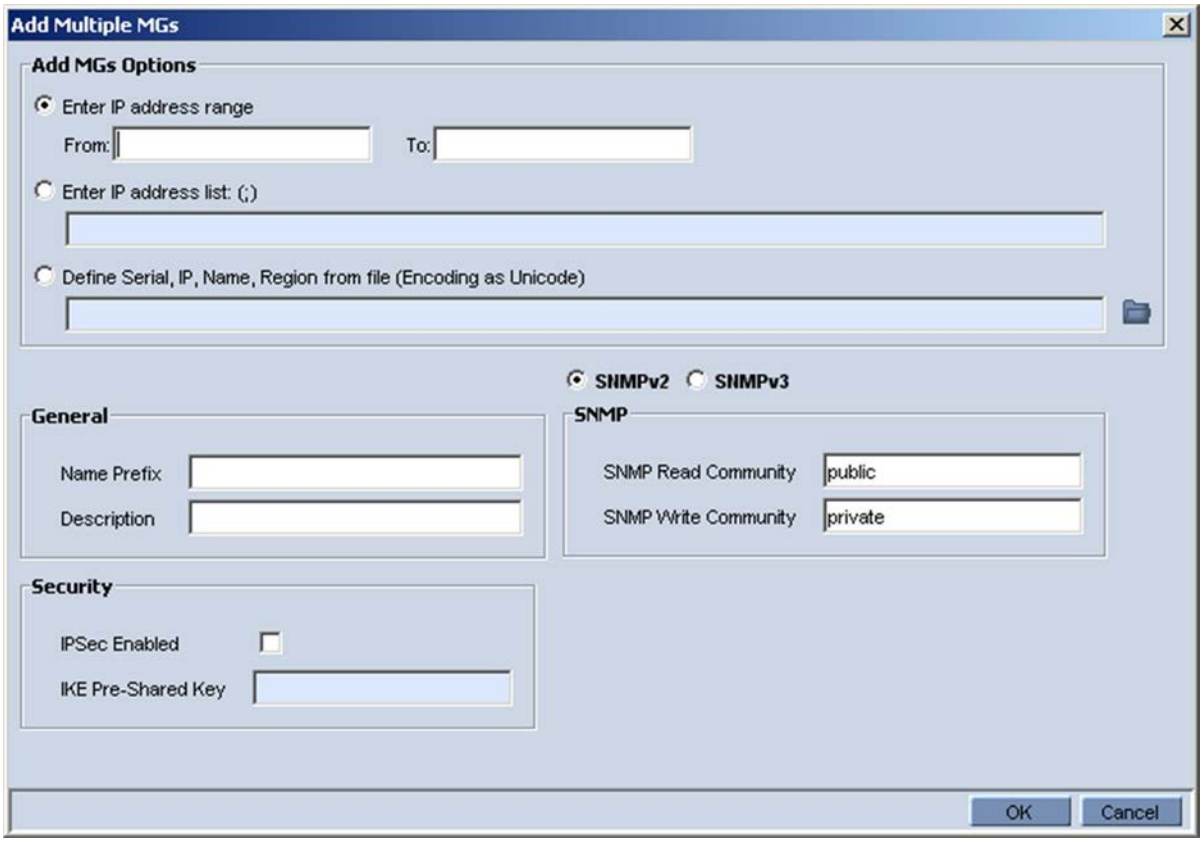
6.2.1 Defining Multiple Mediant 5000, Mediant 8000 Gateways

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



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.

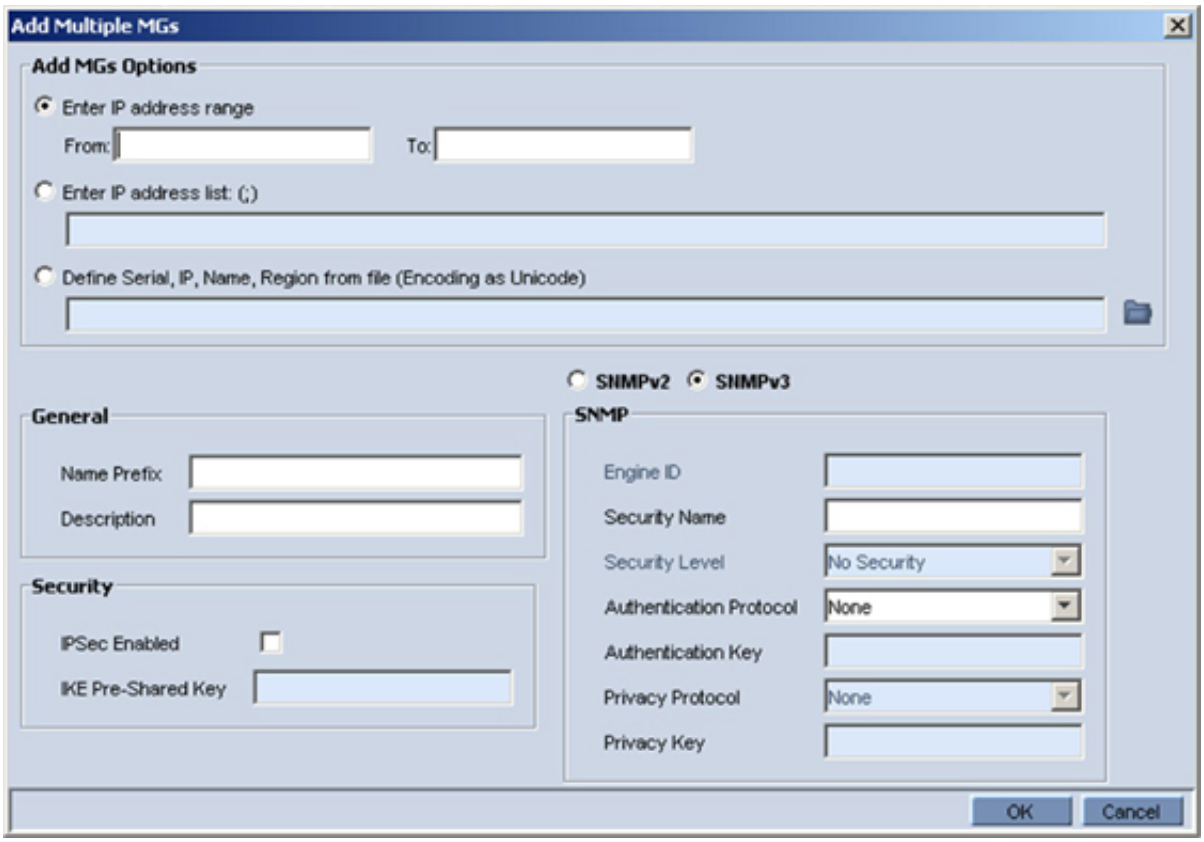
5. Verify that all the gateways are successfully defined in the EMS: Firstly, check the MGs List information; secondly, enter each gateway's status screen. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of the gateway, including its LEDs, must be displayed in the Status screen (refer to the figures displaying gateway status under 'MediaPack' on page 187). If you do not view a graphic representation of the gateway in the Status screen, see Section 'Troubleshooting' on page 453 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



