AudioCodes One Voice Operations Center

Element Management System (EMS)

User's Manual

Version 7.0

AudioCodes

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank.

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.

Date Published: August-23-2015

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

Abbreviations and Terminology

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

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

Documentation Feedback

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

Related Documentation

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

This page is intentionally left blank.

1 Introducing the AudioCodes Element Management System

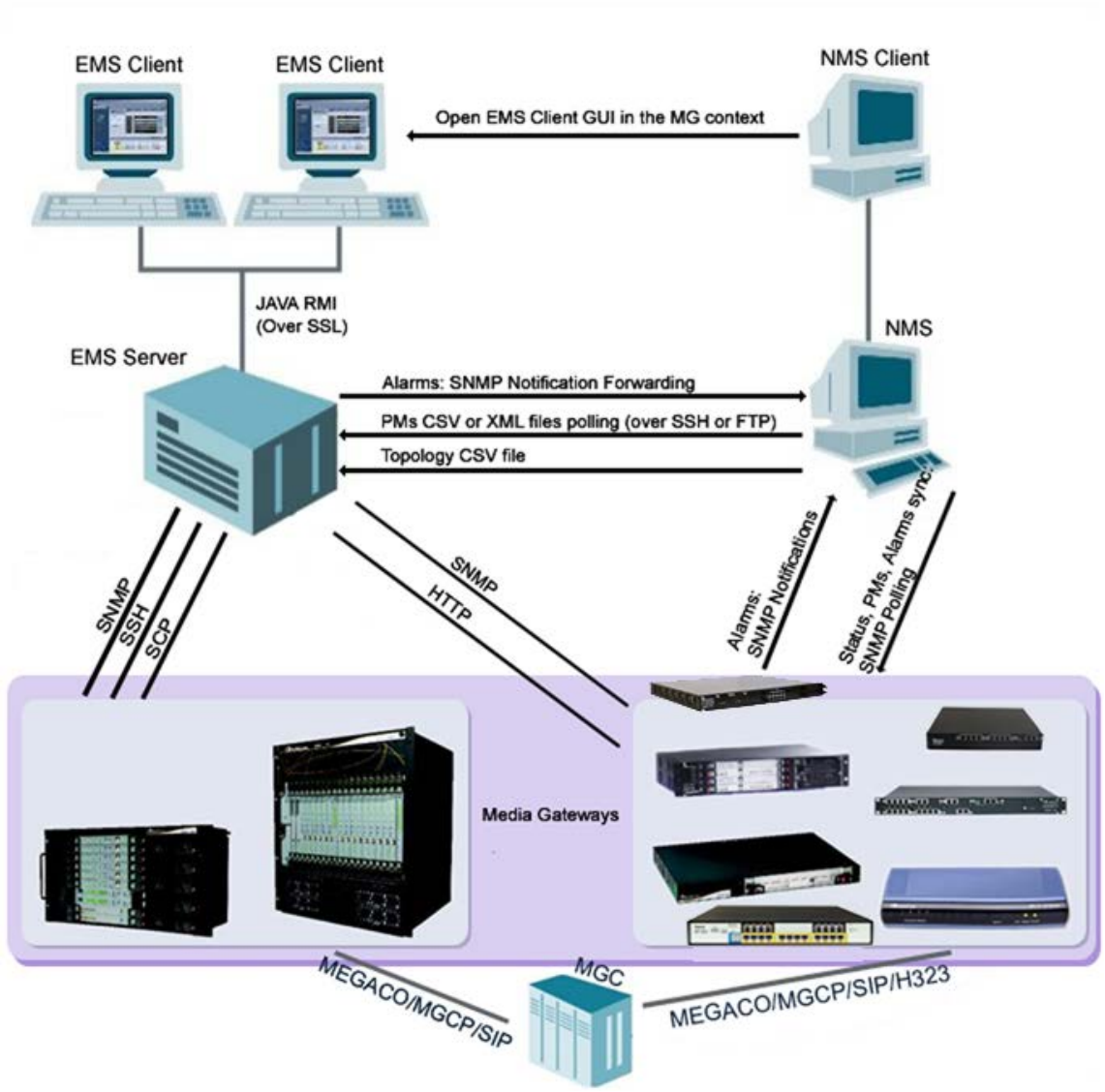
The Element Management System (EMS) is an advanced solution for standards-based management of multiple devices within VoIP networks. This management covers all areas vital for the efficient operation, administration, and management of the AudioCodes' families of devices, including analog VoIP Media Gateways, Multi-Service Business Routers (MSBRs) and Session Border Controllers (SBCs). Additionally, Endpoints (IP Phones) can also be managed by the EMS.

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

The standards-compliant EMS for devices uses distributed SNMP-based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a f eature-rich management framework, including fault management and security. Additionally, the REST protocol is implemented between the EMS and Endpoints (IP Phones).

The figure below shows the EMS integrated in a network system.

Figure 1-1: EMS Integrated in a Network System



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

1.1 Feature Specifications

- Software Version Number: **7.0**
- Release Date: **Q3 2015**
- 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 devices (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 devices 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
Devices 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 devices. A Summary of all managed devices' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.

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 devices 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 – device communication is secured using SNMPv2c/SNMPv3, HTTP/HTTPS, Telnet, SSH and SCP. **Application Security** User Management using a RADIUS, TACACS+ and LDAP server for centralized user authentication and Authorization or using 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.
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.
Devices Maintenance Actions	Mediant 8000 and Mediant 5000: ▪ Online software upgrade via a Wizard ▪ Gateway installation, startup and shutdown ▪ All maintenance actions (lock, unlock, switchover, add / remove board, etc.) for each device, 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 devices. ▪ Actions (such as Lock / Unlock, Reset, Configuration Download, Upload, etc.) can be performed to the set of devices.

Table 1-2: User Interface and External Interfaces Specifications

Subject	Description
User Access Control	Local EMS application or centralized RADIUS, TACACS+ and LDAP user's 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, REST, SSH, SCP, NTP
Multi-Platform	Java-based, JDK version 1.8
Relational Database	Oracle *11g* relational database is used for data storage.

1.2 Supported VoIP Equipment

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

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **MediaPack**	These analog VoIP devices incorporate up to 24 analog ports to be connected either directly to an enterprise PBX (FXO), to phones, or to fax (FXS), supporting up to 24 simultaneous VoIP calls. (Refer to the product documentation for detailed information.)
 **Mediant 500 E-SBC**	The Mediant 500 Enterprise Session Border Controller (E-SBC), hereafter referred to as *the device*, is a member of AudioCodes family of E-SBCs, enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device provides voice-over-IP (VoIP) SBC functionality. The device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 500 MSBR**  **Mediant 500L MSBR**  **Mediant 800 MSBR**  **Mediant 1000 MSBR**	These Multi-Service Business Routers (MSBR) are networking devices that combine multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server. The device's Stand Alone Survivability (SAS) functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX. The devices also provide an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing. (Refer to the specific product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 1000 Media Gateway**	The Mediant 1000 Media Gateway is a convergence platform integrating an enterprise's data and telephony (voice/fax) communications providing a cost-effective, cutting-edge technology solution with superior voice quality and optimized packet voice streaming (voice, fax and data traffic) over the IP network. Designed to interface between TDM and IP networks in enterprises as well as in small-scale carrier locations, the Mediant 1000 Media Gateway supports multiple analog and digital modules with a variety in the number of spans, as well as mixed digital and analog configurations. The device supports up to 4 digital trunks (fully flexibile), from a single trunk per module all the way to a single module with all 4 trunks) or as a purely analog configuration, supporting up to 24 analog ports (6 modules with 4 ports on each).
 **Mediant 600 Media Gateway**	The Mediant 600 Media Gateway supports multiple analog and digital modules with a variety in the number of spans, as well as mixed digital and analog configurations. The device supports up to 2 E1/T1/J1 spans (including fractional E1/T1); up to 8 ISDN Basic Rate Interface (BRI) interfaces; up to four FXO interfaces (RJ-11 ports) - for connecting analog lines of an enterprise's PBX or the PSTN to the IP network; up to 4 FXS interfaces (RJ-11 ports) - for connecting legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS interfaces can be connected to the external trunk lines of a PBX. (Refer to the product documentation for detailed information.)

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 2000 Media Gateway**	The Mediant 2000 Media Gateway contains the TP-1610 cPCI VoIP communication board, an ideal building block for deploying high-density, high availability Voice over IP (VoIP) and wireless enterprise systems. The Mediant 2000 incorporates 2, 4, 8 or 16 E1 or T1 spans for connection, either directly to PSTN telephony trunks, or to an enterprise PBX, and two 10/100 Base-T Ethernet ports for redundant connection to the LAN. (Refer to the product documentation for detailed information).
 **Mediant 500 Enterprise Session Border Controller (E-SBC)**	The Mediant 500 Enterprise Session Border Controller (E-SBC), hereafter referred to as *the device*, is a member of AudioCodes family of E-SBCs, enabling connectivity and security between small medium businesses (SMB) and service providers' VoIP networks. The device provides voice-over-IP (VoIP) SBC functionality. The device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.

Table 1-3: Supported VoIP Equipment

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

Table 1-3: Supported VoIP Equipment

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

Table 1-3: Supported VoIP Equipment

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

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 5000 Media Gateway**	The Mediant 5000 is the medium-sized member of the family of market-ready, standards-compliant, device 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 devices, IP-Centrex devices, VoP Access devices Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; VoiceCoders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall-back to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1, SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP (Refer to the product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 **Mediant 8000 Media Gateway**	The Mediant 8000 is the large-scale member of the family of market-ready, standards-compliant Media Gateway Voice Network products designed for the carrier environment. The Mediant 8000 reliability features include N+1 redundancy for Media Gateway boards, external interface redundancy and 1+1 redundancy for common equipment. The density of the device 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 devices, IP Centrex devices, VoP Access devices **Selected Specifications**: Up to 7,200 independent, simultaneous LBR VoP to PSTN voice calls; Voice coders include G.711, G.723.1, G.726, G.728, G.729A, Independent dynamic vocoder selection per channel; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall back to G.711 analog, fax and modem support; Call progress tones, VAD, CNG, Dynamic programmable jitter buffer, Modem detection, DTMF detection and generation. (Refer to the product documentation for detailed information).

Table 1-3: Supported VoIP Equipment

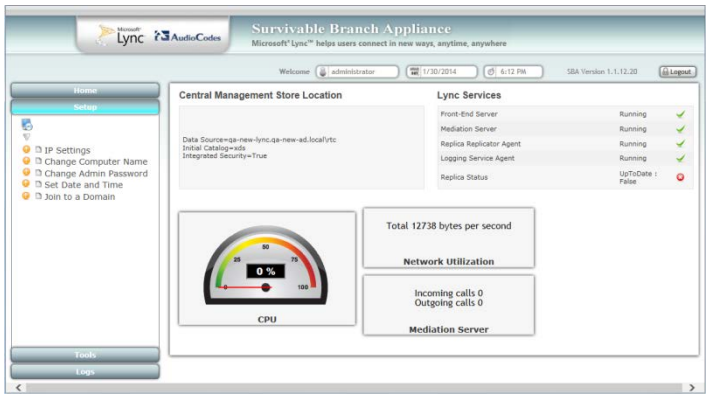
Supported VoIP Equipment	Description
 **Mediant 9000 SBC**	AudioCodes Mediant 9000 Session Border Controller is a highly scalable Session Border Controller (SBC) designed for deployment in large enterprise and contact center locations and as an access SBC for service provider environments. The Mediant 9000 is a high-capacity SBC, supporting thousands of concurrent sessions and extensive SIP connectivity with wide-ranging interoperability, enhanced perimeter defense against cyber-attacks, and advanced voice quality monitoring. The device also supports active/standby (1+1) redundancy (High Availability) by employing two devices in the network. The device offers branch survivability during WAN failure, ensuring call service continuity.
Survivable Branch Appliance (SBA) 	The Survivable Branch Appliance (SBA) is an AudioCodes product designed for Microsoft Lync Server which allows remote branch resiliency in a Microsoft Lync Server network (Microsoft Lync Server 2010 and Microsoft Lync Server 2013). The AudioCodes SBA resides on the OSN server platform of the Mediant 800B and the Mediant 1000B running on a Microsoft Windows 2008 Telco R2 operating system. In the EMS, the SBA is displayed as a module of the Mediant 800B and the Mediant 1000B devices. When you add either of these platforms to the EMS, there is an option to enable the SBA module. The SBA module has a separate IP address and FQDN Name.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
	AudioCodes AudioCodes ' 420HD 430HD and 440HD IPPhones are based on AudioCodes' High Definition voice technology, providing clarity and a rich audio experience in Voice-over-IP (VoIP) calls. All models include a large monochrome multi-language graphic LCD display The phones provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, etc. Phone models support both Microsoft Lync and non-Lync environments.

1.3 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.

1.3.1 Versatile System

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

1.3.2 FCAPS

The EMS supports FCAPS functionality:

- 'Fault management' on page 269
- 'Configuration management' on page 73
- Accounting (managed by a higher-level management system such as an NMS)
- 'Performance Management' on page 315
- 'Security Management' on page 341

1.3.3 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.

1.3.4 Private Labeling

Private labeling enables you to customize and label the EMS and devices, according to their customer specific requirements. The private labeling feature enables telephone companies to use the EMS under their own corporate name, device 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 devices, and the names of the TP boards populating the devices.
- 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.

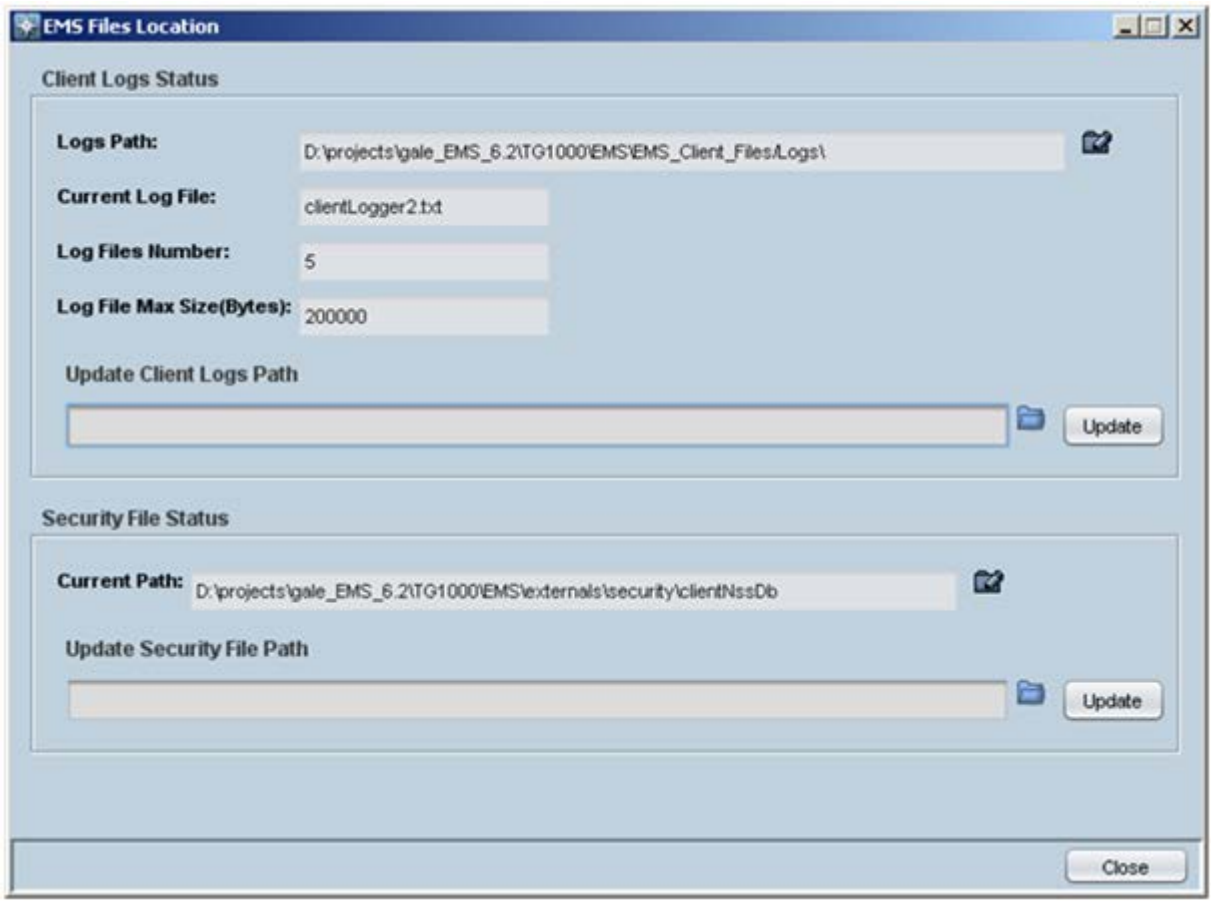
➢ **To install the EMS from the supplied DVD:**

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 its 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

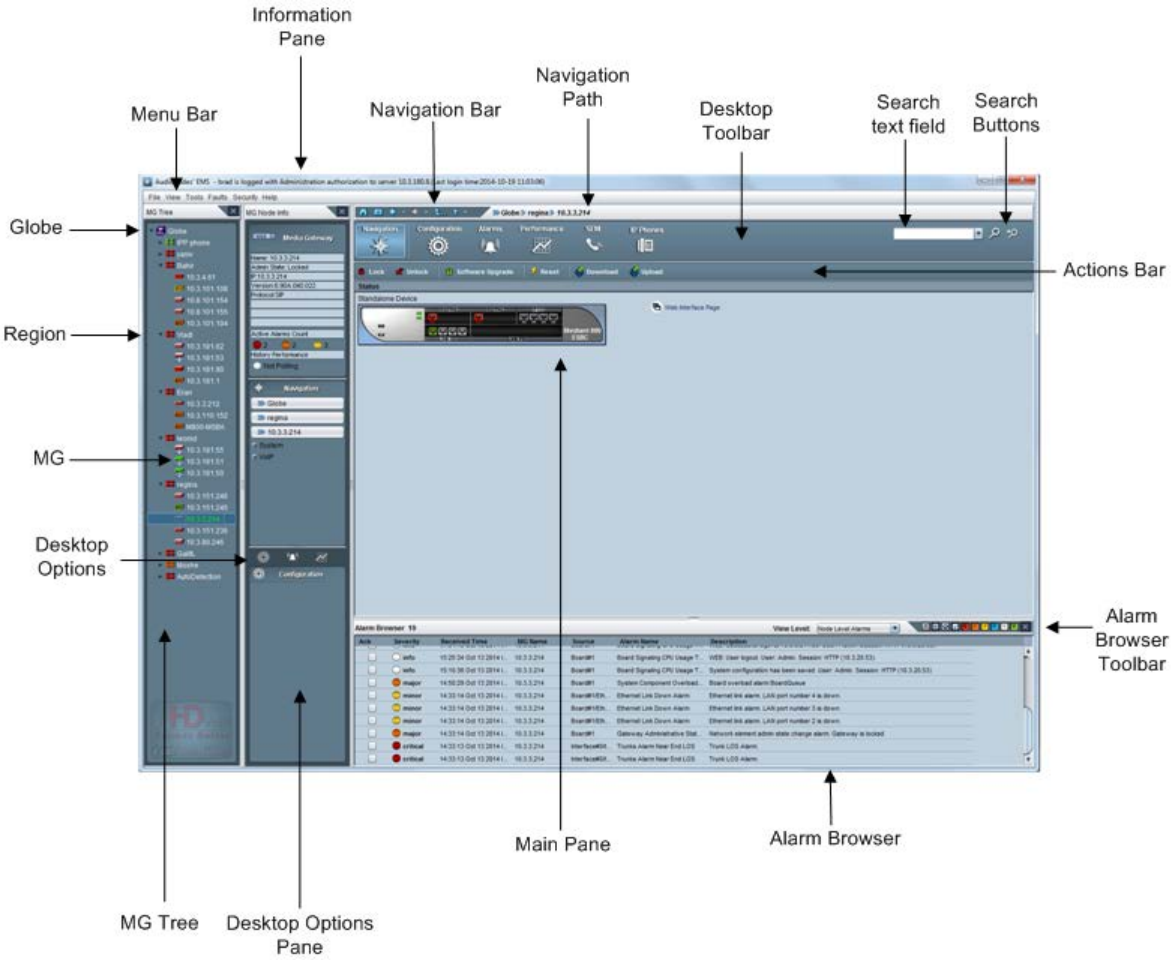
This subsection acquaints operators with the EMS. Read this section for a qui ck orientation to navigating in the EMS. This section explains the following:

- 'Navigating Down and Up System Hierarchy' on page 51.
- 'Selecting an Interface in the Context of an Element' on page 57 (and the concept of context-oriented screens).
- 'Using Color Coding to Assess Element Status' on page 59.

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.
- **Desktop Options** –Located above the Configuration pane. This pane provides quick access buttons to the Desktop Toolbar options.
- **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 device.
- **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 device in the MG Tree, the EMS by default displays the Media Gateway Status screen. By default, top-level device provisioning options are displayed in the Navigation pane. When you select a device board or other device 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 device, 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 device 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 269.

- **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 315.

- **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.

- **IP Phones Desktop**

  You can open the browser of the IP Phone Server Manager Home login page by clicking the **IP Phones** button in the Desktop toolbar.

  AudioCodes' IP Phone Management server enables enterprise network administrators to easily set up, configure, and maintain up to 10000 AudioCodes 400HD Series IP phones in globally distributed corporations. A configuration file template feature lets network administrators customize configuration files per phone model, region, and device. The IP Phone Management Server client enables statuses, commands and alarms to be communicated between the IP phones and the server and also with the EMS. The IP phones send their status to the server periodically for display in the user interface. For more information, refer to the *IP Phone Management Server User Guide.*

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., device).
	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 device in the MG Tree, select a device in the MGs List; the MG Node Info pane is immediately updated with basic information (if available) corresponding to the selected device.
2. Double-click the device listed under the MGs List; the device level Status pane graphically representing the device 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 device 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 and Mediant 8000 (v2.1)' on page 152. 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 Boards and CPE

This section describes how to select an interface in the context of an element for boards 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 / device, 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 device 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.

This page is intentionally left blank.