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
```

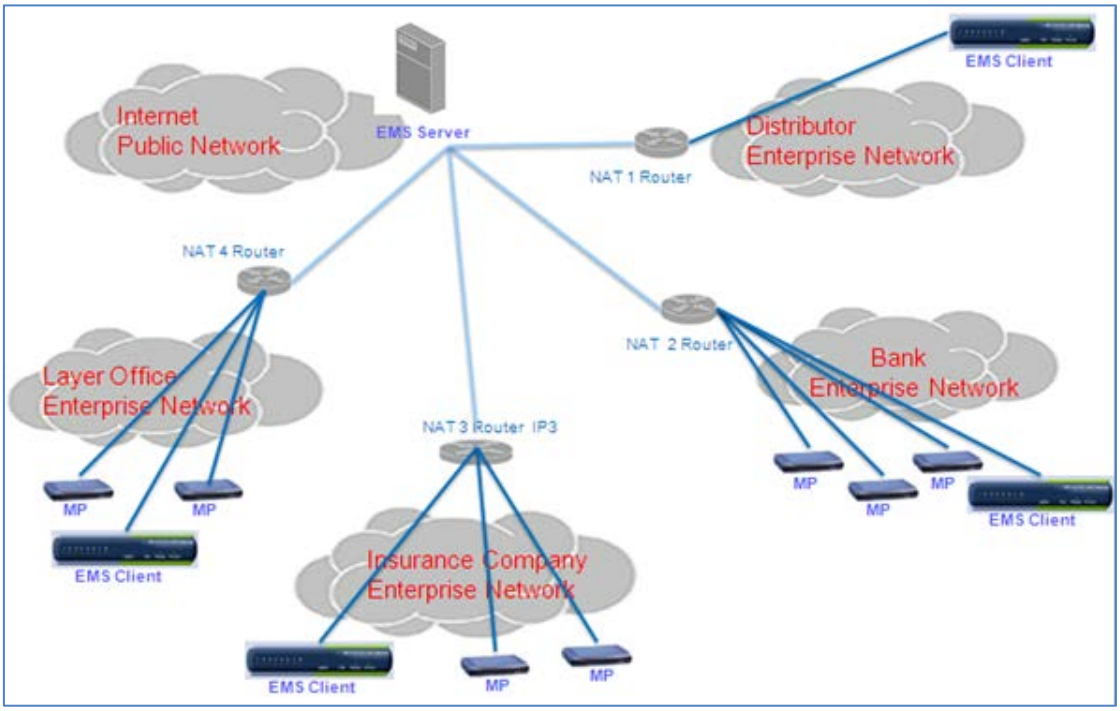
3. After the device is connected to the power supply and the network at the customer's premises, it performs a reboot and at the end of the initialization process, sends a coldStart trap event to the pre-provisioned 'SNMP Manager' name. When the coldStart trap is received, the EMS connects the device, 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.

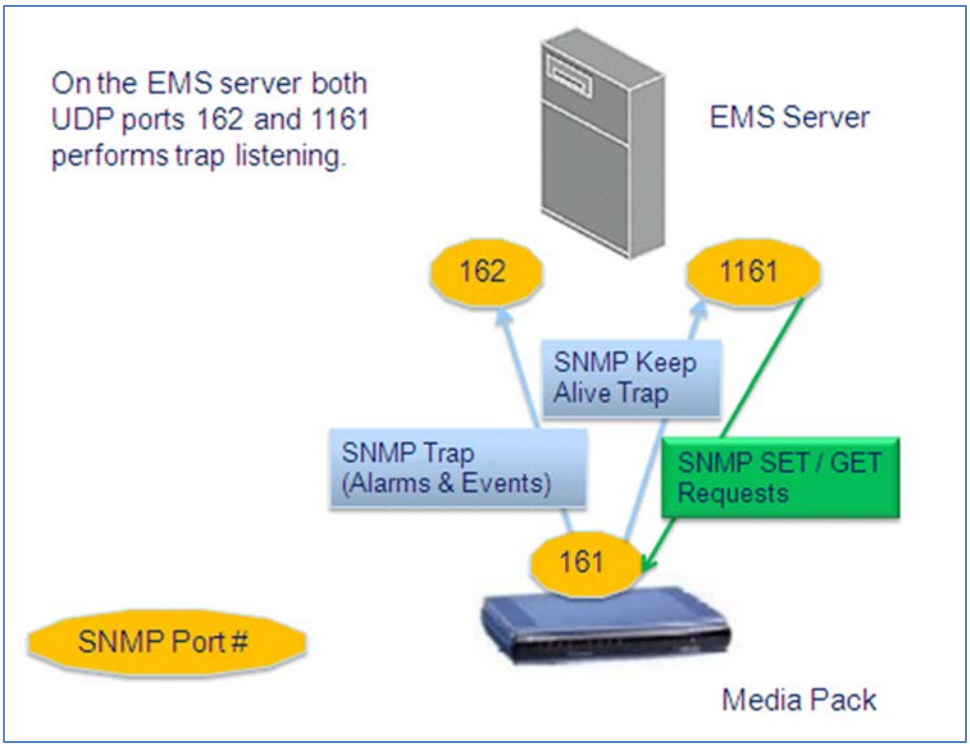
Figure 6-7: MP-NAT Configuration



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)



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**.

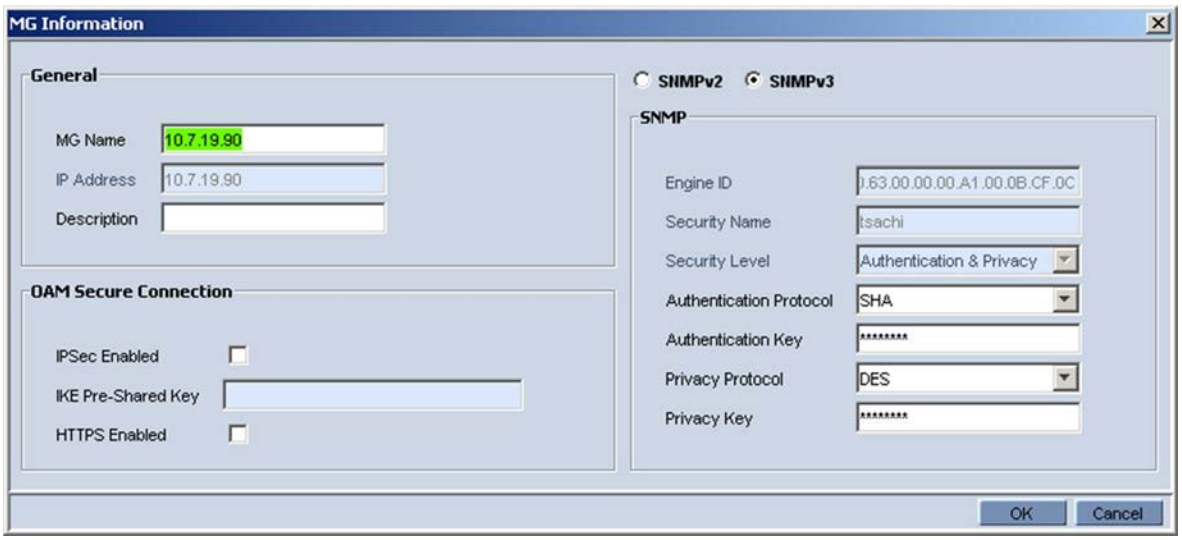
Figure 6-9: MG Information - SNMP2

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 453 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



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 405.

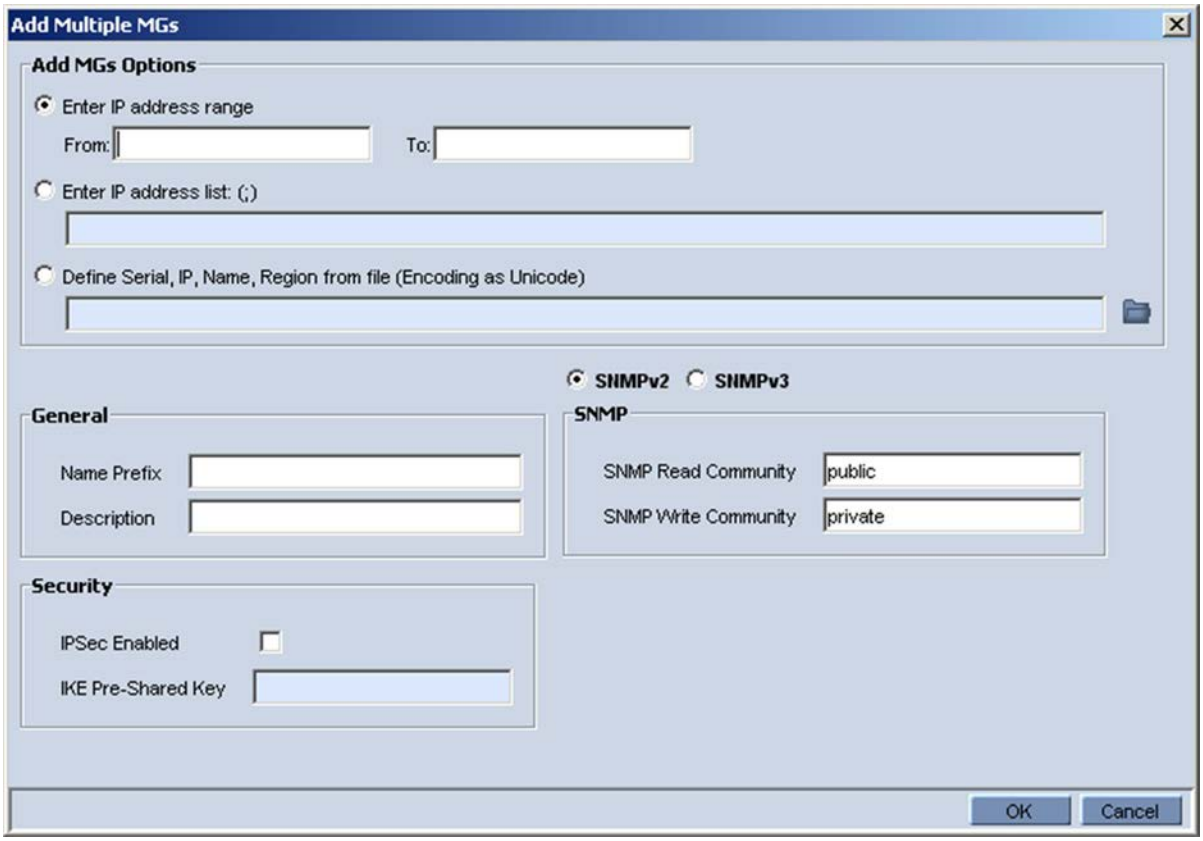
6.3.4 Defining Multiple Blades and CPEs

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.

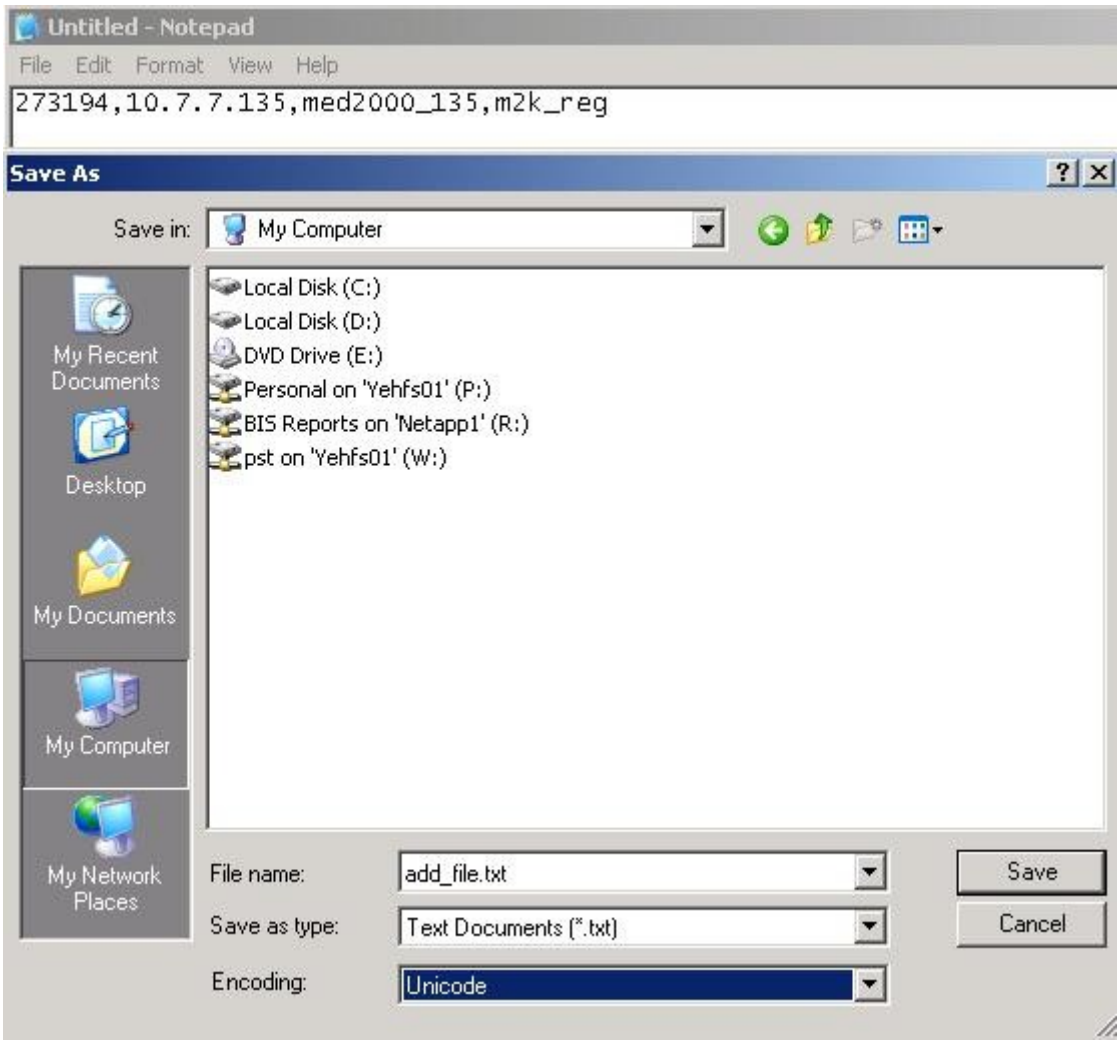
Figure 6-11: Add Multiple MGs-SNMPv2



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).

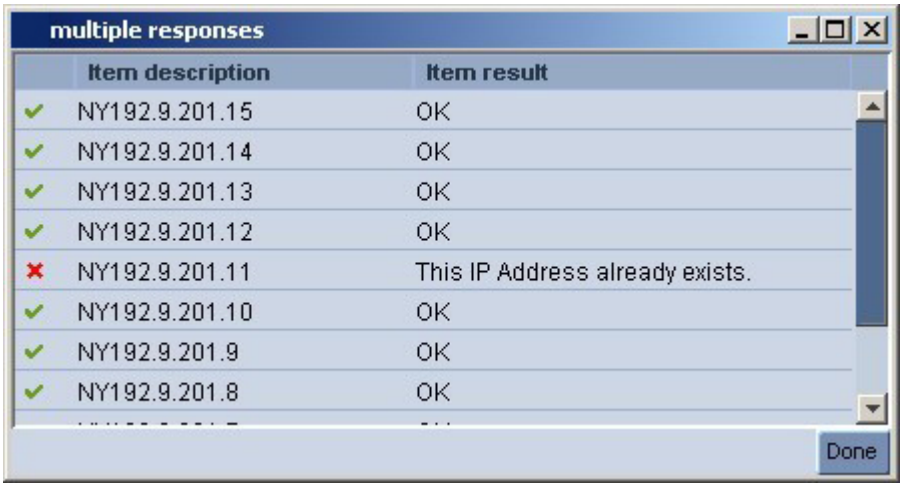
Figure 6-12: Add File Unicode



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 84.
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



Note:

- 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 405.

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 problem when defining your gateways, see Section 'Troubleshooting' on page 453 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 453 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:

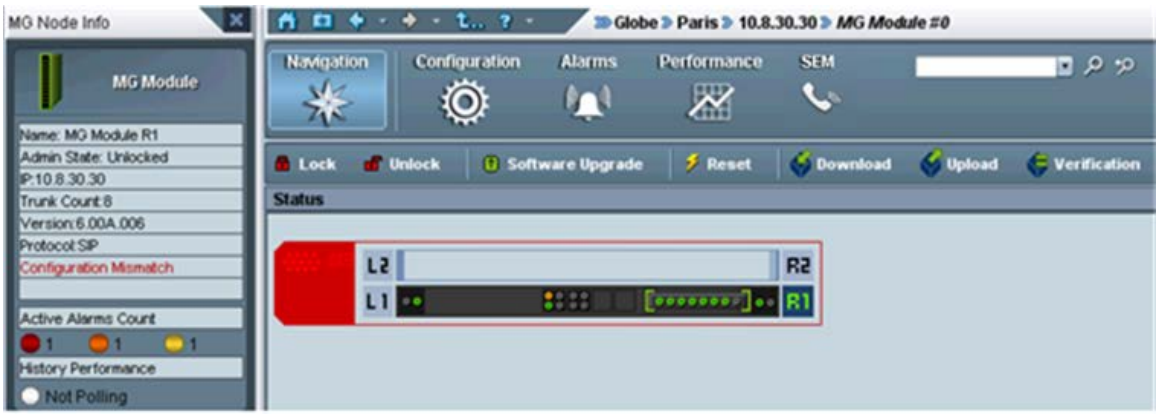
- **Unknown Hardware:** The Product Type, returned by the MIBII sysDescr value, is not recognized by the EMS. The gateway cannot be managed by the EMS.
- **Unknown Software**: The Software Version, returned by the MIBII sysDescr value, is not recognized by the EMS. Either add the specified version to 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



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

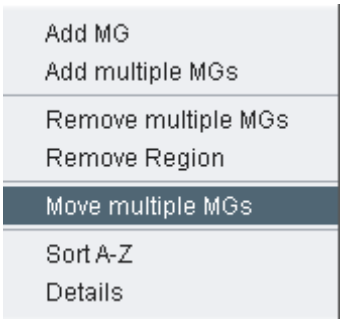


Figure 6-17: Multiple Move from Region to Region

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.

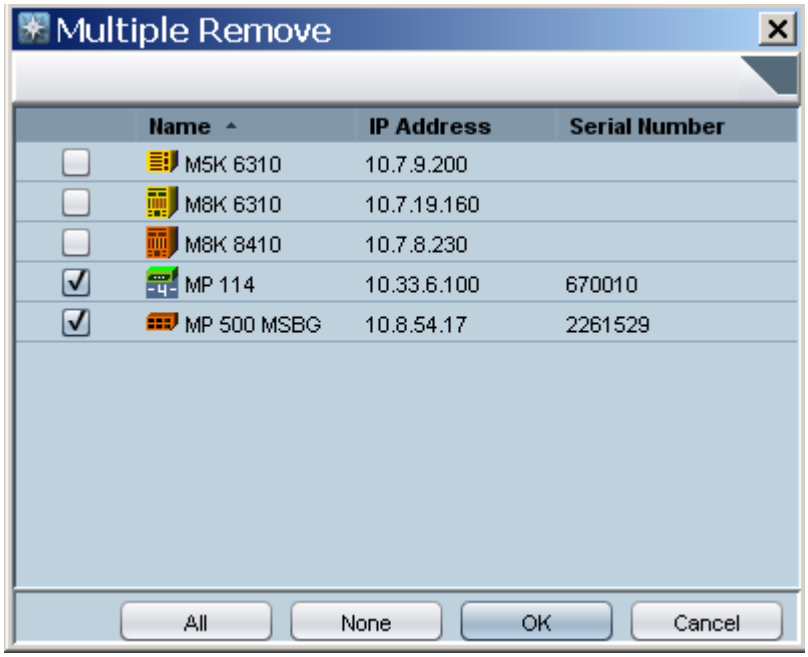
6.9 Removing Multiple Gateways

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



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

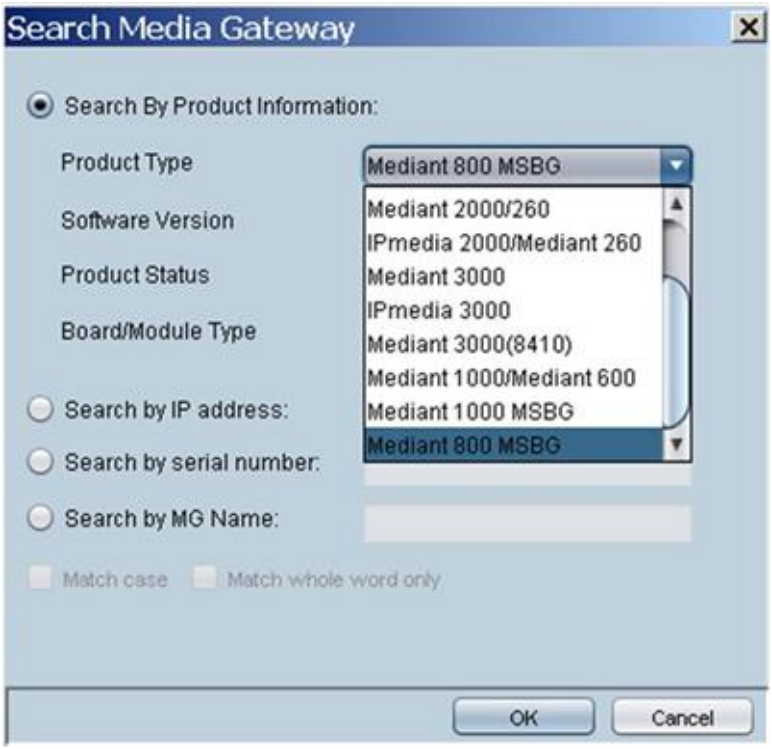
This section describes how to search for a media gateway.

➢ **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



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.

This page is intentionally left blank

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 101
- 'MGs List' on page 103

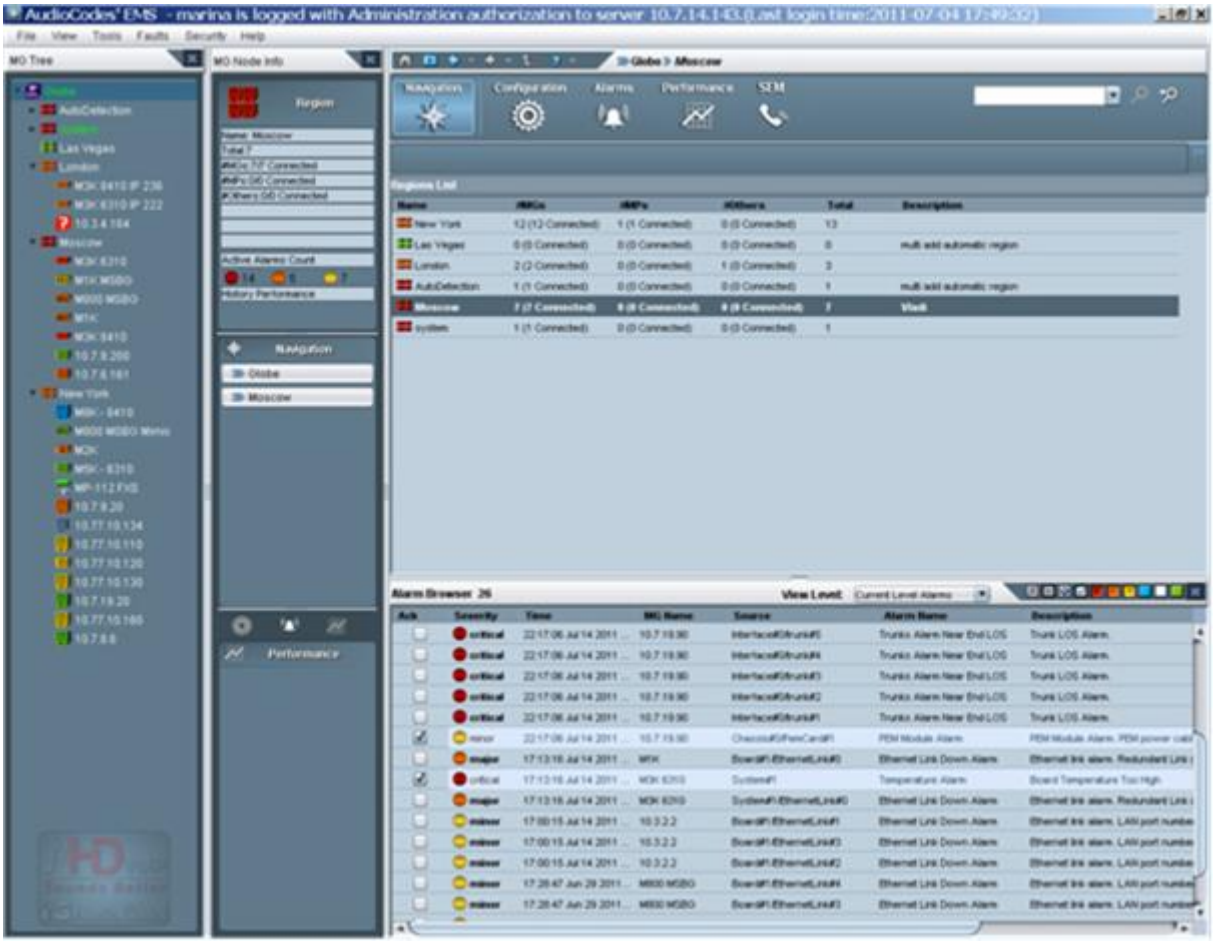
7.1 Regions List

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



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

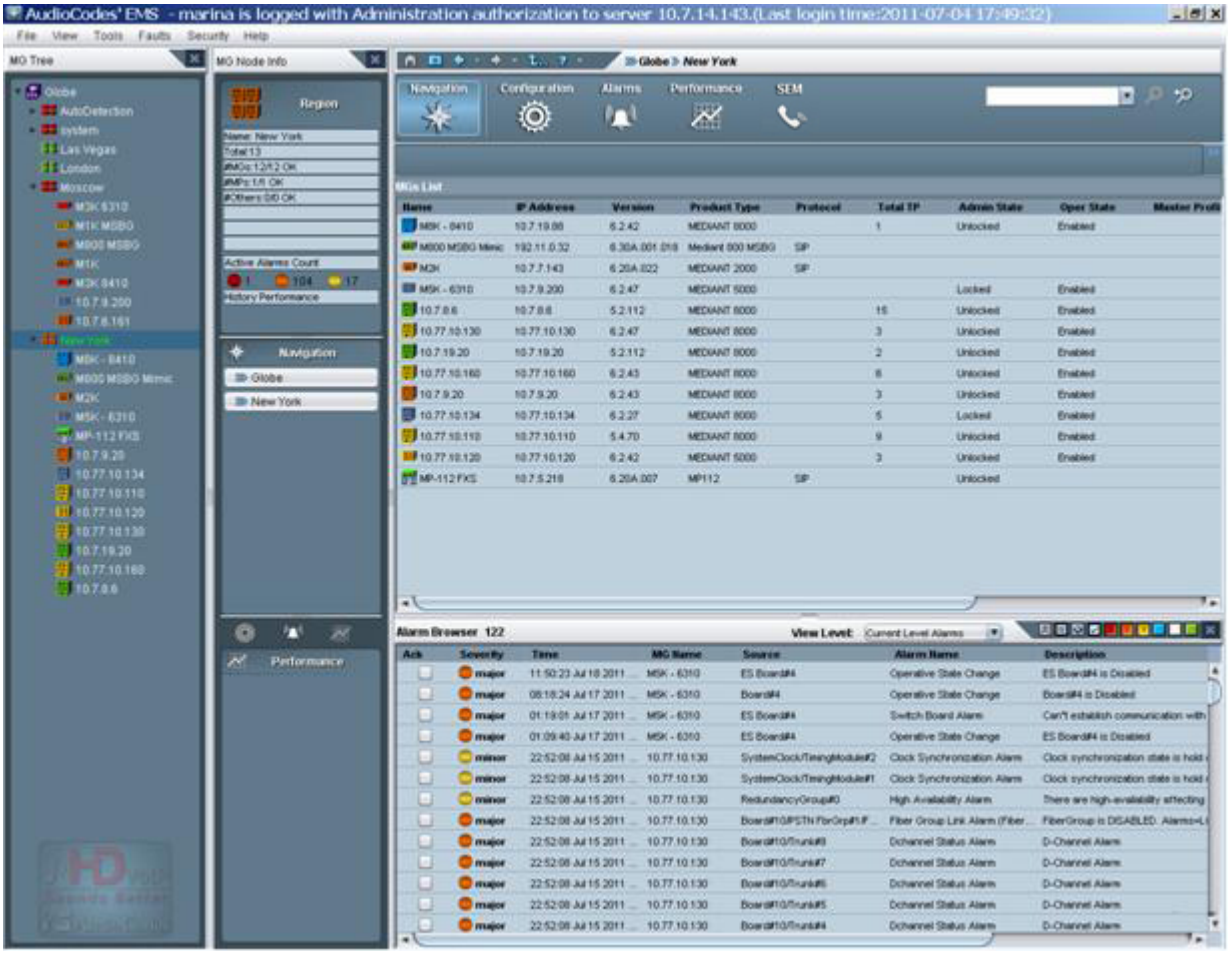
This section describes the MGs list.

➢ 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



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

- Master Profile (CPE products).

  Indicates the name of the Master Profile when a master profile is attached to the device.
- 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 MSBG, Mediant 1000 and Mediant 1000 MSBG devices (Digital, Analog, BRI, IPmedia) and channels status distribution – on hook / off hook. This view consists of two pie charts; one for the module distribution and another for the channels status distribution.

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

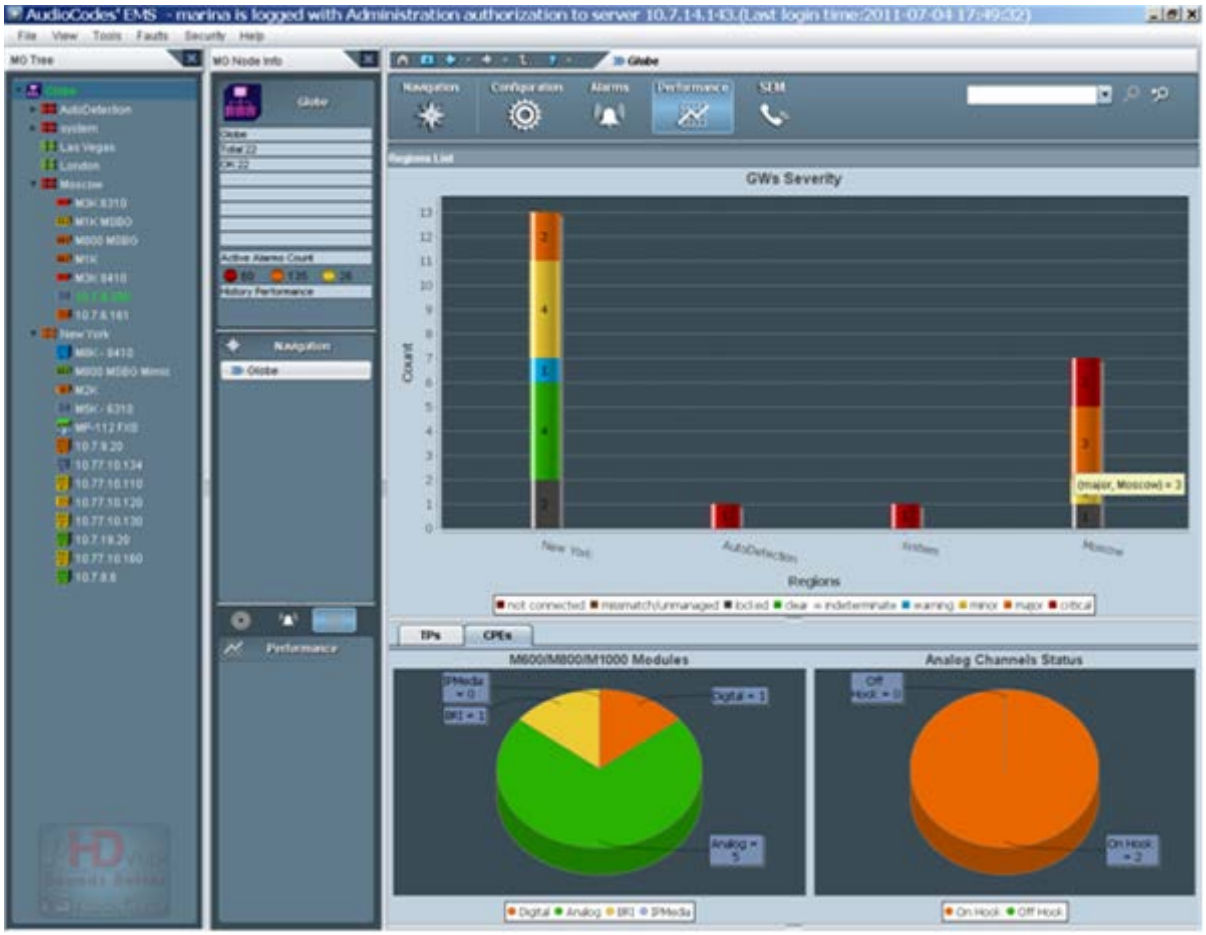
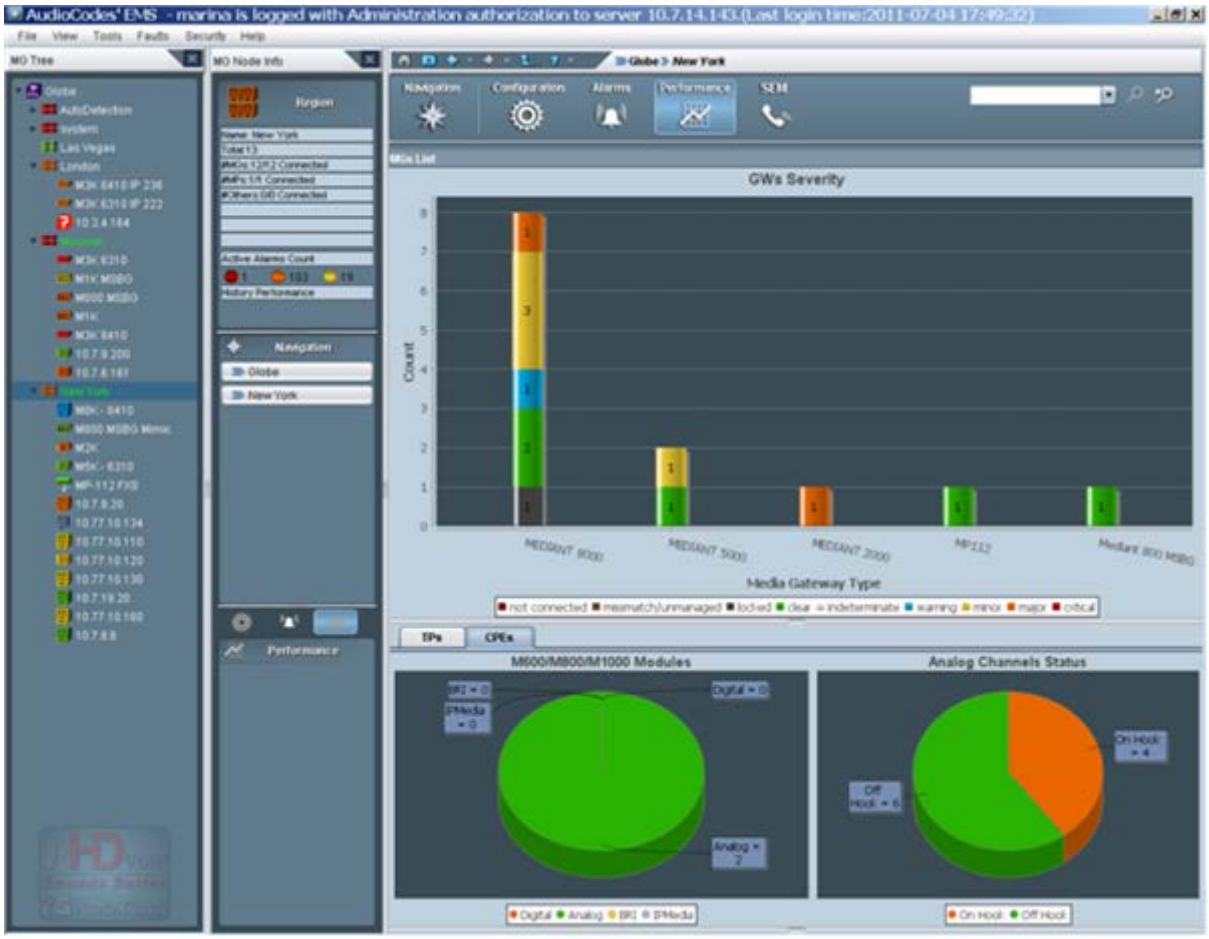


Figure 7-5: Region Level – TPs

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.

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

- 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:

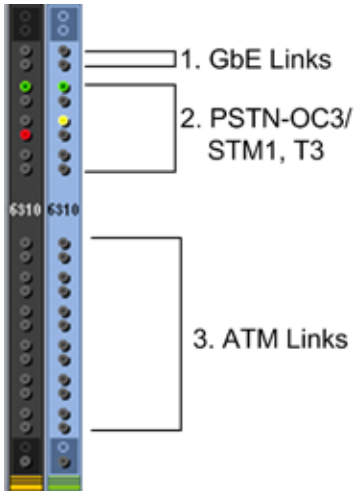
Figure 8-4: 6310 Board-Active and Redundant Status

- 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

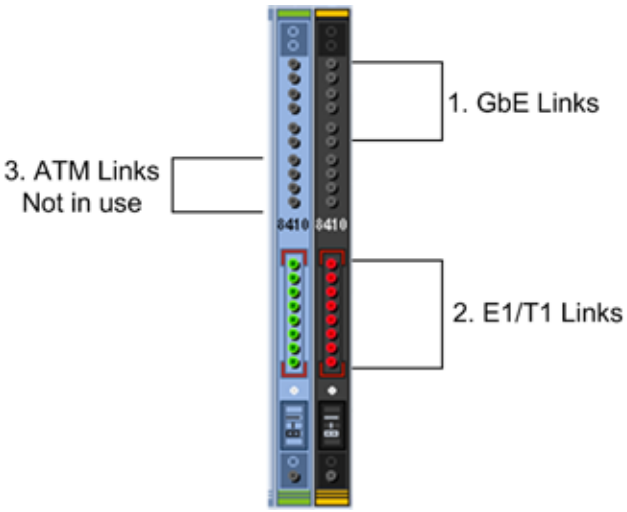
Figure 8-6: 6310-LED Status



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'.

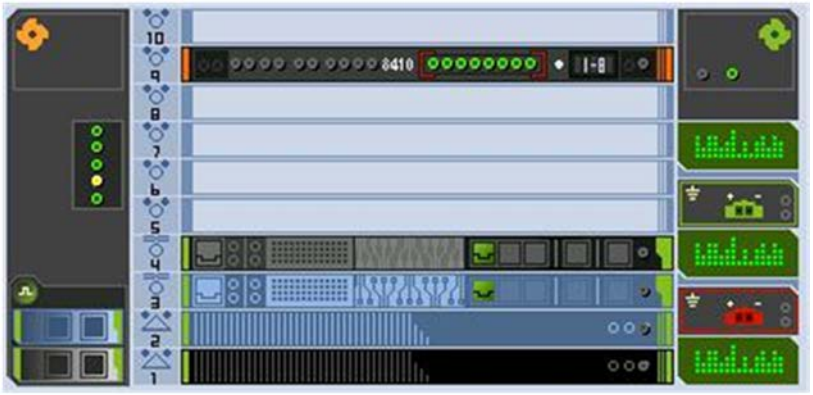
8.2 Mediant 5000 Status Pane

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

- 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:

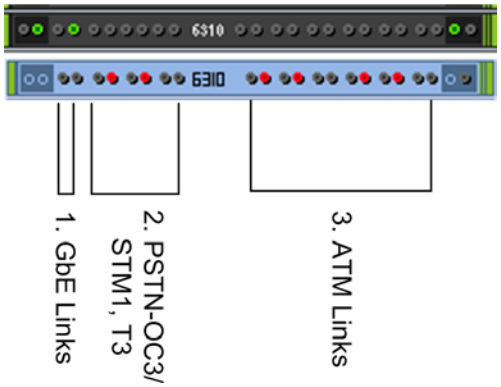
Figure 8-18: 8410 Active Board Status

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

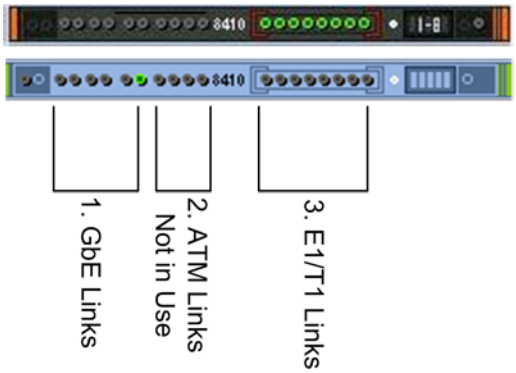


Legend

- 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)

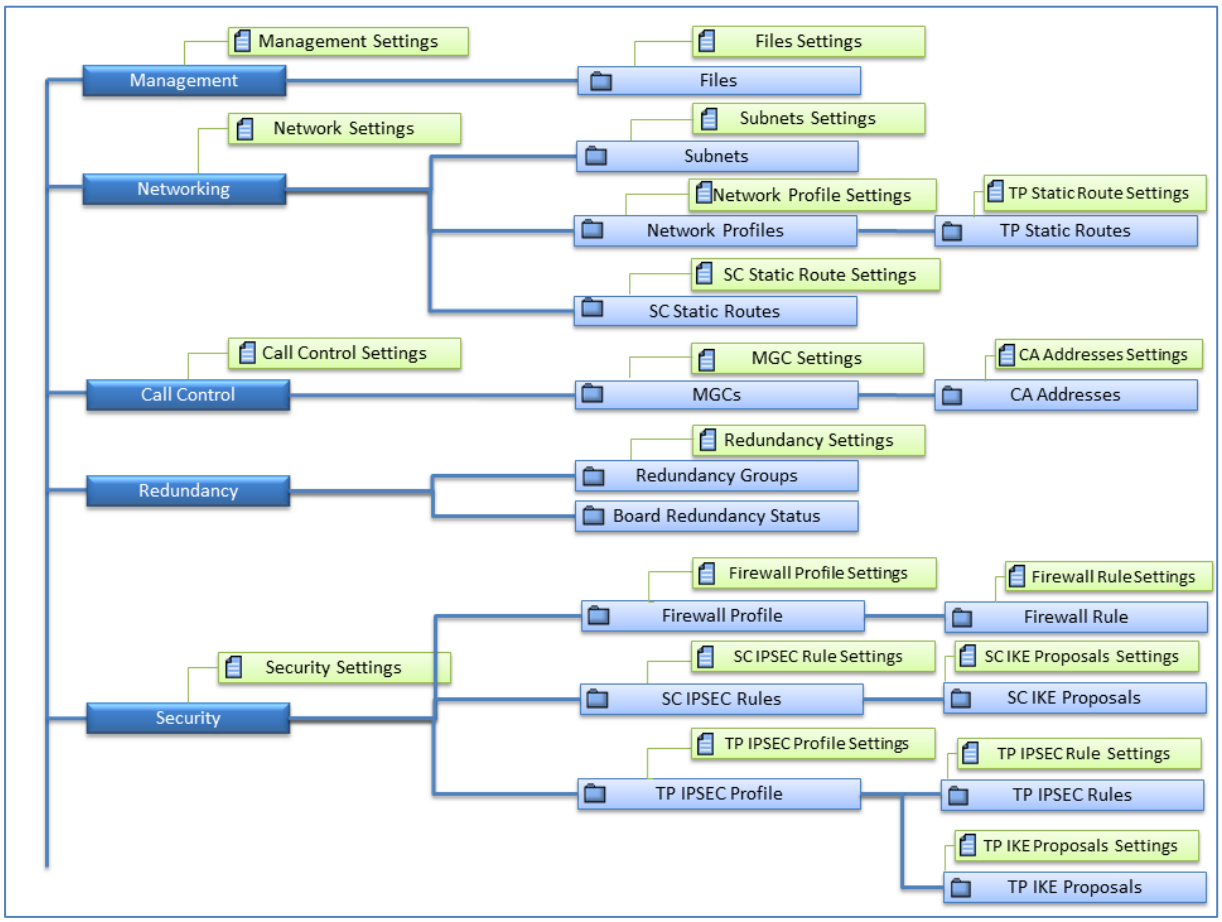
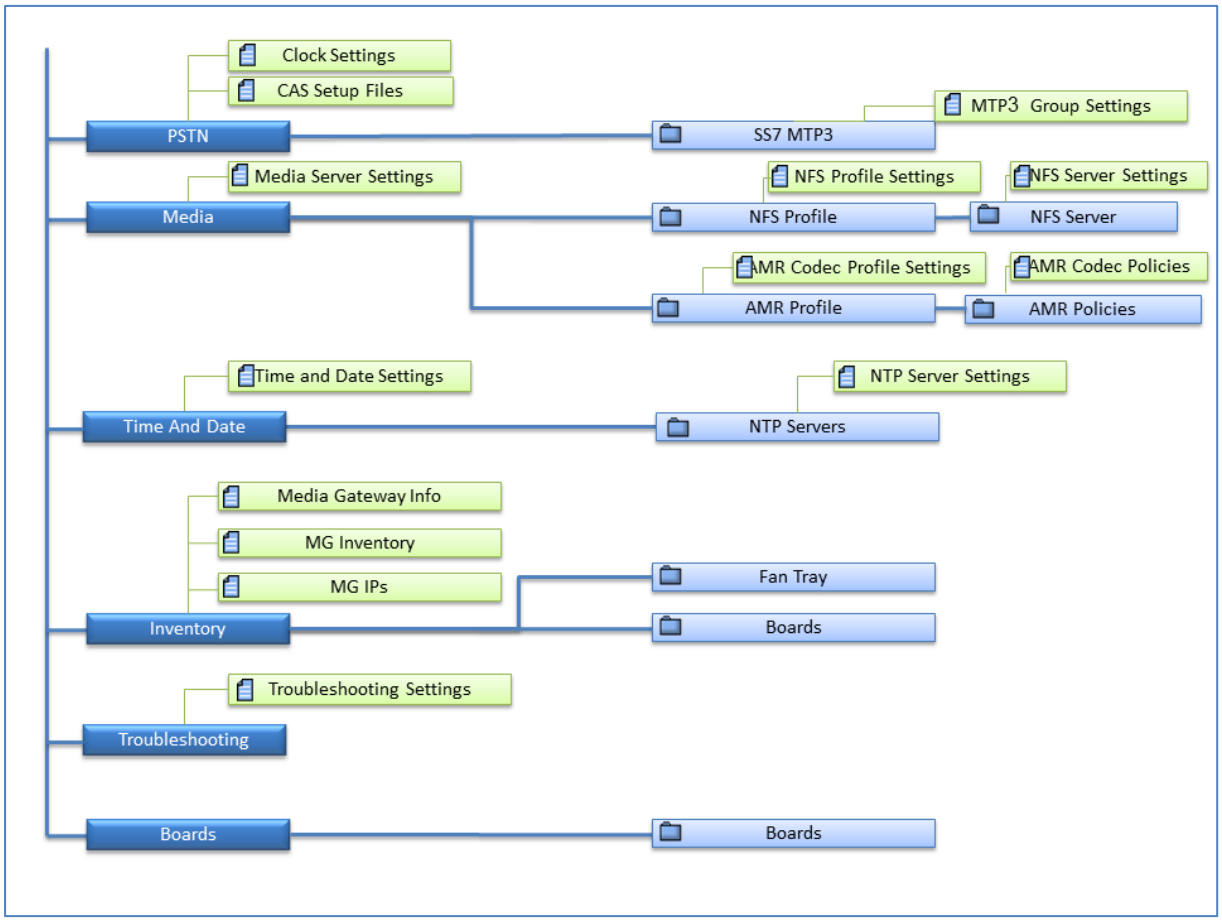


Figure 8-27: Media Gateway Level Navigation Buttons (Part 2)

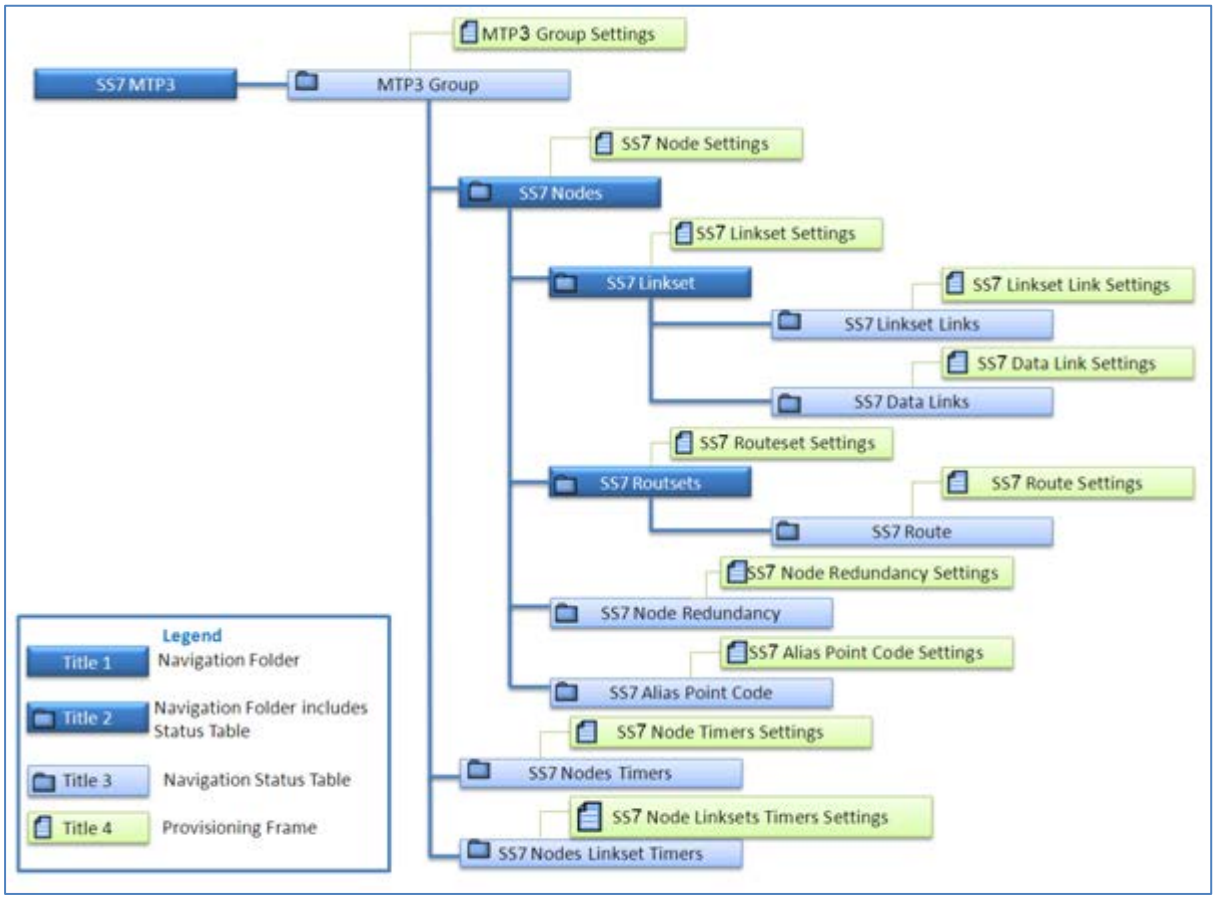


For more information, refer to the relevant *IOM Guide.*

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 61.

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	Create Master profile	-	Creates a Master Profile with all information related to board level and main interfaces (DS1, DS3, Fiber Group), etc.
	Apply Master profile	Board is locked	Applies a selected master profile to one or more 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.
	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).

Table 8-8: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
	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
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.

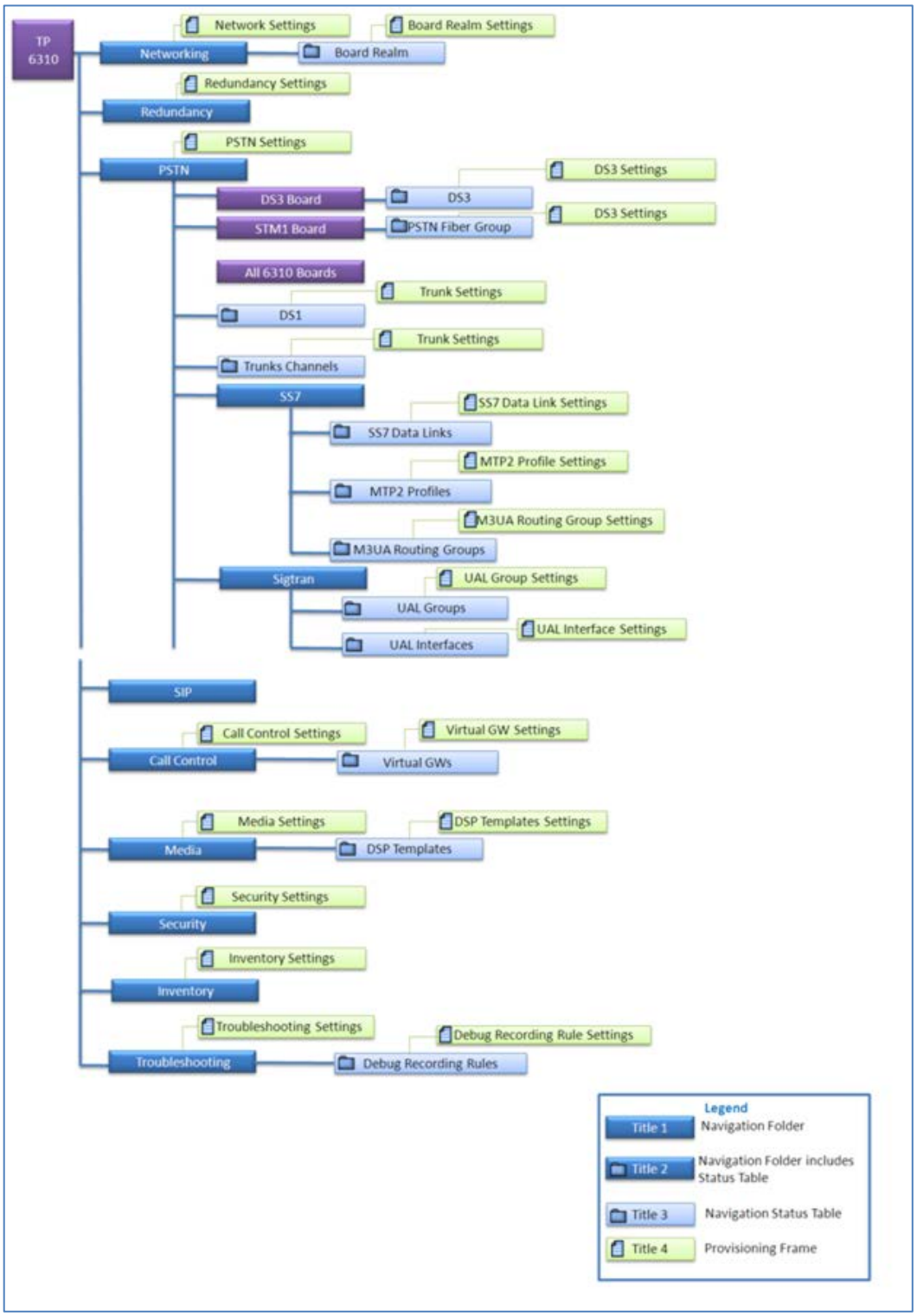
8.5 Accessing a TP-6310 Board

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 139.

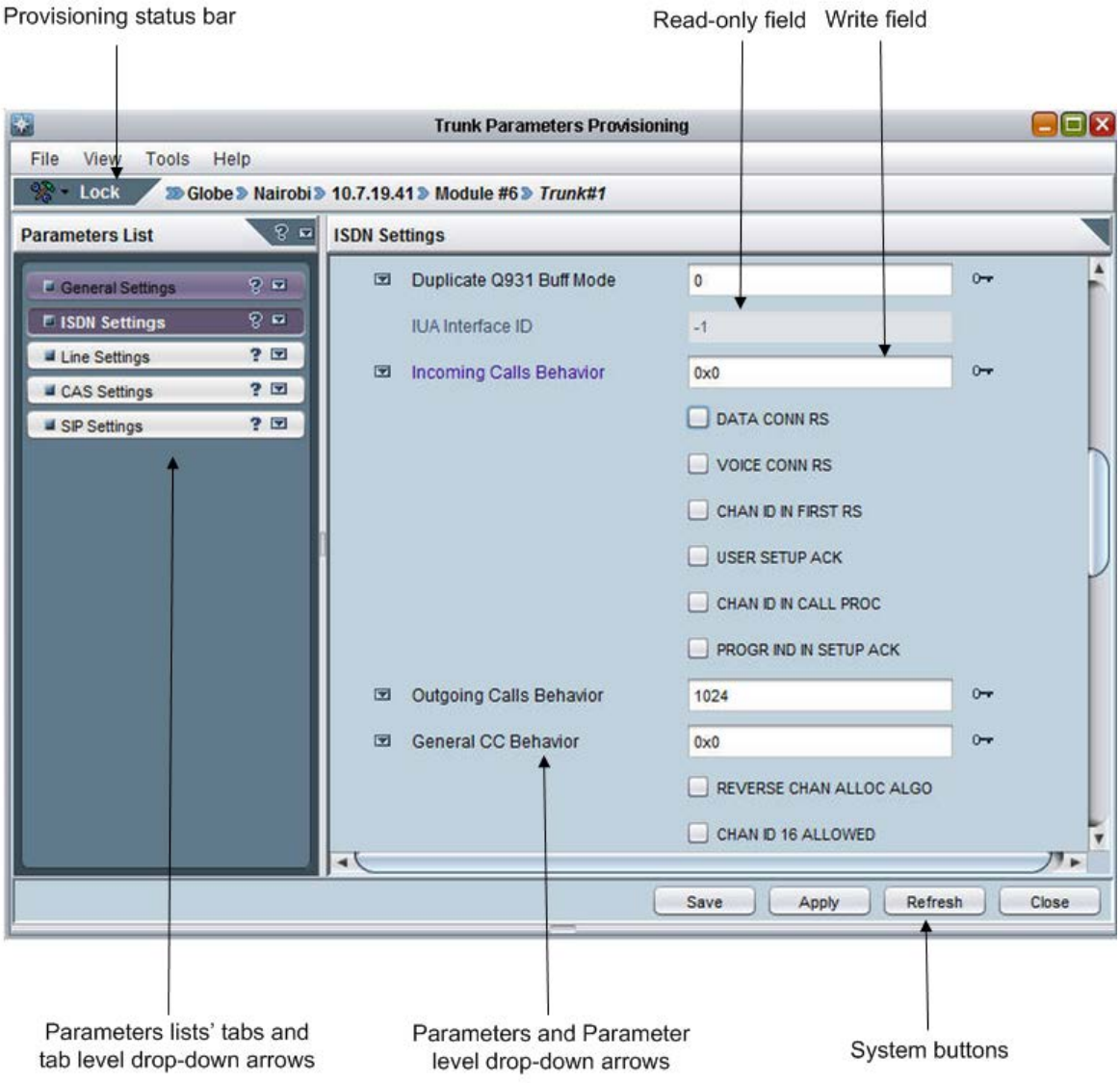
8.5.1 Accessing the TP Board Level Provisioning Screen

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



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:

1. 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

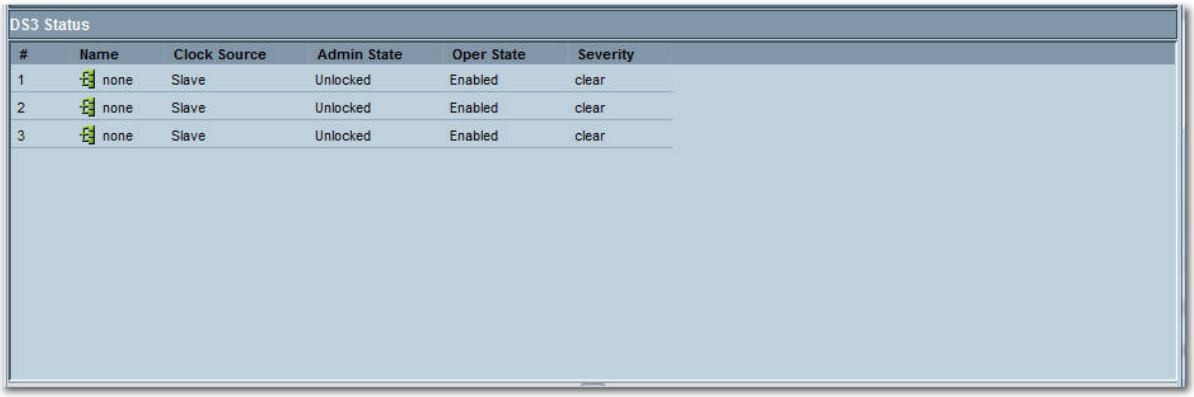
➢ To access the TP-6310 DS3 screen:

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:

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

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



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

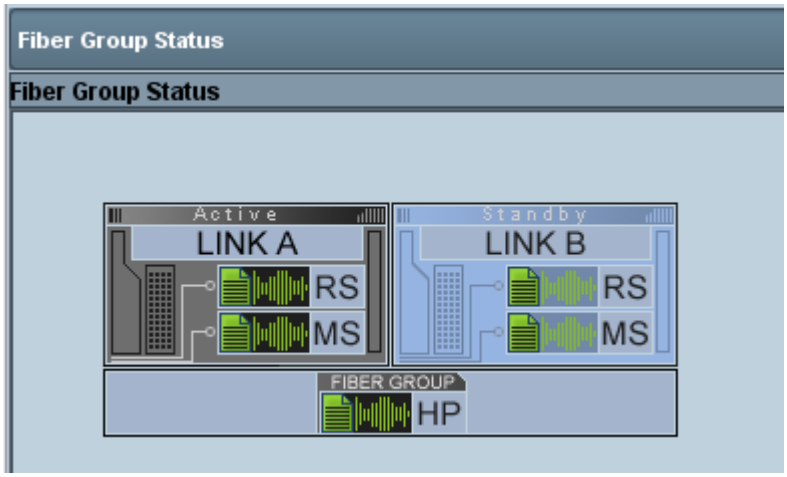
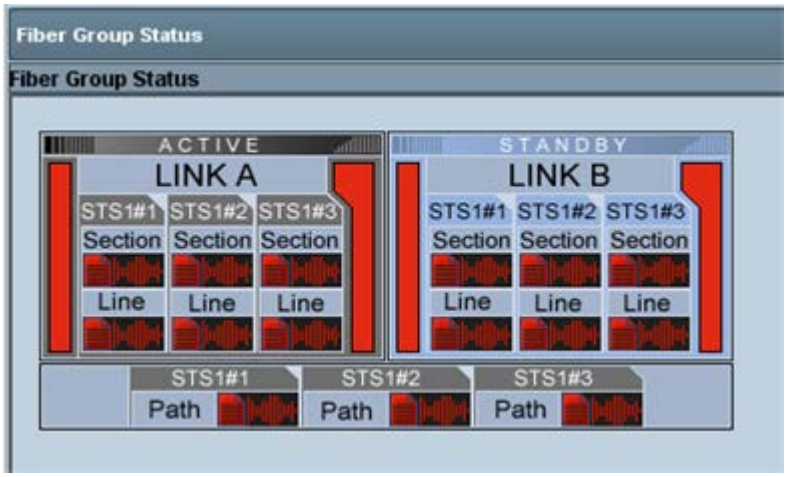


Figure 8-34: PSTN Fiber Group (Sonet OC3/STS Interface) Screen



➢ 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.

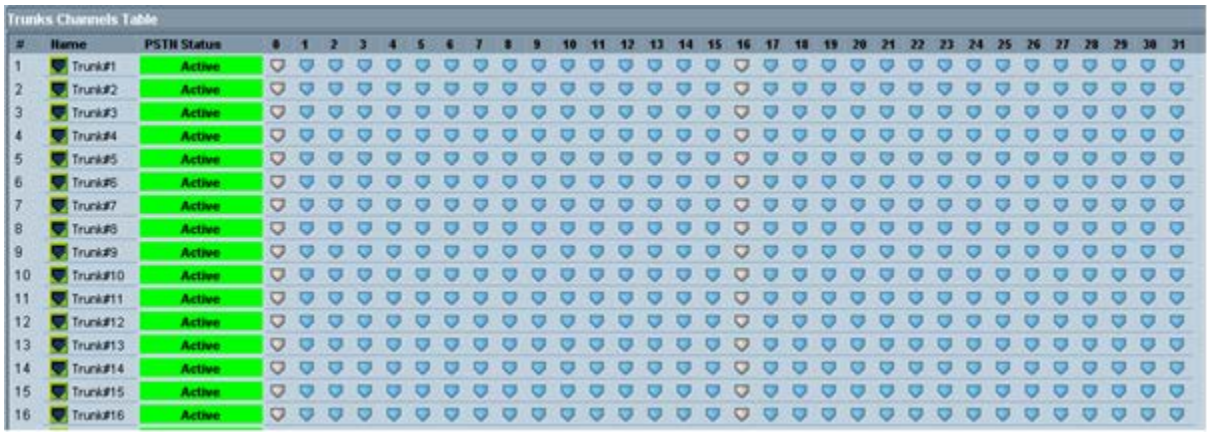
➢ To access DS1 trunks:

- 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 191.

Figure 8-36: Trunk Channels Status



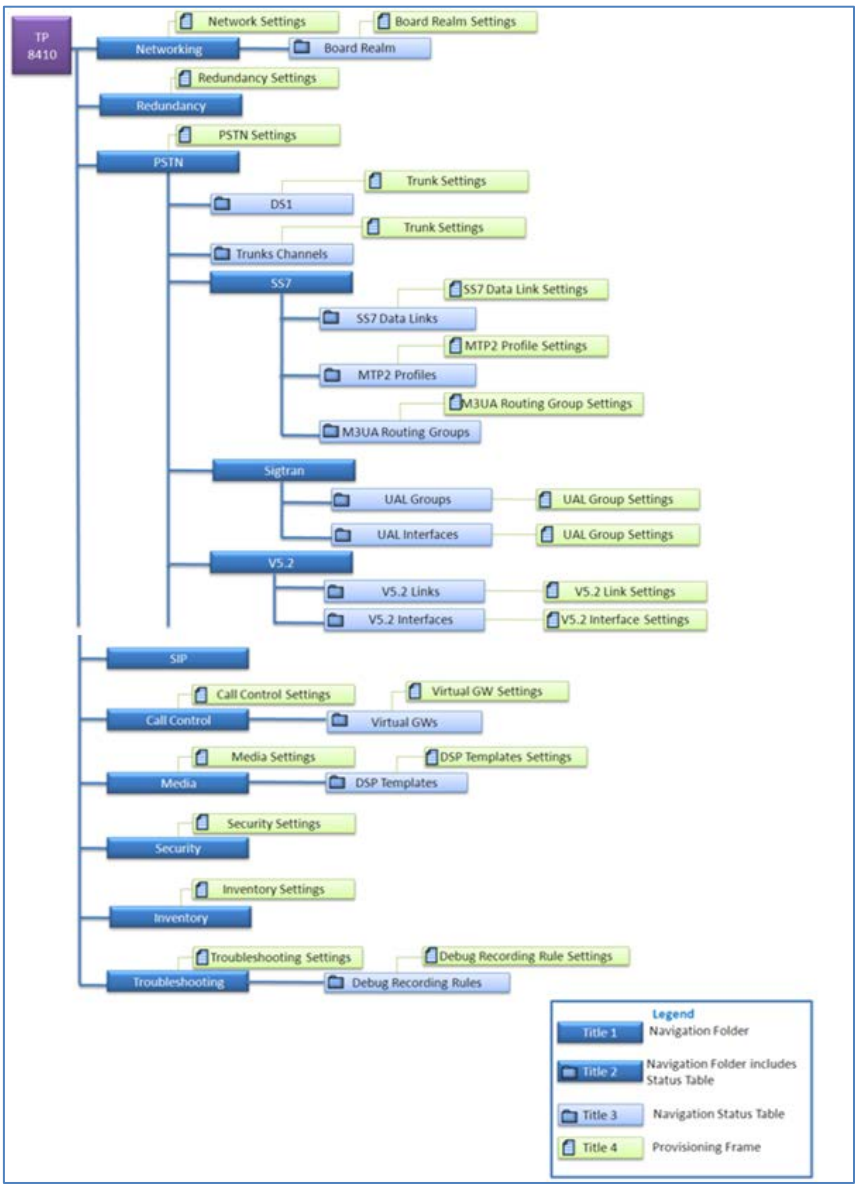
Note: The same actions as described for the 'DS1 Trunks Actions' above are available in the Channel right-click menu.

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

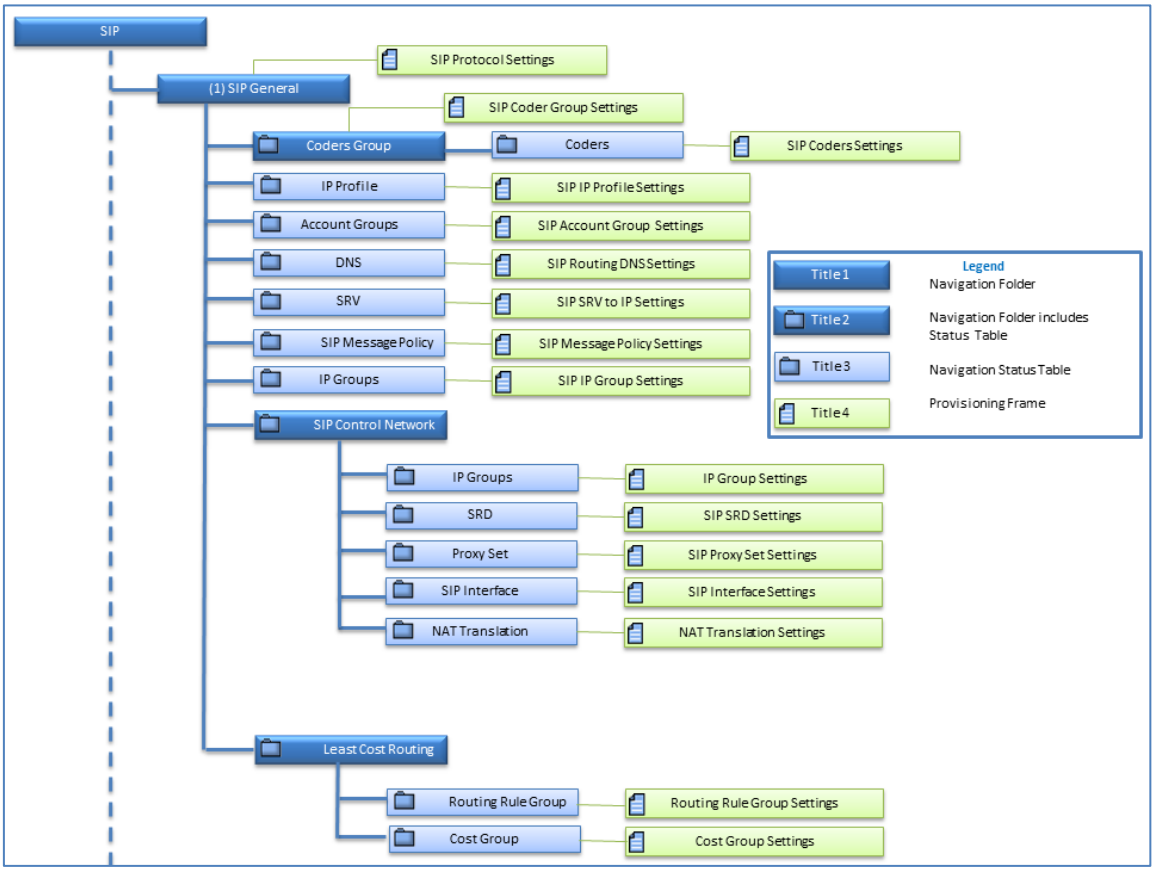


Figure 8-39: SIP GW/IP to IP Hierarchy Links

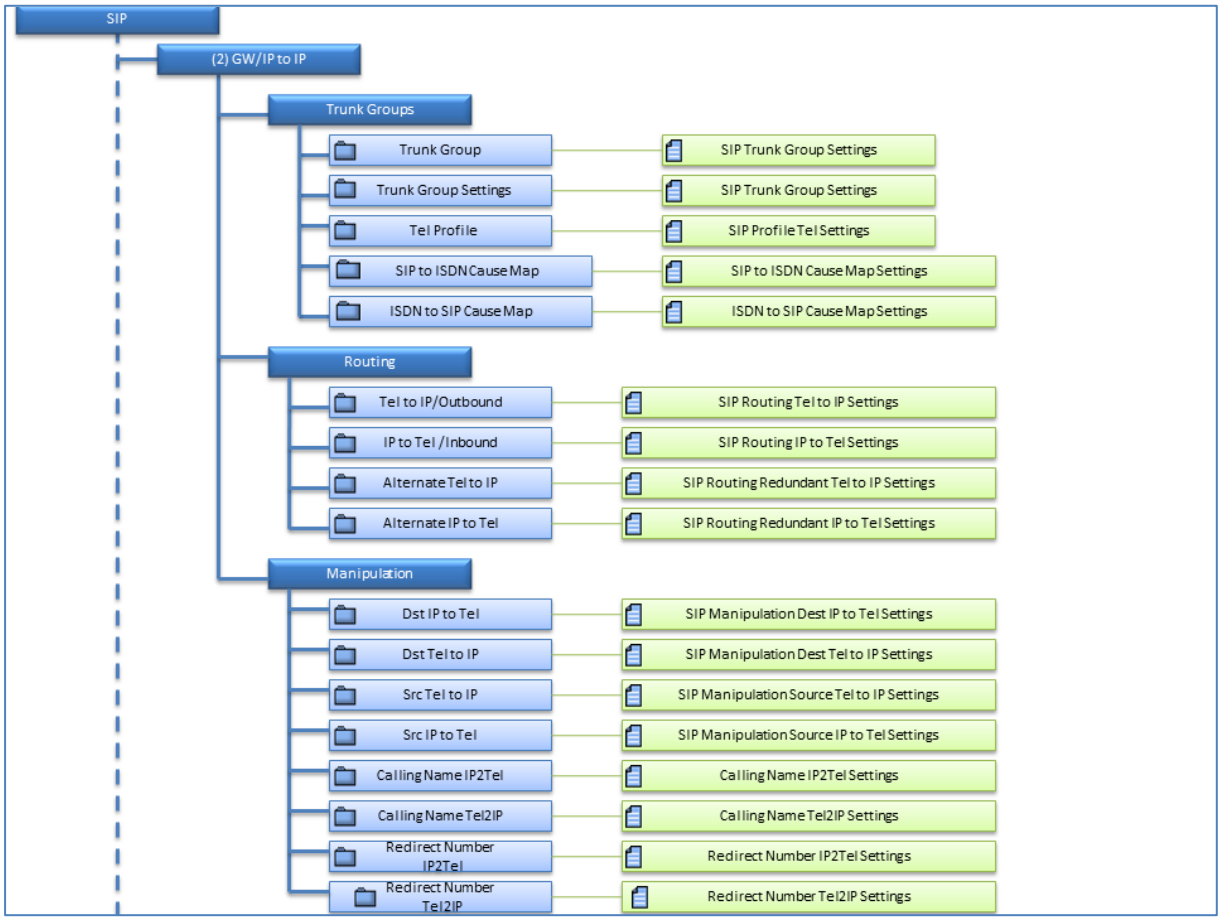


Figure 8-40: SIP SBC Hierarchy Links

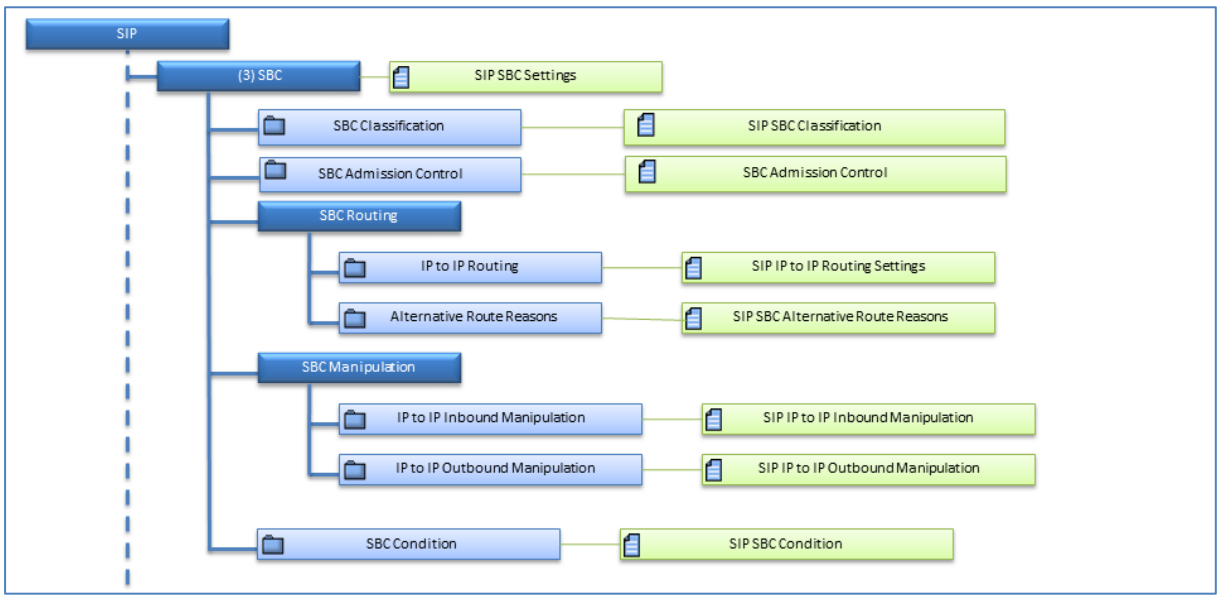
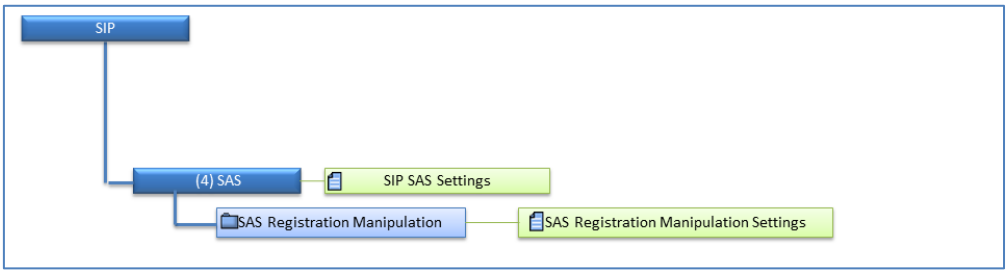


Figure 8-41: SIP SAS Settings

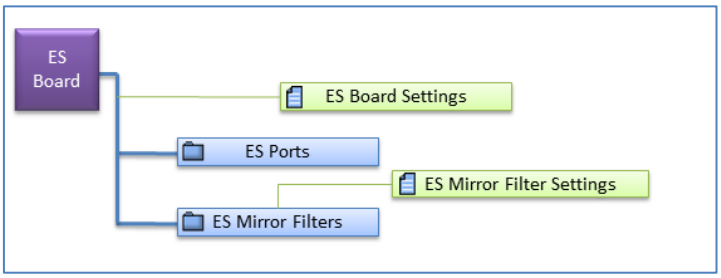


8.8 Ethernet Switch Board's

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



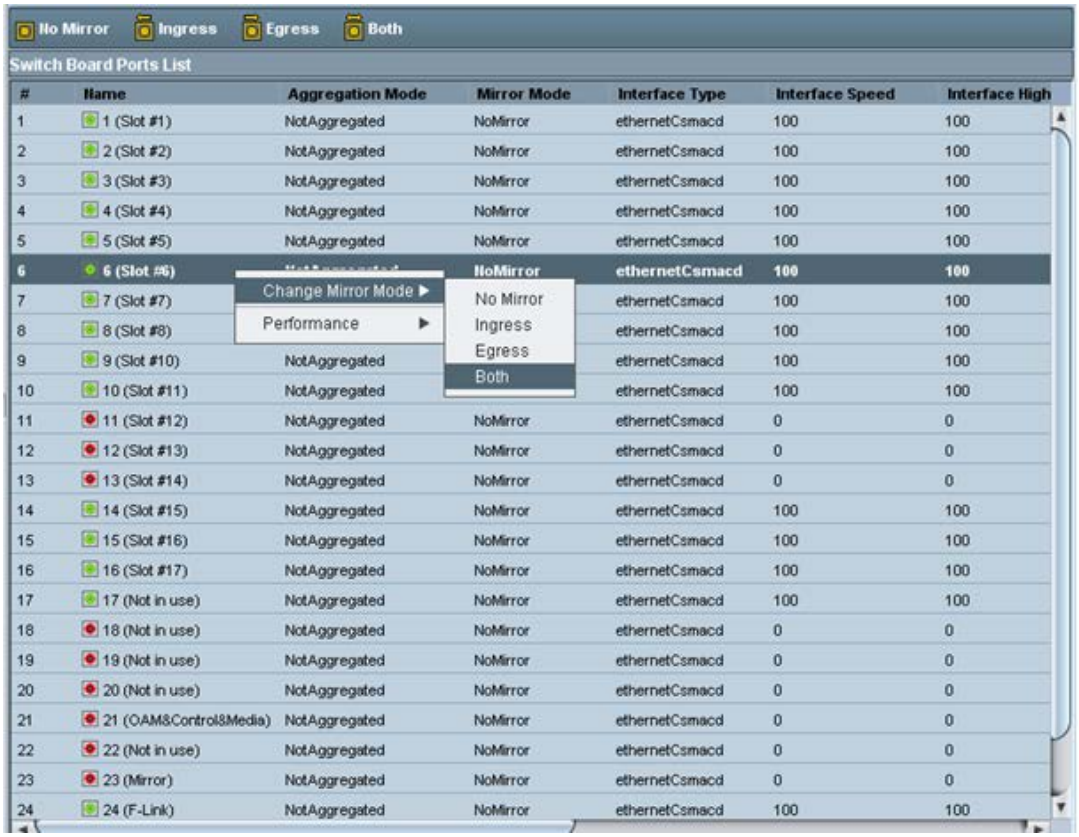
8.8.2 Links' Status

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)		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

This page is intentionally left blank

9 Mediant 4000

This section describes the Mediant 4000 status pane and provisioning.

9.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Standalone (Simplex) Mediant 4000
- High Availability Mediant 4000

9.2 Initial Configuration

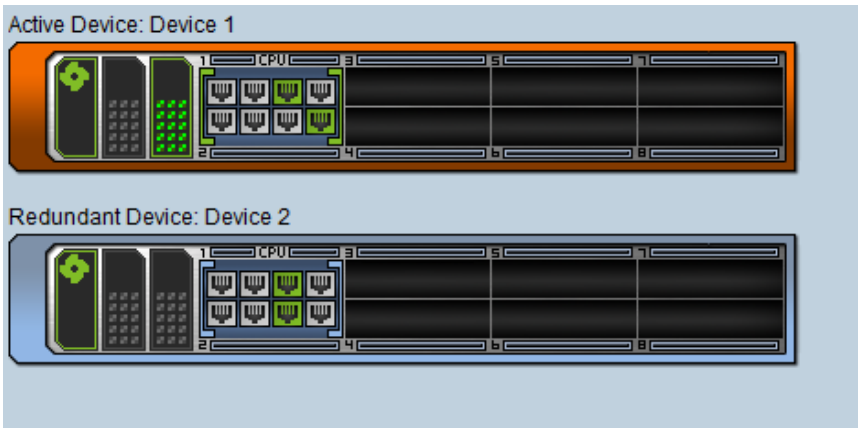
Refer to the *Mediant 4000 User Manual* for the Gateway iinitial Configuration.

9.3 Status Pane

EMS version 6.6 supports the Mediant 4000: HA (1+ 1) and Simplex mode. 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.
- Mediant 4000 device active / redundant coloring is supported
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

Figure 9-1: Mediant 4000 Status Pane



The Status pane graphically displays the status of the gateway.

- **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.

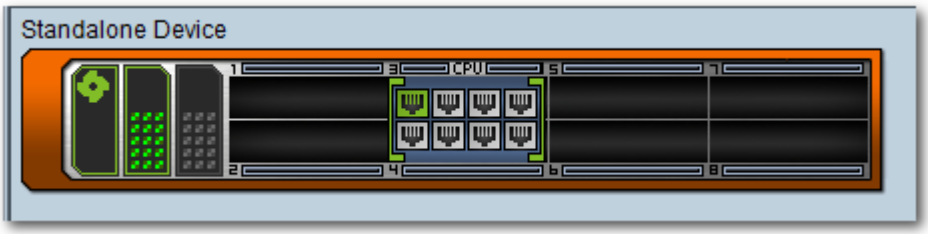
9.3.1 Hardware Component Status in Table View

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 9-2: 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

9.4 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 Mediant 4000 SBC.

Figure 9-3: Navigation Hierarchy Links - Mediant 4000 (Part 1)

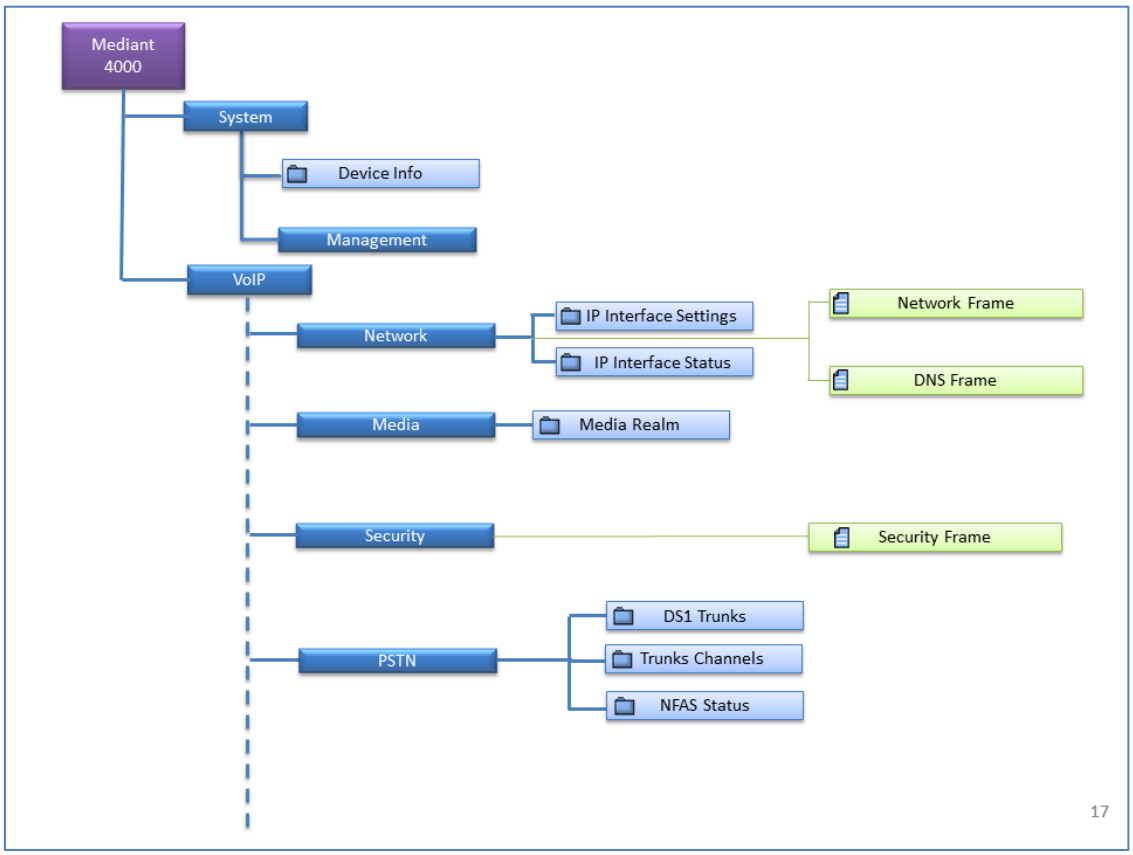


Figure 9-4: Navigation Hierarchy Links - Mediant 4000 (Part 2)

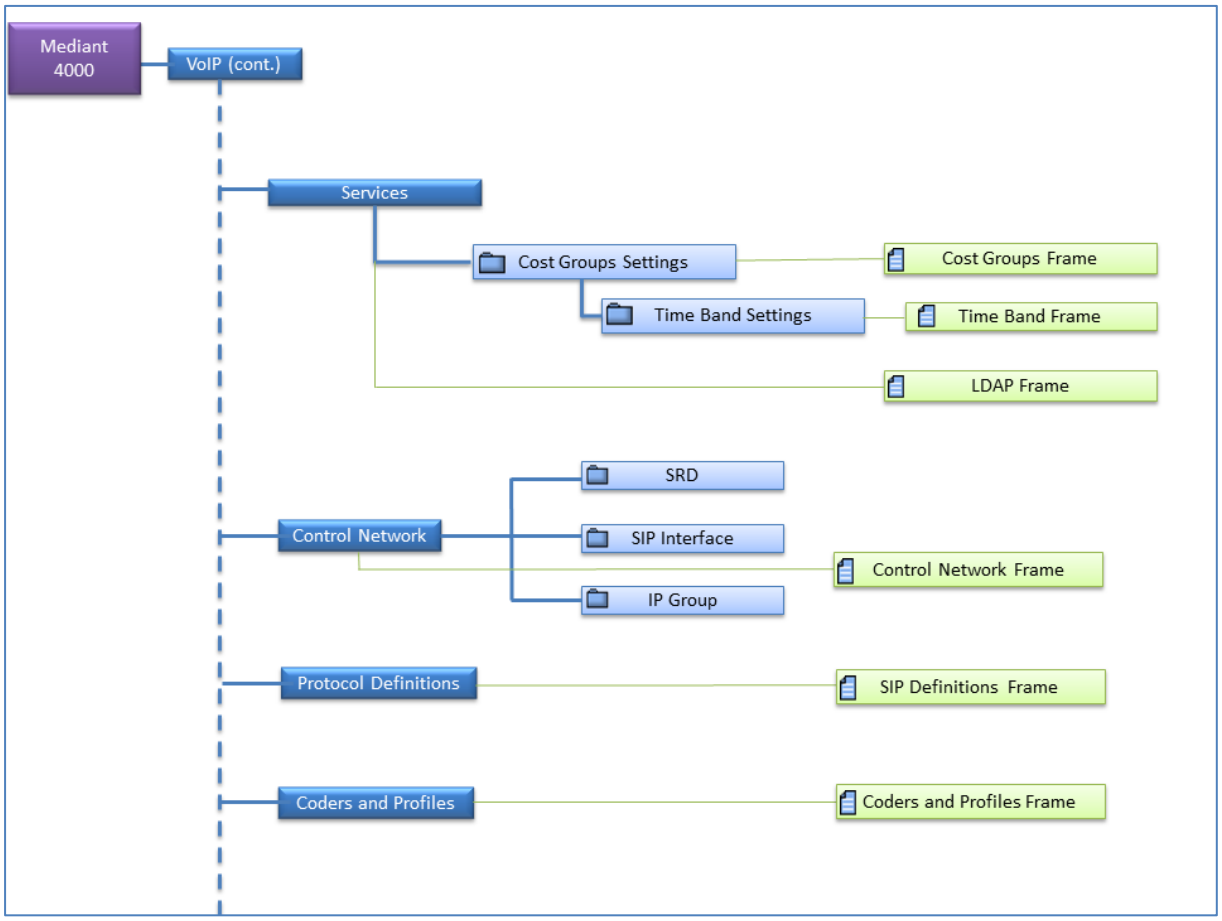
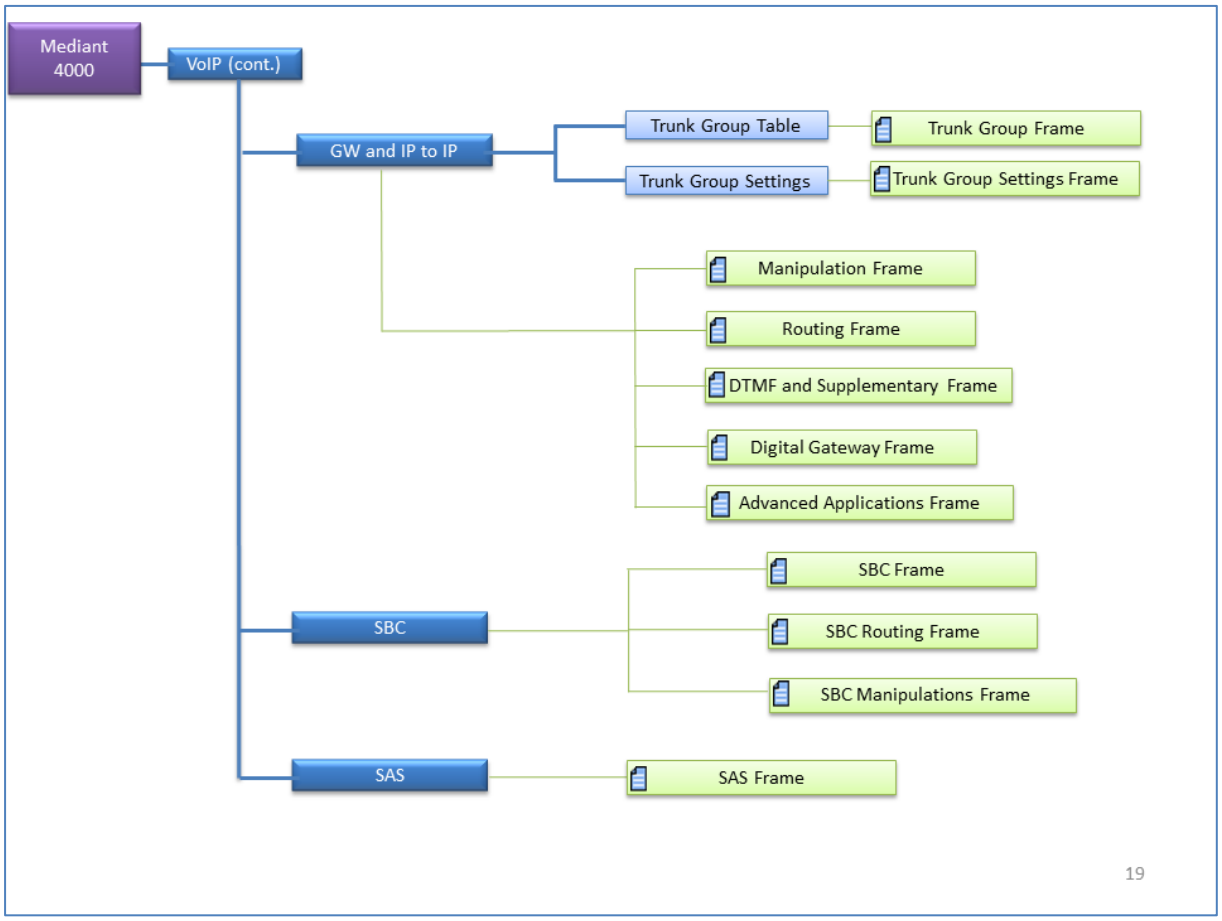


Figure 9-5: Navigation Hierarchy Links - Mediant 4000 (Part 3)



See Section 'Provisioning Concepts' on page 194 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

9.5 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 197.

10 Mediant 3000

This section describes the Mediant 3000 status pane and provisioning.

10.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

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

10.2 Initial Configuration

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

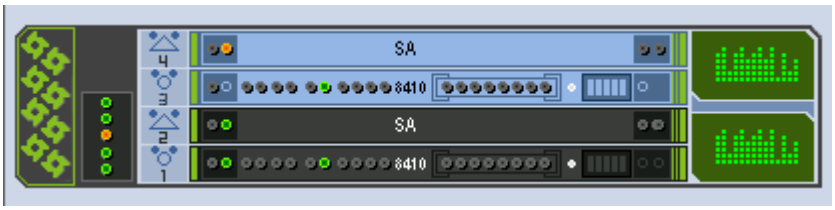
10.3 Status Pane

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).

Figure 10-1: Mediant 3000 6310 Status Pane

Figure 10-2: Mediant 3000 8410 Status Pane



The Status pane graphically presents the status of the gateway.

10.3.1 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 10-3: 6310 Active Board Status

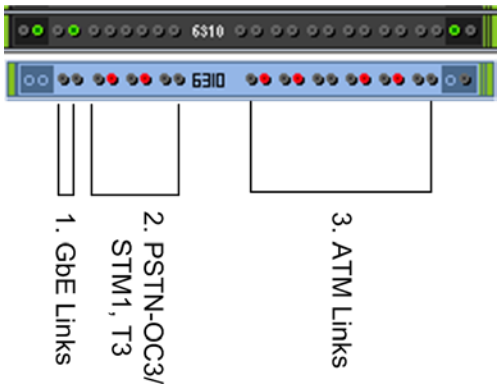
Figure 10-4: 6310 Redundant Board Status

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 10-5: 6310 Board-LED Status



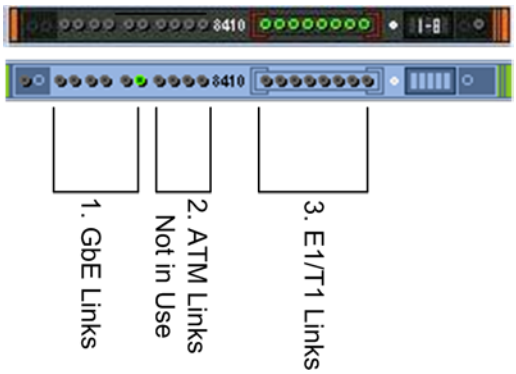
Legend

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 10-6: 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

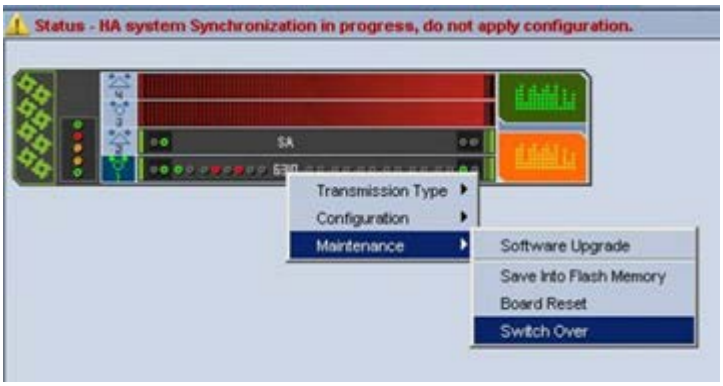
- **Power Supplies Status**

  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 10-7: Status Screen Displaying Failed Redundant Boards and Warning Notification



10.3.2 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 10-8: 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

10.3.3 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 SA board with a BITs Timing module will have the following status screen:

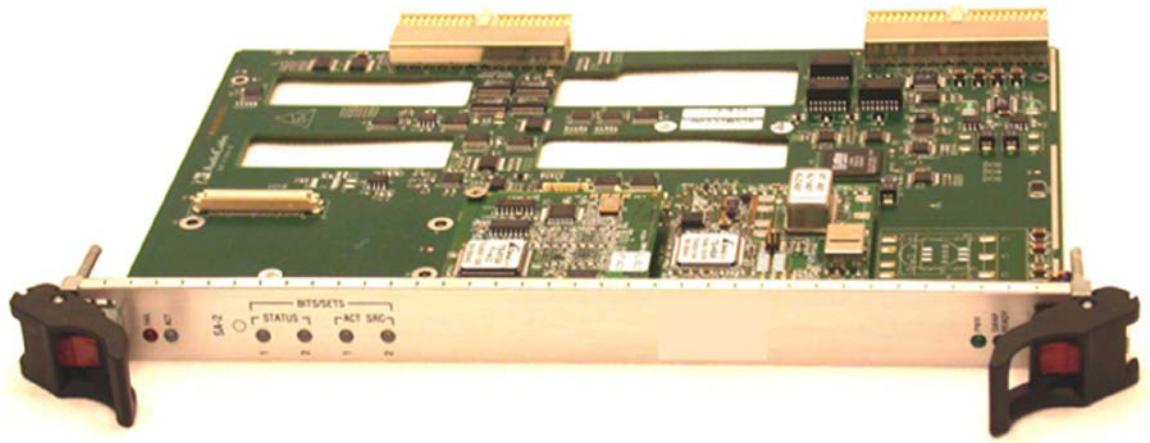
Figure 10-9: Mediant 3000 SA Board Status

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 alarm (problem), Grey -represents OFF

Figure 10-10: 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 10-11: 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

10.4 Physical and Logical Components Status and Provisioning

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

10.4.1 Navigation Hierarchy

The gateways' provisioning parameters are divided into groups / entities. Each group/entity is represented by links and sub-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 10-12: Navigation Hierarchy Links-Mediant 3000-TP-8410 Part 1

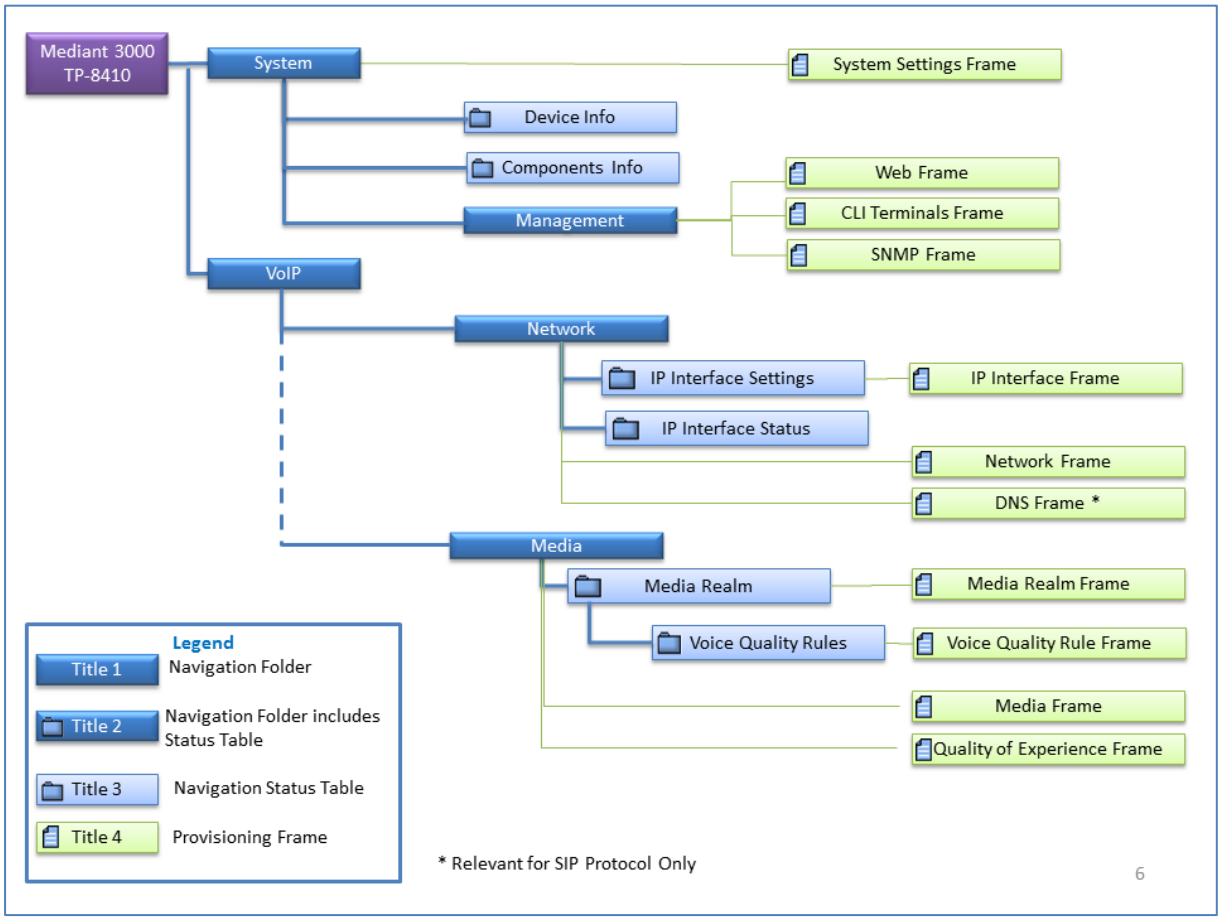


Figure 10-13: Navigation Hierarchy Links-Mediant 3000-TP-8410 Part 2

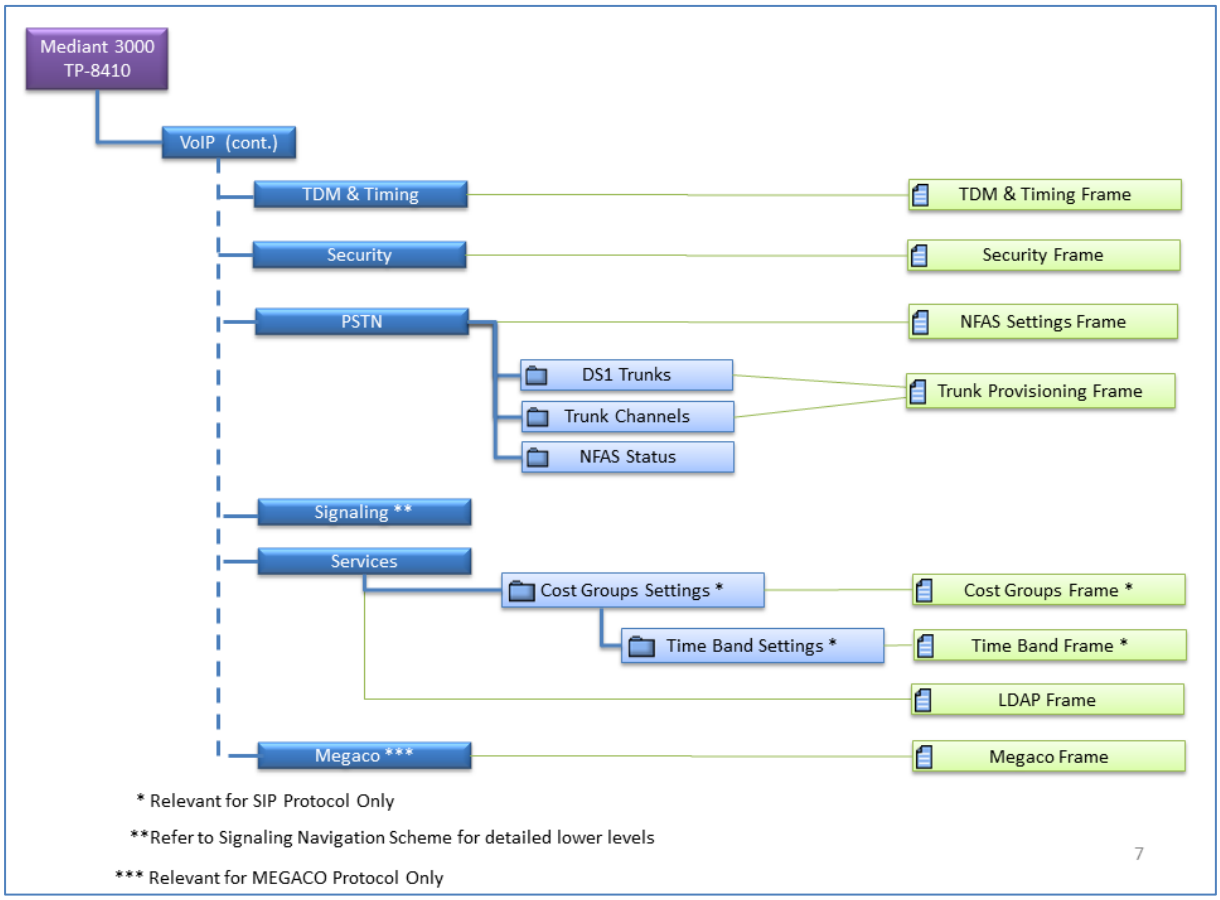


Figure 10-14: Navigation Hierarchy Links-Mediant 3000-TP-6310 Part 1

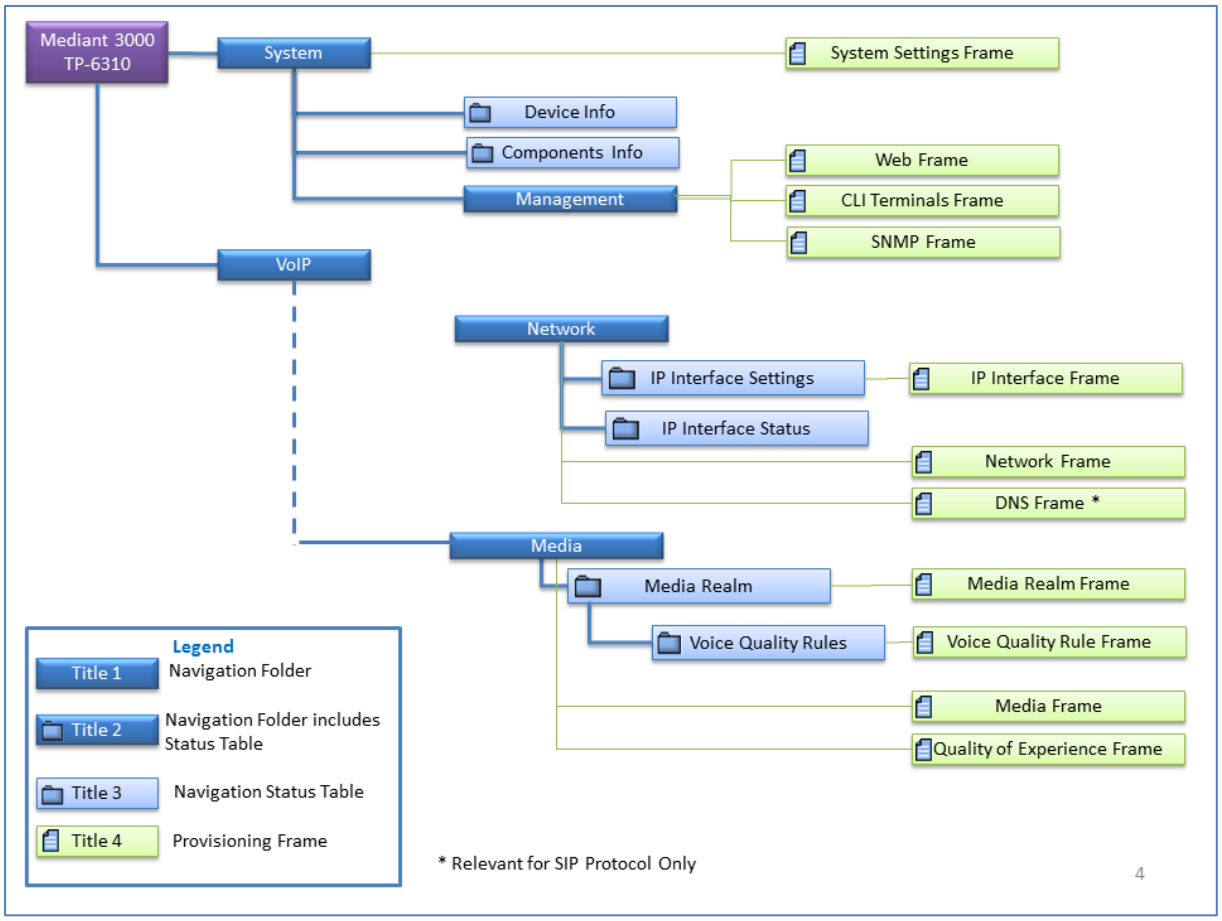


Figure 10-15: Navigation Hierarchy Links-Mediant 3000-TP-6310 Part 2

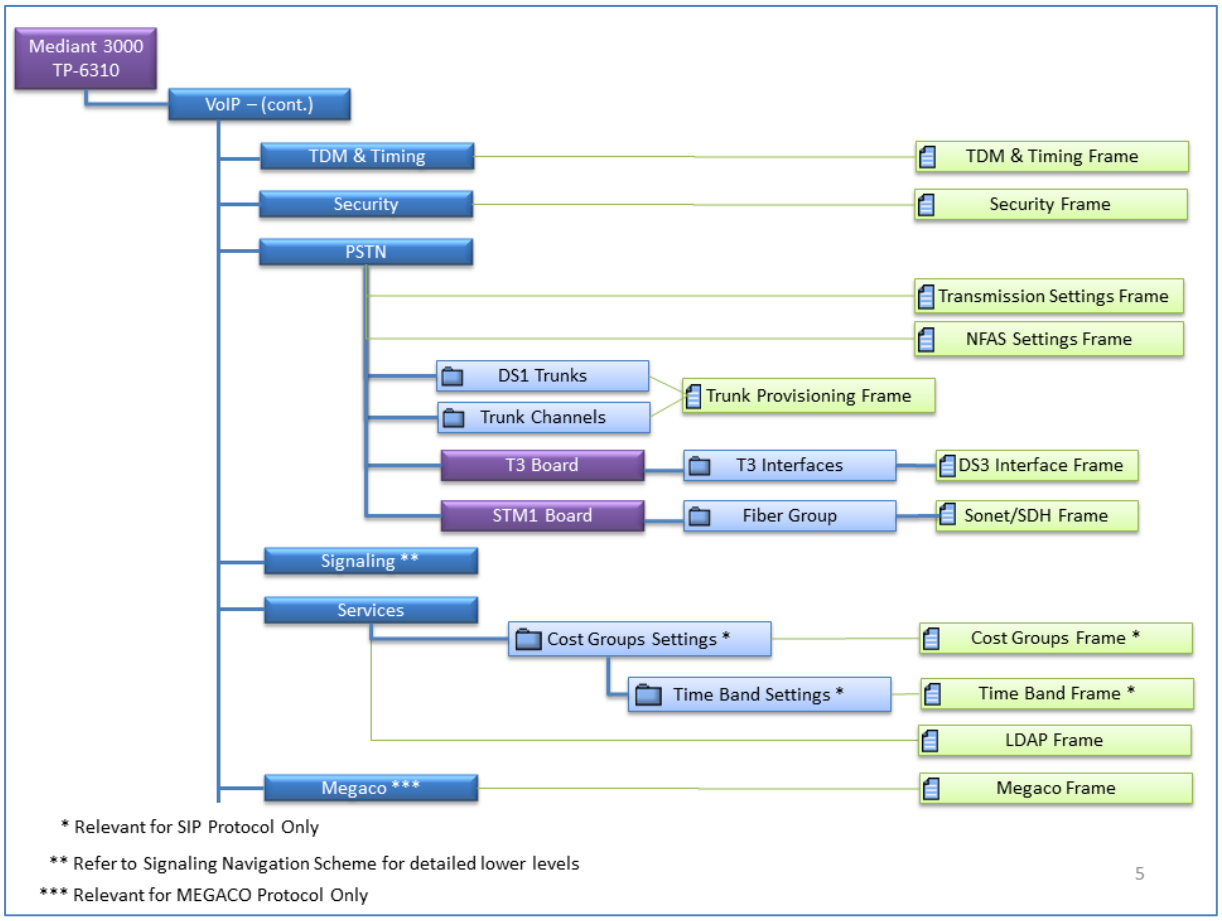


Figure 10-16: Navigation Hierarchy Links-Mediant 3000-TP-8410 and TP-6310 Part 1

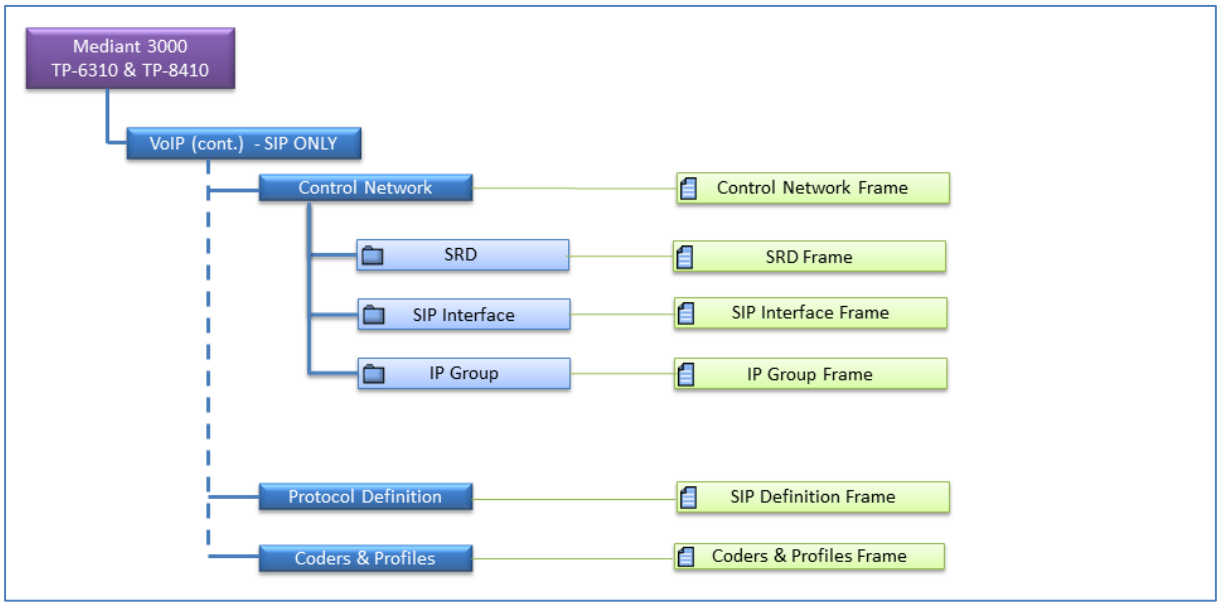
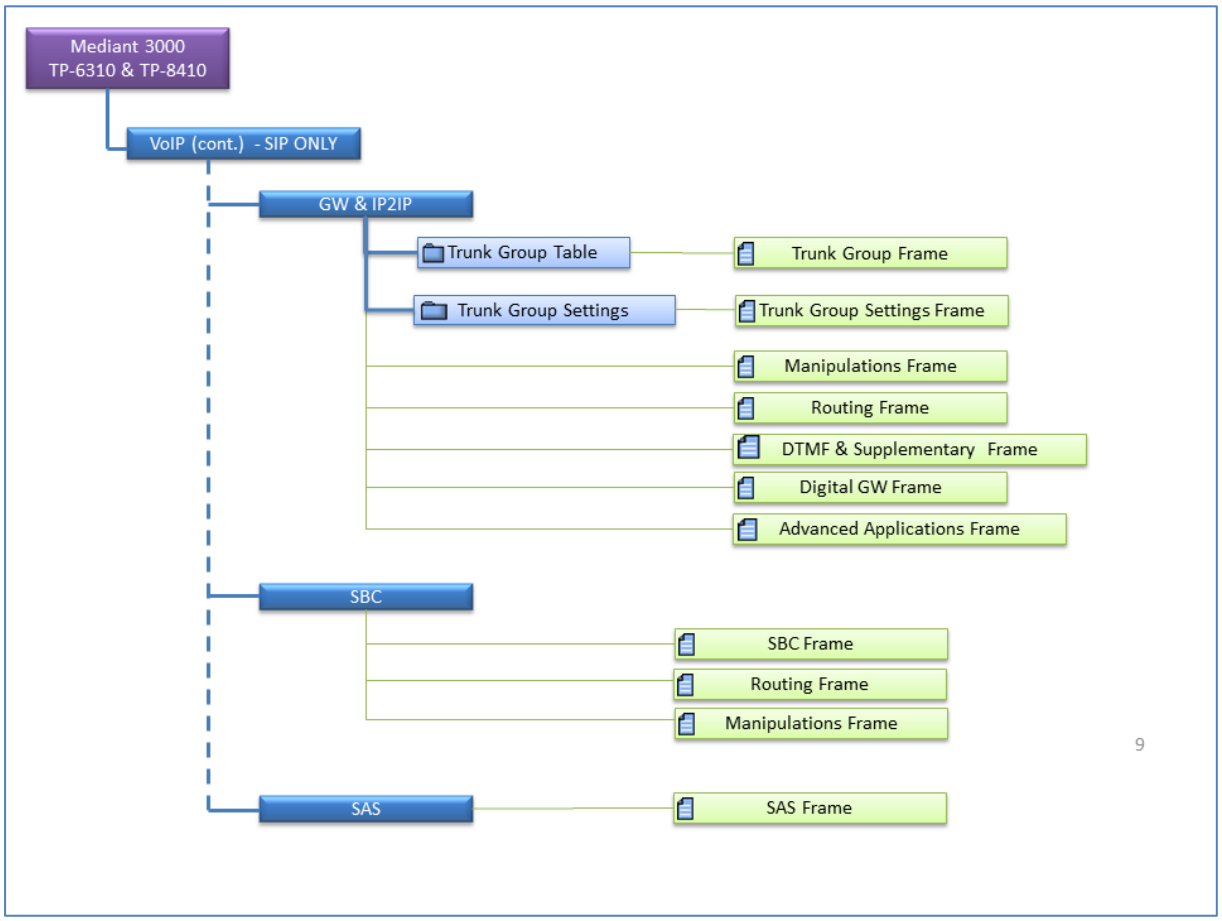


Figure 10-17: Navigation Hierarchy Links-Mediant 3000-TP-8410 and TP-6310 Part 2



See Section 'Provisioning Concepts' on page 194 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 194.

10.4.1.1 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 61.

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)*.

10.4.2 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 the TP-6310 board supports mapping to three DS3 channels using STS1 (*DS3 Channelization-Asynchronous DS3*).

The Sonet interface on the 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 151 and refer to the *Mediant 5000/8000 IOM Guide*.

Figure 10-18: SONET / SDH Table

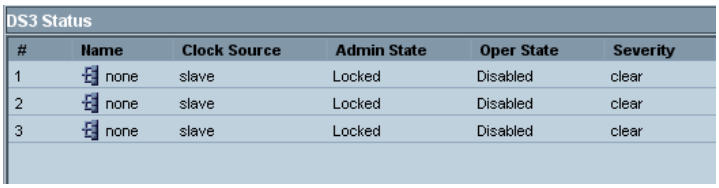
Sonet/SDH Table

#	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

10.4.3 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 10-19: Provisioning a DS3 Interface



10.4.4 DS1 Interfaces

DS1 Trunks and Trunks Channels Status screens are described in 'MediaPack' on page 187.

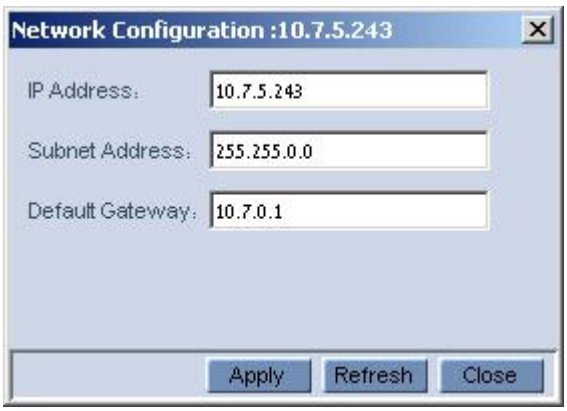
10.5 Executable Actions

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

10.5.1 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 10-20: Changing a Mediant 3000 Gateways' Network Configuration



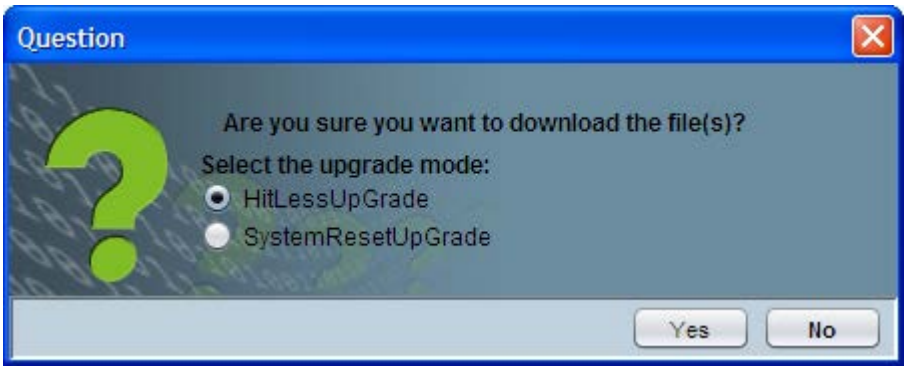
Note: Reconfiguring the network parameters might cause a loss of connection with the device. Make sure that the IP address you reconfigure is distinct from those of other devices in the tree.

10.5.2 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 10-21: Hitless Upgrade Prompt



10.5.3 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.

10.5.4 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 190.

This page is intentionally left blank

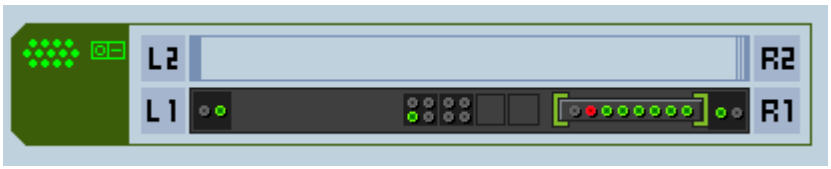
11 Mediant 2000

This section describes the Mediant 2000 status pane and provisioning.

11.1 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 11-1: 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 11-2: 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 11-3: 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 11-4: 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 172.

11.2 Provisioning

The Gateways' provisioning parameters are divided into groups / entities. Each group/entity 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 Mediant 2000 media gateway.

Figure 11-5: Navigation Hierarchy Links- Mediant 2000 (Part 1)

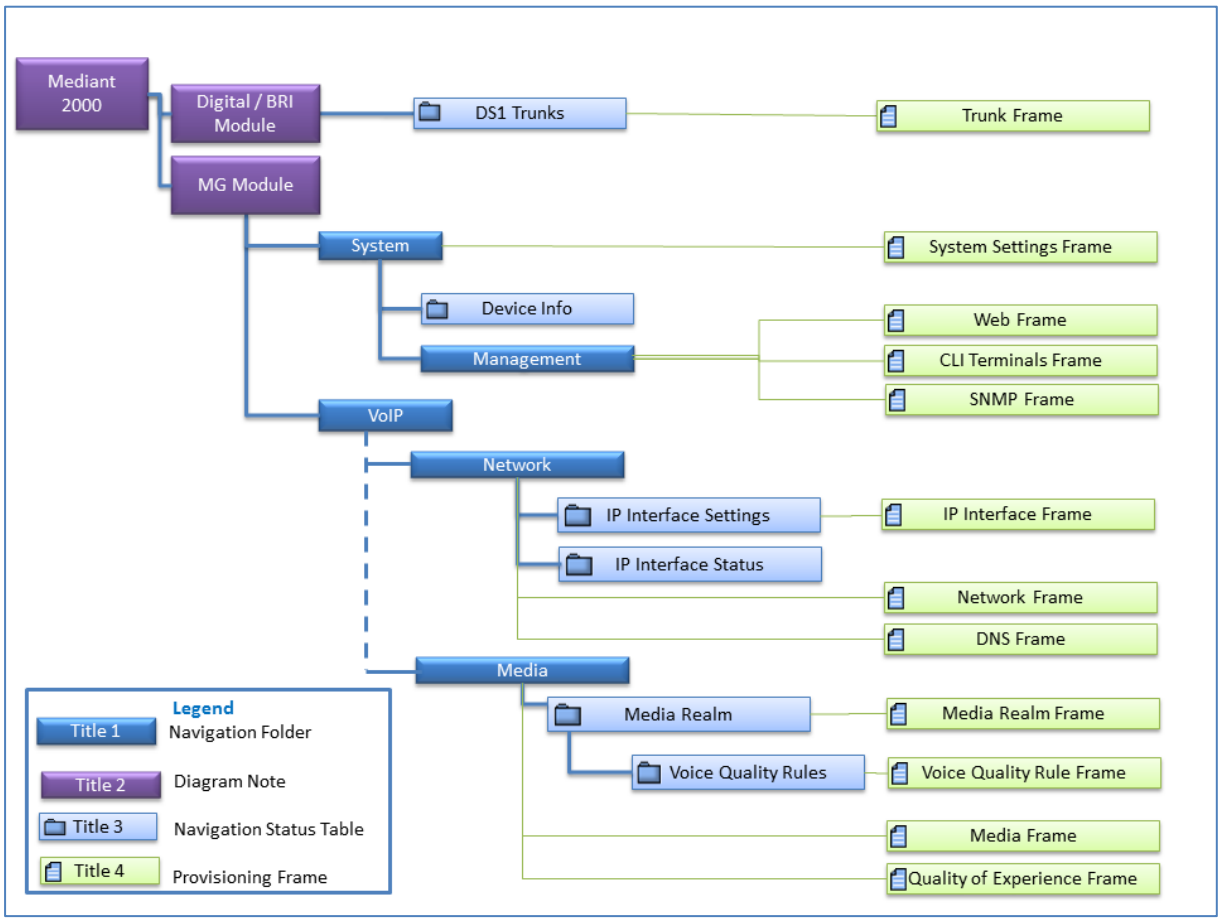


Figure 11-6: Navigation Hierarchy Links-Mediant 2000 (Part 2)

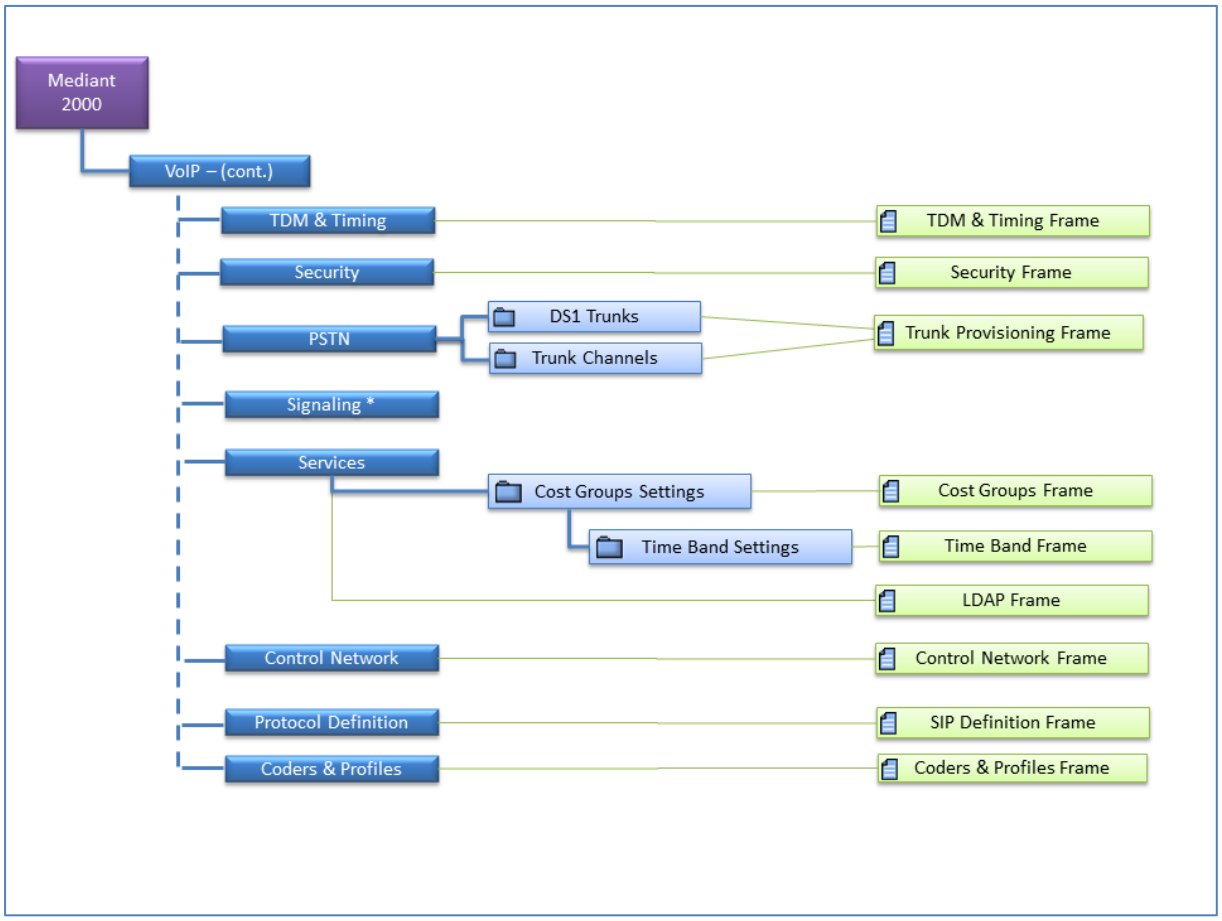
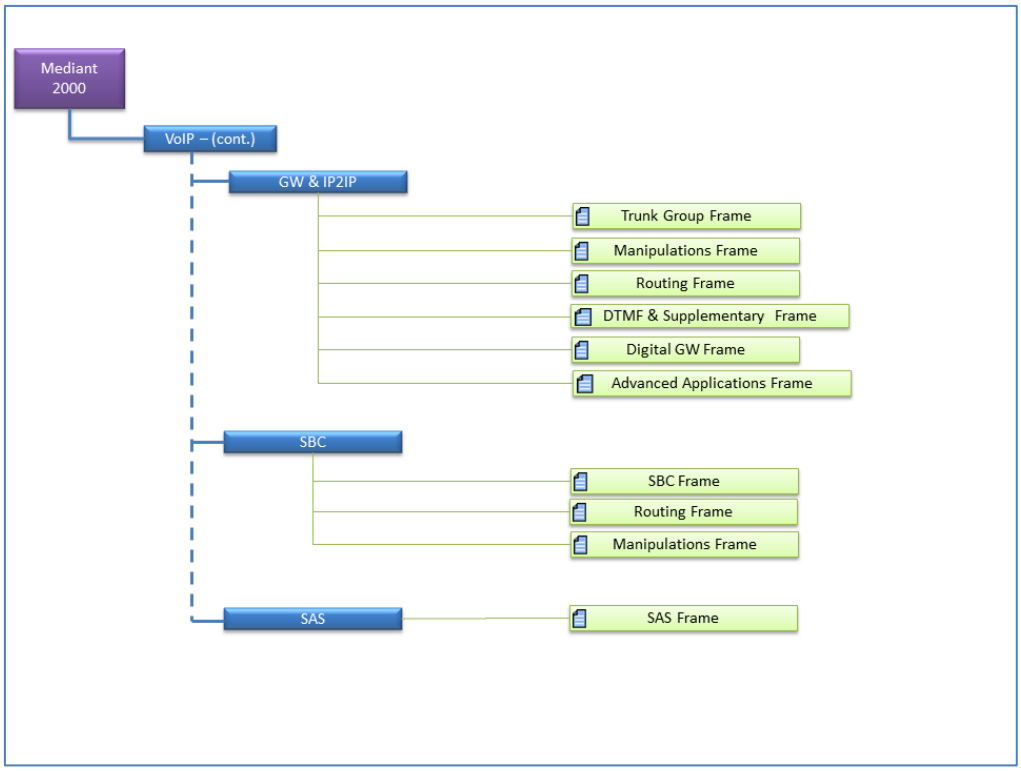


Figure 11-7: Navigation Hierarchy Links-Mediant 2000 (Part 3)



See Section 'Provisioning Concepts' on page 194 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles.

11.3 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 197.

This page is intentionally left blank

12 Mediant 600 and Mediant 1000

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

12.1 Mediant 1000 Status Pane

The figure below displays the Mediant 1000 status pane.

Figure 12-1: 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 172.

12.2 Mediant 600 Status Pane

The Mediant 600 status pane is illustrated below.

Figure 12-2: Mediant 600 Status Pane

12.3 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 Mediant 600, Mediant 800 MSBG, Mediant 800 E-SBC, Mediant 1000, Mediant 1000 MSBG and Mediant 1000 E-SBC gateways.

Figure 12-3: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 (Part 1)

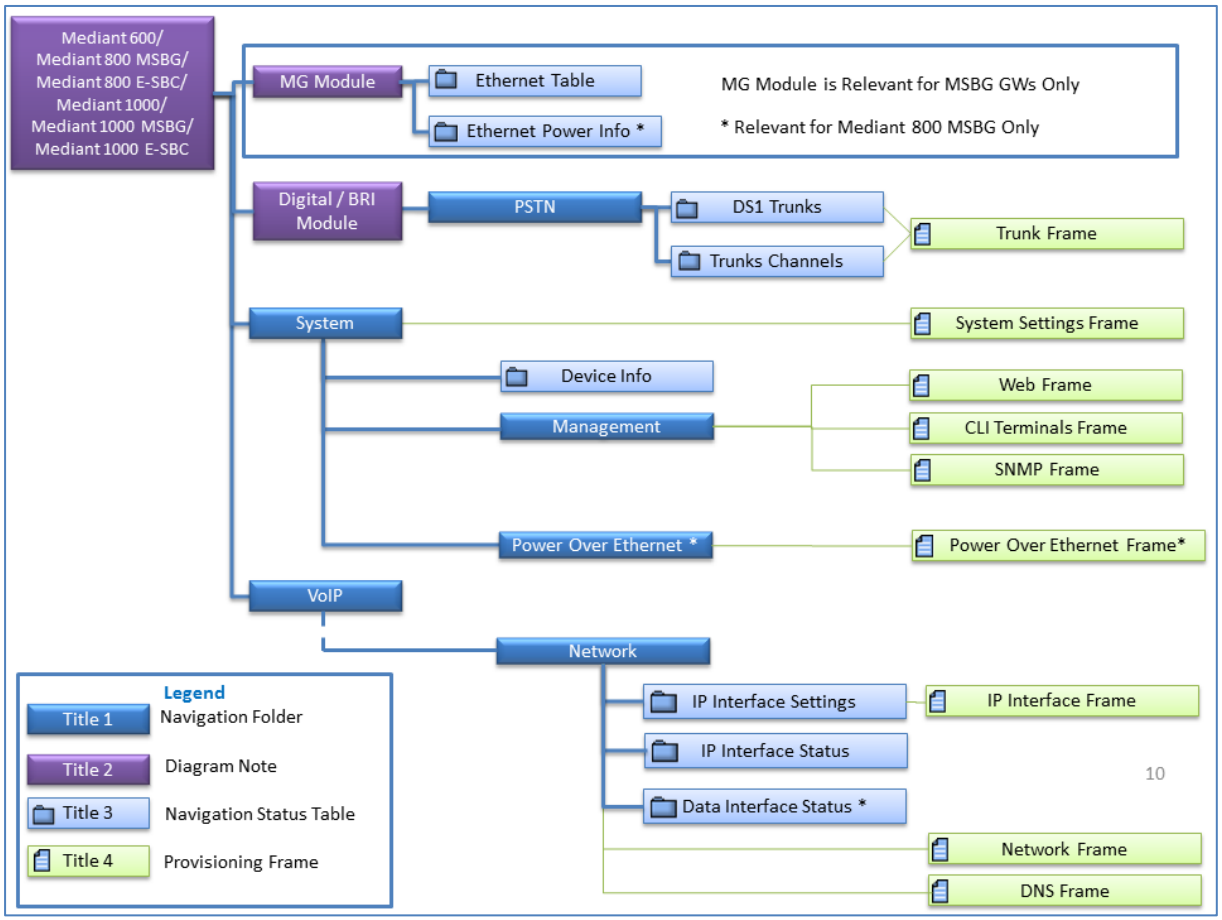


Figure 12-4: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 (Part 2)

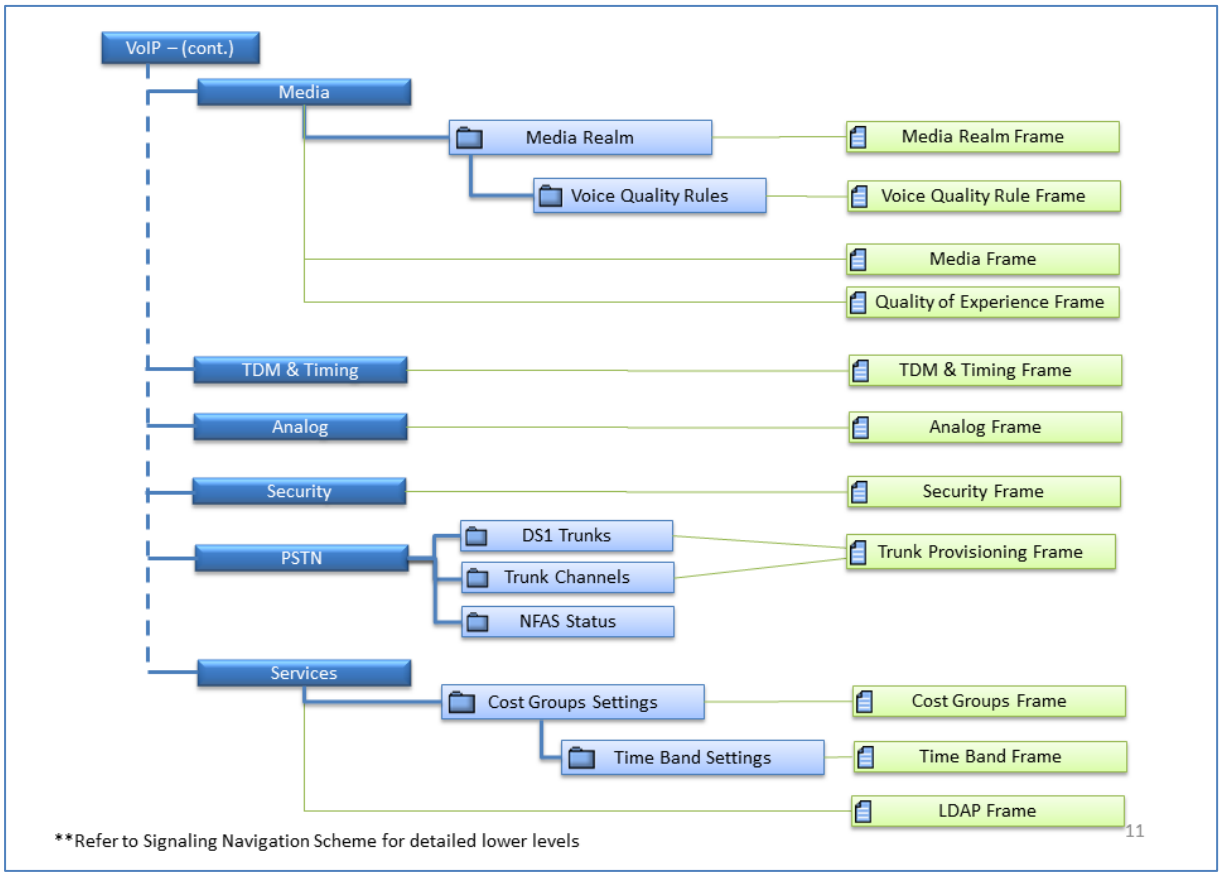


Figure 12-5: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 (Part 3)

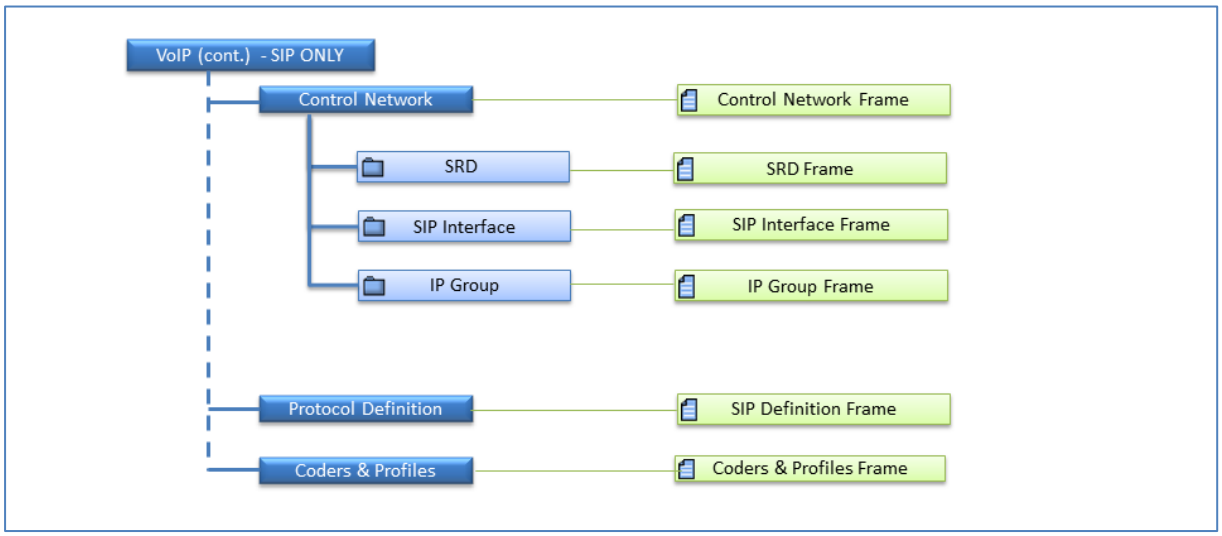
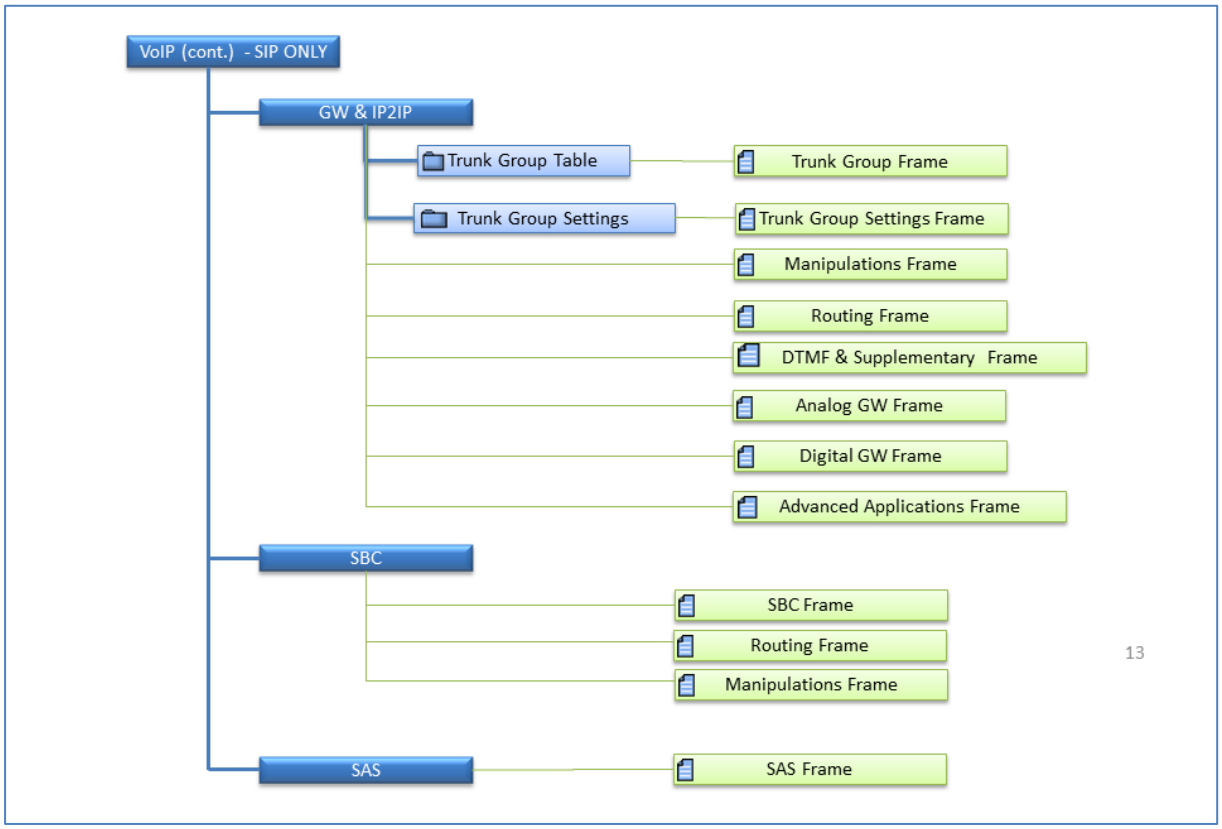


Figure 12-6: Navigation Hierarchy Links-Mediant 600/Mediant 800 and Mediant 1000 (Part 4)



See Section 'Provisioning Concepts' on page 194 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

12.4 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 197.

13 Mediant 800 MSBG

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

13.1 Status Pane

The figure below displays the Mediant 800 MSBG status pane.

Figure 13-1: Mediant 800 Status Screen

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 one of the Ethernet ports to display the detailed status for each port.

Figure 13-2: Mediant 800 MSBG 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

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: Mediant 800 MSBG 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 *Mediant 800 MSBG SIP User's Manual.*

13.2 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 Mediant 800 MSBG navigation hierarchy links are included in the Mediant 1000 and Mediant 600 schema ('Mediant 1000 and Mediant 600 Provisioning' on page 182).

13.3 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 197.

14 MediaPack

This section describes the MediaPack status pane and provisioning.

14.1 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 14-1: MediaPack Status Pane

The Status pane represents MediaPacks and their 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 14-1: 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 14-1: 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 that a reset must be performed to apply these parameters to the media gateway.

14.2 Line Test

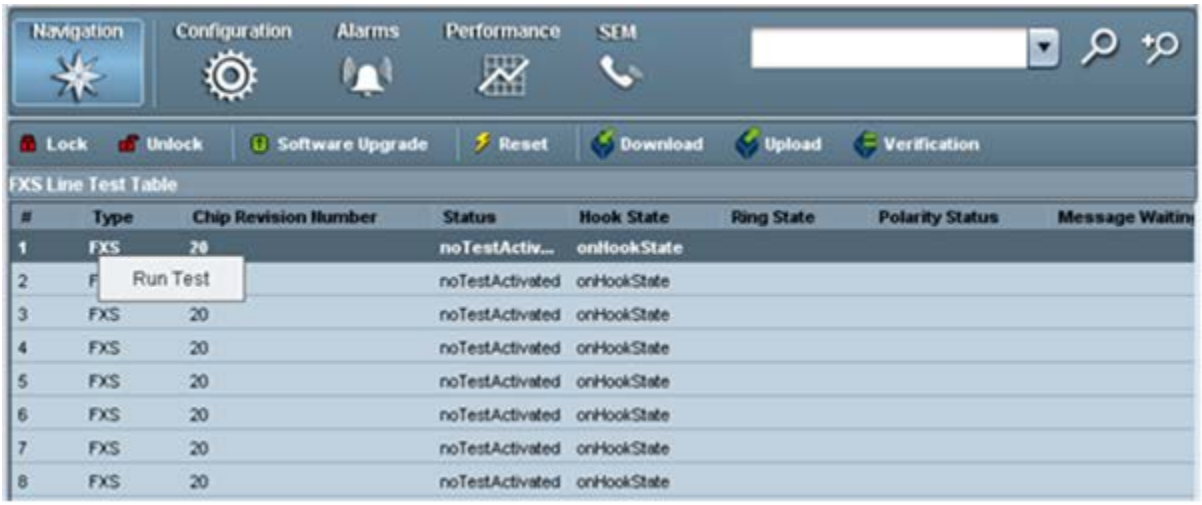
The MediaPack media gateway supports Line Testing.

➢ **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 14-2: MediaPack Line Test



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 MediaPack.

Figure 14-3: Navigation Hierarchy Links-MediaPack

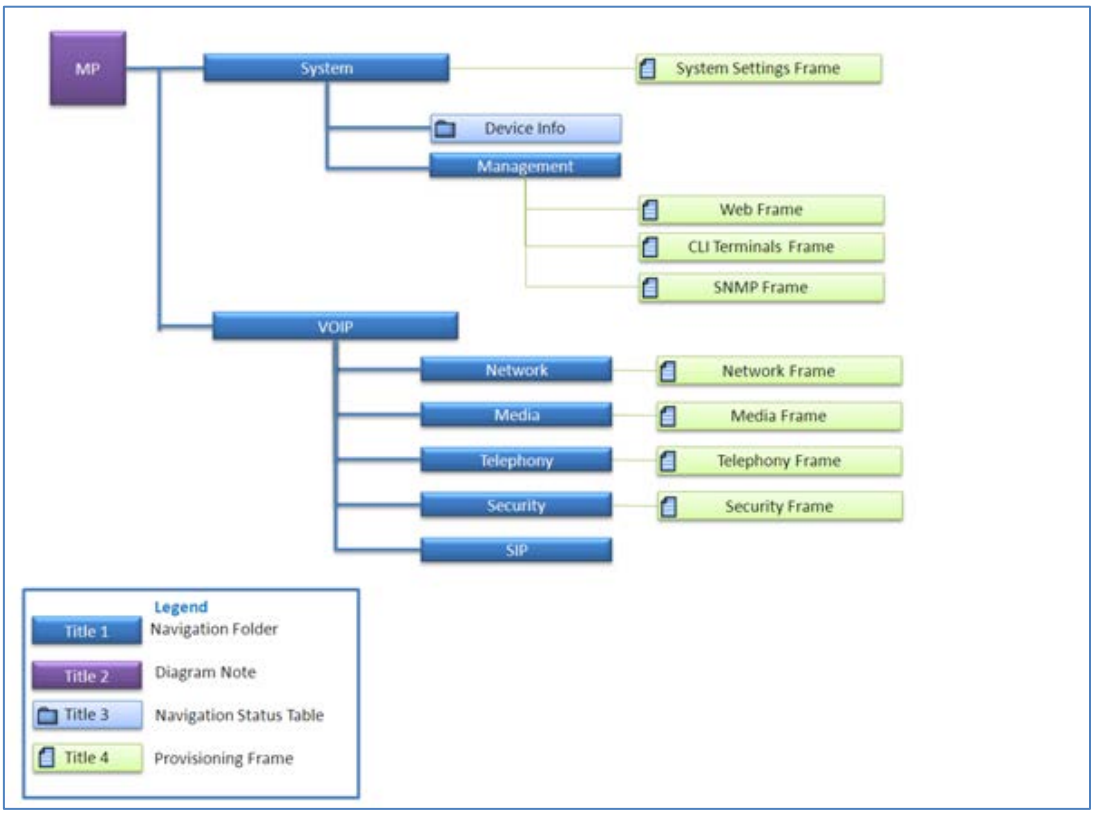
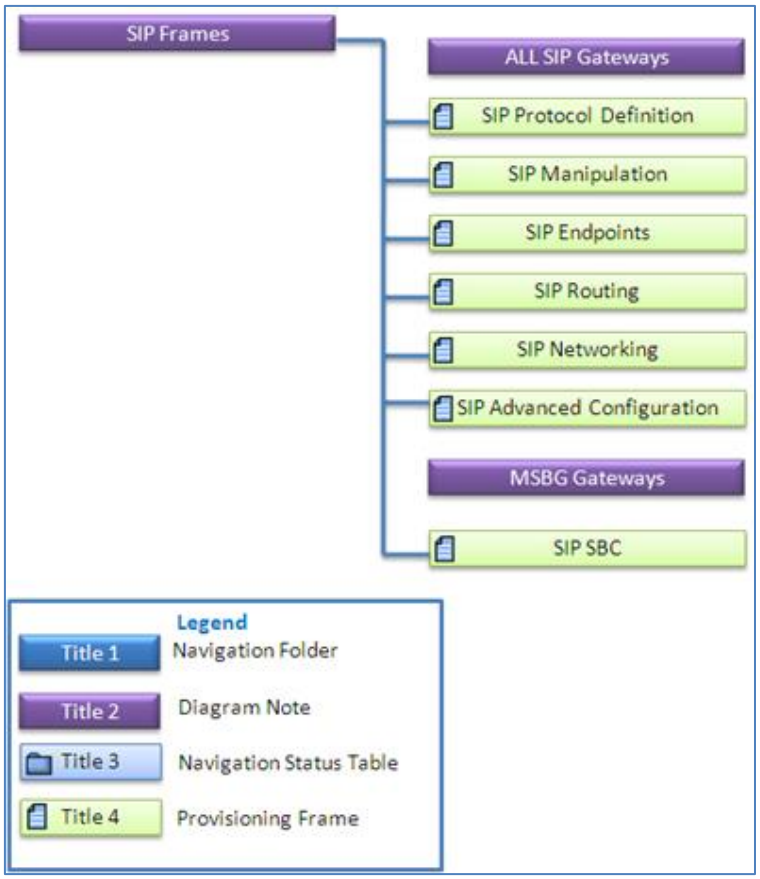


Figure 14-4: MediaPack-Hierarchy Links (Part 2)



See Section 'Provisioning Concepts' on page 194 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles on provisioning parameters.

14.4 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 197.

15 Trunks and Channels Status

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

15.1 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 trunk 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 reset. 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 15-1: 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 15-1: 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

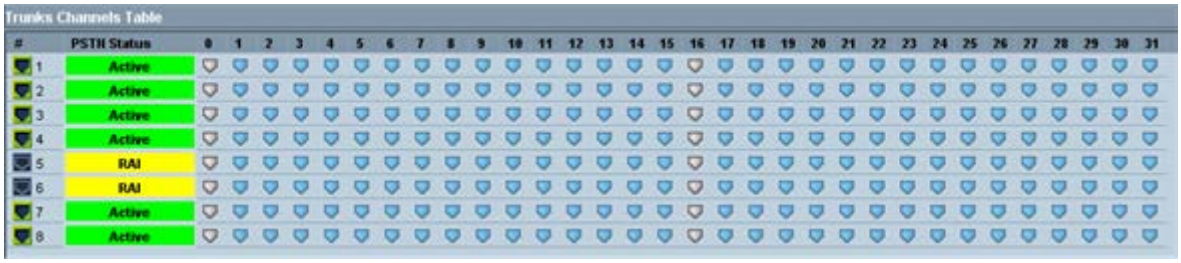
15.2 Trunk Channel Call Status

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 15-2: Trunk Channel Call Status

Channel Color	Channel Call Status
	Active
	Inactive
	Non-Voice
	SS7
	ISDN Signaling (D-channel)
	CAS Blocked

Figure 15-2: 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																																

16 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 194 for information on the parameter provisioning types, how to work with table status columns and how to create and apply profiles.

16.1 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 16-1: SS7 Hierarchy Levels-Mediant 3000 and Mediant 2000

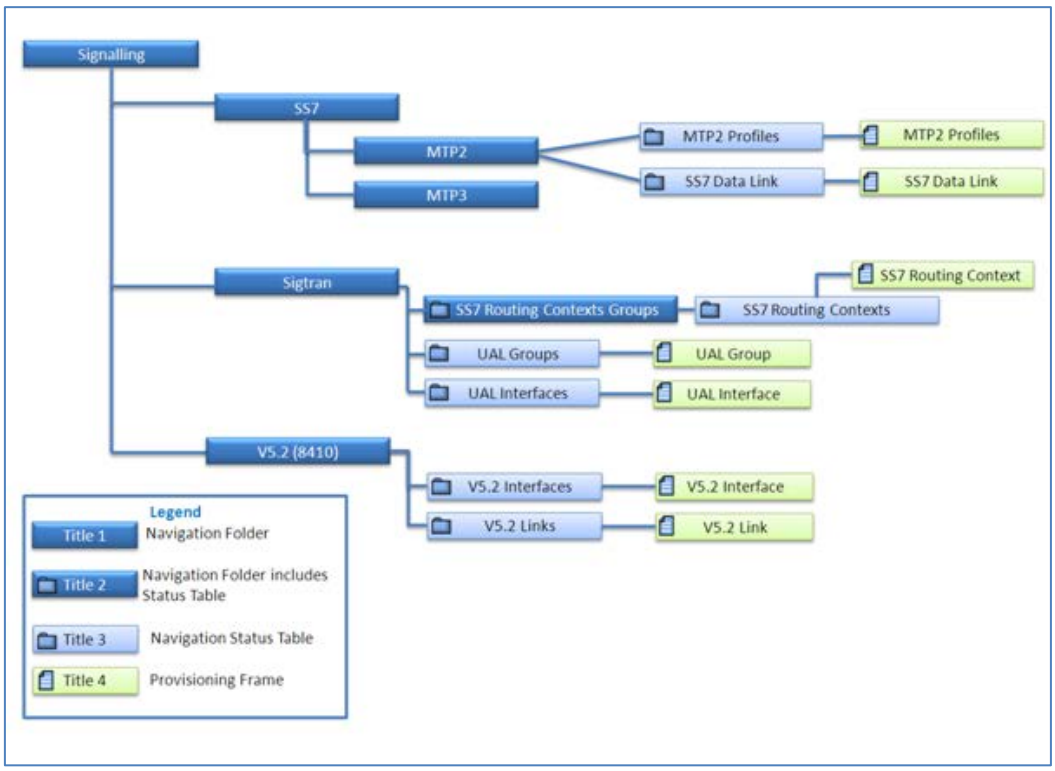
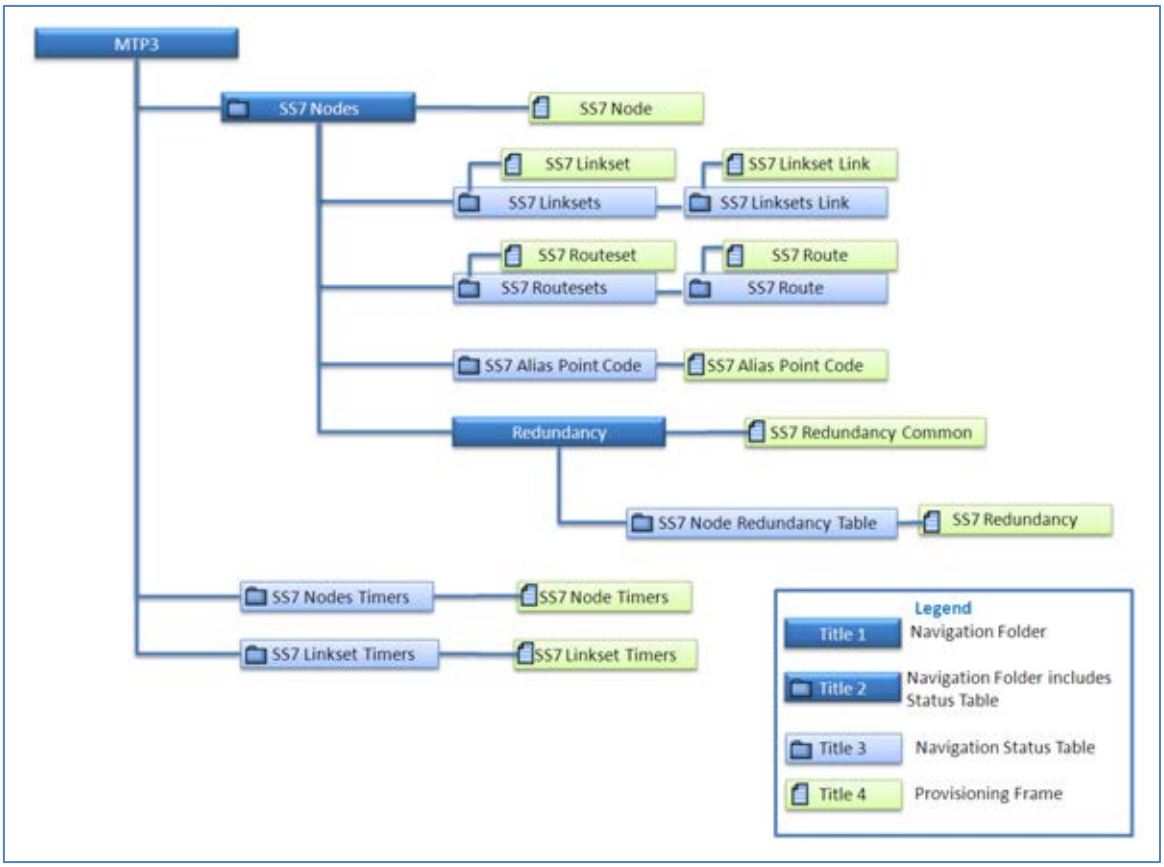


Figure 16-2: MTP3 Hierarchy Levels-Mediant 3000 and Mediant 2000



Part III

Actions and Provisioning

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

.

17 CPE Configuration and Maintenance Actions

This section describes the CPE Configuration and Maintenance actions.

17.1 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 subset of the most commonly performed actions and may differ according to the relevant media gateway type and version.

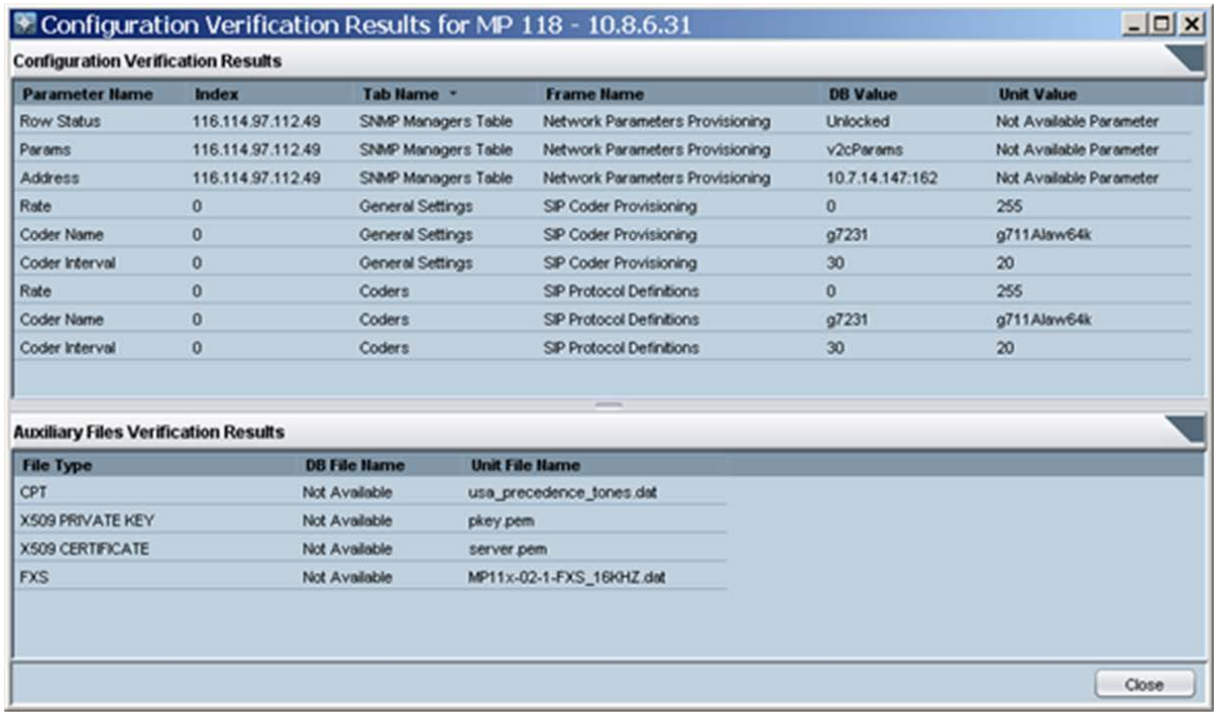
Figure 17-1: Configuration Actions menu

- **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 17-2: Configuration Verification Results



- **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.
- **Create Master Profile**: Saves all profiled media gateway parameters as a Master Profile. For more information regarding Master Profile, see Section 'Creating a Master Profile' on page 219.
- **Apply Master Profile**: Loads the Master Profile configuration to the media gateway. For more information in reference to the Master Profile, see Section 'Attaching a Master Profile to one or to Multiple media gateways' on page 221.

17.2 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 17-3: 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).

17.3 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.

This page is intentionally left blank

18 Provisioning Concepts

This section describes the EMS provisioning concepts.

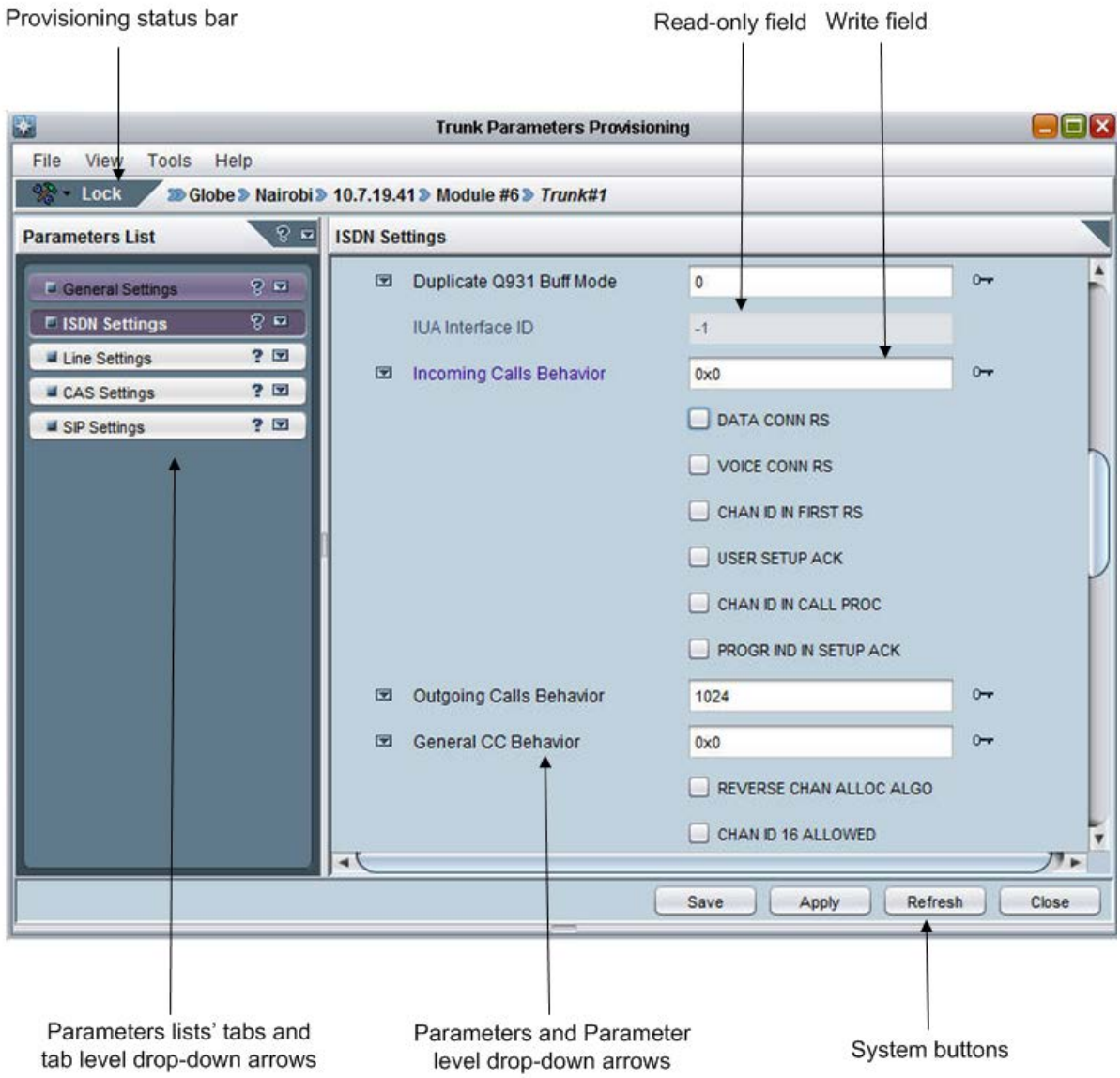
18.1 Working with the EMS's Provisioning Screens

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 18-1: TP-6310 Board Provisioning Parameters



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 18-1: 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 18-2: 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:

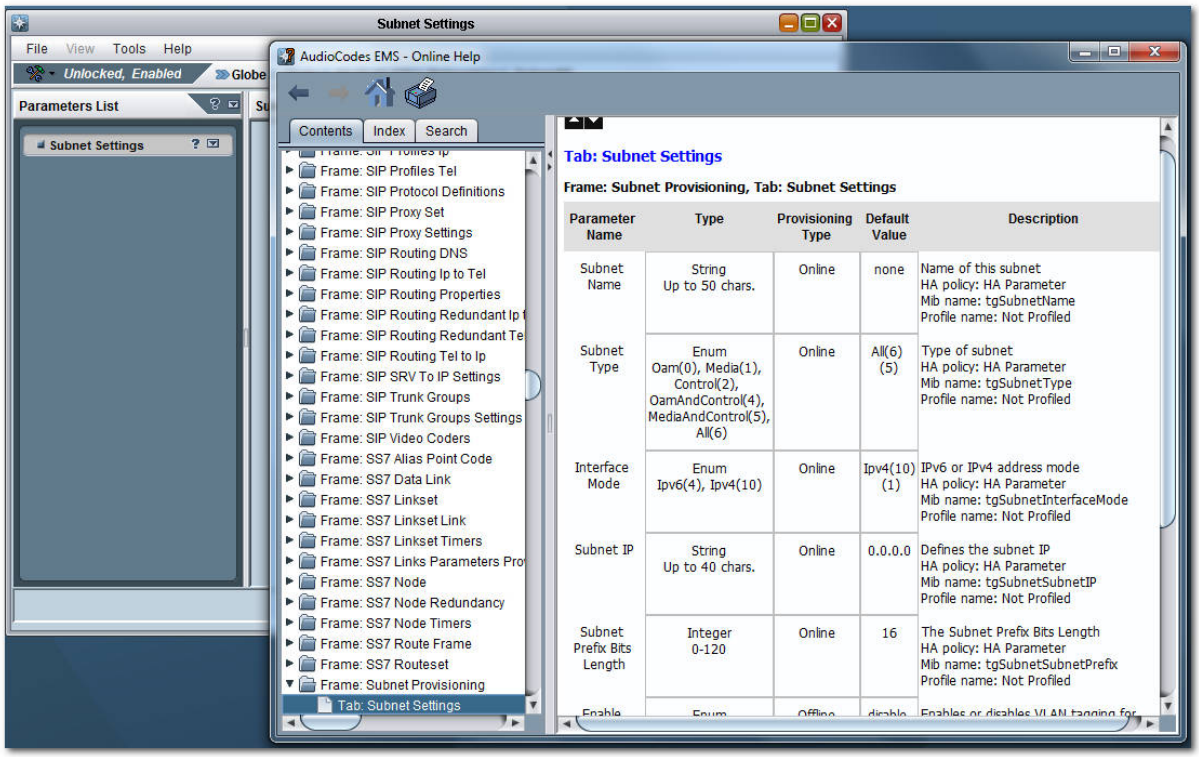
  - Right-clicking on a table row and choosing an Add / Remove / Lock / Unlock action does not then require clicking the **Apply** button; the action is executed immediately. Pressing CTRL-A enables you to select all rows in the configuration table at the same time.
  - When you finish editing a cell in 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 18-3: Online Help



18.1.1 Provisioning Procedure for Mediant 5000 and Mediant 8000

This section covers the Mediant 5000 media gateway and Mediant 8000 media gateways.

➢ **To provision a Mediant 5000 Media Gateway and Mediant 8000 Media 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.

18.1.2 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.

18.2 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 18-2: 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.

18.3 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):

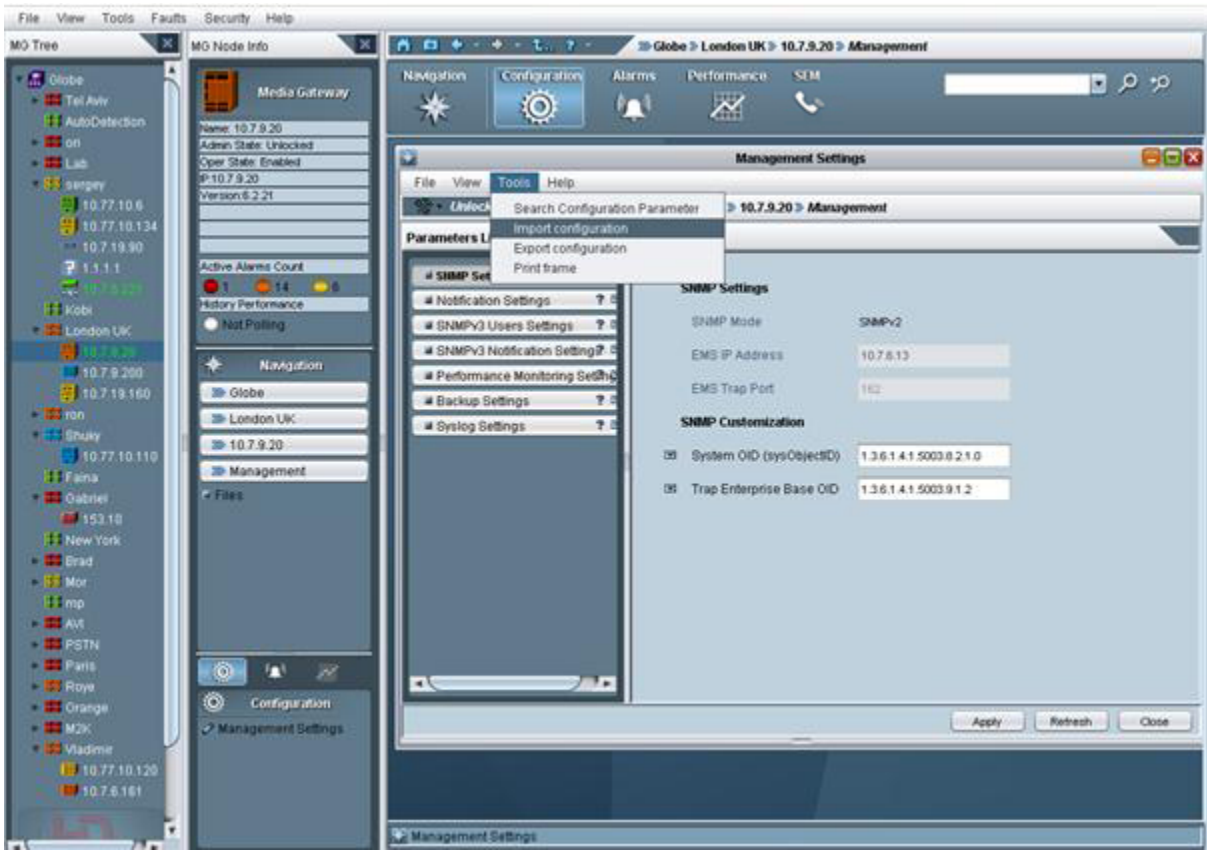
Table 18-3: Indication Mapping Summary-Parameters HA Type

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

18.4 Exporting, Importing an Entity Configuration as a File

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

Figure 18-4: Importing an Entity Configuration



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.

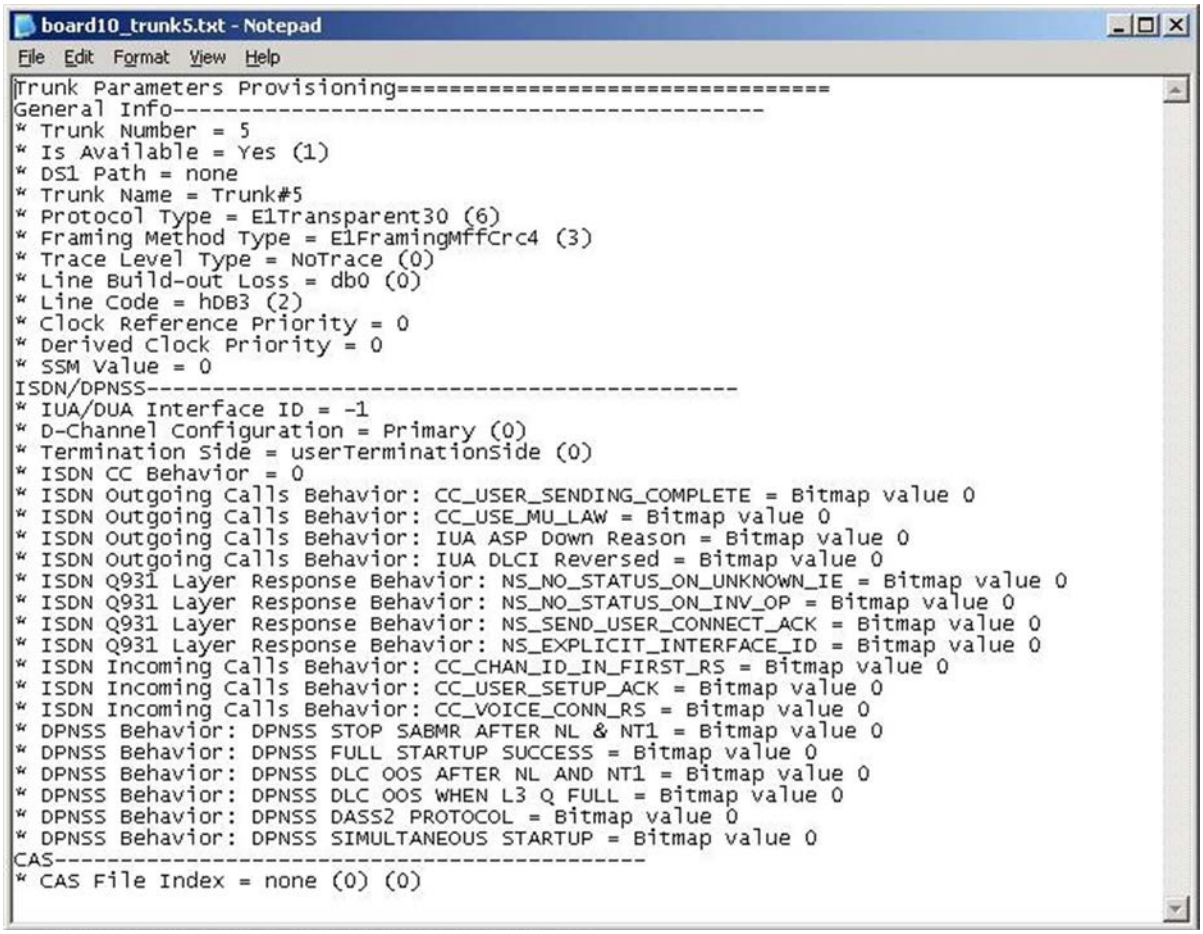
18.5 Printing an Entity's Configuration as a File

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 18-5: Trunk Print Format



18.6 Provisioning Entity Profiles

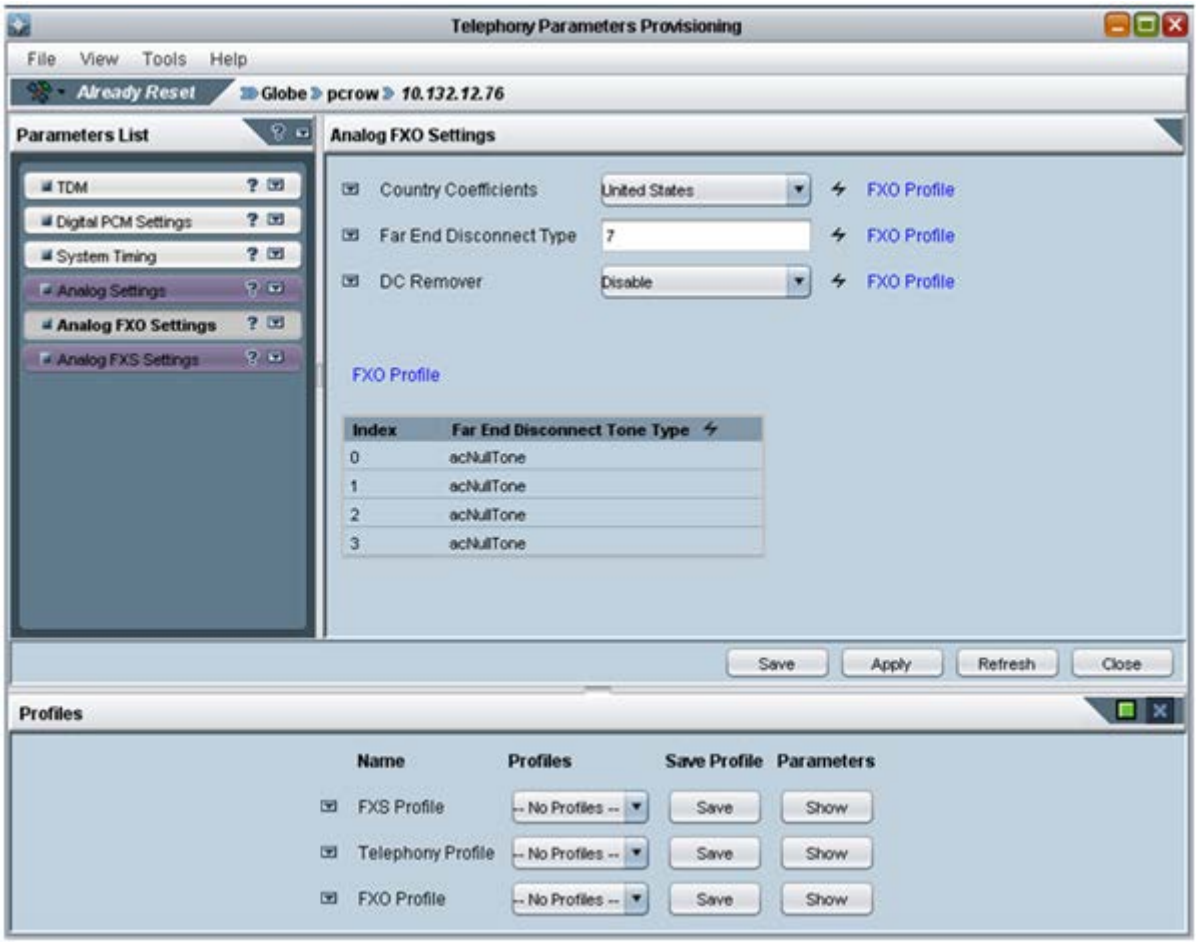
The EMS's Profile Management enables Customers to rapidly provision values to entity parameters by loading a profile. To enable the Profile Manager, in the Provisioning Frame View menu, select **View > Profiles Manager**. The Profile Manager is displayed in the lower pane of the Provisioning screen.

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

Customers can also delete profiles from the pool of profiles.

Each profile includes a specific entity's parameters displayed in that entity's parameters provisioning screen.

Figure 18-6: Profile Management



18.6.1 Creating Entity Profiles

This section describes how to create entity profiles.

Note: Entity profiles cannot be modified.

➢ **To save an entity's parameter values in an entity profile:**

1. Click the **Show** button located in the same row as that of the profile; the 'Show Parameters' screen is displayed on top of the parameters provisioning screen, listing all parameters that are under the requested profile and their tab location. Alternatively, you can select **Show** icon on the 'Profile Management' pane, and Name of the profiles will be added to the profiled parameters.
2. Edit/modify the parameter/s field/s and click the **Save** button in the Profiles Management pane; you're prompted in the 'New Profile' prompt (field 'Provide a New Profile Name') for a new name for the profile whose parameter/s / field/s you've modified.
3. Click **OK**; the modified values of the parameter/s field/s are saved in the new profile and the new profile is added to the 'Profiles' drop-down list; the current media gateway's entity is now attached to the new profile.

18.6.2 Loading and Attaching an Entity Profile

This section describes how to load and attach an Entity Profile.

➢ **To load an entity profile:**

1. From the 'Choose Profile' drop-down list, select the profile to attach to the entity.
2. Click **Apply** to load your changes to the media gateway and save the attachment.

➢ **To attach a profile to all trunks in the Trunks Parameters Provisioning screen:**

1. In the 'Choose Profile' drop-down list, select the profile to attach to the trunks.
2. Click the **Apply to All** button to attach the profile to the trunks.

18.6.3 Detaching a Profile from an Entity

A profile is detached from an entity when one of the following events occurs:

- You change one of the parameters in a profile already attached to an entity. When saving the new profile (with the modified parameter), the previous profile is detached from the entity. After clicking **Save** or **Apply**, you're prompted with a notification message indicating that the profile is detached from the entity.
- You loaded a different profile to an entity already attached to a profile. When clicking the **Save** or **Apply** button, the entity is detached from the previous profile and attached to the new profile.
- You delete a profile from an entity and the entity is the only entity attached to the profile.

18.6.4 Removing a Profile

This section describes how to remove an entity profile.

➢ **To remove a profile from the profiles pool:**

- Click the arrow adjacent to the Profile Name to choose option **Remove Current Profile** from the pop-up.

Note: The current profile is removed if and only if no other entity is attached to this profile beside the current entity (for whom the screen is opened). If there is another entity attached to the profile, the 'Remove Profile' function fails and a list of the currently attached entities is displayed.
Therefore, before removing a profile from the profiles pool, first detach it from any entity it may be attached to (see Section 'Detaching a Profile from an Entity' on page 217).

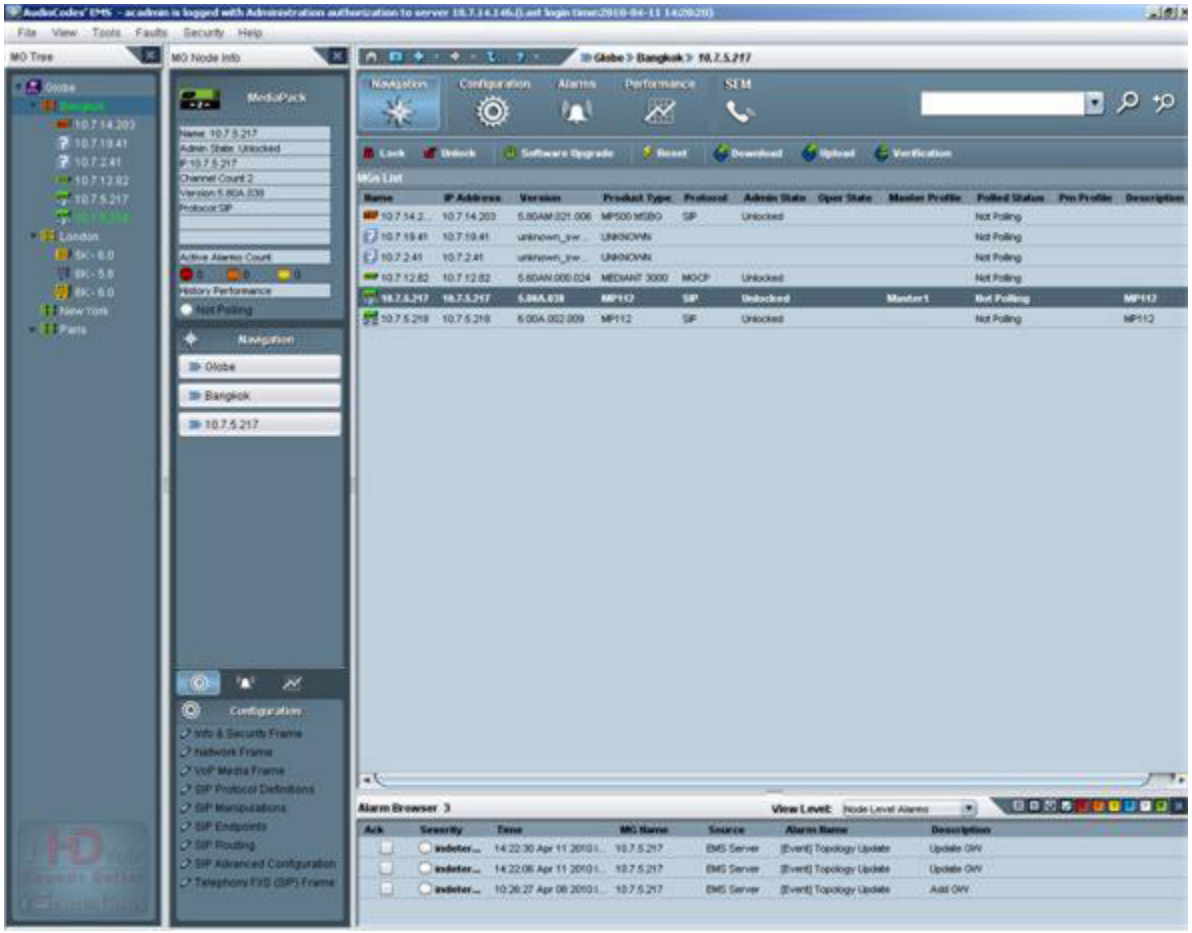
18.7 Master Profile for CPE Products

This section describes how to manage the Master Profile for CPE Products.

18.7.1 Ascertaining a Device's Master Profile

In the column captioned Master Profile in the MGs List status screen, operators can ascertain whether a master profile is attached to a media gateway and (in the event that a master profile is attached) the name of the master profile (refer the figure below).

Figure 18-7: PROFILE Column in MGs List Status Screen



18.7.2 Creating a Master Profile

This section describes how to create a Master Profile.

Notes:

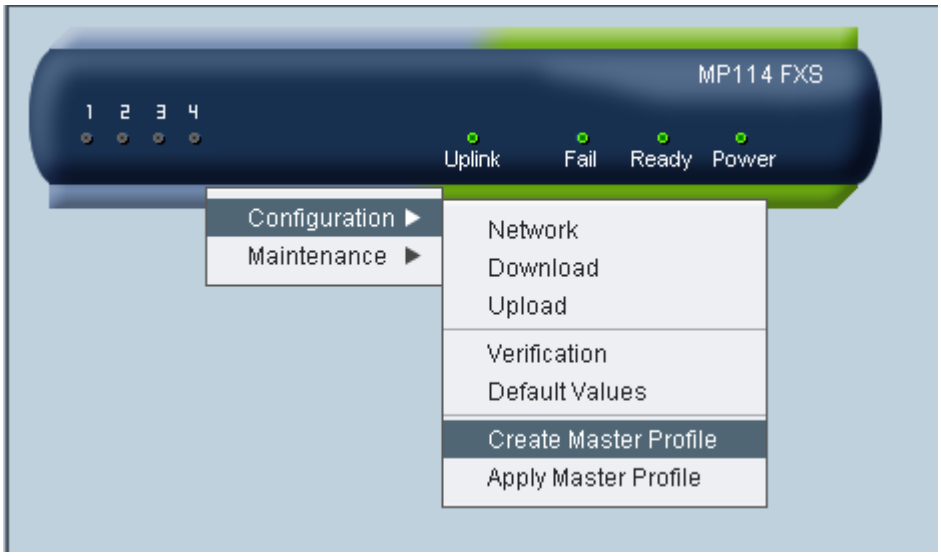
- All tables MUST be unlocked to create a master profile (CPE products).
- A master profile cannot be modified after it is created. Operators must instead modify the configuration of the media gateway and then save the new configuration as a new master profile (to be applied to the media gateways).

After configuring the parameters of the media gateway, operators can save the configuration as a master profile. The master file comprises five or more (depending on the control protocol configured in the device) entity profiles (for detailed information on entity profiles, see Section 'Creating Entity Profiles' on page 216).

If an entity profile is created and loaded to the media gateway prior to the creation of the master profile, then when the media gateway configuration is saved as a master profile, the master profile incorporates and uses this (previously created and loaded) entity profile.

In the event that no entity profile/s was/were created and loaded prior to the creation of a master profile, the master profile is created from individual parameters (associated with each of the 5 entities).

Figure 18-8: Creating a Master Profile for the Media Pack



➢ To create a master profile:

1. Select a media gateway board, right-click and in the Configuration sub-menu, choose **Create Master Profile**; the prompt 'New Master Profile' appears (shown in the figure below).

Figure 18-9: New Master Profile Prompt

2. Enter a name for the master profile in the field 'Save Master Profile' and click **OK**.

➢ To create a master profile using an alternative procedure:

1. In the MGs List, select the media gateway to which to attach a master profile.
2. Right-click the selected media gateway and from the pop-up menu, choose option **Create Master Profile**; the New Master Profile prompt appears (shown in the figure above).
3. Enter a name for the master profile in the field 'Save Master Profile' and click **OK**.

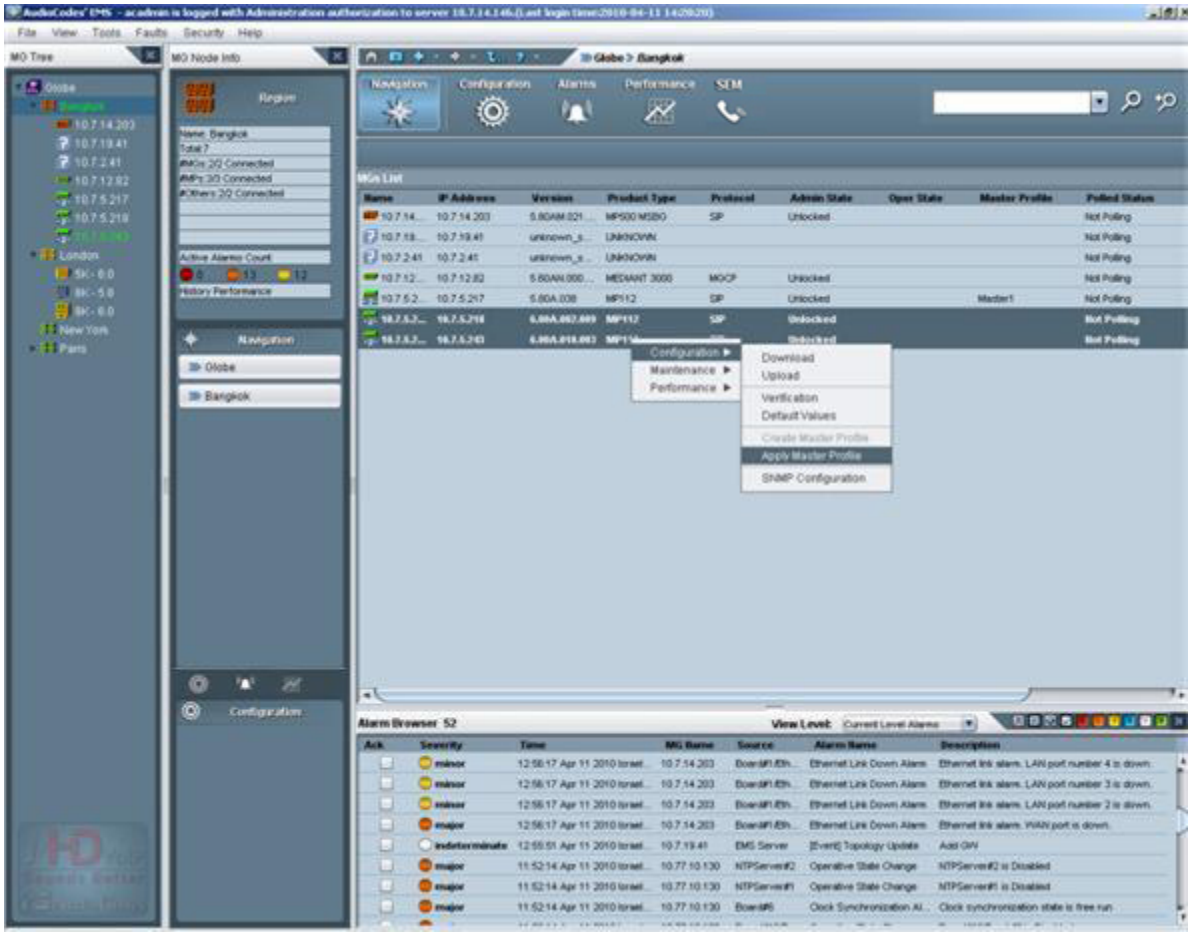
18.7.3 Attaching a Master Profile to Media Gateways

This section describes how to attach a Master Profile to a single media gateway or to multiple media gateways.

➢ **To attach a master profile to a media gateway (or to multiple media gateways of the same type, configured with the same call control protocol):**

1. In the MGs List, select a CPE device (or select multiple instances of the same device configured with the same call control protocol).

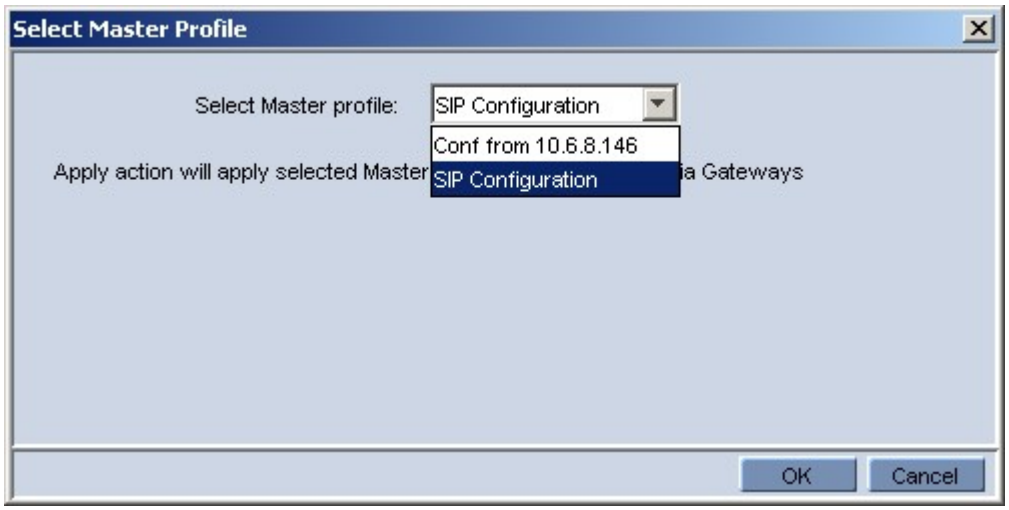
Figure 18-10: Selecting the MediaPacks to Which to Attach a Master Profile (in the MGs List)



2. Right-click the selected media gateway (or on multiple selected devices) and from the pop-up menu, choose option **Apply Master Profile**; the 'Select Master Profile' prompt appears on the screen (shown in the figure below).

Figure 18-11: Select Master Profile Screen

Figure 18-12: Selecting a Master Profile to Apply



3. Select the Master Profile you require (refer to the figure above) and click **OK**; the master profile you selected is attached to all selected devices.

18.7.4 Detaching a Master Profile

A profile is detached from a media gateway in the event:

- You change one of the configuration parameters in the media gateway. After clicking **Save** or **Apply**, you're prompted with a notification message indicating that the profile is detached from the media gateway.
- You apply a master profile to a media gateway that is already attached to a master profile and the two master profiles are different. When clicking **Save** or **Apply**, the media gateways detached from the previously applied master profile and the new profile is applied.

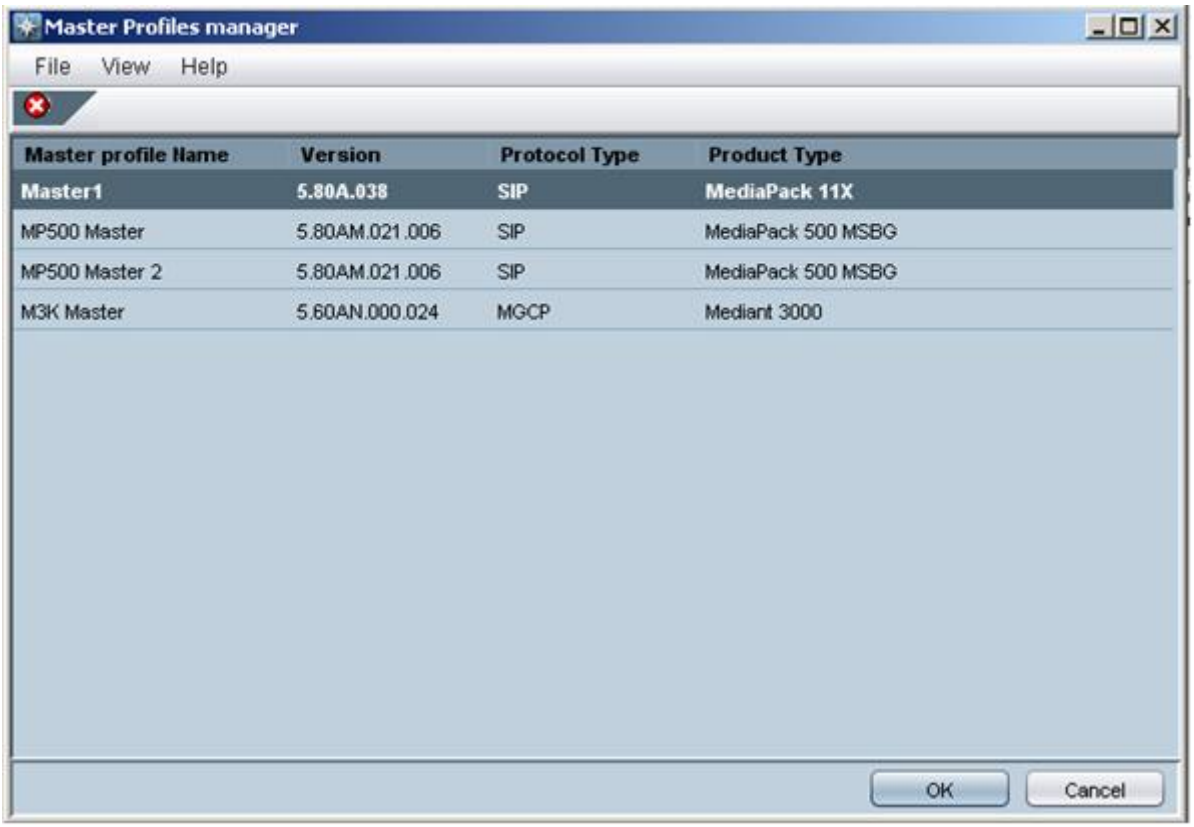
18.7.5 Removing a Master Profile

This section describes how to remove a Master Profile.

➢ **To remove a master profile from the profiles pool:**

1. In the Tools menu, choose the option **MP Master Profiles Manager**; the MP Master Profiles Manager screen opens (shown in the figure below).

Figure 18-13: Master Profiles Manager - Media Pack



2. Select the master profile/s that you require to be removed from the master profiles pool and click the button to remove the master profile/s you selected.
3. If a master profile is used by one or more MediaPacks it cannot be removed.

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

This section describes the TP-6310 and TP-8410 Master Profile (Mediant 5000 media gateway, Mediant 8000 media gateway).

18.8.1 Ascertaining a TP-6310 and TP-8410 Board Master Profile

This section describes how to ascertain a TP-6310 and TP-8410 Board Master Profile.

A TP-6310 STM1 master profile is composed of the following:

- The board-level configuration
- The trunks configuration
- The PSTN Fiber Group configuration
- The MTP2 profiles configuration

A TP-6310 DS3 master profile is composed of the following:

- The board-level configuration
- The trunks configuration
- The DS3 interfaces configuration
- The MTP2 profiles configuration

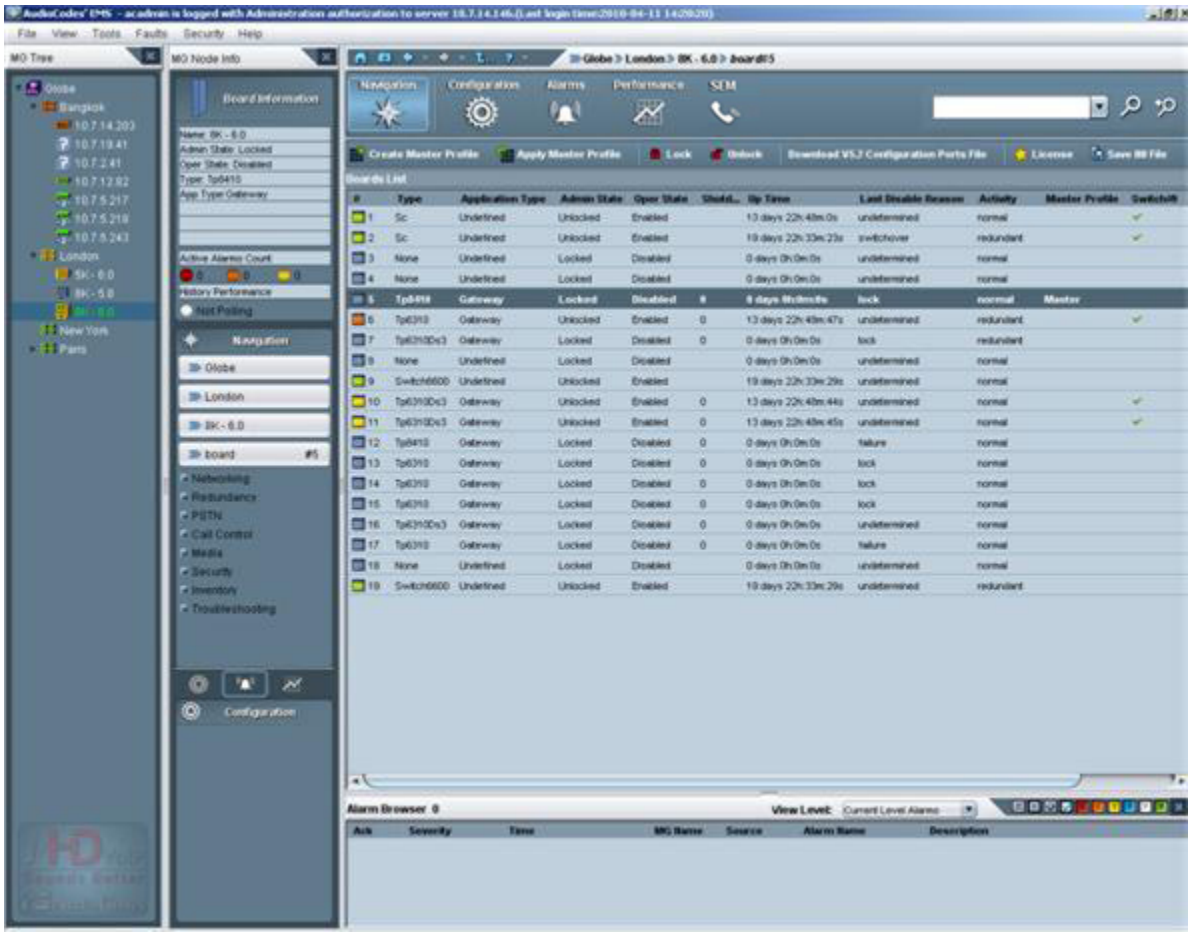
A TP-8410 DS1 master profile is composed of the following:

- The board-level configuration
- The trunks configuration
- The MTP2 profiles configuration

For SIP Control Protocol, the entire profiled configuration is transferred as part of the Master Profile.

To ascertain whether a master profile is attached to a TP-6310 or TP-8410 board and (in the event that a master profile is attached) the name of the master profile (refer to the figure below), click the icon 'Table View' in the gateway Status screen and check the 'Profile' column.

Figure 18-14: Profile Column in the Boards List Screen



18.8.2 Creating a Master Profile

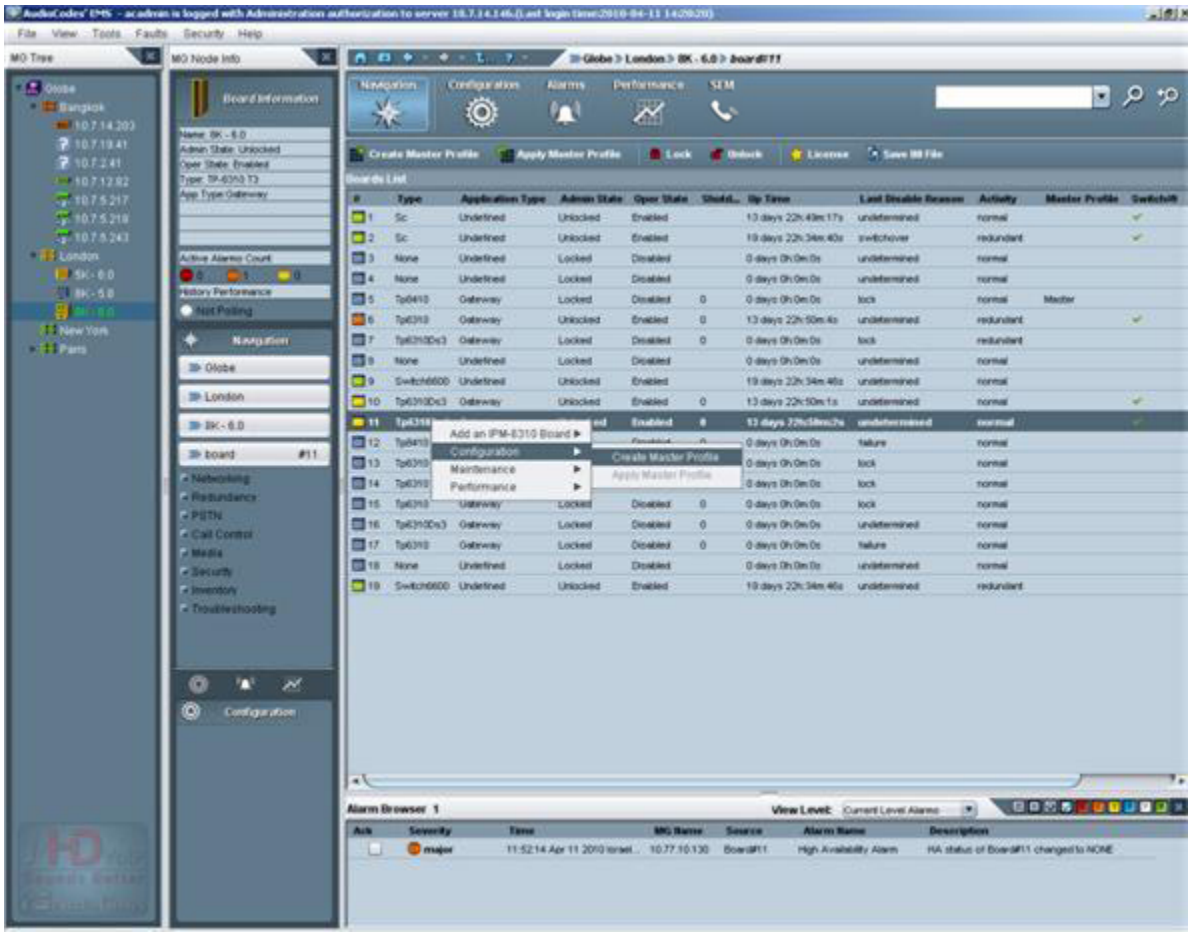
This section describes how to create a Master Profile.

Note: A master profile cannot be modified after it is created. Operators must instead modify the configuration of a TP-6310 / TP-8410 and then save the new configuration as a new master profile (to be applied to the boards).
To apply a master profile to the TP-6310 / TP-8410 board, all its trunks must be profiled. If all trunks have the same configuration, operators can use the button 'Apply to All' in the 'Trunk Properties Profile Manager' pane.

If an entity profile is created and loaded to the board prior to the creation of the master profile, the loaded profile is saved as part of master profile.

In the event that no entity profile/s was/were created and loaded prior to the creation of a master profile, the master profile automatically creates entity profiles for all entities.

Figure 18-15: Creating a Master Profile - TP-6310



➢ To create a master profile:

1. In the MG Status pane, select a TP board.
2. Do one of the following:
   - In the Actions bar, click **Create Master Profile**.
   - Right-click the selected board and from the pop-up menu, choose option **Configuration > Create Master Profile**.

   The New Master Profile prompt appears:

Figure 18-16: New Master Profile Prompt

3. Enter a name for the master profile in the field 'Save Master Profile' and click **OK**.

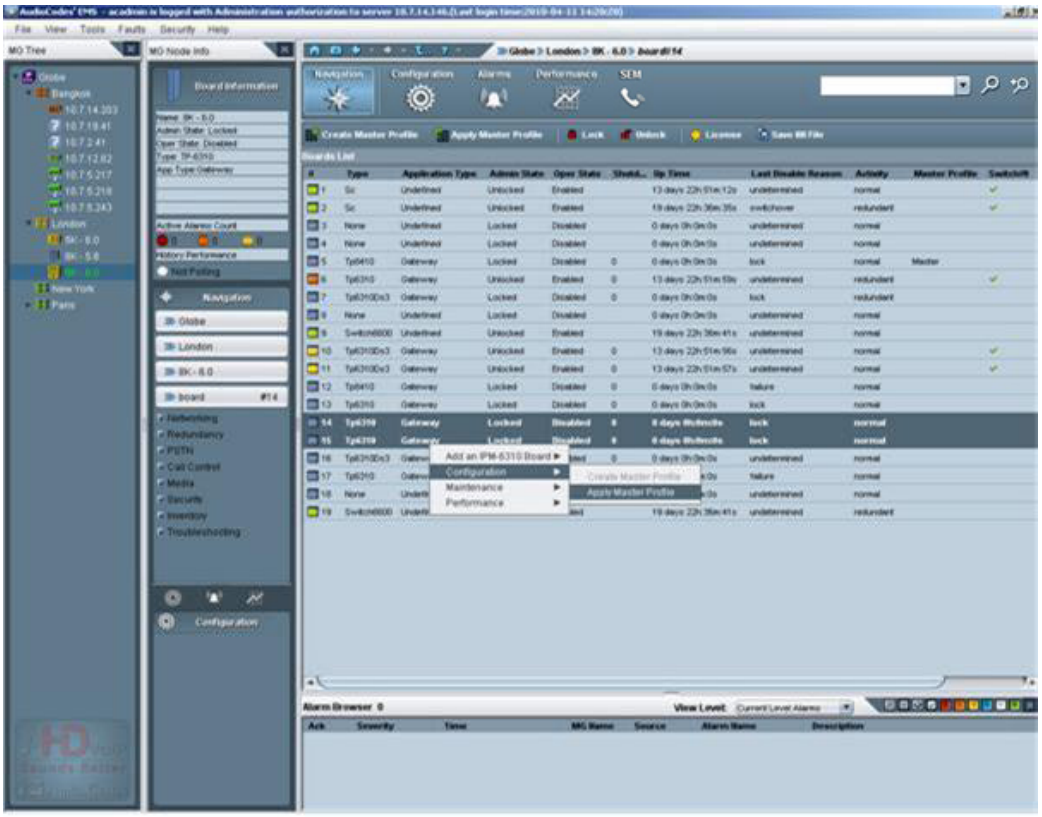
18.8.3 Attaching a Master Profile to TP Boards

This section describes how to attach a master profile to TP boards.

➢ To attach a master profile to TP board/s:

1. In the Boards List, select the TP-8410 / TP-6310 board (or select multiple boards). Alternatively, in the media gateway Status pane, select the TP-8410 / TP-6310 board/s.

Figure 18-17: Selecting TP-6310 Boards



2. Do one of the following:
   - In the Navigation pane, select boards; the boards list is displayed. Select the TP-8410 / TP-6310 board (or select multiple boards).
   - In the media gateway Status pane, select the TP-8410 / TP-6310 board/s.
3. Do one of the following:
   - In the Actions bar, click **Apply Master Profile**.
   - Right-click the selected board (or on multiple selected boards) and from the popup menu, choose option **Configuration > Apply Master Profile**; the 'Select Master Profile' prompt appears on the screen.
4. Select the Master Profile you require and click **OK**; the master profile you selected is attached to all selected boards.

18.8.4 Detaching a Master Profile from TP-8410 and TP-6310 Boards

A profile is detached from the TP-8410/TP-6310 board under the following circumstances:

- You change the configuration of one of the profiled parameters. After clicking **Apply**, the master profile is detached from the TP-8410/TP-6310 board.
- You apply a master profile to an TP-8410/TP-6310 board that is already attached to a master profile and the two master profiles are different. When clicking **Apply**, the TP-8410/TP-6310 is detached from the previously applied master profile and the new profile is applied.

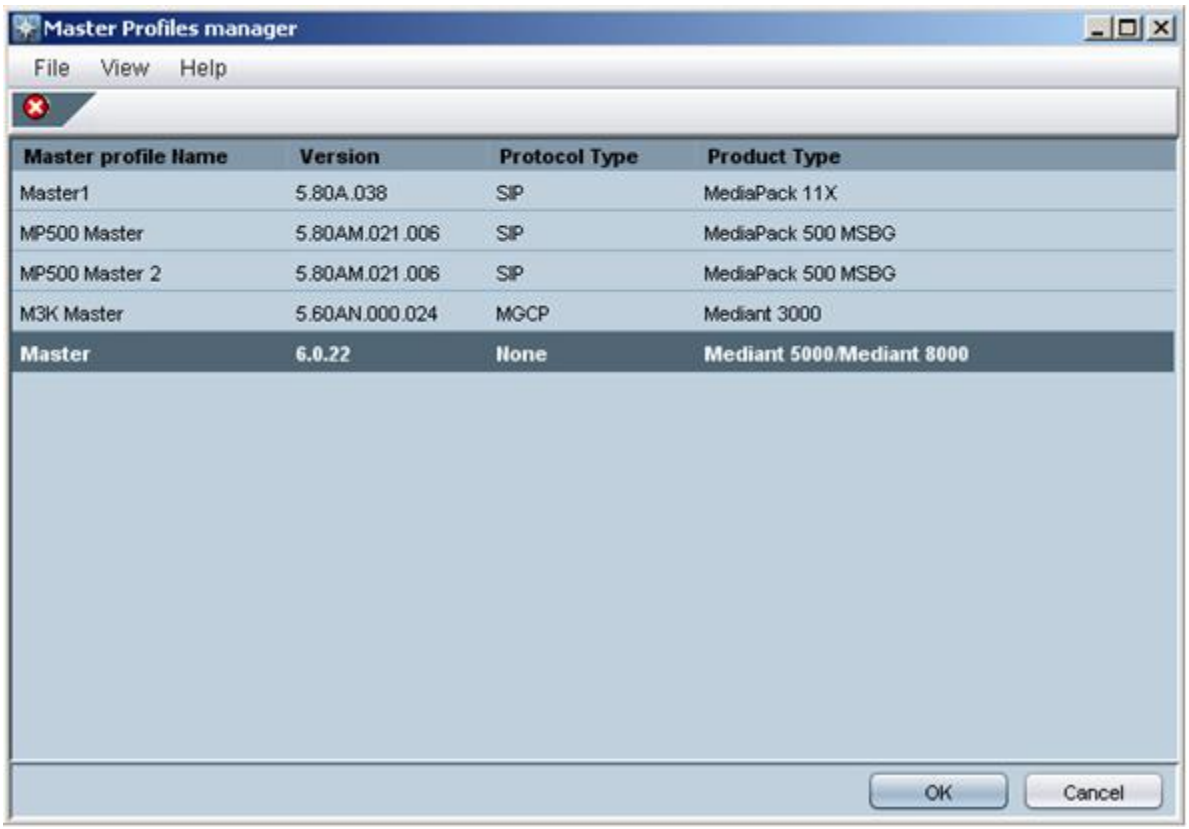
18.8.5 Master Profiles Manager

This section describes the Master Profiles Manager.

➢ To remove a master profile from the profiles pool:

1. In the Tools menu, choose the option **Master Profiles Manager**; the Master Profiles Manager screen opens (shown in the figure below).

Figure 18-18: Master Profiles Manager



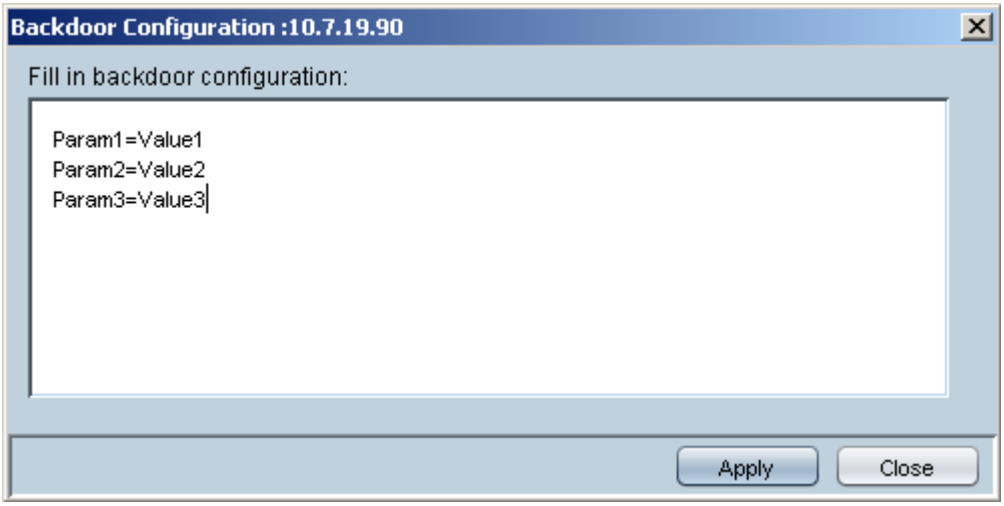
2. Select the master profile/s that you require to be removed from the master profiles pool and click the button to remove the master profile/s you selected.
3. If a master profile is used by one or more devices, it cannot be removed.

18.9 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 18-19: Backdoor Configuration

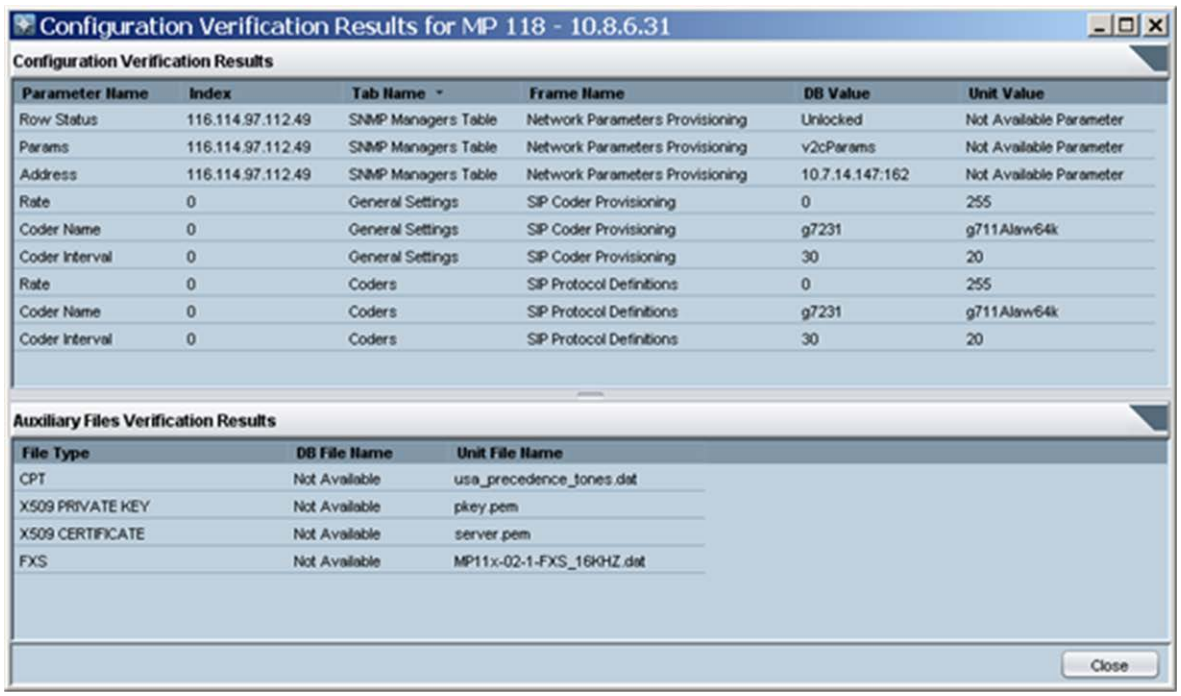


Note: Backdoor parameters are downloaded directly to the gateway and are not saved in the EMS Database, and therefore they are not downloaded as part of the Configuration Download and are not tested as part of the Upload and Verification commands.

18.10 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 18-20: Configuration Verification Results



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.

18.11 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 18-21: 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.

Note: 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 18-22: Advanced Search Configuration Parameter Dialog

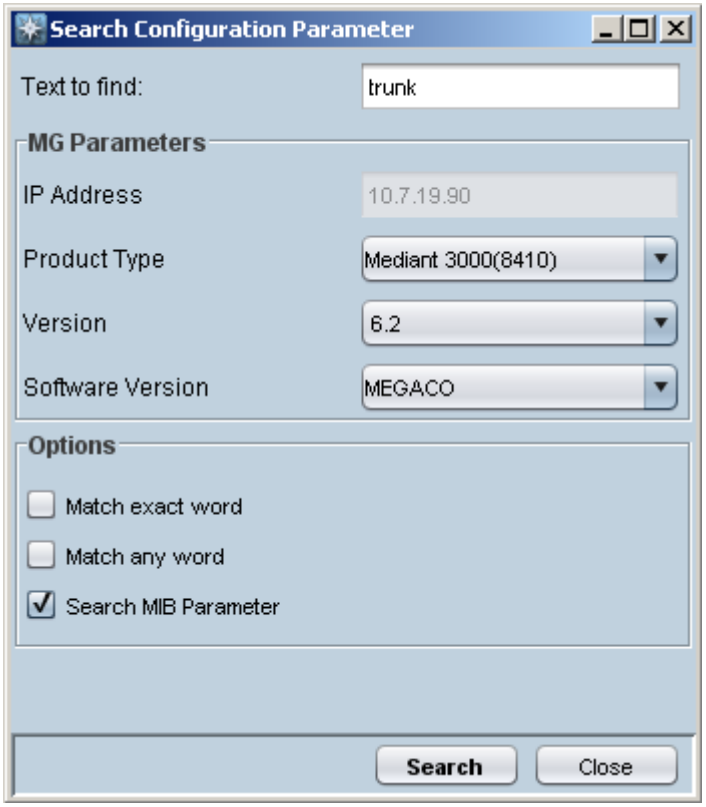
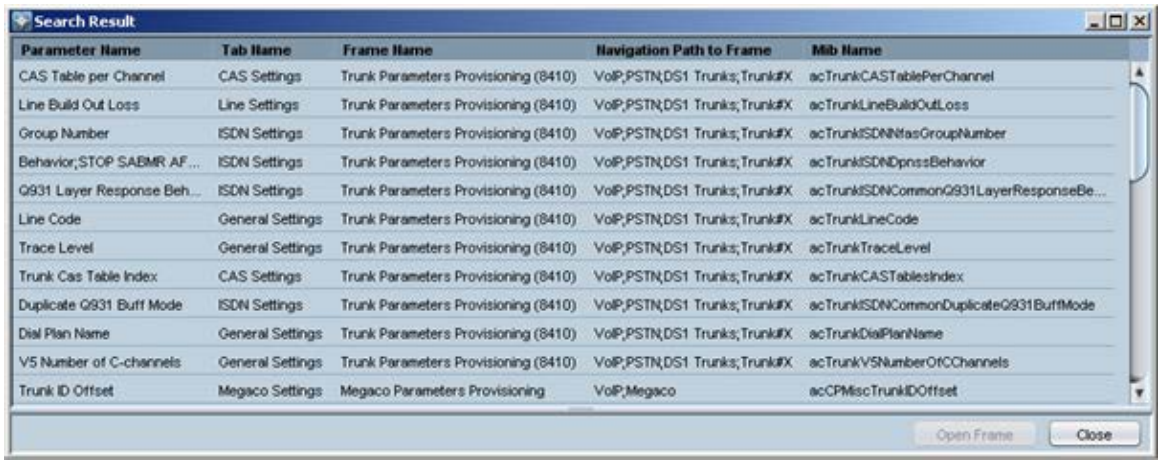


Figure 18-23: Advanced Search Configuration Results Dialog

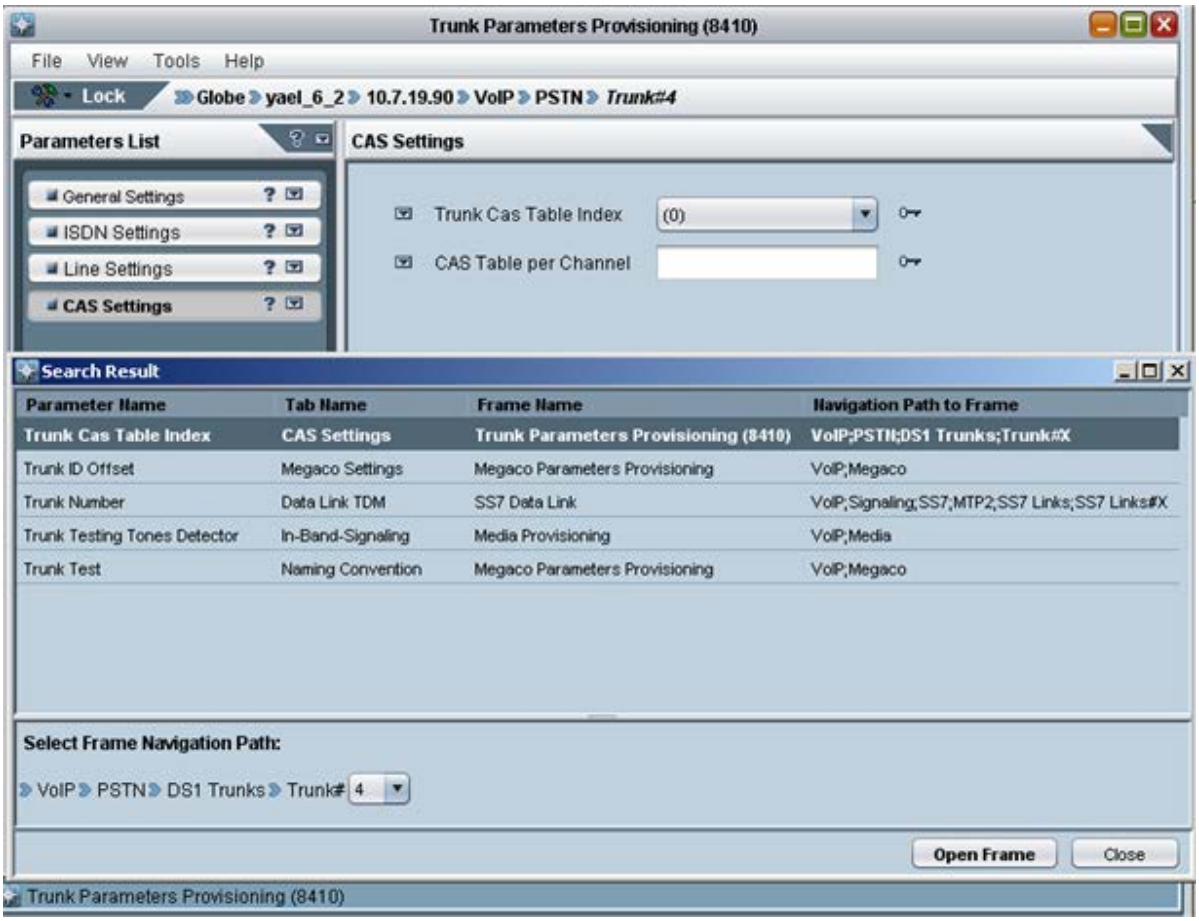


➢ Navigating to the searched entity:

- 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 18-24: Advanced Search Results screen and related Provisioning screen



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.

19 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.

19.1 Software Manager

See Section 'Software Manager' on page 61.

19.2 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.

Note:

1. 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).
2. 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).
3. 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.

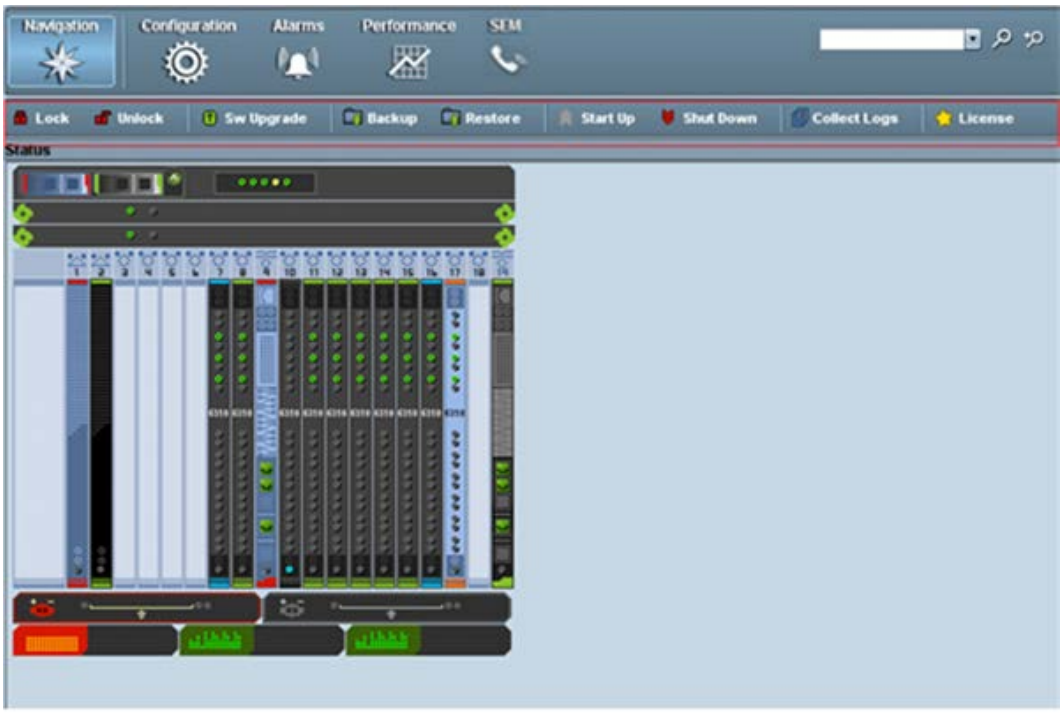
19.3 Mediant 5000, Mediant 8000 Maintenance Actions

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 site 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 19-1: 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.

19.3.1 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.

Note : 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.

19.3.2 License Key Update

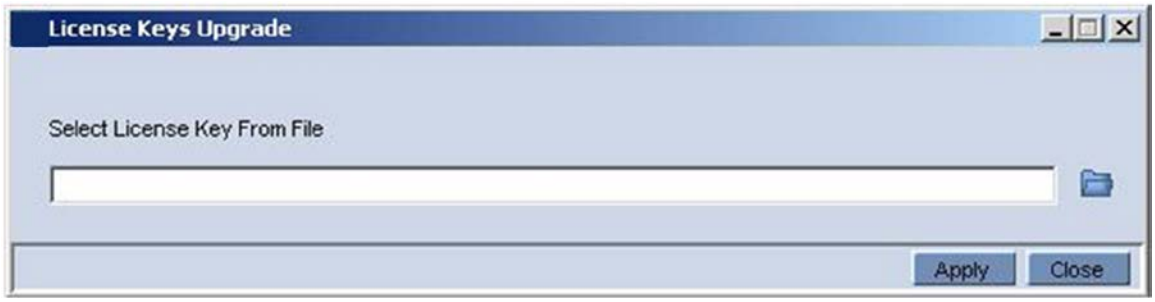
You can update the License Key for multiple TP boards managed in the same Gateway using a single file which includes all the corresponding Keys.

➢ **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 19-2: 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.

19.3.3 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

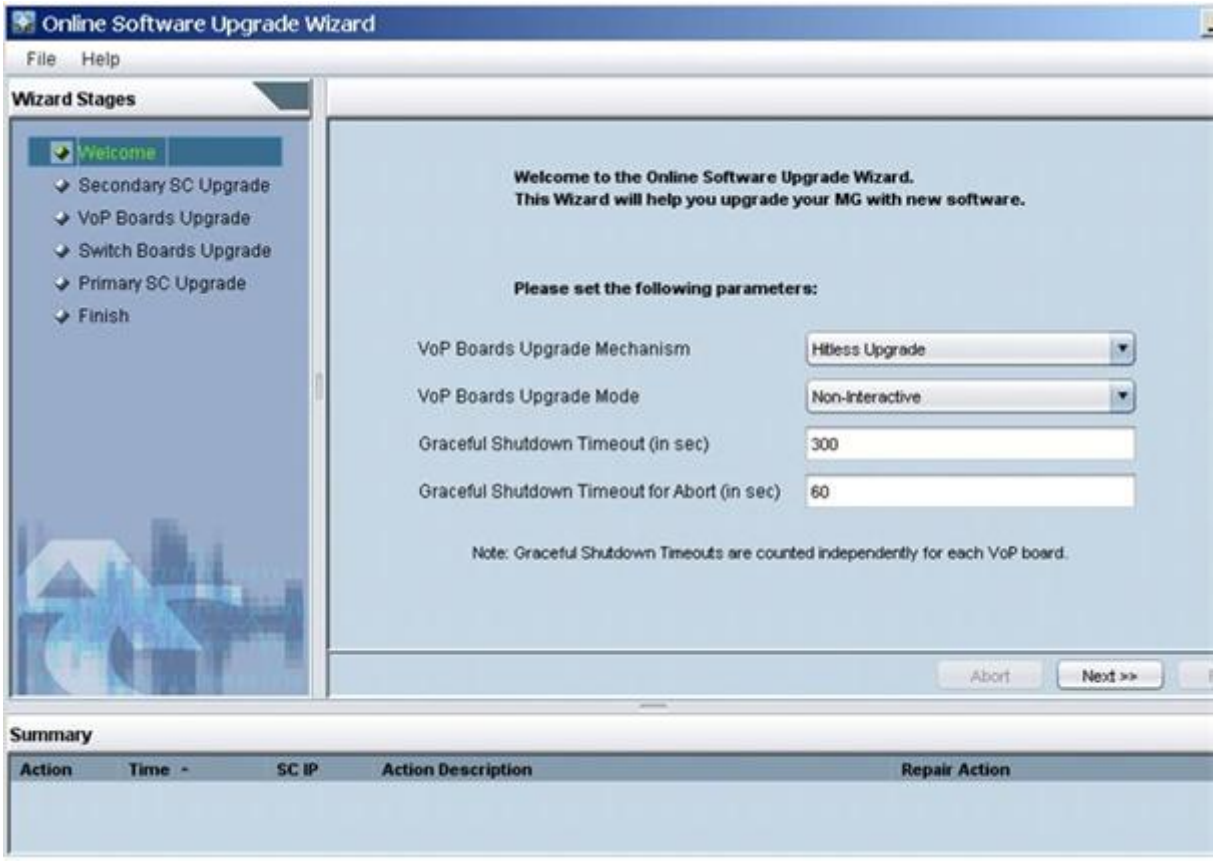
- **Pause after each gateway board** - allows a pause after each board is upgraded. The user controls the start time of each board upgrade. This option further minimizes the number of calls impacted by the upgrade.

- **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.

Note :

1. 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.
2. 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.
3. 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 19-3: Welcome to the Online Software Upgrade Wizard

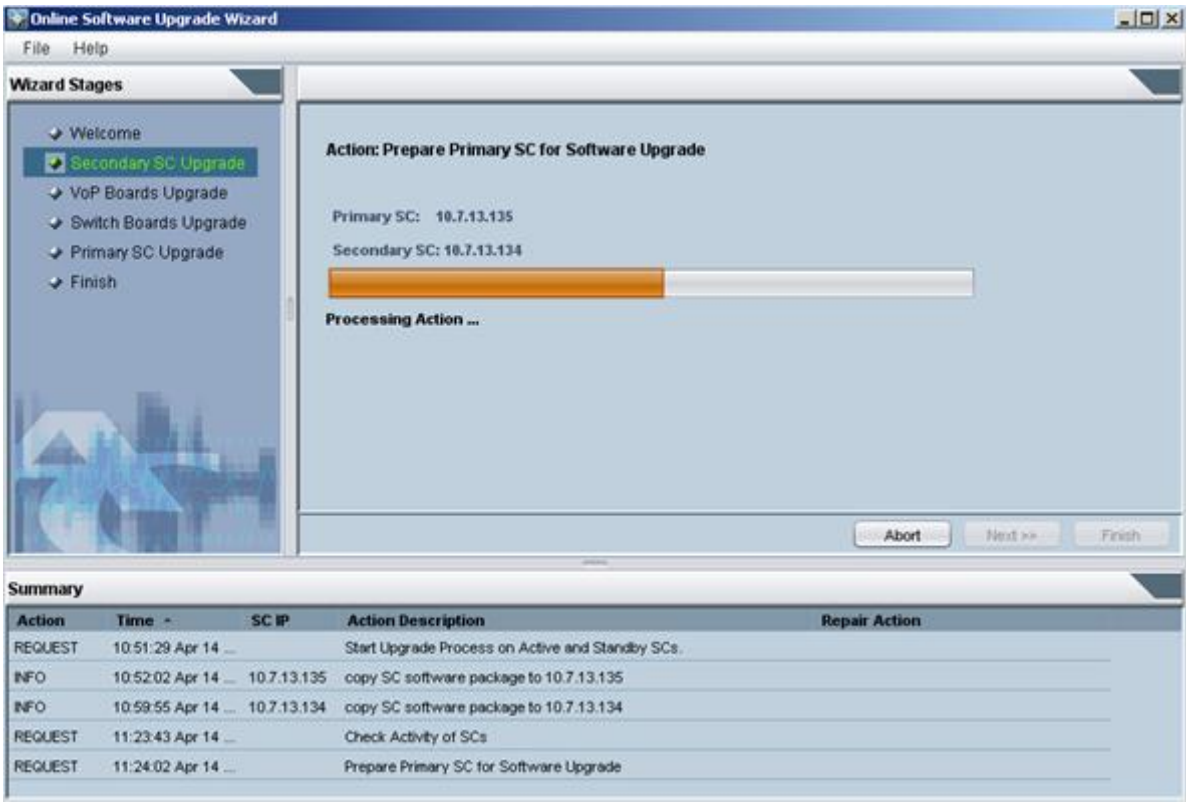


2. Secondary SC Update

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 19-4: Software Upgrade in Process, Managed by the System Controller



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**

19.3.3.1 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 service-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.

19.3.3.2 Troubleshooting

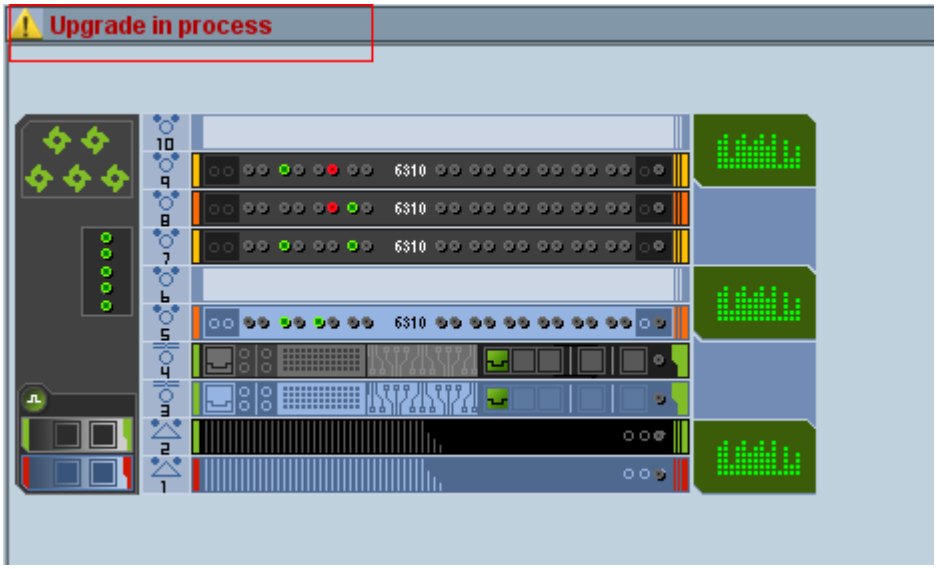
If you experience an unexpected network or software problem during online software upgrade (e.g., if the PC, on which the EMS client runs, crashes or the network connection to the media gateway is lost) you have several options to continue the upgrade session from the same stage. If your network fails, 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.

Note: 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 19-5: Upgrade Indicator



19.3.4 Backing Up and Restoring the Media Gateway

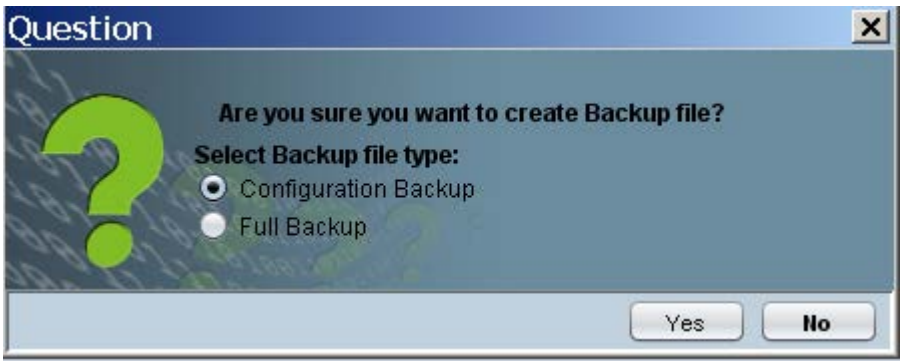
This section describes how to backup and restore the media gateway.

➢ 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 19-6: Create Backup File Prompt



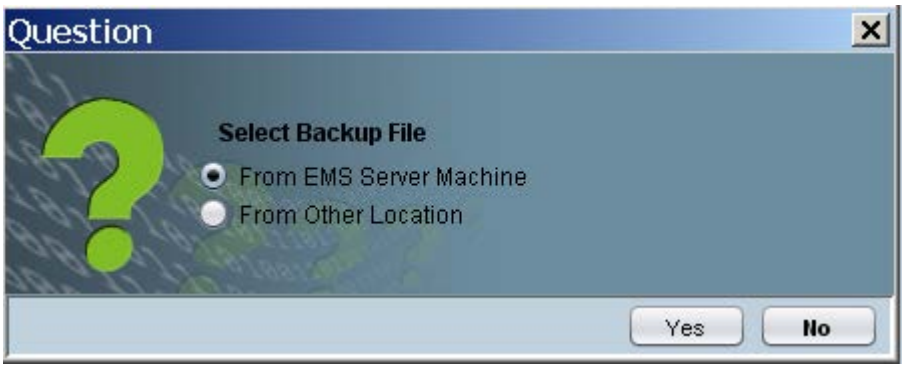
➢ **To restore the gateway:**

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 19-7: Restore Media Gateway Note

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 19-8: Select Backup File Prompt



Upon selecting the backup file, EMS will transfer it to both SCs and run the restore procedure.

19.4 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.

19.5 Collecting Log Files

This section describes how to collect log files.

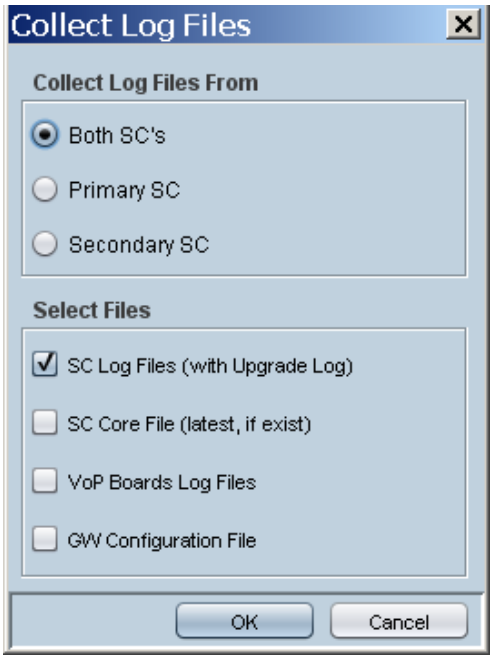
➢ To collect MG logs:

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 collection 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 19-9: Collecting Log Files



19.6 Mediant 5000, Mediant 8000 Configuration Backup Files Collection

EMS can collect backup files (.bk files) that were created and locally stored on the media gateway and store them on the 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

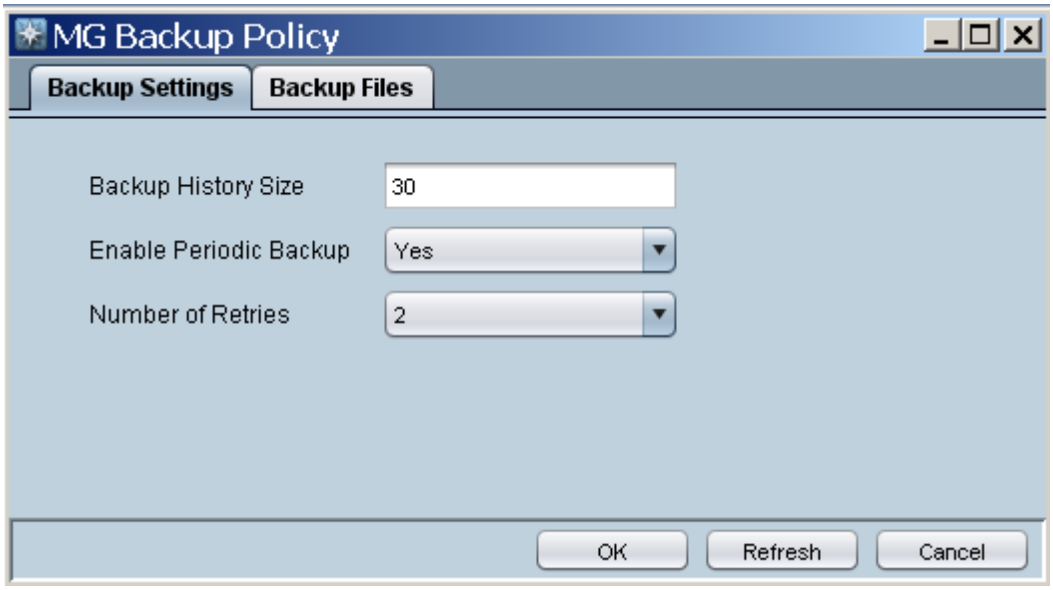
Media gateway backup files are located in the EMS Server machine under ACEMS/NBIF/mgBackup folder. File can be accessed and transferred using SSH, and SFTP.

➢ **To provision EMS to collect the Mediant 5000 / 8000 backup files: :**

1. Open **Tools > MG Backup Policy**; the MG Backup Policy Dialog is displayed.
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. Select **Yes** to Enable Periodic Backup collection.
4. Define the number of retries that must be made on each connection to the media gateway. Default-2.

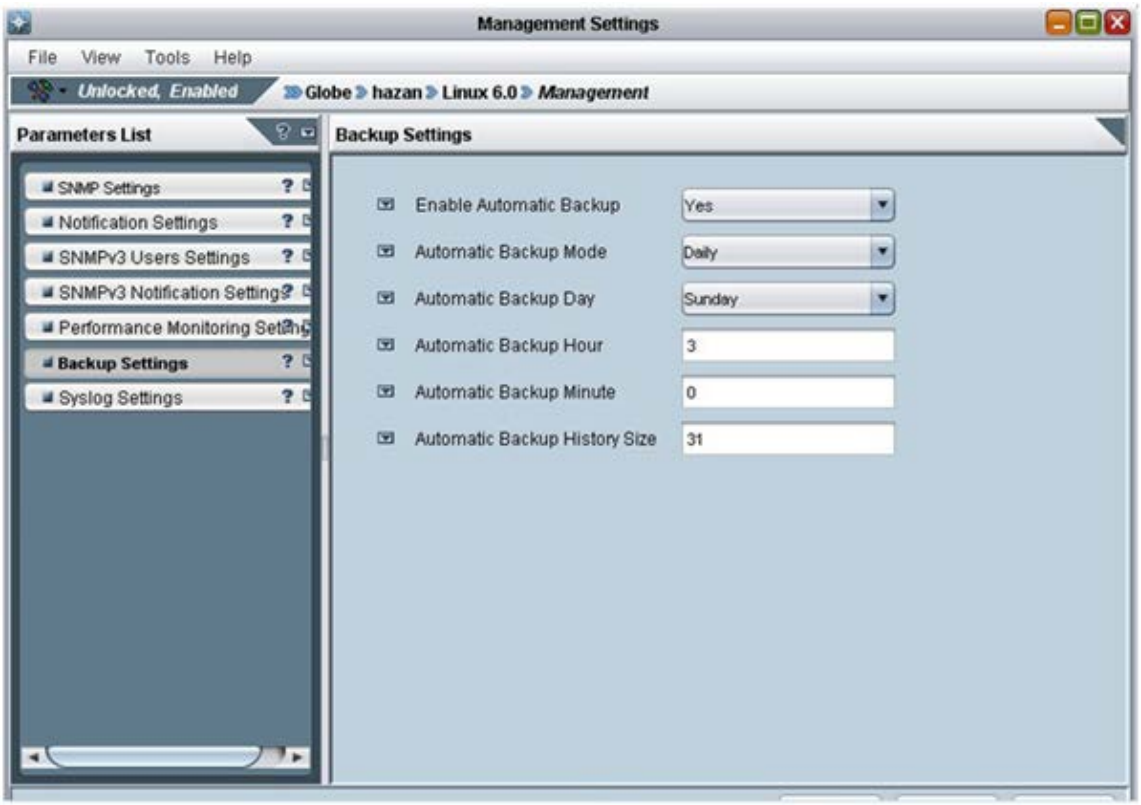
Note: EMS periodically checks each of the media gateways and when a new backup file is created on the gateway, transfers it to the EMS server machine. You can define different backup file creation rules for each of the Gateways.

Figure 19-10: Backup Settings



5. 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 / 8000 IOM Guide*.

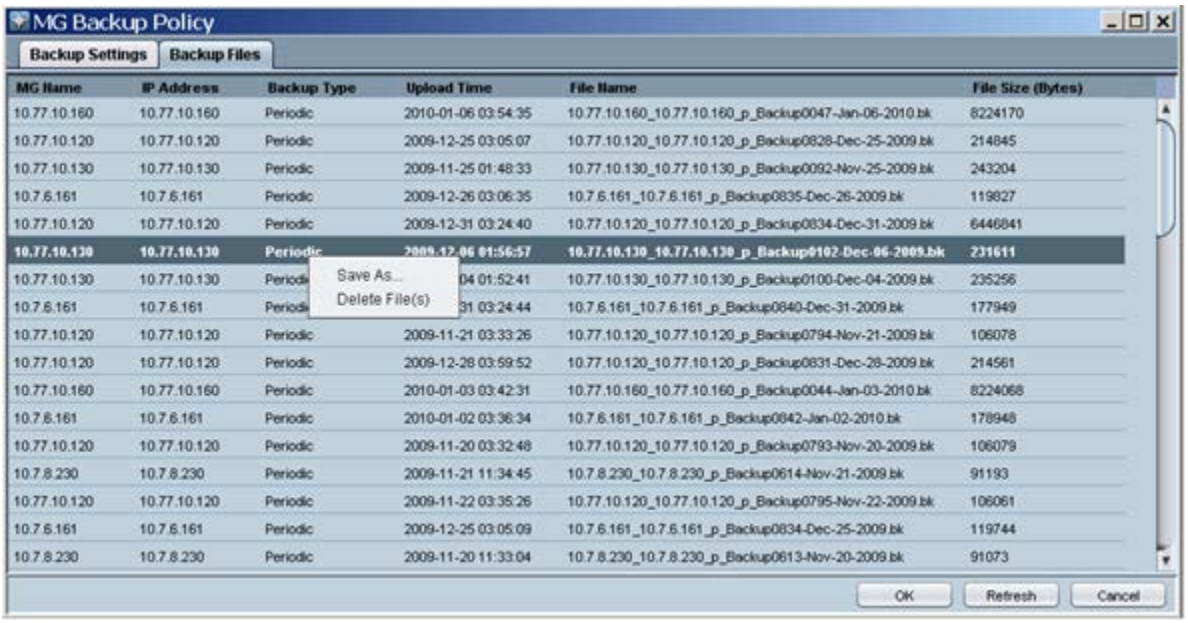
Figure 19-11: Automatic Backup Setup



➢ **To view currently stored backup files, do the following:**

1. In the Tools menu, choose **MG Backup Policy**.
2. Select the **Backup File Specification** tab.
3. Right-click an entry to save the backup file or remove it from the EMS server storage.

Figure 19-12: Backup File Specifications



Part IV

Fault and Performance Management

This section describes fault and performance management.

20 Introduction

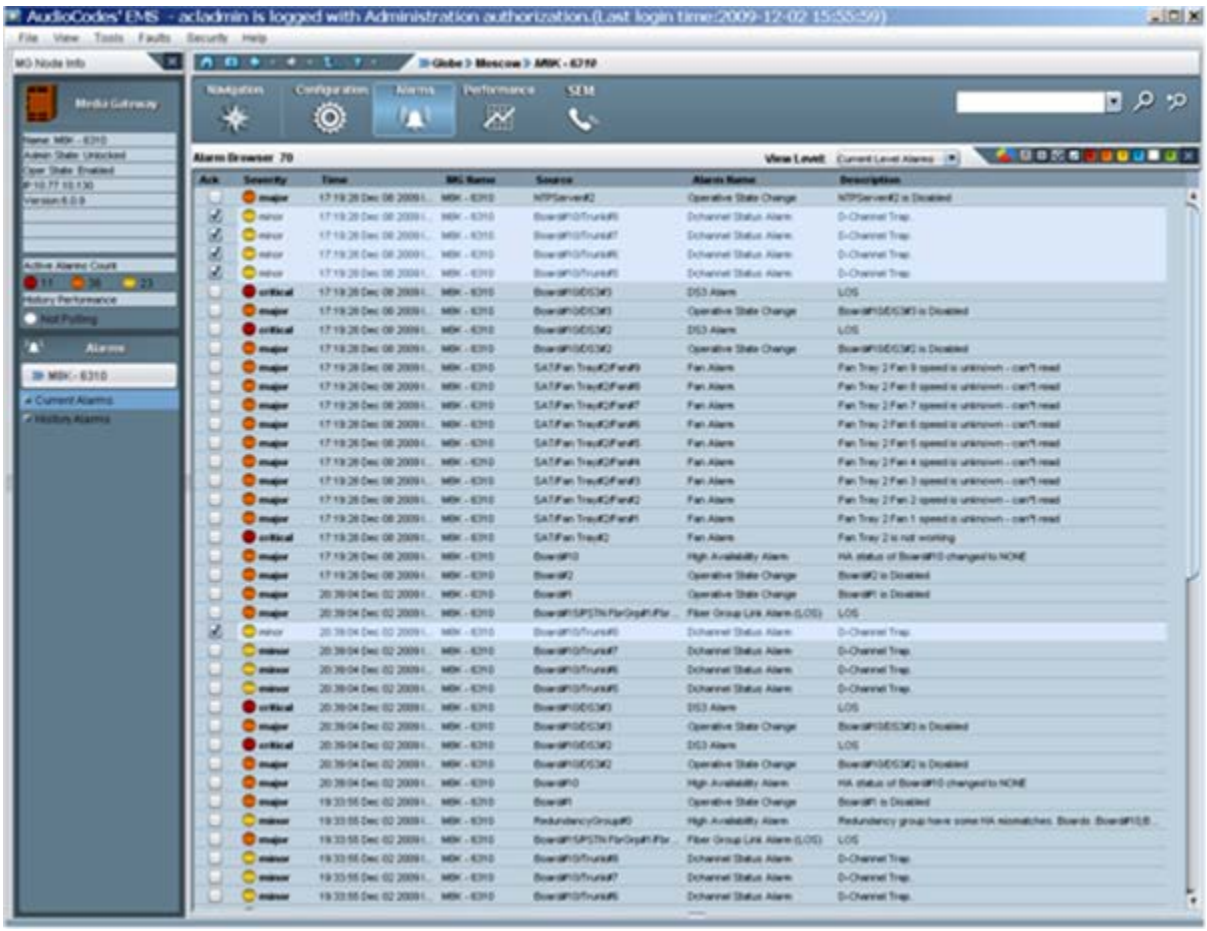
After service is provisioned for a subscriber under a given QoS level, the service provider must ensure that the purchased level of service is delivered. In the domain of the EMS, this process involves high-level fault and performance management of the managed entities. This section describes the fault 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 each 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 20-1: Alarm Browser in Main Screen



21 Alarm Browser

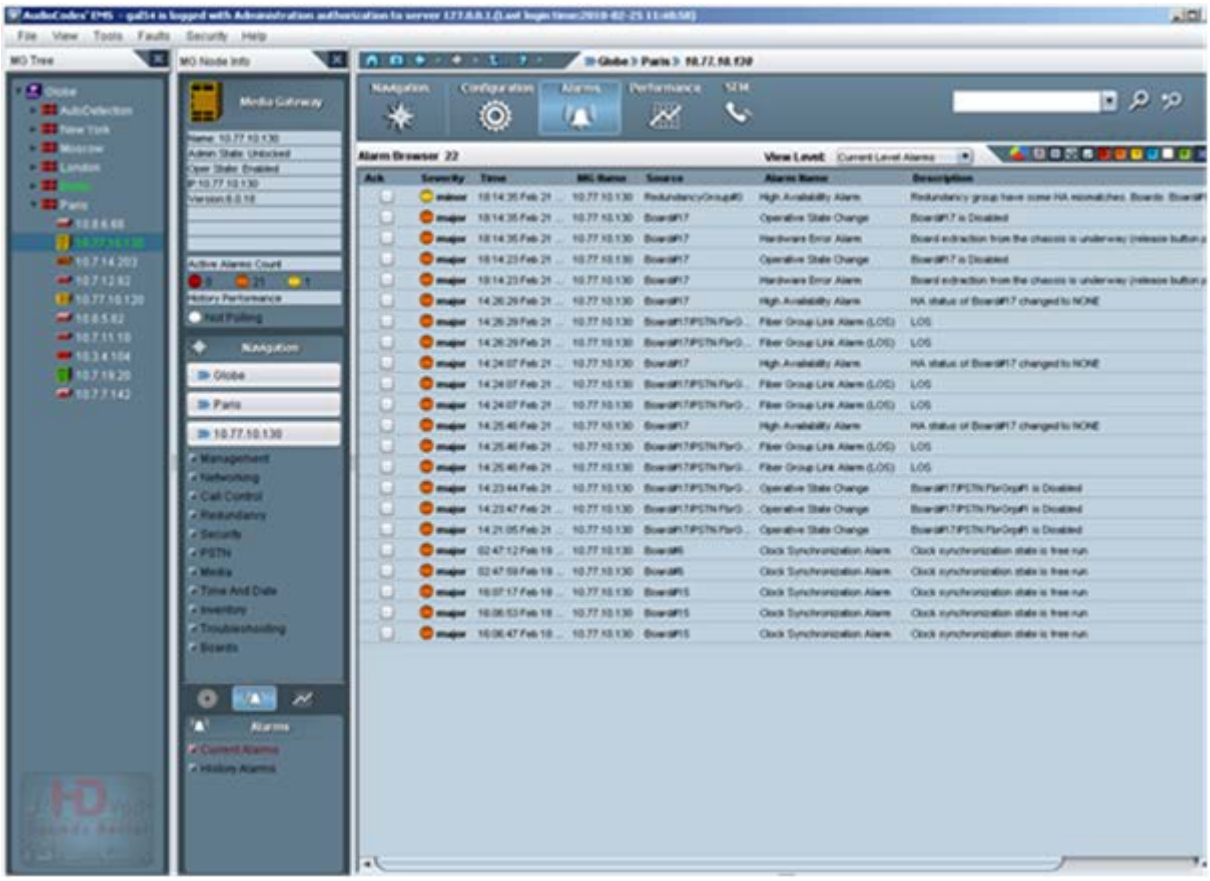
The EMS's fault management functionality manages and displays all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system.

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 21-1: Alarms Browser Mediant 8000



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)

Note: 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**.

21.1 Filtering Alarms

The Alarm Browser lists all the currently active alarms in the EMS for a context 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 21-1: 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.
	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.

	Close Alarm Browser

Note: 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.

21.2 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.

21.3 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).

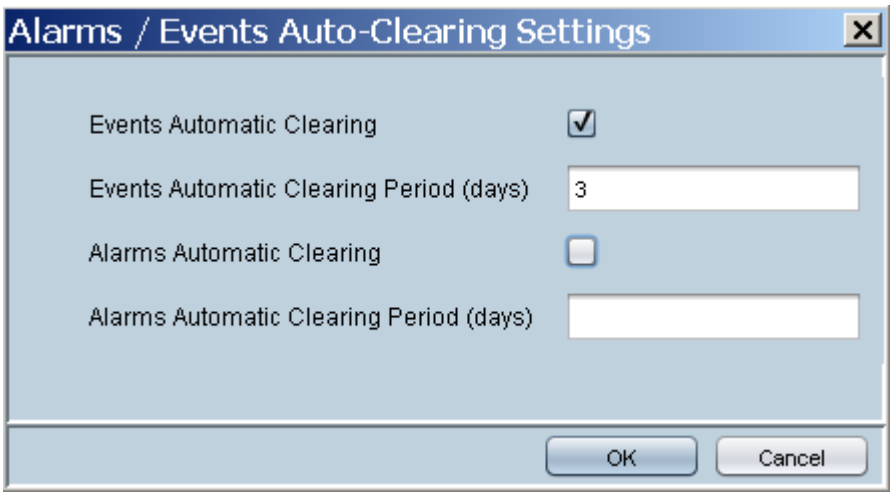
Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) when a Clear alarm is generated by the same entity (source) and same media gateway that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature 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 21-2: Alarm and Event Auto-Clearing Settings



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'.

21.4 Changing the Alarms Browser Views

This section describes how to change the Alarms Browser Views.

21.4.1 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:

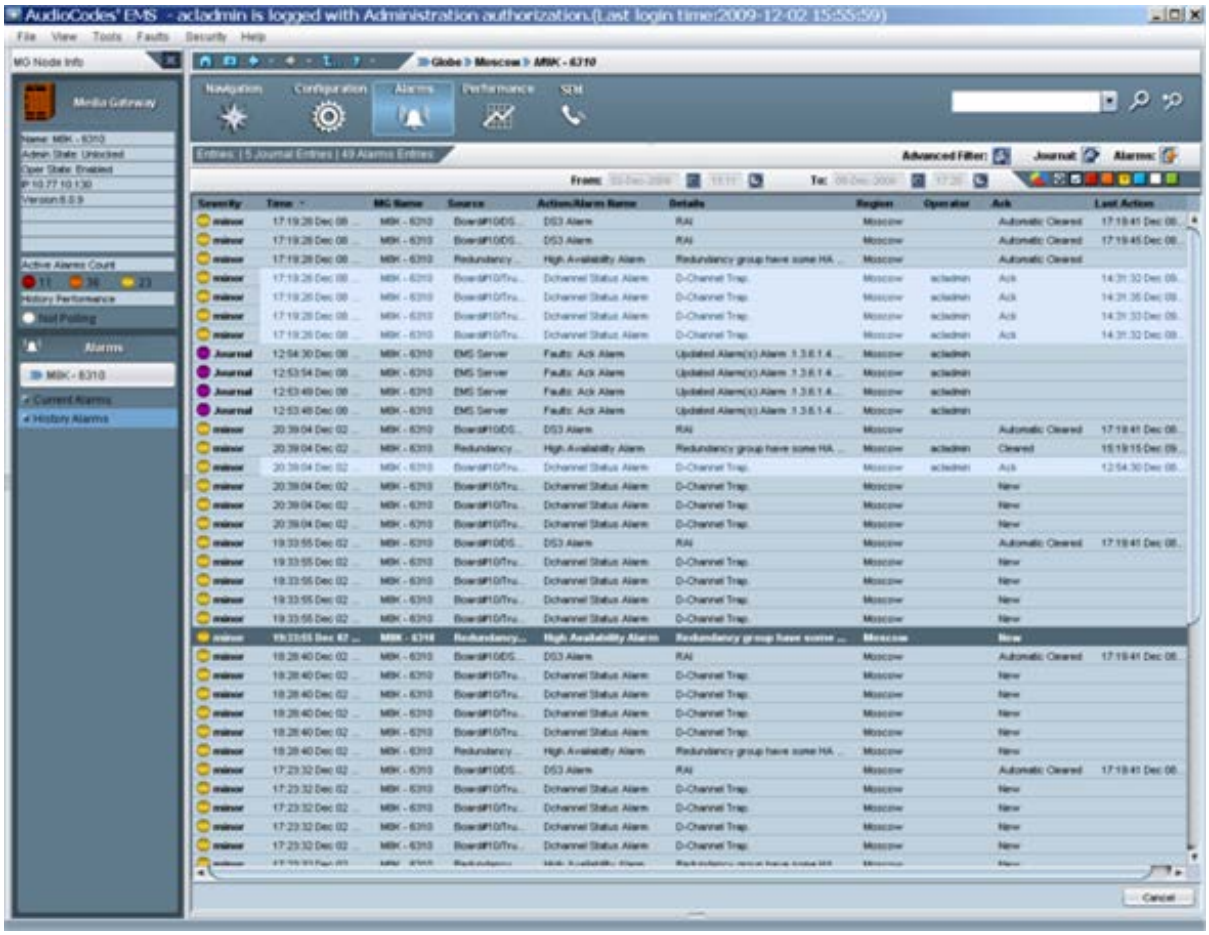
- **Current Level Alarms (default)** - users view alarms filtered according to the context they're viewing in the status pane
- **Node Level Alarms** – users always view all alarms received from the node they're viewing, regardless of the lower level context (board, trunk) they've accessed.
- **Region 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.

21.4.2 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 21-3: Alarm Browser Column View

Figure 21-4: Alarm History



21.5 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 262.

21.6 Open Journal

To review Journal records for the selected context, click **Journal** on the Alarm Browser tool bar. For the specifications and features pertaining to the Journal, see Section 'Viewing Operator Actions in the Actions Journal' on page 441.

21.7 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.

21.8 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.

21.9 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]

21.10 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**.

22 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.

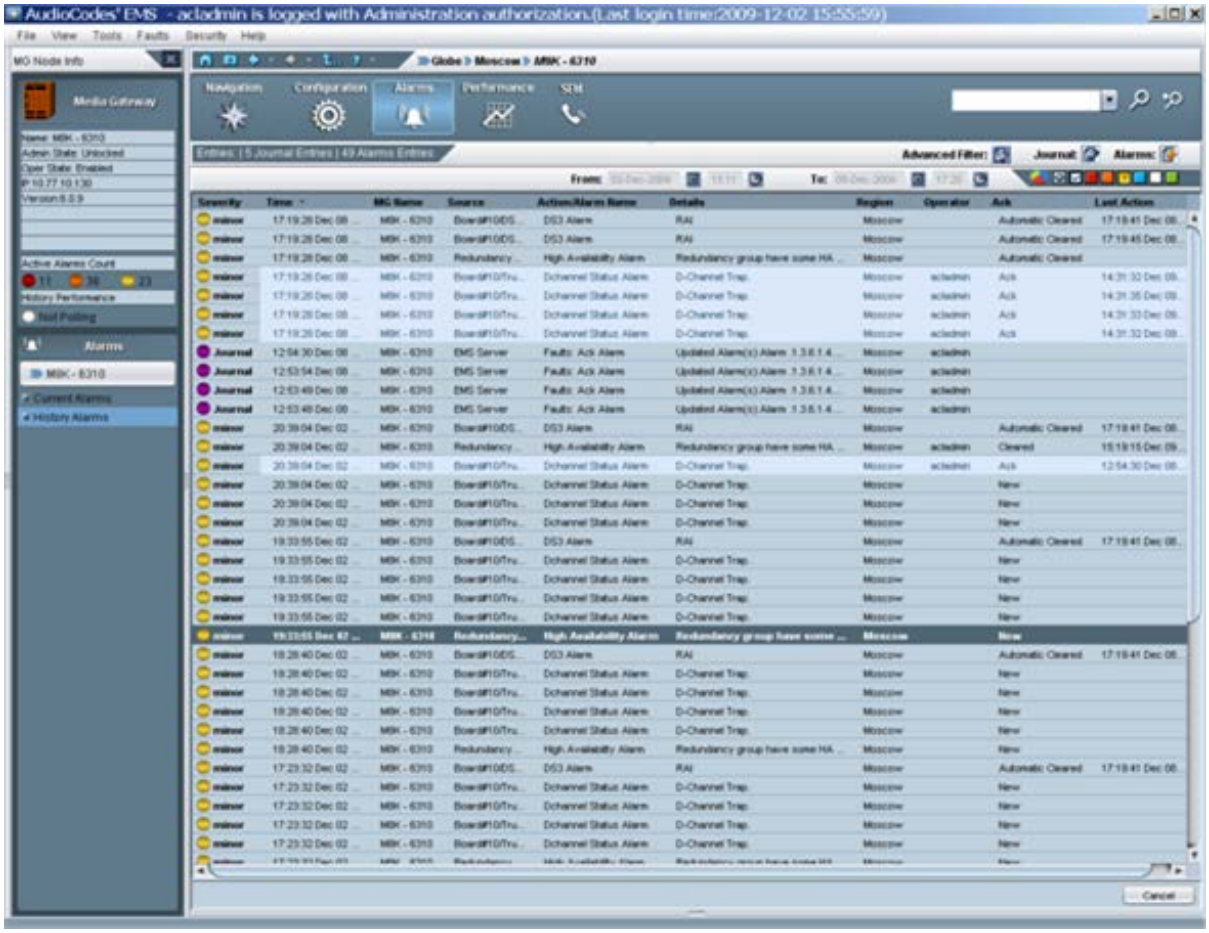
Open the Alarms History screen from the Alarms module by clicking the 'History Alarms' option. The Alarms History screen is context-sensitive like the Alarm Browser; the context is displayed in the title of the screen.

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 the alarm and the name of the operator who performed the last action for the alarm.

Figure 22-1: Alarms History



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**.

23 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.

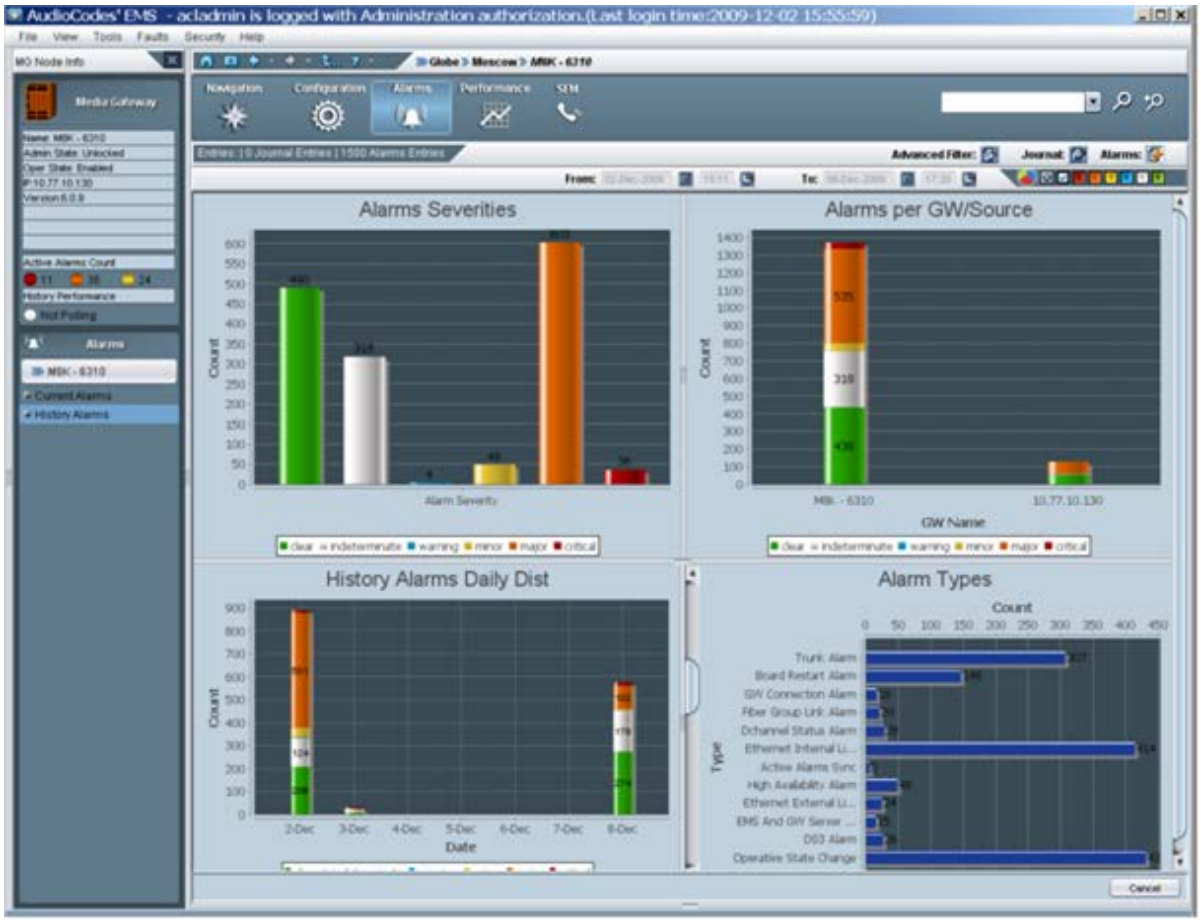
When you move the mouse over each one of the graph items, a tooltip is displayed with detailed information of the graph type and number of alarms in the view. You can view either a list of Current Alarms or a list of History Alarms.

The following screen illustrates the Current Alarms graph for the media gateway:

Figure 23-1: Current Alarms Graph

The following screen illustrates the History Alarms graph for the media gateway:

Figure 23-2: History Alarms Graph



This page is intentionally left blank

24 Using Alarm Filters

This section describes how to use the alarm filters.

24.1 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 24-1: Alarms History Screen: Defining Time Filtration using Calendar

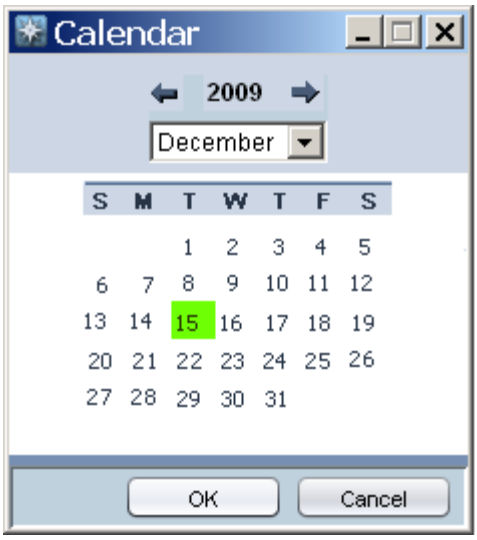
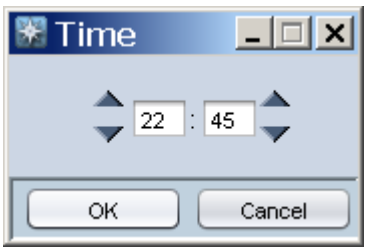


Figure 24-2: Alarms History Screen: Defining Time Filtration using Hour & Minutes



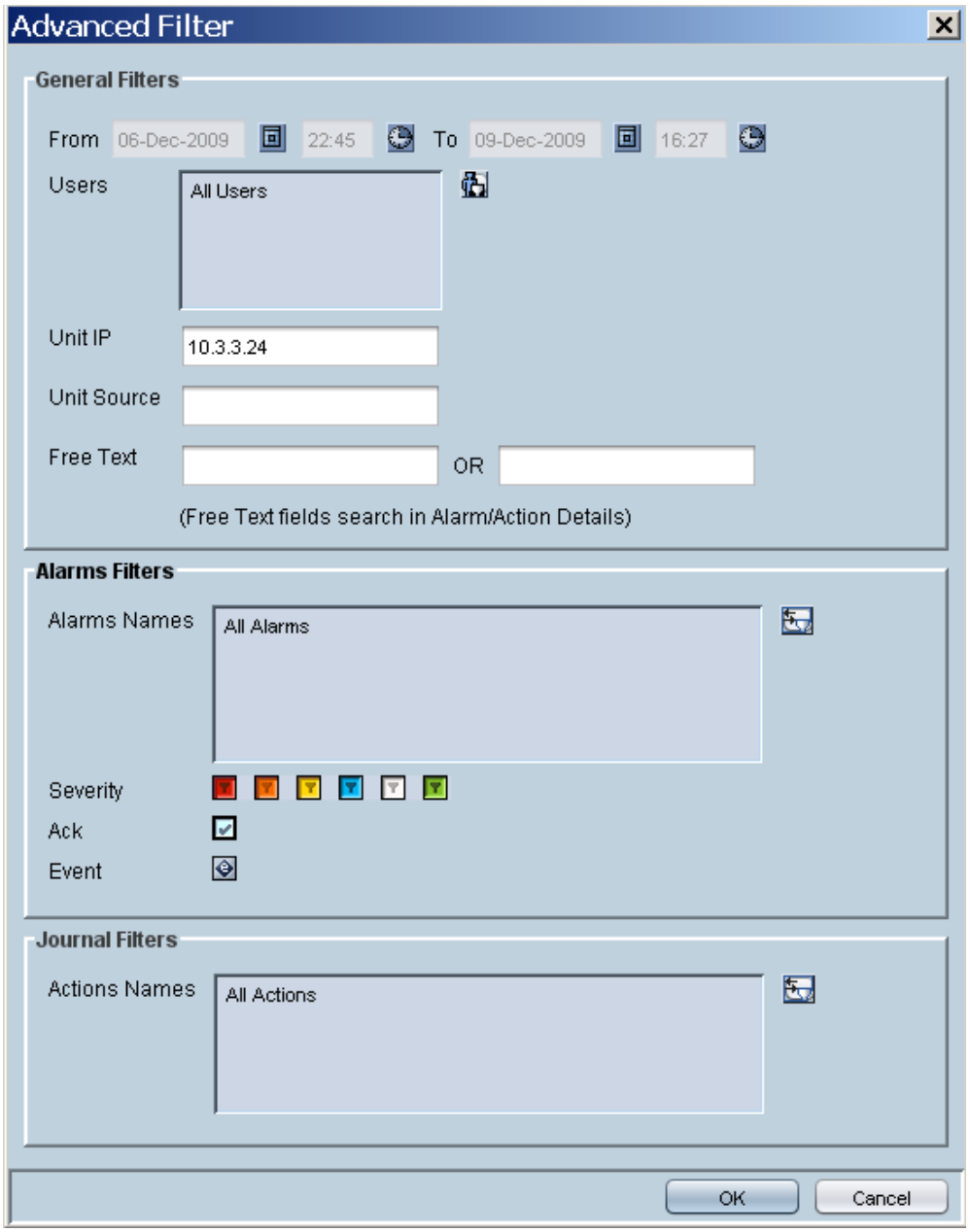
24.2 Using Advanced Filters

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 24-3: Advanced Filter



- **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

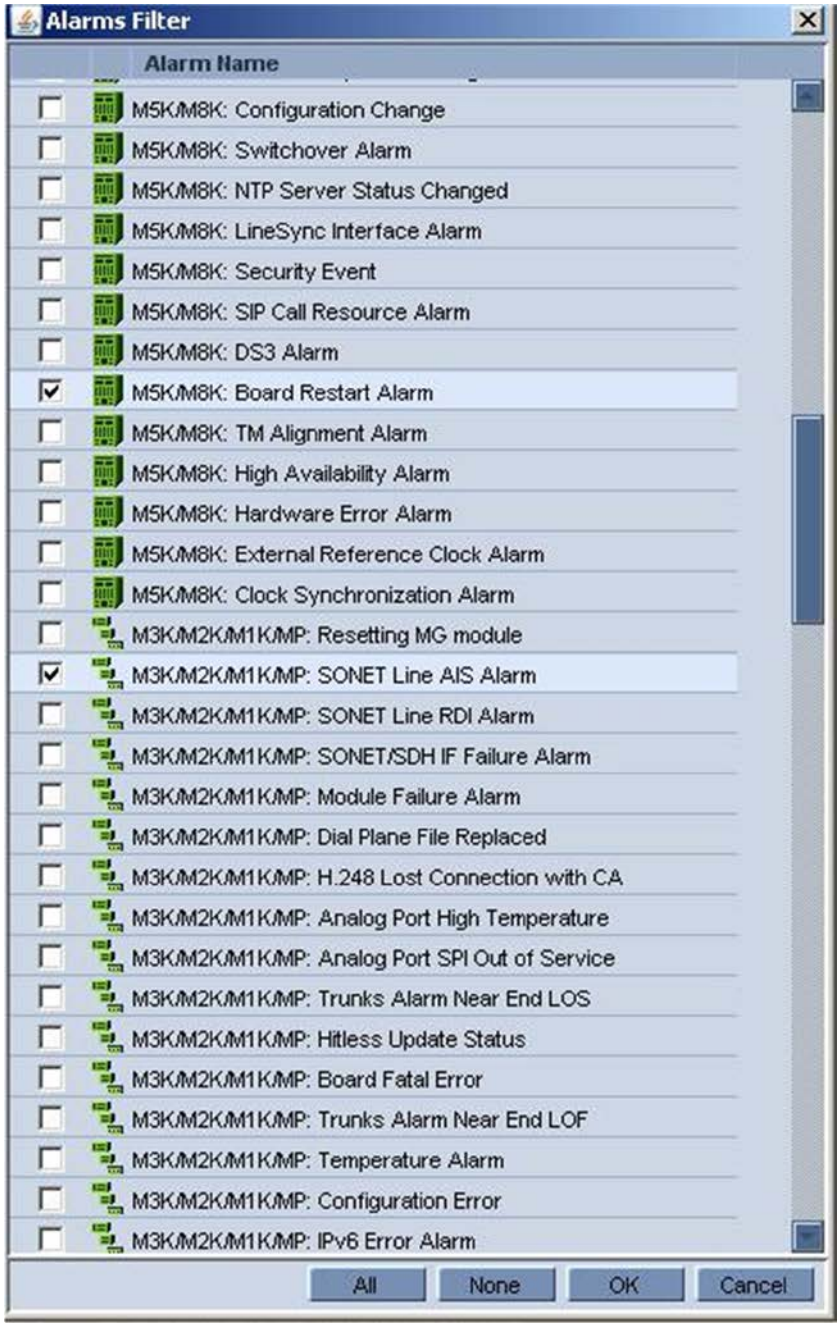
- **Journal Filters**

  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 24-4: Alarms Filter



25 Defining Complex Queries using a Combination of Filters

Using a combination of filtering options, users can easily create complex queries.

25.1 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 specific 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**.

This page is intentionally left blank

26 Viewing, Interpreting an Alarm's Details

This section describes how to view and interpret an Alarm's Details.

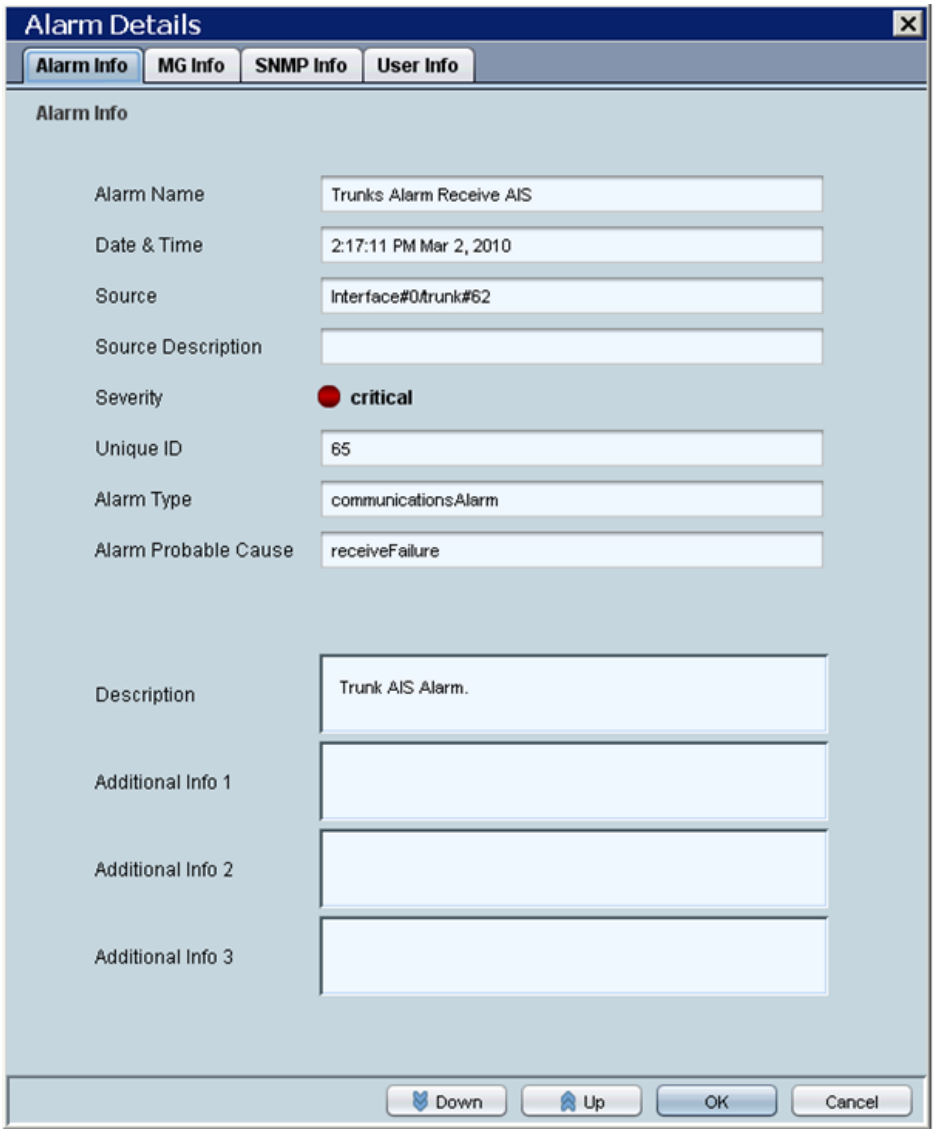
➢ **To view/interpret an alarm's details, do one of the following:**

- 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 26-1: Alarm Details



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).

26.1 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.)

Note: 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

Note: The parameter 'Probable Cause' is based on ITU X.733, X736 standards.

- Description

  Textual description of the alarm, received as part of the alarm information

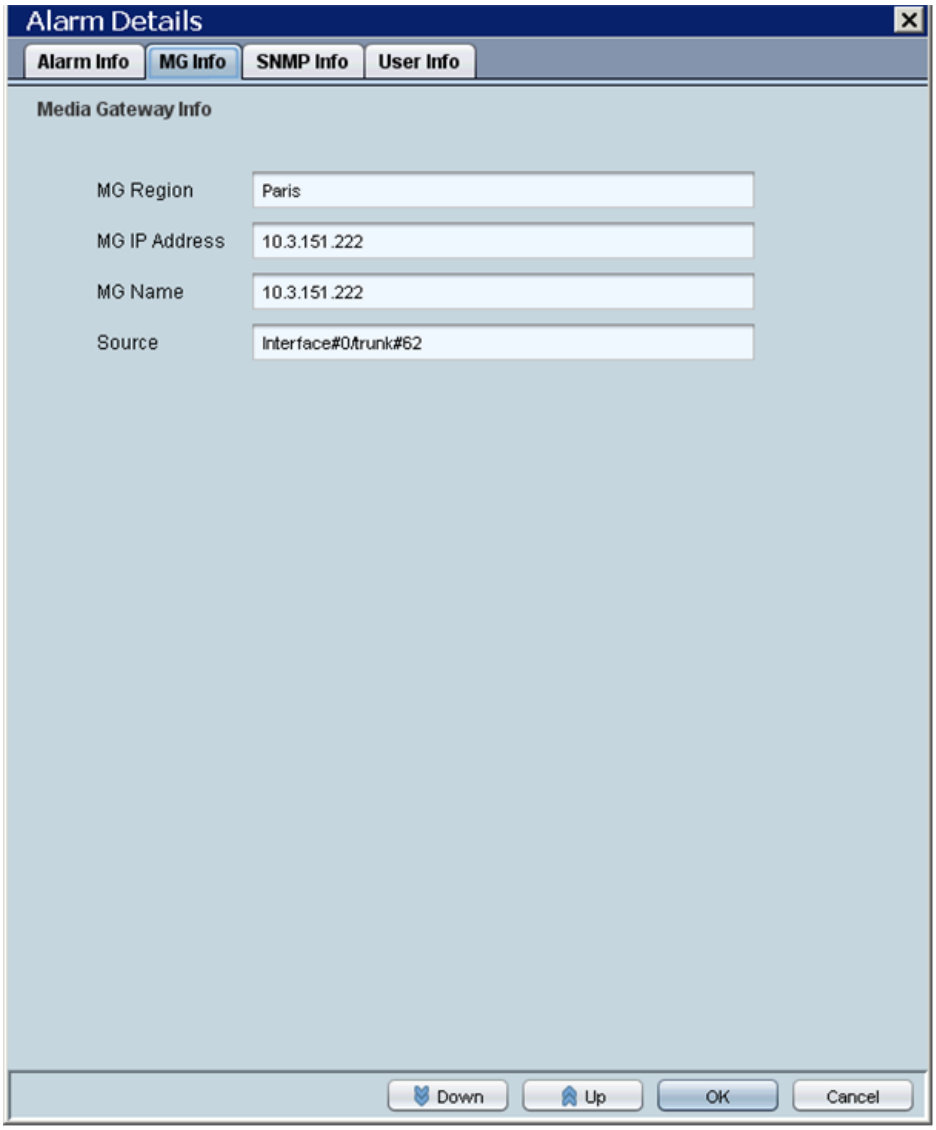
- Additional Info 1-3

  These three fields are provided as part of the alarm information, supplying additional information on the alarm.

26.2 Alarm Details - Tab MG Info

This section describes the MG Info tab.

Figure 26-2: Alarm Details-MG Info



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

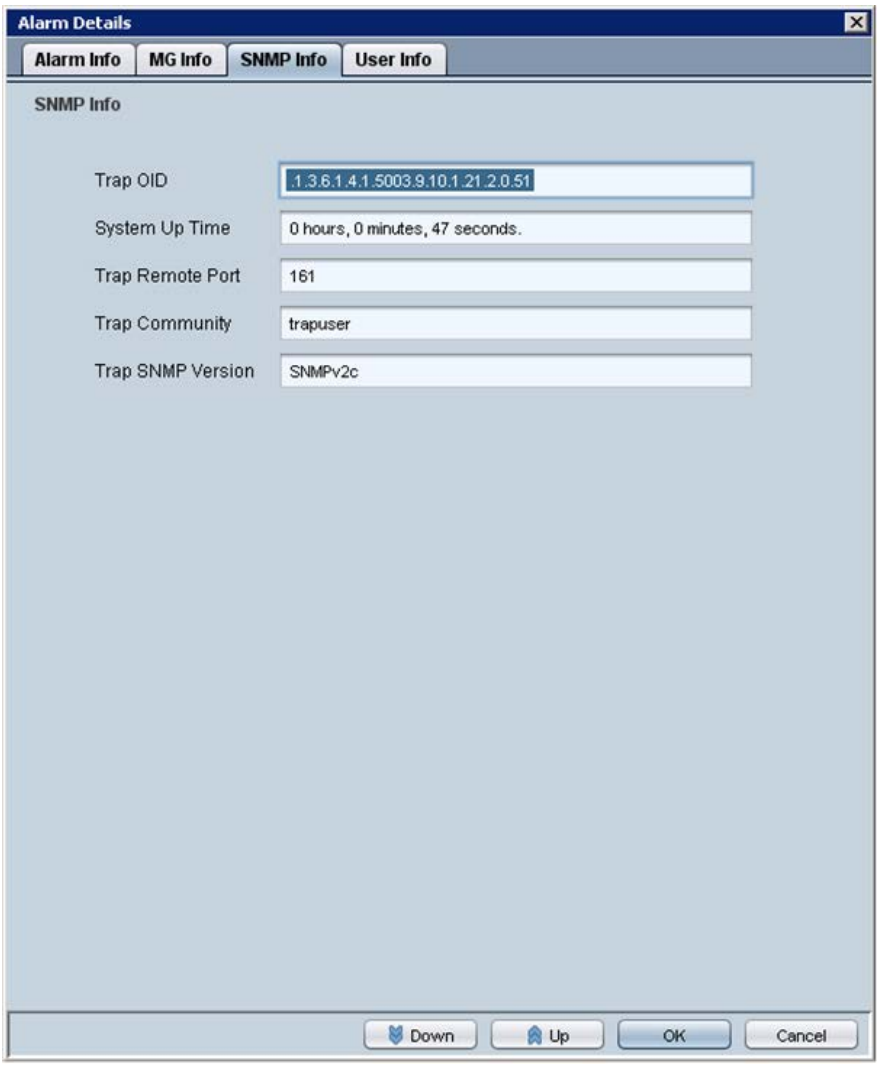
  Name of the media gateway that originated the alarm.
- Source

  The exact alarm source, in format 'board#3/trunk#7'

26.3 Alarm Details > Tab SNMP Info

This section describes the SNMP Info tab.

Figure 26-3: Alarm Details-SNMP Info



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

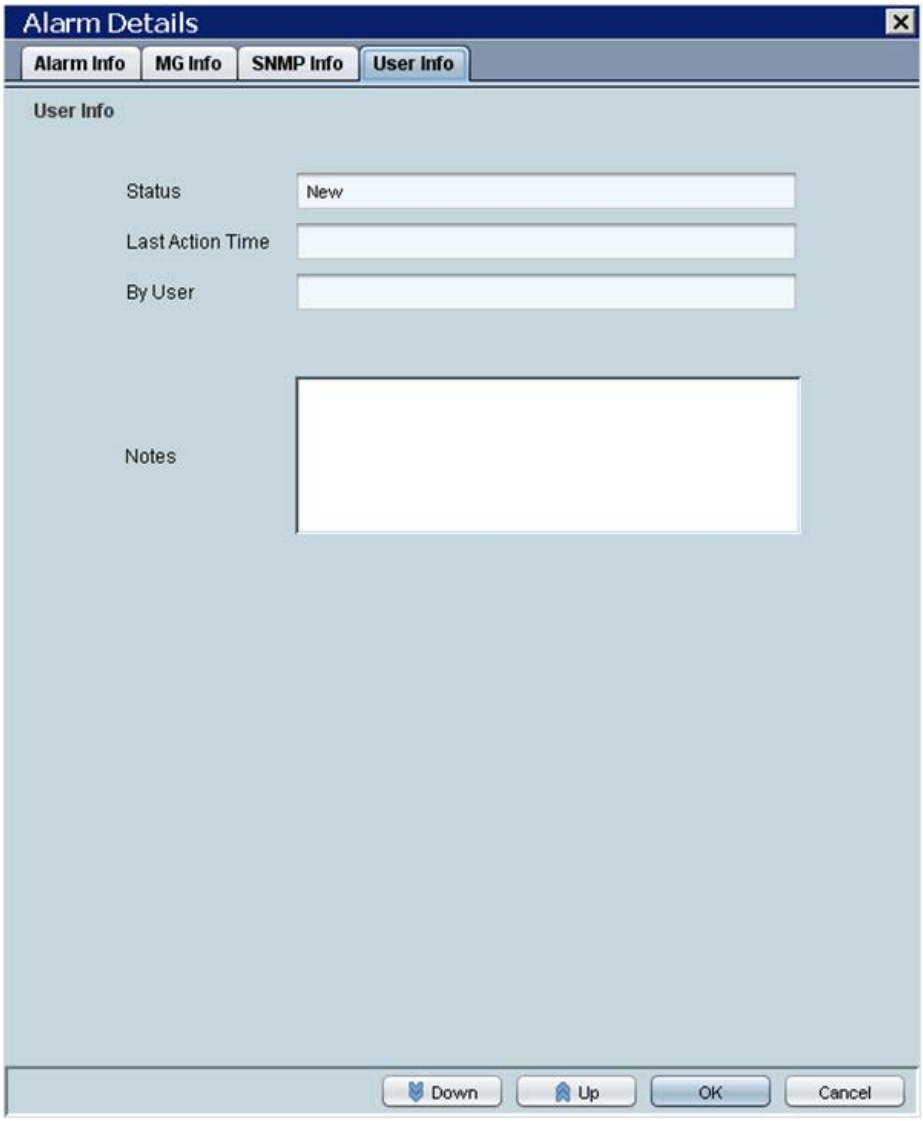
The SNMP version of the Agent that sent the trap. The SNMP version can be one of the following:

- SNMPv1
- SNMPv2c
- SNMPv3

26.4 Alarm Details > Tab User Info

This section describes the User Info tab.

Figure 26-4: Alarm Details-User Info



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.

This page is intentionally left blank

27 Trap Forwarding

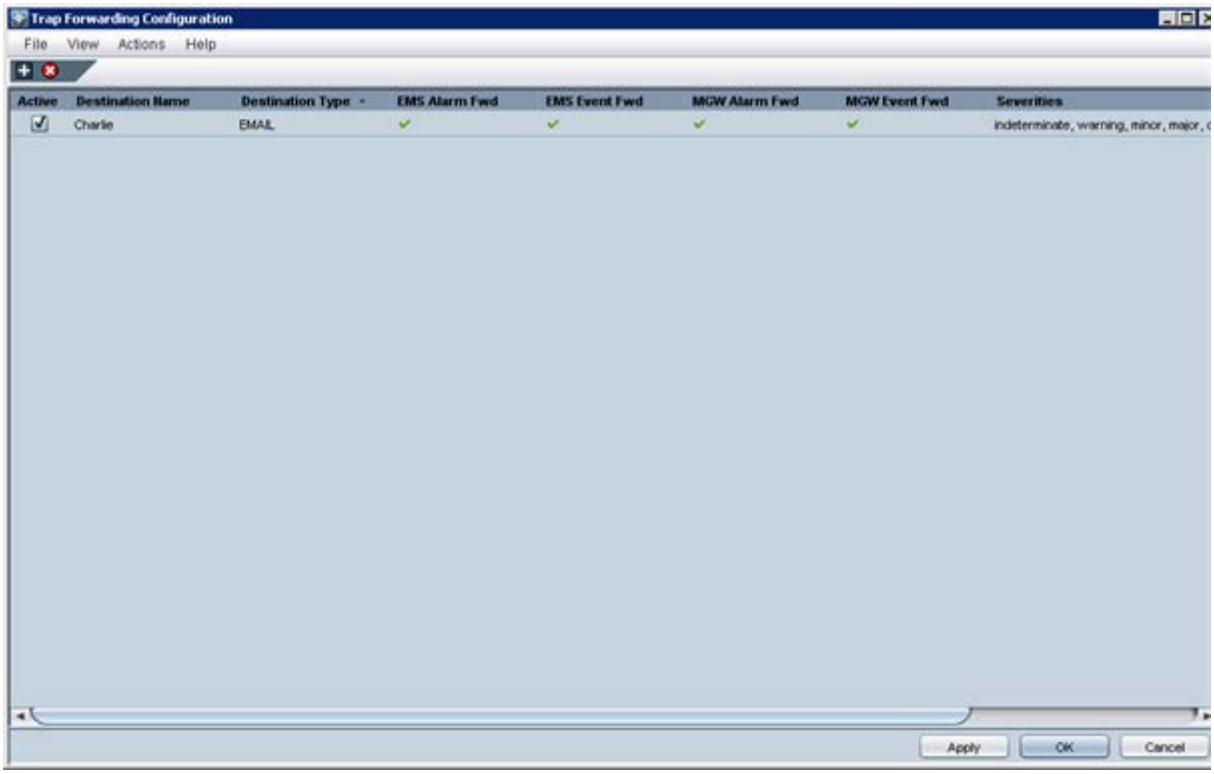
All the alarms and events issues by media gateways are send as SNMP Notifications. EMS can forward alarms and events in the following formats:

- 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 27-1: Trap Forwarding Summary-Mail



27.1 Trap Forwarding in Mail Format

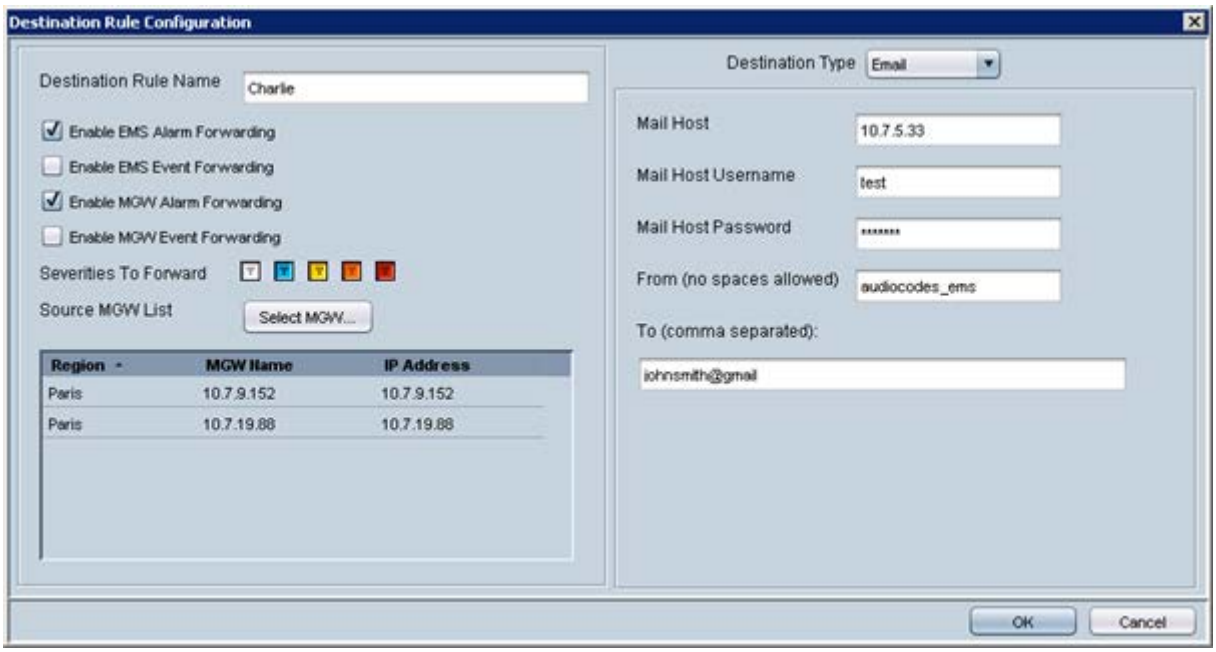
This option describes how to forward traps from EMS to a mail server host in e-mail format.

➢ **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.

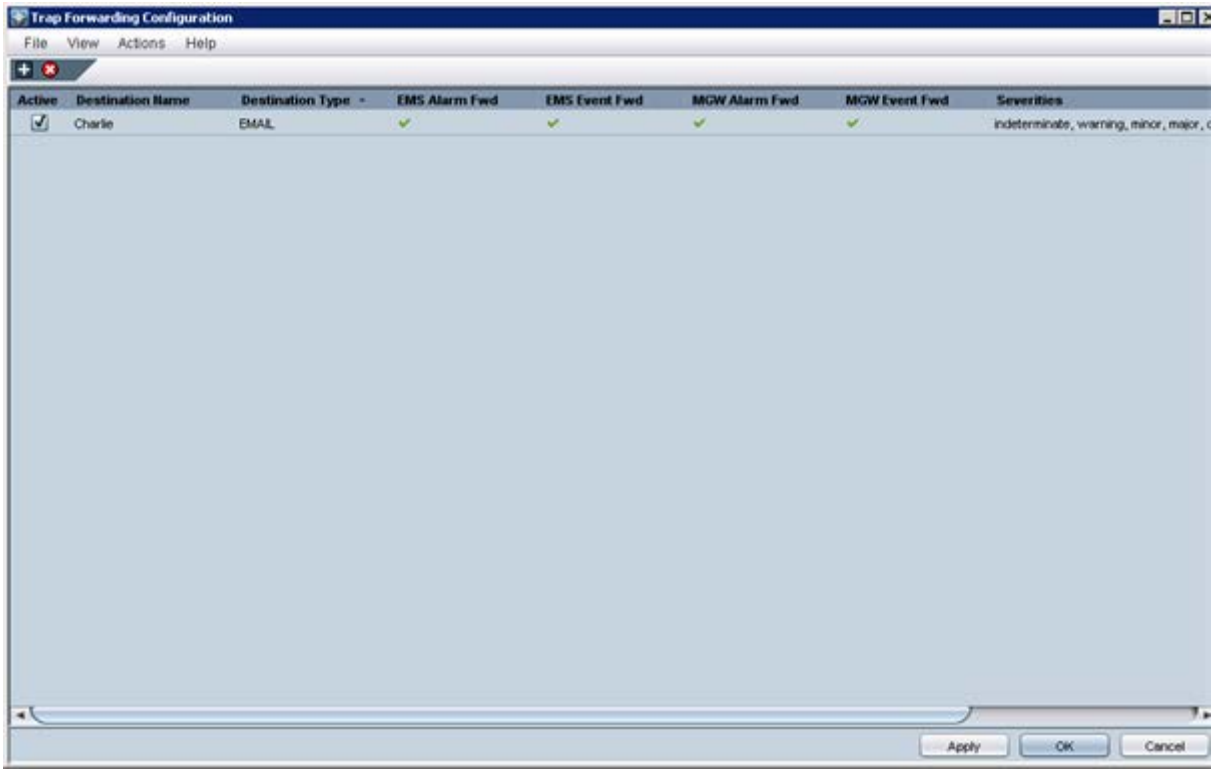
Figure 27-2: Trap Forwarding-Email



6. Click **OK**.

Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 27-3: Trap Forwarding Summary-Mail



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
```