4 Software Manager

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

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

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

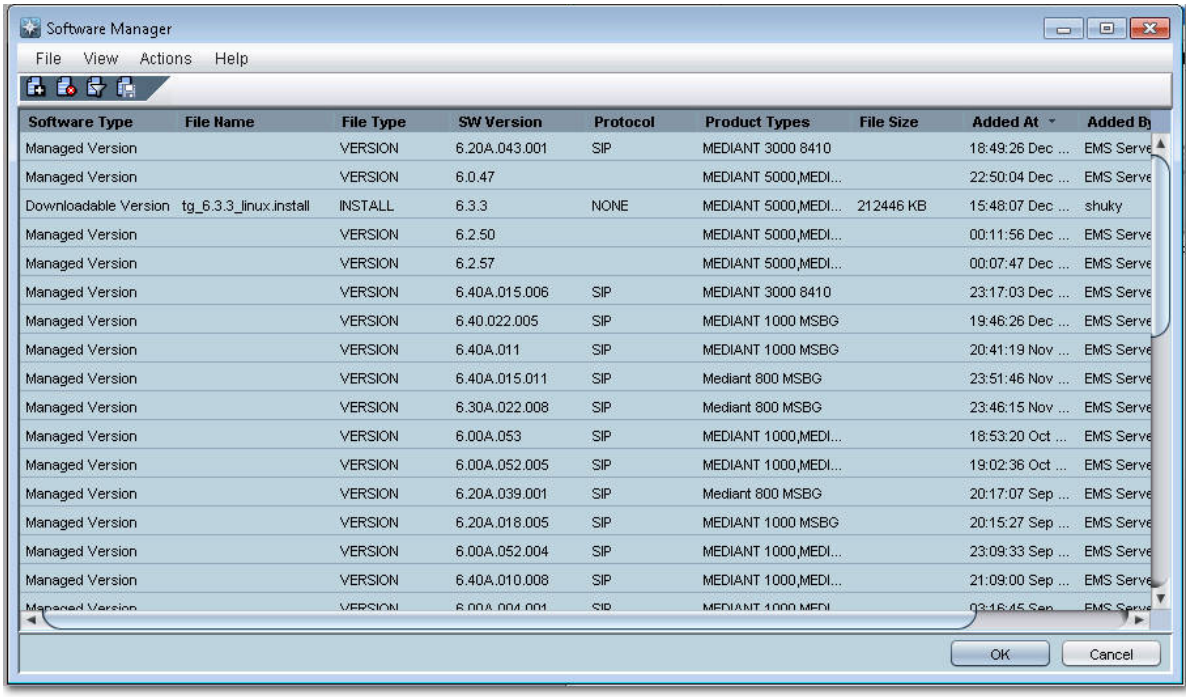
- **Software Type:**

  Three software types are supported:

  - Downloadable version: devices of this version are recognized and managed by the EMS and users can load the version to the device.
  - Managed version: devices of this version are recognized and managed by the EMS. The version cannot be loaded to any device.
  - Auxiliary file: An auxiliary file can be loaded to any MG.
- **File Name:**
- **File Type:** *cmp, tar* or *tar.gz*, *cpt, vp*, *casdat and txt.* 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 4-1: Software Manager



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

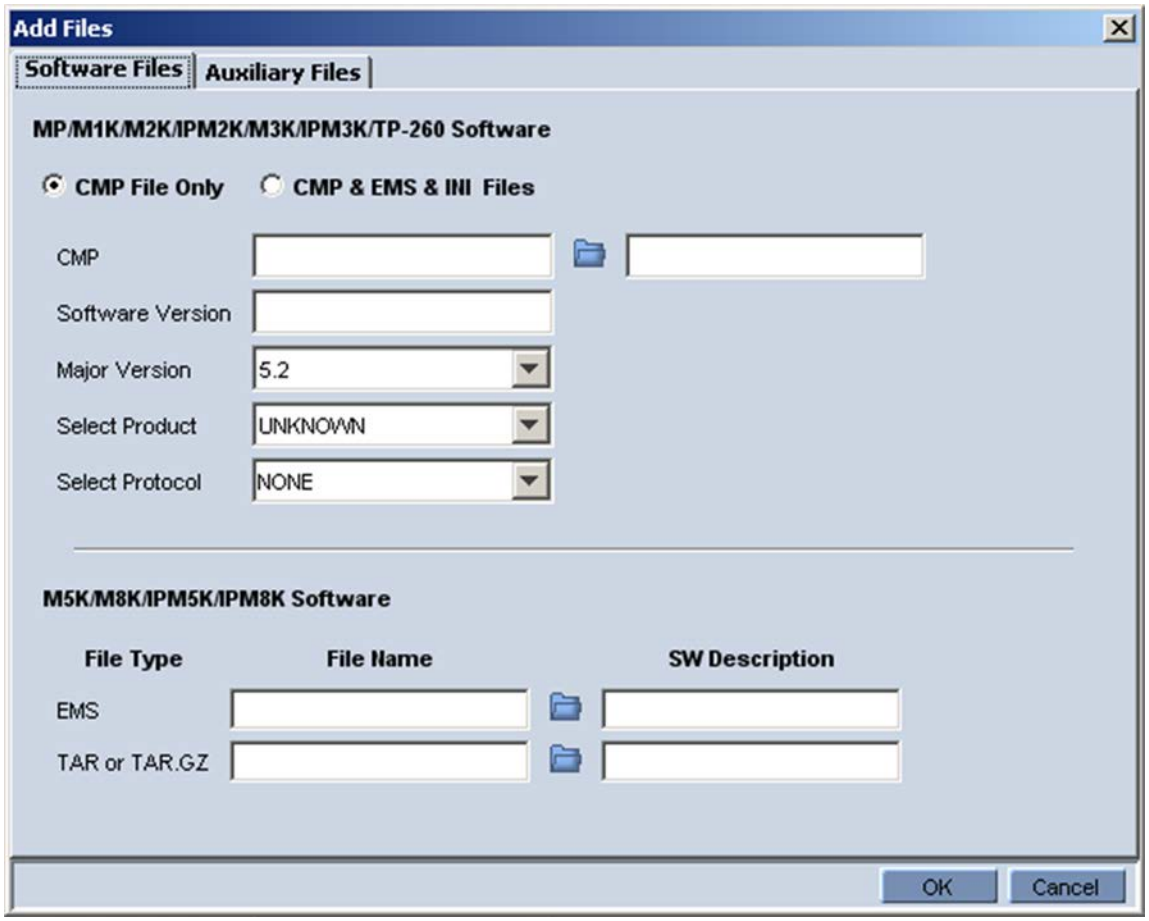
Figure 4-2: Software Manager File Details

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).
  - Select a protocol from the list e.g. SIP
  - *cmp* & *ini* & *ems* files

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

Figure 4-3: Add CMP File



- Configuration files for the Mediant 5000 and Mediant 8000:
  - **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 device.

Auxiliary Files

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

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

Figure 4-4: Software Manager-Adding Auxiliary Files

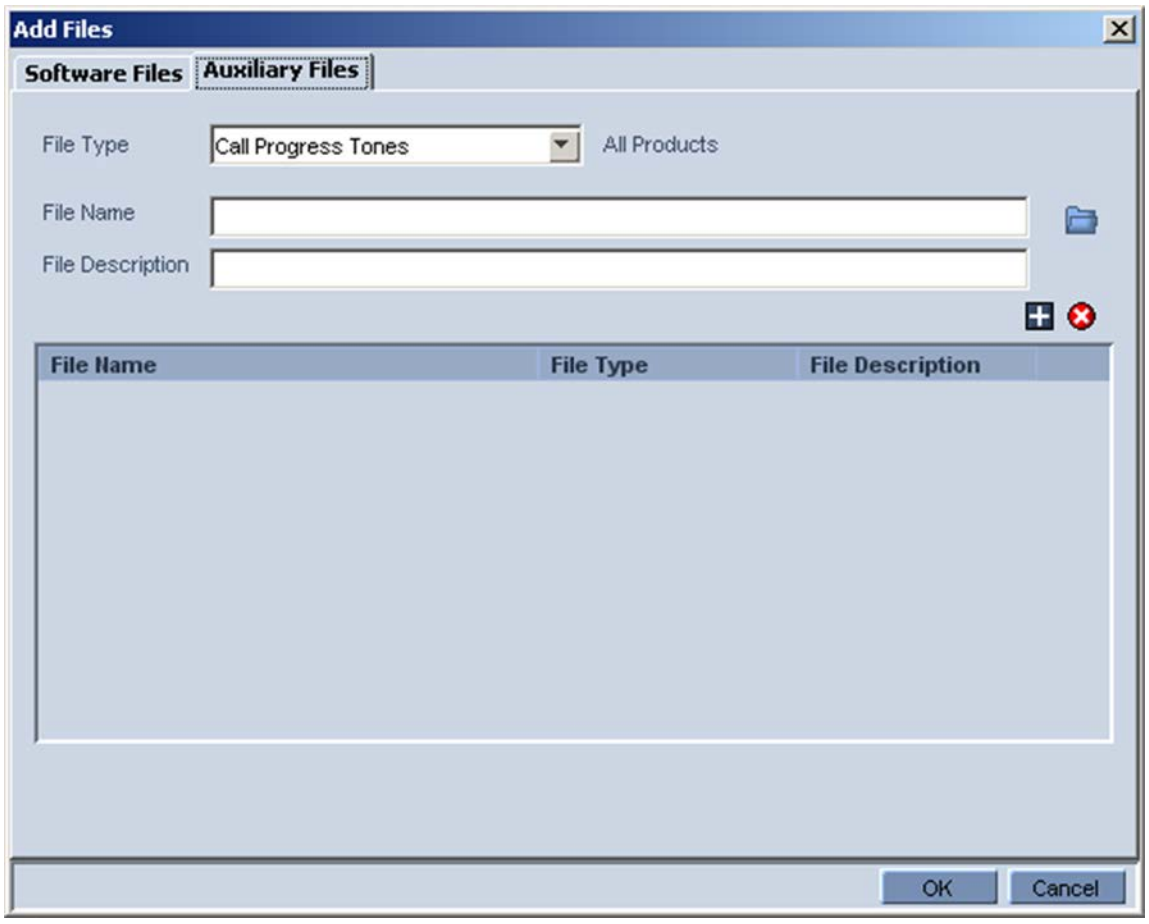


Table 4-1: Auxiliary Files

File Type	MediaPack (Analog Gateway)	CPEs	Mediant 5000 / 8000 TP Lock / Unlock required
Call Progress Tone (All Products)	√(Reset)	√(Reset)	√
Pre-recorded Tones (All Products)	√	√	√
Voice Prompts (All Products)	√	√	√
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 /	√	√	√

File Type	MediaPack (Analog Gateway)	CPEs	Mediant 5000 / 8000 TP Lock / Unlock required
MEGACO)	(Reset)	(Reset)	
License Keys (All Products)	-	✓	✓
INI Stand Alone	✓	✓	-
Alarms Properties File (M5K/M8K)	-	-	-
Alarm Propagation Rules (M5K/M8K)	-	-	✓
V5.2 File	-	Mediant 3000 8410 only	-
AMD Sensitivity File	-	✓	-
Data, System and Voice Configuration File (CLI Script File)	-	MSBR Products only	-

- **Tones**
  - Call Progress Tones (all products) - This is a region-specific, telephone exchange-dependent file. Four common Call Progress Tones are: Dial tone, Busy tone, Ringback tone and Reorder tone. Call Progress Tones provide call status/call progress to customers, operators and connected equipment. Default Tone: U.S.A.
  - Pre-Recorded Tones – This dat file enhances the VoIP device's capabilities of playing telephone exchange tones. Tones that cannot be defined in the Call Progress Tones file can be defined in this file, thereby enabling the device to offer a wide range of tones.
  - Voice Prompts - Played by the VoIP device during the phone conversation on Call Agent/Gatekeeper/Proxy request. Load it if you have an application requiring Voice Prompts (All MEGACO/MGCP-configured analog and digital devices support 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 device is connected. The device 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 devices) 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 device board.
  - **License Keys** – Customers can upgrade a single device's features or multiple devices' 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 'device Installation, Software Upgrade and Regional Files Distribution' on page 249. The new key overwrites the previous key.
  - **INI Stand Alone**: Includes initial configuration of MediaPack parameters that cannot be configured after adding (defining) the device in the EMS.

    During the ini file download user can select one of the three options below:
    - Full Configuration ini file download – with validation and apply (recommended).
    - Full Configuration ini file download – without validation and apply (for software upgrade).
    - Incremental ini file download (previous configuration remains).
  - **Alarms Properties File** – Used to customize the SNMP alarm's description and severities. When this file is absent (default state), the system generates SNMP alarms using the default descriptions and severities. Customers may override or modify properties of specific SNMP alarms by creating the Alarm Properties file. For additional information, refer to the *Programmer's User Guide*.
  - **Alarm Propagation Rules File** – When an alarm is raised on the MO, the Severity attribute of the MO itself is updated accordingly. In addition, the Severity attribute of the "father MO" may be updated as well. For example, when a major PSTN alarm is raised on Trunk, severity of the Trunk is set to

a major and severity of the device board where this trunk resides is set to minor. The alarm propagation behavior is tuned for each and every alarm and is not configurable.

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

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

Notes:

- 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 device (for example a separate file per V5.2 Interface) and download these files to the device. When managing multiple files for a single device, 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
```

4.1 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.

4.2 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 device is using it. When removing a *cmp* file, the *ini* file is removed with it.

4.3 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**.

5 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.

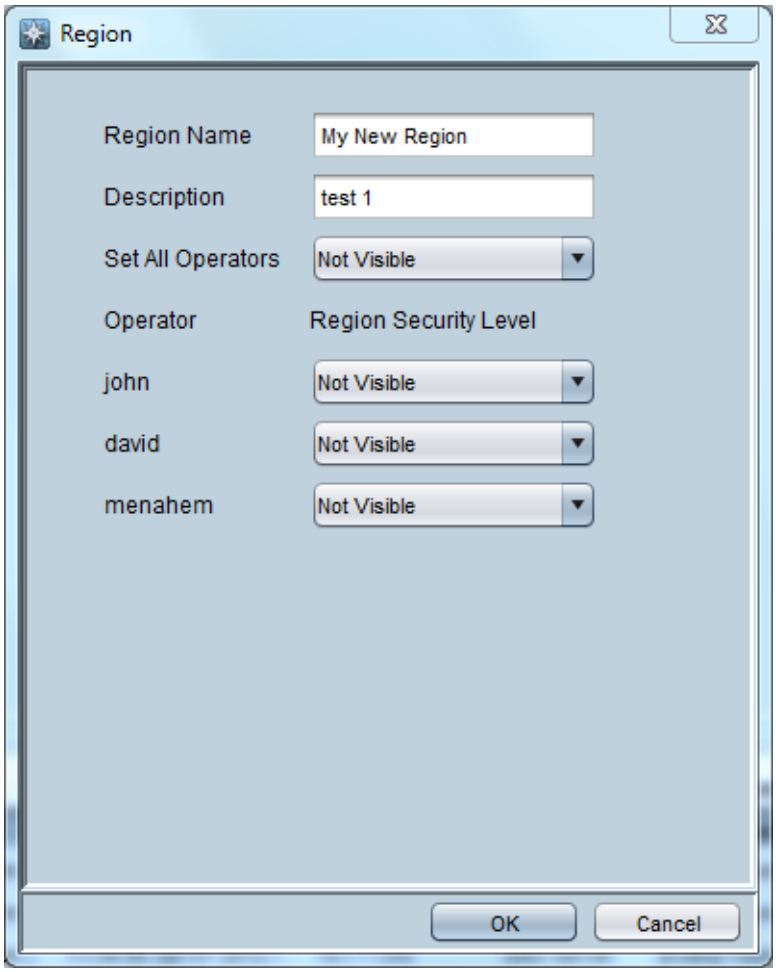
5.1 Configuring a Region

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 5-1: 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.

Note: Setting the security level for other users is relevant only for Operator/Monitoring users in the system. If no such users are defined, this option is not displayed.

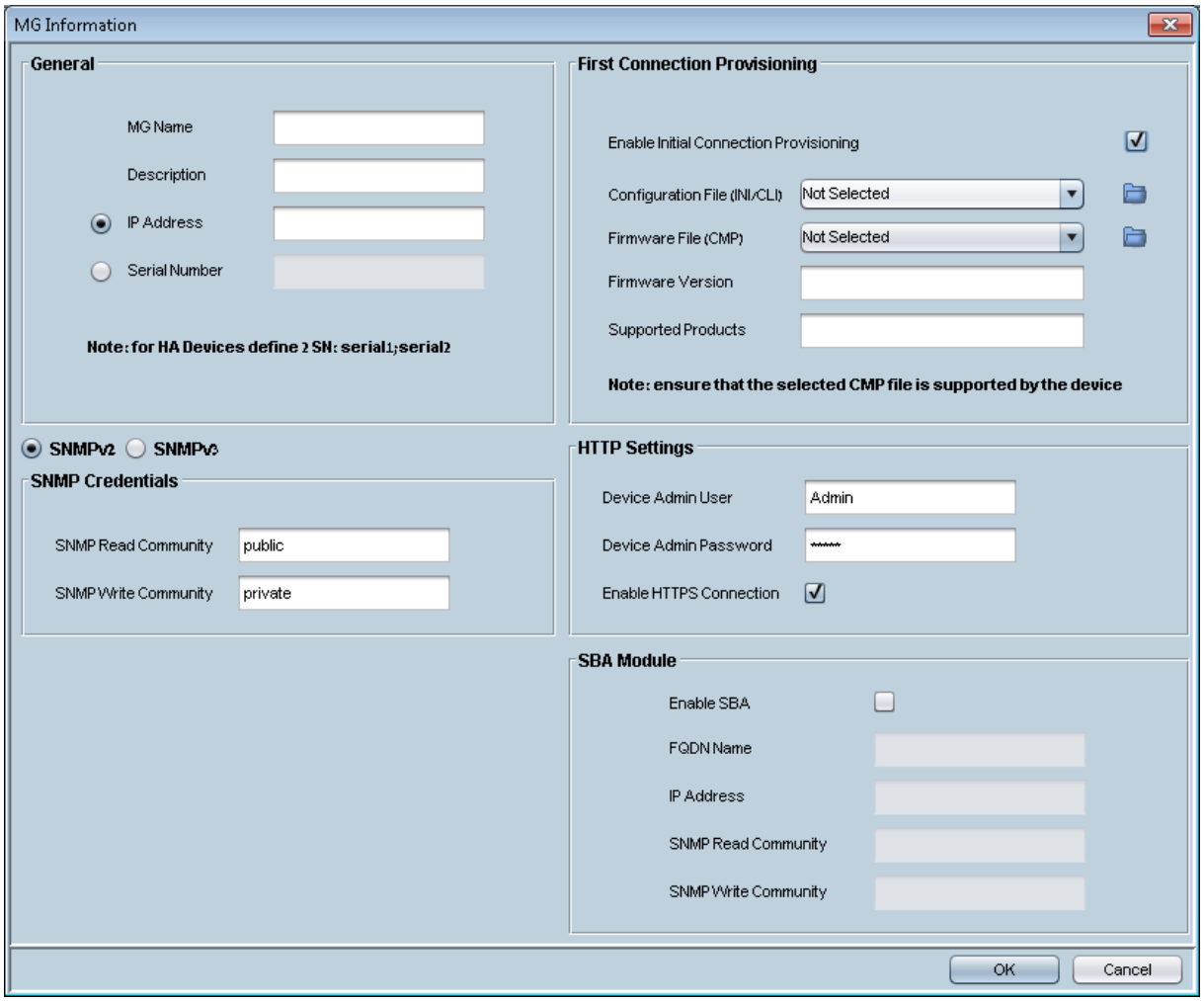
5.2 Defining a Mediant 5000, Mediant 8000

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

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

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

Figure 5-2: MG Information - SNMP2



2. In the MG Name field, define the device name as you would like it to be referenced in the EMS; enter the device's IP address, description, the SNMP and Security Information.

Note: The SNMP related security settings configured in this procedure should match the device installation definitions.

3. Configure SNMP between the EMS and the device; select either the **SNMPv2c** (default) or **SNMPv3** checkboxes.
4. 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, 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.
5. Click **OK**; the requested device is added to the required region.
6. Verify if the device 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 device in the Status screen, see Section 'Troubleshooting' on page 383 to resolve the issue.

   The device is added with all fields set to their default values. To change the defaults, right-click the device in the MG Tree and choose **Details**; the MG Information screen opens.
7. 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 device and the EMS are identical; if you remove/add a device, 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 device is identical, and vice-versa. To change a password, first change the password in the device and then open the screen 'MG Details' in the EMS and update the field accordingly.
8. Click **OK**; the requested device is added to the required region. Click **OK**; an Action Report is displayed, indicating the result of the add action for each device added.

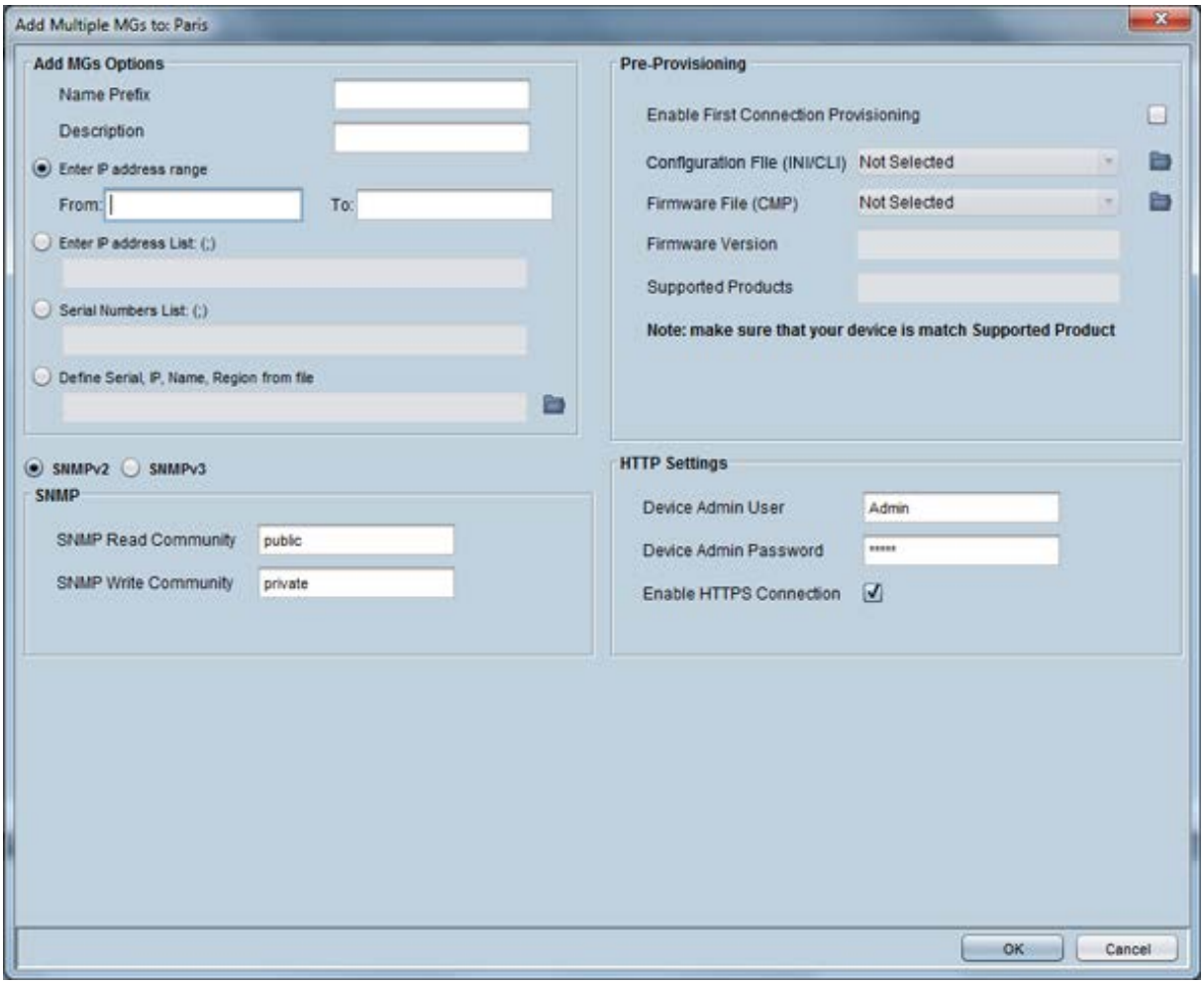
5.2.1 Defining Multiple Mediant 5000, Mediant 8000 Devices

This section describes how to define multiple devices.

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

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

Figure 5-3: 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 devices to be added, separating the IP address from each other with a semi colon.
4. Define the device name prefix as you would like it to be referenced in the EMS (a device's name comprises the prefix and IP address) and the device's SNMP Read and Write Community strings.

5. Verify that all the devices are successfully defined in the EMS: Firstly, check the MGs List information; secondly, enter each device's status screen. Verify if the device 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 device, including its LEDs, must be displayed in the Status screen (refer to the figures displaying device status under 'MediaPack' on page 215). If you do not view a graphic representation of the device in the Status screen, see Section 'Troubleshooting' on page 383 to resolve the issue.
6. To change the default Telnet user name and password, right-click in the MGs Tree on each device and choose **Details**. Define the FTP and Telnet user and password to be used during the Software Upgrade procedure.

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

7. Configure SNMP between the EMS and the device; select either the SNMPv2c (default) or SNMPv3 checkboxes.
8. 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, 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.
9. Click **OK**; the requested device is added to the required region. Click **OK**; an Action Report is displayed, indicating the result of the add action for each device added.

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

5.3 Predefinition or Automatic Detection

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

5.3.1 Boards and CPE

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

5.3.2 Automatic Detection

This section describes how to enable an automatic detection event (coldStart) to be sent to a configured SNMP Manager when a device is connected to the power supply and the network at the customer's premises and 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 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 device is configured behind a NAT, you also need to configure the keep alive trap ini parameters on the device as follows:

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

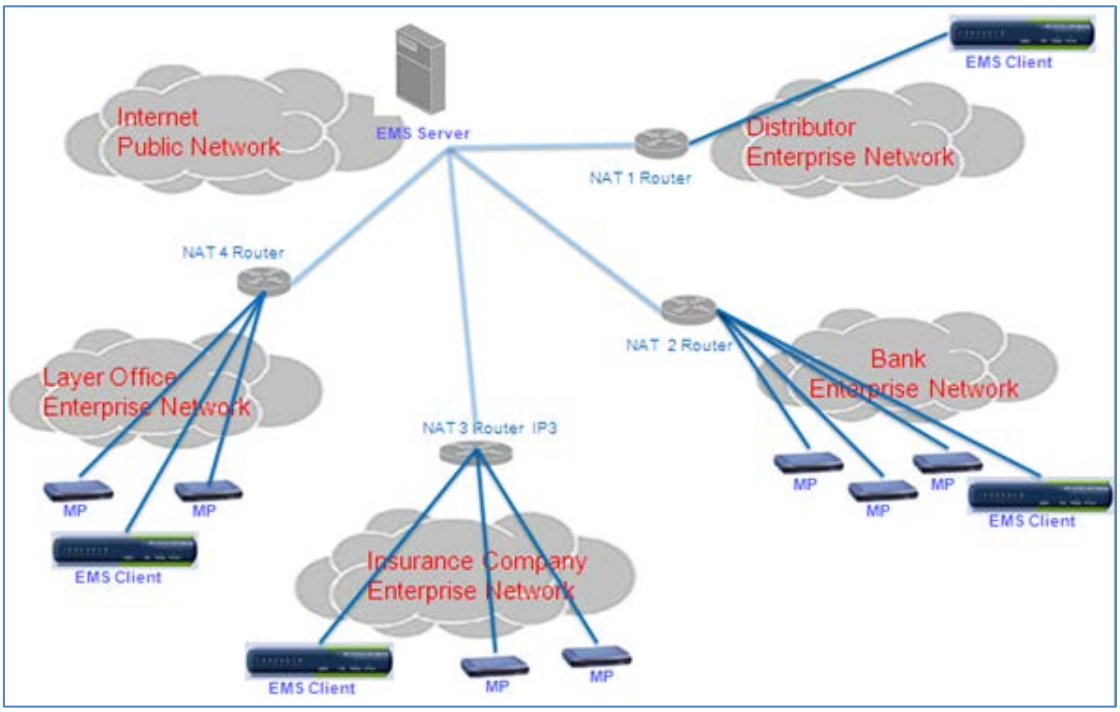
3. After the device is connected to the power supply and the network at the customer's premises, it performs a reboot and at the end of the initialization process, sends a coldStart trap event to the pre-provisioned 'SNMP Manager' name. When the coldStart trap is received, the EMS connects the device,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

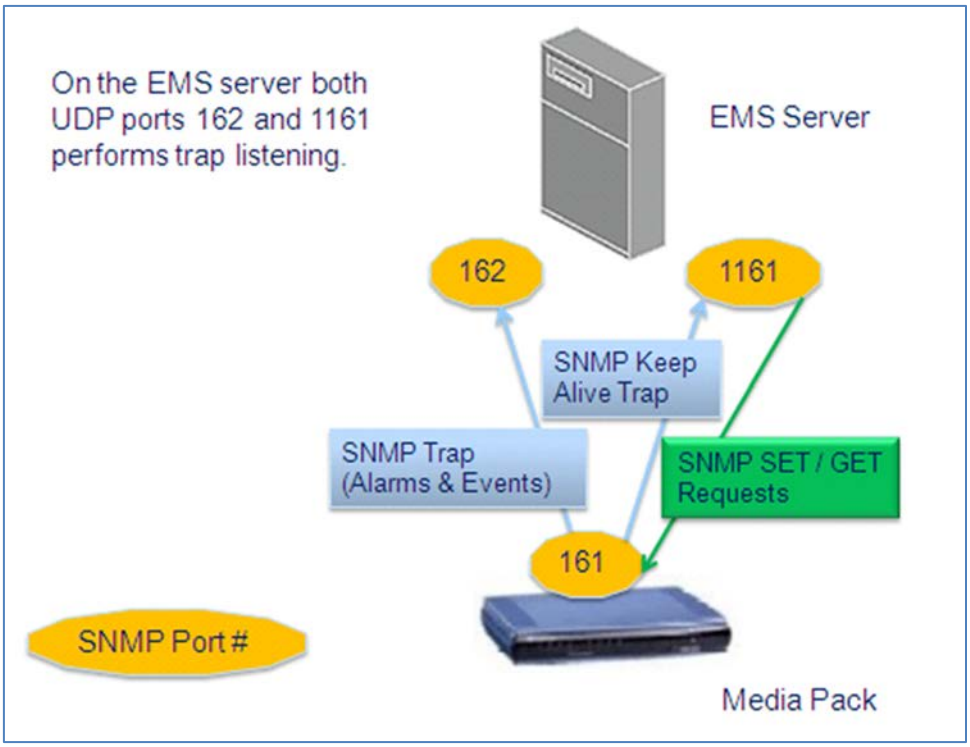
Figure 5-4: MP-NAT Configuration



The figure below describes how the EMS and the devices 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 5-5: Sending SNMP Traps to EMS Server (Behind a NAT)



5.3.3 Defining a Single Board or CPE

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

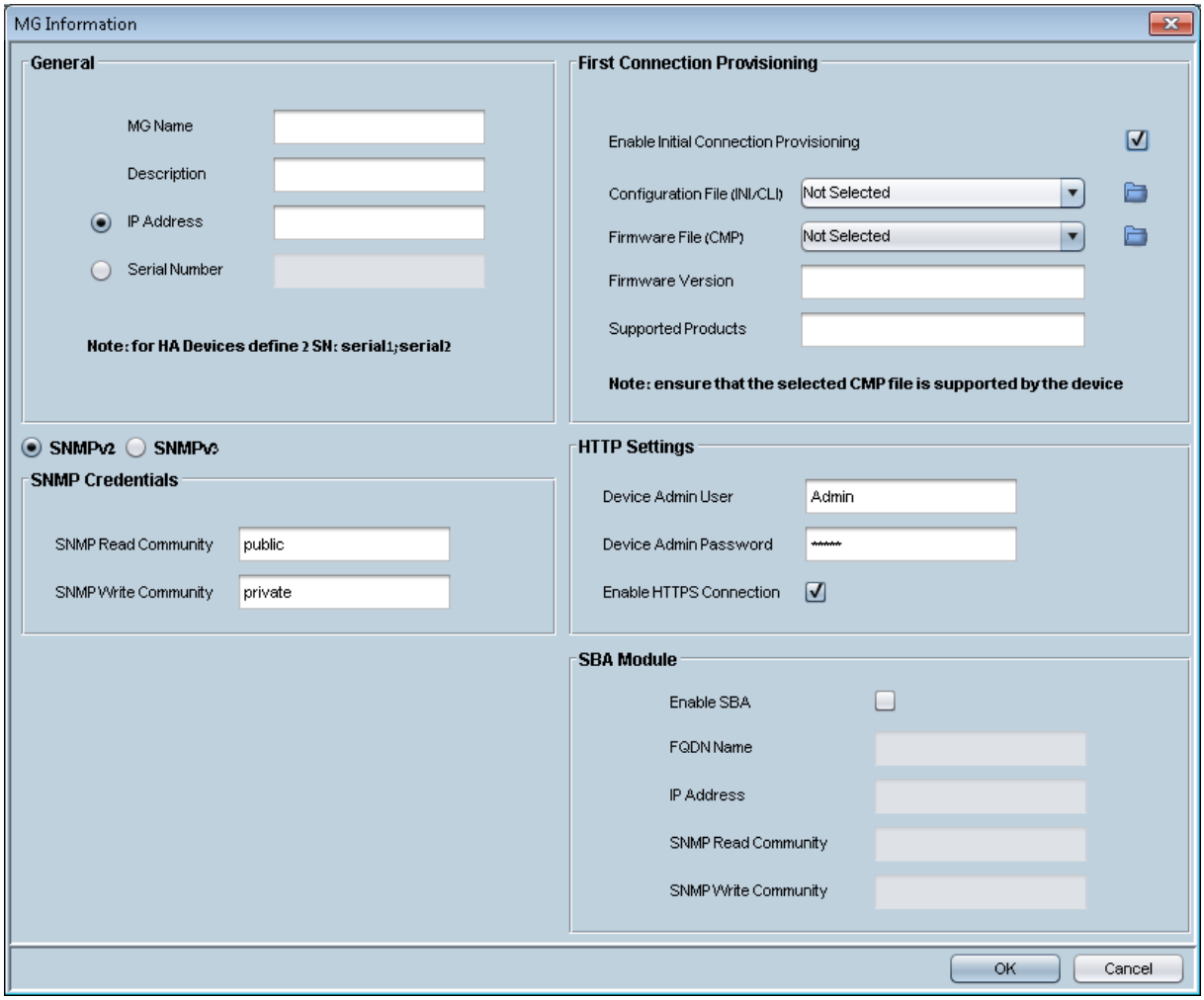
Notes:

- This procedure includes the configuration of the Interoperability Automatic Provisioning feature. If you wish to implement this feature, refer to Chapter 22 before proceeding.
- This procedure includes the option to set the Web user name and password for automatically logging into the device's Web server tool from EMS, therefore ensure that you note these credentials.
- This procedure includes the configuration of the SNMP settings for the connection between the device and the EMS; therefore ensure that you note the relevant SNMPv2 or SNMPv3 credentials.

➢ To predefine a single board or CPE:

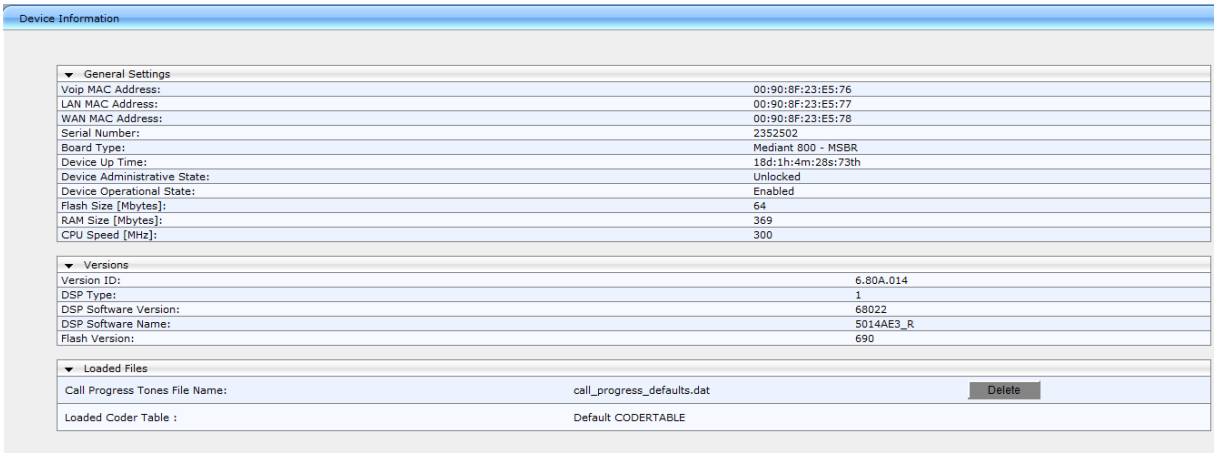
1. Right-click the region in the MG Tree to which to add the device and from the sub-menu, choose option **Add MG**.

Figure 5-6: MG Information



2. Define the device name as you would like it to be referenced in the EMS and provide a description of the device.
3. Define the device to the EMS using one of the following methods:
   - Enter the **IP address** of the device.
   - Enter the **Serial Number** of the device. You can find the device serial number from the Web server device Information page (**Status & Diagnostics** menu> **System Status** > **Device Information**).

Figure 5-7: Device Information



4. Do one of the following:
   - If you are configuring SNMPv2, enter the device's SNMP Read and Write Community strings.
   - If you are configuring SNMPv3, enter the following fields:
     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.
5. Select the 'Enable Initial Connection Provisioning' check box to enable the Interoperability Automatic Provisioning feature, and then do the following:
   - In the 'Configuration File' (ini or CLI script - MSBR devices) field, from the drop-down list box, select the desired file, or click the button to choose the ini file.
   - (Optional) In the 'Firmware File' (.cmp) field, from the drop-down list box, select the desired .cmp file or click the button to choose a .cmp file.

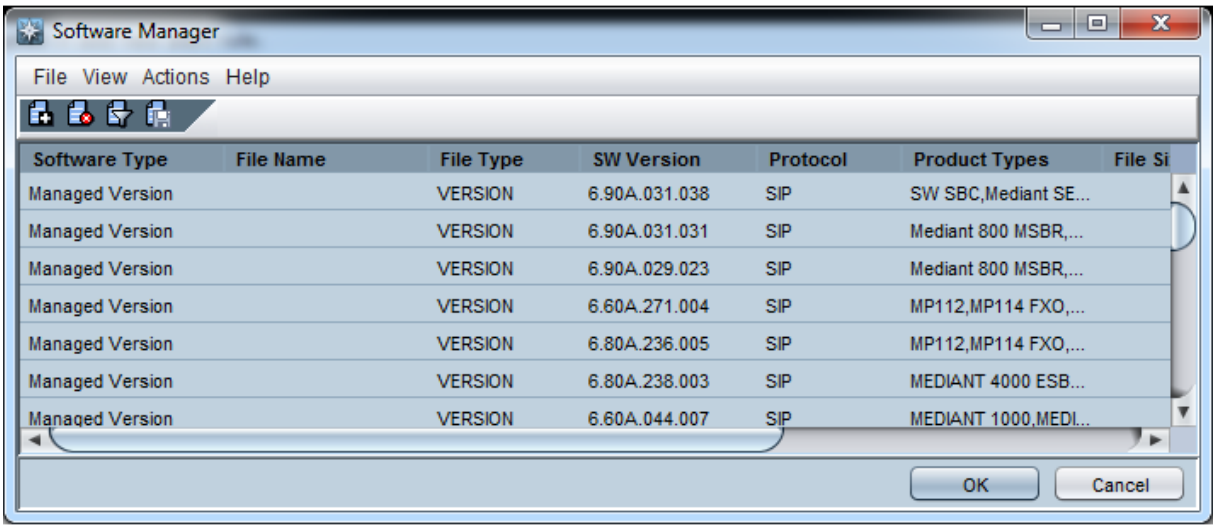
   When you choose a .cmp file, the corresponding firmware version is displayed as well as the products that are supported for this file.

Notes:

- When choosing a .cmp file, ensure that this file matches the device type. If the selected file is not supported by the device, then the Interoperability Automatic Provisioning process fails and an alarm is sent to EMS (see Section 22.6.2).
- To activate the Interoperability Automatic Provisioning feature, you *must* select an ini file and can *optionally* select a .cmp file.

If you choose to browse for a file, the Software Manager opens displaying the available configuration and firmware files (cmp and ini). When you add them, they are automatically made available in the respective Enable Initial Connection Provisioning drop-down lists.