27.2 Trap Forwarding in Mail2SMS Format

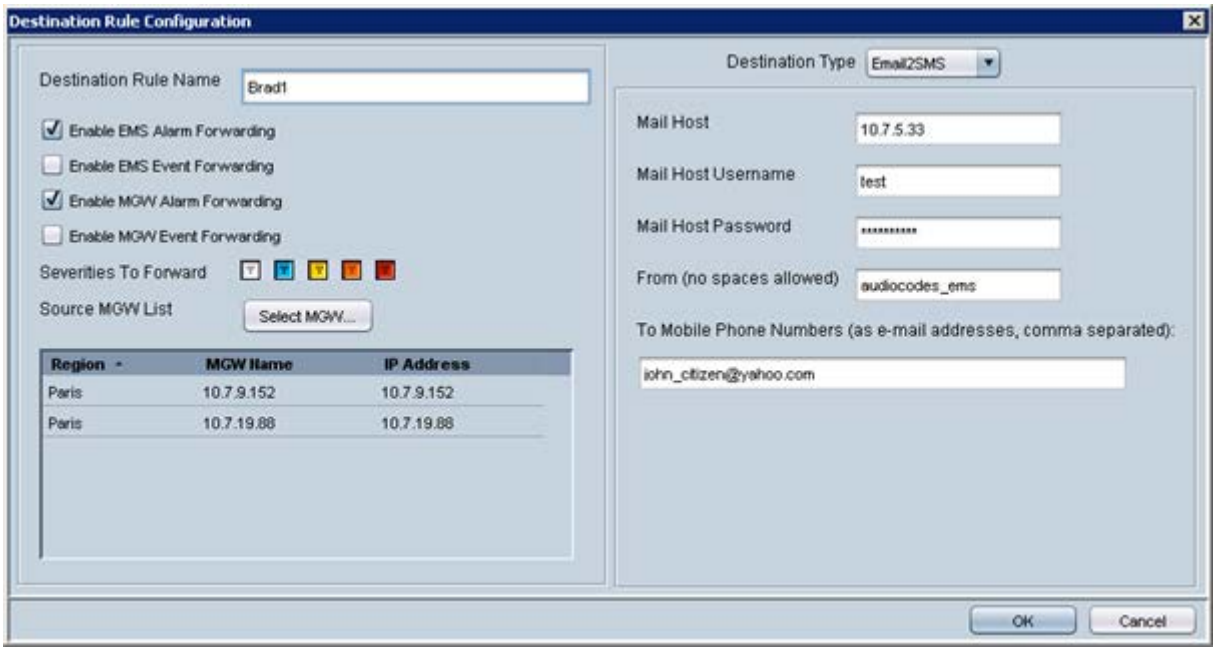
This option describes how to forward traps from EMS to a mail server host in mail2SMS format.