Figure 5-8: Software Manager



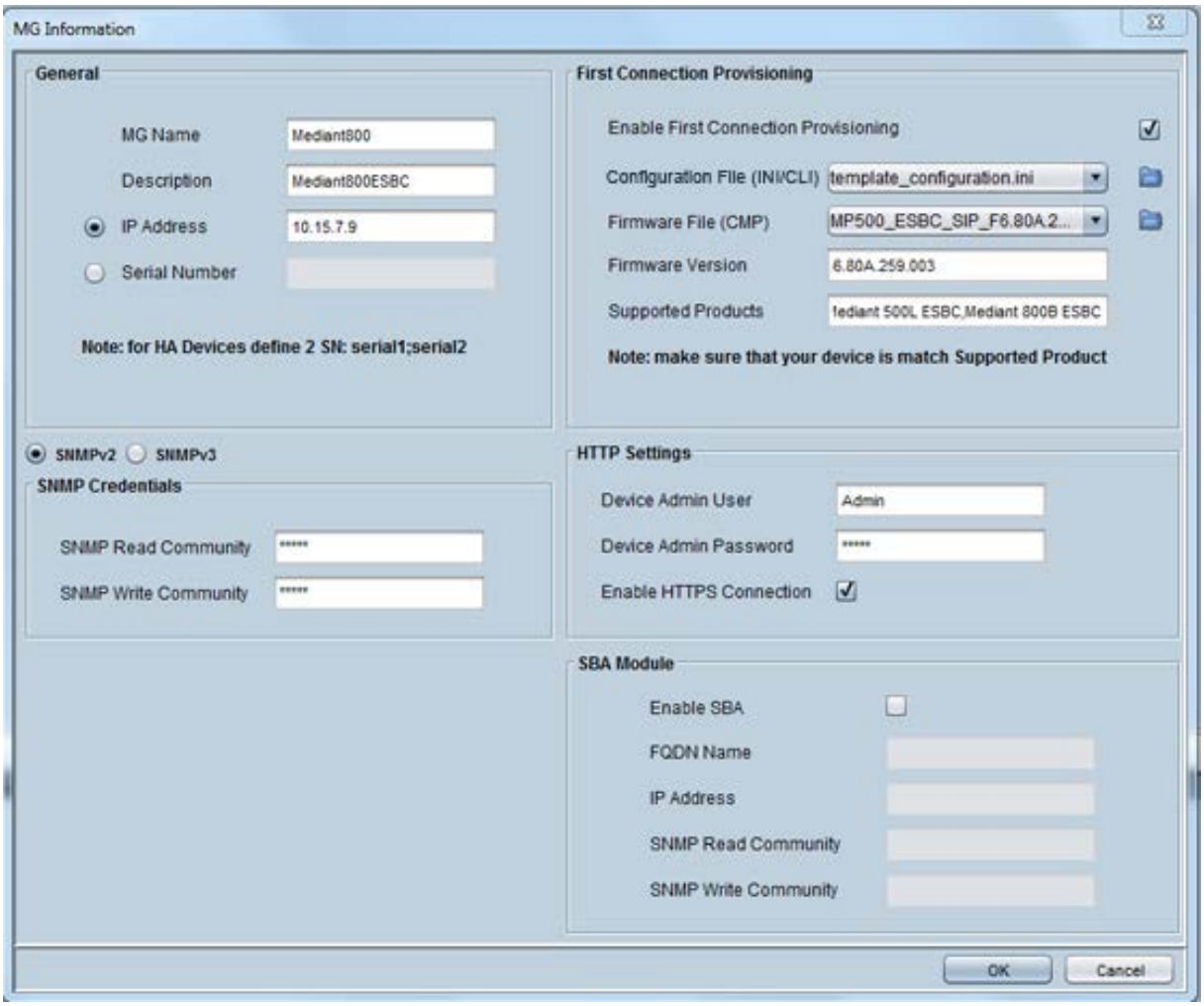
6. (Optional) In the Device Admin User field, enter the device Web server user name and in the Device Admin Password field, enter the Web server password. For example, User -"Admin", Password - "Admin".

Note: For version 7.0 devices and later, the EMS includes a link to the device's embedded Web server. Configuring the above credentials enables the user to automatically login to the device's Web server home page (using a Single Sign On mechanism) whenever the Web server link in the device's status screen is clicked.

7. If you wish to secure the connection with device, select the 'Enable HTTPS Connection' option. For more information on HTTPS, see Section 34.2 on page 347.

The device is added to the EMS database. To change the defaults, right-click the device in the MG Tree and choose **Details**; the MG Information screen opens (refer to the figure below).

Figure 5-9: MG Details



8. Click **OK**; the requested devices added to the required region.

Note: To perform changes in the EMS and device connectivity related to SNMP, see Chapter 34 on page 343

9. If you are pre-provisioning devices using Interoperability Automatic Provisioning then proceed to Chapter 22.

5.3.4 Defining Multiple Devices

The EMS supports defining multiple devices (Multiple CPE devices) in a single screen on condition that all devices have identical SNMP settings.

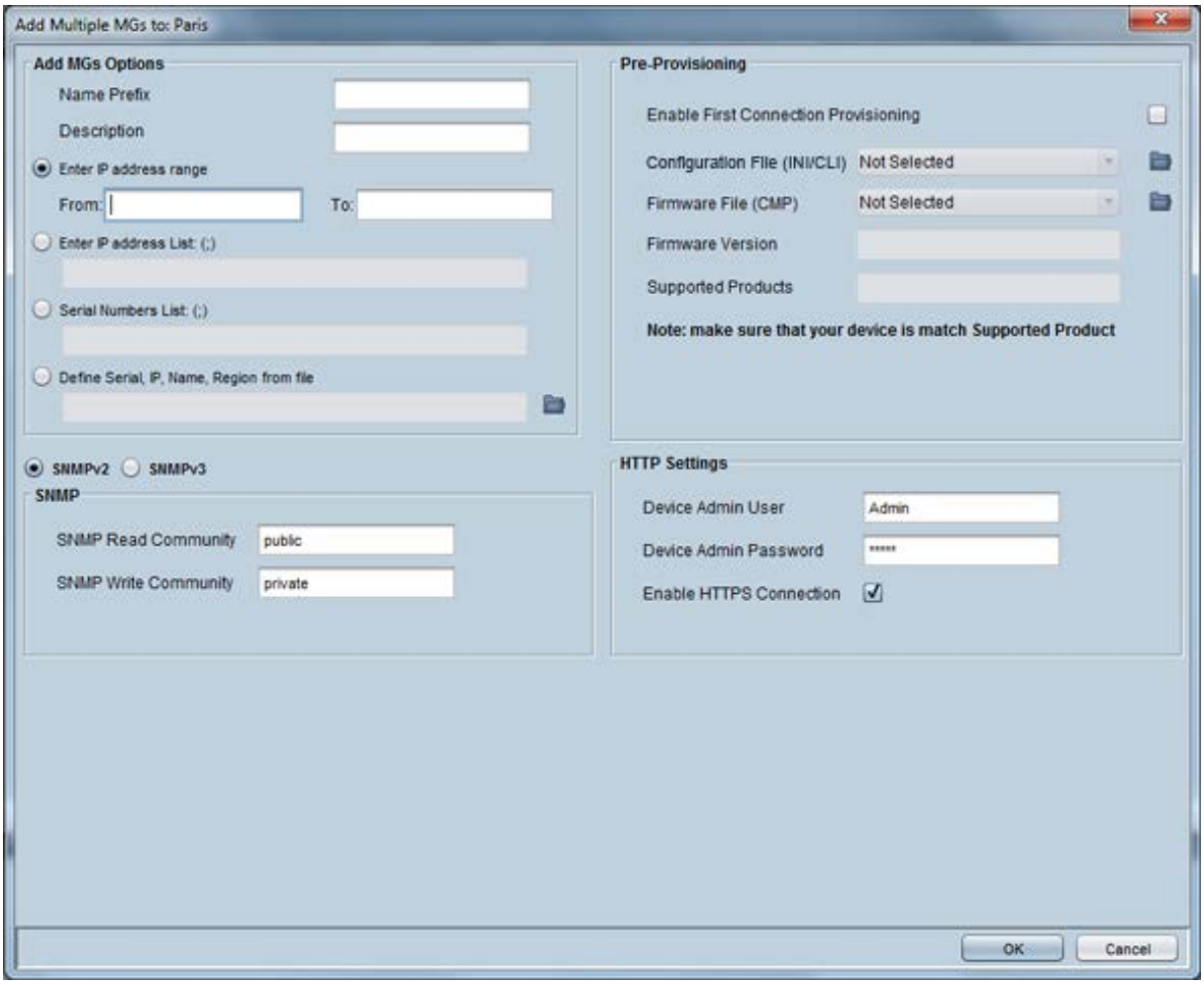
Notes:

- This procedure includes the configuration of the Interoperability Automatic Provisioning feature. If you wish to provision devices using this feature, then ensure that you have added the relevant template ini files and .cmp firmware files to the EMS Software Manager (see Chapter 4). At the end this procedure you are directed to Chapter 22 which provides detailed information on this feature.
- This procedure includes the Single-Sign-On setting for automatically logging into the device's Web server tool from EMS; therefore ensure that you know the Web user and password.
- This procedure includes the configuration of the SNMP settings for the connection between the device and the EMS; therefore ensure that you know the relevant SNMPv2 or SNMPv3 credentials.

➢ **To add multiple devices:**

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

Figure 5-10: Add Multiple MGs-SNMPv2



2. Enter the Name Prefix for device group e.g. type of device and Description for the group of devices.

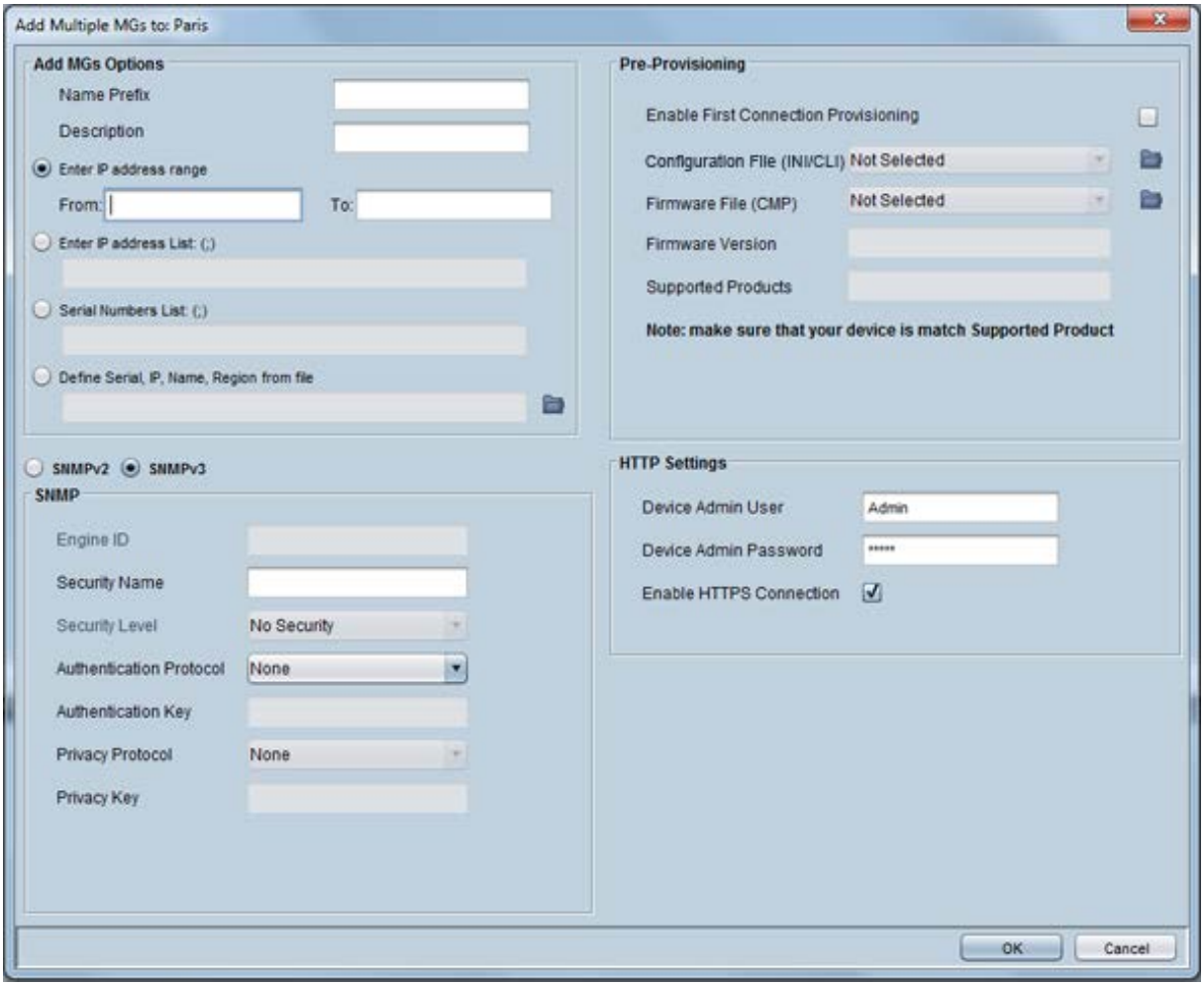
3. Use one of the following methods to connect the multiple devices to the EMS:
   - Select the 'Enter IP address range' option, define the 'From' and 'To' fields and click OK. All devices in the defined range are added to the MG Tree with name combined as 'Name Prefix' + 'IP Address'.
   - Define multiple devices by checking check box 'Enter IP address list, and then define the IP addresses of the multiple devices that you wish to add, separating the IP address from each other with a semi-colon.
   - Define multiple devices by checking the check box 'Serial Numbers list' option, and then enter a list of multiple devices with ";" separated values.
   - Define multiple devices by checking the check box 'Define Serial, IP, Name, Region from file', navigate to a pre-prepared *csv* predefinition file and click **OK**. Each device 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.

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 i.e. the MGs Report or the Topology Report files (for more information, see page 99).

10. Do one of the following:
    - If you are configuring SNMPv2, enter the device's SNMP Read and Write Community strings.
    - If you are configuring SNMPv3, enter the following fields:

    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.

Figure 5-11: Add Multiple MGs-SNMPv3



11. Select the 'Enable First Connection Provisioning' checkbox to enable the Interoperability Automatic Provisioning feature, and then do the following:
    - In the 'Configuration File' (ini or CLI script file - MSBR devices) field, from the drop-down list box, select the desired file, or click the button to choose the ini file.
    - (Optional) In the 'Firmware File' (.cmp) field, from the drop-down list box, select the desired .cmp file or click the button to choose a .cmp File.

      When you choose a .cmp file, the corresponding firmware version is displayed as well as the products that are supported for this file.

Notes:

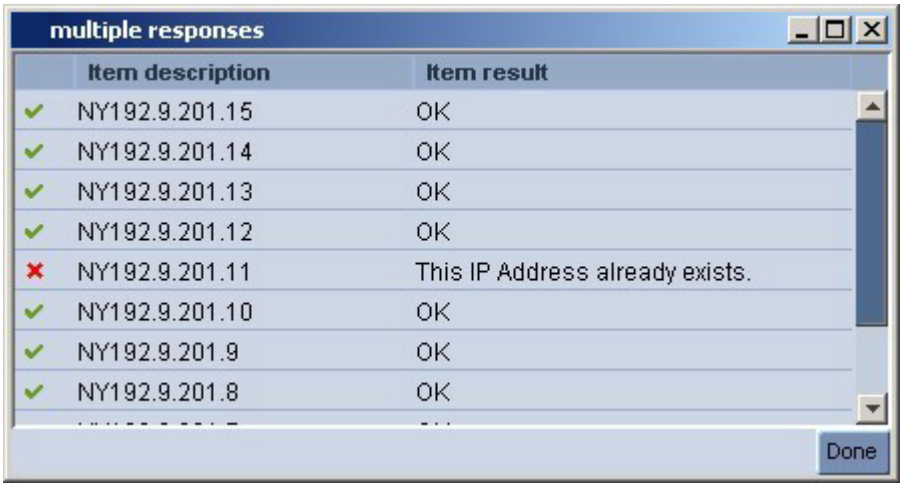
- When choosing a .cmp file, ensure that this file matches the device type. If the selected file is not supported by the device, then the Interoperability Automatic Provisioning process fails and an alarm is sent to EMS (see Section 22.6).
- To activate the Interoperability Automatic Provisioning feature, you *must* select an ini file and can *optionally* select a .cmp file.

12. (Optional) In the Device Admin User field, enter the device Web server user name and in the Device Admin Password field, enter the Web server password. For example, User -"Admin", Password - "Admin".

Note: These parameters are only applicable for devices with version 7.0 and later. Such devices cannot be provisioned in the EMS. When these credentials are entered, the user can login to the device using a Single Sign On mechanism (the Web server home page is opened directly and the user is not prompted to enter their login credentials).

13. If you wish to secure the connection with device, select the 'Enable HTTPS Connection' option. For more information on HTTPS, see Section 34.2 on page 347.
14. Click **OK**; an Action Report is displayed, indicating the result of the add action for each device added.

Figure 5-12: Action Report for Adding Multiple Devices Result



Note: To perform changes in the EMS and device connectivity related to the SNMP, see Chapter 34.1 on page 343.

5.3.4.1 Devices Connected to the Network

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

If you encounter a problem when defining your devices, see Section 'Troubleshooting' on page 383 to resolve the issue (or contact AudioCodes).

5.3.4.2 Devices not Connected to the Network

The EMS is capable of defining the device type before it is connected to the device for the first time. Until the first connection with the device 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 383 to resolve the issue (or contact AudioCodes).

5.3.5 Sorting Regions and Devices

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

➢ **To sort regions / devices:**

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

Figure 5-13: Sort Regions

5.4 First-Time Connection Problems

A device is indicated by in one of the following cases:

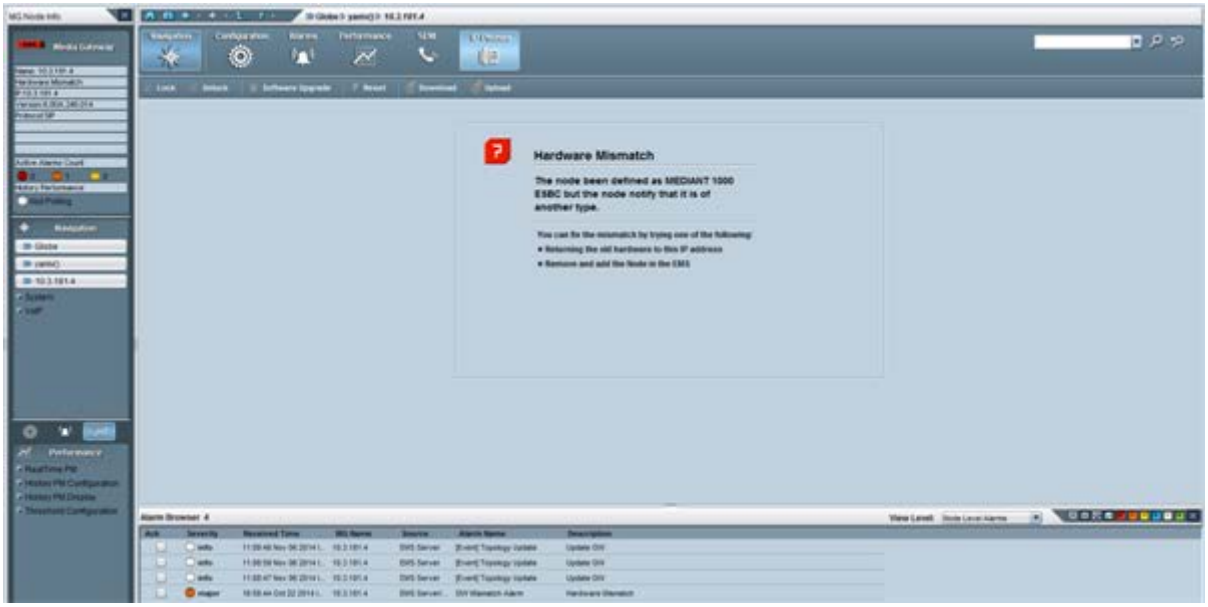
- **Unknown Hardware:** The Product Type, returned by the MIBII sysDescr value, is not recognized by the EMS. The device cannot be managed by the EMS.
- **Unknown Software**: The Software Version, returned by the MIBII sysDescr value, is not recognized by the EMS. Either add the specified version to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

5.5 Mismatch Indications

Three types of mismatch between the database and device 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 the Reset State (relevant for CPE products). Whenever a mismatch occurs, a Device Mismatch alarm is raised. The severity of the alarm is determined according to the type of mismatch.

- **Hardware Type Mismatch:** If a hardware type mismatch occurs, the device 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 device as the 24-port device (for example) during the predefinition stage; however when connecting for the first time, the device type returned by the device itself is the 8-port FXS device (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 device returns a different software version to the software version that was configured by the operator. The EMS does not change the status of a device 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 5-14: Mediant 2000 Information pane Indicating Mismatch



5.6 Moving a Device from Region to Region

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

➢ **To move a device 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 device 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 device is moved.

5.7 Moving Multiple Devices from Region to Region

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

➢ **To move multiple devices from one region to another:**

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

Figure 5-15: Moving Multiple MGs from Region to Region

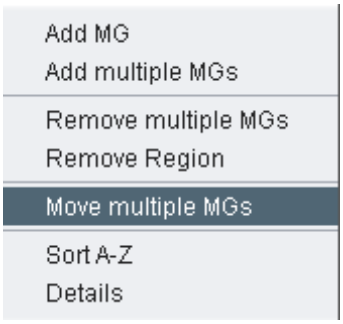


Figure 5-16: Multiple Move from Region to Region

2. In the 'Multiple Move' screen, select the devices 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 devices.
4. Click **OK**; a Multiple Response screen opens, showing the results of the operation.

5.8 Removing a Device

This section describes how to remove a device.

➢ **To remove a device:**

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

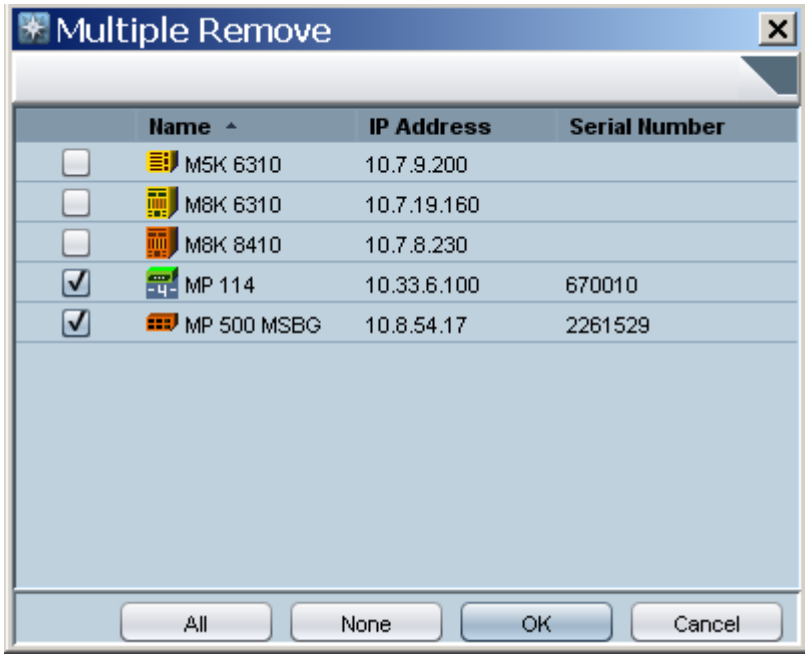
5.9 Removing Multiple Devices

The EMS supports the removal of multiple devices 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 and the Mediant 8000 must be locked prior to their removal.

➢ **To remove multiple devices:**

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

Figure 5-17: Removing Multiple Devices



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

5.10 Searching for a Device

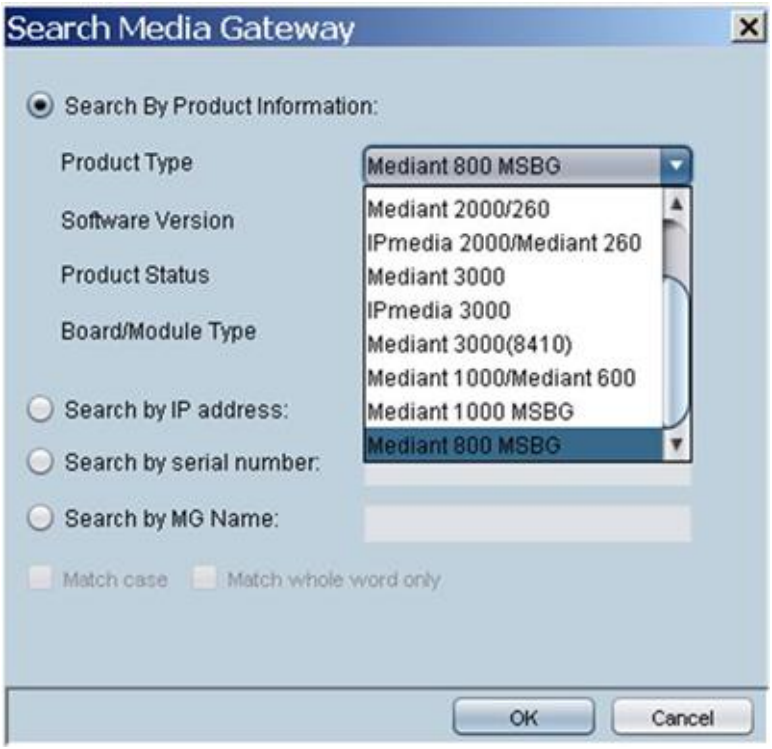
This section describes how to search for a device.

➢ To search for a device:

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 5-18: Search MGs



2. Search by Product Information: Enter the following device 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 device 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 device is located, it is selected in the MG Tree and its Status screen is opened. If more than one appropriate device is located, the Search Result screen is displayed.

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

Note: You can enhance your search for a device (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.

5.11 Saving the EMS Tree MGs Report in an External File

The MGs Report CSV file includes configuration and status data of all devices 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 device or upon updates to the device 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 then 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 devices).
- 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 devices.
- Master Profile
- Reset Needed
- SBA FQDN Name
- SBA IP Address
- SNMP Version – options are SNMPv2/SNMPv3
- SNMP Read – encrypted SNMP read community
- SNMP Write – encrypted SNMP write community
- SNMP User Profile - SNMP v3 user credentials in format: (EnginID;SecurityName;SecurityLevel;AuthProtocol;PrivacyKey)
- Gateway User – user name for MG web access Gateway Password– user password for MG web access
- HTTPS Enabled – 0-disabled/1-enabled HTTPS access to the MG

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

Figure 5-19: Device Pre-Definition File

Serial Nu	IP Address	Node Nam	Region	Product T	Software	Connectic	Administr	Operative	Mismatch	Last Chan	Preformai	Performai	Protocol T	Master Pr	Reset Nee	Descriptic	SBA FQDN	SBA IP A	SNMP Ve	SNMP Re	SNMP Write	SNMP User	Gateway	Gateway	HTTPS	Enabled
3583846	192.168.1(	SSO-Proxy	Eran	UNKNOW	unknown_	Not Connected			No Misma	2014-12-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
3846546	10.3.101.1	M4K	Eran	MEDIANT	7.00A.003.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
1242278	10.3.151.2	SSBC	Eran	SW SBC	7.00A.005.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		0	
123456	1.1.1.1		Eran	UNKNOW	unknown_	Not Connected			No Misma	2014-12-0	Not Polling					1.1.1.1			SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
273196	10.4.100.3	10.4.100.3	Vladi	MEDIANT	6.80A.255.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
4773083	10.3.181.9	10.4.100.1	AutoDete	MEDIANT	7.00A.004.	Not Conn	Unlocked		No Misma	2015-02-0	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
760978	10.3.80.16	10.3.80.16	AutoDete	MP124	6.60A.290.	Not Conn	Unlocked		No Misma	2015-02-0	Not Polling		SIP		Reset Not	Needed			SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
3480922	10.15.4.6	10.15.4.6-	AutoDete	Mediant 8	6.80A.261.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
5200544	10.3.181.7	10.3.181.7	AutoDete	Mediant 5	6.90A.048	Not Conn	Unlocked	Enabled	No Misma	2014-12-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		0	
893335	10.3.181.2	10.3.181.2	AutoDete	MEDIANT	6.80A.219.	Not Conn	Unlocked	Enabled	No Misma	2015-01-0	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF				1	
3037728	10.3.181.6	10.3.181.6	AutoDete	Mediant 5	6.80.244.0	Connecte	Unlocked		Hardware	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
5264110	10.3.181.1	10.3.181.1	AutoDete	UNKNOW	unknown_	Not Connected			No Misma	2014-12-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF	Admin	fseUajPSa		1	
4979399	10.3.3.214	10.3.3.214	AutoDete	Mediant 8	7.00A.001	Not Conn	Unlocked		No Misma	2015-01-0	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6ryki4hF				1	

5.12 EMS Application Welcome Message

The Welcome Screen is displayed to the user upon successful Login information validation and is composed of Administrator defined textual message and previous Successful and Unsuccessful Login Information including Date, Time, and Login Machine IP.

The Administrator can set a w elcome message note using the Help -> Advisory Message menu.

The Administrator can define one of the following three Welcome Message Options:

- **Mandatory** – the Welcome Message is always displayed. The Administrator can define per user if the Login Info part is displayed.
- **Optional (default)** – the Welcome Message is displayed according to definition in the Users table in the field 'Display Welcome Message'. The user can disable the Welcome Message or Login Information parts and thereby disable the entire Welcome Message starting next session.
- **Disable** – the Welcome Message is displayed with only the Login Information pane. The user can disable the Login Information part (by selecting the 'Do Not Display Login Information on the next Login' button) and thereby disable the entire Welcome Message starting next session.

  Any changes made to the Welcome Message are stored in the Actions Journal.

Figure 5-20: Welcome Message Settings

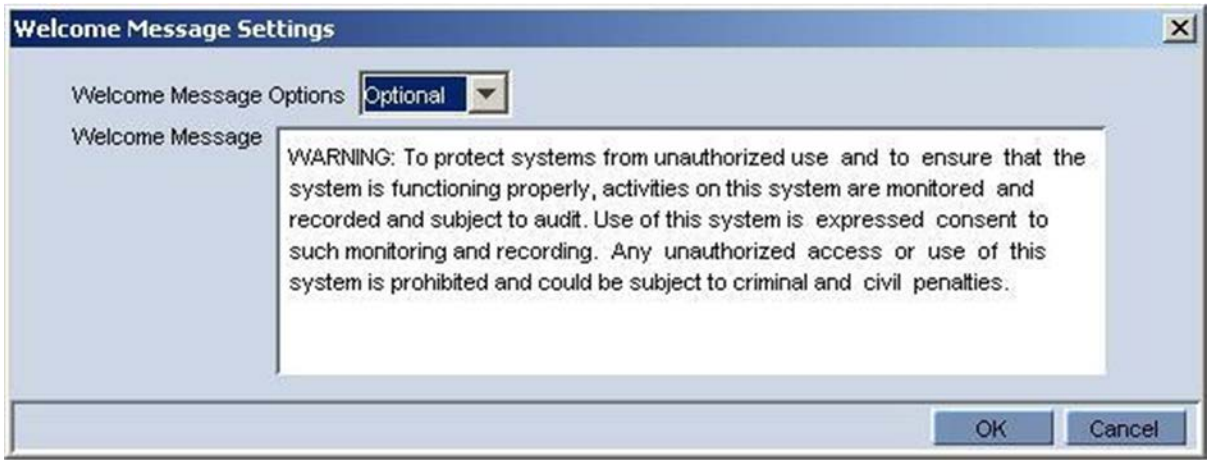
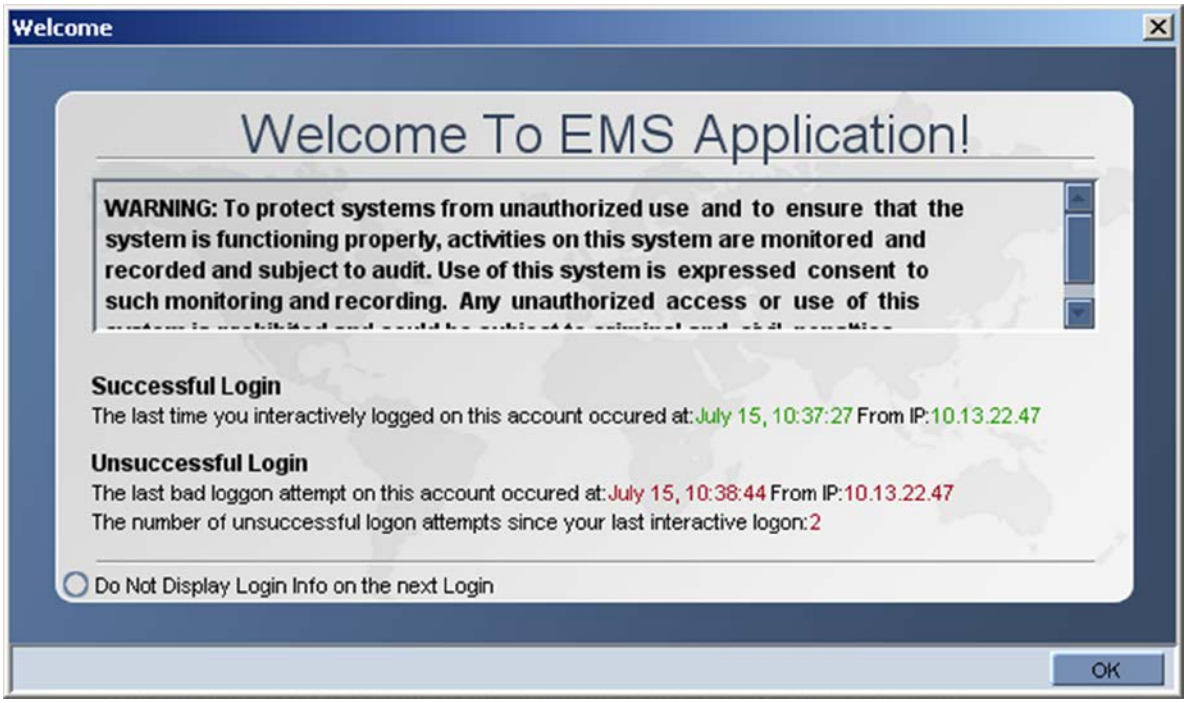


Figure 5-21: Welcome Message with Login Information

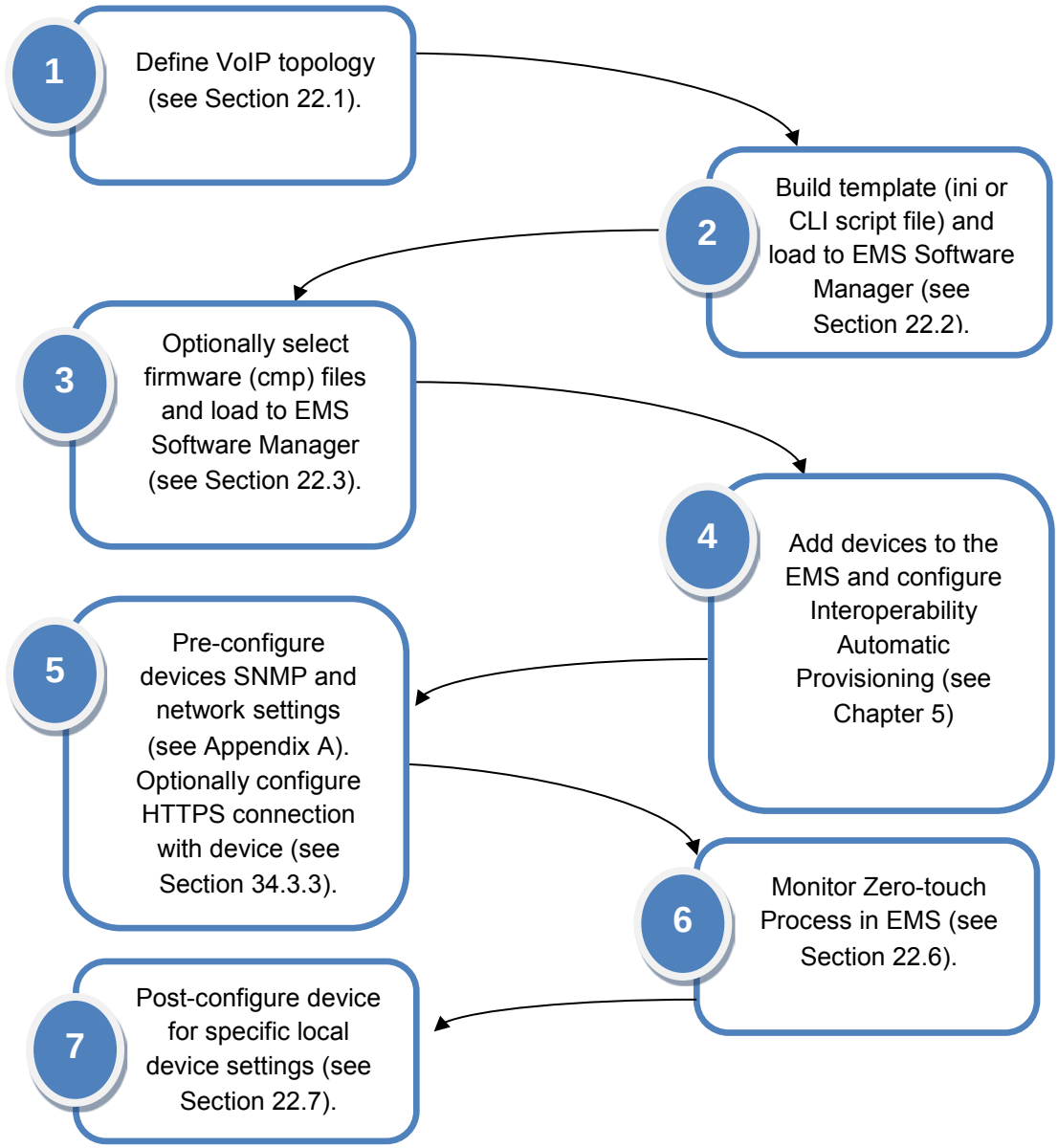


6 Interoperability Automatic Provisioning

The Interoperability Automatic Provisioning feature enables the mass deployment of multiple devices in your network. This is achieved by providing an automated mechanism for loading configuration and firmware files to new devices, using EMS. This feature offers an almost plug-and-play experience for quick-and-easy initial deployment of multiple devices in the customer network. Interoperability Automatic Provisioning requires only minimal pre-configuration of the device for SNMP and network connectivity. Once the new device and EMS connection is configured, the template configuration file (ini) can automatically be loaded to the device upon power up. In addition, a firmware file (.cmp) can also be optionally loaded.

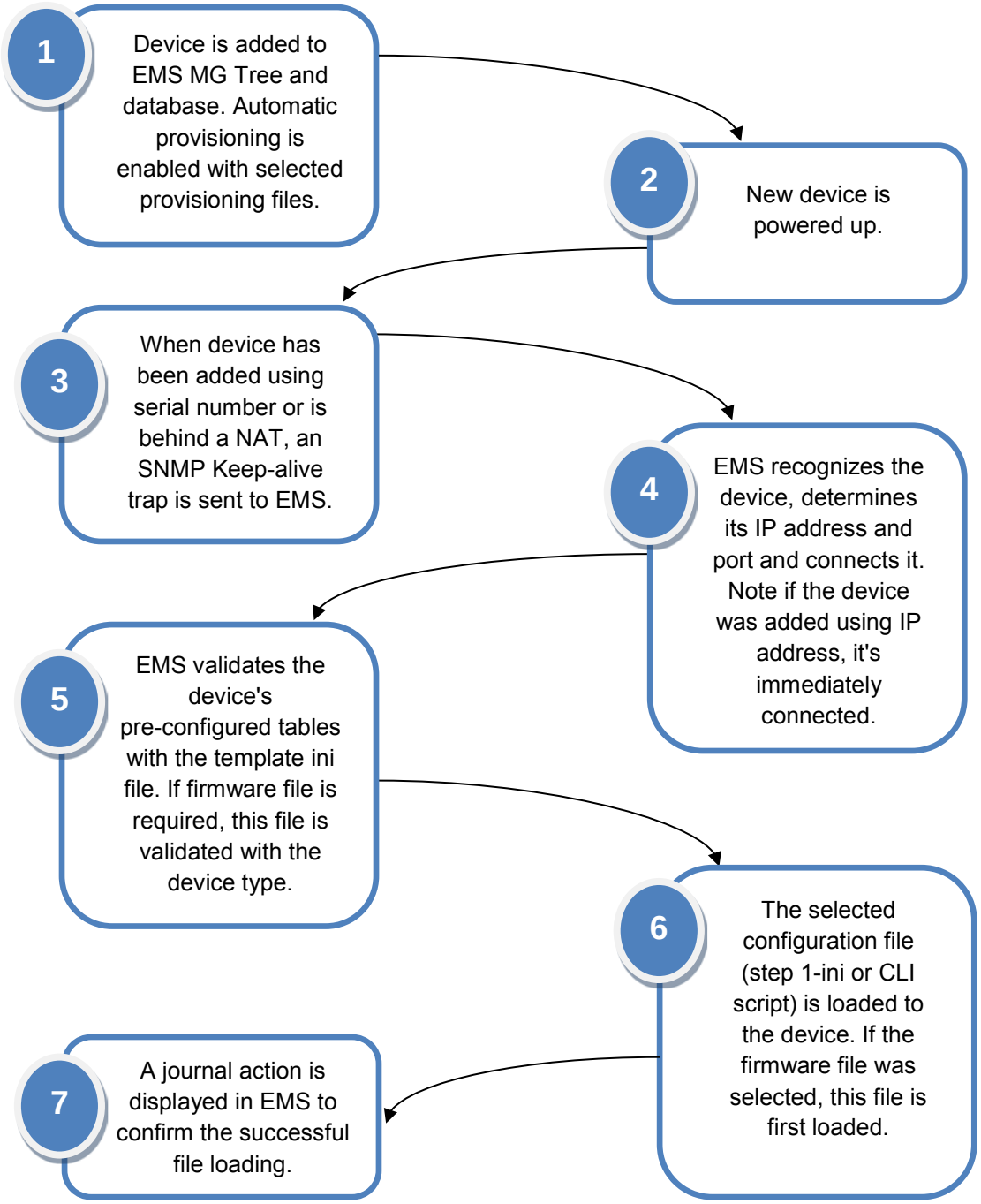
The following figure guides you step-by-step through the required actions in the Interoperability Automatic Provisioning process with the appropriate procedure references:

Figure 22-1: Interoperability Automatic Provisioning Configuration and Monitoring Flow



The following figure illustrates the Interoperability Automatic Provisioning process flow.

Figure 22-2: Interoperability Automatic Provisioning Process Flow



6.1 Step 1: Defining Enterprise VoIP Topology

The Enterprise's VoIP network topology includes the deployment of AudioCodes devices and other different components. The configuration of the AudioCodes devices is determined by which components are deployed and the interconnectivity requirements for the different call legs between these components. The following sections provide a checklist for accounting for these components and their deployment requirements in the VoIP network topology.

6.1.1 AudioCodes Devices

- SBC, E-SBC or Gateway Vendor
- Models
- Software Version
- Protocol
- Additional Notes

6.1.2 SIP Trunking

- Vendor/Service Provider
- Model
- Software Version
- Protocol
- Additional Notes

6.1.3 Microsoft Lync Server

- Vendor
- Model
- Software Version
- Protocol
- Additional Notes

6.1.4 Contact Center

- Vendor
- Software Version
- Protocol
- Additional Notes

6.1.5 IP-PBX

- Vendor
- Software Version
- Protocol
- Additional Notes

6.1.6 Environment Setup

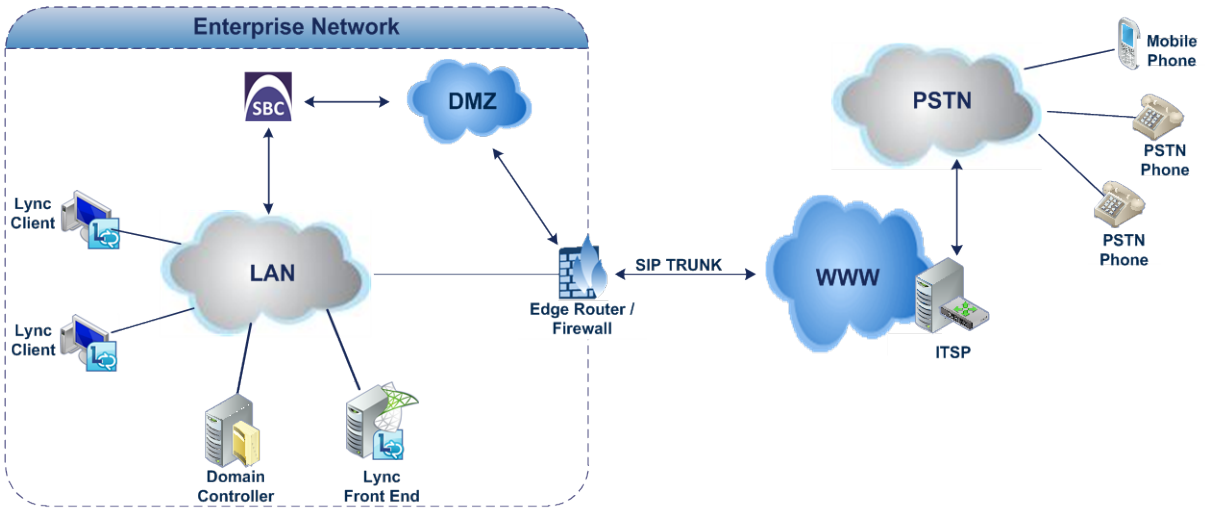
The table below illustrates an example environment setup:

Table 22-1: Environment Setup

Area	Setup
Network	▪ IP-PBX-NET environment is located on the Enterprise's LAN ▪ SIP Trunk is located on the WAN.
Signaling Transcoding	▪ IP-PBX-NET operates with SIP-over-TLS transport type. ▪ SIP Trunk operates with SIP-over-UDP transport type.
Codecs Transcoding	▪ IP-PBX-NET supports G.711A-law and G.711U-law coders. ▪ SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder.