➢ **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.

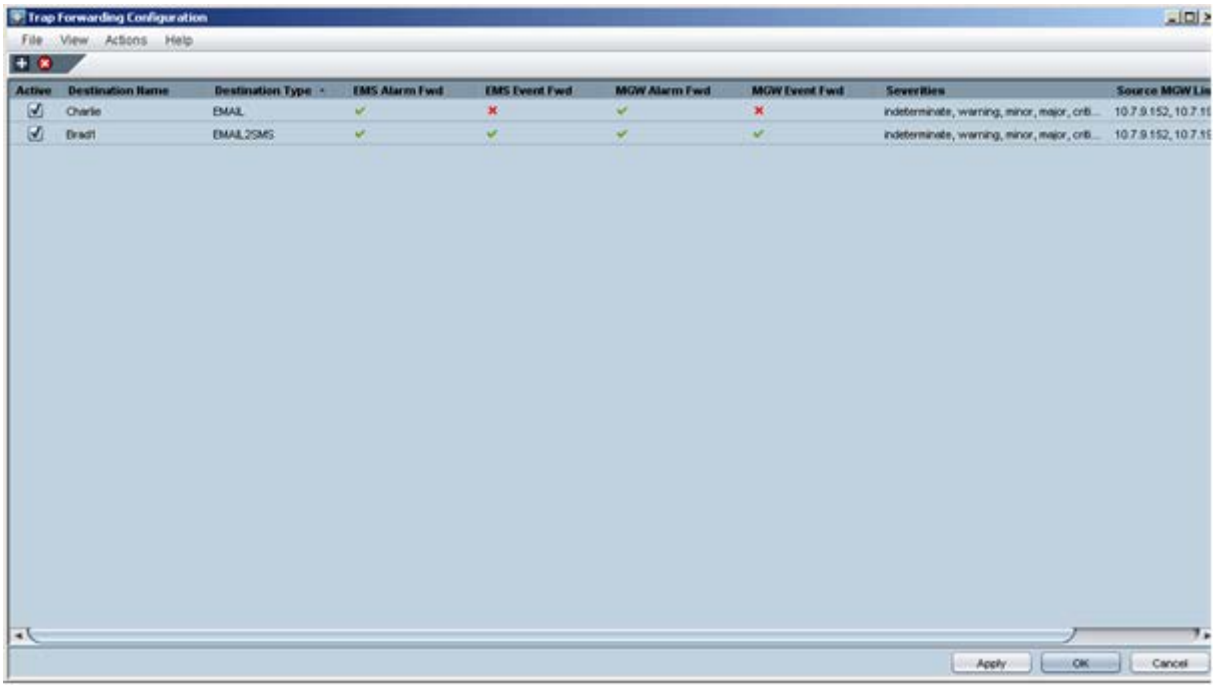
Figure 27-4: Trap Forwarding-SMS



6. Click **OK.**

   Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 27-5: Trap Forwarding Summary-Mail2SMS



SMS traps are forwarded to specified destinations in the following format:

```
SMS format
New <Alarm/Event> <Alarm Name>, received from <Node Name, Node IP>
with Severity <Severity>. Description:
```

27.3 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:**

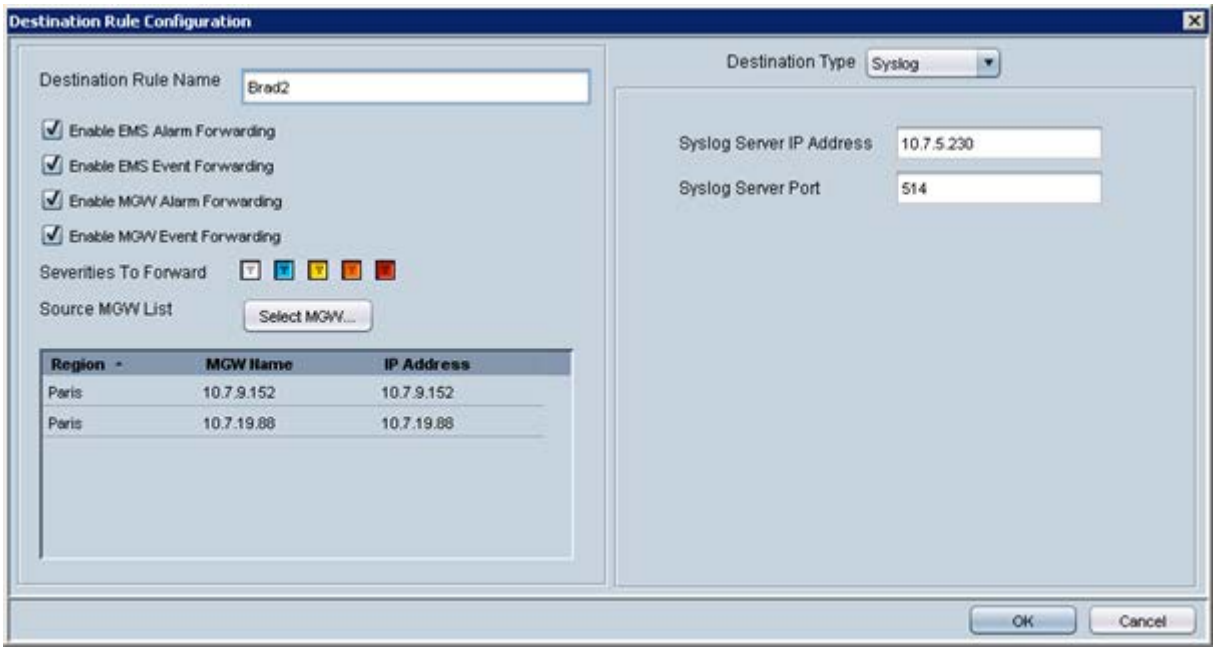
1. Open the **Faults** > **Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Syslog**.
4. In the left-hand pane, provision the following parameters:
   - '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.

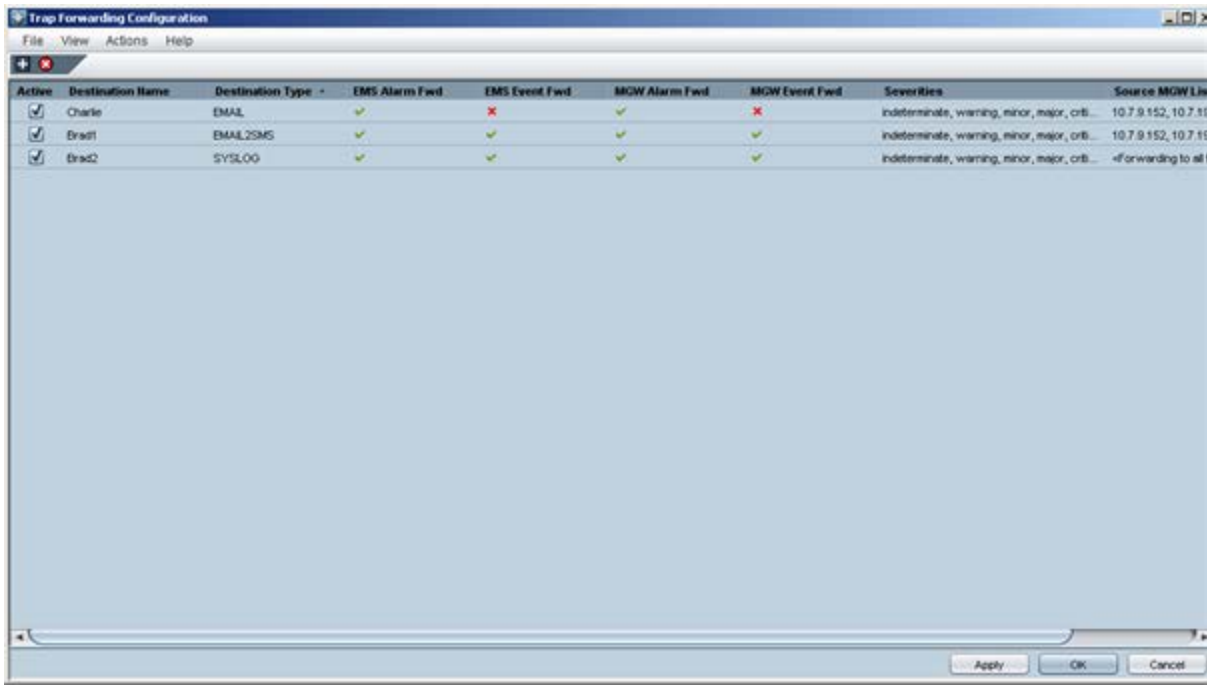
Figure 27-6: Trap Forwarding-Syslog



6. Click **OK.**

Your new rule is displayed in the Trap Forwarding Configuration summary screen.

Figure 27-7: Trap Forwarding Configuration Summary-Syslog



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 27-1: 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>
```

This page is intentionally left blank

28 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.

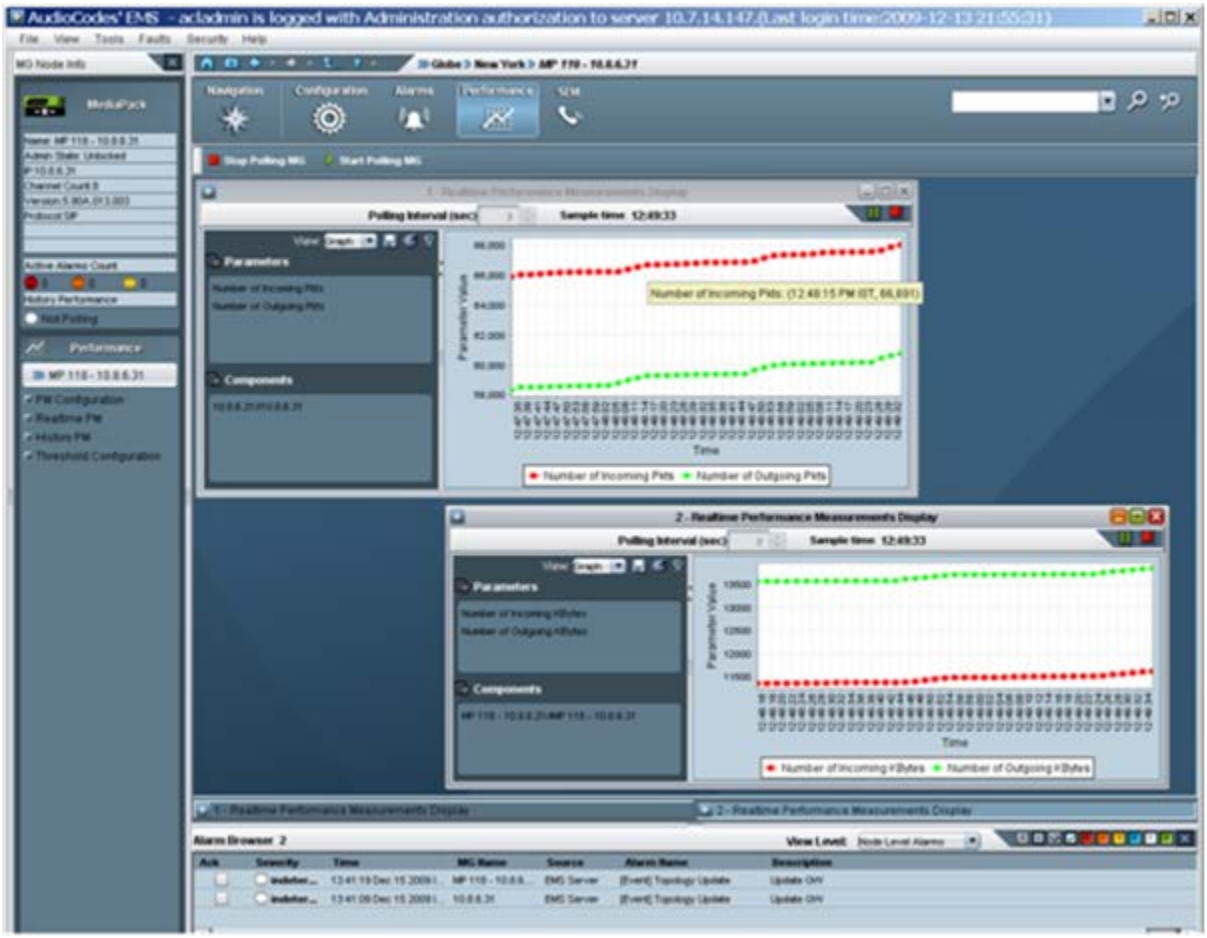
This page is intentionally left blank

29 Performance Management

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

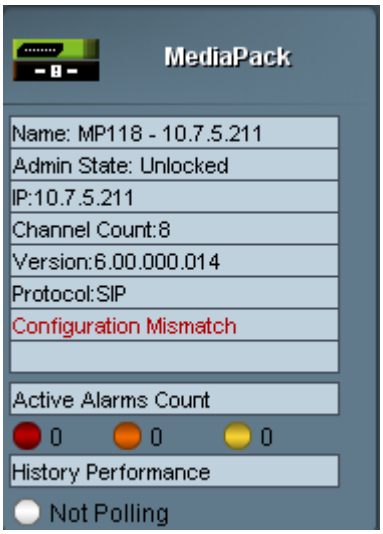
The EMS's Performance Management is composed of real-time and historical data monitoring. Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. Historical data can be used for long-term network analysis 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 29-1: Performance Desktop



Note: 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.

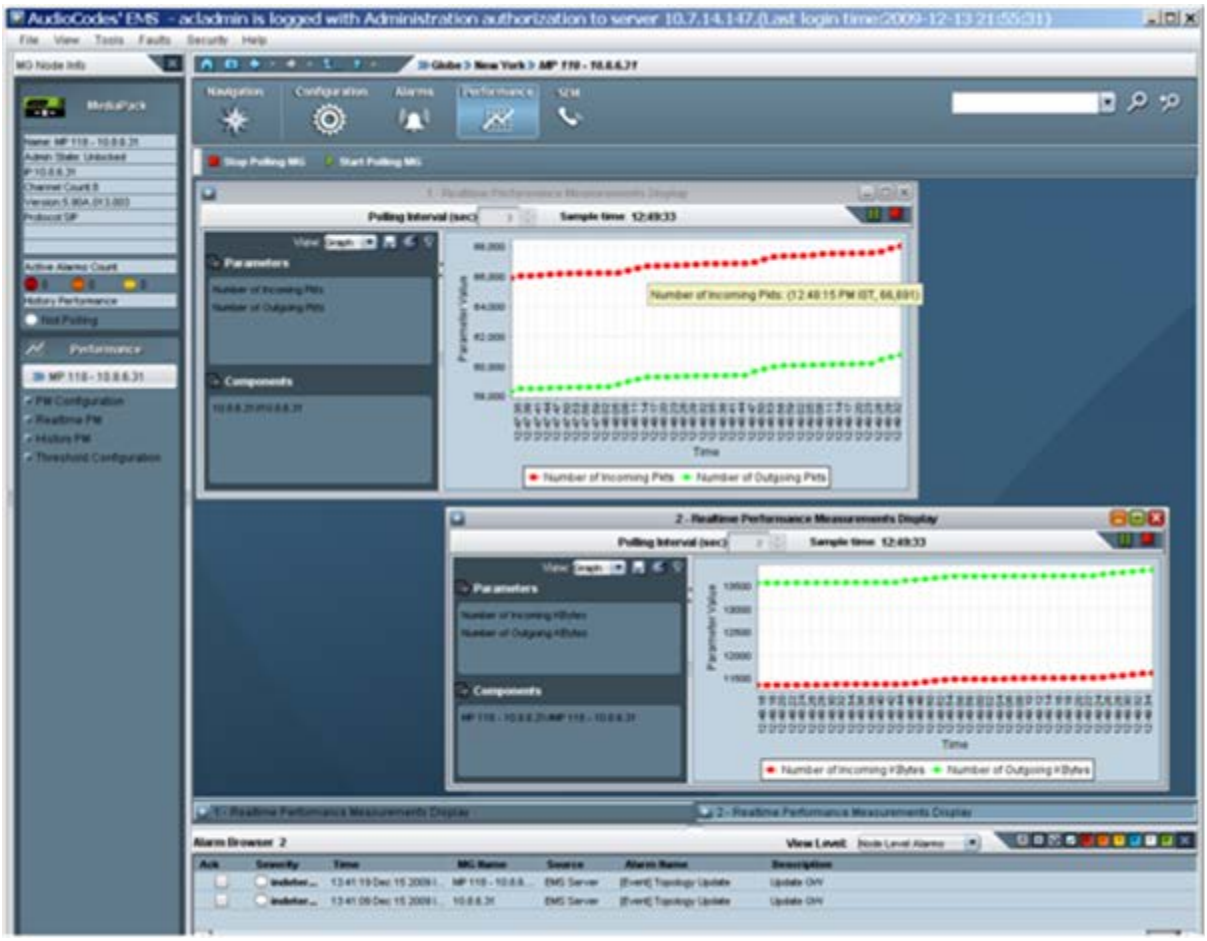
Figure 29-2: Performance Monitoring Icon in the Info Pane



29.1 Real-Time Performance Monitoring

Real-time performance monitoring provides EMS users with the ability to perform high-frequency polling of various system parameters.

Figure 29-3: Real-time PMs



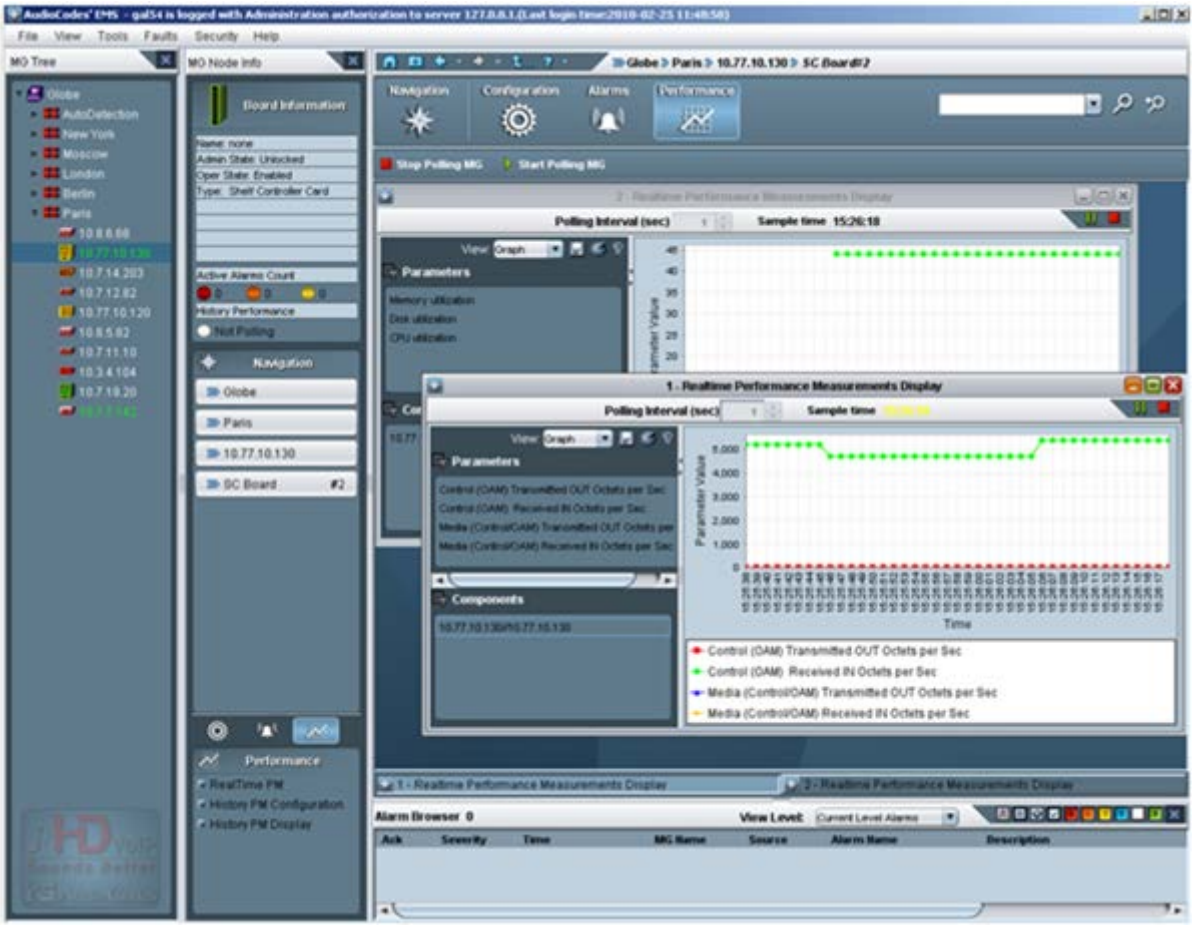
➢ **To select an entity to poll:**

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.

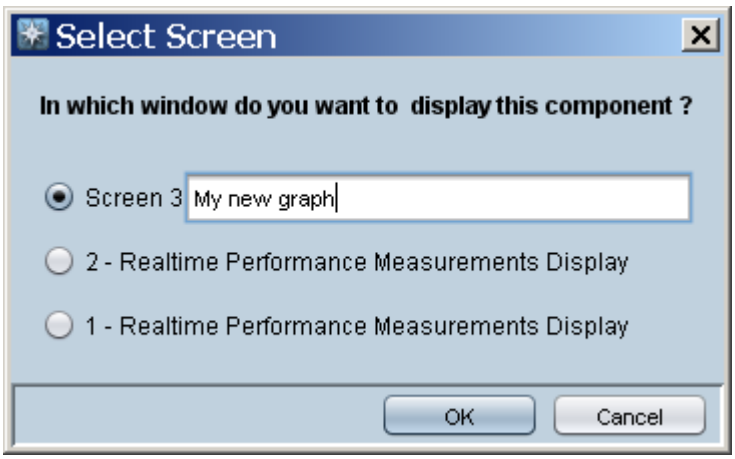
2. To define additional real-time performance monitoring windows, in the Performance pane, select **RealTime PM**.

Figure 29-4: 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 29-5: Selecting the Frame to Display the Graph of the Entity's Performance



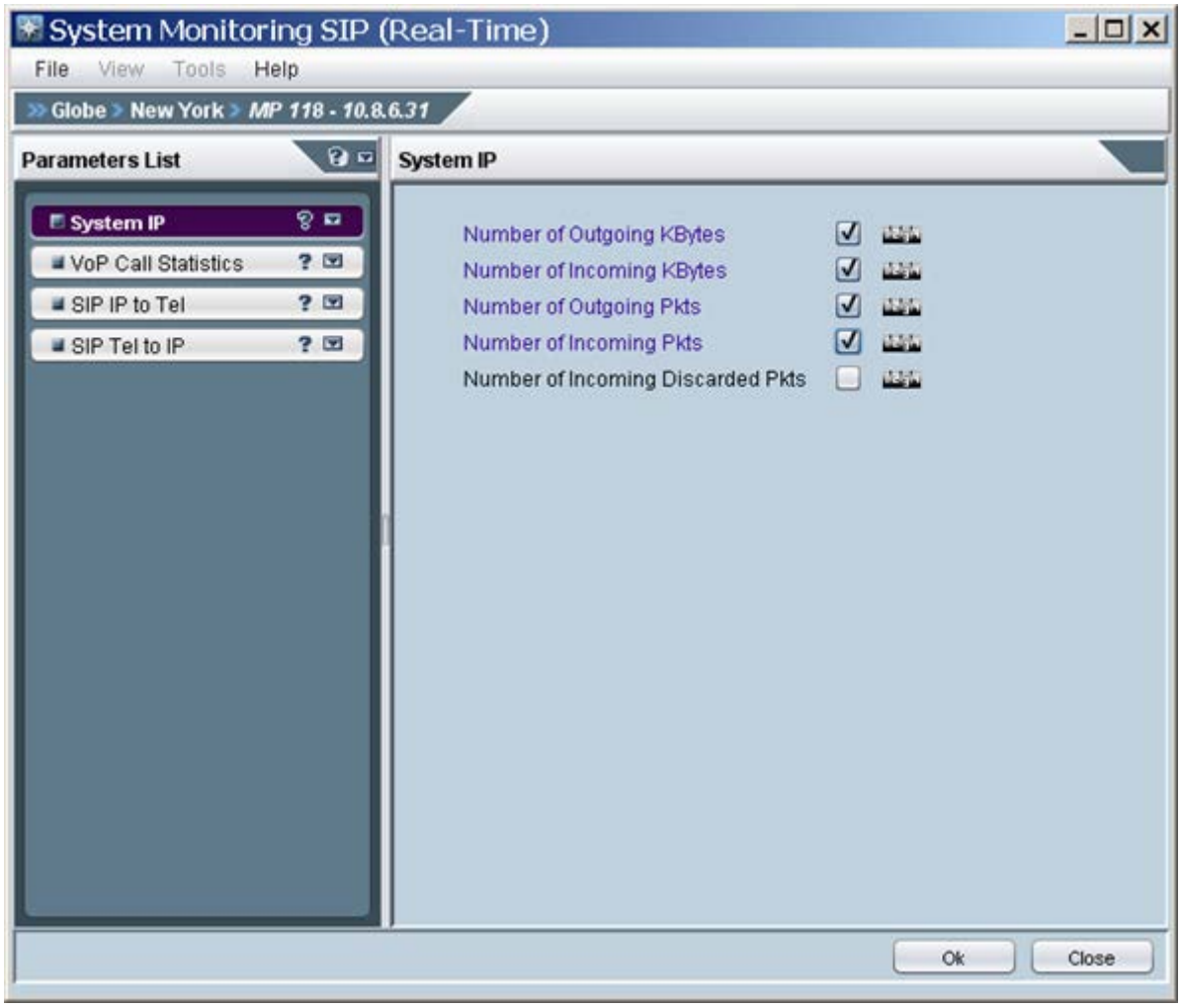
Users can open up to five separate real-time graphs in the same client application. There are two graph types that operators can use: Line Graph and Table View. In most cases, Line Graph is recommended when only a few parameters are compared. Table View is recommended when extensive data is displayed 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 .

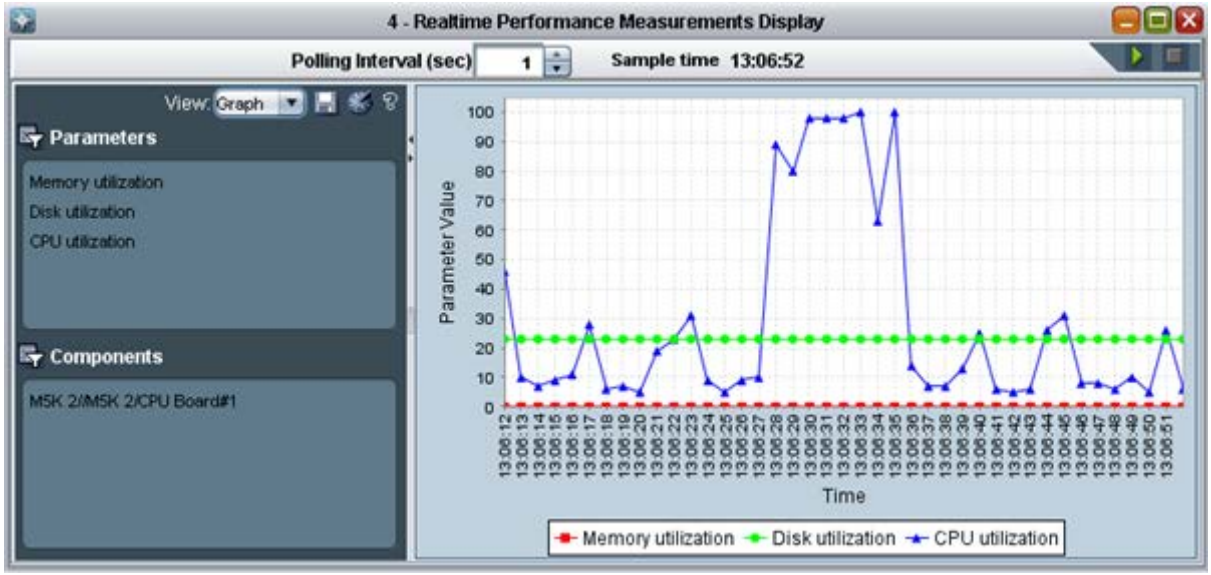
Figure 29-6: Parameter Type - Counters



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 29-7: Graph Comparing CPU, Disk and Memory Utilization of SC Boards in Media Gateways



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.

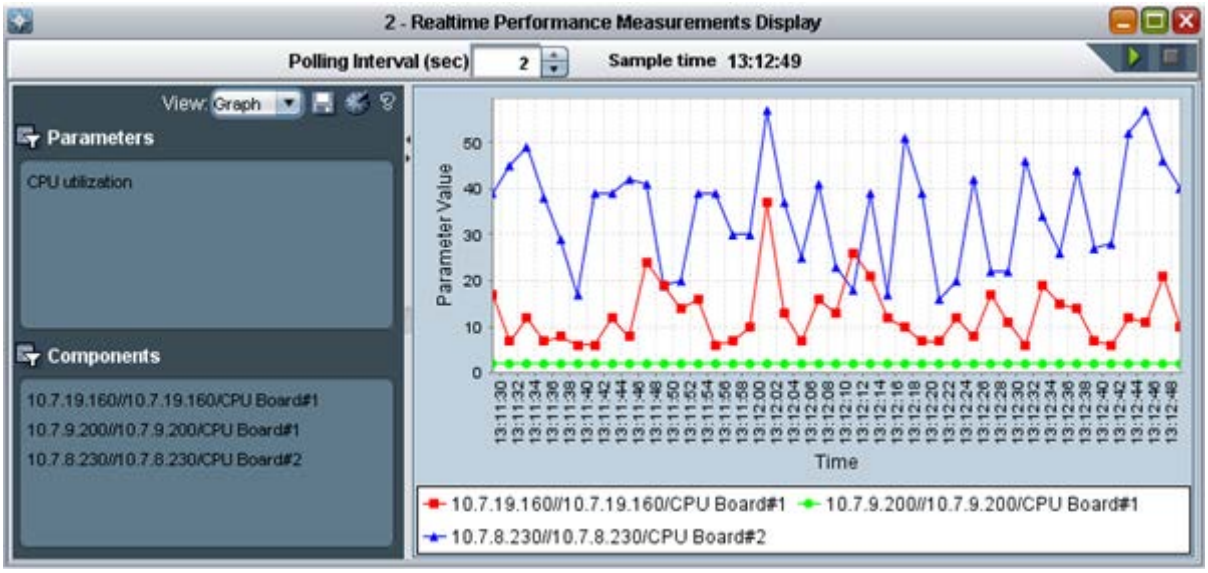
  At each stage, you can position your cursor over the nodes in the graph and view - in the tool tip - the precise information you require (the exact value of the parameter at the monitored point in time).

  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):

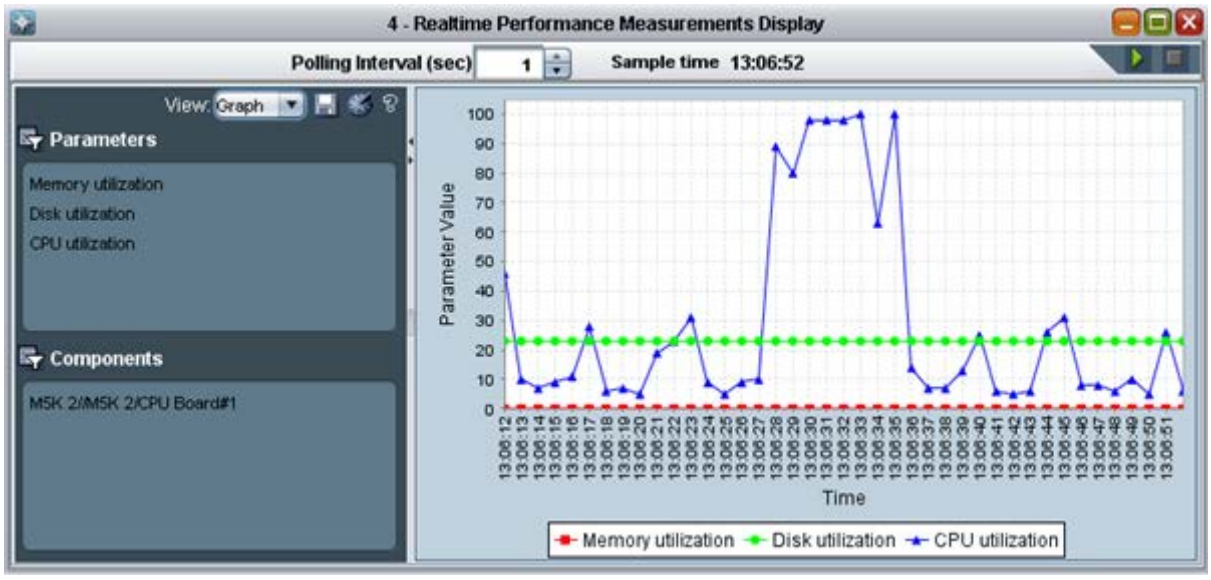
- Compare CPU utilization of System Controller boards in the gateways.

Figure 29-8: Graph Comparing CPU Utilization of SC Boards in Media Gateways



- View CPU, Memory and Disk utilization of the System Controller board #1 in the Mediant 5000 media gateway.

Figure 29-9: View CPU, Memory and Disk Utilization of Mediant 5000 SC Board 1



29.2 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\

Note: Before collecting History Performance measurements, you must define a PM profile. For more information, see 'Configuring Background Monitoring' on page 303 below.

- Exporting Background Monitoring Data as a file
- Viewing Historical Data

29.2.1 Configuring Background Monitoring

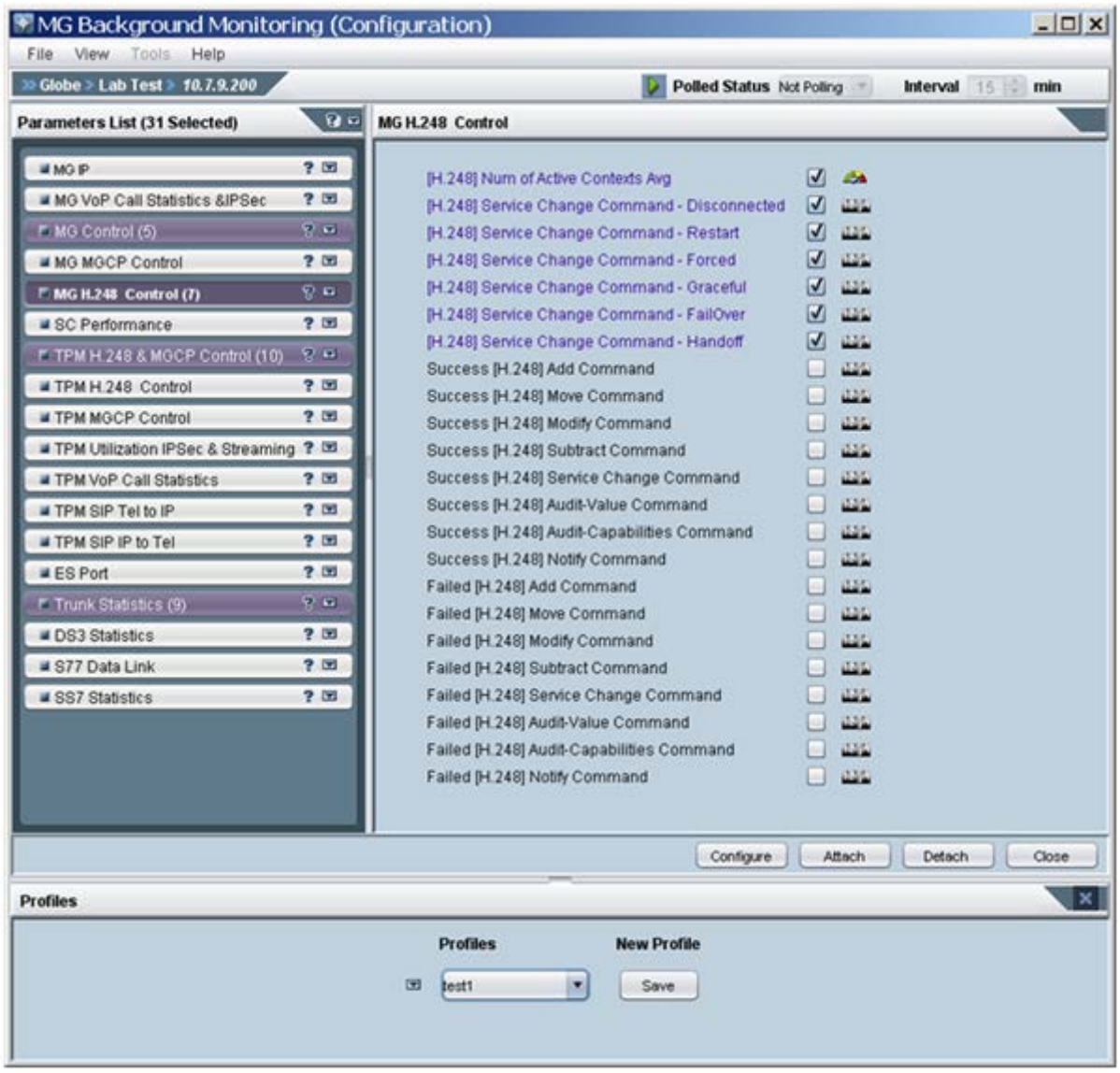
This section describes how to define a performance management profile. This procedure must be performed before you can view historical data.

➢ **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 29-10: Background Monitoring Provisioning Parameters



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.

29.2.2 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
```

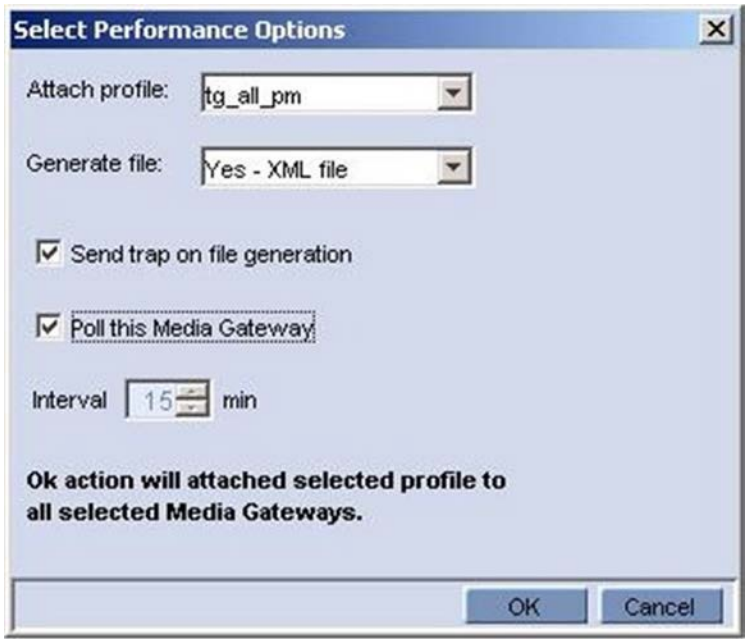
Users should forward the trap to the NMS (Network Management System) (see Section 'Trap Forwarding to NB IF' on page 282).

➢ 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 29-11: Background Monitoring - Generate File Options



Note: A performance data file cannot be created unless the media gateway is polled (see section 'Configuring Background Monitoring' on page 303.

- 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*.

29.2.3 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 needs be) 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.

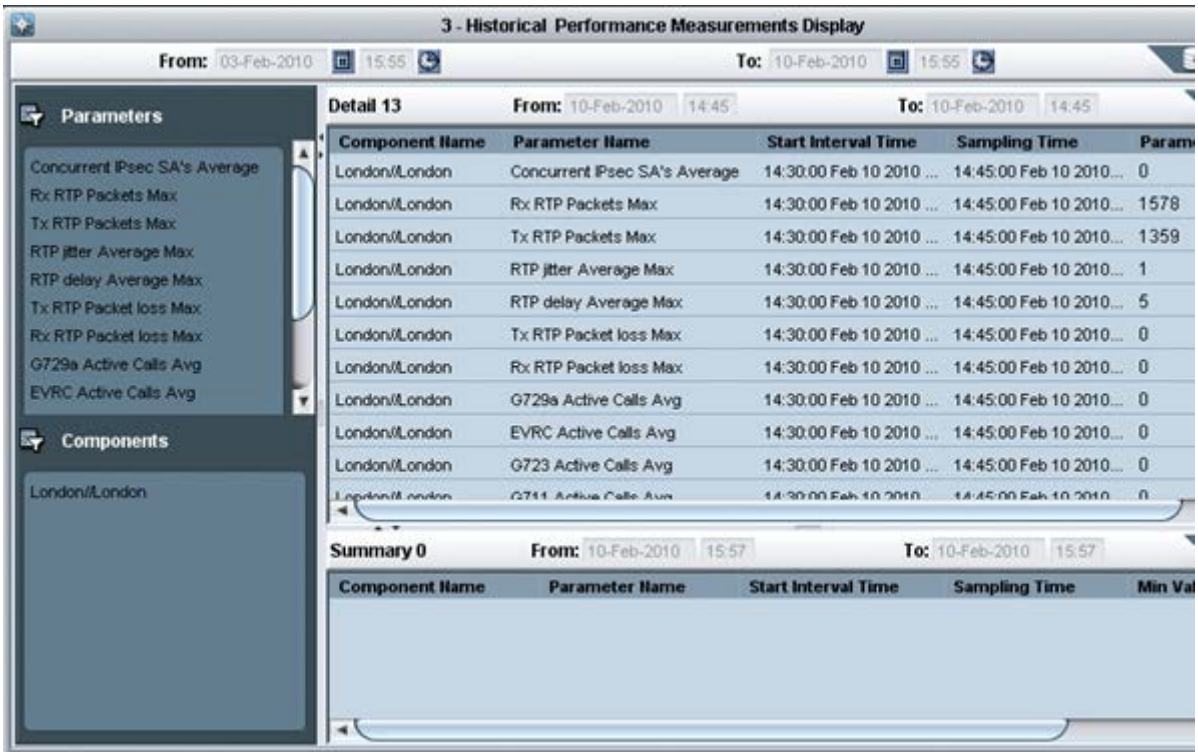
   Historical data comprises two tables: The uppermost table displaying detailed data (in user-defined intervals) and the table below it displaying summarized data.

   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 start and stop summary time is stored and the average, minimal and maximal value is displayed.

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 29-12: Performance Monitoring - Historical Data



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.

29.3 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.

29.3.1 Configuring Performance Monitoring Threshold Values for CPE Products

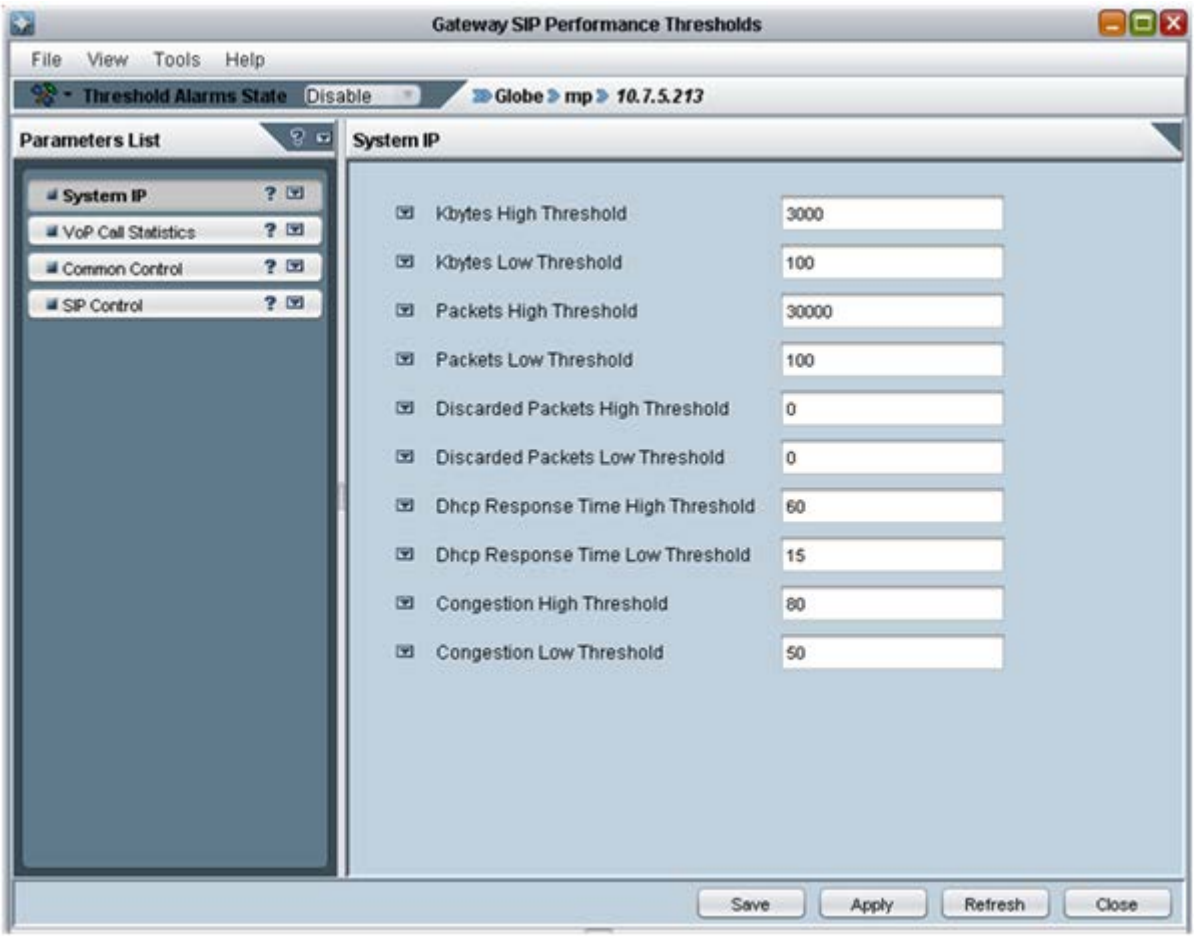
This section describes how to configure performance monitoring thresholds for CPE Products.

➢ **To provision the gateway to issue a Threshold Crossing Alarm:**

1. Select the relevant MO entity for which you wish to display Historical PMs. For example, select the media gateway board, 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 29-13: MediaPack Performance Thresholds



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.

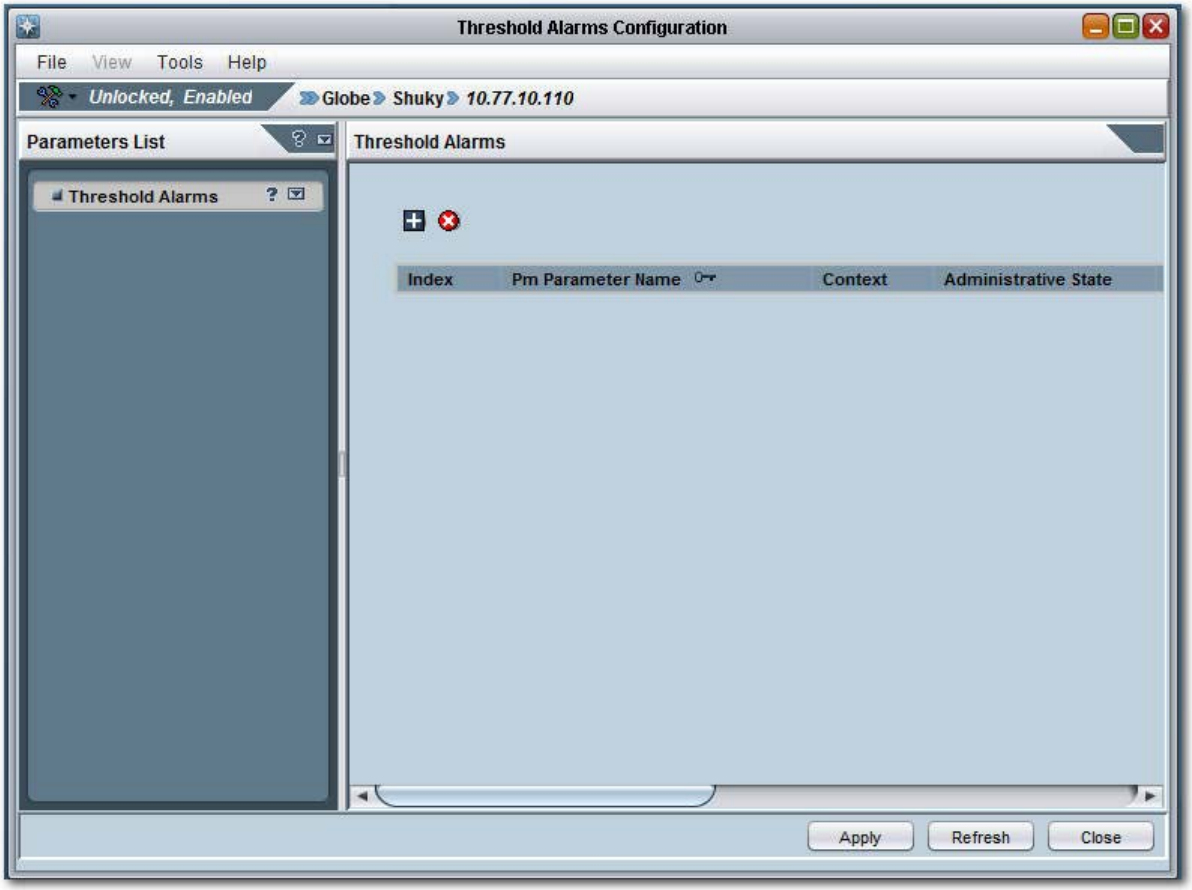
29.3.2 Configuring Performance Monitoring Threshold Values for Mediant 5000 / 8000 Media Gateways.

The feature is applicable for History PMs only, for both Counters and Gauge 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 29-14: 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 29-15: Threshold Alarms Parameters-MG VoP Statistics and IPSec

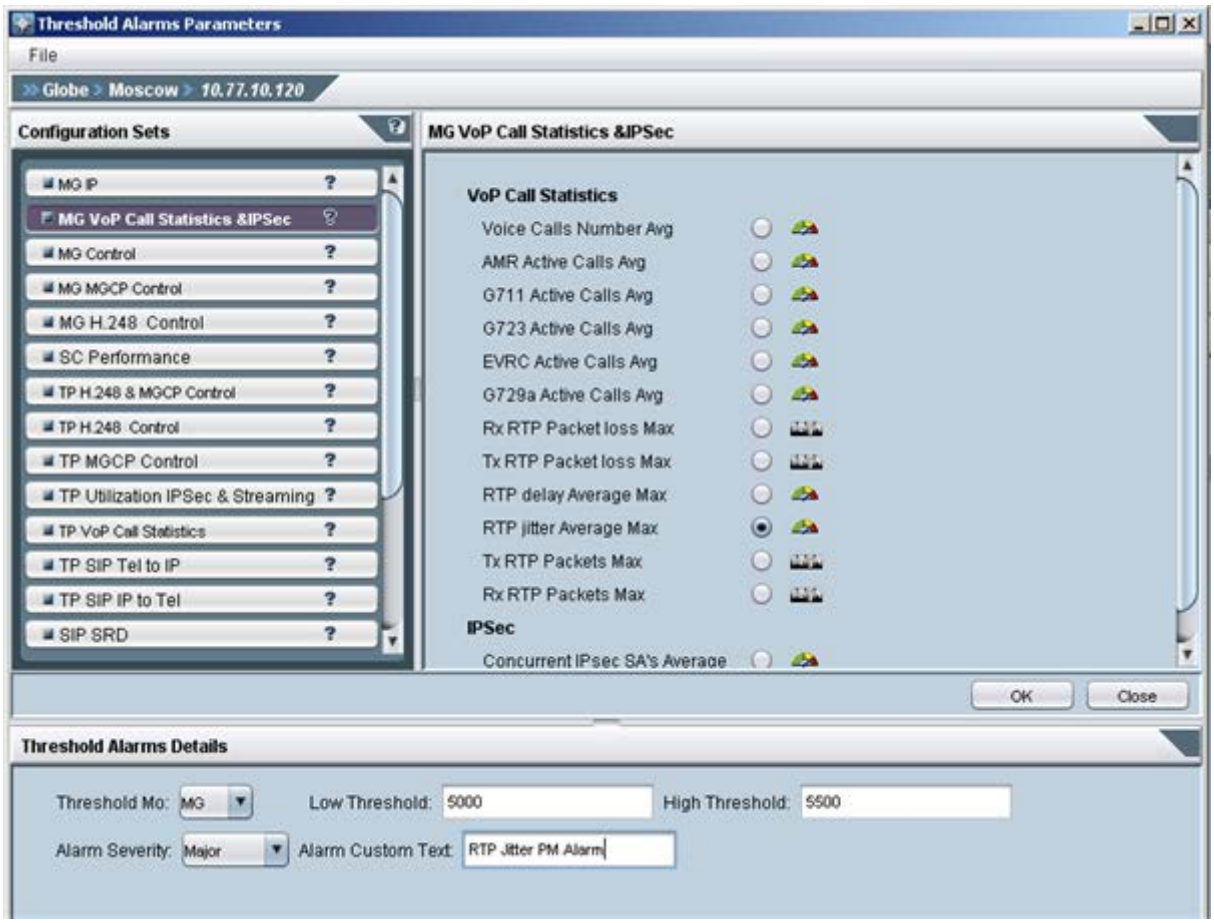
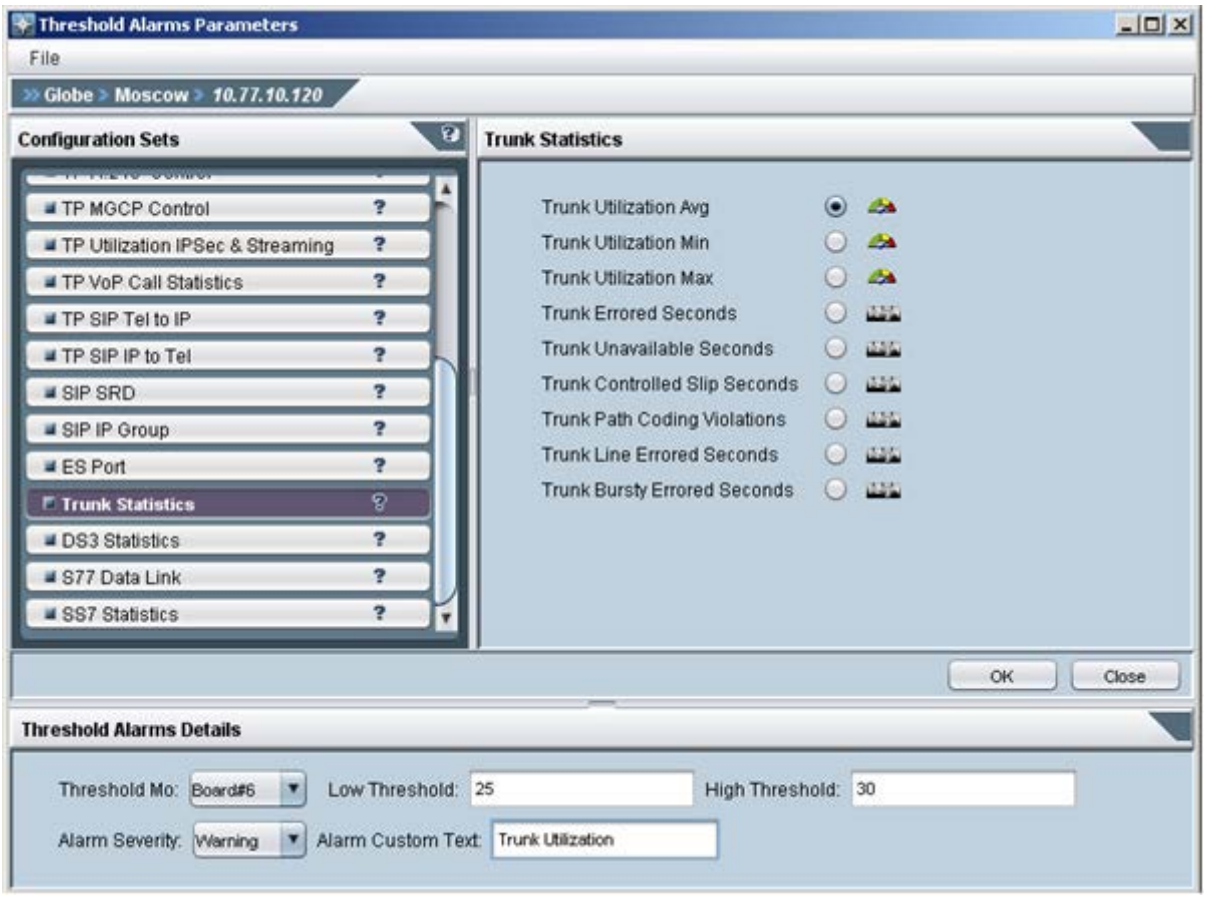
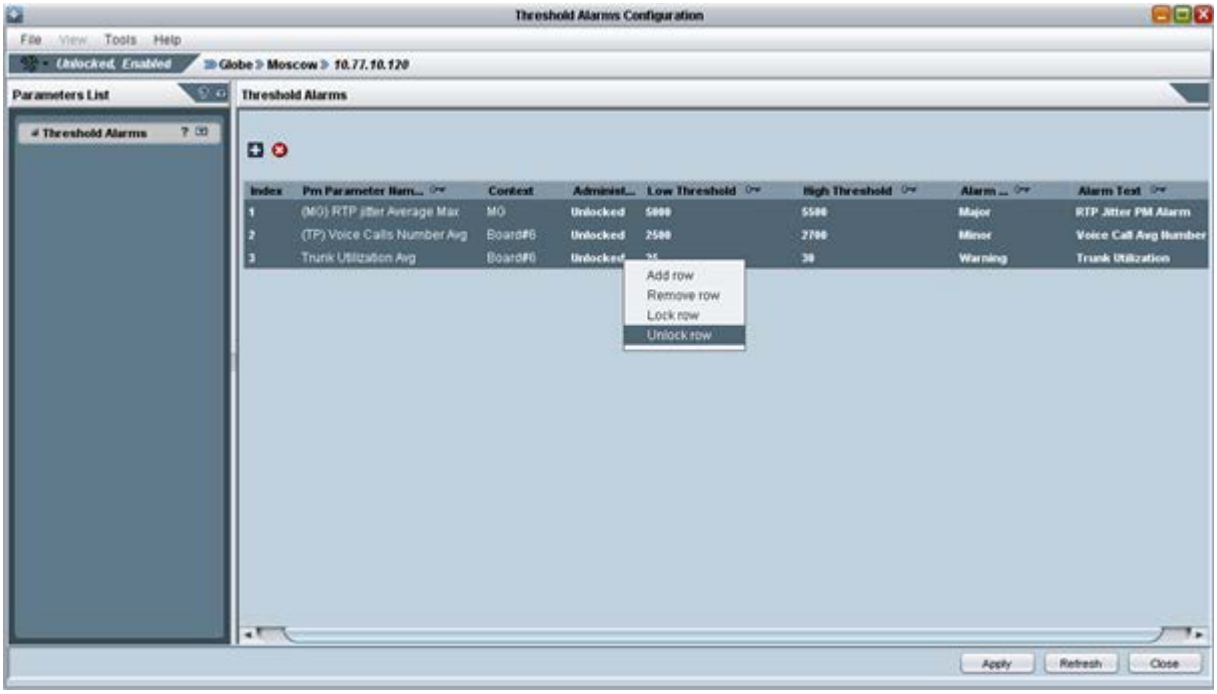


Figure 29-16: Threshold Alarms Parameters-Trunk Statistics



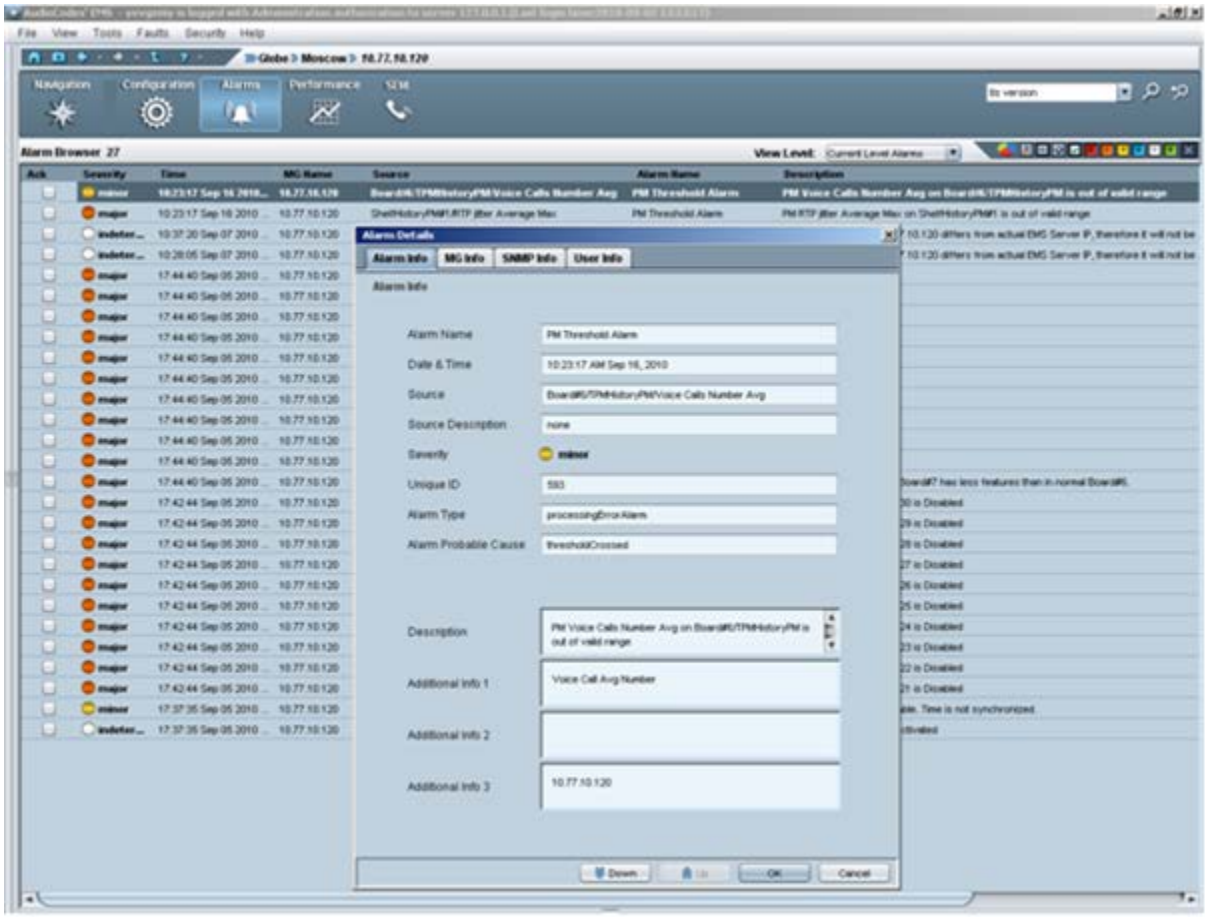
5. When all the required thresholds are defined, the user should perform **Unlock** to unlock all the rows in the Thresholds table. Once all the entries are Unlocked, the Gateway starts to collect measurements.

Figure 29-17: Threshold Alarms Configuration



6. When the threshold value is crossed, the gateway generates a Threshold alarm with all the required information. See the example below.

Figure 29-18: Threshold Alarm Details



29.4 Performance Monitoring Actions on Multiple Media Gateways

This section describes performance monitoring actions on multiple media gateways.

Figure 29-19: Performance Monitoring Actions on Multiple Media Gateways

Users can perform following actions on multiple gateways:

- Attach / Detach Profile
- Start / Stop Polling

Note: 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.

This page is intentionally left blank

Part V

Session Experience Manager (SEM)

This section describes the Session Experience Manager (SEM) for voice quality management.

30 Overview

AudioCodes' Session Experience Manager (SEM) is a valuable new tool that delivers important technical and business statistics based on AudioCodes methodologies developed over years of experience in VoIP.

The SEM provides real-time management of VoIP traffic, giving VoIP network administrators a network health monitoring functionality that includes alarms and diagnostics capability.

This document shows how to deploy and utilize the SEM to maximum advantage, to enhance the quality of experience enjoyed by VoIP users.

30.1 How the SEM Benefits VoIP Network Administrators

The SEM enables VoIP network administrators to do the following:

- Quickly identify the metric or metrics responsible for degradation in the quality of any VoIP call made over the network.
- Accurately diagnose voice quality problems in response to VoIP user criticism.
- Prevent VoIP quality degradation.
- Optimize quality of experience for VoIP users.

30.2 Measuring Voice Quality in a VoIP Network

The following important metrics are factorized into the equation when measuring voice quality of calls made over a VoIP network:

- **Mean Opinion Score (MOS)** (specified by ITU-T recommendation P.800) is the average grade on a quality scale of Good to Failed, given by the SEM to voice calls made over a VoIP network, after testing.
  MOS-LQ = listening quality, i.e., the quality of audio for listening purposes; it doesn't take bi-directional effects, such as delay and echo into account.
  MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects.
- **Jitter,** measured by the SEM, can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
- **Packet Loss**, measured by the SEM, can result in choppy voice transmission. Lost packets are RTP packets that aren't received by the voice endpoint for processing.
- **Delay** (or latency), calculated by the SEM, is the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.

This page is intentionally left blank

31 Configuring Devices to Measure QoE and Report to the SEM

This section describes how to measure QoE and Report to the SEM.

31.1 Generic Device Configuration

➢ **To provision an AudioCodes device to report quality metrics to the SEM:**

1. In the Navigation pane, select **VoIP** > **Media** and then in the Configuration pane, click **Quality of Experience**. The following screen is displayed:

Figure 31-1: Quality of Experience

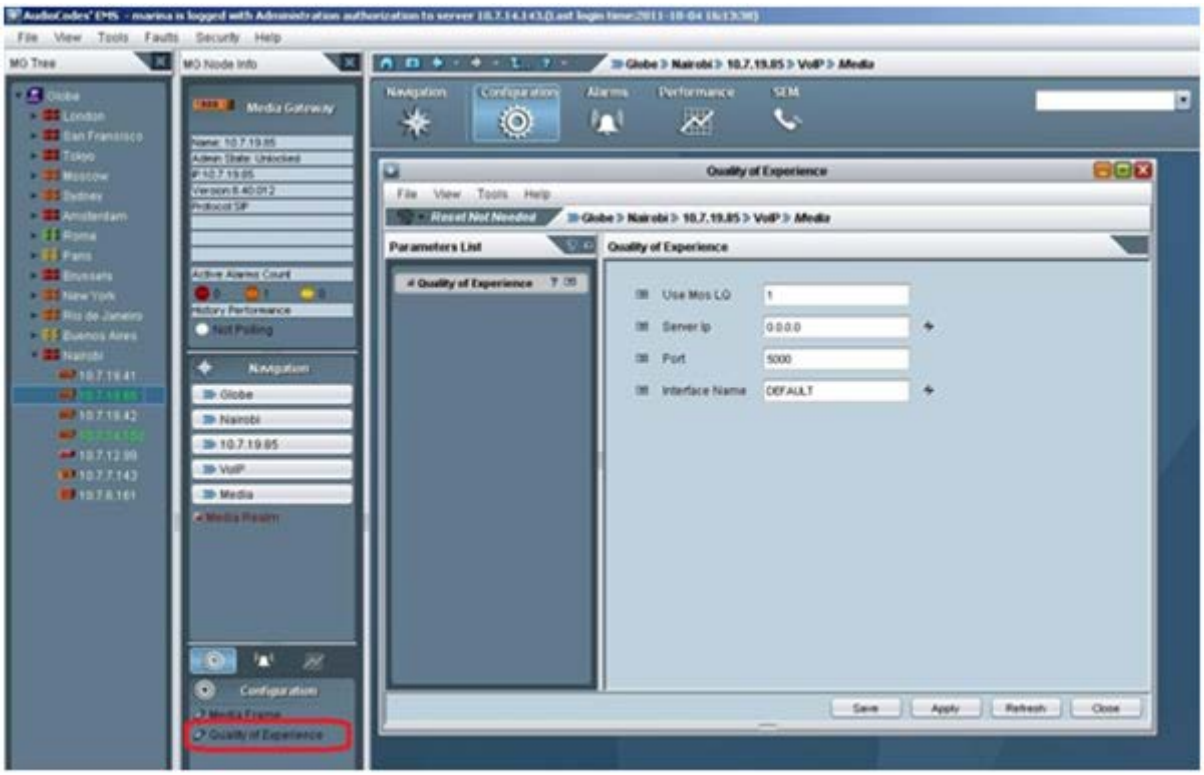


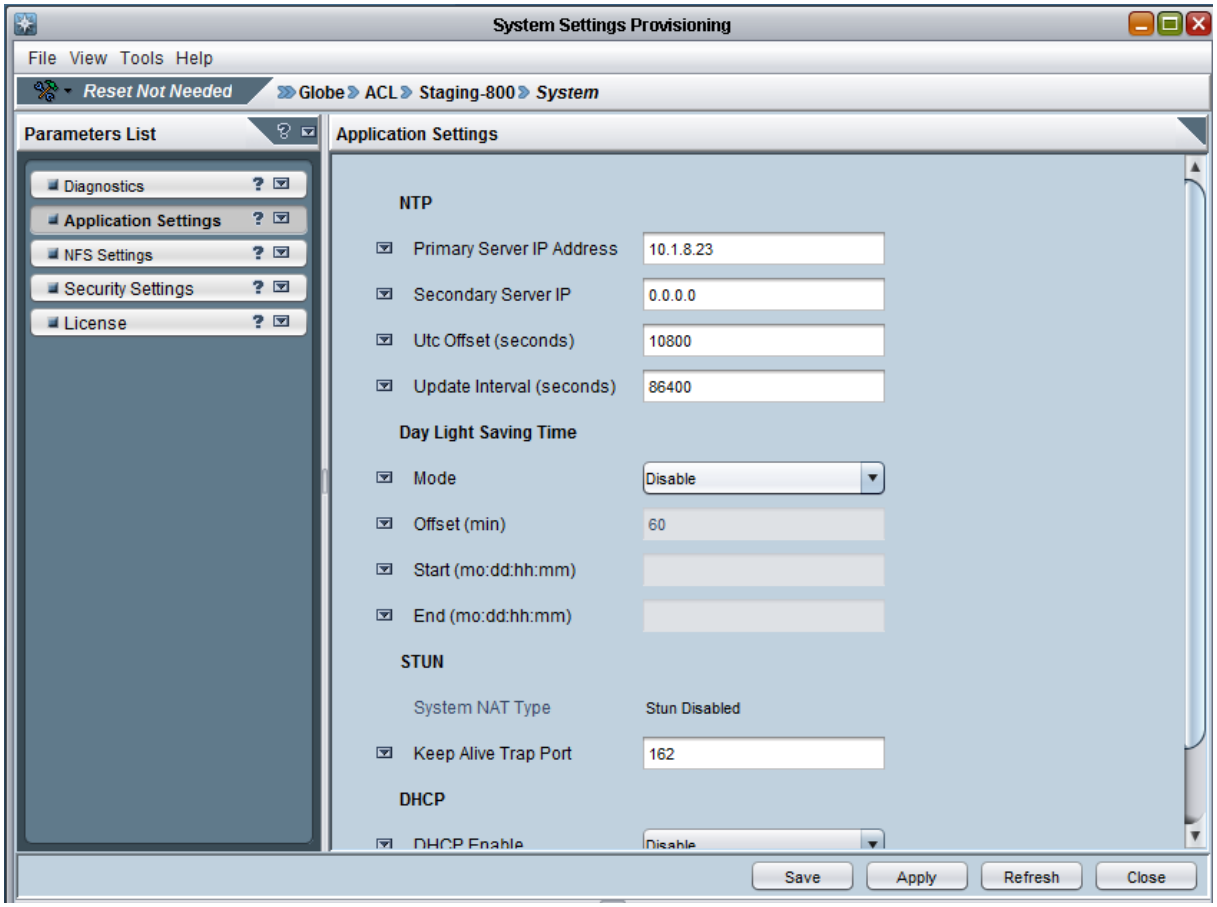
Table 31-1: Quality of Experience Parameters

Parameter Name	Description	Values
Use MOS LQ	Enables reporting of MOS-LQ (listening quality). If disabled, MOS-CQ (conversational quality) is reported. MOS-LQ measures the quality of audio for listening purposes only. MOS-LQ does not take into account bi-directional effects such as delay and echo. MOS-CQ takes into account listening quality in both directions, as well as the bi-directional effects.	Disable (0) (default) or Enable (1) By default, MOS_CQ is used to calculate MOS.
Server IP	The IP address of the EMS server.	For the parameter to take effect, the device must be reset.
Port	TCP port of the EMS server to which to send metrics. Default = 500.	Range=0-65534 Default=5000
Interface Name	The IP network interface on which the quality experience reports are sent. The default is "DEFAULT".	String of up to 64 characters. For the parameter to take effect, the device must be reset.

➢ **To provision an AudioCodes device to use EMS Server NTP server as Device NTP server:**

1. In the Navigation pane, choose **System** ▶ **Device Info** ▶ **System Settings Frame**. The following screen is displayed:

Figure 31-2: System Settings Provisioning



2. Configure 'NTP Primary Server IP Address' to be EMS Server IP.

31.2 Voice Quality Metrics Provisioning

The device calculates a score for call quality (the 'color'), based on the device's default values or on provisioned voice quality rules.

In most cases, you can use the device's voice quality metrics default values. However, voice quality provisioning may be used under the following circumstances:

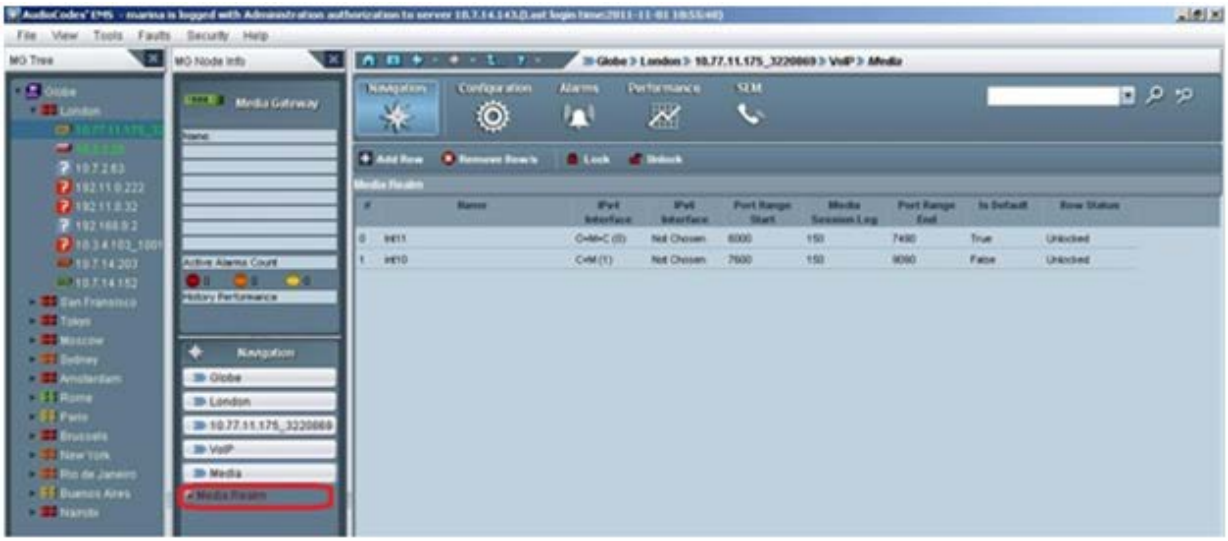
- When you know the specific sensitivity level in one or more Media Realms
- When you wish to base voice quality measurement on a specific parameter (MOS, Packet Loss, Jitter or Delay).

When voice quality provisioning is used, voice quality rules are defined for each device's Media Realm. In SIP gateways, a different Media Realm is usually defined for each direction and the voice quality rules are also different. For example, when a Media Realm is defined for a high-quality VoIP network, it's advantageous to utilize high-quality sensitivity settings. Conversely, it's recommended to utilize a low-quality sensitivity level for a Media Realm in an inferior-quality VoIP network.

➢ To provision Voice Quality rules:

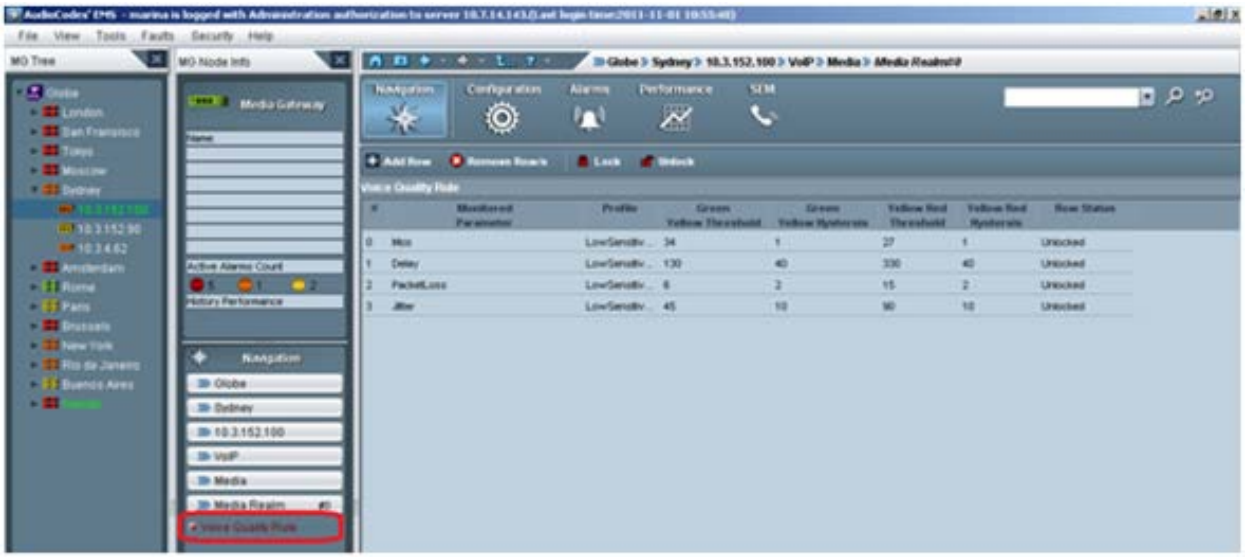
1. In the Navigation pane, select **VoIP** ▸ **Media** ▸ **Media Realm**. The Media Realm table is displayed.

Figure 31-3: Media Realm Table



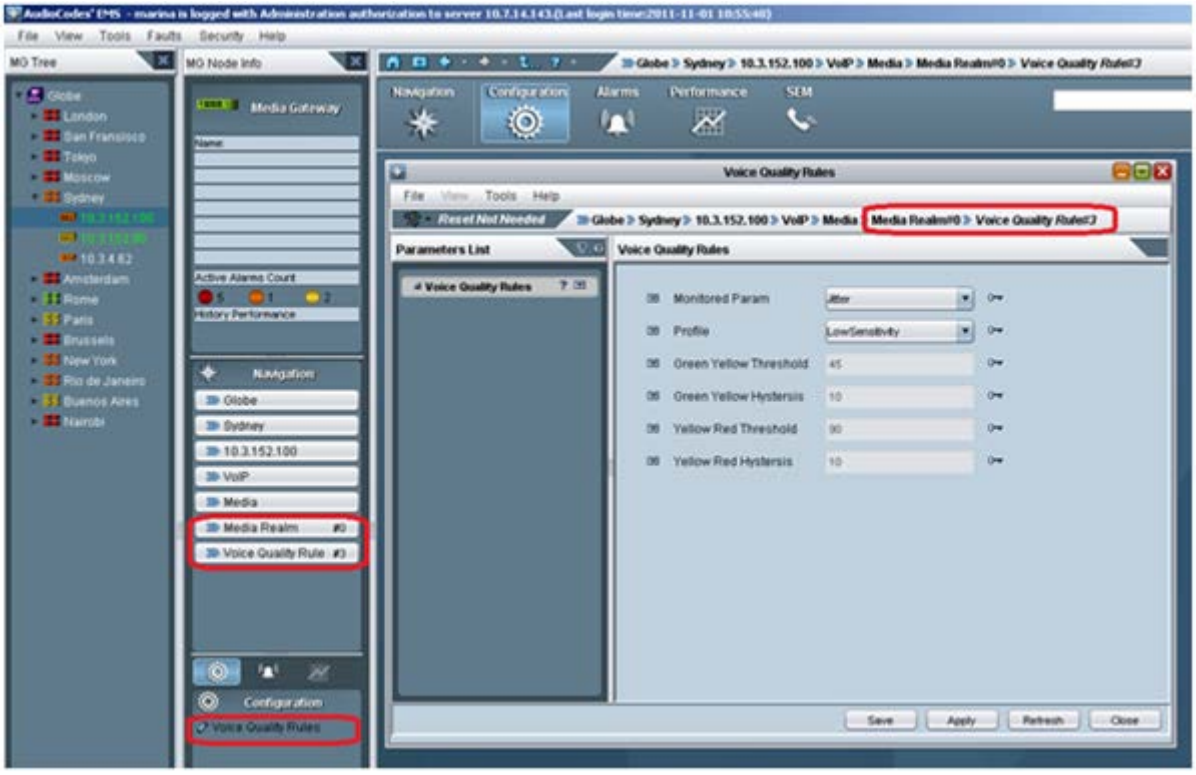
2. In the Media Realm table, select an entry and then in the Navigation pane, select **Voice Quality Rule**. The Voice Quality Rule table is displayed.

Figure 31-4: Voice Quality Rule Table



3. In the Voice Quality Rule table, click  to add an entry and then in the Configuration pane, select **Voice Quality Rules**. The Voice Quality Rules provisioning screen is displayed.

Figure 31-5: Voice Quality Rules Provisioning



4. From the 'Monitored Parameters' drop-down list, select a Monitored parameter upon which to define Voice Quality Rules.
5. From the 'Profile' drop-down list, select the desired Sensitivity Level; the Threshold and Hysteresis values are updated accordingly (see the table below for appropriate values for each parameter sensitivity level).

   Note that if you choose 'No Profile', each parameter field can be manually updated.

   The table below shows the monitored parameters MOS, Delay, Packet Loss and Jitter, each associated with each of the 3 sensitivity-level profiles: Low, Default and High. Each parameter's Green-Yellow Threshold and Yellow-Red Threshold differ in association with the configured Profile.

   Hysteresis is the amount of fluctuation from a Threshold. A report is sent only after the Hysteresis is exceeded. Hysteresis is used to avoid false reports being sent.

   For each monitored parameter, administrators can use Threshold and Hysteresis in the predefined Profile, or define their own Threshold and Hysteresis.

Table 31-2: Voice Quality Profile Parameters

Parameter(units)	Sensitivity Level	Green-Yellow Threshold (Green / Yellow)	Yellow-Red Threshold (Yellow / Red)	Hysteresis
MOS (value/10)	Low	34	27	10
	Default	35	28	
	High	36	29	
Delay (msec)	Low	130	330	40
	Default	120	300	
	High	110	270	
Packet Loss (%)	Low	6	15	2
	Default	5	13	
	High	4	11	
Jitter (msec)	Low	45	90	10
	Default	40	80	
	High	35	70	

6. Click **Apply** to save the changes.

32 Starting the SEM Tool

After installing EMS version 6.4 or later (see the *EMS Server IOM Manual*), click the **SEM** button on the Desktop toolbar of the EMS main screen. The tool opens in your browser (Internet Explorer) in the Network page, map view (default)..

By default, all VoIP devices managed in the network are displayed. By default, data on calls made in the Time Range of the past 24 hours are displayed.

To familiarize yourself with the various areas of the GUI, see the figure below and the subsequent table for terms used in this document to describe them.

Figure 32-1: SEM GUI Areas

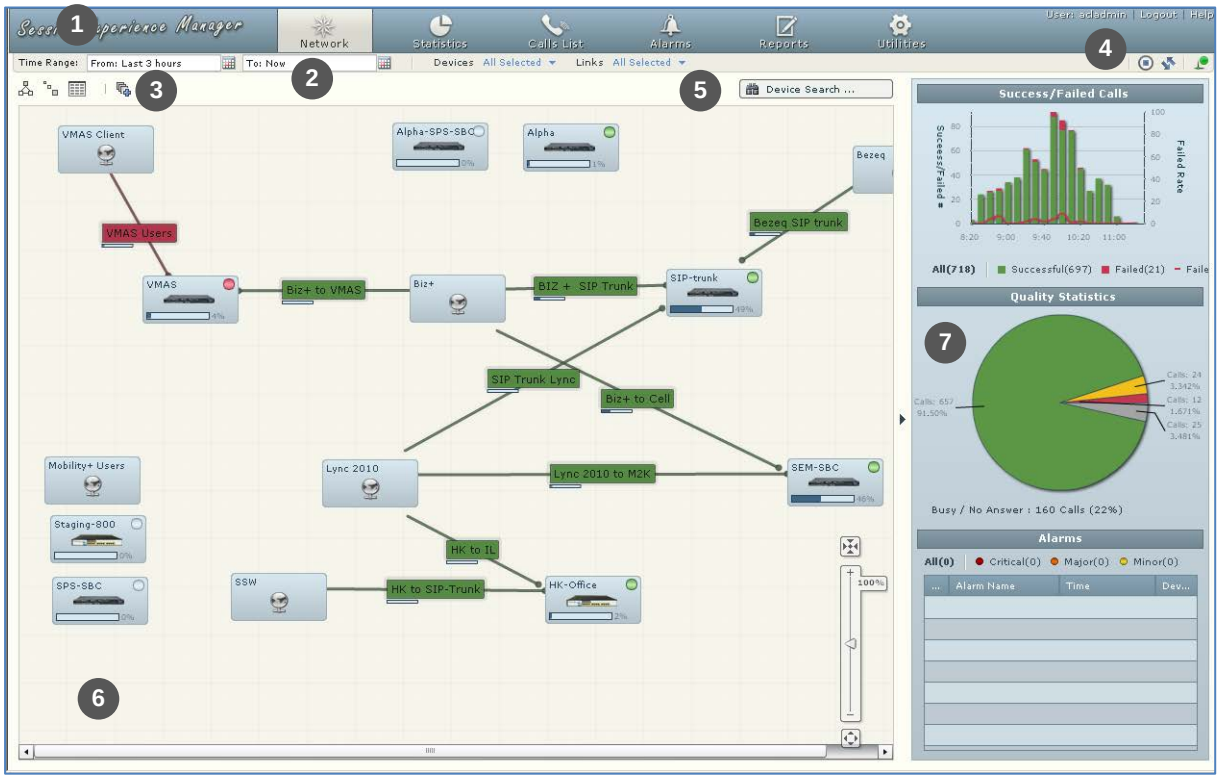
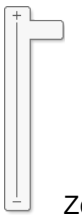


Table 32-1: SEM GUI Areas

Area	Description
1 Toolbar (from left to right)	Icons on the toolbar enable navigating between different SEM pages: Network (default) Statistics, Calls List, Alarms, Reports and Utilities
	Username (read-only); Logout (click to log out of the SEM); Help (link to the pending online help)
2 Filters (from left to right)	Time Range, Devices, Links
3 Actions Bar (from left to right)	▪ Map view / Regions view / Table view ▪ Add Non ACL Device
4 Refresh Page Functionalities (left to right)	[Start/Stop Auto Refresh] Switches on/off automatic refresh of SEM pages.
	[Refresh Now] Refreshes this SEM page.
	Connected or Disconnected (read-only).
5 Search	Searches for a specific device in the Network view and for random text strings in the Calls List and Alarms views.
6 Main Screen	Displays the main working area of the SEM tool for each of the SEM views. For example, in the Network view displayed above, the main screen displays all of the devices that are currently configured on the EMS server.
	 Zoom. Magnifies the main screen.
	Save devices locations. Saves devices' locations in Network Map view.
7 Summary Panes	Network and Statistics pages show three summary panes providing additional information to that provided in the main screen. Network view shows summarizes for Call Performance, Quality Statistics and Alarms. Statistics view shows summaries for Top Fail Reasons, Quality Statistics and Avg. Utilization.
	To hide the summary panes / expand the main screen, click

33 Filtering to Display Specific Info

Filters enable users to exclude unwanted information and display only required information in Network, Statistics, Calls List, Alarms and Reports pages:

Figure 33-1: Filter Bar

Table 33-1: Filters

Filter	Description
Time Range	Displays information only for a time range that is predefined or user defined.
Devices	Displays information only on devices specified.
Links	Displays information only on specified communication paths (links) between devices.

Filters eliminate irrelevant clutter from views, speeding access to required information. Information is filtered so that only data on specific devices / links during a specific time range is displayed.

Note: To filter a single device, select the device in the Devices filter and select 'None' in the Links filter.

After defining filters, they remain unchanged for all views until the next time you set them. Users can filter anew from any of these views at any time.

33.1 Filtering by Time Range

This section describes how to filter by time range.

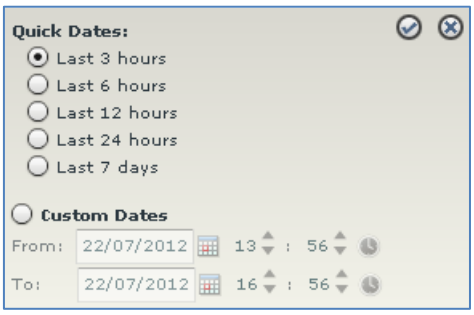
33.1.1 Predefined Quick Filters

Users can take advantage of predefined time ranges for convenient, quick filtering.

➢ **To filter by a predefined time range:**

1. On the Filter bar, click the 'From' or the 'To' field:

Figure 33-2: Time Range Filter – Quick Dates



2. Under 'Quick Dates', select a predefined time range option and click ; the filtering process is performed and the Filter bar shows this:

Figure 33-3: Filter Bar Showing Quick Date

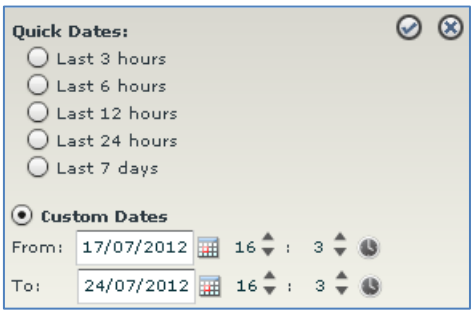
33.1.2 Custom Filters

This section describes how to custom filters.

➢ **To customize a time range filter:**

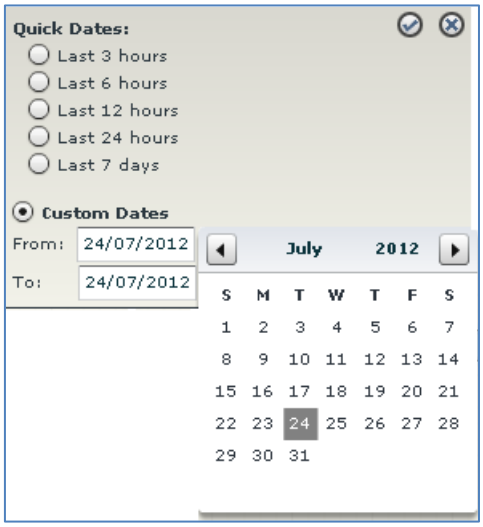
1. On the Filter bar, click the 'From' field or the 'To' field and select the **Custom Dates** option:

Figure 33-4: Time Range Filter - Custom



2. Under **Custom Dates**, define the **From** date and then **To** date using the calendar icon:

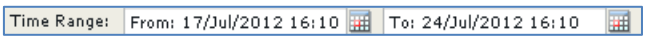
Figure 33-5: Time Range Filter – Custom Dates



3. Define the time of day/night, if you require, using ▲▼.

4. Click the icon to accept; the filtering process is performed and the Filter bar shows the following:

Figure 33-6: Filter Bar - From Date-To Date



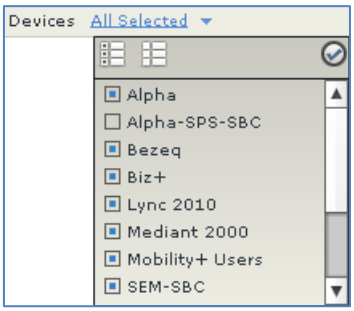
33.2 Filtering by Device

You can filter from a list of devices that are currently connected to the EMS server.

➢ To filter by device:

1. On the Filter bar, click the 'Devices' drop-down list.

Figure 33-7: Devices Filter



2. Do one of the following:
   - Click the **Select All** icon to automatically select all devices (save the time of manual selection) -OR-
   - Click the **Select None** icon to clear all selections (save the time of manually clearing) -OR-
   - Individually select each device for the SEM to display

   After selecting, click  ; only devices you selected are displayed in blue; unselected devices are displayed in light gray.

33.3 Filtering by Links

You can also filter by links. Links are IP communication paths between devices that measure and display key metrics on calls made on them. Links are defined according to IP Group, Trunk Group, Phone Number or SIP IP address.

The 'source' device on which key metrics monitoring is based must be an AudioCodes device. The second device can be an AudioCodes device or a non-AudioCodes device defined by users. Users can define one or more links between devices. The links are displayed in Network Map view. Each device and link status is displayed as 'Red' or 'Green'. If red, then:

- Failed Calls threshold is reached (default = 10%)

  -OR-

- Poor Calls Quality threshold is reached (default = 5%)

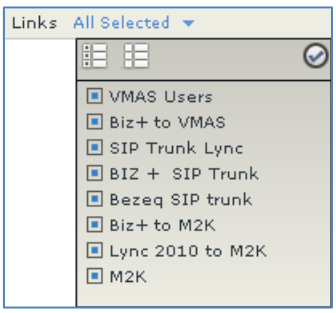
Users can define third-party non-AudioCodes devices in Network Map view. The SEM doesn't directly monitor them but enables users to view all relevant devices in the VoIP network and to monitor links with AudioCodes devices.

Most commonly used non-AudioCodes devices are Microsoft Lync Server 2010, IP PBX, ITSP and routers. The SEM can calculate, for example, call quality for the link defined between AudioCodes devices and Microsoft Lync Server 2010 devices. Non-AudioCodes devices are defined by name and IP address.

➢ To filter by links:

1. On the Filter bar, click the 'Links' drop-down list; the links are displayed.

Figure 33-8: Links Filter



2. Either:
   - Click **Select All** to automatically select all links and save the time of manually selecting -OR-
   - Click **Select None** to clear all selections and save the time of manually deselecting -OR-
   - Individually select each link for the SEM to display.

   After selecting, click **OK**; only links you selected are displayed (in blue); unselected devices are displayed in light gray.

34 Displaying VoIP Network Entities

The SEM opens by default in the Network page where you can navigate to the following options (selectable from the actions bar):

- Map view (default)
  Displays a map of all devices and links currently monitored by the SEM.
- Regions view
  Displays devices distributed *per region*, as defined in the EMS.
- Table view
  Displays each device's or link's records *in a table*, where each record includes call quality metrics.

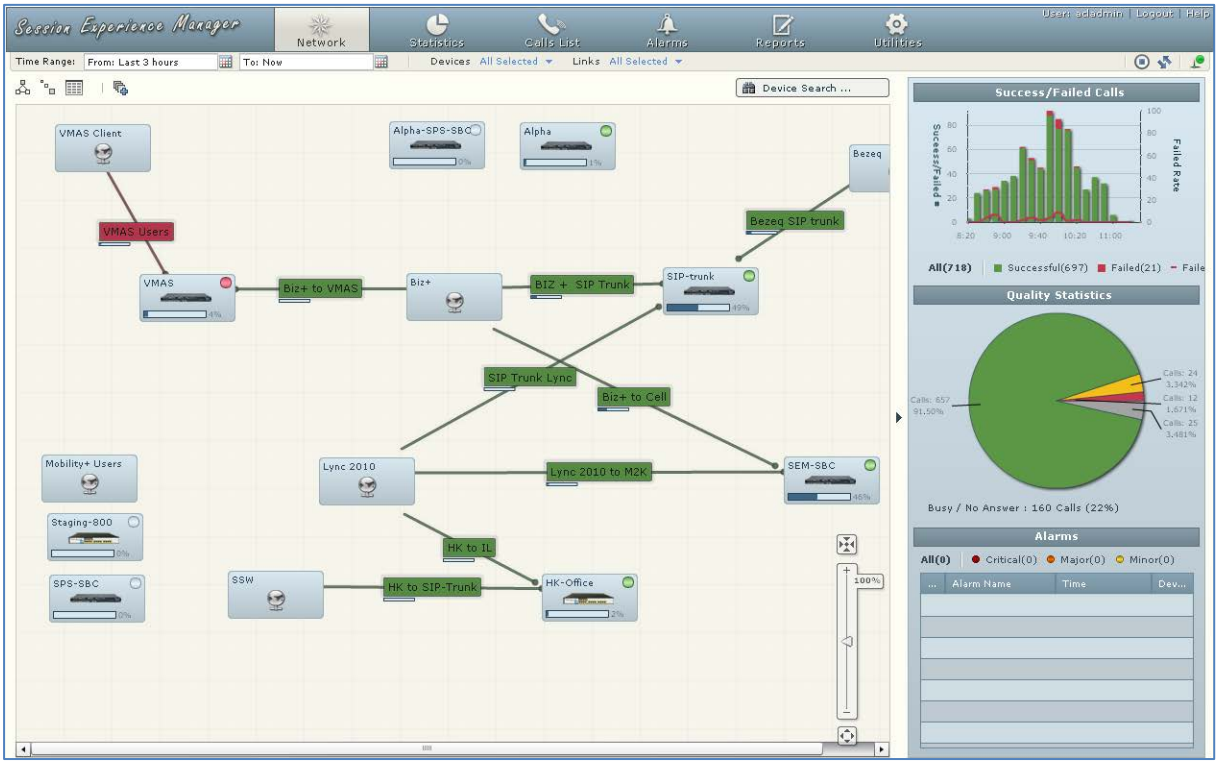
Note:

- AudioCodes devices must be defined in the EMS for them to be displayed in the SEM. Not all are displayed as the SEM only displays and monitors a supported subset.
- Non-ACL devices must be defined in the SEM (not in the EMS) for them to be displayed in the SEM, because of links provisioning which applies only to the SEM (see below).

34.1 Map View

On the Actions bar, click the **Map** icon ; VoIP network entities and their links are graphically displayed as icons.

Figure 34-1: Map View



About Map view:

- Selected entities are displayed light blue; filtered-out entities are displayed in gray.
- If an entity shows it indicates that the percentage of failed calls > 30% *or* that the percentage of poor quality calls > 15%.
  If an entity shows it indicates that the percentage of failed calls < 30% *and* that the percentage of poor quality calls < 15%.
- Entities can be positioned or repositioned in the map. After dragging an entity and dropping it in a different location, click **Topology changed! Save devices locations** at the top of the zoom bar. Entity locations are saved per EMS application and not per client. The last saved location determines devices' locations in the map for all users.
- Three summary panes (to the right) enable quick assessment of (1) successful/failed calls rates (2) quality statistics and (3) alarms.

34.1.1 Viewing Device / Link Information

In Map view, click a device or a link and then click the now-displayed ; the Device/Link Info popup opens:

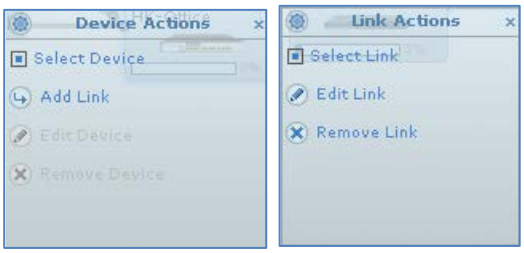
Figure 34-2: Device Info / Link Info

See Section 30.2 on page 319 for quality metrics descriptions.

34.1.2 Performing Device / Link Actions

In Map view, click a device / link and then click the now-displayed ; the Device/Link Actions popup opens:

Figure 34-3: Device Actions / Link Actions



[Device Actions] Select the device, add a link, edit the device or remove it.

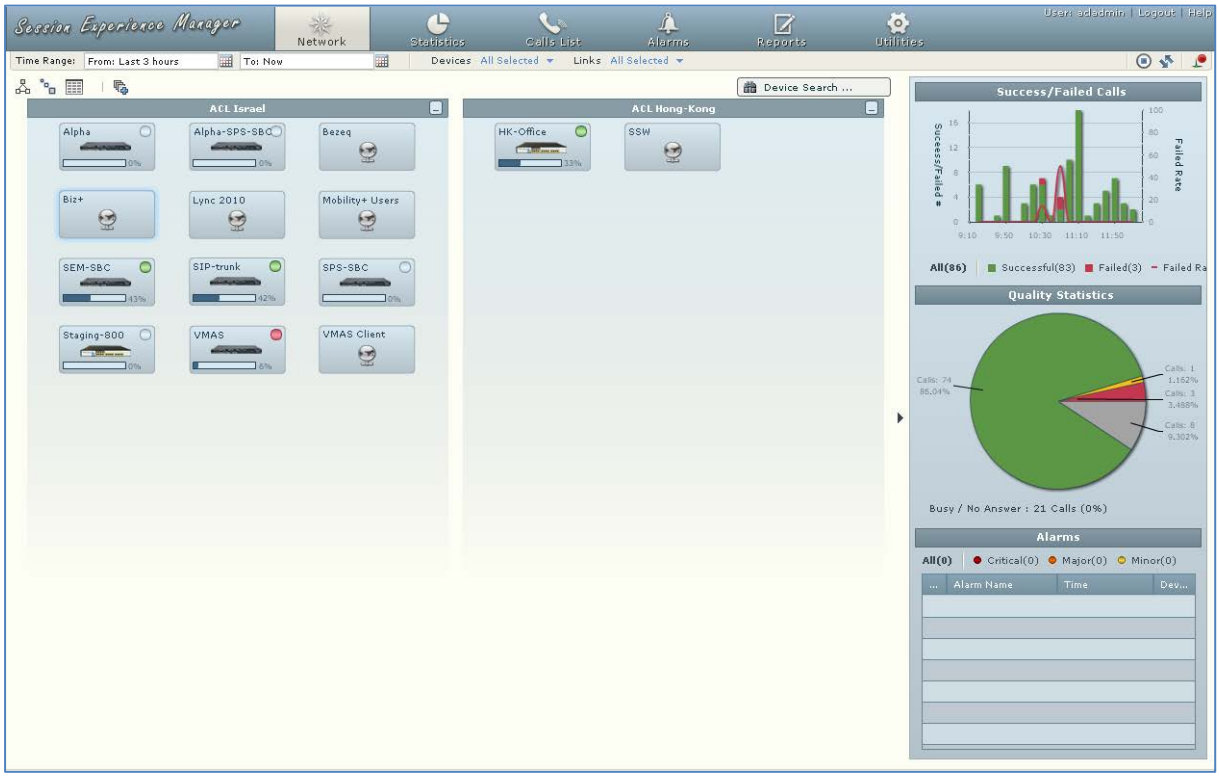
[Link Actions] Select the link, edit it or remove it.

34.2 Regions View

On the Actions bar, click the **Regions View** icon ; entities are sorted and displayed according to region, thereby facilitating user access to specific information and as a result enhancing management efficiency.

Note: Regions are displayed according to the user defined settings in the Regions Info tab in the User's List in the EMS GUI.

Figure 34-4: Regions View

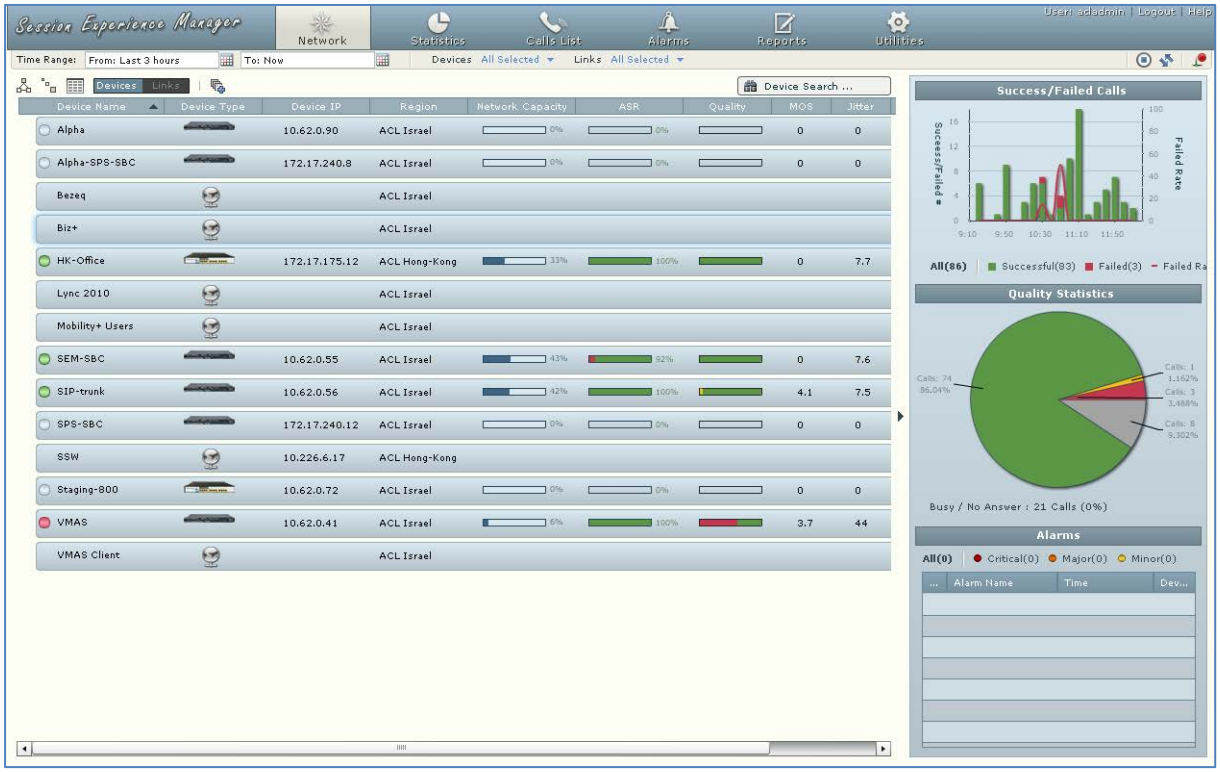


34.3 Table View

On the Actions bar, click the **Table** icon ; devices are displayed by default (see the figure below). Columns in the table show each device's network capacity, ASR (average success rate), quality statistics and voice metrics, facilitating users' access to specific information and consequently enhancing management efficiency.

To display links in the table, click Devices Links Links. Columns in the links table show the # of calls on each link, MOS, Jitter, Delay and Packet Loss.

Figure 34-5: Table View



34.3.1 Sorting by Column

Table view features sorting by column, enabling administrators to quickly compare across devices/links for enhanced comparative analysis capability.

Tip: Before sorting columns, in the Refresh Page, stop Auto Refresh and Start it again after the sorting results have been displayed.

For example:

➢ **To sort columns according to Network Capacity:**

- Click the column header and click again if necessary until ▼ shows; entities that consumed the most network capacity are listed highest, and those the least are listed lowest.
- Click the header again; ▲ shows; entities that consumed most network capacity are now listed lowest, and those the least highest.

34.4 Adding a Non-ACL Device

Non-ACL devices can be viewed in the SEM if they're supported. To view a non-ACL device in the SEM you must first add it.

➢ **To add a non-ACL device to the SEM:**

1. Click the icon on the actions bar; this screen opens:

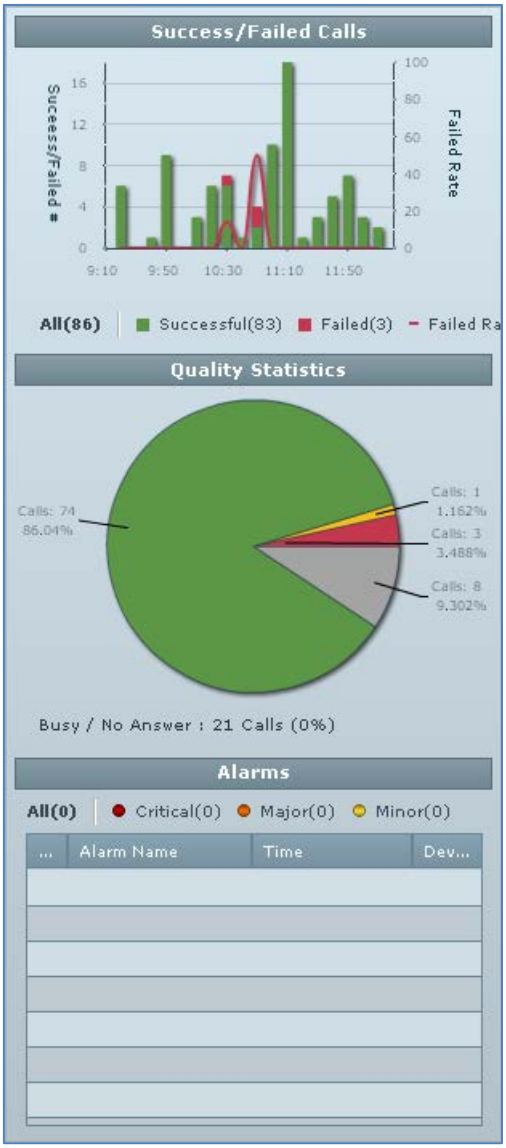
Figure 34-6: Adding a Non-ACL Device

2. Define the device's Name, IP address and Region and click **Apply**; the device is added and displayed in the SEM.

34.5 Summary Panes: Success/Failed Calls, Quality Statistics and Alarms

All views feature three summary panes, enabling at-a-glance assessment of the overall VoIP network operation.

Figure 34-7: Network Summary Panes



Network summary panes (top to bottom):

3. **Success/Failed Calls**: Chart enabling quick assessment of the distribution of the rate of successful / failed calls over time.
4. **Quality Statistics**: Color-coded pie chart enabling quick preview of the percentage and number of calls whose voice quality was measured as Good (green), Fair (yellow) or Failed (red). Enables quickly identifying the *ratio* of Good/Fair/Failed quality calls. Also indicates the number of calls in each quality category and each category's percentage out of the total number of calls made.
5. **Alarms**: Lists the names of the most recently active alarms, each alarm's Severity level (color-coded), the Time it was received, and the Name of the device triggering it. Sorting by column enhances information accessibility.

34.5.1 Successful/Failed Calls

The 'Successful/Failed Calls' chart displayed in the upper summary pane facilitates quick access to detailed information on calls performance. At a glance you can see the rate of successful calls versus the rate of failed calls distributed over time in 10 minute intervals, where each bar is an interval. The total number of successful and failed calls is indicated below the chart.

➢ To view information:

- Point your cursor over a green-coded bar segment; a popup shows the # of successful calls made in that 10-minute interval out of the total # of calls made, the % of successful calls made relative to the total # of calls made in the interval.
- Point your cursor over a red-coded bar segment; a popup shows the # of failed calls made in that 10-minute interval out of the total # of calls made, the % of failed calls made relative to the total # of calls made in the interval.
- Point your cursor over the red-coded line chart; a popup shows the rate of calls that failed during that interval (i.e., Failed Rate) and the end time of the interval.
- Click the **Successful (n)** link below the pie; the Calls List page opens showing information on *all* successful calls in the network (see Section 36 on page 353).
- Click the **Failed (n)** link below the pie; the Calls List page opens showing information on *all* failed calls in the network (see Section 36 on page 353).
- Click a green-coded bar segment; the Calls List page opens showing information on calls that failed in that 10-minute interval (see Section 36 on page 353).
- Click a red-coded bar segment; the Calls List page opens showing information on calls that failed in that specific 10-minute time interval (see Section 36 on page 353).

34.5.2 Quality Statistics

The 'Quality Statistics' pie displayed in the middle summary pane facilitates quick access to information related to calls quality. At a glance you can see the % and # of good quality calls that were made relative to the fair quality, poor quality and unknown quality calls.

➢ To view information:

Point your cursor over a *green* / *yellow* / *red* / *gray* pie segment; the % and # of calls whose quality was graded *good* / *fair* / *poor* / *unknown* pops up.

➢ To view detailed information:

Click a *green* / *yellow* / *red* / *gray* pie segment; the Calls List page opens showing detailed information on calls whose quality was graded *good* / *fair* / *poor* / *unknown* (see Section 36 on page 353).

34.5.3 Alarms

The 'Alarms' table pane displayed in the lowermost summary pane facilitates quick access to alarms-related information. At a glance you can see how many alarms are currently active (All) and how many there are of each Severity level (Critical, Major, Minor).

➢ To view detailed information:

Click the **All (n)** link; the Alarms page opens showing alarms of all Severity levels and detailed information on them (see Section 37 on page 373).

Click the **Critical (n)** / **Major (n)** / **Minor (n)** link; the Alarms page opens showing alarms of that specific Severity level and detailed information on them (see Section 37 on page 373).

35 Displaying Statistics

The Statistics page displays by default three charts (top to bottom):

- Successful / Failed Calls (see Section 35.1 on page 347 below)
- Calls Quality (Good, Fair, Poor or Unknown) (see Section 35.2 on page 348 below)
- Utilization Distribution (Rx/Tx Rate Kbit/sec) (see Section 35.3 on page 349 below)

Figure 35-1: Statistics

The page enables users to quickly and effectively compare statistics and identify correlations and patterns important for the diagnosis and optimization of VoIP network health status.

The **Compare** check boxes located below the uppermost chart make this possible:

Figure 35-2: Compare Options

Select the **Utilization** option and deselect the others; the Statistics page only displays the Successful / Failed Calls chart (always displayed) and the Utilization Distribution chart:

Figure 35-3: Comparing Successful/Failed Calls with Utilization Distribution

The Successful / Failed Calls chart is by default always displayed. You can opt to show / hide any of the others, i.e., Utilization, MOS, Packet Loss, Jitter, Delay and/or Echo, to quickly identify correlations.

35.1 Success/Failed Calls Chart

The Success/Failed Calls chart shows by default the distribution of successful / failed calls over time.

From the pane title's dropdown, two other measurements can be selected for display:

- Average Call Duration (ACD)
- Failed Rate

All three measurements are displayable as linear or bar chart, selectable from the dropdown.

Figure 35-4: Success/Failed Calls – Linear Chart

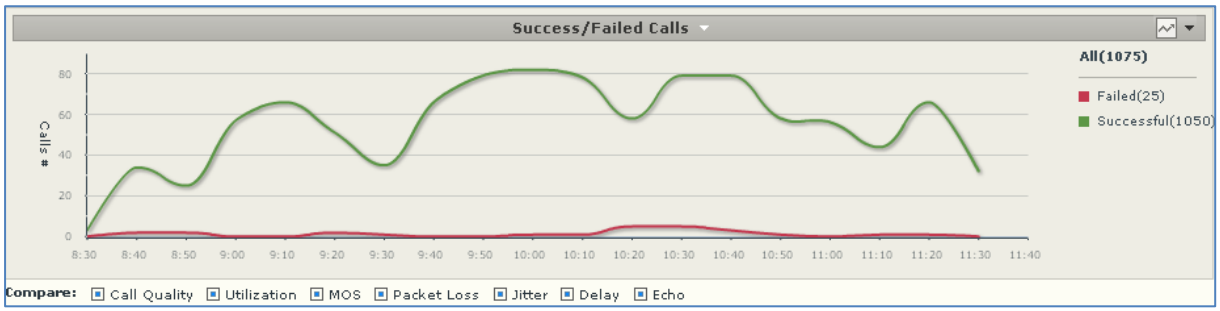
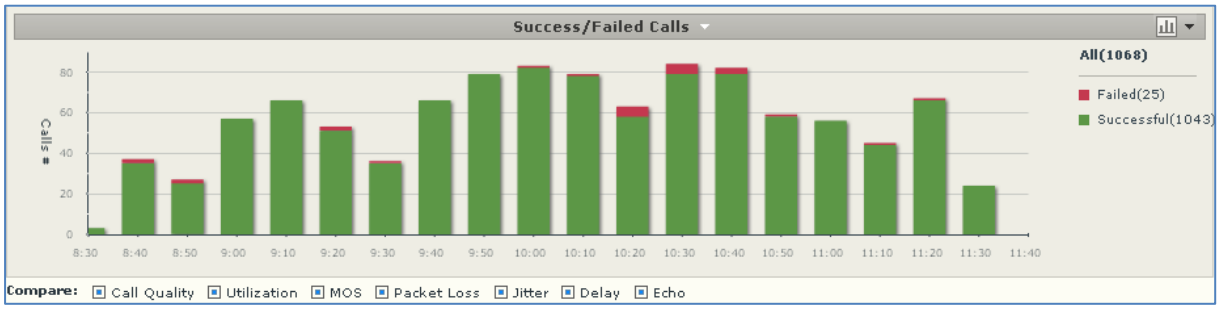


Figure 35-5: Successful/Failed Calls – Bar Chart



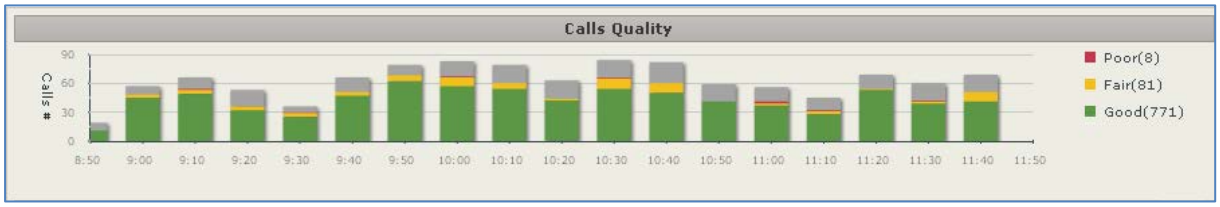
Users can display this chart for at-a-glance assessment of calls performance. The chart shows *when* successful calls peaked compared to *when* failed calls peaked. This can then quickly be compared with Calls Quality, Utilization Distribution, MOS, Packet Loss, Jitter, Delay or Echo charts, to identify correlation and make a diagnosis.

35.2 Calls Quality Chart

The Calls Quality bar chart shows the distribution of calls voice quality over time. A glance at the chart shows users when and in what measure calls voice quality scored 'Good' (green), 'Fair' (yellow) and 'Fail' (red). Gray indicates unknown voice quality.

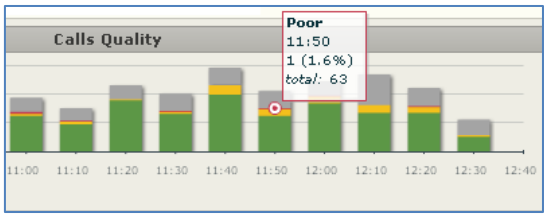
The Calls Quality chart is displayed as a bar chart.

Figure 35-6: Calls Quality Bar Chart



- Point the cursor over a color-coded bar segment in any time period; a popup (see below) shows the time the period ended, the number and percentage of calls made whose quality scored in the category represented by the color-coded bar segment, and the total number of calls made in the period.

Figure 35-7: Calls Quality Bar Chart - Popup



- To view detailed information on calls scoring 'Good', 'Fair' or 'Poor' in any time interval; click the relevant color-coded segment of the bar; the Calls List page opens (see Section 36 on page 353).
- To view information on *all* calls whose voice quality scored:
  - 'Poor' - click the **Poor (n)** link; the Calls List page opens
  - 'Fair' - click the **Fair (n)** link; the Calls List page opens
  - 'Good' - click the **Good (n)** link; the Calls List page opens (see Section 36 on page 353).

Compare Calls Quality to Utilization Distribution, MOS, Packet Loss, Jitter, Delay and/or Echo. Use the **Compare** check boxes located below the Success/Fail Calls chart to select a measurement for which to compare.

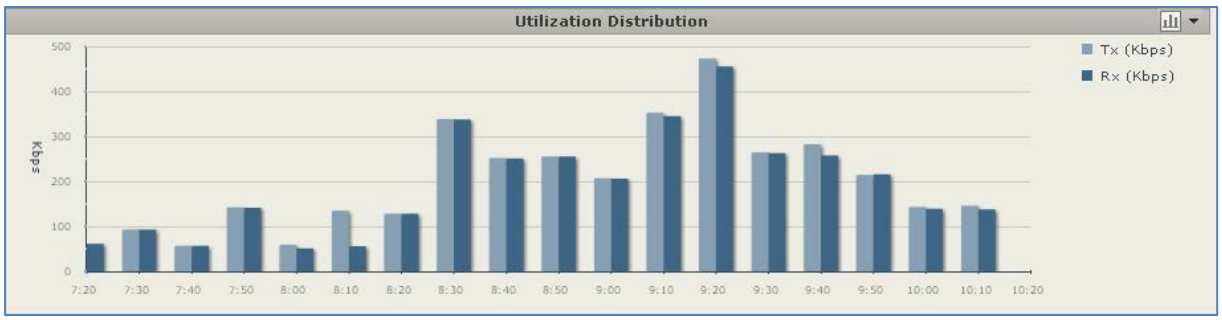
If for example, you identify a correlation over time between 'Failed' quality calls, and Jitter, then this metric is the reason for the quality failure.

35.3 Utilization Distribution Chart

The Utilization Distribution chart shows distribution of network utilization over time. A glance at the chart shows when a high rate (in Kbps) was received or transmitted. The chart thus indicates when a network is congested or uncongested, i.e., when voice quality scores may be lower.

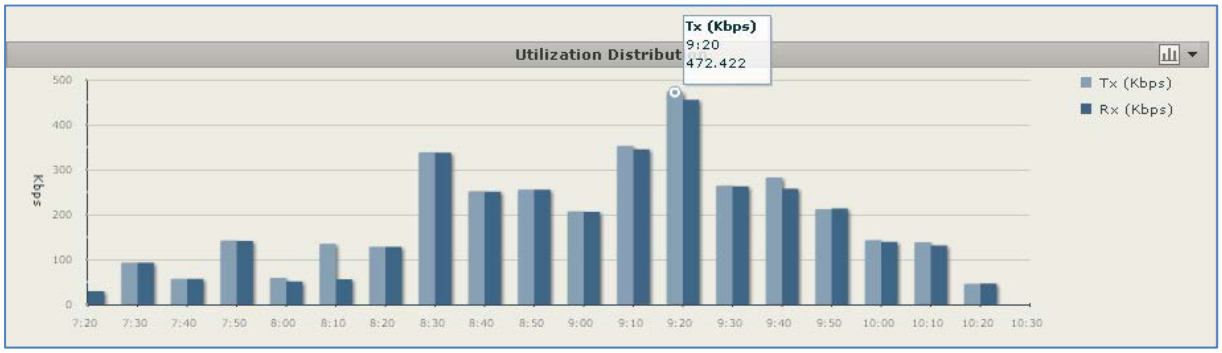
The chart is by default displayed as a bar chart; however, is also displayable as a linear chart, selectable from the dropdown.

Figure 35-8: Utilization Distribution Chart



To view information on a specific time period, position the cursor over the bar representing the time period; a popup (see below) pops up showing the time at which the period ended, the Rx / Tx rate in Kbps, and the kilobits consumed per second during the time period.

Figure 35-9: Utilization Distribution Chart – Popup

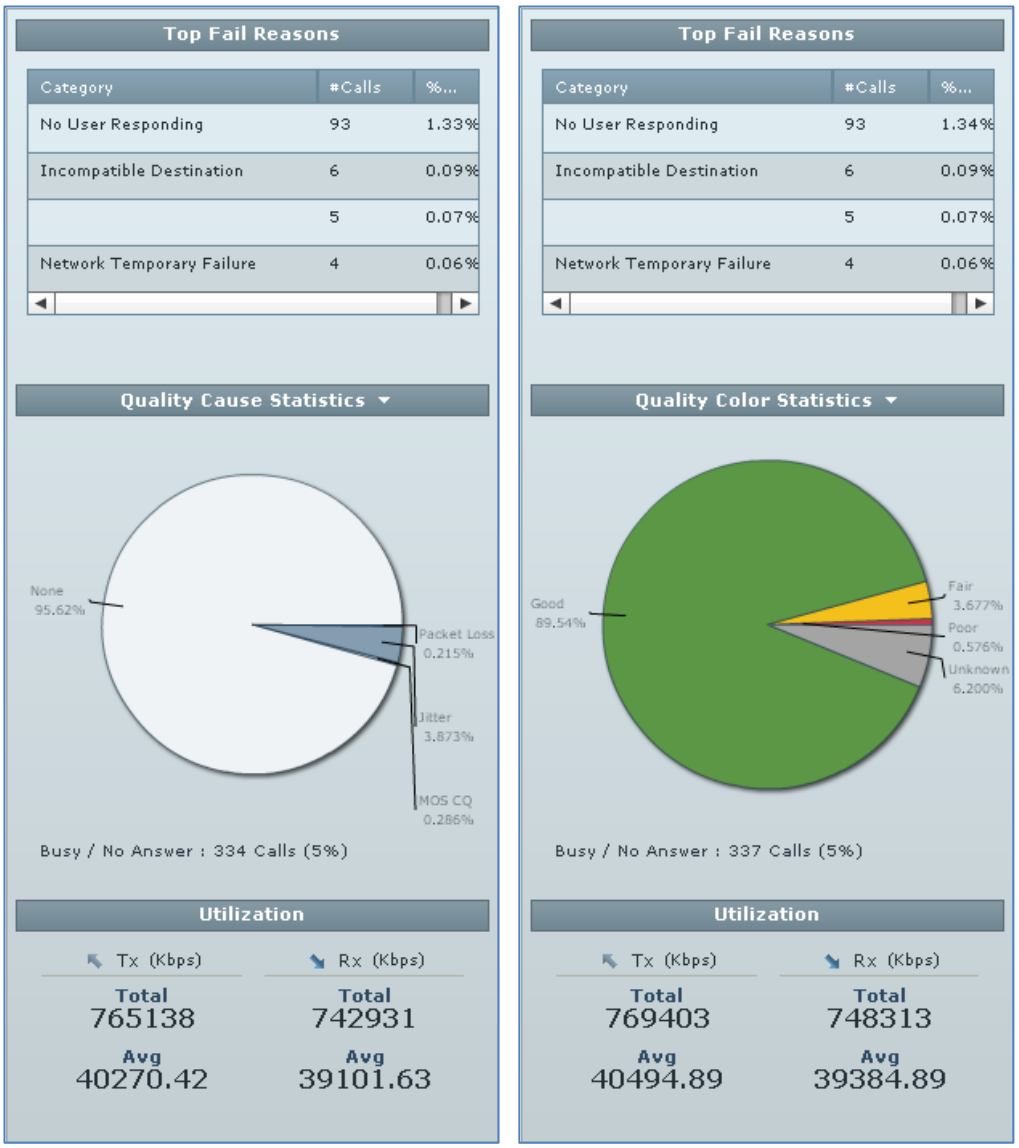


35.4 Summary Panes: Top Fail Reasons, Quality Cause Statistics and Utilization

The Statistics page displays three summary panes to the right of the charts:

- Top Fail Reasons (uppermost)
- Quality Cause Statistics (middle)
- Utilization (lowermost)

Figure 35-10: Statistics Summary Panes



35.4.1 Top Fail Reasons

The Top Fail Reasons pane (uppermost) shows in a table:

- The predominant causes of performance failures (e.g., Unassigned Number, Incompatible Destination, Temporary Network Failure, No User Responding)
- The # and % of calls that failed due to that cause

35.4.2 Quality Cause Statistics

The Quality Cause Statistics summary pane (middle) (default) enables quick identification of metrics affecting calls quality.

The pie chart shows the following:

- % of calls whose quality was unaffected (None) by the quality metrics
- % of calls whose quality was affected by each metric (Jitter, Delay, Echo)
- % and # of busy / unanswered calls

➢ To view detailed information:

- Point your cursor over a pie segment to view the # of calls affected by that metric and that metric's measurement as a % of the quality.
- Click the Jitter segment of the pie (for example); the Calls List page opens showing all calls on which Jitter was measured (see Section 36 on page 353). Similarly, you can view information on calls upon which Packet Loss, Delay and Jitter were measured.

35.4.3 Quality Color Statistics

From the drop-down list on the Quality Cause Statistics pane title bar, choose **Quality Color Statistics**; a color-coded pie chart shows the % of calls whose voice quality was measured as good (green), fair (yellow), poor (red), or unknown (gray).

➢ To view information:

- Point your cursor over a segment of the pie; a popup indicates % and # of calls classified in this voice quality category.

➢ To view detailed information:

- Click a segment in the pie; the Calls List page opens, enabling viewing of detailed information on calls in this quality category (see Section 36 on page 353).

35.4.4 Utilization

The Utilization summary pane (lowermost) shows:

- The overall **Total Tx** (transmission) rate (Kbps)
- The **average Tx** rate over time periods (Kbps)
- The overall **Total Rx** (reception) rate (Kbps)
- The **average Rx** rate (Kbps)

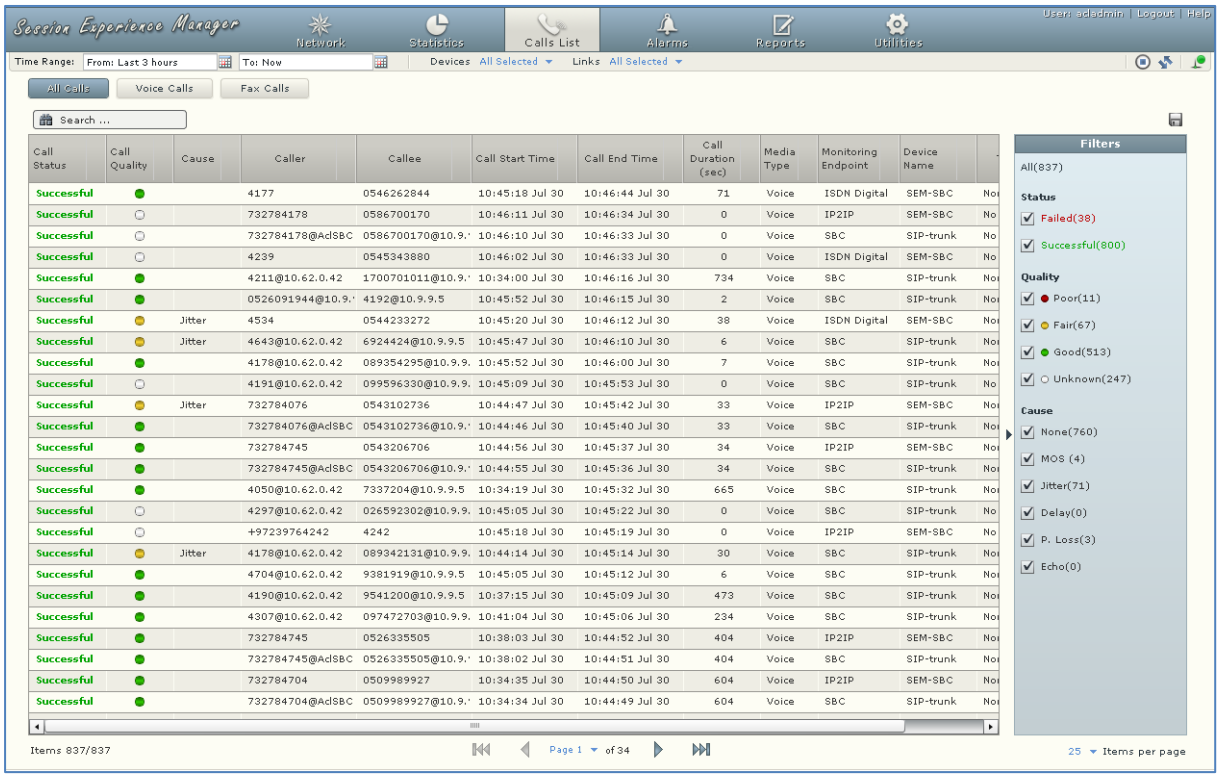
The pane facilitates the quick assessment of overall utilization distribution.

This page is intentionally left blank

36 Displaying the Calls List

The Calls List page lists and shows details on all calls made in the network. The page features advanced filtering capabilities to facilitate obtaining precise information on calls quickly and efficiently. The list can be filtered by Time Range (see 'Filtering by Time Range' on page 326) and / or Devices (see 'Filtering by Device' on page 326) and / or Links (see 'Filtering by Links' on page 333).

Figure 36-1: Calls List



Administrators can click the **Save As** icon to download the information (numbers and text) in a coma-separated *calls.csv* file format that can later be easily opened and read in any text editor, as well as sent as an attachment in an email to others.

Go to a page using the pager:

Figure 36-2: Pager

- Select the number of calls to display per page from the 'Items per page' drop-down list: 10, 25, 30, 40, 50, 100 or 1000.
- Click the Page 1 link; a popup menu listing page numbers and a ▼ scroll enables direct access to a specific page.
- Page forwards or backwards, one page at a time.

- Use the **Go to last page** or **Go to first page** icons, in combination with the previous paging capability.

36.1 Filtering to Display Required Information Only

Flexible, intuitive filtering options on the Calls List page enable users to exclude irrelevant information and display only required information. Filtering is an essential feature in the management of call sessions, thereby facilitating enhanced call session experiences.

36.1.1 Preliminary Filtering

The page opens by default with 

selected.

Perform preliminary filtering selecting 

or 

. Optionally filter further using any of the methods explained below, or combine filtering methods. The Voice Calls and Fax Calls filtered pages provide extensive additional columns and information relative to the default All Calls page (see

Table 36-1).

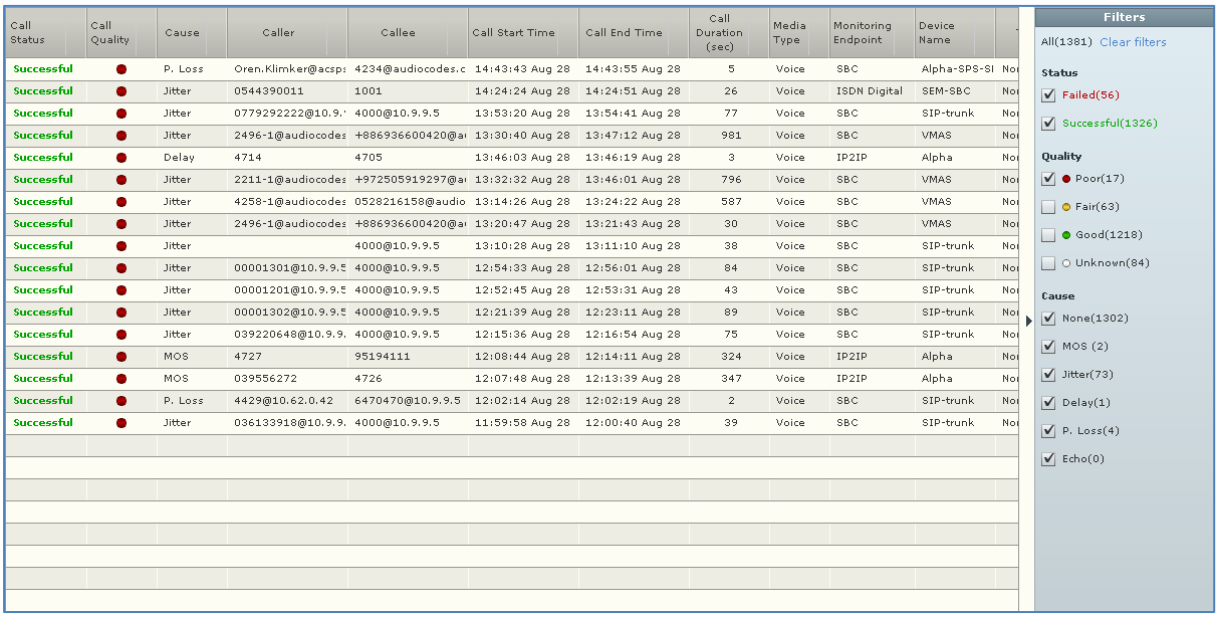
36.1.2 Using the Filters Pane

Three critically significant filters are located in the Filters pane on the Calls List page (see the figure below): (1) Status - Failed or Successful (2) Quality - Poor, Fair, Good or Unknown and (3) Cause - None, MOS, Jitter, Delay, P. Loss or Echo. Below is an intuitive example of how to filter.

Figure 36-3: Filters Pane

The figure above shows how to filter calls for 'Poor' quality only. The result is displayed in the screen below:

Figure 36-4: Poor Quality Calls Only

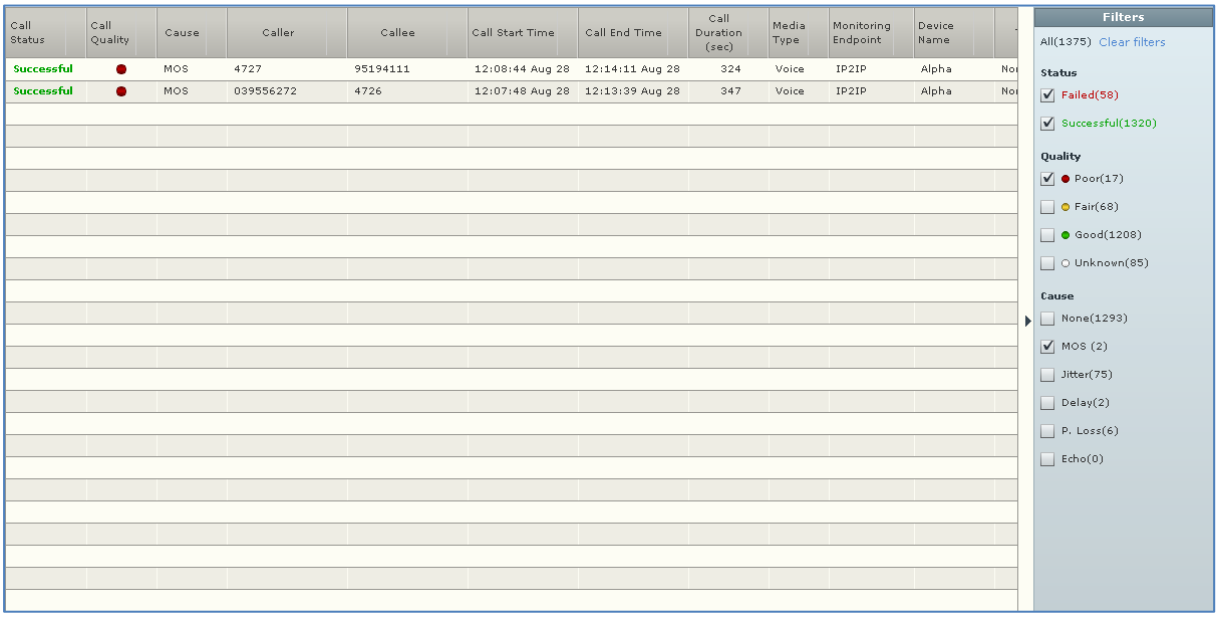


Call Status	Call Quality	Cause	Caller	Callee	Call Start Time	Call End Time	Call Duration (sec)	Media Type	Monitoring Endpoint	Device Name
Successful	●	P. Loss	Oren.Klimker@acsp	4234@audiocodes.c	14:43:43 Aug 28	14:43:55 Aug 28	5	Voice	SBC	Alpha-SPS-SI
Successful	●	Jitter	0544390011	1001	14:24:24 Aug 28	14:24:51 Aug 28	26	Voice	ISDN Digital	SEM-SBC
Successful	●	Jitter	0779292222@10.9.	4000@10.9.9.5	13:53:20 Aug 28	13:54:41 Aug 28	77	Voice	SBC	SIP-trunk
Successful	●	Jitter	2496-1@audiocodes	+8869366004 20@a	13:30:40 Aug 28	13:47:12 Aug 28	981	Voice	SBC	VMAS
Successful	●	Delay	4714	4705	13:46:03 Aug 28	13:46:19 Aug 28	3	Voice	IP2IP	Alpha
Successful	●	Jitter	2211-1@audiocodes	+972505919297@a	13:32:32 Aug 28	13:46:01 Aug 28	796	Voice	SBC	VMAS
Successful	●	Jitter	4258-1@audiocodes	0528216158@audio	13:14:26 Aug 28	13:24:22 Aug 28	587	Voice	SBC	VMAS
Successful	●	Jitter	2496-1@audiocodes	+8869366004 20@a	13:20:47 Aug 28	13:21:43 Aug 28	30	Voice	SBC	VMAS
Successful	●	Jitter		4000@10.9.9.5	13:10:28 Aug 28	13:11:10 Aug 28	38	Voice	SBC	SIP-trunk
Successful	●	Jitter	00001301@10.9.9.5	4000@10.9.9.5	12:54:33 Aug 28	12:56:01 Aug 28	84	Voice	SBC	SIP-trunk
Successful	●	Jitter	00001201@10.9.9.5	4000@10.9.9.5	12:52:45 Aug 28	12:53:31 Aug 28	43	Voice	SBC	SIP-trunk
Successful	●	Jitter	00001302@10.9.9.5	4000@10.9.9.5	12:21:39 Aug 28	12:23:11 Aug 28	89	Voice	SBC	SIP-trunk
Successful	●	Jitter	039220648@10.9.9.	4000@10.9.9.5	12:15:36 Aug 28	12:16:54 Aug 28	75	Voice	SBC	SIP-trunk
Successful	●	MOS	4727	95194111	12:08:44 Aug 28	12:14:11 Aug 28	324	Voice	IP2IP	Alpha
Successful	●	MOS	039556272	4726	12:07:48 Aug 28	12:13:39 Aug 28	347	Voice	IP2IP	Alpha
Successful	●	P. Loss	4429@10.62.0.42	6470470@10.9.9.5	12:02:14 Aug 28	12:02:19 Aug 28	2	Voice	SBC	SIP-trunk
Successful	●	Jitter	036133918@10.9.9.	4000@10.9.9.5	11:59:58 Aug 28	12:00:40 Aug 28	39	Voice	SBC	SIP-trunk

Filters
All(1381) Clear filters
Status
Failed(56)
Successful(1326)
Quality
Poor(17)
Fair(63)
Good(1218)
Unknown(84)
Cause
None(1302)
MOS (2)
Jitter(73)
Delay(1)
P. Loss(4)
Echo(0)

Calls of poor quality are exclusively displayed. As you can see, Packet Loss, Jitter, Delay and MOS are the causes. Now filter these poor quality calls for those whose poor quality was caused *only* by MOS, i.e., deselect every cause except MOS. Below is the result:

Figure 36-5: Poor Quality Calls Caused by MOS Only



Call Status	Call Quality	Cause	Caller	Callee	Call Start Time	Call End Time	Call Duration (sec)	Media Type	Monitoring Endpoint	Device Name
Successful	●	MOS	4727	95194111	12:08:44 Aug 28	12:14:11 Aug 28	324	Voice	IP2IP	Alpha
Successful	●	MOS	039556272	4726	12:07:48 Aug 28	12:13:39 Aug 28	347	Voice	IP2IP	Alpha

Filters
All(1375) Clear filters
Status
Failed(58)
Successful(1320)
Quality
Poor(17)
Fair(68)
Good(1208)
Unknown(85)
Cause
None(1293)
MOS (2)
Jitter(75)
Delay(2)
P. Loss(6)
Echo(0)

You now display only those calls on which you require information. For explanations of columns, see

Table 36-1 below. View an individual call's details by clicking its row; the Call Details page opens (see Section 36.2 on page 362).

36.1.3 Sorting Calls in the List

Tip: Before sorting calls in the list, in the Refresh Page, stop Auto Refresh and Start it again after the sorting results have been displayed.

Sort calls in the list by clicking a column header; calls are sorted in the order of that column. Click another column header's sort arrow; calls already sorted are now further sorted in the order of *this* column. Therefore, the Calls List enables you to set multiple sort keys to determine correlations between the information displayed in the different columns. This capability facilitates quick and easy access to those calls on which information is most required. Calls on which information is less critical is listed lower.

Below is an intuitive example of how to perform multiple columns sorting.

To sort the calls in the list:

1. Click the column header 'Call Status'; the sort arrow points down ▼ indicating that successful calls are displayed first, followed by failed calls. If you then click the sort arrow, it points up ▲ indicating that failed calls are displayed first followed by successful calls; indicated by **1** in the column header.
2. Position your cursor over another column and click its now-displayed sort arrow, for example, 'Call Quality'; calls are now sorted successful-failed *and* in order of quality (Good > Fair > Poor > Unknown), indicated by **2** in the column header.
3. Click a third column header's sort arrow, for example, 'Cause'; calls are now sorted (1) successful-failed (2) in order of quality *and* (3) in order of cause (Delay, Echo, Jitter, MOS, Packet Loss and None, in *alphabetic order*), indicated by **3** in the Cause column header.

   Calls have now been sorted in three separate columns each in the respective desired sort order. You can now visually draw correlations between the data displayed in each respective sorted column, whilst at the same time, the integrity of each record is maintained.

Note: To reset column sort ordering, click any column header; a new column sort order begins..

Table 36-1: Calls List Columns

Column	Description	
All Calls		
Call Status	**Successful** or **Failed**	
Call Quality	= Good = Fair = Poor = Unknown	
Cause	Delay (msec)	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter (msec)	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss (%)	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side.
	None	Indeterminate cause
Caller	The phone number or address of the person who initiated the call.	
Callee	The phone number or address of the person who answered the call.	
Call Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was started.	
Call End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Call Duration (sec)	The duration of the call, in seconds.	
Media Type	Voice or Fax.	
Monitoring Endpoint	SBC (session board controller), ISDN Digital, or IP2IP.	
Device Name	The IP address of the device on which the call was made.	

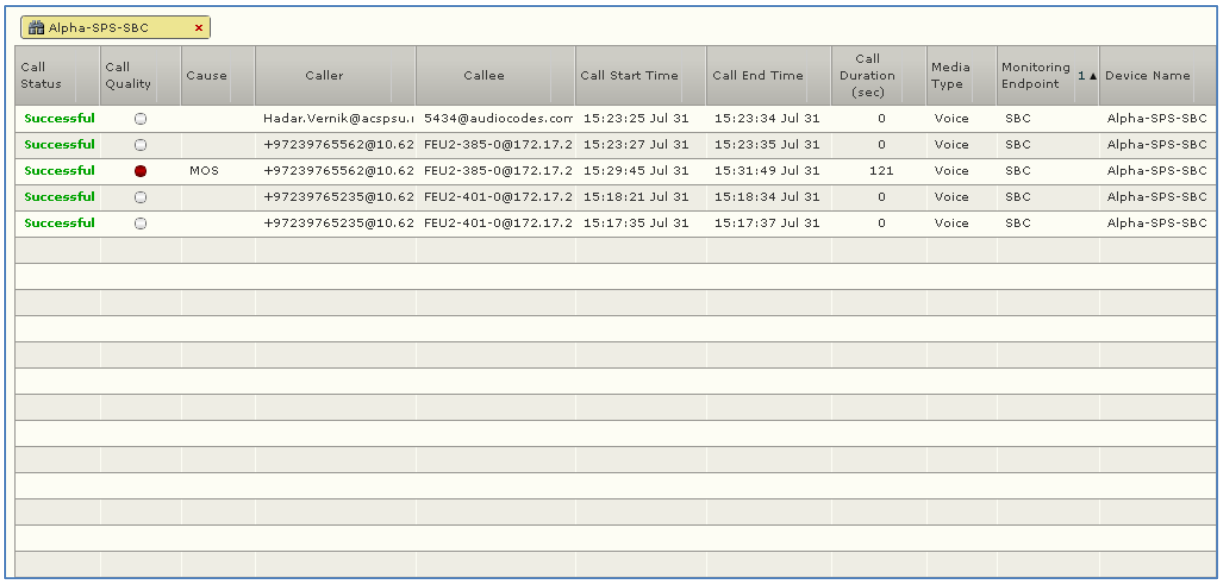
Column	Description
Termination Reason	The reason why the call was terminated, e.g., No Answer.
Voice Calls	
Cause Leg	The leg that caused the call to be graded a poor quality score (red) or a fair quality score (yellow).
Cause Leg [Red] %	The percentage of time that the problematic leg was graded poor quality (red) relative to the total duration of the call.
Cause Leg [Yellow] %	The percentage of time that the problematic leg was graded fair quality (yellow) relative to the total duration of the call.
MOS	Measured on two legs (four segments) of the call: (1) Caller leg, on the caller side and the device side of the network (2) Callee leg, on the callee side and the device side of the network.
Jitter	Measured on two legs (four segments) of the call: (1) Caller leg, on the caller side and the device side of the network (2) Callee leg, on the callee side and the device side of the network.
Packet Loss (%)	Measured on two legs (four segments) of the call: (1) Caller leg, on the caller side and the device side of the network (2) Callee leg, on the callee side and the device side of the network.
Delay (msec)	Measured on two legs (four segments) of the call: (1) Caller leg, on the caller side and the device side of the network (2) Callee leg, on the callee side and the device side of the network.
Echo	Measured on two legs (four segments) of the call: (1) Caller leg, on the caller side and the device side of the network (2) Callee leg, on the callee side and the device side of the network.
Fax Calls	
Fax Quality (FOM)	Indicates the score measured for quality for transmission, according to the ITU E.450 Figure Of Merit (FOM) standard.
Number of Pages	Indicates the number of pages transmitted.
Pages at MAX Rate	Indicates the number of pages transmitted at the maximum rate.

36.1.4 Filtering Using the 'Search' Field

Use the 'Search' field as a quick alternative to other filtering methods, or use it combined with other methods as a supplement.

The 'Search' option is a single filter; it cannot filter calls already filtered by a previous filter, or order calls already ordered, as the other methods can do. But you can perform an initial quick filter and then use another method to narrow the results. Enter a device name, e.g., Alpha-SPS-SBC, in the 'Search' field (see the figure below); only calls made and answered on this device are listed.

Figure 36-6: Results after Searching for a Device Name



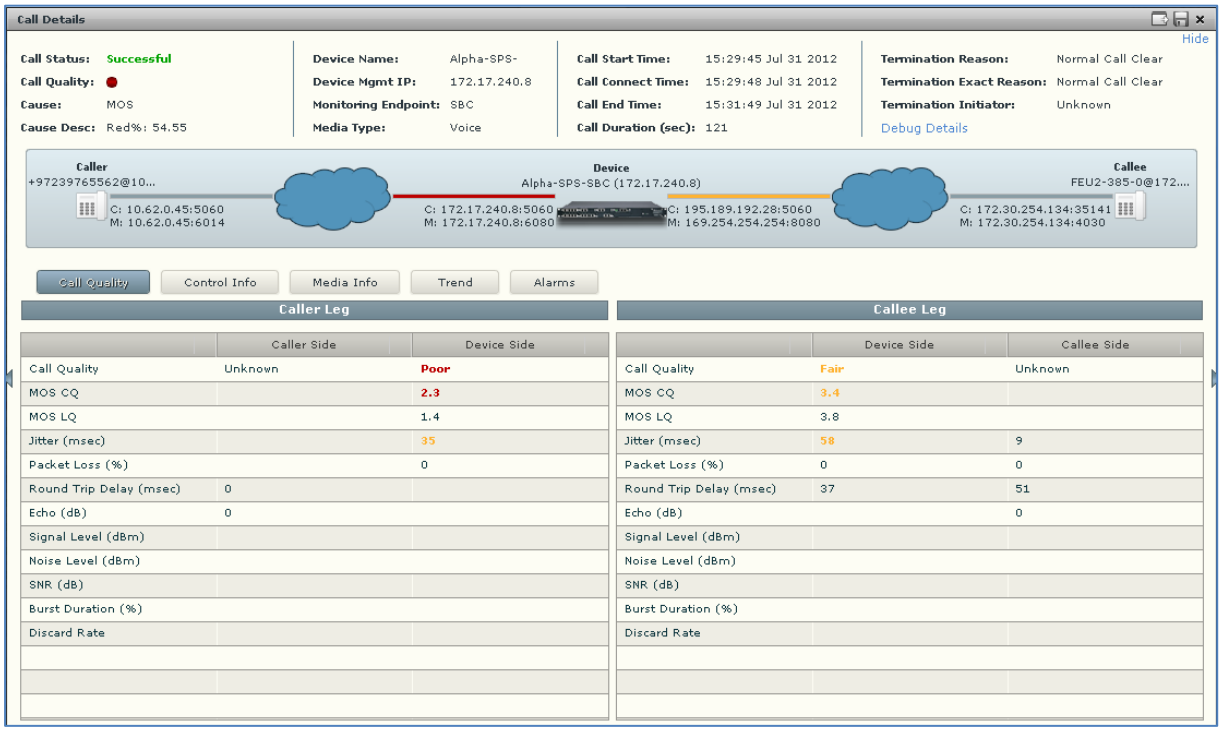
After the search results are displayed, click the ‘x’ to undo the filter or narrow the search further using another filter method.

Access a call's details by clicking its row; the Call Details page opens (see Section 36.2 below).

36.2 Displaying the Details of a Call

View details on any call listed in the Calls List by clicking its row. The Call Details page gives you detailed diagnostic information on every detail of the call, in graphic and textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

Figure 36-7: Call Details



The table below describes the page's subdivisions.

Table 36-2: Call Details Page Subdivisions

Page Subdivision	Description
(Uppermost) Call summary	Displays parameters and values identical to those displayed in the Calls List rows. See Section 36 on page 353.
(Middle) Graphic illustration	Displays a graphical illustration of voice quality on each leg of the call, on both the caller and callee side. Each leg is: ▪ Connected via the VoIP cloud to the device ▪ Color-coded to indicate quality (green = good, yellow = fair, red = poor, grey = unknown) ▪ Tagged by **C** and **M** C = Control summary (point the cursor to view as tooltip) M = Media IP address and Port (point the cursor to view as tooltip)
(Lowermost) Five tabs	Each opens a page displaying detailed information: ▪ Call Quality (see Section 36.2.1 on page 364 below) ▪ Control Info (see Section 36.2.2 on page 367 below) ▪ Media Info (see Section 36.2.3 on page 369 below) ▪ Trend (see Section 36.2.4 on page 370 below) ▪ Alarms (see Section 36.2.5 on page 372 below)

36.2.1 Call Quality

The Call Quality tab centralizes all parameters associated with the quality of an individual call, including Round Trip Delay, Signal Level, Noise Level, SNR, RERL and Burst Duration, in a central location for users to comprehensively assess voice quality, perform precise diagnosis and effectively troubleshoot and manage session experience.

Figure 36-8: Call Quality

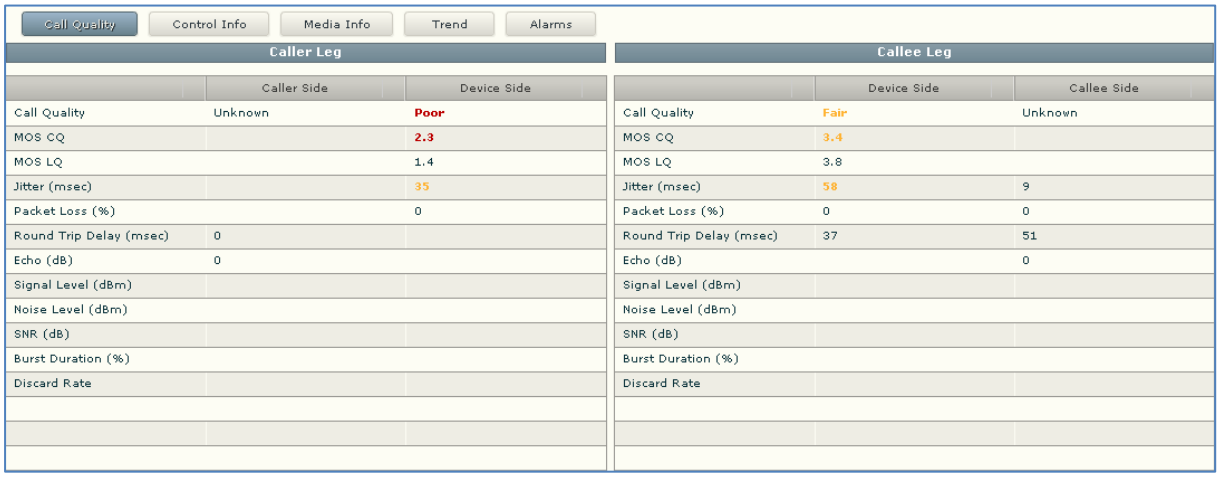


Table 36-3: Call Quality Parameters

Parameter	Description
Call Quality	Good (green), Fair (yellow), Poor (red), Unknown (grey). Indicates the call quality grade scored by both the caller and the device side, on both caller *and* callee legs.
MOS LQ / CQ	MOS = Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined by the SEM after testing calls made over a VoIP network. MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets = RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and for the one value for the callee side.

Parameter	Description
Round Trip Delay (msec)	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two values are shown, one caller side and another for the callee side.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Signal Level (mW)	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level (mW)	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR (mW)	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Burst Duration (msec)	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
Discard Rate	The fraction of RTP data packets from the source that have been discarded since the initial call reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer.

For detailed information, see:

- RFC-3611 RTCP-XR protocol (go to http://tools.ietf.org/rfc/rfc3611.txt)
- RFC-3350 RTP protocol (go to http://tools.ietf.org/html/rfc3550)

36.2.1.1 Call Quality – PSTN Leg

Quality can also apply to voice over PSTN (not only to VoIP). The figure below shows the Call Details screen of an IP to PSTN call whose callee leg is over PSTN.

Figure 36-9: Call Quality - PSTN Leg

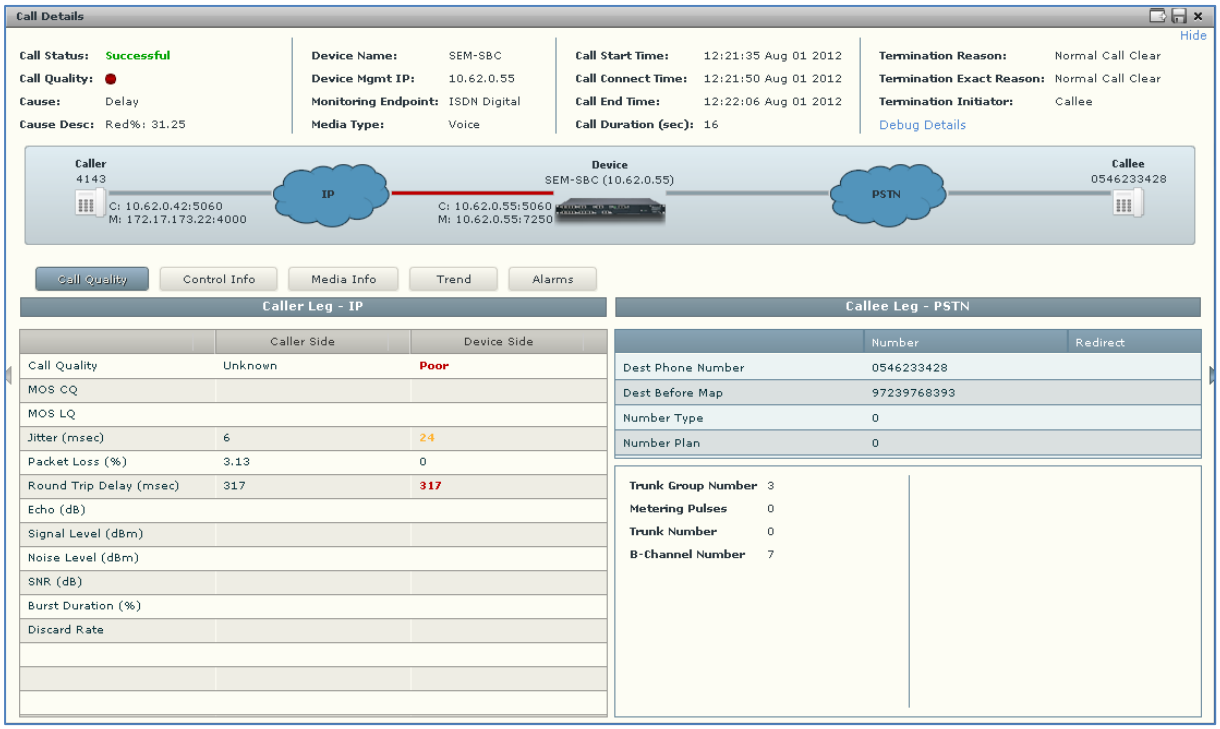


Table 36-4: Call Quality Parameters – PSTN Leg

Parameter	Description
Dest Phone Number (Callee) Source Phone Number (Caller)	Called (destination) phone number Caller's (source) phone number
Dest Before Map (Callee) Source Before Map (Caller)	Called (destination) number before manipulation (if any) was done on it Caller's number before manipulation (if any) was done on it
Number Type	Applies only to IP to Tel calls. Options are: Unknown, Level 2 Regional, Level 1 Regional, PISN Specific, Level 0 Regional (Local), International, National, Network Specific, Subscriber or Abbreviated.
Number Plan	Applies only to IP to Tel calls. Options are: Unknown, Private, E.164 Public, Value Received from PSTN/IP
Trunk Group Number	Defines the Trunk Group number provisioned by the user.
Metering Pulses	Applies only to gateways. Number of 12/16 KHz metering pulses generated toward the Tel side, e.g., for connection to a pay phone or private meter.