Media Transcoding	▪ IP-PBX-NET operates with SRTP media type. ▪ SIP Trunk operates with RTP media type.

The following figure illustrates an example topology for the Microsoft Lync environment in the LAN connecting to a SIP trunk and PSTN network (note, you can edit this example template file by double-clicking to open the Microsoft Visio object).

Figure 22-3: Example Network Topology-Microsoft Lync with SIP Trunk



6.2 Step 2: Building a Template File

Before you provision the devices, you need to build the generic ini template file that you wish to apply to the devices in the Enterprise's site deployment.

The generic ini file should be built according to the VoIP topology defined in Step 1 (see Section 22.1). The file should include a full configuration of a device as you wish it to be implemented in the Enterprise site. For example, a generic configuration may include an IP Profile which defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method). For example, the IP Profile may be configured for the Microsoft Lync Server to operate in secure mode using SRTP and TLS and for the SIP trunk to operate in non-secure mode using RTP and UDP.

The generic ini file could be generated using:

- Using AudioCodes Mediant SBC Configuration Wizard - a user-friendly online tool that enables you to quickly and easily build template configuration files based on a library of existing configurations that have already been implemented and tested. For example, a configuration that sets up calling between an Enterprise which deploys Microsoft Lync in its local network to a specific proprietary SIP Trunking Service. The Wizard takes engineers step-by-step through the setup process, presenting clear and easy-to-understand configuration options.
- Using a Lab device (same type) - you can take the ini file configuration of an existing device in the Enterprise's network that best represents a typical configuration that can be replicated to multiple devices.
- Using Professional Services or Customer Support team with their vast experience in generating ini files.

An example template ini file is illustrated in Appendix B. Once the ini file is generated, it can be added to the EMS Software Manager (see Chapter 4).

Notes:

- For information on purchasing the SBC Configuration Wizard, contact your AudioCodes sales representative.
- For assistance in building ini files, contact your AudioCodes Customer Support or Professional Services representative.

6.3 Step 3: Selecting Firmware Files (Optional)

You can also optionally pre-provision devices with firmware files. Ensure that the files that the selected files are for Version 7.0 firmware and that they match the device types that you wish to pre-provision. See Chapter 4 for instructions on how to add firmware files to the EMS Software Manager.

6.4 Step 4: Adding Devices to EMS and Enabling Interoperability Automatic Provisioning

Use the regular procedure for adding devices to the EMS and to enable the Interoperability Automatic Provisioning feature. You can optionally add the devices to pre-provision using its IP address or its serial number (see Section 5.3.3).

6.5 Step 5: Pre-Configuring Devices

You must pre-configure the device's network and S NMP settings as described in Appendix A. These settings are necessary for establishing the device connection with the EMS for the pre-provisioning process and thereafter.

If you wish to configure an HTTPS connection between the EMS and the device for the provisioning process and thereafter, you must do the following:

- Enable HTTPS ("Enable HTTPS Connection") when adding the devices to the EMS (see Section 5.3.3 on page 82).
- Pre-configure the devices for securing this process and thereafter to maintain an active HTTPS connection after the template file has been loaded to the device (refer to the *EMS Server IOM* manual).

6.6 Step 6: Monitoring Interoperability Automatic Provisioning Process in EMS

The following describes the Automatic provisioning process according to the method which you added the device to the EMS:

- f you have added the device to the EMS using a serial number:

  When you added the device to the EMS, it is initially displayed as an Unknown device  until it's fully connected to the EMS. The device is connected to the network when the EMS receives an SNMP keep alive trap (which you configured in Appendix A.

  Once the keep-alive trap is received, and the device is recognized, the IP address and port is determined and then it can be connected to the network. Once the device is successfully connected, the pre-configured configuration and optionally firmware files are loaded.

- If you have added the device to the EMS using an IP address:

  If when you add the device to the EMS, it is already connected to the network; therefore the pre-configured configuration or firmware file is immediately loaded. If the device is not connected to the network, it is initially displayed as an

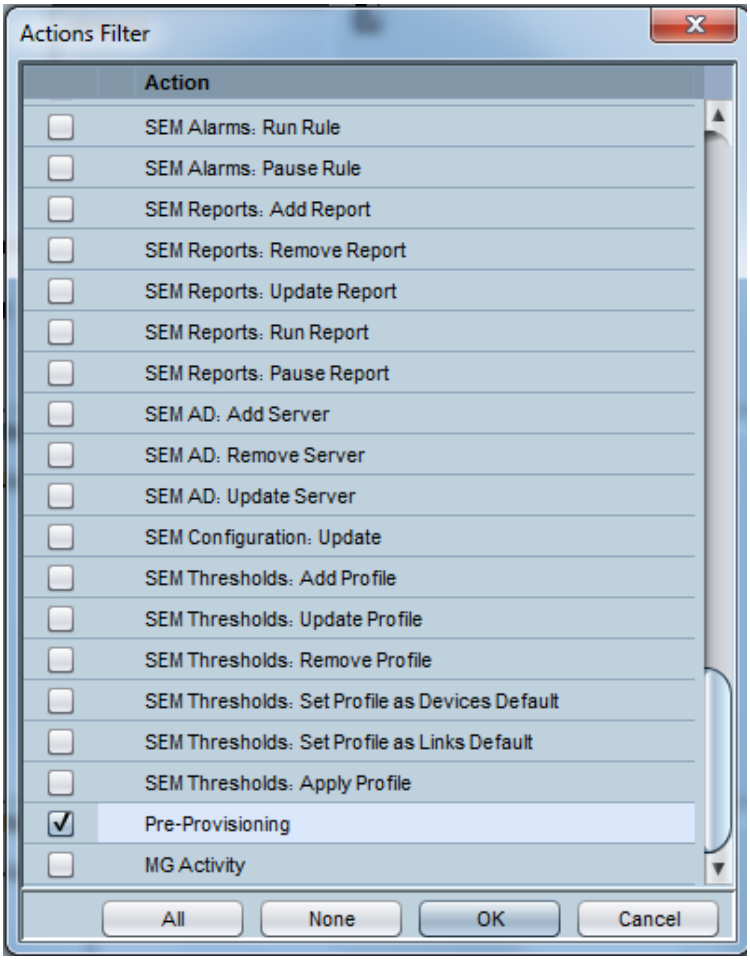
Unknown device  until it's fully connected to the EMS. The Pre-provisioning process only starts once the device is fully connected to the EMS.

If your devices are located behind a NAT and therefore you configured an SNMP keep-alive trap (see Appendix A.2) the process is the same as described above for the serial number method.

6.6.1 Successful Provisioning

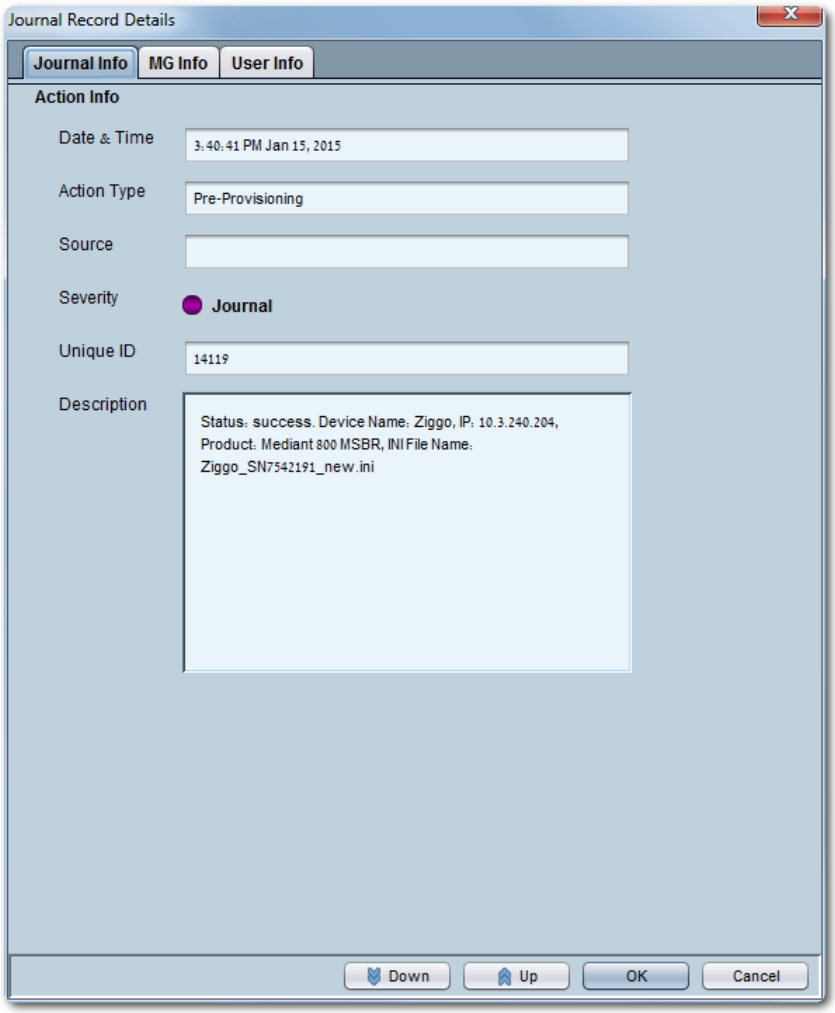
You can monitor the automatic provisioning process in the Actions Journal. You can filter the Actions Journal screen to view the Pre-provisioning related events:

Figure 22-4: Actions Filter



When a device has been successfully pre-provisioned with the appropriate configuration or firmware, a journal record similar to the following is displayed in the EMS Actions Journal:

Figure 22-5: Journal Record Details - Successful Pre-Provisioning



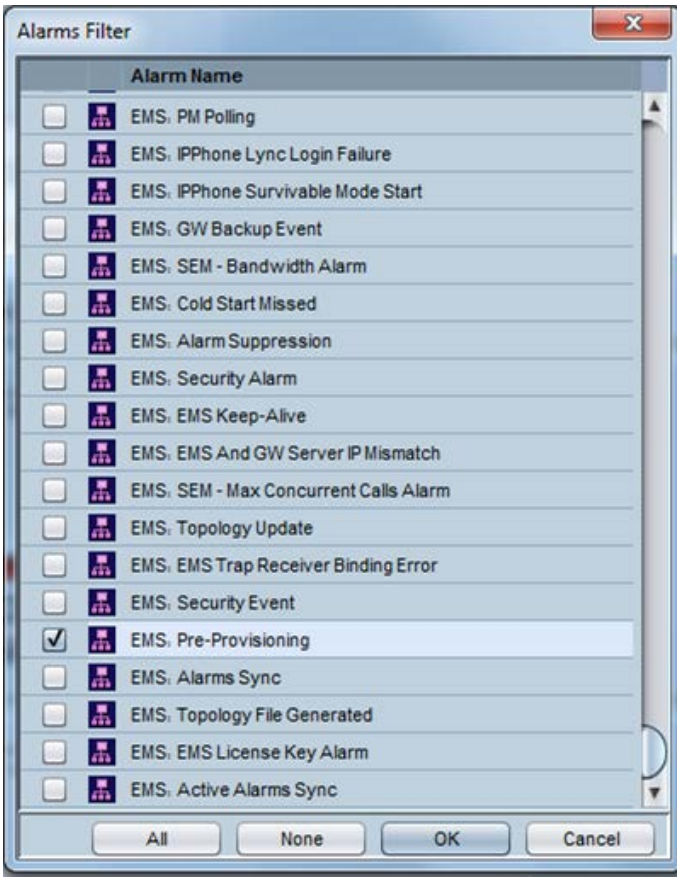
Notes:

- After the process has completed, you cannot change the Pre-provisioning settings (change the selected .cmp or ini file). If you wish to reload different configuration files to the device using this feature, you need to remove the device from the EMS and re-add it (see Chapter 5.)
- When a device is removed from the EMS, the EMS Server IP address in the Trap Destination Rule is reset to 0.0.0.0. Consequently if you re-add the device to the EMS, you need to also reconfigure this IP address in the SNMP Trap Destinations table (see Appendix A.3).

6.6.2 Unsuccessful Provisioning

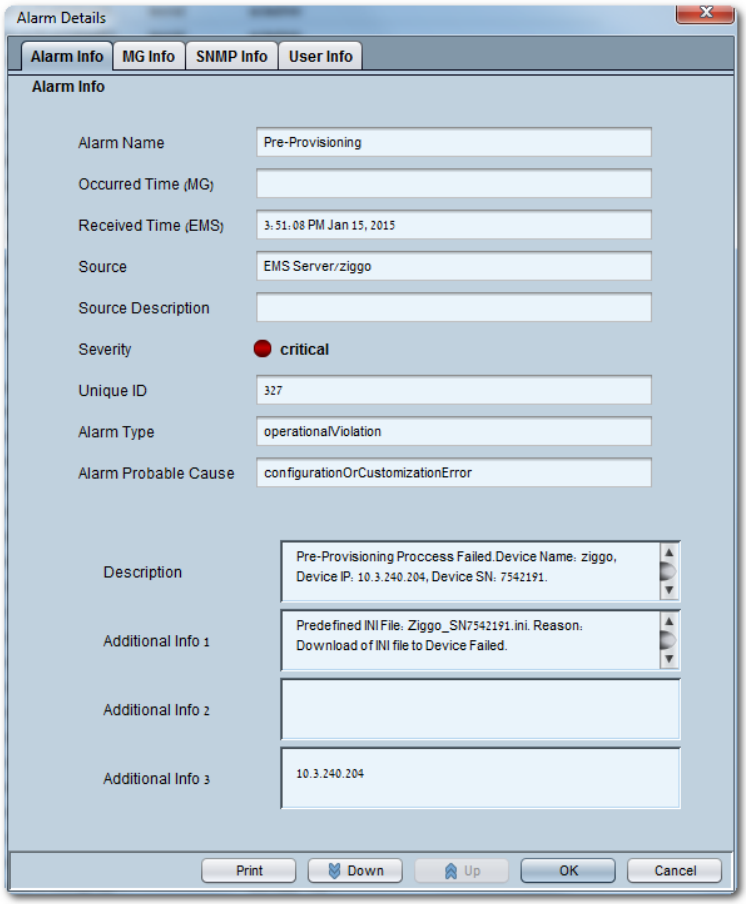
The Interoperability Automatic Provisioning process may not succeed due to various factors as described in this document. You can filter the Alarm browser to display the Interoperability Automatic Provisioning-related critical events:

Figure 22-6: Alarms Filter



When the Pre-Provisioning of the device is not successful, a critical event similar to the following is raised:

Figure 22-7: Alarm Details-Pre-Provisioning Process Failure



Note: When an attempt to download the ini file or cmp to the device using this feature fails and a critical event is raised, you cannot reload these files using this feature as the device has already been connected to the EMS. Instead, you must download the configuration or firmware file to the device using the Software Manager and then use the 'Software Upgrade' action (in the EMS Action's bar) (see Chapter 19).

6.7 Step 7: Post-Provisioning Device Configuration

After the template file is deployed on the devices, you may need to customize the configuration of specific devices to suite the specific requirements of different Enterprises or the different sites within an Enterprise. For example, an Enterprise may have different sites which each connect to the same SIP Trunking service; however, in the local network for each site, different IP-PBXs or different Lync Front-Ends and DCs are deployed. As a consequence, different configurations are required. For example, for IP Network Interfaces, Proxy Sets, IP Groups and SIP Interfaces configuration. In addition, you may, for example, in an SBC deployment with a SIP Trunking service, desire to register each IP-PBX in the SIP Registration Accounts table. This may be required for security reasons, where the SBC registers each of its Enterprise customers IP-PBXs with the SIP Trunk for securing calls from the IP-PBX to the SIP Trunk via the SBC. The SIP Trunk therefore only provides service to the Enterprise IP-PBX user after it is authenticated (the SIP Trunk does not require registration). In this configuration, the Served IP Group is the Enterprise's IP-PBX (e.g. IP Group 1) and the Serving IP Group is the Service Provider's SIP Trunk (e.g. IP Group 2). In this example, customized configuration is required for each of the Enterprise's different sites because the Service Provider provides a unique username and password for each registered account (for more information, refer to the relevant *SIP User's Manual*).