Parameter	Description
Trunk Number	Applies only to gateways. Defines the physical trunk number, where 0 is the first trunk.
B-Channel Number	Applies only to gateways. Defines the selected B (bearer) channel, i.e., the channel in which primary voice communication is carried).

36.2.2 Control Info

The Control Info tab shows a call's control protocol (SIP) parameter settings that users can refer to for diagnostic, troubleshooting and session experience management issues.

The same parameters apply to both the Caller and Callee legs. These parameters are explained in the table below.

Figure 36-10: Control Info

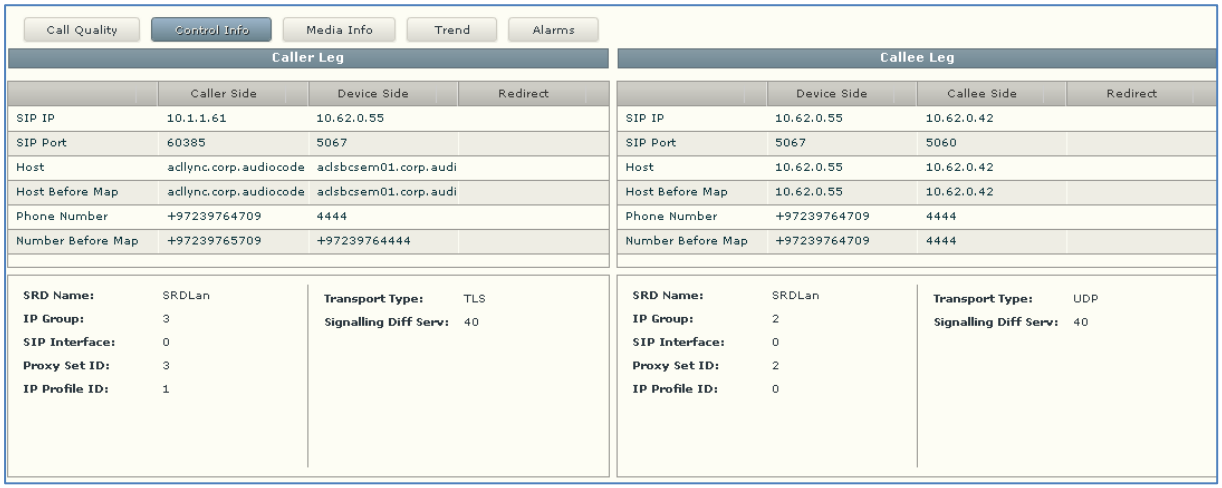


Table 36-5: Control Info Parameters Descriptions

Parameter	Description
SIP IP	IP address (source and destination) of the SIP call
SIP Port	Port number used for the SIP call
Host	The URI (Uniform Resource Identifier) of the host. The SIP URI is the user's SIP phone number (after manipulation, if any). The SIP URI resembles an e-mail address and is written in the following format: sip:x@y:Port, where x=Username and y=host (domain or IP).
Host Before Map	SIP URI address before manipulation (if any) was done on the URI.
Phone number	Caller's phone number after manipulation (if any) was performed on it.
Number Before Map	Caller's phone number before manipulation (if any) was performed on it.
SRD Name	The unique name configured for the signaling routing domain (SRD).
IP Group	The ID of the IP Group with which call is associated.
SIP Interface	The ID of the SIP Interface with which the call is associated.
Proxy Set ID	The ID of the Proxy Set to which the call is associated. A Proxy Set is a group of Proxy servers defined by IP address. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.
IP Profile ID	The ID of the IP Profile assigned to this IP destination call. The IP Profile assigns numerous configuration attributes (e.g., voice codes) per routing rule.

36.2.3 Media Info

The Media Info tab displays a call's media parameter settings that users can refer to for diagnostics, troubleshooting and session experience management issues.

The same parameters apply to both the Caller and Callee legs. These parameters are described in the table below. .

Figure 36-11: Media Info

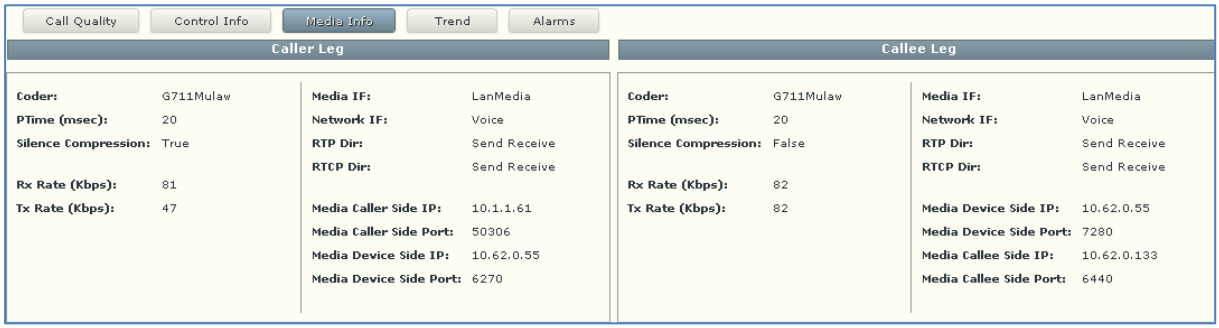


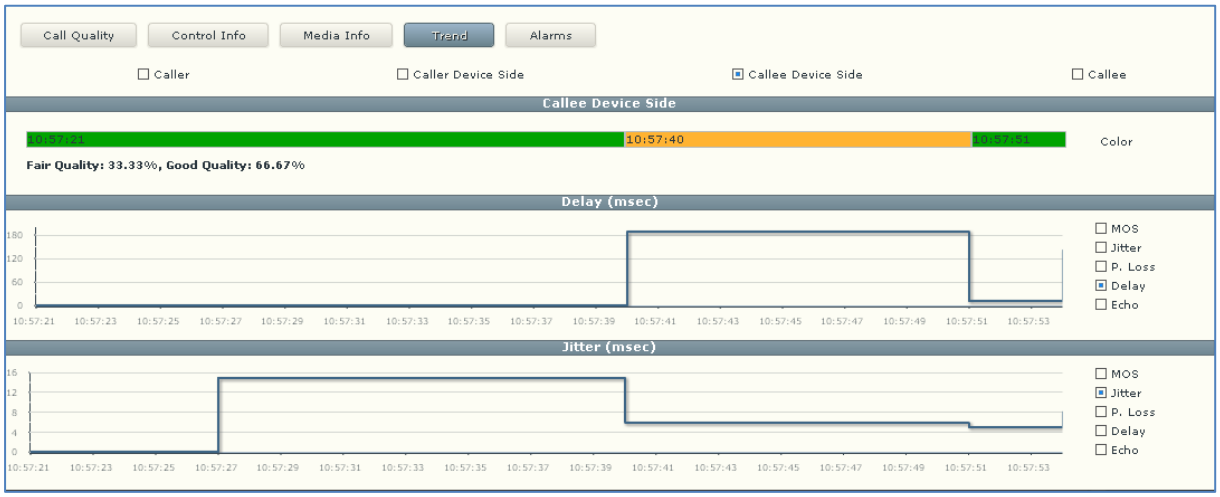
Table 36-6: Media Info Parameters

Parameter	Description
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.
Silence Compression	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).
Rx Rate (Kbps)	Shows the call's reception rate, in Kbps.
Tx Rate (Kbps)	Shows the call's transmission rate, in Kbps.
Media IF	Media Realm name.
Network IF	Network Interface Name.
RTP Dir	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Dir	RTCP Directional Control. Controlled internally by the device according to the selected coder.
Media Caller Side IP	The device's source IP address in the operations, administration, maintenance, and provisioning (OAMP) network.
Media Caller Side Port	The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network.
Media Device Side IP	IP address of the destination host / media network.
Media Device Side Port	Port of the destination host / media network.

36.2.4 Trend

The Trend tab shows the quality trend of a call that users can refer to for diagnostic, troubleshooting and session management experience issues.

Figure 36-12: Trend



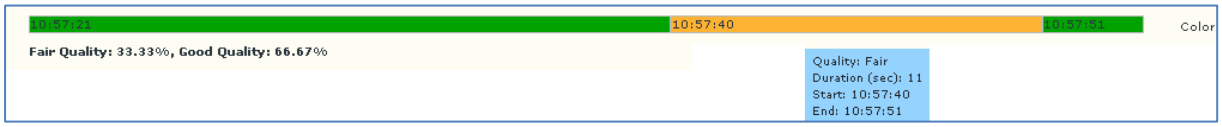
Quality applies to two legs of the call:

- Caller leg
  - caller side (of cloud)
  - device side (of cloud)
- Callee leg
  - callee side (of cloud)
  - device side (of cloud)

➢ To assess call quality:

1. Select one of the four leg options (uppermost row of check boxes).
2. Point the cursor over the color bar; a popup shows data at that point:

Figure 36-13: Call Quality Color Bar



The popup in Figure 36-13 indicates the quality measurement that the call scored in this segment (good = green, fair = yellow, poor = red), how long the segment lasted, and the time the segment started and ended.

Each quality category's percentage of the total length of the call is textually indicated below the color bar.

Note: Legs over PSTN are not measured for quality, only legs over IP. Check box options are disabled for legs over PSTN.

➢ **To compare one call quality metric with another:**

1. Select one of the four leg options (uppermost row of check boxes).
2. Adjacent to the two lower panes, select MOS, Jitter, Packet Loss, Delay or Echo check boxes; you can immediately visually compare one metric with another (see Figure 36-12 above).
3. Optionally select another of the four leg check box options; you can immediately compare the same metrics across this leg, or, optionally, select different metrics to compare.

36.2.5 Alarms

The Alarms tab lists alarms (if any) issued by the device associated with the call. Users can refer to the data displayed to quickly assess a call's alarm/s and consequently effectively diagnose, troubleshoot and manage session experience issues.

Figure 36-14: Alarms

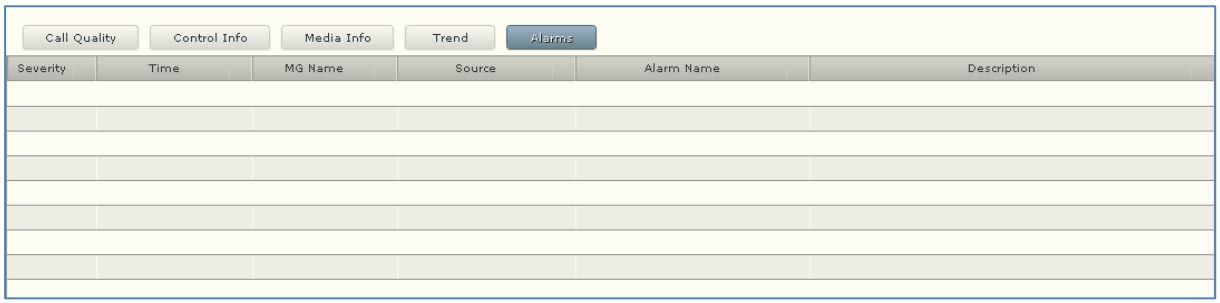


Table 36-7: Alarms Columns*

Column	Description
Severity	For detailed information, see Section 37 below.
Time	The precise time (hour, minutes and seconds) and date (month, day and year) at which the alarm was received.
MG Name	The name of the device on which the individual call's alarm/s were issued.
Source	The entity that triggered the alarm.
Alarm Name	The name of the alarm.
Description	A textual description of the alarm.

* Extracted from ITU X.733

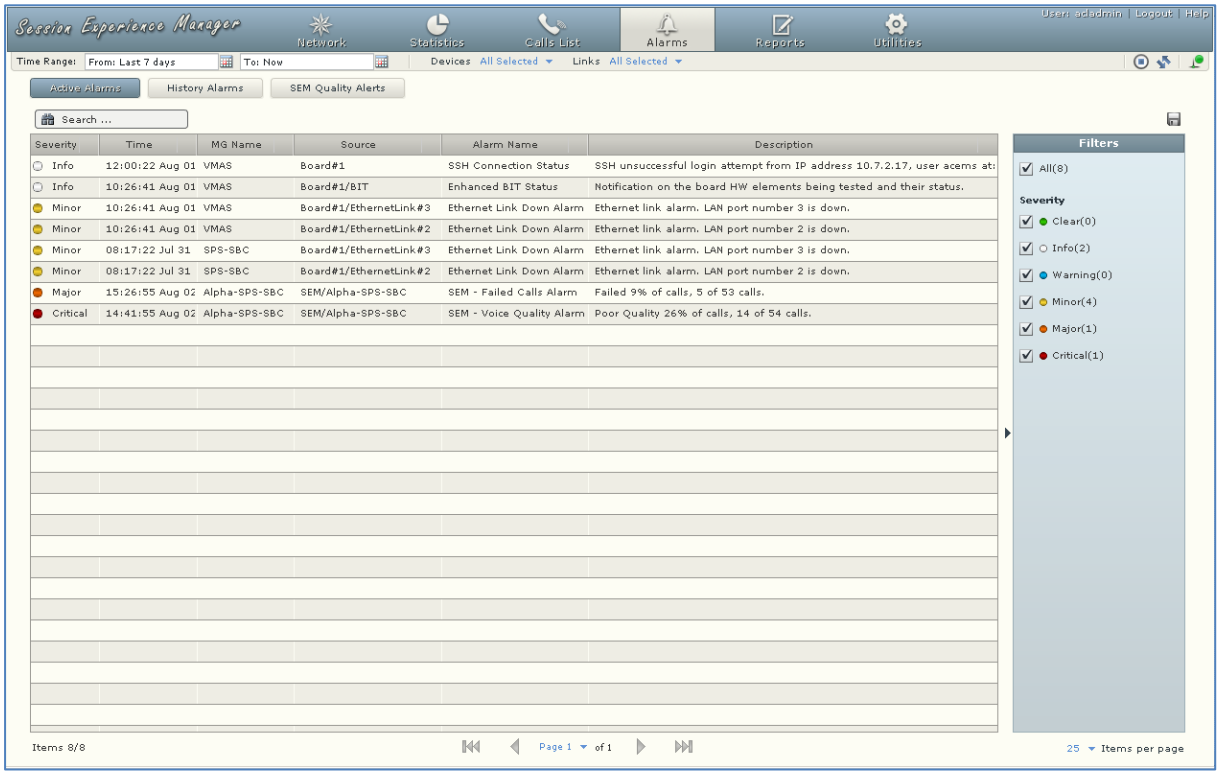
37 Displaying Alarms

The Alarms page features three distinct functionalities:

- Active Alarms
- Historical Alarms
- SEM Quality Alerts

Three tabs in the page enable quick access to each of these:

Figure 37-1: Alarms Page - Active Alarms



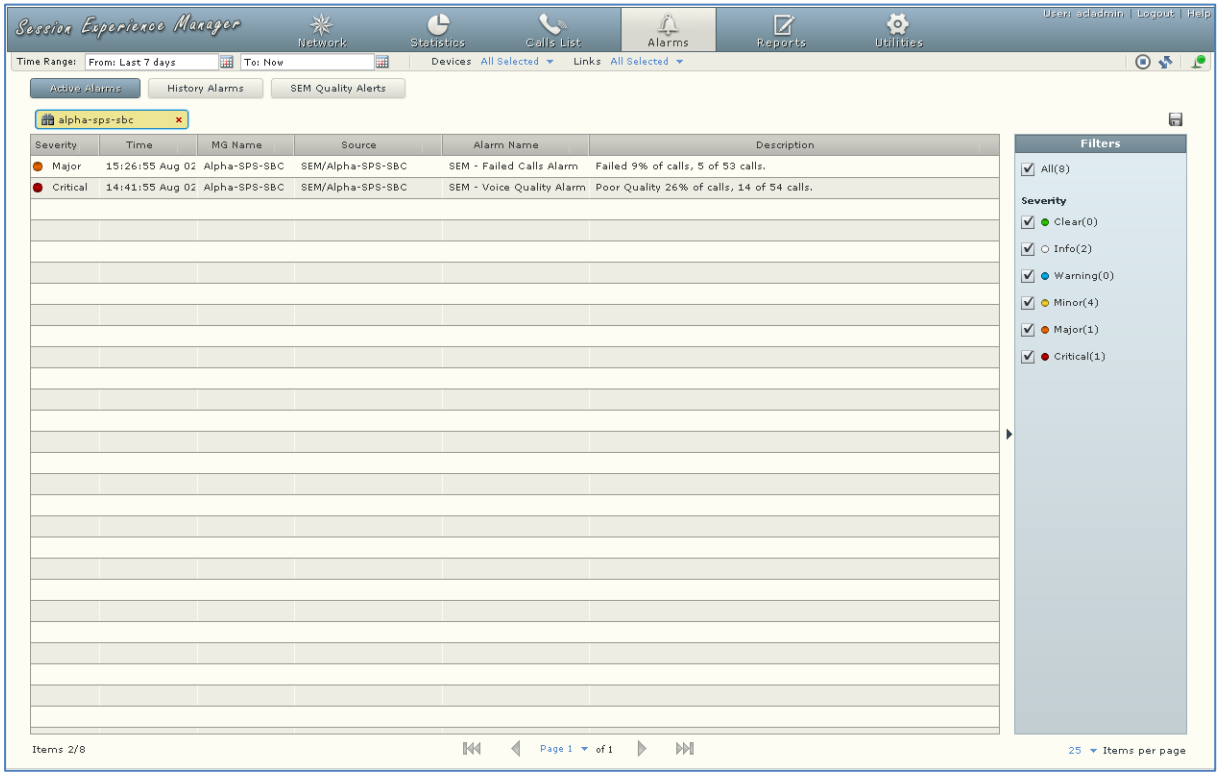
37.1 Displaying Active Alarms

The Active Alarms page lists all active alarms on devices selected in the 'Devices' filter and on links selected in the 'Links' filter, issued during the period defined in the 'Time Range' filter. Filtering using the 'Time Range', 'Devices' and the 'Links' filter is performed identically across all pages. For filtering information see under Section 33 on page 329.

37.1.1 Filtering Using the 'Search' Field

The 'Search' field is used to filter active alarms exactly as it's used on other pages to quickly find specific information. Enter a device name, e.g., Alpha-SPS-SBC, in the 'Search' field; only active alarms made and answered on this device are listed. Click the 'x' to delete a search entry.

Figure 37-2: Alarms Page - Active Alarms – Search Filter



37.1.2 Sorting Listed Alarms

Alarms can be sorted in the same manner as calls in the Calls List (see Section 36.1.3 on page 358). Click the header of the Severity column for example; calls are sorted according to severity, in order of *most* to *least severe* (▼). Most severe alarms are highest in the list. To sort from *least* to *most severe*, click the column header again; the sort order is reversed (▲); less severe alarms are listed lower.

Click another column header, e.g., Time; calls already ordered by severity level are now also ordered in order of time. Multiple ordering is supported.

The feature of multiple sorting columns facilitates quick and easy access to required alarm information.

Table 37-1: Severity in Ascending Order*

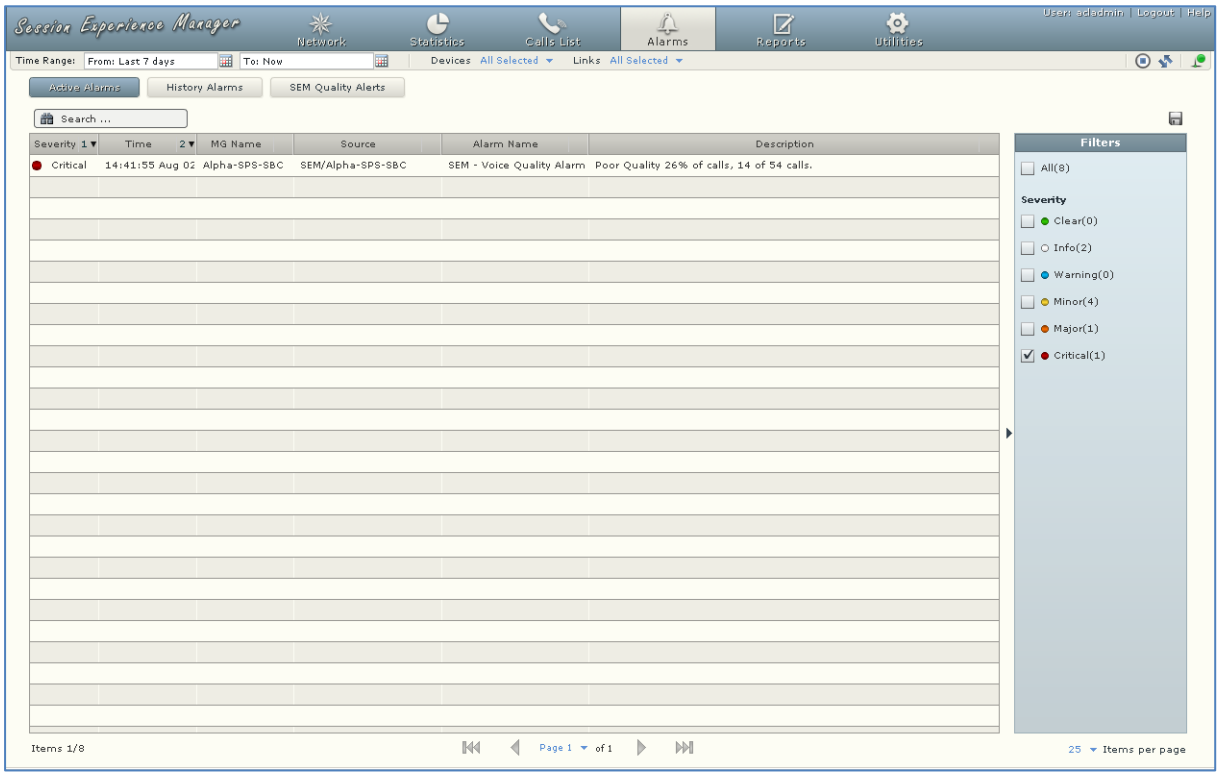
Severity	Description
	Critical (red): Indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when a device becomes totally out of service and its capability must be restored.
	Major (orange): Indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the device and its full capability must be restored.
	Minor (yellow): Indicates the existence of a non-service affecting fault condition and that corrective action should be taken to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the device.
	Warning (blue): Indicates the detection of a potential or impending service affecting fault, before any significant effects occur. Action should be taken to further diagnose (if necessary) and correct the problem to prevent it from becoming a more serious service affecting fault.
	Info (grey): Indicates that the severity level cannot be determined.
	Cleared (green): Indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this device that have the same Alarm type, Probable cause and Specific problems (if given).

* Extracted from ITU X.733

37.1.3 Filtering Using a Severity Filter

The page can be filtered according to a severity level, where only required alarms are displayed. The figure below shows alarms filtered according to the 'Severity' filter (Critical). By contrast, the *sorting* feature displays all alarms; however, with the required alarm/s are listed highest.

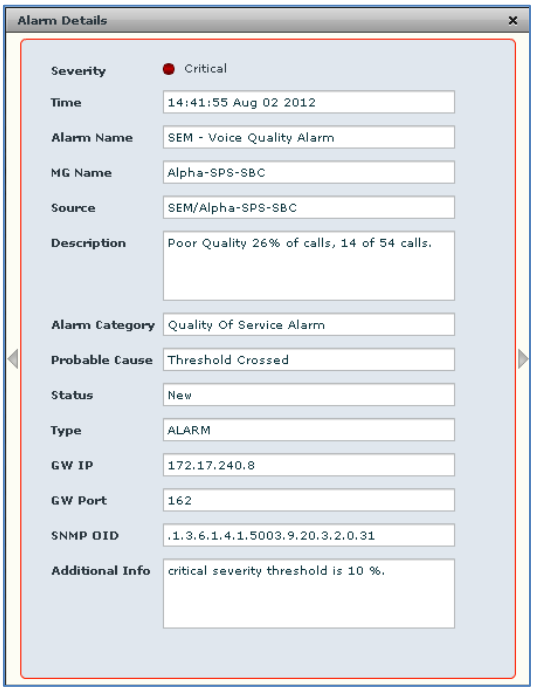
Figure 37-3: Severity Filters - Critical



37.1.4 Displaying Alarm Details

Alarm Details can quickly and easily be accessed to determine the incidence of the severity across the network. Click any row page before or after filtering:

Figure 37-4: Alarm Details



Click the ► or ◄ handlebar to move to the next or previous. Refer to this table:

Table 37-2: Alarm Details – Parameters

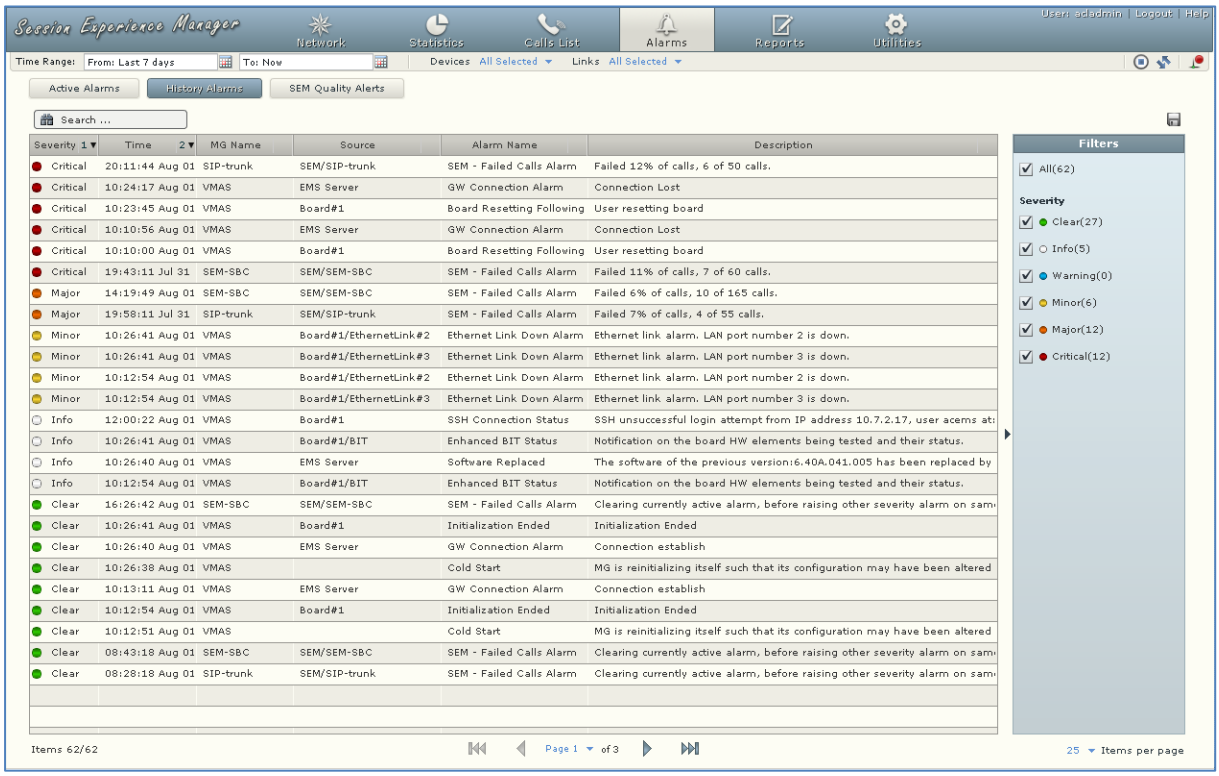
Parameter	Description
Alarm Category	The category in which the alarm is classified, according to ITU X.733. Five categories are specified: Communications: the procedures and/or processes required to convey information from one point to another. Quality of service: Degradation in the QoS. Processing error: Software or processing faults. Equipment: Equipment faults. Environmental: Conditions relating to an enclosure in which the equipment resides.
Probable Cause	The probable cause. See ITU X.733 for probable causes and descriptions.
Status	Can be either one of the following: • **Active Alarms**: New, Ack (acknowledged by the user). • **Historical Alarms**: Cleared (manually cleared by the user), Automatically Cleared (by the device or EMS) or ColdStart Cleared (if system is reset, all alarms are cleared).
Type	The alarm type. EVENT or ALARM. According to RFC 3877:

Parameter	Description
	EVENT = User Information, for example, a fault, a change in status, crossing a threshold, or an external input to the system. **ALARM** = Persistent indication of a fault (where fault = a lasting error or warning condition, and error = a deviation of a system from normal operation). An alarm is automatically cleared when the condition disappears; by contrast an event is not automatically cleared.
GW IP	The IP address of the device from which the alarm was sent.
GW Port	The port number of the device from which the alarm was sent.
SNMP OID	Identifier used to identify the alarm information available on a managed VoIP network entity, in the alarm management information base (MIB).
Additional Info	Possible corrective action, when applicable.

37.2 Displaying History Alarms

The History Alarms page lists currently active alarms and already-cleared historical alarms on devices selected in the 'Devices' filter and on links selected in the 'Links' filter, issued in the period defined in the 'Time Range' filter. These filters are identical on all pages (see under Section 33 on page 329). The page shows retroactive diagnostic data informative when taking proactive steps to prevent future repetitions and improve future VoIP network functionality.

Figure 37-5: Historical Alarms



- The 'Search' field operates identically to its counterpart in the Active Alarms page (see under Section 37.1.1 on page 374).
- Order alarms precisely as you order alarms in the Active Alarms page (see under Section 0 on page 375).
- Filter alarms using the 'Severity' filter precisely as alarms in the Active Alarms page are filtered with its counterpart filter (see under Section 0 on page 376).

37.3 Triggering Quality Alerts

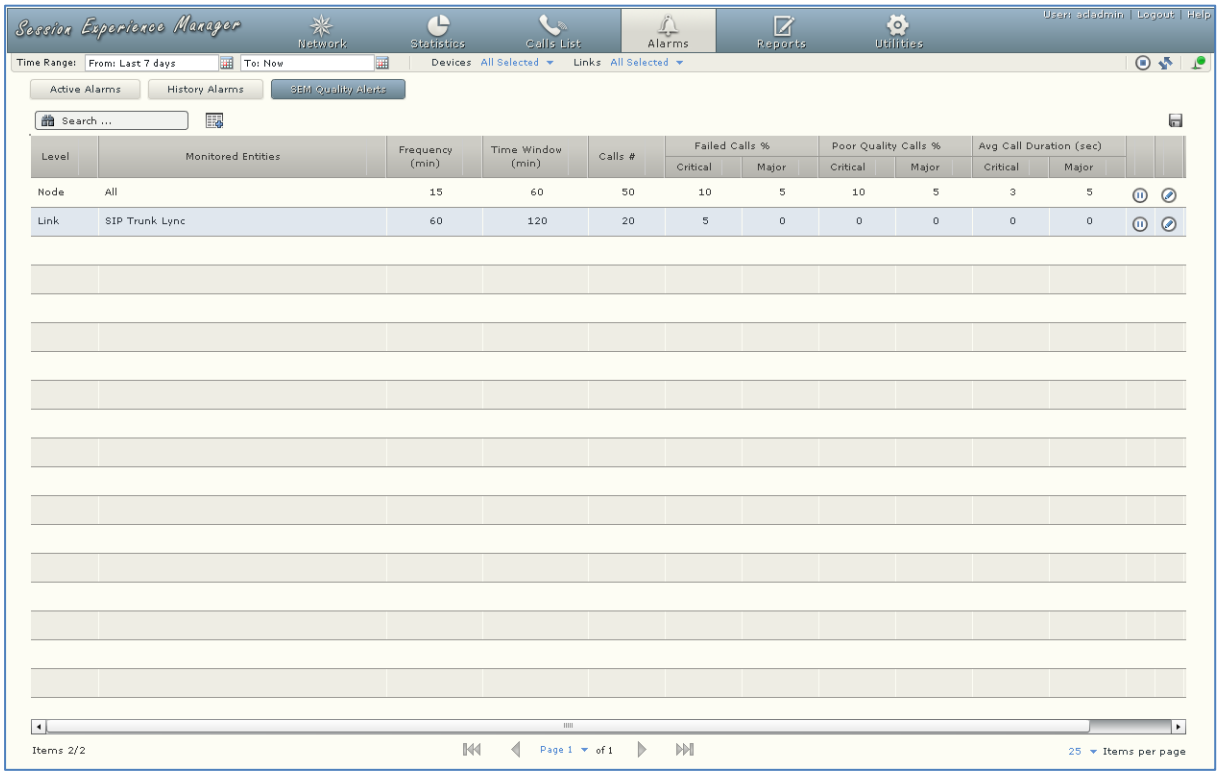
Quality alerts optimize session experience management by providing VoIP network administrators *automatic quality analysis* capability, *automatically triggering alerts* if the quality of service analyzed falls below that defined in rules.

Alerts are triggered by rules defined by network administrators. Alerts, triggered after SEM data analysis, are displayed in the 'Alarms' page as regular alarms and/or sent to administrators' as mail, SMSs, SNMP traps or syslog message (see Section 27 on page 283 for detailed information).

➢ To add a rule:

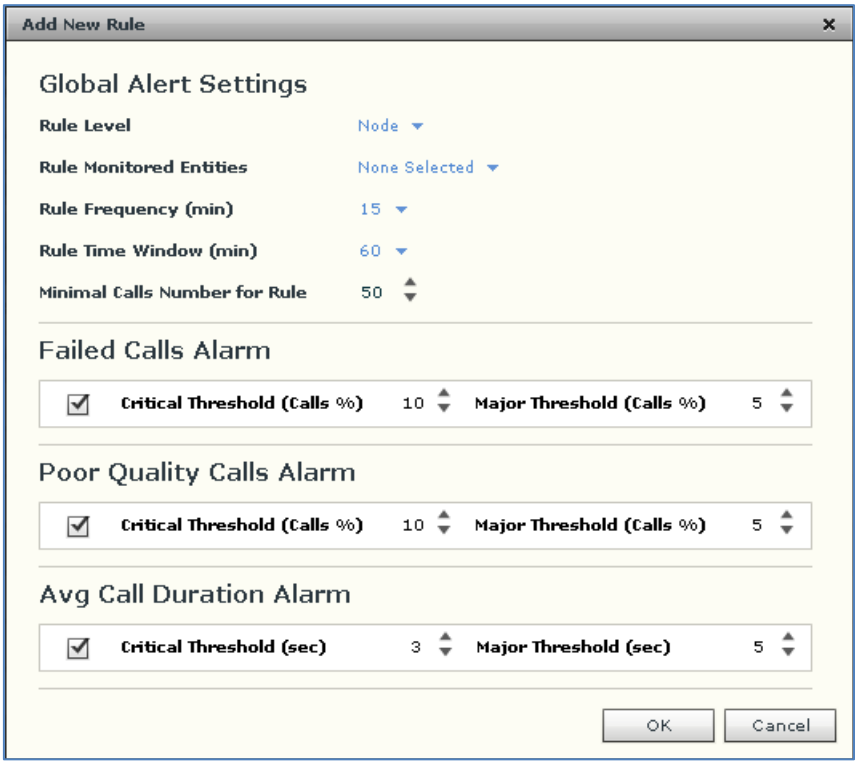
1. Open the SEM Quality Alerts page (Alarms page>**SEM Quality Alerts** tab).

Figure 37-6: SEM Quality Alerts



2. Click the **Add Rule** icon ; the following screen pops up:

Figure 37-7: Add New Rule



3. In this screen define the following:

Table 37-3: Add New Rule

Setting	Definition
Level to Monitor	Device or Link
Entities to Monitor	All devices/links, specific devices/links, or a set of devices/links.
Monitoring Frequency (min)	Determines how frequently the SEM automatically performs data analysis. Defines every 15 (default), 30 or 60 minutes.
Analyse the Past *n* Minutes	Determines the period up to the present for which the SEM will perform data analysis. Define 60 minutes (default), 90 minutes or 120 minutes.
Minimum # of Calls to Analyze	Defines the number of calls to analyze. Default = 50 calls. Up to 1000 calls can be defined. If the number of calls made doesn't exceed the defined # of calls to analyze, the SEM won't perform data analysis.
Failed Calls Alarm	Critical Threshold: **5**% of calls (default); if this threshold is exceeded, the alert is triggered. Major Threshold: **3**% of calls (default); if this threshold is exceeded, the alert is triggered.

Setting	Definition
Poor Quality Calls Alarm	Critical Threshold: **10**% of calls (default); if this threshold is exceeded, the alert is triggered. Major Threshold: **8**% of calls (default); if this threshold is exceeded, the alert is triggered.
Avg Call Duration Alarm	Critical Threshold: **5** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alert is triggered. Major Threshold: **10** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alert is triggered.

4. Click the **Run Rule** icon to activate the rule, or the 'Pause Rule' icon to deactivate it.
5. Click the **Update Rule** icon to redefine the settings.

37.3.1 Defining a Rule to Trigger an Alert (Example)

This example shows how to define rule settings to determine monitoring. Using this example, you can intuitively determine how to define a rule to trigger an alert.

If you define in a rule with the following settings:

- 'Level to Monitor' = Device
- 'Monitored Devices' = All
- 'Monitoring Frequency' = 15 minutes
- 'For the Past' = 60 minutes
- 'Minimum # of Calls to Analyze' = 50
- 'Failed Calls Alarm' = defaults
- 'Poor Quality Calls Alarm' = defaults
- 'Avg Call Duration Alarm' = defaults

Then the SEM will perform the following:

- Check every 15 minutes the # of calls made on all devices in the past 60 minutes and for devices on which the # of calls is greater than 50:
  - Compare failed / successful calls % to the defined settings
  - Compare poor quality calls % (red-coded) to the defined settings
  - Compare average call duration to the defined settings

37.4 Distributing Alarm Information

Alarms information displayed in the Active Alarms, History Alarms and Quality Alerts pages are easily downloaded and saved by clicking the **Save As** icon .

- Active Alarms information is saved in a plain-text *ActiveAlarms.csv* file.
- History Alarms information is saved in a plain-text *HistoryAlarms.csv* file.
- SEM Quality Alerts information is saved in a plain-text *SEMQualityAlerts.csv* file.

Open and read in any text editor, these files can be sent by the administrator as an attachment in an email to others to distribute the information.

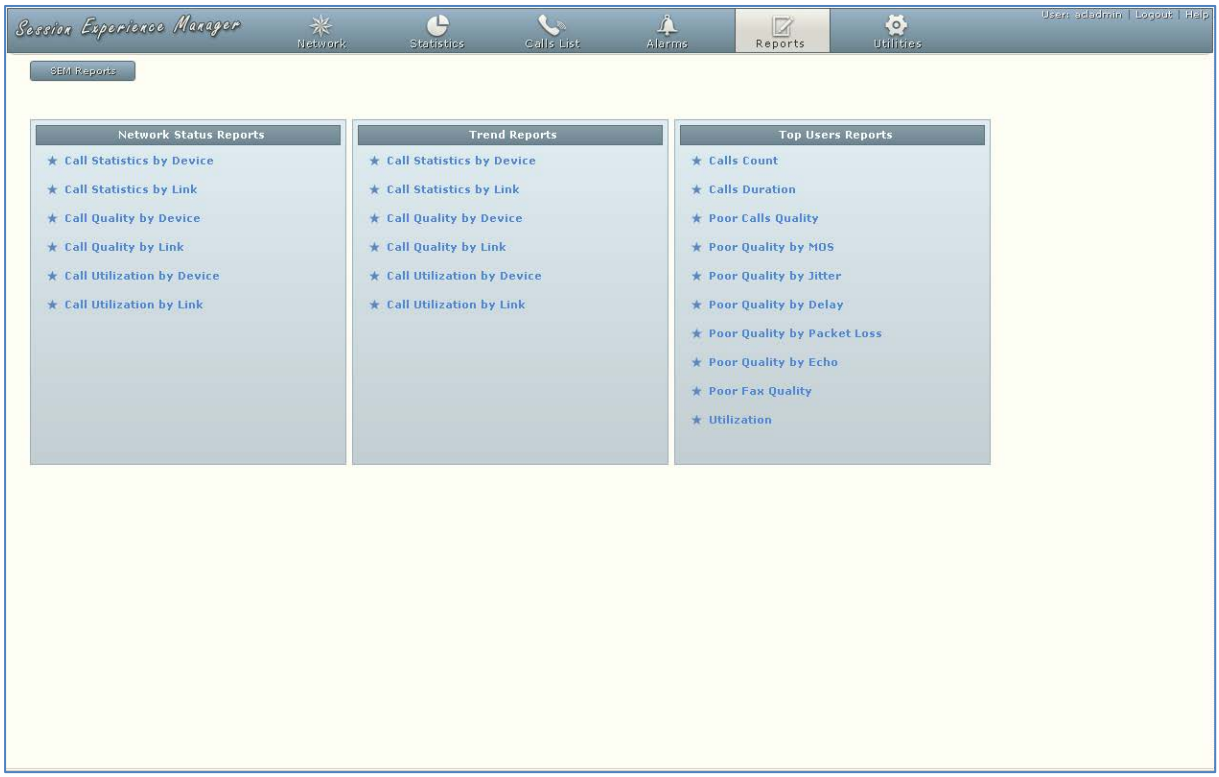
See Section 27 on page 283 for the available forwarding options.

This page is intentionally left blank

38 Generating Reports

The SEM features essential reports-generation capability that administrators can utilize *to distribute session experience data and comparative analyses* quickly and effectively to responsible persons within the enterprise and to external authorities associated with the enterprise's VoIP network, for *accurate diagnosis and correction* of degraded sessions and for general *network optimization.*

Figure 38-1: Reports Page



Three categories of reports help users to quickly and thoroughly analyze different aspects of calls made over the VoIP network:

1. Summary Reports
2. Trend Reports
3. Top Users Reports

Categories 1 and 2 are identical in terms of the information displayed (columns); however the *calculation* differs.

Category 1 is calculated as a *summary of calls made over the entire period* for specified entities (devices / links). The x axis represents the specified entities.

Category 2 is calculated *per time interval* specified, summarizing the same entity in the specified interval. The x axis represents the time interval (hour / day / week / month).

Table 38-1 shows the categories and the reports options in each.

Table 38-1: Reports Categories

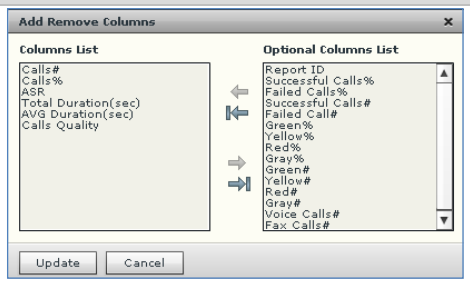
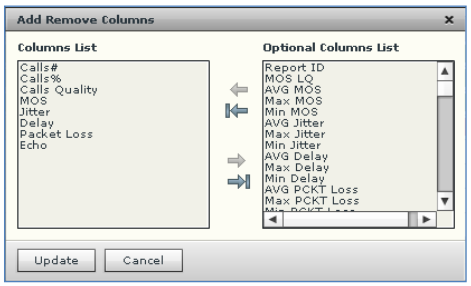
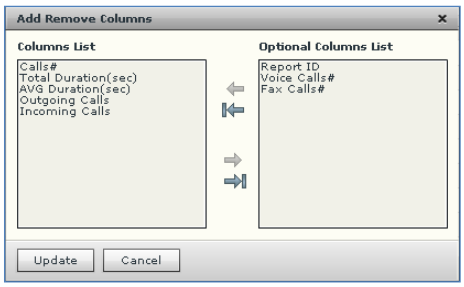
Report Category	Explanation
Summary Reports ▪ Call Statistics by Device ▪ Call Statistics by Link ▪ Call Quality by Device ▪ Call Quality by Link ▪ Call Utilization by Device ▪ Call Utilization by Link	Displays a summary of key call metrics during a specified time period with a separate row entry for each device/link. Purpose: To compare performance, quality and utilization across devices/links. For example, the 'Call Statistics by Device' report summarizes the % of successful and failed calls and the # of calls that scored in each quality, across specified devices/links. By contrast, a 'Call Quality by Device' report summarizes key metrics affecting voice quality (jitter, delay, packet loss).
Trend Reports ▪ Call Statistics by Device ▪ Call Statistics by Link ▪ Call Quality by Device ▪ Call Quality by Link ▪ Call Utilization by Device ▪ Call Utilization by Link	Displays a summary of key call metrics over specified time intervals of a specified device/link. For example, the 'Calls Trend by Device' report displays 'Number of Calls', 'ASR' and 'Total Duration' in hourly intervals.
Top Users Reports ▪ Calls Count ▪ Calls Duration ▪ Poor Calls Quality ▪ Poor Quality by MOS ▪ Poor Quality by Jitter ▪ Poor Quality by Delay ▪ Poor Quality by Packet Loss ▪ Poor Quality by Echo ▪ Poor Fax Quality ▪ Utilization	Displays users graded according to number of calls made, calls duration, and calls whose quality scored 'Poor' based on specified metrics.

38.1 Using Reports Pages Features

The features below apply to all reports pages across all three reports categories unless stated otherwise:

Table 38-2: Reports Pages Features

Feature	Description
Export (save as PDF)	Enables users to generate a PDF file of the report reflecting selected filters, columns, graphs, etc.
Filters	Enable you to specify the following: • The Time Range for the report to cover (in the Summary Report page) • The Time Range *and* the Interval for the report to cover (in the Trend Report page) • on which Devices / Links to produce the report • Top 10/20/30 Users on which to produce the report (in the Top Users Report page)
SEM Reports	Click at any time to return to the Reports page displaying the three reports categories and the report options available under each. Click an option to produce a report.
Run now	Displayed after selecting a report to produce in the reports menu. First filter (see above) and then click it; the report is produced and displayed.
Charts view / Table view	Two views are displayed in every report produced: Charts (uppermost) and table (lowermost). Click to expand charts view; table view is eclipsed. Click to revert to both views.
Switch to horizontal / Switch to vertical	Charts are by default displayed vertically, one below the other, in this order: Calls #, Calls %, ASR, Total Duration, AVG Duration and Calls Quality. Use the scrollbar to scroll down from one to the next. They can optionally be displayed horizontally to suit user preference. To display horizontally, click the link. Click next or previous to navigate from chart to chart.
Bar / Linear	By default, charts are displayed as bar charts. Click the drop-down to choose linear charts if required.
Add / Remove Columns	Click the icon; optional table view columns are displayed. To add, if required, select an optional column and click or select all and click . To remove a column, select it in the Columns List pane and click or select all and click . Default metrics columns (left pane) and optional metrics columns (right pane) in the Summary/Trend category (except 'Call Quality by Device / Link') are as follows:

Feature	Description
	 Default metrics columns (left pane) and optional metrics columns (right pane) in a 'Call Quality by Device / Link' report in the Summary/Trend category are:  Default metrics columns (left pane) and optional metrics columns (right pane) in the Top Users reports category are:  See under Section 0 on page 394 for variations across reports in the Top Users Reports category.
 Show Column Graphical Representation	Column headers in Table view display this icon. If you click one of these column headers, that metric column's counterpart chart opens in Charts view. If the chart is already open, you're notified. After report generation, the table's ASR metric column is the only one displayed as a chart in Charts view.
Table Bottom Line (Total)	The table's bottom line shows column's total. For example: • Calls # column's bottom line shows the total sum of all counts of all calls on all devices / links • ASR column's bottom line shows the average success rate of the average success rates of all devices / links. 'Total' is calculated according to the measured parameter. It can be SUM, AVG, MIN or MAX.

Feature	Description
Search	Users can use the 'Search' option to search for and find precise information related to a query. When information related to the search query is found, the report exclusively displays only that information.

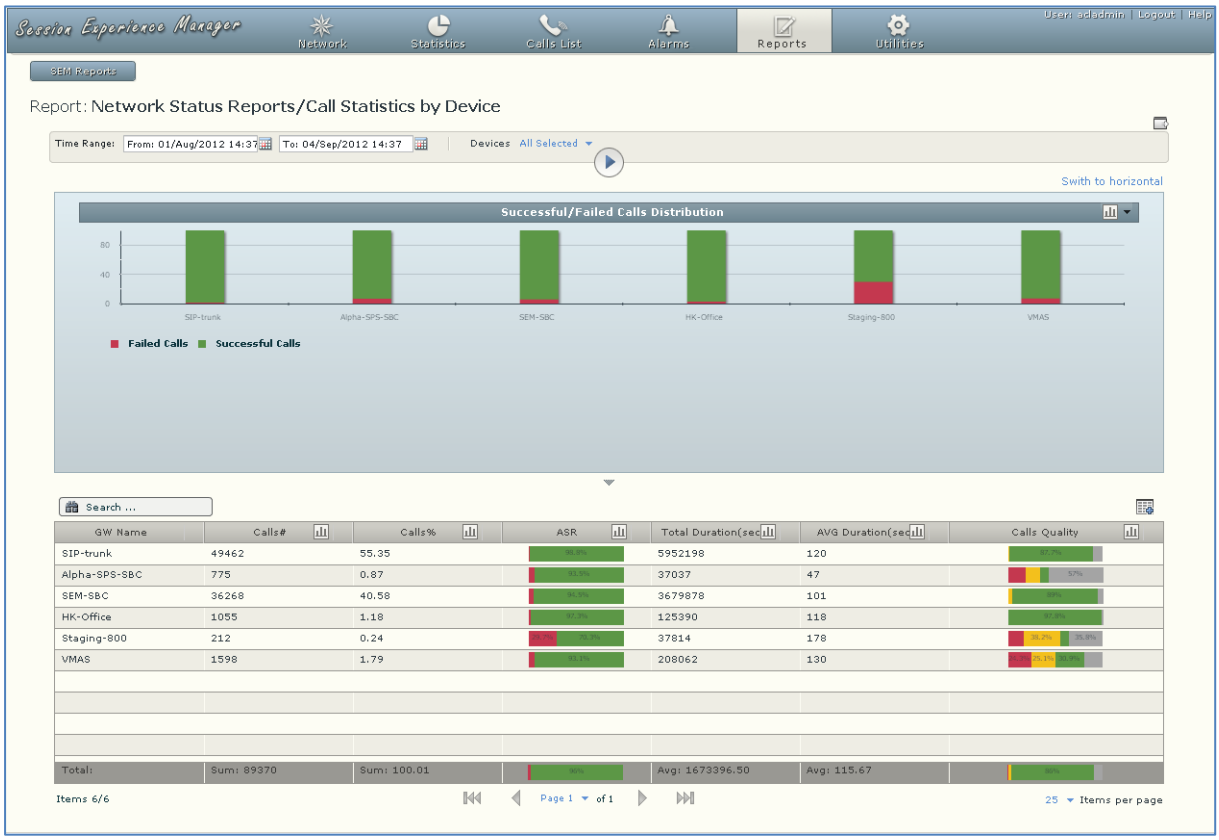
38.1.1 Generating Summary Reports

Summary Reports show *the sum totals, over the entire period,* of calls performance scores, quality scores, #s, %s, total duration and average duration (default metrics). Reports in this category are identical in terms of metrics measured. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in Table 38-2).

To generate a summary report:

1. Click a report option in this category, for example, click the first option, i.e., Call Statistics by Device; the 'Run now' page opens.
2. Filter for 'Time Range' and 'Devices' (described under Section 33 on page 329).
3. Click the 'Run now' icon; the report is produced:

Figure 38-2: Summary Report – Call Statistics by Device

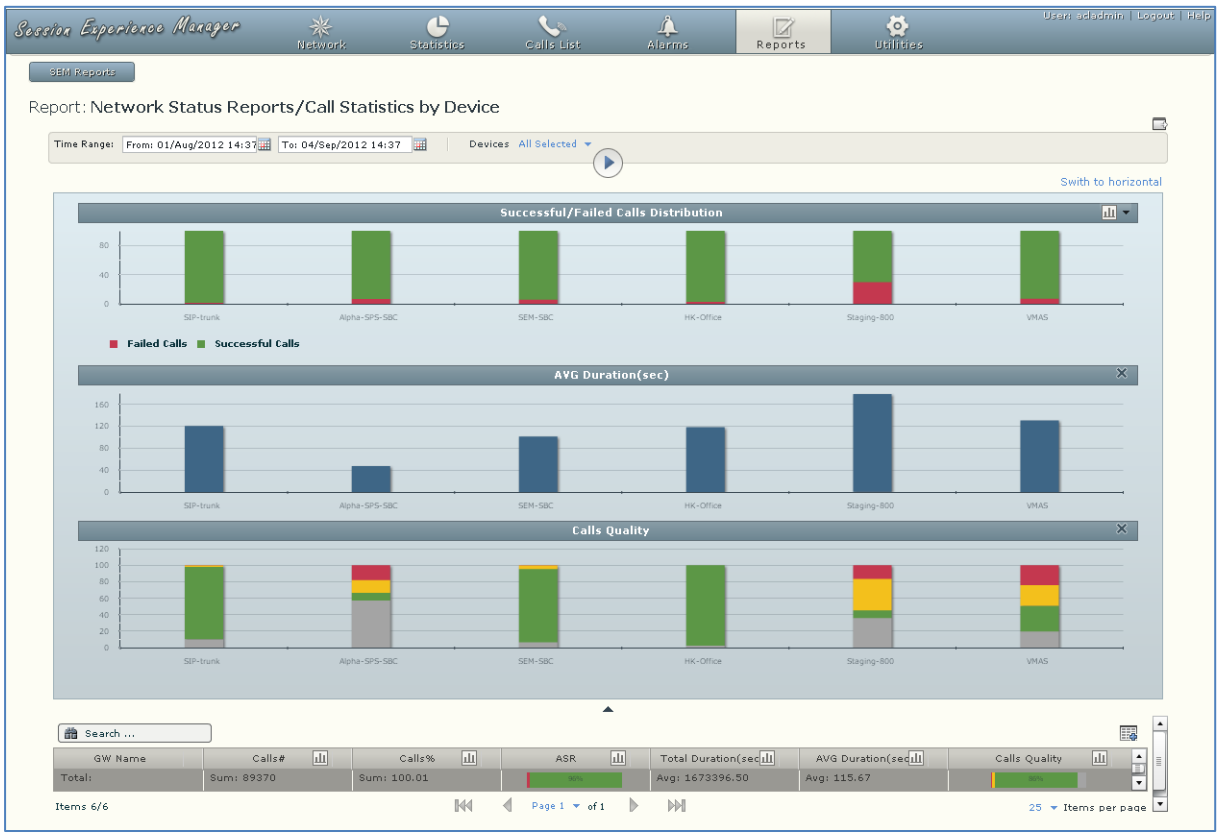


Following report generation, the ASR metric column is the only one displayed in charts view.

To display another metric (other metrics) in charts view:

- Click the  icon shown in the metric's column header (see 'Show Column Graphical Representation' in Table 38-2):

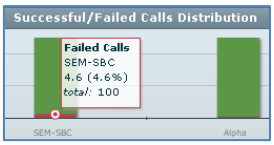
Figure 38-3: Displaying Multiple Metrics in Charts View (Vertical)



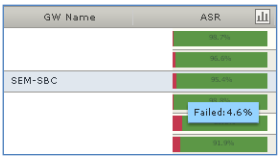
Graphics view is extended by clicking ▼ (as in the figure above); to restore, click ▲.

In the report page:

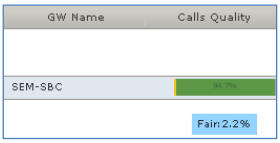
- See from chart view which entities registered the highest failed / successful calls rate
- See from table view on which entities most calls were made, what % of calls were made on each, on which entities most failed / successful calls were made, on which entities was most call time recorded, on which entities was the average call duration longest / shortest and on which entity did voice quality score highest (green = good, yellow = fair, red = poor, grey = unknown)
- View an entity's success / fail rate (%) by pointing your cursor over a color in a bar in its chart (green = successful, red = failed):



- View an entity's success / fail rate (%) in the table by pointing your cursor over the entity's ASR row (green = successful, red = failed):



- View quality scores by pointing your cursor over a color in the entity's Calls Quality row (green = good, yellow = fair, red = poor, grey = unknown):



- Switch charts view from vertical (default) to horizontal by clicking the link 'Switch to horizontal' (see Table 38-2)
- Change charts view from bar  (default) to linear by selecting  from the drop-down (see 'Charts view / Table view' in Table 38-2)
- Add a column to table view or remove a column from table view by clicking the  icon (see 'Add / Remove Columns' in Table 38-2).

Default and optional table columns in Summary reports are:

Table 38-3: Table Columns in Summary Reports

Report	Default Columns	Optional Columns
Call Statistics by Device/Link	Calls #, Calls %, ASR, Total Duration, Average Duration, Calls Quality	Successful/Failed Calls % Successful/Failed Calls # Green/Yellow/Red/Gray % Green/Yellow/Red/Gray # Voice Calls # Fax Calls #
Call Quality by Device/Link	Calls #, Calls %, Calls Quality, MOS, Jitter, Delay, Packet Loss, Echo	MOS LQ AVG/Max/Min MOS/Jitter/Delay/Packet Loss/Echo AVG MOS LQ AVG Signal Level/SNR MOS/MOS LQ/Jitter/Delay/Packet Loss/Echo Remote AVG/Max/Min MOS R/Jitter R/Delay R/P. Loss R/Echo R Red #, Yellow #, Green #, Gray # Red %, Yellow %, Green %, Gray % MOS/MOS LQ/Jitter/Delay/Packet Loss/Echo Red % [Same for Yellow, Green and Gray] MOS Red Remote % [Same for Yellow, Green and Gray]

Report	Default Columns	Optional Columns
		MOS/Jitter/Delay/Packet Loss/Echo LQ Red Remote % [Same for Yellow, Green and Gray]
Call Utilization by Device/Link	AVG Total Kbps AVG Rx Kbps AVG Tx Kbps AVG Packet Loss	AVG Total Kbps Remote AVG Rx/Tx Kbps Remote AVG Packet Loss R

- Re-filter and re-run the report (see 'Filters' in Table 38-2)
- Choose to generate another report by clicking SEM Reports

38.1.2 Generating Trend Reports

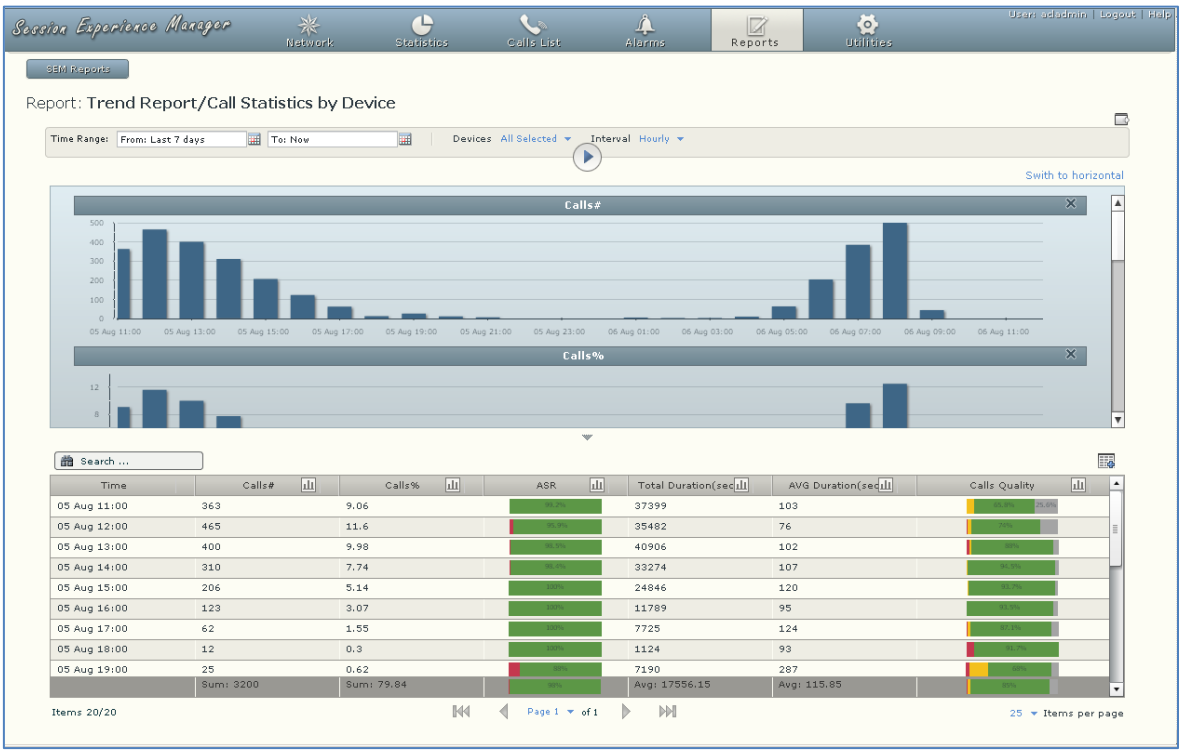
Trend reports show *general tendencies, over intervals,* of calls performance, quality, #s, %s, total duration and average duration (default metrics measured).

Reports in this category are identical in terms of metrics columns displayed. Columns can optionally be added / removed (see 'Add / Remove Columns' in Table 38-2).

To produce a trend report:

1. Click a report option in this category, e.g., the first; the 'Run now' page opens
2. Filter for 'Time Range' and 'Devices' (described under Section 33 on page 329). For the 'Interval' filter select Hourly, Daily, Weekly or Monthly.
3. Click the 'Run now' icon; the report opens:

Figure 38-4: Trend Report – Call Statistics by Device



In this page you can do the following:

- Export the report to PDF by clicking  (see 'Export…' in Table 38-2)
- Immediately determine *when* most/least calls were made, how many, % of total, each period's success/fail rate and each period's quality scores.
- Switch charts view from vertical (default) to horizontal by clicking the link 'Switch to horizontal' (see Table 38-2)
- Change charts view from bar  (default) to linear by selecting  from the drop-down (see 'Charts view / Table view' in Table 38-2)
- Display a column in the table in charts view by clicking the  icon shown in that column's header (see 'Show Column Graphical Representation' in Table 38-2)
- Add a column to table view or remove a column from table view by clicking the  icon (see 'Add / Remove Columns' in Table 38-2). Default columns and optional columns are identical to the 'Call Statistics by Device/Link' and 'Call Quality by Device/Link' reports in the Summary Reports category.
- Page if the 'Interval' filter is set to 'Daily' (see under Section 36)
- Re-filter and re-run the report (see 'Filters' in Table 38-2)
- Choose to produce another report by clicking 

38.1.3 Generating Top Users Reports

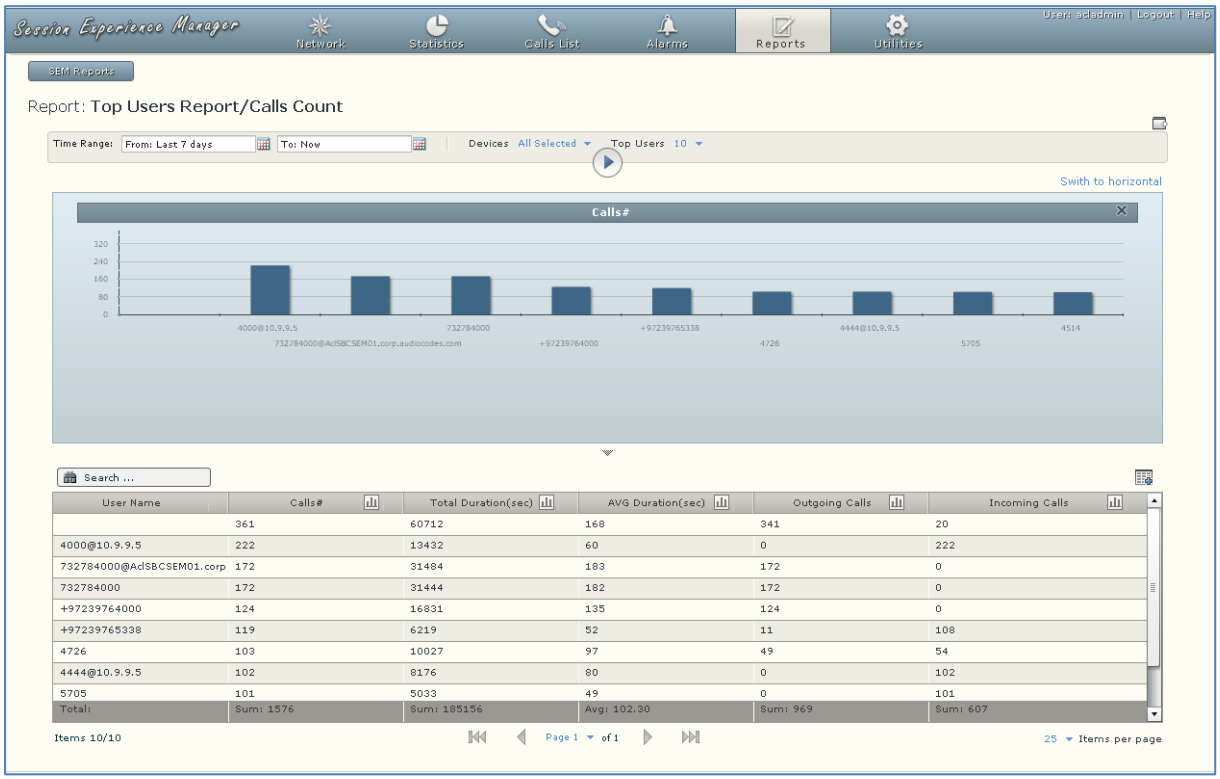
Top Users reports display the *top 10, 20 or 30 users* in terms of # of calls made, total duration, average duration, outgoing calls and incoming calls (default metrics measured).

Reports in this report category are identical in terms of metrics columns displayed. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in Table 38-2).

➢ To generate a top users report:

1. Click a report option in this category, for example, click the first report option, i.e., Calls Count; the 'Run now' page opens.
2. Filter for 'Time Range' and 'Devices' (described under Section 33 on page 329). For the 'Top Users' filter, select 10, 20 or 30.
3. Click the 'Run now' icon; the report opens:

Figure 38-5: Top Users Report – Calls Count



In this page you can do the following:

- Export the report to PDF by clicking (see 'Export…' in Table 38-2)
- Switch charts view from vertical (default) to horizontal by clicking the link 'Switch to horizontal' (see Table 38-2)
- Display a column in the table in charts view by clicking the icon shown in that column's header (see 'Show Column Graphical Representation' in Table 38-2)

- Add a column to table view or remove a column from table view by clicking the  icon (see 'Add / Remove Columns' in Table 38-2).

  Default and optional table columns in Top Users reports are:

Table 38-4: Table Columns in Top Users Reports

Report	Default Columns	Optional Columns
Calls Count	Calls #, Total Duration, Average Duration, Outgoing Calls, Incoming Calls	Voice Calls #/Fax Calls #
Calls Duration	Total Duration, Calls #, Average Duration, Outgoing Calls, Incoming Calls	None
Poor Calls Quality	Poor Quality Calls, Calls #, Calls Quality	Gray/Green/Yellow/Red % Yellow/Red #
Poor Quality by MOS / Jitter / Delay / Packet Loss / Echo	AVG MOS / Jitter / Delay / Packet Loss / Echo, Calls #, Total Duration	None
Poor Fax Quality	Poor Quality Faxes, Poor Quality Pages, Total Faxes, Total Pages	None
Utilization	Total Bytes, RX Bytes, TX Bytes	None

- Page if the top 30 users are selected for a prolonged period in which case multiple report pages may occur (see under Section 36 on page 353)
- Re-filter and re-run the report (see 'Filters' in Table 38-2)
- Choose to produce another report by clicking 

This page is intentionally left blank

39 Use Cases

Review the use case scenarios described in this section to better understand how you can effectively utilize the SEM to monitor VoIP network health and to benefit from its diagnostics capability.

Future SEM versions will directly inform network administrators how to troubleshoot problems, in addition to providing diagnostics functionality.

Note: See chapter 'Starting the SEM Tool' on page 326 for information on the screen areas of the SEM tool.

39.1 How Can I Assess Overall Voice Quality in my Network?

How can the overall voice quality in my VoIP network be assessed?

➢ **Do one or more of the following:**

1. On the toolbar, click **Networks** to open the Networks view.

   By default, all devices in the network are displayed. By default, data obtained over the past 3 hours is displayed. These defaults can be changed using the filters 'Time Range' and 'Devices'.
2. Glance at the Quality Statistics pie chart in the center of the Preview pane.
   - From the color-coded slices of the pie chart, assess the quality of calls. If the largest slice is green, you can conclude that the majority of calls were Good voice quality (yellow = Fair quality; red = Fail quality).
   - Point your cursor over each slice to open a popup that displays the quality and the # and % of calls associated with this quality category. The callouts display the same statistical information.
3. On the toolbar, click **Networks** to open the Networks view.
4. On the Actions bar, click the Table icon to display the Table view and do the following:
   - Sort according to the # Calls (per device) column.
   - Glance under the adjacent 'Quality' column.
   - From the color-coded bars, assess the quality of calls. If the bars are mostly green, you can conclude that the majority of calls were of Good voice quality (yellow = Fair quality; red = Fail quality).
   - Note the number of devices whose 'Quality' column is indicated as red (for example), and the # Calls made on that device.

5. On the toolbar, click **Statistics** to open the Statistics view.
   - In the Call Quality pane, glance at the quality bar chart, showing distribution over time.
   - From the color-coded bars in the chart, assess the quality of calls made over the network. If the bars are mostly green, you can conclude that most calls were of Good voice quality; yellow = Fair quality; red = Fail quality. Point your cursor over each color to open a popup, which displays quality category, time, # and % of calls classified in this category.

39.2 Why are Calls of 'Fail' Quality Predominantly on one Device?

On one of my devices, I see an abnormally high number of red-coded, Fail-quality calls compared to other devices.

Why? What should be done?

➢ **Do the following:**

1. On the Filter bar, use the Devices filter to isolate the specific device.
2. On the toolbar, click **Statistics** to open the Statistics view.

   This view determines how this device performed over the past 24 hours.
3. See if there's correlation between the distribution of quality (in the Call Quality pane, upper pane) and the distribution of calls (in the Call Quality pane, lower graph). See if there is a correlation between quality and network bandwidth (lowermost window). If you notice a correlation between these distributions, the problem may be caused by network overload.
4. If no correlation is noticeable, verify which voice quality metric most affected Fail quality, by displaying the calls distribution (Call Quality pane, lower graph) according to MOS, Jitter, Delay and then Packet Loss. If you identify a correlation between the distribution of one of these metrics and the quality distribution, you've identified the reason for the high number of Fail-quality calls on the device.
5. On the toolbar, click **Calls List** to open the Calls List view. See if *specific users* aren't causing the problem. Sort the list according to the column 'Call Quality' so that Fail-quality calls are listed first.
6. On the toolbar, click **Alarms** to open the Alarms view to see if any alarms were reported by the device.

39.3 Why Did Performance Deteriorate as Numbers of Calls Increased?

In the Network page it's noticeable that the peak of the status distribution graph is red-coded, indicating a correlation between the distribution of numbers of calls made and the distribution of Failed-status calls.

How can I discover why?

➢ **Do the following:**

1. On the toolbar, click **Calls List** to open the Calls List view.
2. In the 'Search' field, enter the string 'fail'; only calls whose call status is 'Failed' are listed.
3. Sort Failed-status calls according to column 'Device Name' to determine if the peak in the numbers of calls made and Failed-quality calls is related to a specific device.
4. Sort according to columns Caller / Callee and view the calls Termination Reason.
5. If the problem seems related to a specific device, see Section 9.2.

39.4 How Should a New Alarm Be Handled in a Network Recently Free of alarms?

I received a new alarm; however, recently there has been no indication of problems in the network.

How should the new alarm be handled?

➢ **Do the following:**

1. On the toolbar, click **Network** to open the Networks view.
2. In the Alarms pane (the lowermost pane in the Preview pane), identify the source device of the new alarm from the 'Device Name' column.
3. On the Filter pane, use the Devices filter to isolate the device (filter out all other devices).
4. On the toolbar, click **Alarms** to open the Alarms view. View all alarms for the selected device.
5. On the Actions bar, click **History Alarms** to display Historical Alarms. Examine the historical performance of the device. Search for similar / same alarms according to column 'Alarm Name' or any other parameter.
6. Use the Devices filter to view all devices in the network. See if other devices issued similar / same alarms historically. Sort according to the new alarm received. Determine if there was a sequence of alarms similar to / same as the new alarm.

39.5 How Should User Criticism of Voice Quality be Handled?

User **X** does not hear well when talking to User **Y**.

How is the problem diagnosed?

➢ **Do the following:**

1. On the toolbar, click **Call Lists** to open the Call List view.
2. Filter to isolate calls made by User **X**.
3. Click User **X**'s latest call (click the listed call) to open the Call Summary/Call Details window. Open the Call Summary/Call Details window of other calls previously made by User **X** (if any). Determine if the problem is related to *call direction*. Did User **X** originate most calls (caller side) or answer most calls (callee side)? Which calls are problematic (red-coded), those that User **X** originated or those that they answered? Are both legs red-coded or is just User **X**'s leg?
4. Determine whether User **X**'s problem only occurs during phone conversations with User **Y** or if it also occurs during conversations with other users. If problems occur only with calls to User **Y**, view the lower part of the Call Summary/Call Details window to observe the number of calls between User **X** and User **Y** to analyze the problem. Identify the problematic Call Quality metric. If the problem occurs with other users (aside from User **Y)**, determine whether a trend is apparent: Does the problem always occur on the same device? Is it time related?

39.6 Which Users Speak the Most?

I want to know which users speak the most. How's it done?

➢ **Do the following:**

1. On the toolbar, click **Calls List** to open the Calls List view.
2. Sort the list according to the 'Duration' column (primary sort key); longest calls are listed first.
3. Sort the list according to the 'Callee' column (secondary sort key).

39.7 How can Calls Whose Voice Quality Was Classified as 'Fail' be Clarified?

How can calls be clarified whose voice quality was determined as 'Fail'?

➢ **Do the following:**

1. On the toolbar, click **Calls List** to open the Calls List view.
2. Sort the list according to the 'Call Quality' column (red-coded = Fail quality).
3. For each call, open the respective Call Summary / Call Details screen.
4. Determine which metric most influenced the call's quality: MOS / Jitter / Delay or Lost Packets, per caller / callee.
5. Sub-sort the Calls List according to the different metrics columns to determine which metric most impacted upon voice quality.

39.8 How Much Bandwidth is my Network Utilizing?

How can I tell how much bandwidth my network is using?

Is my ISP delivering the promised network speed?

➢ **Do the following:**

1. On the toolbar, click **Statistics** to open the Statistics view.
2. View the Utilization Distribution pane (lowermost pane in the Main screen) displaying bandwidth performance (received and transmitted octets and packets) over time.
3. View the Avg. Utilization pane (the lowermost pane in the Preview pane), displaying a numerical summary of bandwidth performance.
4. On the Filter bar, modify the Time Range filter to observe the distribution of bandwidth performance over different time periods.

Part VI

Security Management

This section describes the security features implemented on the EMS.

40 Overview

EMS Security Management features:

- Network Communication Security (see Section 'Network Communication Security' on page 406).
- 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.

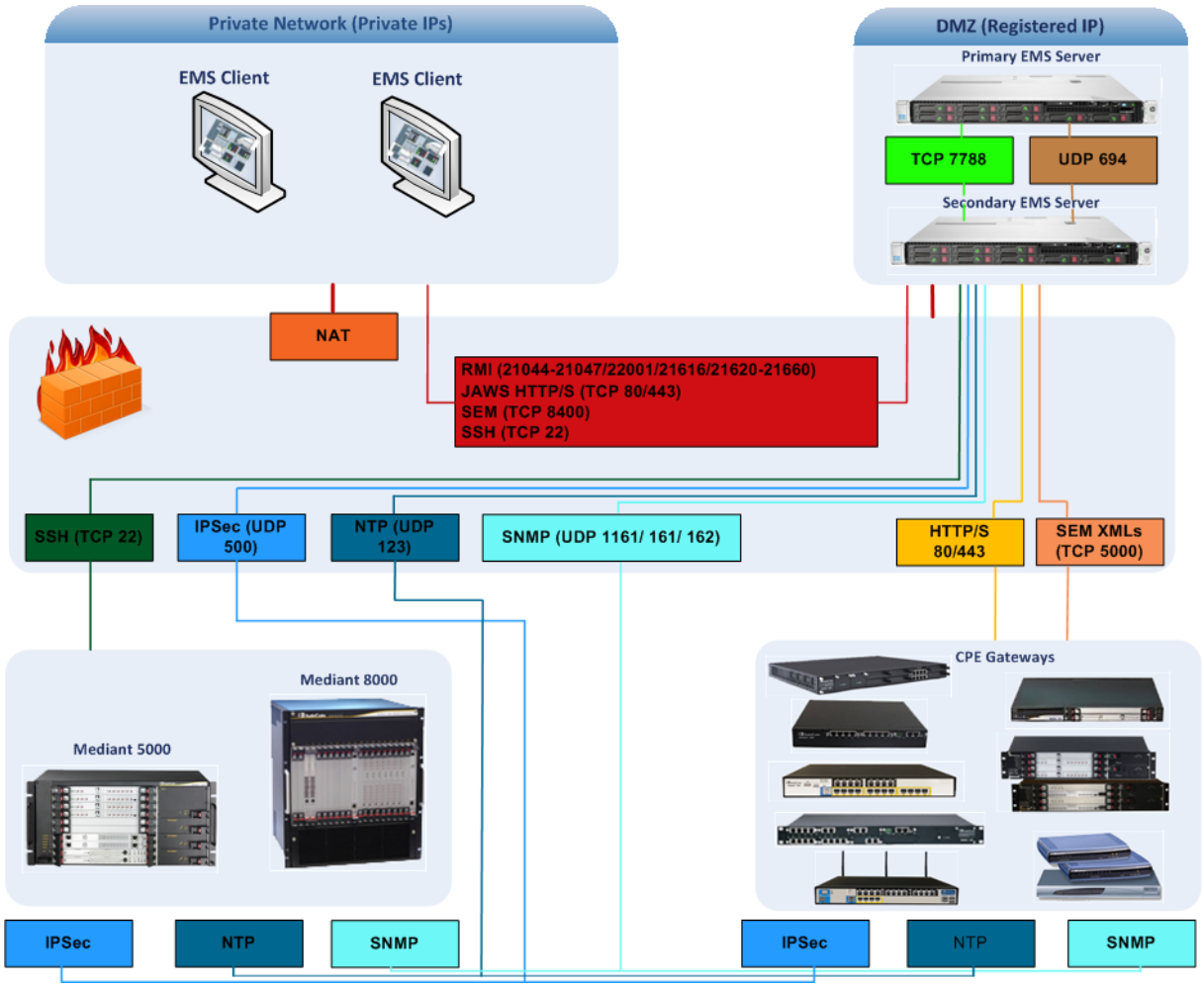
This page is intentionally left blank

41 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 41-1: 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.

41.1 SNMP Management

The SNMP protocol is used for provisioning, maintenance actions, fault and performance management between the EMS Manager and its 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.

41.2 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:

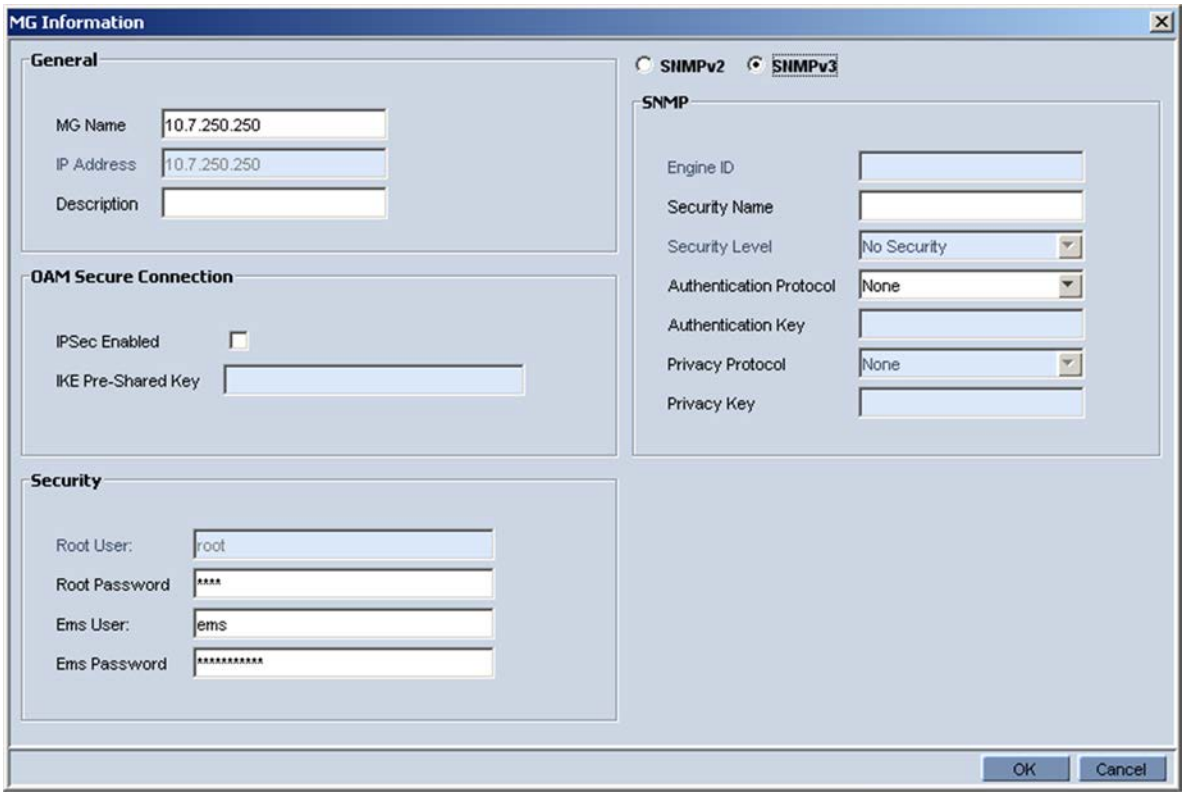
   - It is recommended to select the **IPSec Enabled** checkbox and enter the 'Pre-shared Key' string. This configuration can be performed either during the gateway definition stage or later. The Pre-shared Key string defined in the EMS and in the media gateway must be identical.

   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 41-2: MG Information - Secured Connection Enabled



41.3 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.

41.3.1 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.

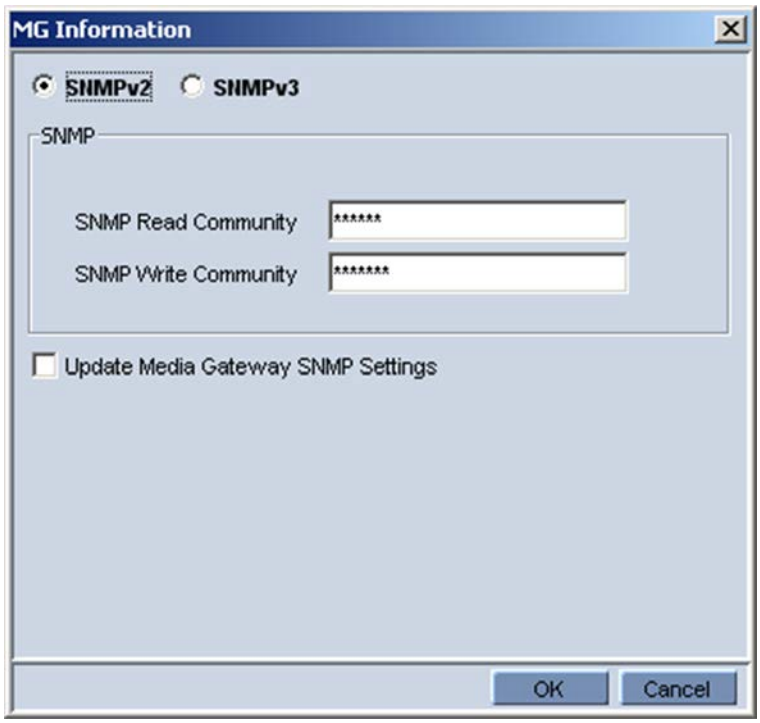
➢ To switch MG & EMS communication from one SNMP version to another via EMS:

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 41-3: MG Information-New SNMPv3 User



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.

41.3.2 Defining (Cloning) SNMPv3 Users

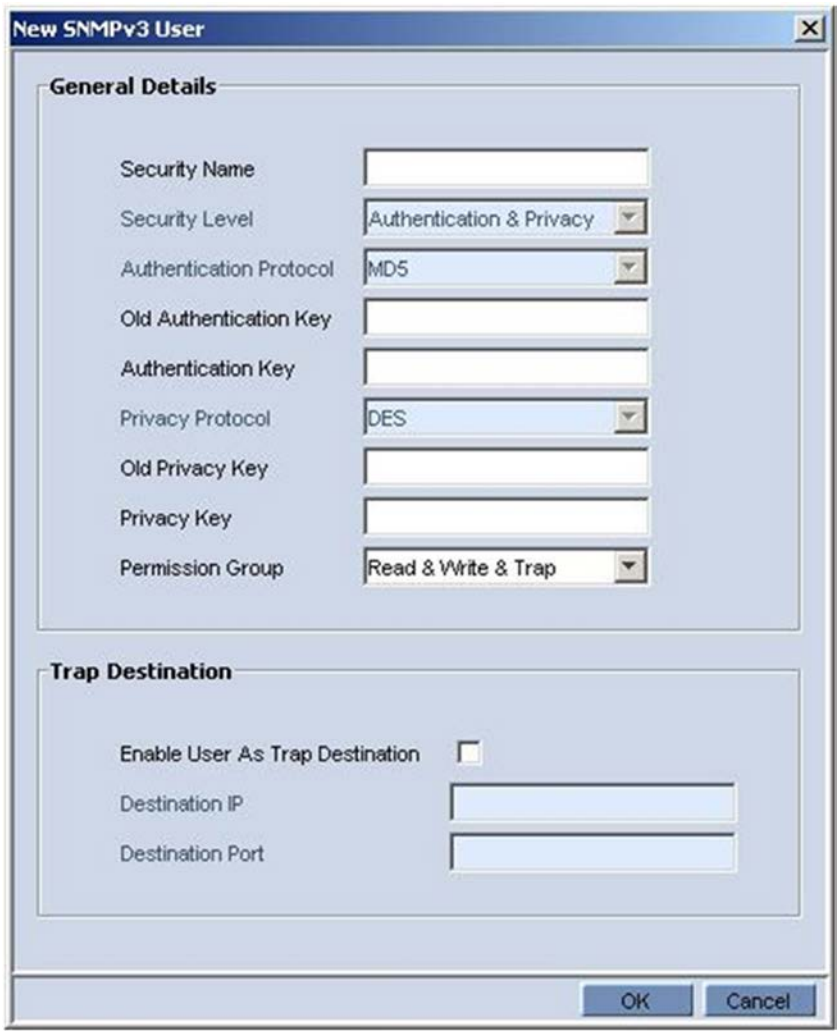
According to the SNMPv3 standard, SNMPv3 users on the SNMP Agent (on the media gateway) cannot be directly added via the SNMP protocol e.g. SNMP Manager (EMS). Instead new users must be defined via User Cloning. The SNMP Manager then creates a new user according to the original user permission levels.

➢ **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 41-4: MG Information Screen-New SNMPv3 User



41.3.3 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 41-5: Securing Communication

2. For CPE products, check the **Secured HTTP Enabled HTTPS** option if required.

41.3.4 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**.

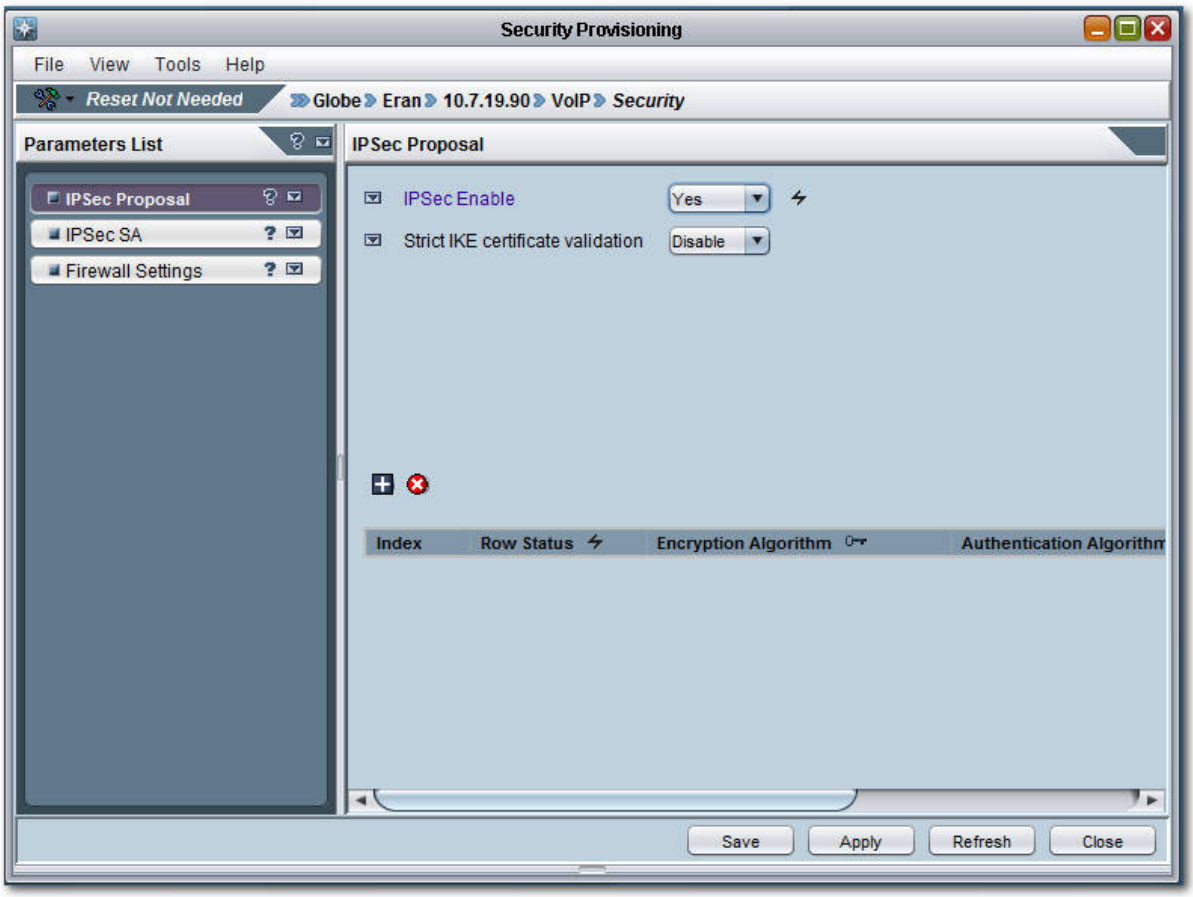
41.3.5 Configuring IPsec

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 41-6:Security Provisioning



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 41-7: IPsec SA Configuration

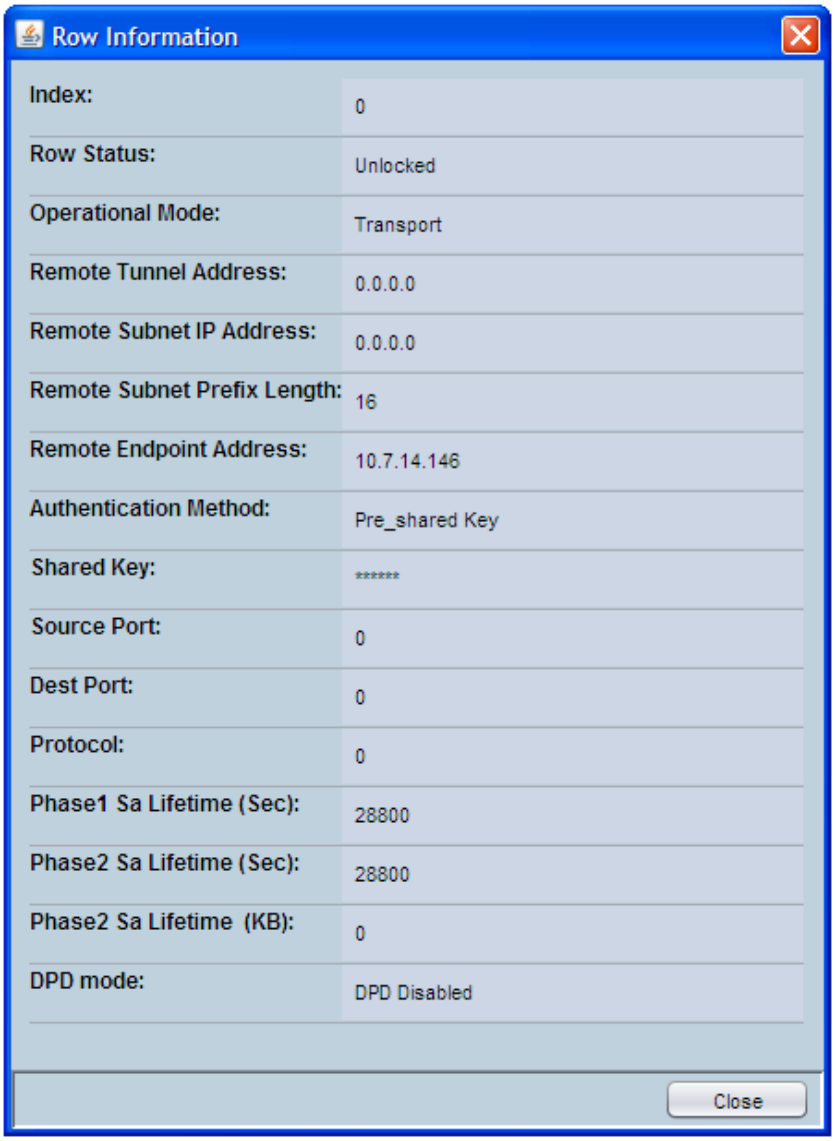
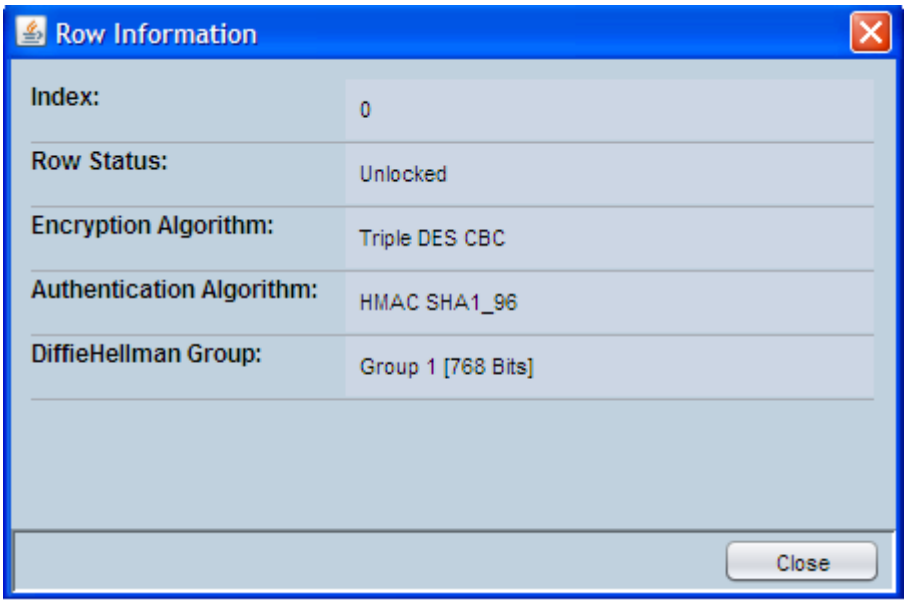
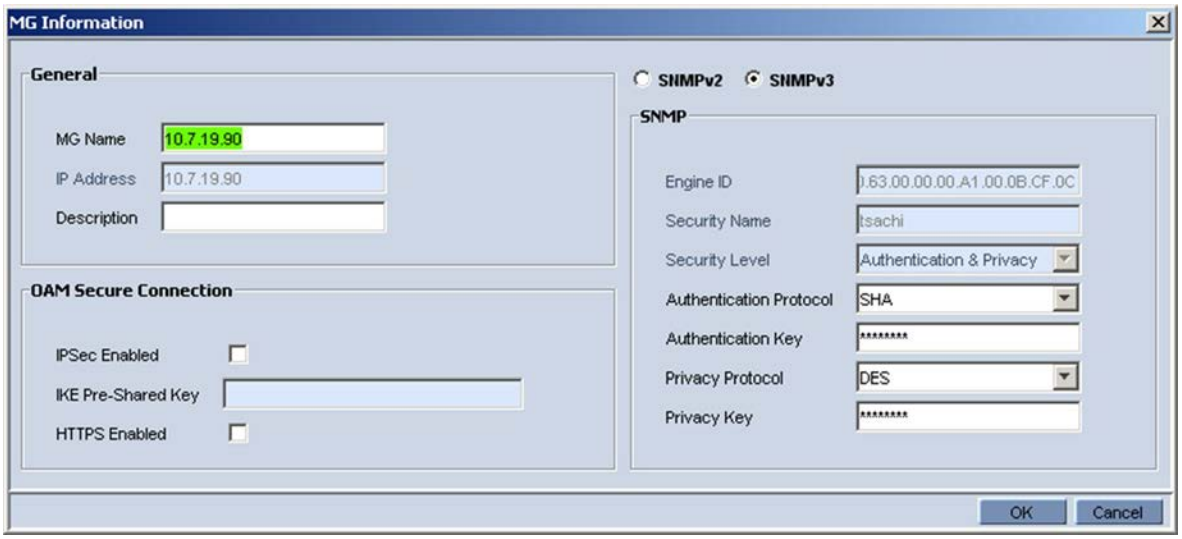


Figure 41-8: IPsec Proposal Configuration



5. Open the screen 'MG Information' (right-click the device in the **MGs List** and choose **Details**).

Figure 41-9: Securing Communication



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 453 to resolve the issue).

41.3.6 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 41-10: Maintenance Action: Generate X.509 Files

The Generate X.509 Files dialog is displayed.

Figure 41-11: Generating a CSR Request

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.

41.3.7 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 to the Software Manager prior to configuring them in the media gateway. For more information, see 'Software Manager' on page 61.

41.3.8 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.

42 EMS Application Security

EMS Operator's Authentication and Authorization can be performed using either local EMS users management tools, or using a centralized RADIUS or TACACS+ Server. By default, the EMS application manages its users in the local EMS server.

In both cases, the user can identify themselves by typing Login & Password or using Common Access Card (CAC) card. The CAC is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard and eligible contractor personnel.

The CAC is used as a general 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 alternative to entering the EMS username and password.

You can determine whether to use local or RADIUS / TACACS+ EMS User Management in the Security menu, 'Authentication and Authorization' window. In addition, this window enables you to set the EMS users Authentication parameters.

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 disrupted 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.

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. Actions Journal screen can be accessed from the Main Screen in the Security menu, option 'Actions Journal'.

42.1 Centralized EMS Users Authentication and Authorization via a RADIUS or TACACS+ Servers

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*.

Figure 42-1: RADIUS Authentication and Authorization

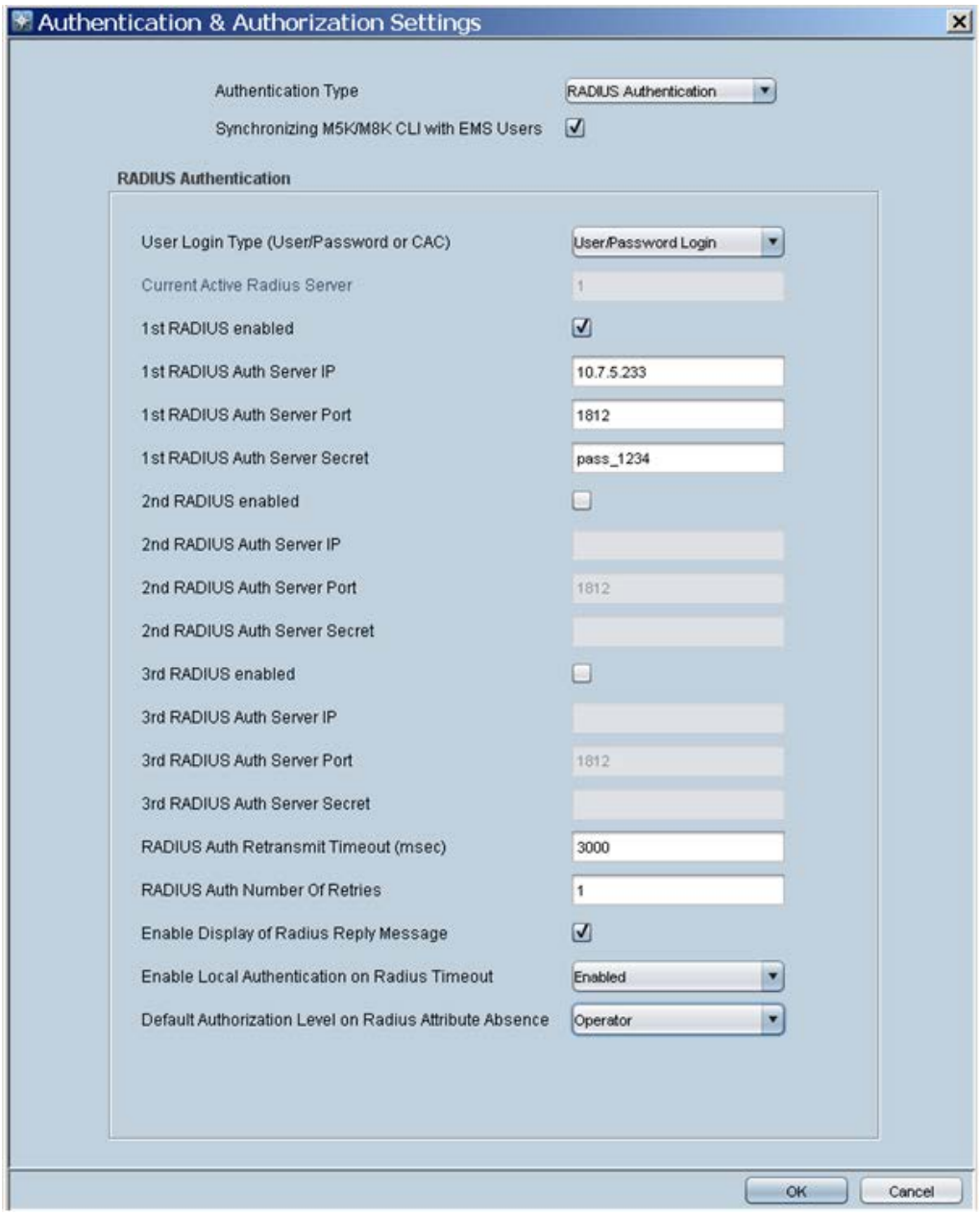
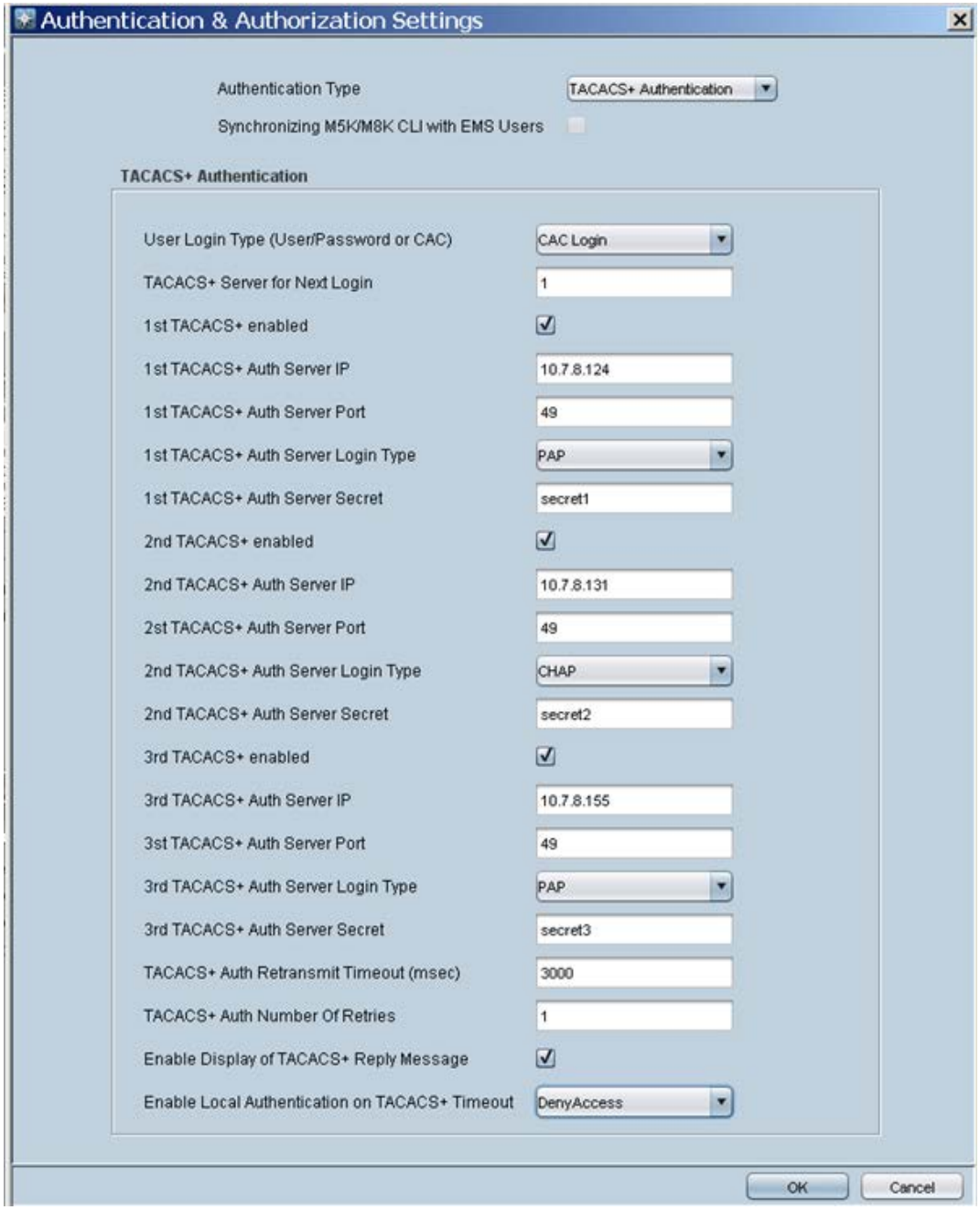


Figure 42-2: TACACS Authentication and Authorization



42.2 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.

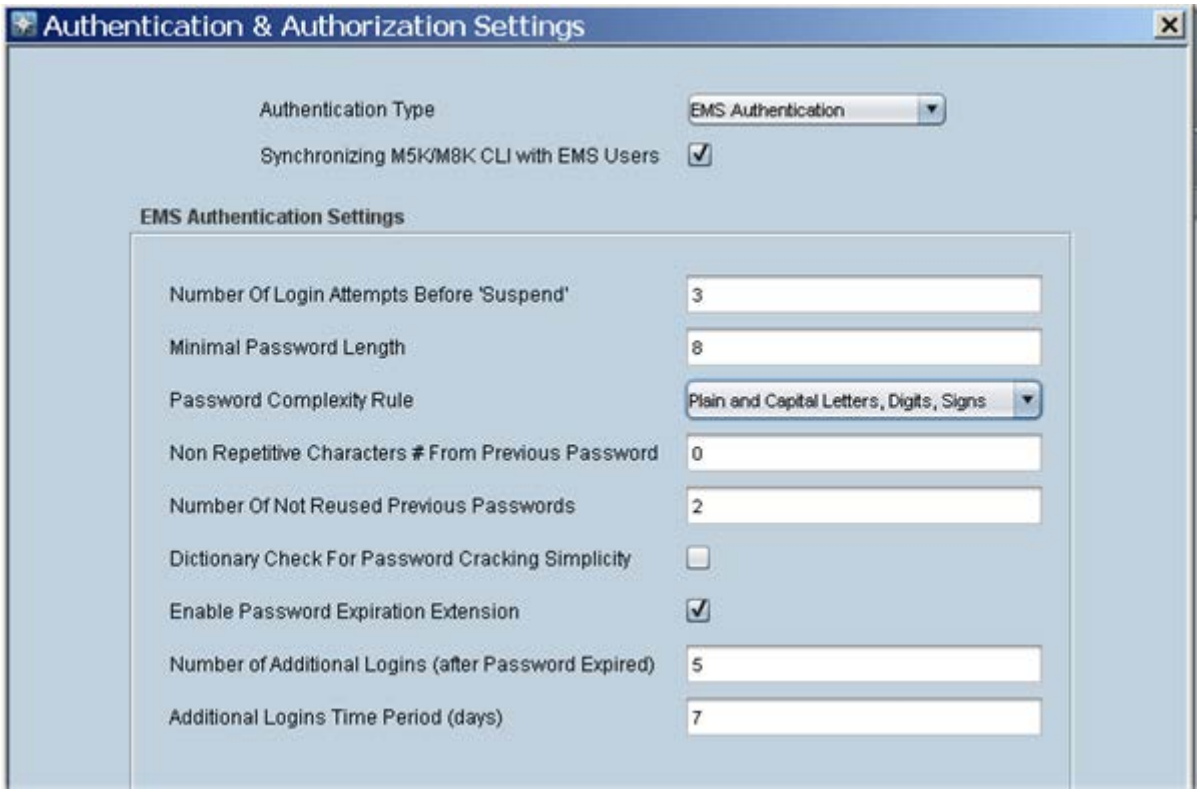
42.2.1 Provisioning Users

This section describes how to provision EMS users via the EMS.

➢ To provision EMS users via the EMS:

1. In the Main EMS menu, choose **Security** ▶ **Authentication and Authorization**.
2. Set the 'Authentication Type' field to **EMS Authentication**.

Figure 42-3: EMS Authentication Settings



42.2.2 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.

42.2.3 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.

42.2.4 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.

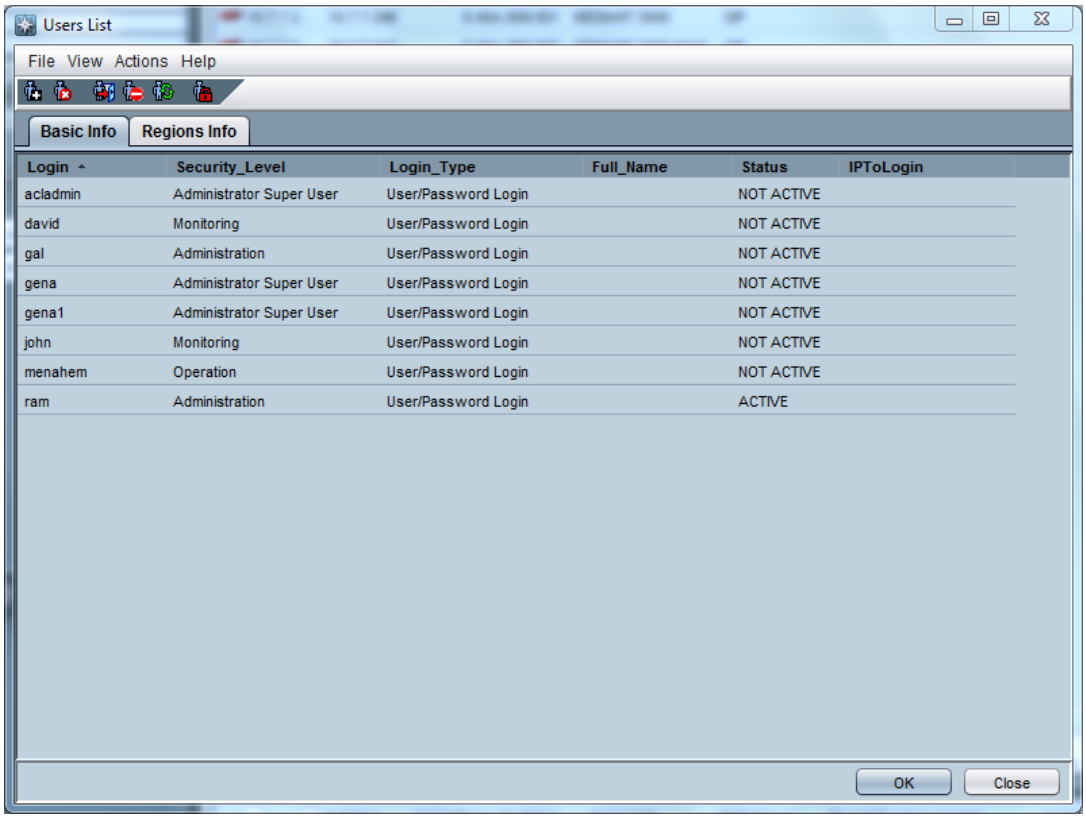
42.3 Managing the Users List

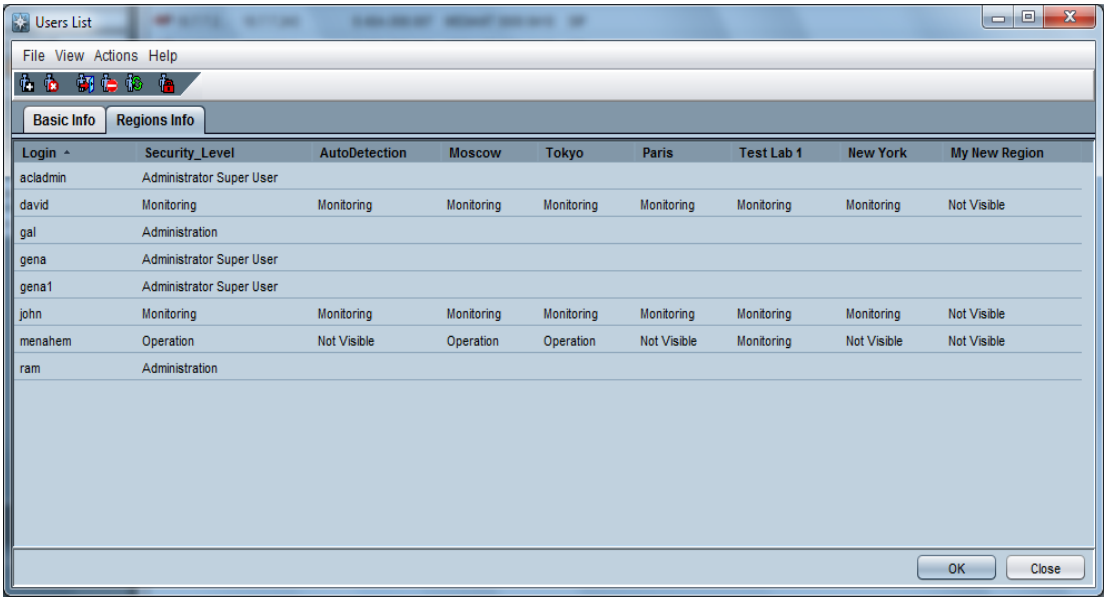
This section describes how to access the EMS Users list. User security level can be defined either per entire application or per Region.

To open the Users List:

- In the EMS Main menu, choose **Security** ▶ **Users List** ; the Users List screen opens:

Figure 42-4: Users List




Users List
File View Actions Help
Basic Info
Regions Info
Login
Security_Level
AutoDetection
Moscow
Tokyo
Paris
Test Lab 1
New York
My New Region
acladmin Administrator Super User
david Monitoring Monitoring Monitoring Monitoring Monitoring Monitoring Monitoring Not Visible
gal Administration
gena Administrator Super User
gena1 Administrator Super User
john Monitoring Monitoring Monitoring Monitoring Monitoring Monitoring Monitoring Not Visible
menahem Operation Not Visible Operation Operation Not Visible Monitoring Not Visible Not Visible
ram Administration
OK
Close

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.

42.3.1 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 42-5: User Details screen - Basic Info

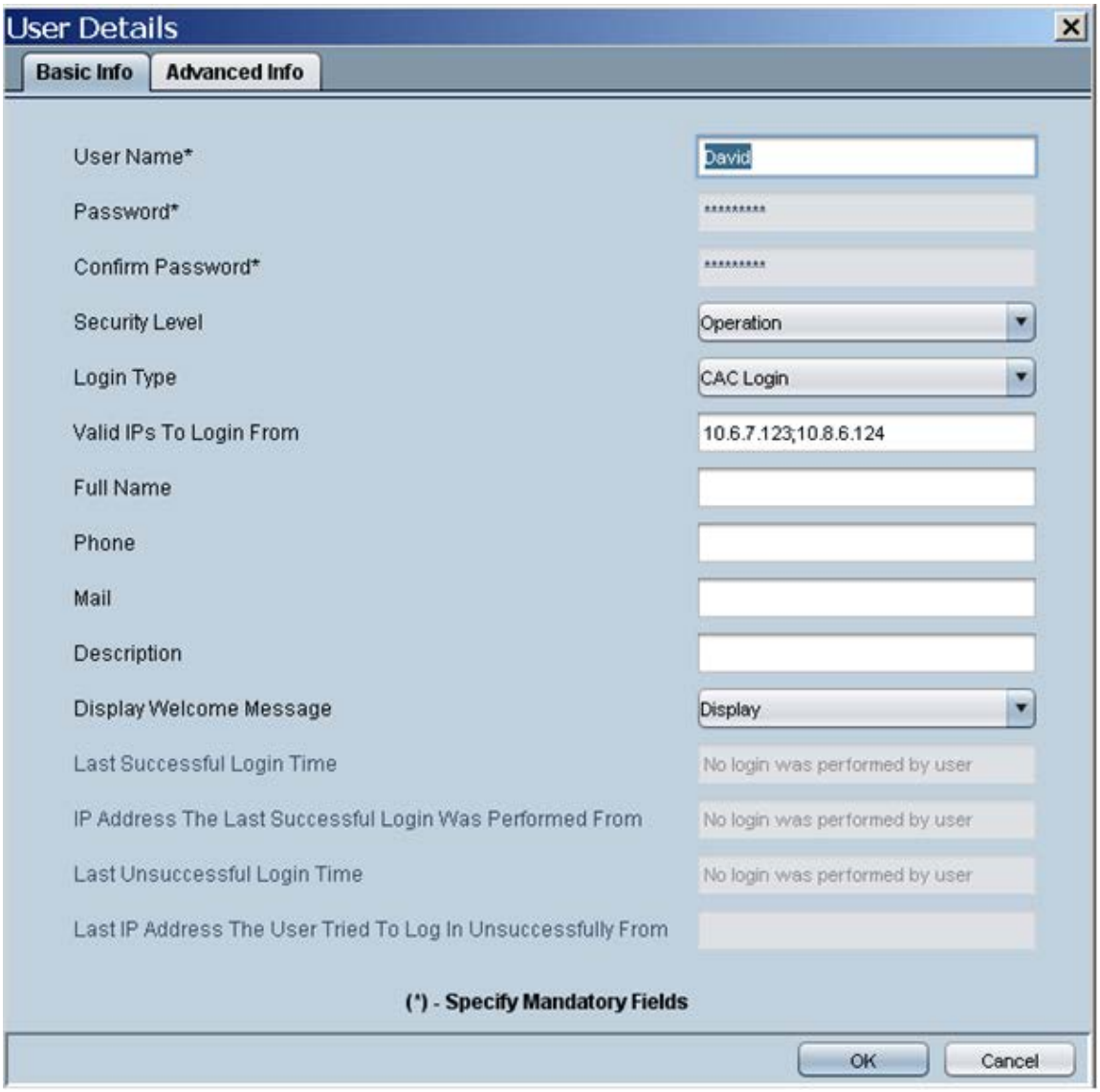
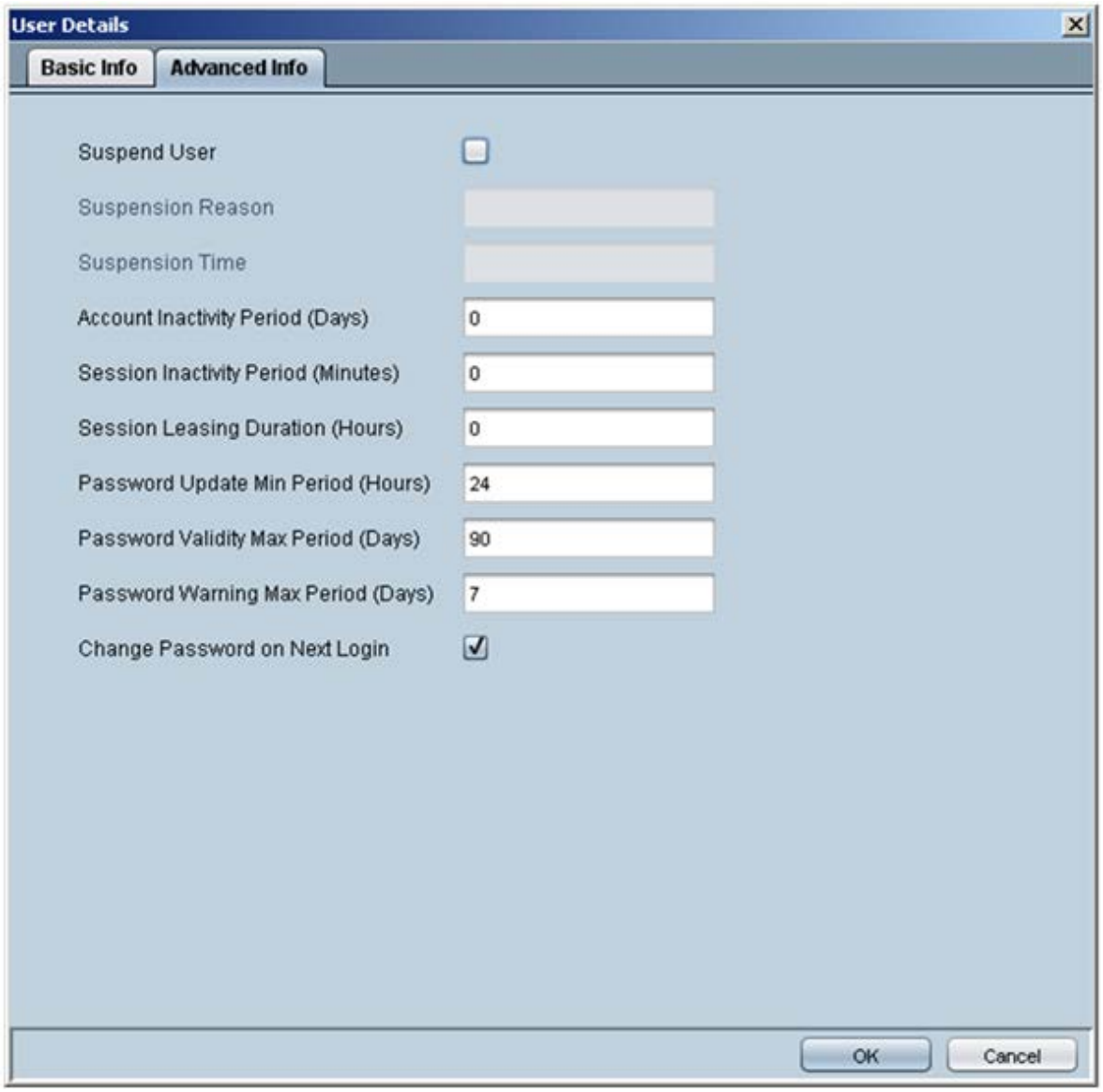


Figure 42-6: User Details screen - Advanced Info



- 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 405, 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.

42.3.1.1 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.

42.3.1.2 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 42-1: 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.

42.3.1.3 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.

42.3.1.4 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:

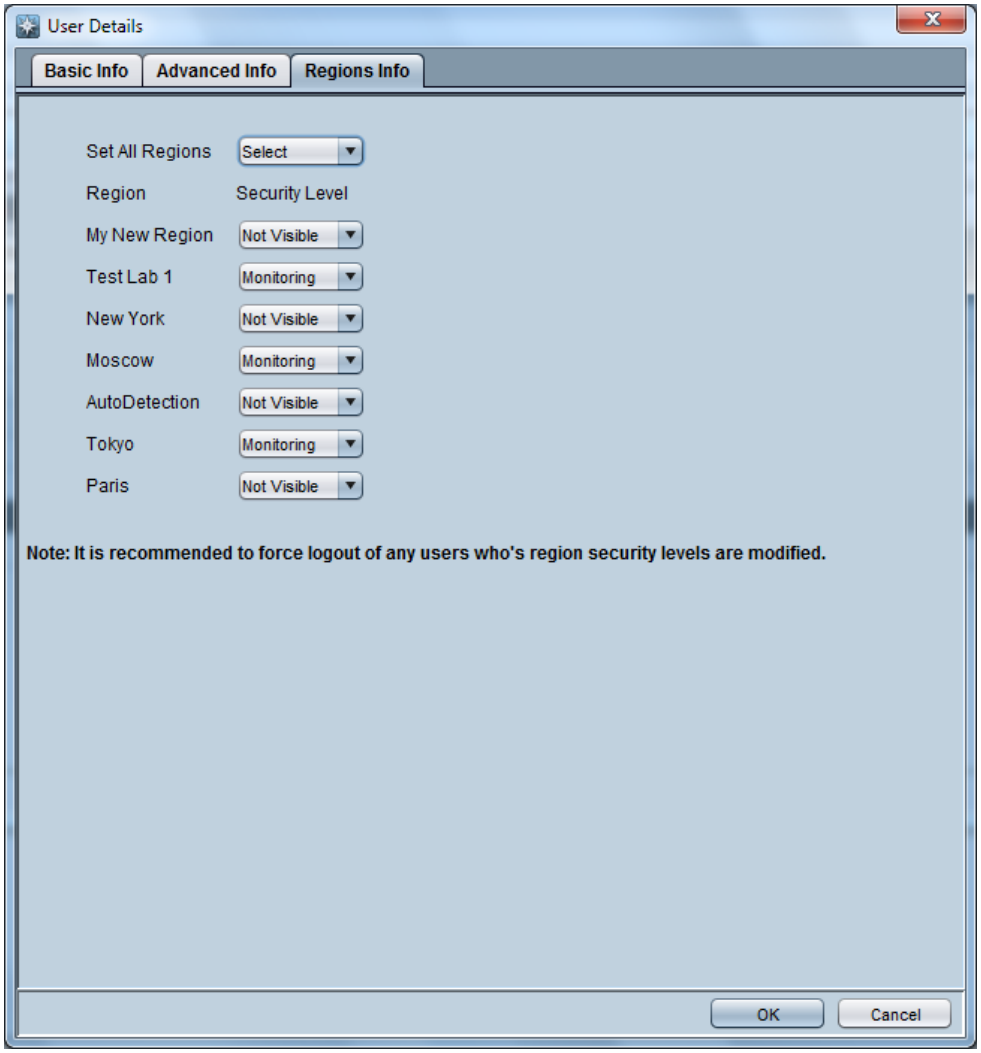
  - Users Management – view, define, edit users and user permissions. Perform actions related to the Users.
  - View Users Actions Journal
  - Perform Software and / or Auxiliary Files definition in the Software Manager (while the download to the gateway can be performed also by Regional Users)
  - Add / 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 42-7: User Details - Regions Info



42.3.2 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 429) 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.

42.3.2.1 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.

42.3.2.2 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.

42.3.2.3 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.

42.3.2.4 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.

42.3.2.5 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.

42.3.2.6 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 42-8: Change Password

2. Change the password previously defined in the Password field.

This page is intentionally left blank

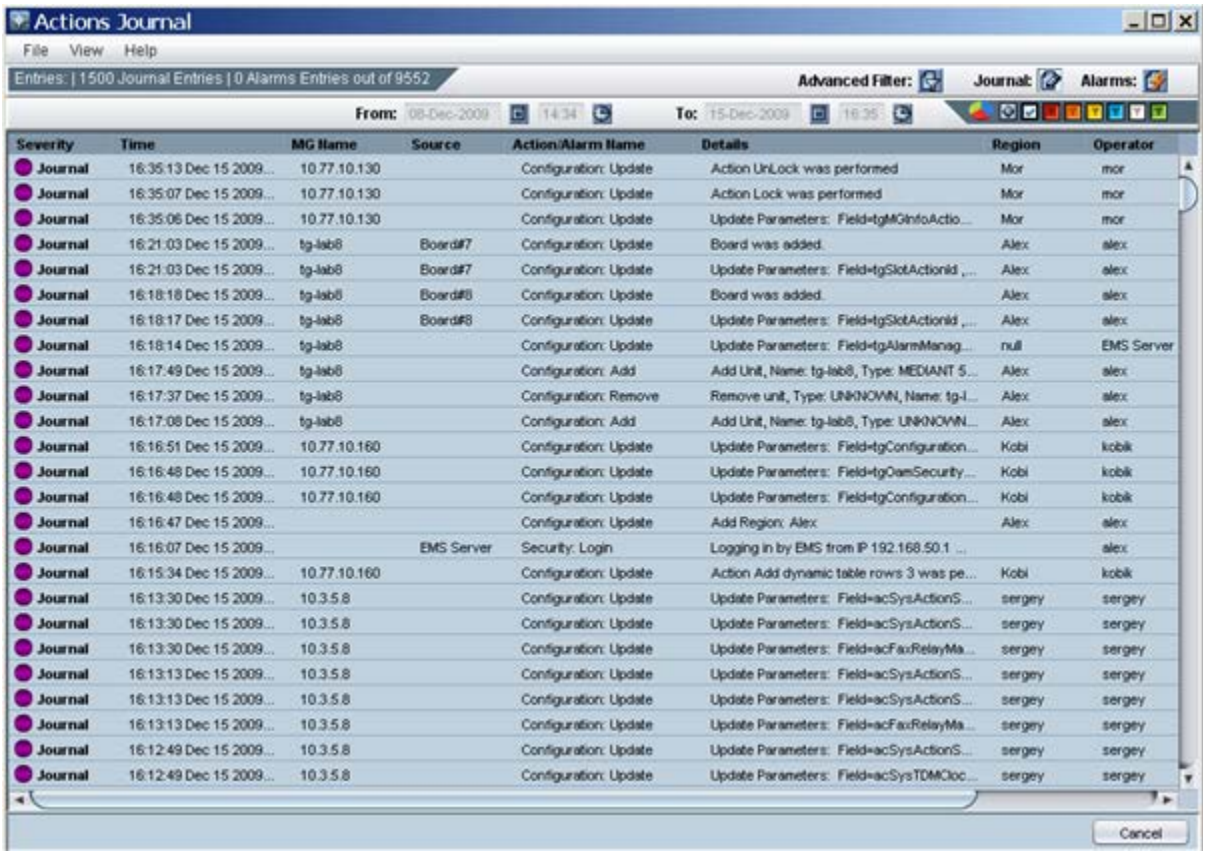
43 Viewing Operator Actions in the Actions Journal

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 43-1: Alarms Journal



- 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 43-2: Journal Actions

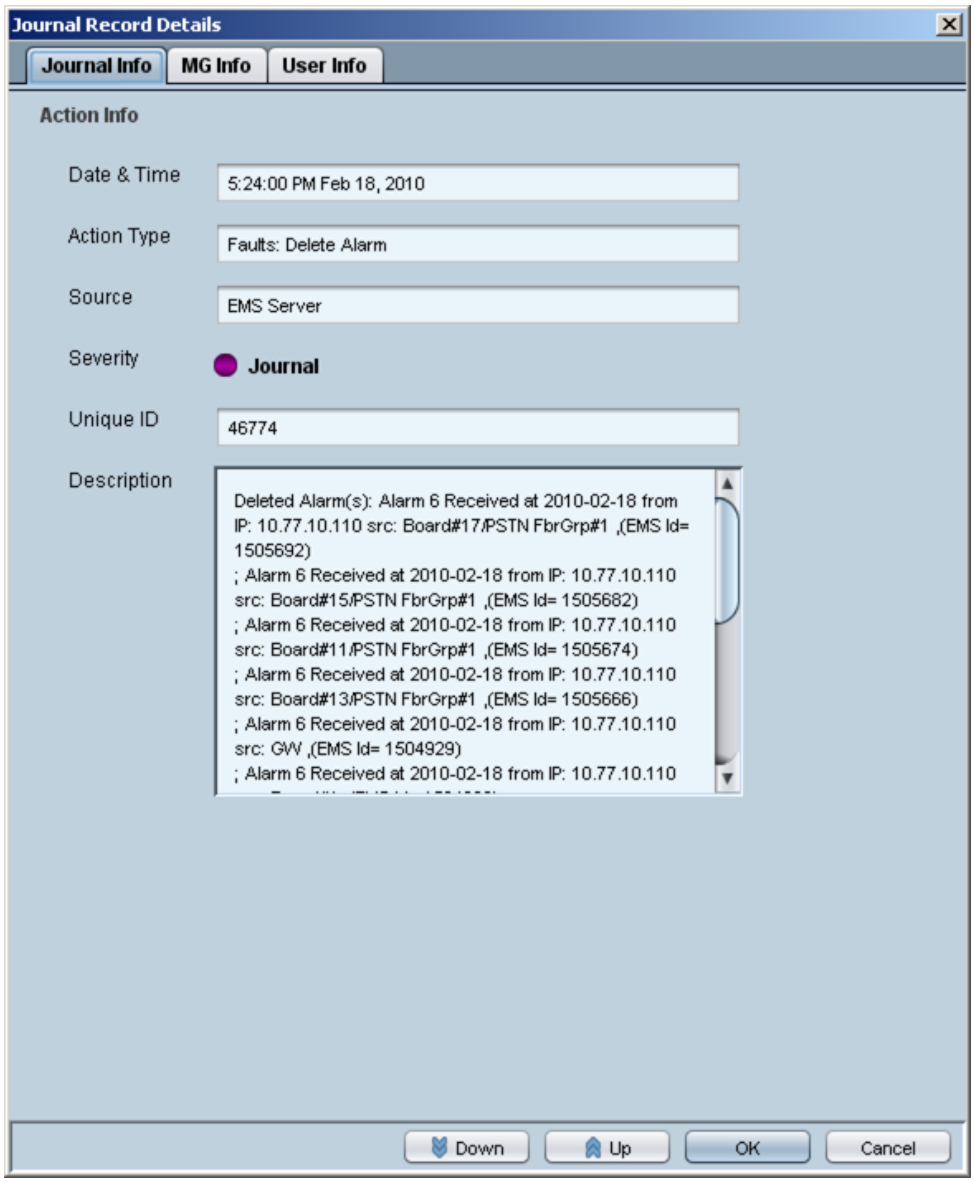
- **Details** - a precisely detailed description of the action, for example, parameter names and values for a Configuration Update action.
- **Operator** - the name of the operator who performed the action.
- **Region** - the region in which the gateway resides.

43.1 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:

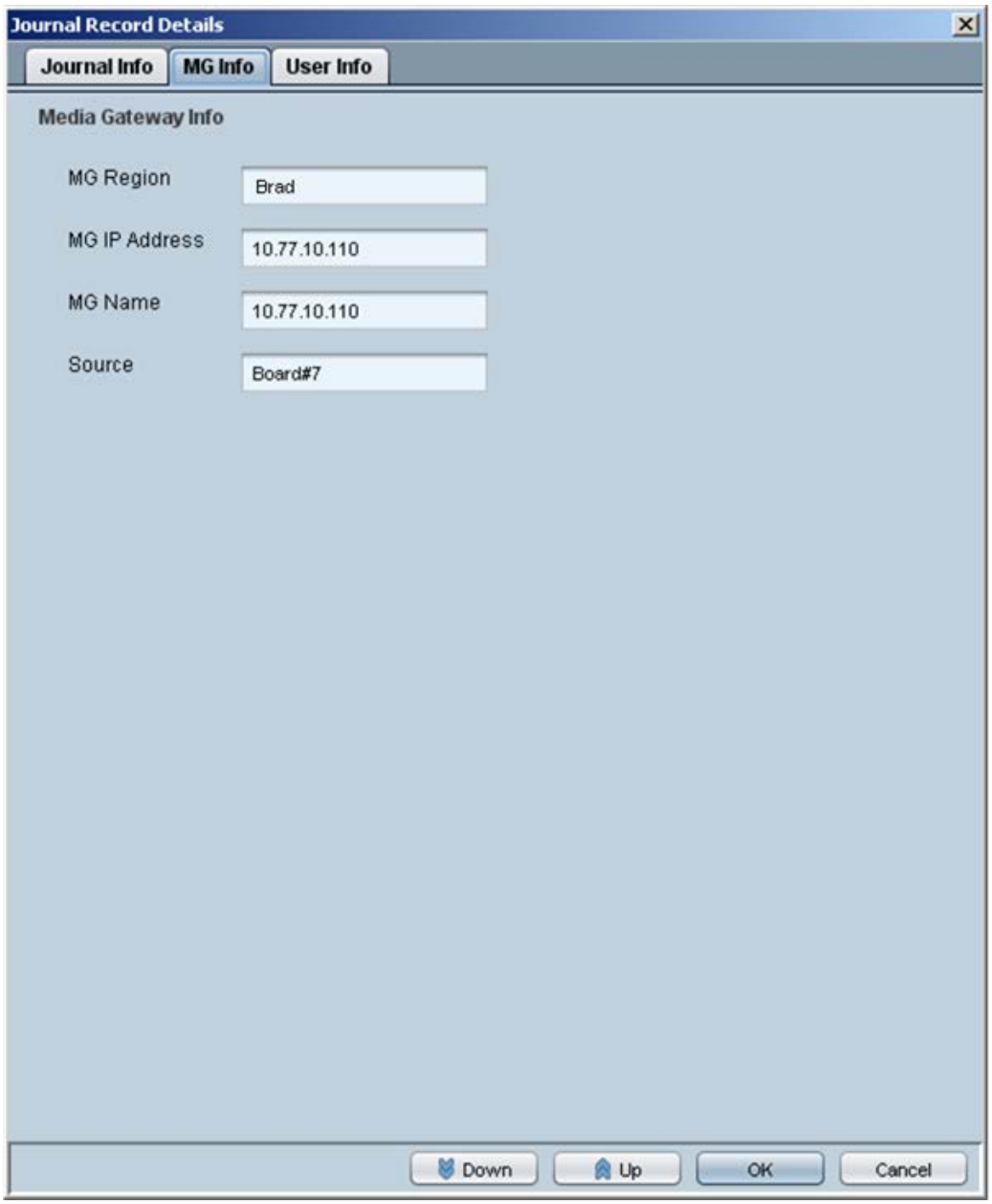
- Journal Info

Figure 43-3: Journal Record Details - Journal Information



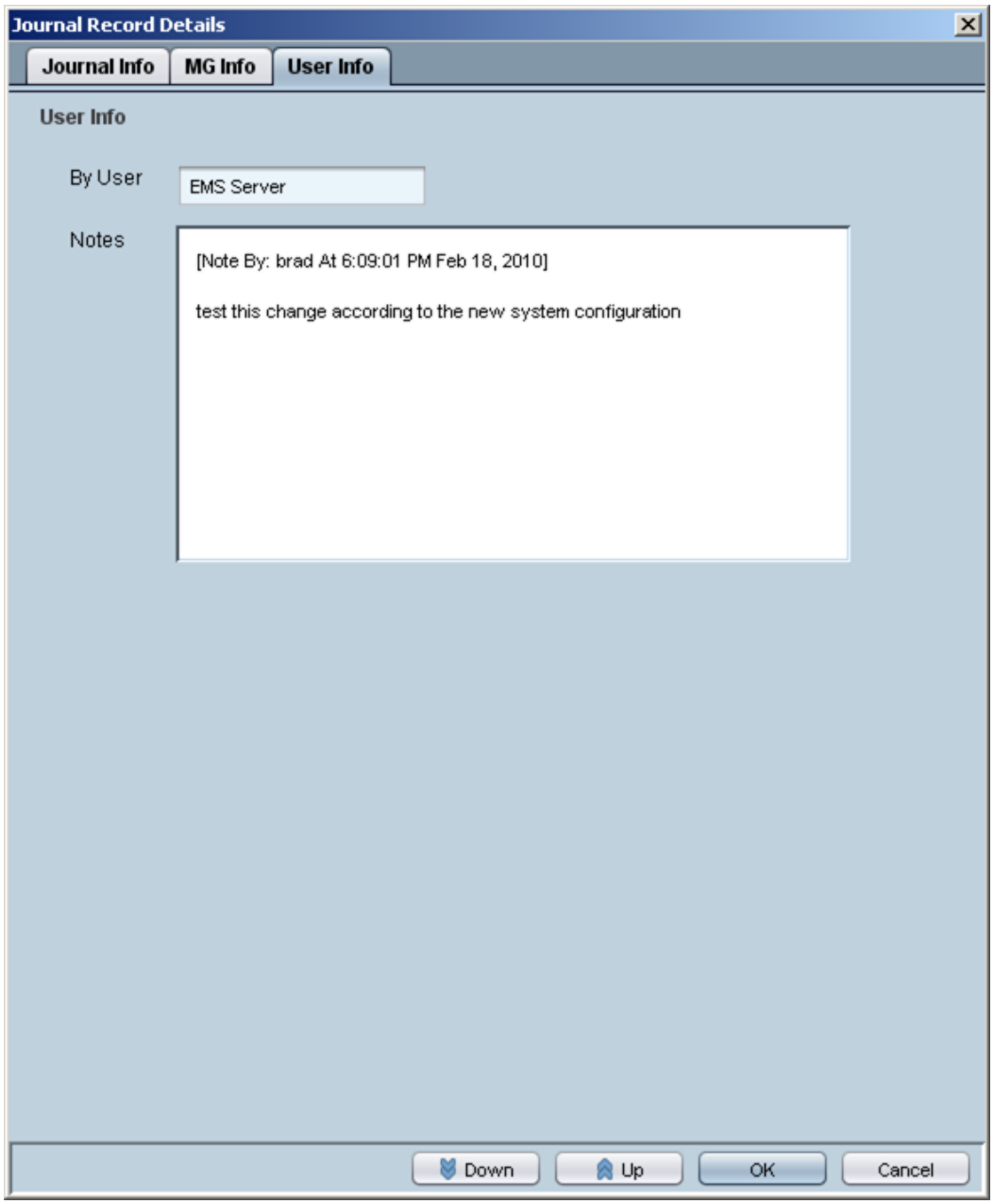
- MG Info

Figure 43-4: Journal Record Details - Media Gateway Information



- User Info

Figure 43-5: Journal Record Details - User Info

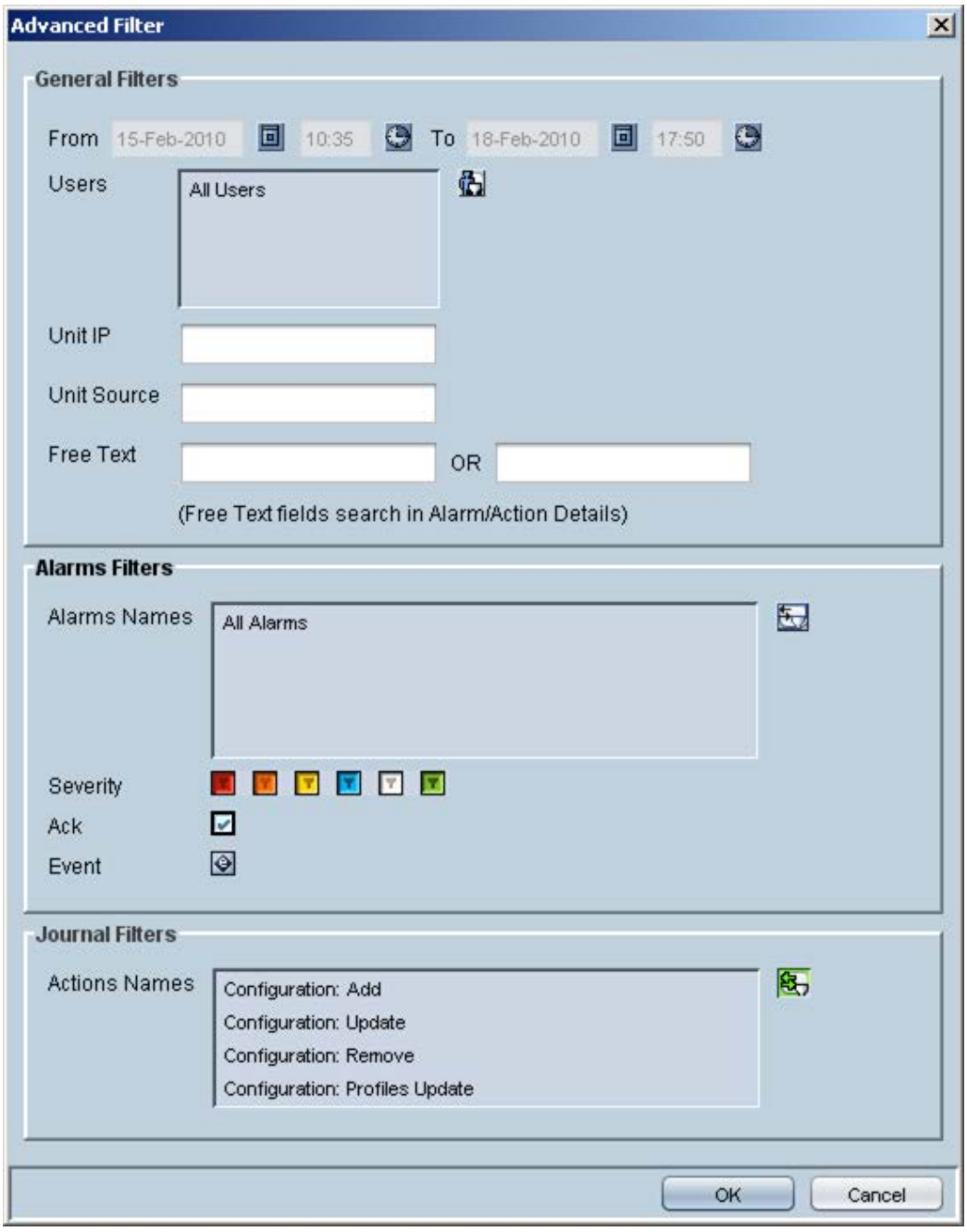


Users can insert data to be saved, together with the journal record in the Journal.

43.2 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 43-6: Filters



- **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 253)
- **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)

43.2.1 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.

43.3 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).

44 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 welcome 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 44-1: Welcome Message Settings

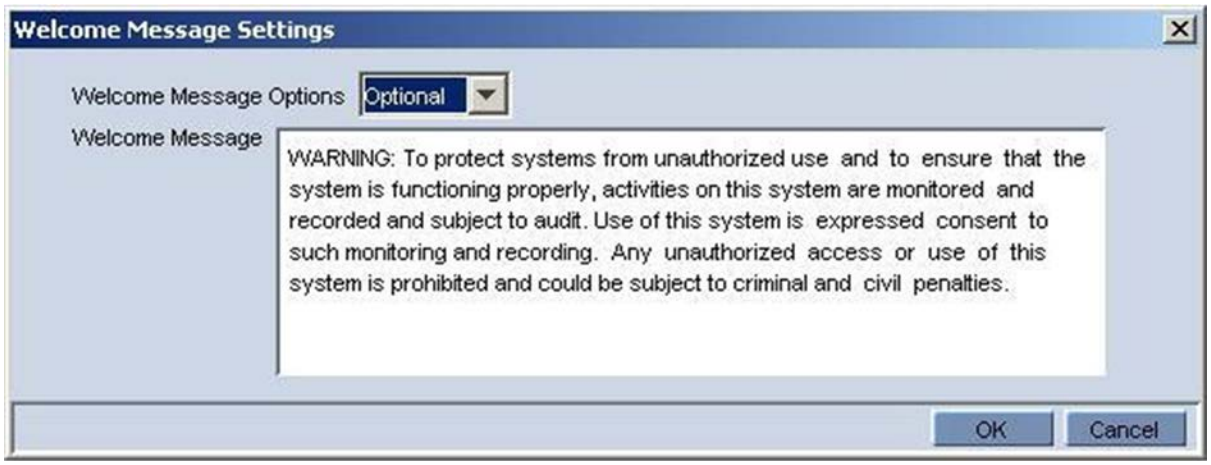
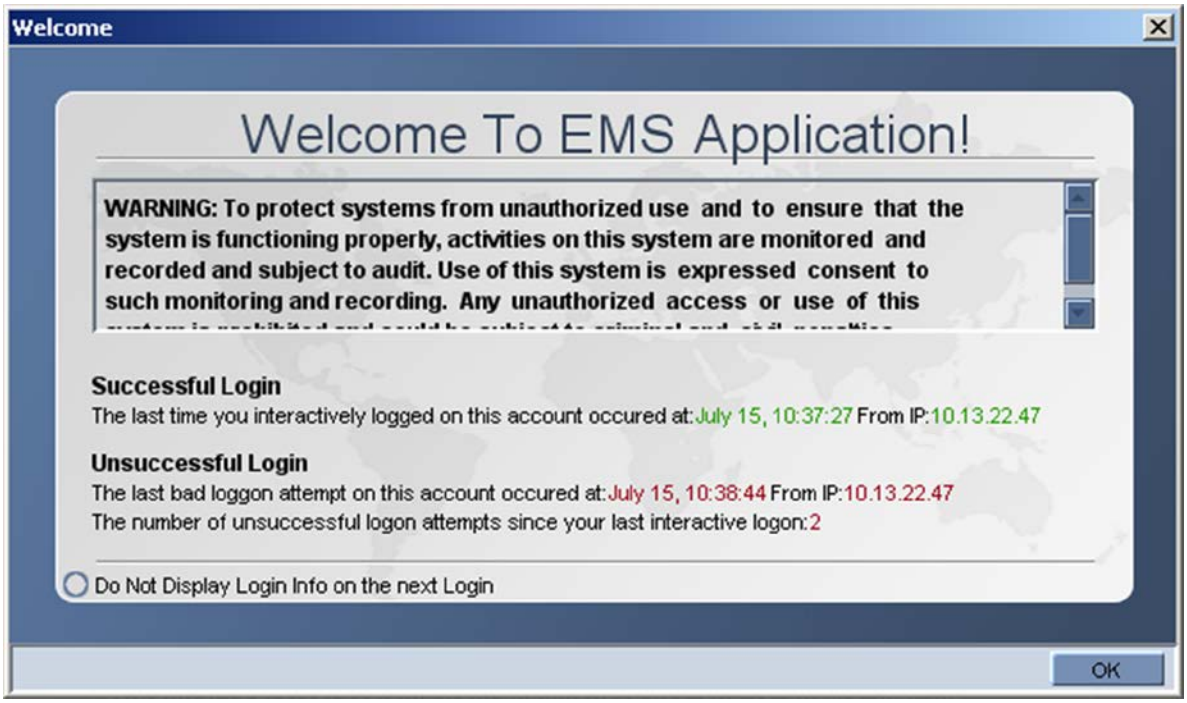


Figure 44-2: Welcome Message with Login Information



Part VII

Troubleshooting

This section describes the various EMS troubleshooting scenarios.

45 Failure to Connect to a Media Gateway - all MGs

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:

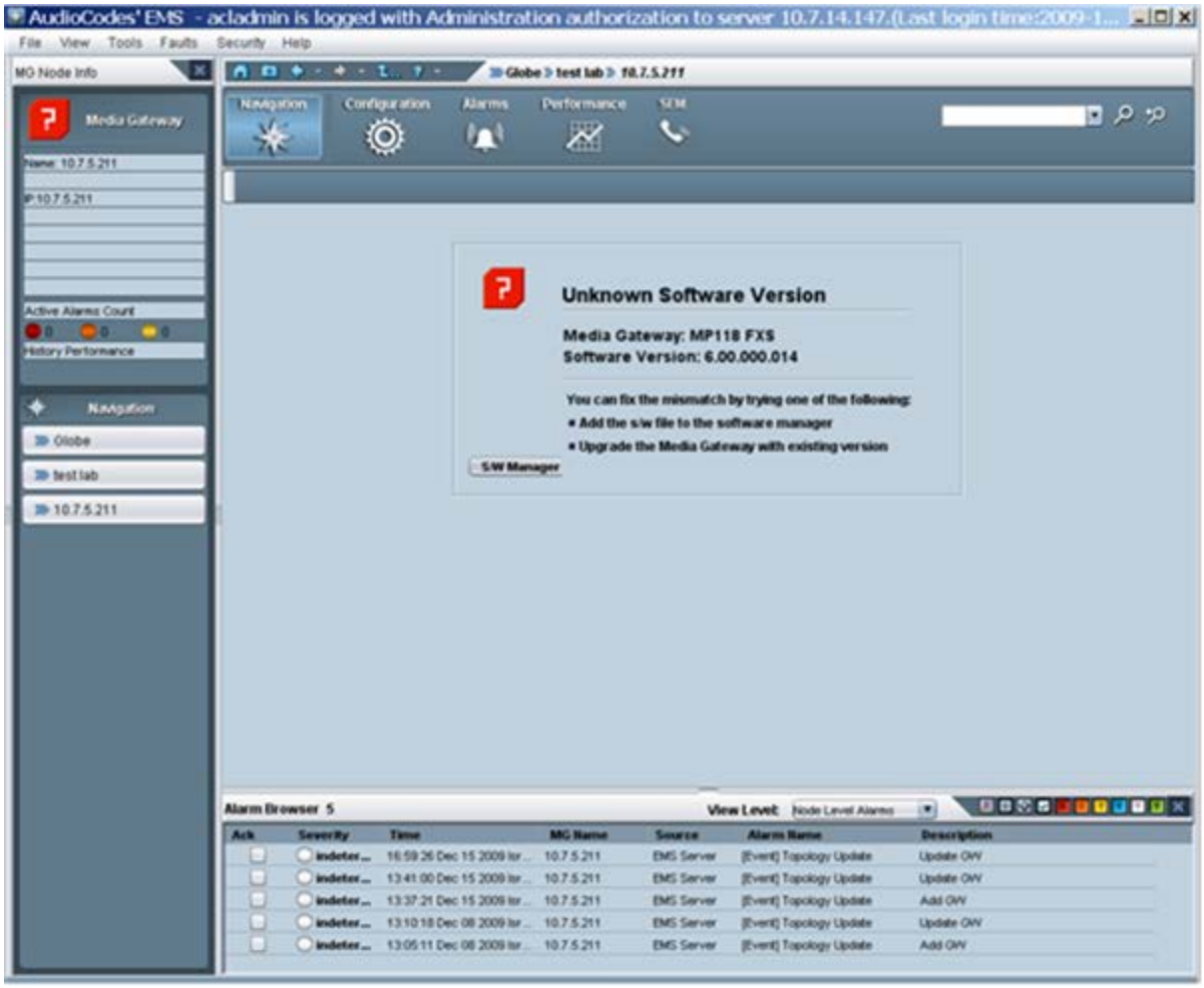
1. You've incorrectly defined the IP address of the media gateway you're attempting to connect to (in the MG Information screen; see the figure 'Incorrectly Defined MG Information Screen', below).
2. An operational problem exists in the system (lack of communication with the server, for example).
3. 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 45-1: 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 73). 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 45-1: Incorrectly Defined MG Information Screen



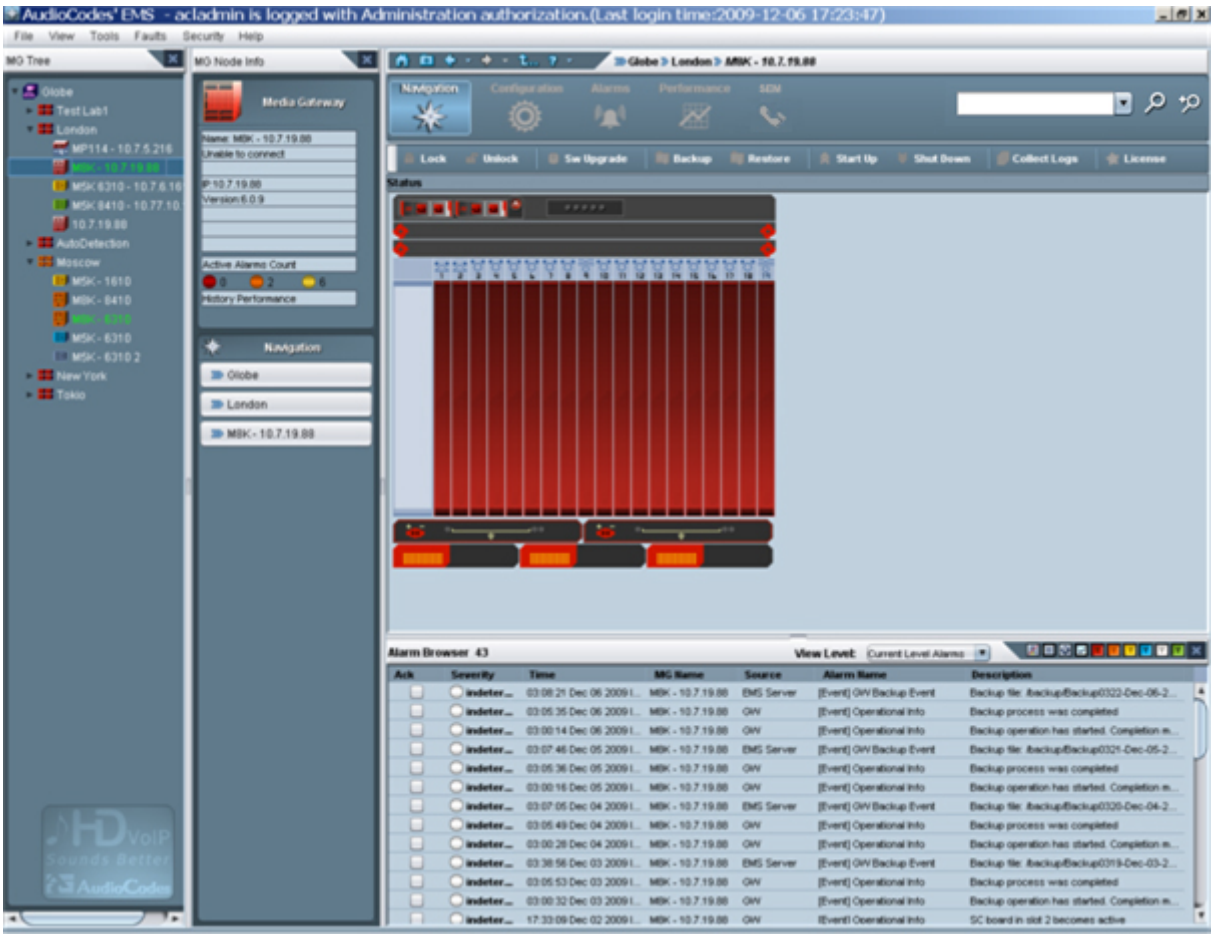
45.1 Failure to Reconnect to a Previously-Connected Media Gateway whose Operation was Interrupted

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 45-2: Failure to Reconnect to a Media Gateway Whose Operation was Interrupted



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 45-2: 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.

45.2 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

46 Index

A

B

C

D

E

F

G

H

I

L

M

Q

R

S

T

U

V

W

This page is intentionally left blank

EMS for AudioCodes Media Gateways and Servers

EMS Element Management System

User's Manual

Version 6.6

AudioCodes

www.audiocodes.com