Note: AudioCodes highly recommends that you consult with AudioCodes Customer Support or Professional Services to plan for special configuration issues such as the examples described above.

Part II

Status Monitoring and Navigation Concepts

This section describes the various status monitoring and navigation concepts.

7 Monitoring Multiple Devices

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

Following are the EMS status components:

- 'Regions List' on page 117
- 'MGs List' on page 118

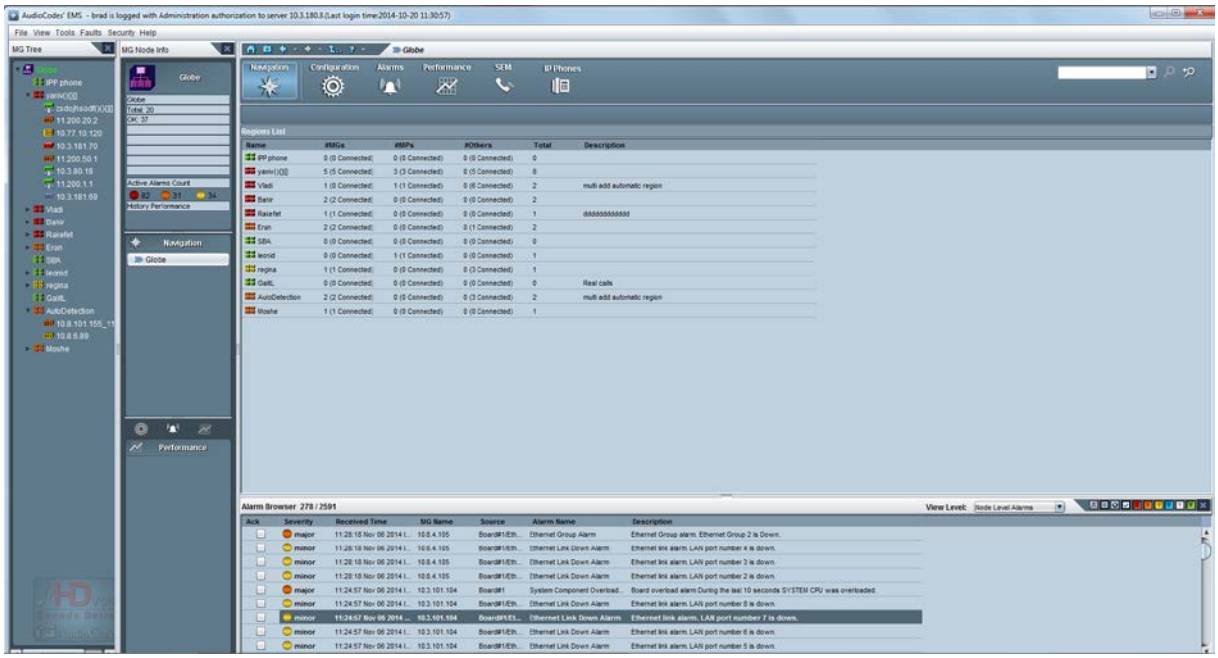
7.1 Regions List

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 6-1: Regions List



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

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

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

- Description

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

An unknown device 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 device severity in each region. For example, when in a specific region there is a single device with a major severity and several devices 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 devices 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.

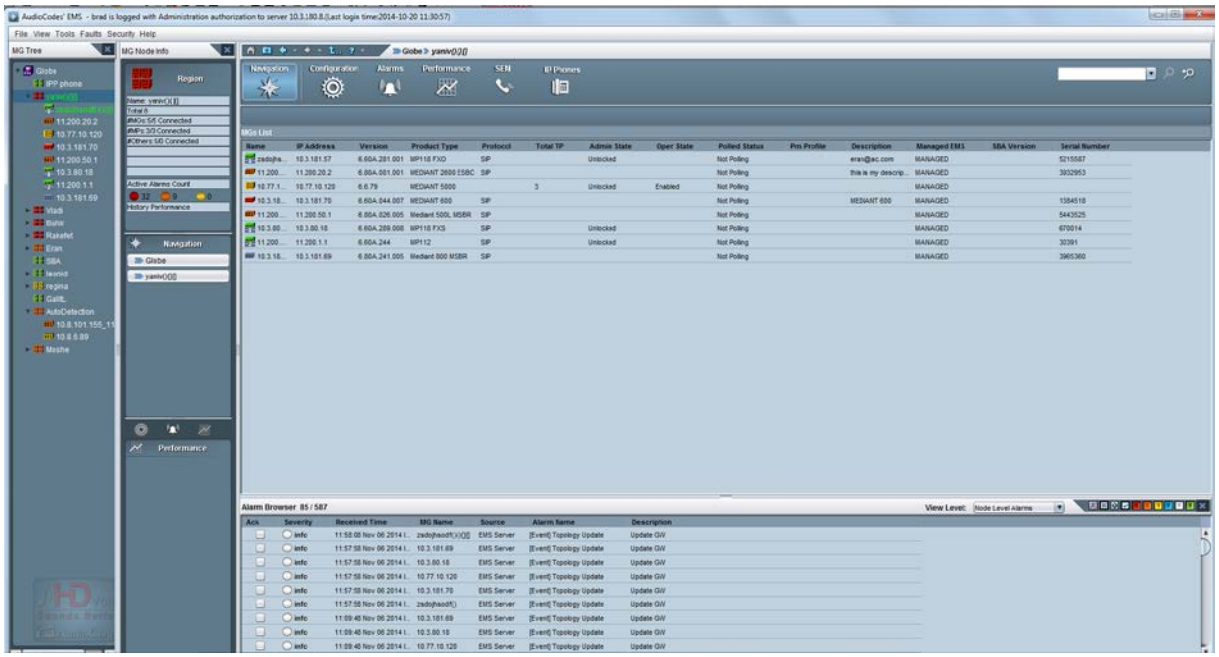
7.2 MGs List

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 devices located under this region.
2. **Mediant 5000 and Mediant 8000**: Click **Lock** or **Unlock** in the Actions bar.
3. **CPE and Boards**: 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 6-2: MGs List



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

- Device name & status (status is indicated by the color coding)
- Device 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 and Mediant 8000.
- Administrative State (Shut Down/Locked/Unlocked) - relevant to the Mediant 5000 and Mediant 8000.
- Operational State (Enabled/Disabled) - relevant to the Mediant 5000 and Mediant 8000
- 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.
- Description
- Managed EMS – Managed or not according to EMS feature key
- SBA Version
- Serial Number

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 device severities as follows:
  - **Globe Level** - Alarm severity and connection status of all devices managed by the EMS server, categorized according to regions (each region is represented by a bar chart that is divided according to alarm severity and connection statuses).
  - **Region Level** - Alarm severity and connection status of all devices loaded to a specific region categorized according to the device product (each device product is represented by a bar chart that is divided according to alarm severity and connection statuses).

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

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

The four example views are displayed below:

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

Figure 6-3: Globe Level - TPs

Figure 6-4: Globe Level – CPEs

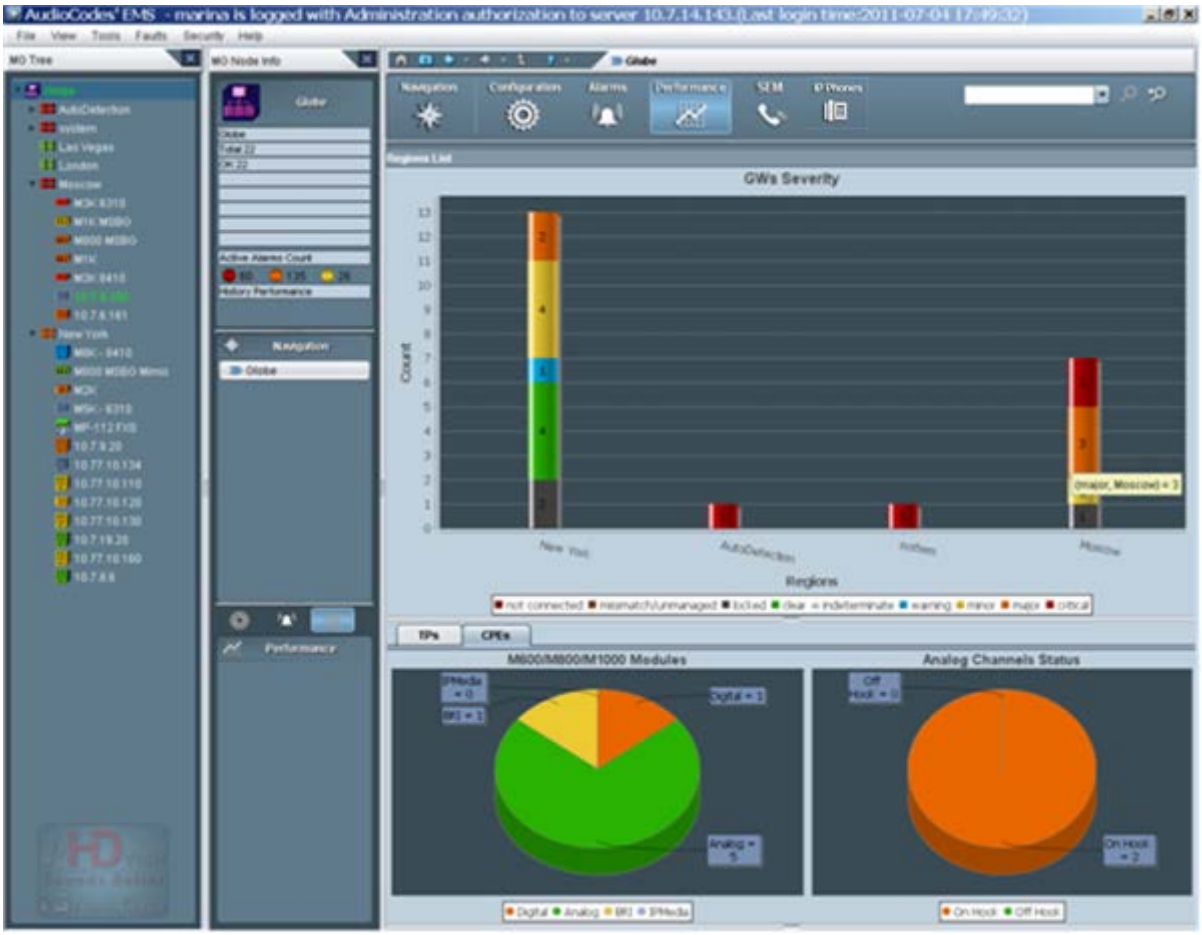


Figure 6-5: Region Level – TPs

Figure 6-6: Region Level – CPEs

7.4 Device Level Status Pane

This section describes how to access the device level status pane.

➢ To access a device:

1. Do one of the following:
   - In the MG Tree, expand the region under which the device is located and click the device; 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 device; a message appears indicating “Contacting Server. Please Wait;” a graphic representation of the device is then displayed (refer to the figures below).
2. Click the **Up** button in the board-level screens to navigate back up a level.

This page is intentionally left blank.

8 Mediant 5000 and Mediant 8000 Devices

This section describes the elements of the Mediant 5000 and Mediant 8000 status panes.

8.1 Mediant 8000 Status Pane

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

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

Figure 7-1: Mediant 8000 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 provides users with relevant additional information.
  - The SAT card  has the following color convention:

Table 7-1: 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 7-2: 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 7-2: SAT Properties screen

- Shelf LEDs  :

  Five LEDs summarize the device'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 7-3: 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:

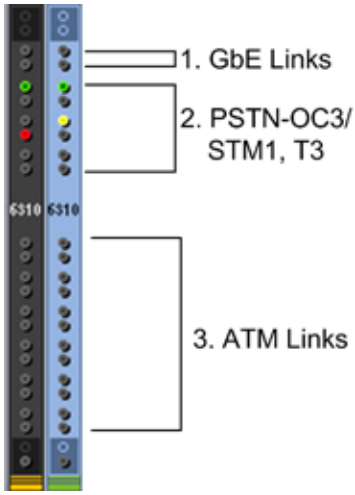
Figure 7-4: 6310 Board-Active and Redundant Status

- 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 7-5: 8410 Board-Active and Redundant Status

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

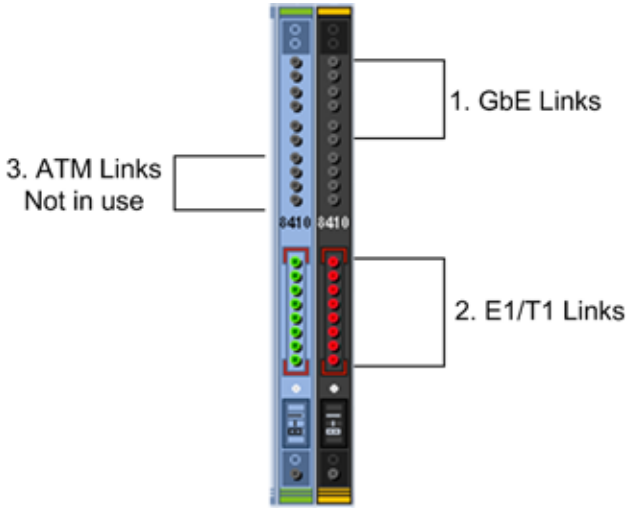
Figure 7-6: 6310-LED Status



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 7-7: 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 7-8: ES/6600 Board Status

Figure 7-9: 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 7-10: Power Status

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

Figure 7-11: 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'.

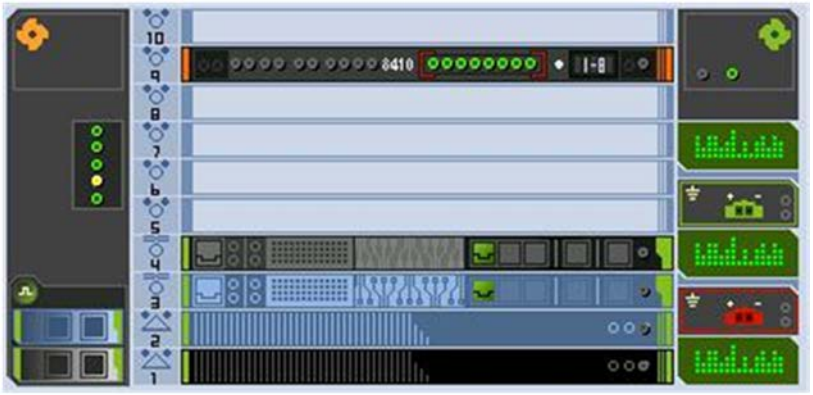
8.2 Mediant 5000 Status Pane

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

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

Figure 7-12: Mediant 5000 6310 Status Pane

Figure 7-13: 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 7-3: 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 7-4: 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 7-14: SAT Properties Screen

- Shelf LEDs  :

  Five LEDs summarize the device'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 7-15: 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 7-16: 6310 Active Board Status

Figure 7-17: 6310 Redundant Board Status

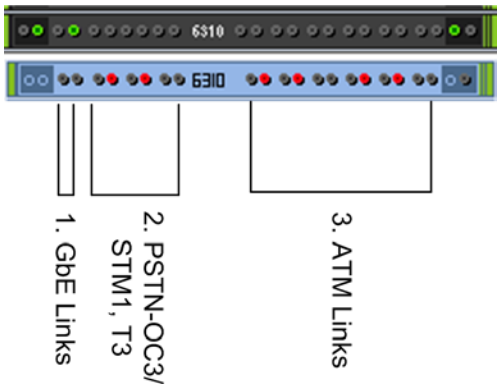
  - ♦ Background color: Dark Gray = Active board; Blue = Redundant board
  - ♦ Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity, Yellow = Minor Severity, Blue = Warning Severity, White = Indeterminate Severity
  - ♦ TP Switchover: The active TP board, after switchover, 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 7-18: 8410 Active Board Status

Figure 7-19: 8410 Redundant Board Status

  - ♦ Trunk (E1/T1) LED color convention: Red = Disabled; Green = Enabled; Gray = Locked
  - LED Group status-TP-6310:

Figure 7-20: 6310 Board-LED Status

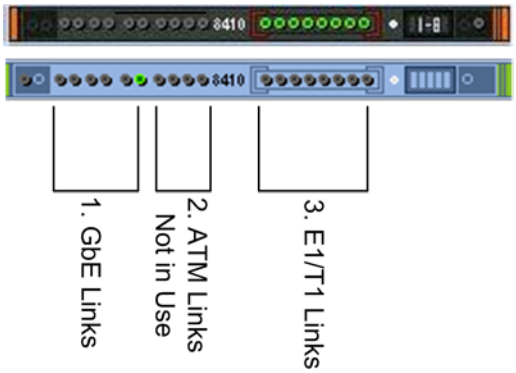


Legend

- 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 7-21: 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 7-22: ES Board Status

Figure 7-23: 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 7-24: Power Supply Status

- Color convention: Red = Failed; Green = OK

- PEM (Power Entry Module) status:

Figure 7-25: 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 devices' 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 device.

Figure 7-26: Device Level Navigation Buttons (Part 1)

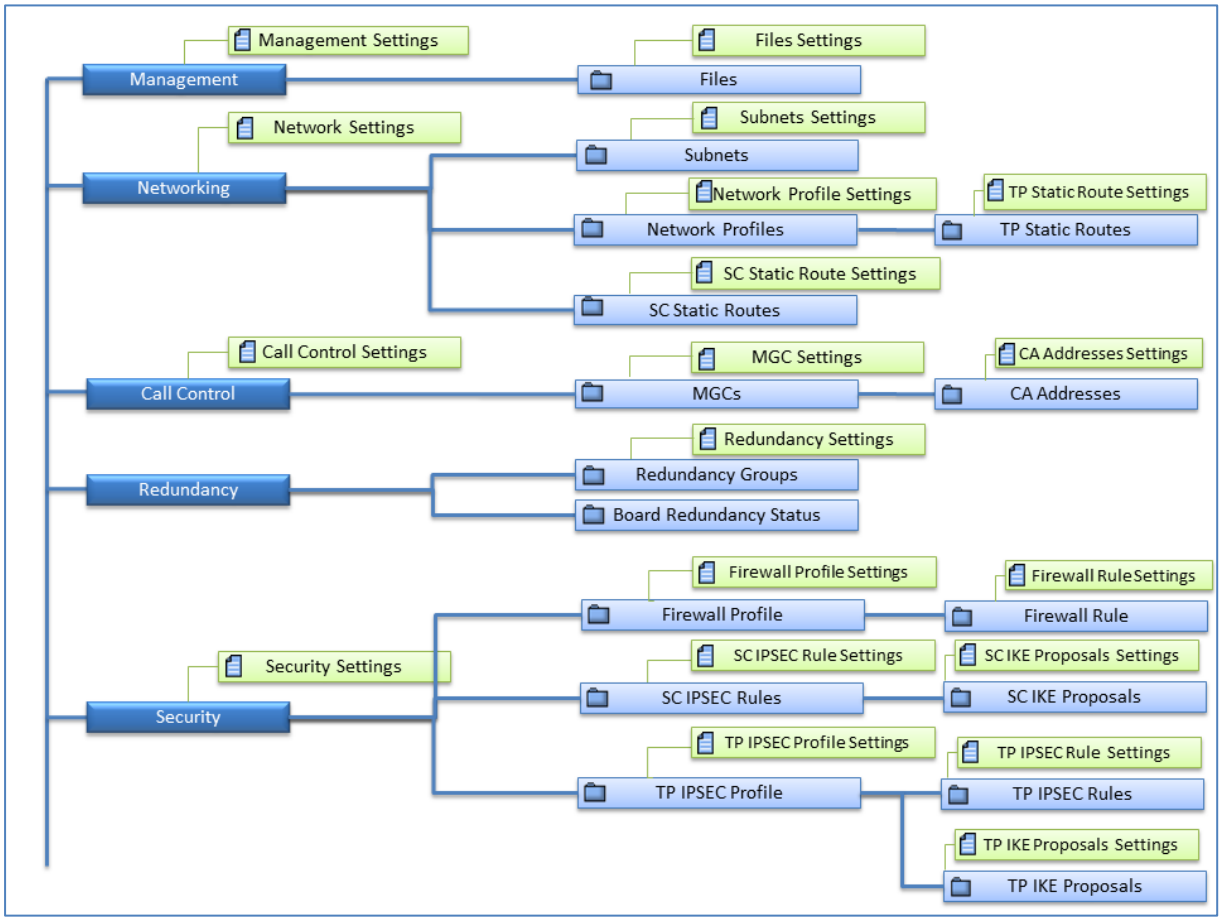
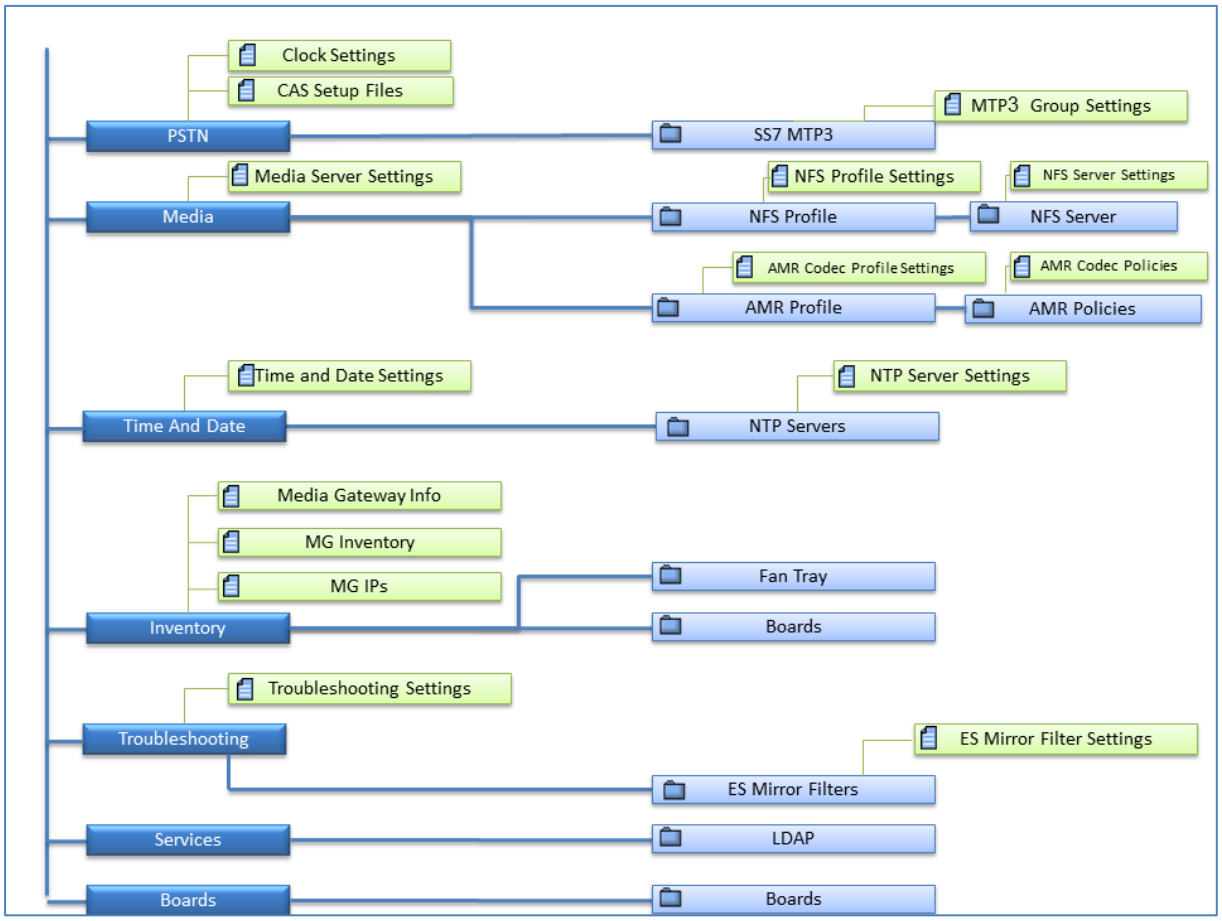


Figure 7-27: Device Level Navigation Buttons (Part 2)

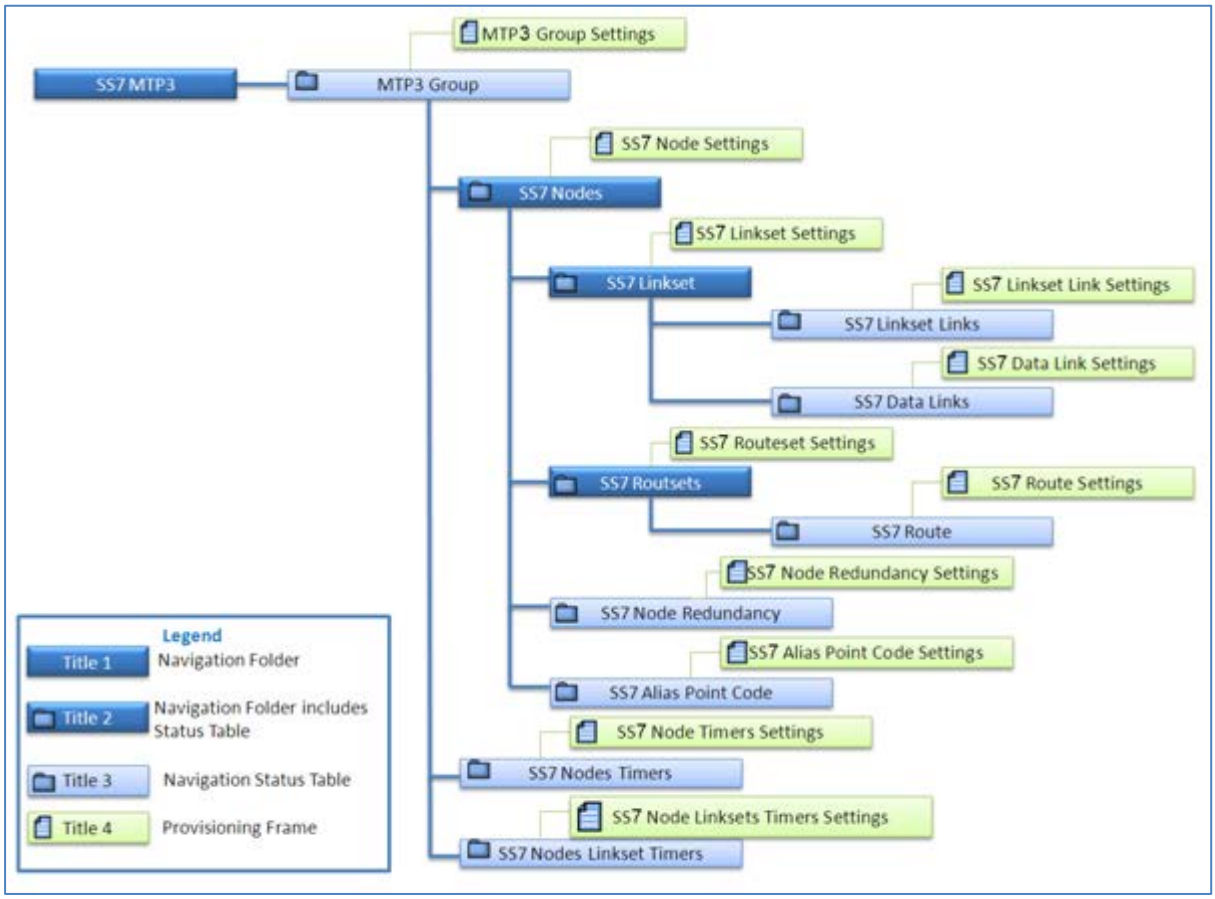


For more information, refer to the relevant *IOM Guide.*

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 7-28: 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 device:**

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

Table 7-5: Board Actions

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

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 7-6: 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 7-7: 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.

Table 7-7: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
	Move To Slot	Board is Locked	This action moves an existing TP board and its entire configuration to a free slot on the device. 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).
	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	

Table 7-7: Board Maintenance Actions

Board Type	Action	Supported Maintenance Actions	Action Description
	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 7-8: 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.

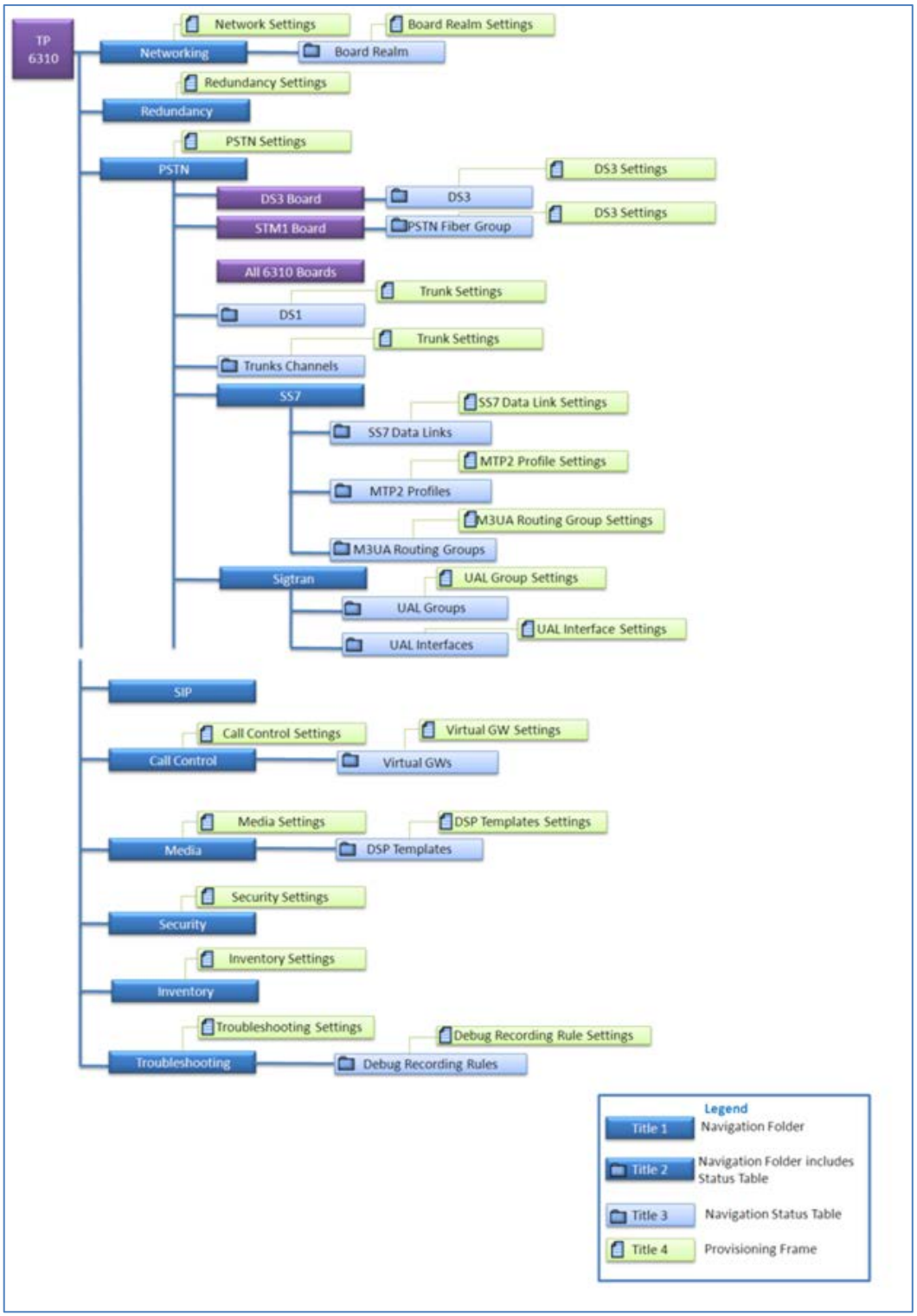
8.5 Accessing a TP-6310 Board

This section refers to the Mediant 5000 and Mediant 8000 devices.

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 board.

Figure 7-29: 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 155.

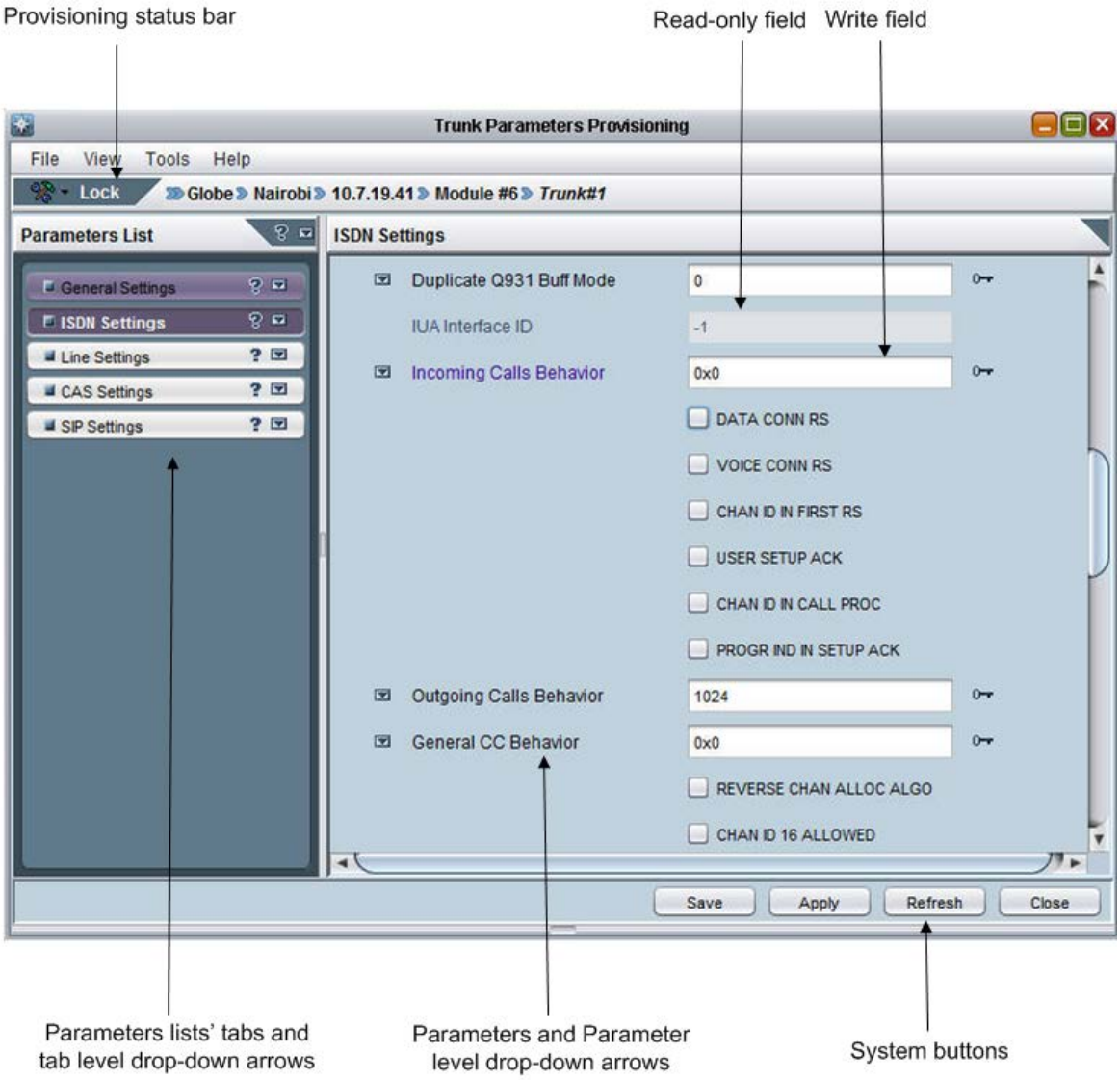
8.5.1 Accessing the TP Board Level Provisioning Screen

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 device 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 7-30: 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:

- 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 7-31: TP-6310 STM1 Board Status Pane

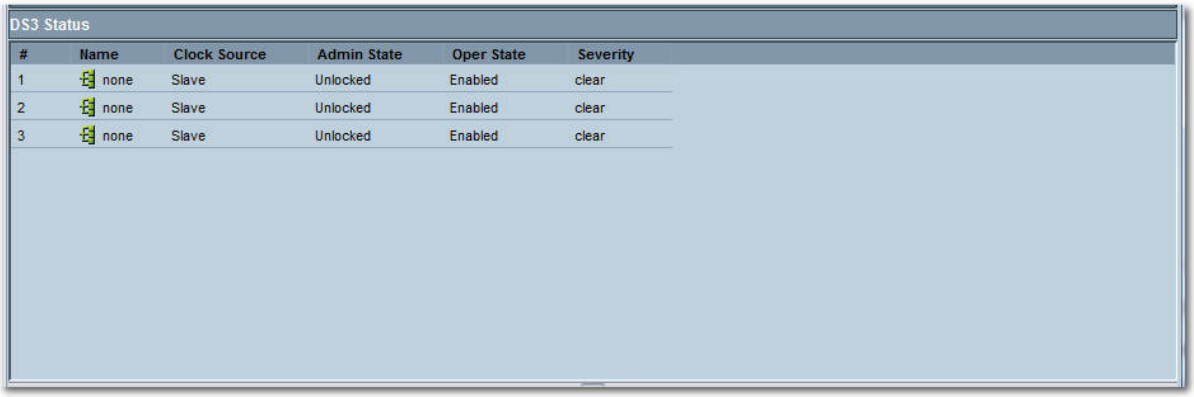
➢ To access the TP-6310 DS3 screen:

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:

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

Figure 7-32: 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 7-33: PSTN Fiber Group (SDH/STM1 Interface) Screen

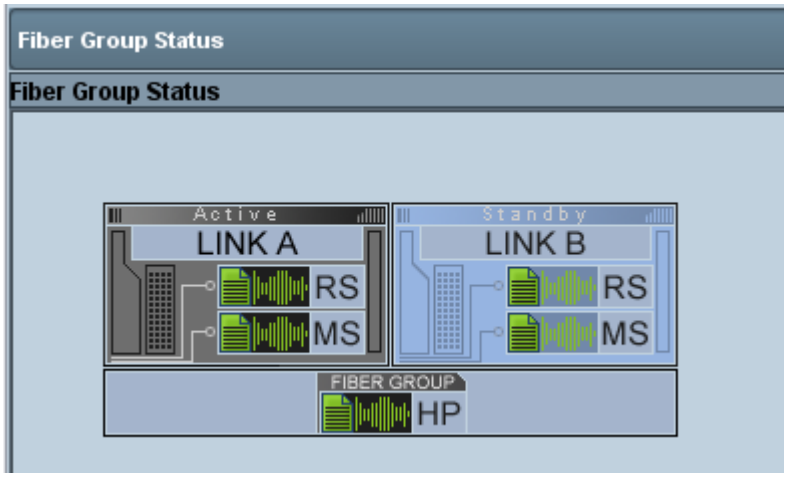
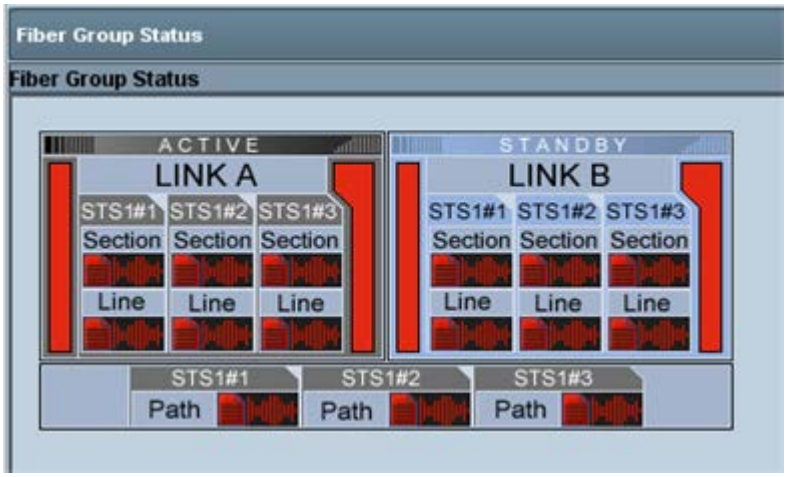


Figure 7-34: PSTN Fiber Group (Sonet OC3/STS Interface) Screen



➢ 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 7-35: 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.

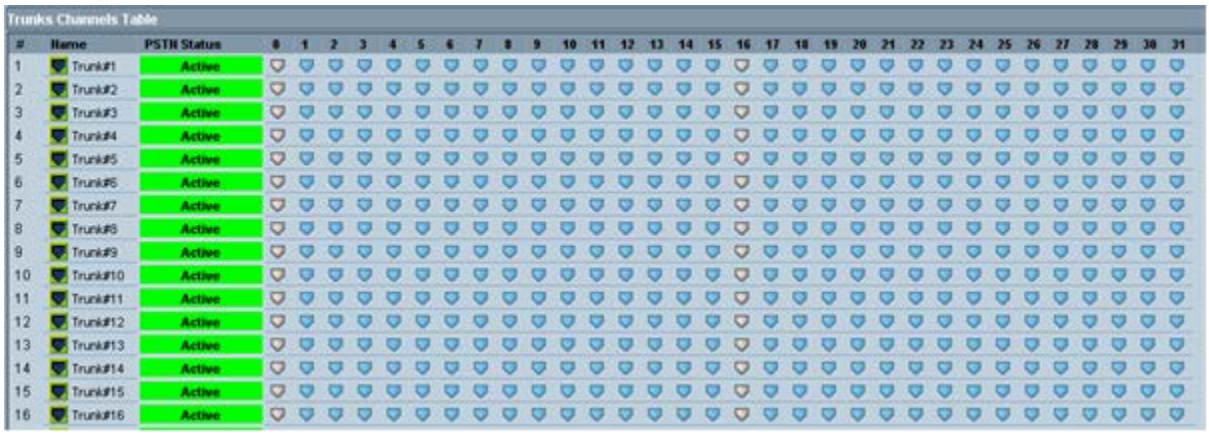
➢ **To access DS1 trunks:**

- 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 device 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 device 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 219.

Figure 7-36: Trunk Channels Status



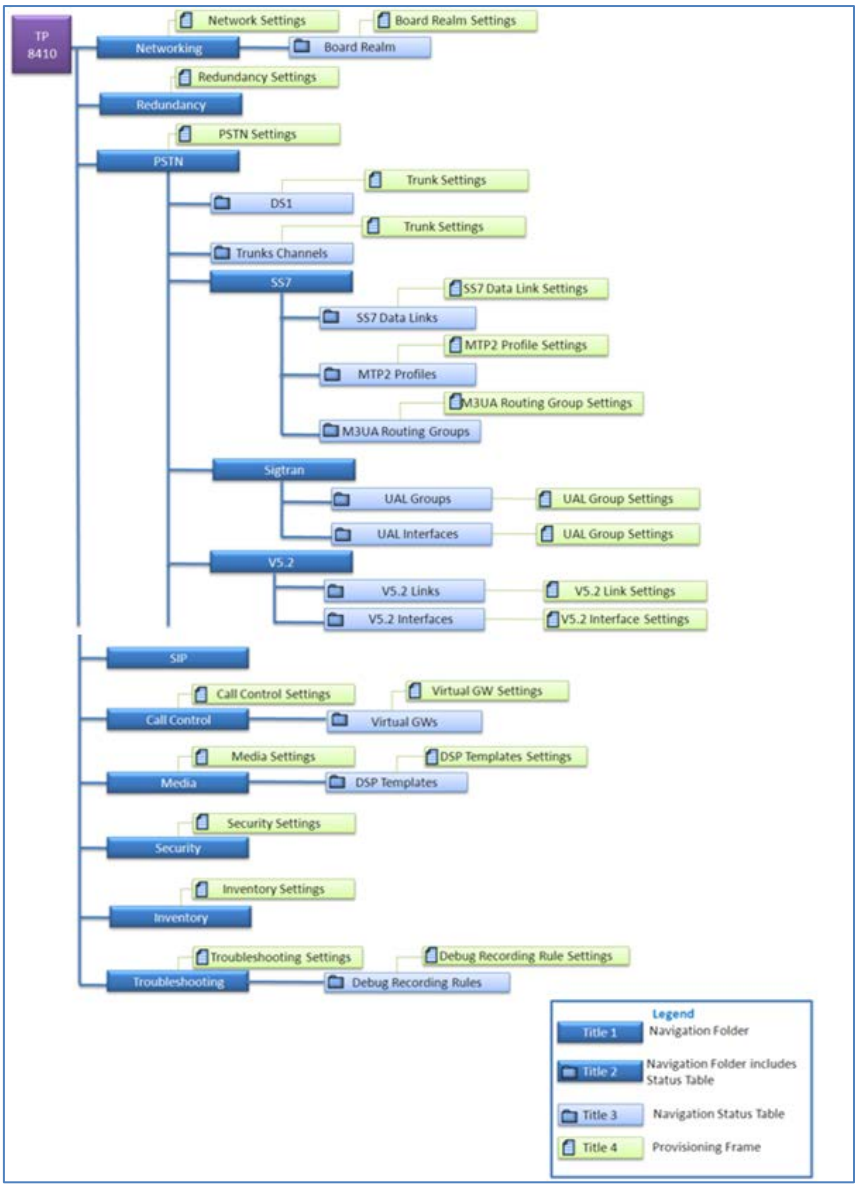
Note: The same actions as described for the 'DS1 Trunks Actions' above are available in the Channel right-click menu.

8.6 Accessing a TP-8410 in the Mediant 5000

The devices' 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 7-37: TP-8410 Board Hierarchy Links



8.7 SIP Provisioning of VoP Board (6310 and 8410)

The devices' 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 7-38: SIP General Hierarchy Links

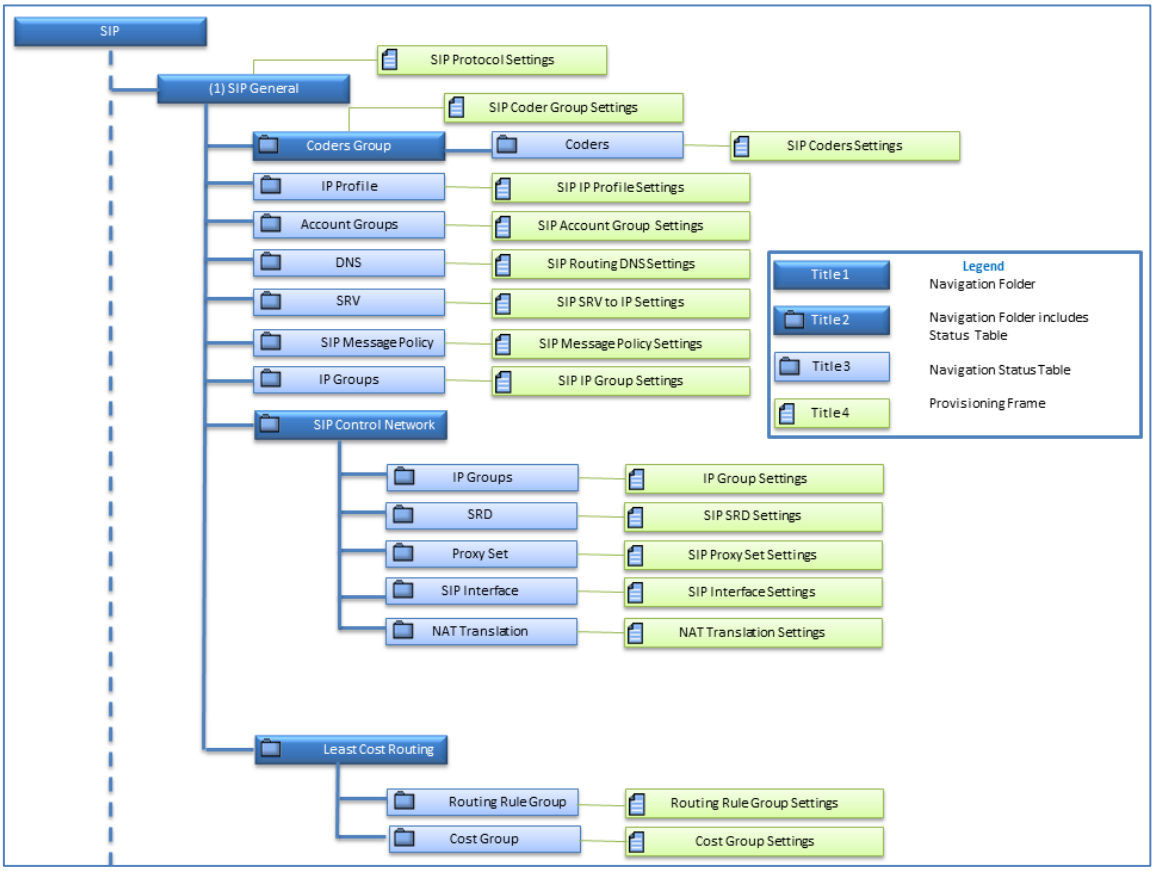


Figure 7-39: SIP GW/IP to IP Hierarchy Links

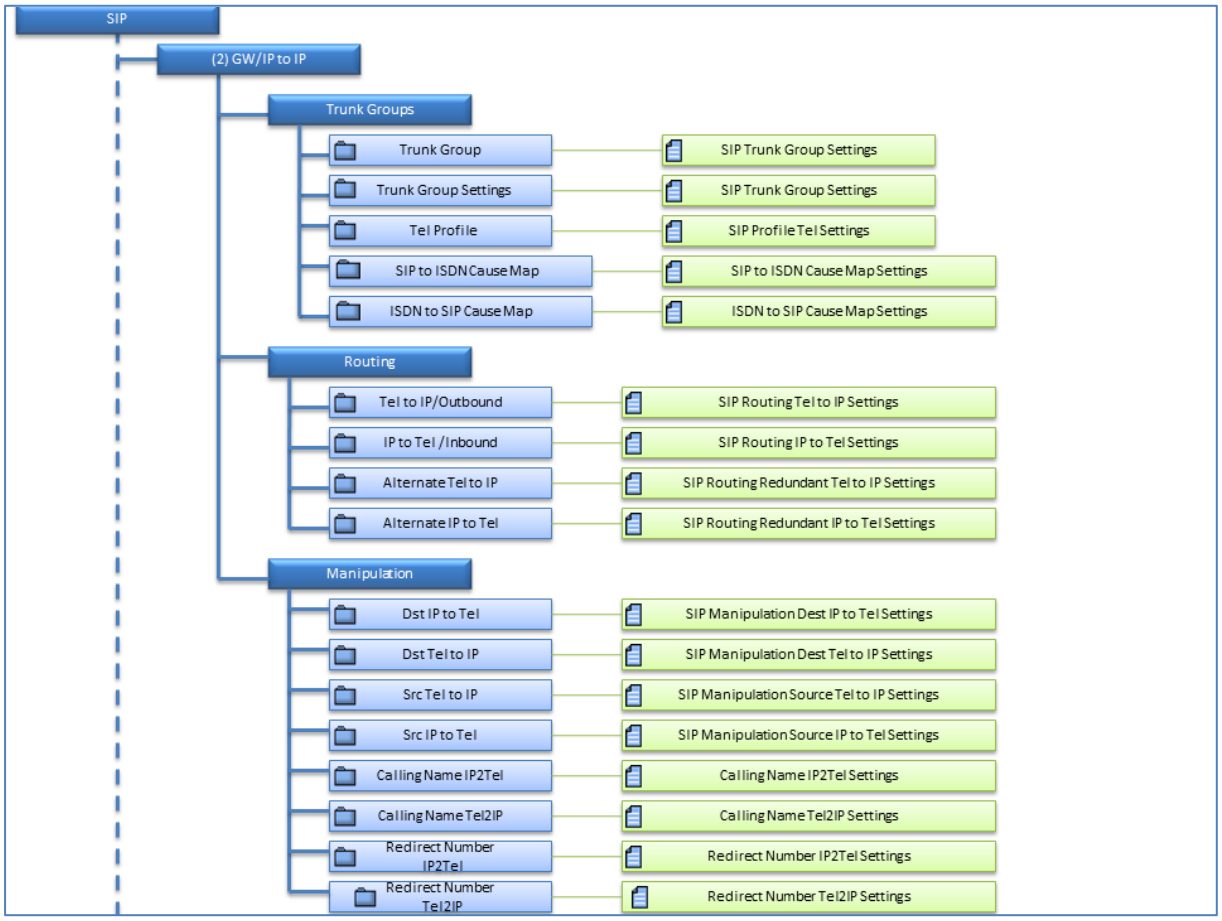


Figure 7-40: SIP SBC Hierarchy Links

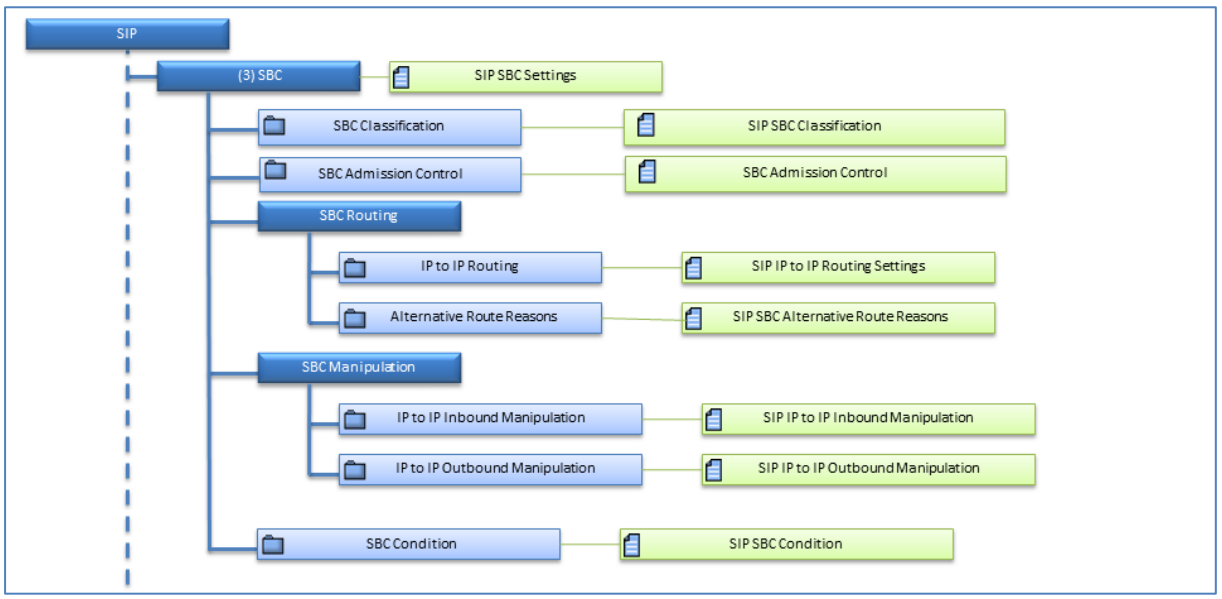
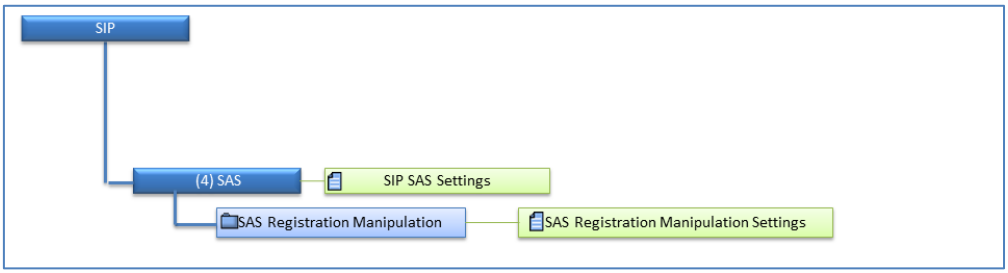


Figure 7-41: SIP SAS Settings

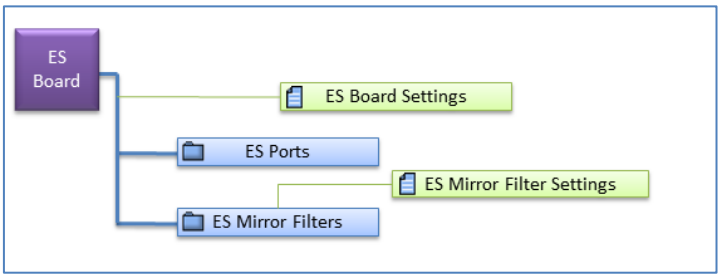


8.8 Ethernet Switch Board's

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 7-42: ES Board Navigation Hierarchy



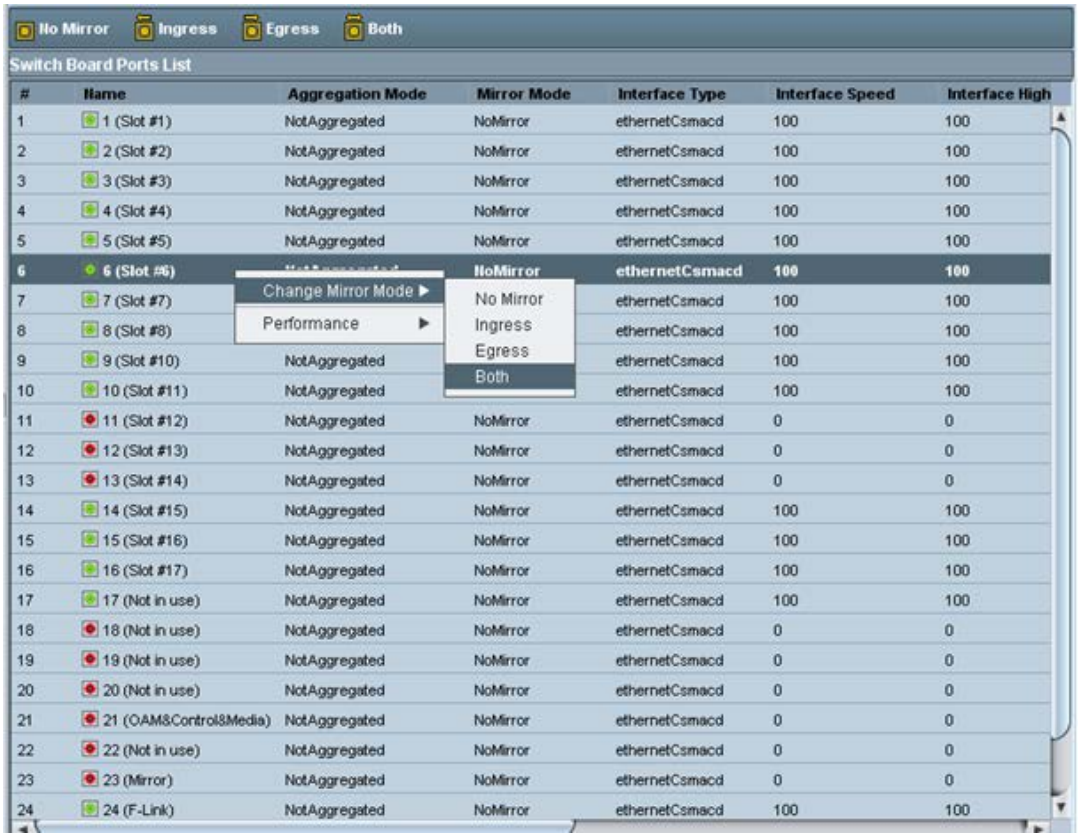
8.8.2 Links' Status

Ethernet Switch boards populate slots 3 and 4 in the Mediant 5000 and slots 9 and 19 in the Mediant 8000. 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 device 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 7-43: 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 mapping which link is connected to each board (the screen for the Mediant 5000 is similar). The mapping differs between the two devices. 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 9000

This section describes the management of the Mediant 9000 device.

9.1 Supported Configuration

The EMS supports the following product configuration:

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

9.2 Initial Configuration

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

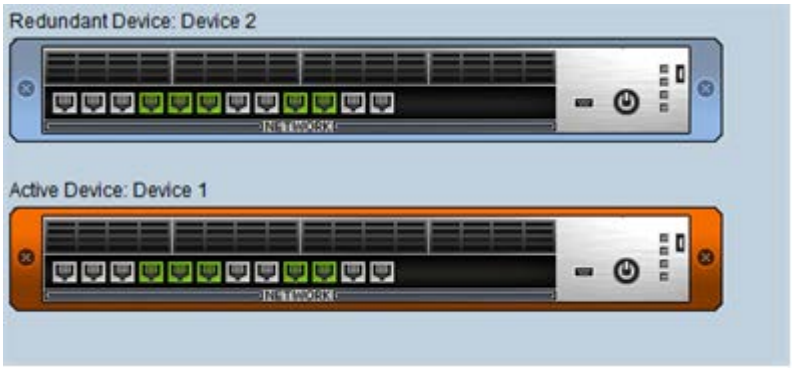
9.3 Status Pane

This Status pane provides the following information:

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

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

Figure 8-1: Mediant 9000 SBC Status Pane

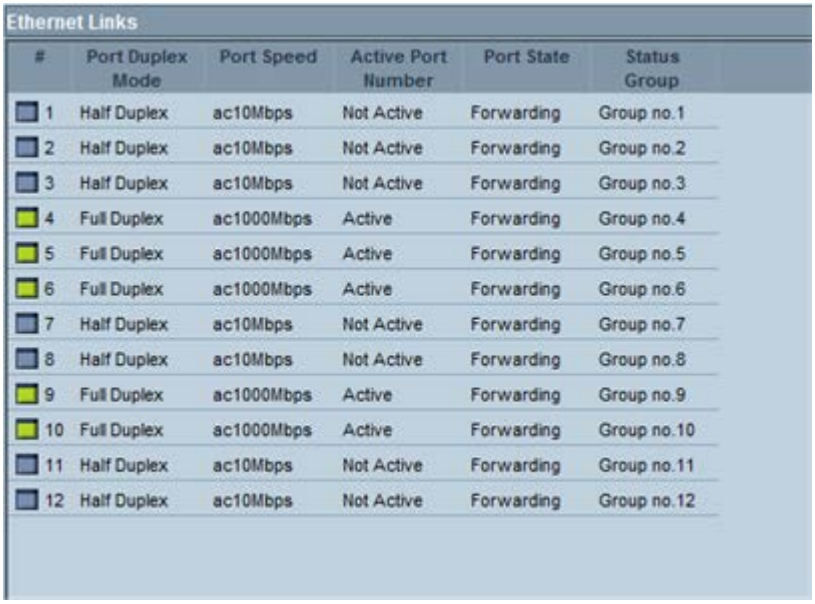


Gigabit Ethernet port status icons:

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

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

Figure 8-2: Ethernet Table-Mediant 9000 SBC



Ethernet Links

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

9.4 Provisioning

For provisioning of the Mediant 9000 SBC, click the 

link in the status screen to open the device's Web server.

Refer to the *Mediant 9000 SBC User's Manual.*

Note: For devices running firmware prior to version 7.0, provisioning is performed using the EMS application. For more information, refer to the *EMS User's Manual* for previous versions.

9.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

This page is intentionally left blank.

10 Mediant Software SBC Products

This section describes the management of the Mediant Software SBC (Mediant SE SBC, Mediant SE-H SBC, Mediant VE SBC and Mediant VE-H SBC) devices.

10.1 Supported Configuration

The EMS supports the following product configurations:

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

10.2 Initial Configuration

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

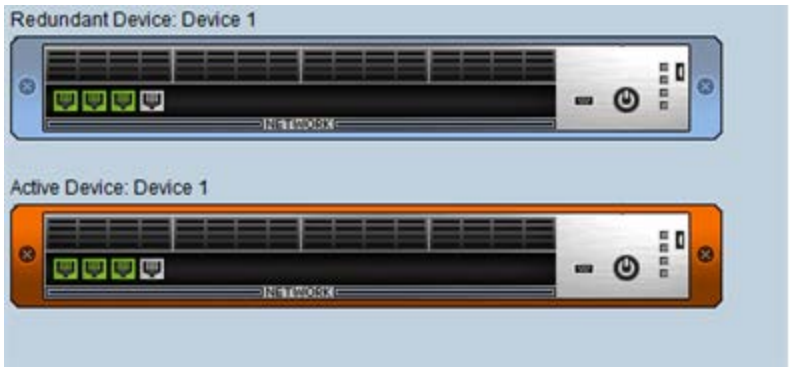
10.3 Status Pane

This Status pane provides the following information:

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

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

Figure 9-1: Software SBC Status Pane

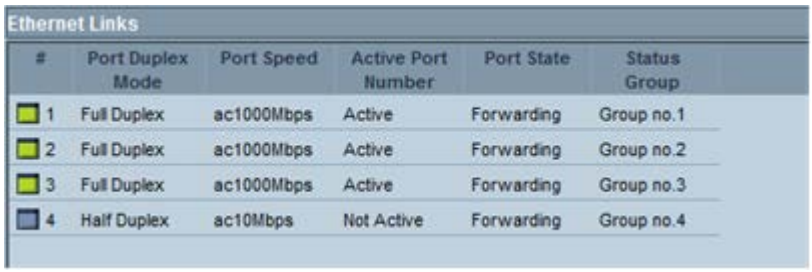


Gigabit Ethernet port status icons:

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

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

Figure 9-2: Ethernet Table-Software SBC



10.4 Provisioning

For provisioning of the Mediant *Software* SBC, click the 

link in the status screen to open the device's Web server.

Refer to the *Mediant Software SBC User's Manual.*

Note: For devices running firmware prior to version 7.0, provisioning is performed using the EMS application. For more information, refer to the *EMS User's Manual* for previous versions.

10.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

11 Mediant 2600 E-SBC and Mediant 4000 SBC

This section describes the management of the Mediant 2600 and Mediant 4000 devices.

11.1 Supported Configuration

The EMS supports the following product configurations:

- Standalone (Simplex) Mediant 4000 SBC
- High Availability-HA (1+ 1) Mediant 4000 SBC
- Standalone (Simplex) Mediant 4000B SBC
- High Availability-HA (1+ 1) Mediant 4000B SBC
- Standalone (Simplex) Mediant 2600 E-SBC
- High Availability-HA (1+ 1) Mediant 2600 E-SBC
- Standalone (Simplex) Mediant 2600B E-SBC
- High Availability-HA (1+ 1) Mediant 2600B E-SBC

11.2 Initial Configuration

Refer to the *Mediant 2600 E-SBC User's Manual* or the *4000 SBC User's Manual* for the initial device configuration.

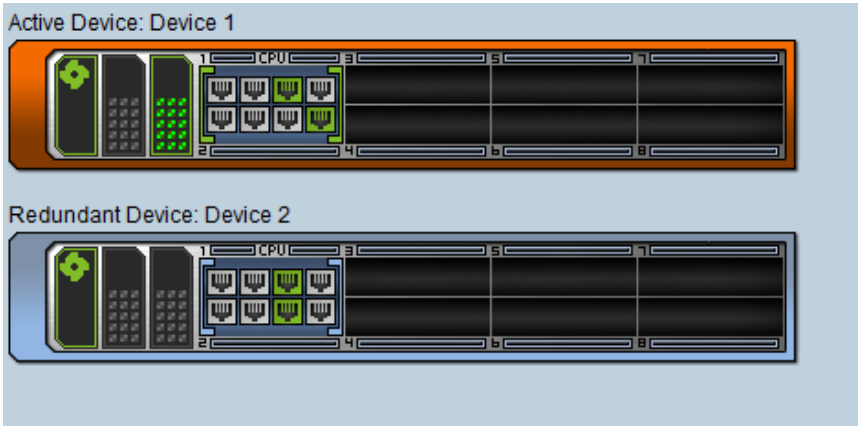
11.3 Status Pane

This Status pane provides the following information:

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

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

Figure 10-1: Mediant 4000 SBC HA Status Pane



- **CPU Module Status**

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

- **Fan Tray status**

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

- **Fan status**

  The status of the 8 fans are read as follows:

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

  Color convention: Red = Failed; Green = OK

- **Power Supplies Status**

  There are 2 Power Supplies: PS Top and PS Bottom

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

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

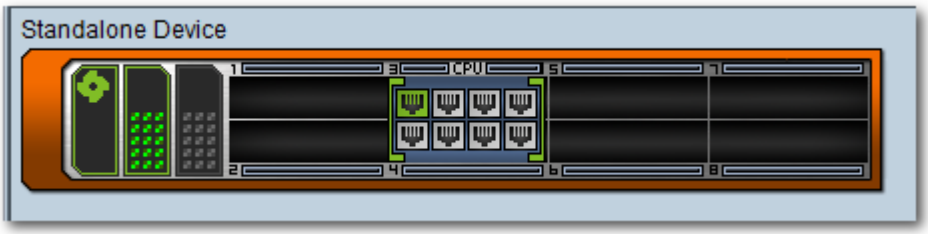
11.3.1 Hardware Component Status in Table View

This section describes the Hardware Component Status in Table View.

➢ **To open the Hardware Component Status in Table View:**

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

Figure 10-2: Mediant 4000 Hardware Components Status Pane



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

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

  The status of the 8 fans are read as follows:

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

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

11.4 Provisioning

For provisioning of the Mediant 2600 E-SBC and Mediant 4000 SBC, click the 

link in the status screen to open the device's Web server.

Refer to the *Mediant 2600 E-SBC User's Manual* or the *Mediant 4000 SBC User's Manual.*

Note: For devices running firmware prior to version 7.0, provisioning is performed using the EMS application. For more information, refer to the *EMS Users Manual* for previous versions.

11.5 Executable Actions

The following maintenance actions are specific the Mediant 2600 and Mediant 4000 devices:

- SwitchOver
- Reset Redundant Device

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

This page is intentionally left blank

12 Mediant 3000

This section describes the management of the Mediant 3000 device.

12.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

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

12.2 Initial Configuration

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

12.3 Status Pane

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

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

The figures below display the Mediant 3000 HA status panes.

Figure 11-1: Mediant 3000 6310 Status Pane

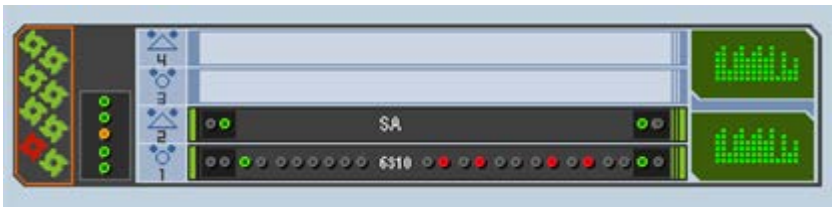
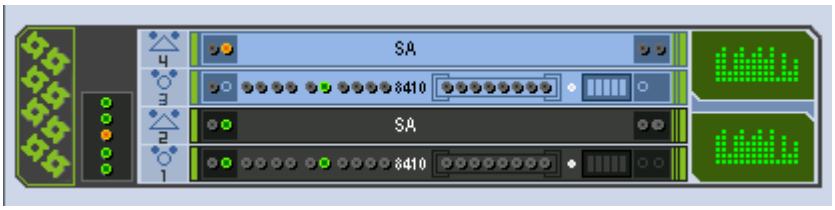


Figure 11-2: Mediant 3000 8410 Status Pane



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

The Information pane indicates the device'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 device, 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 device 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 11-3: 6310 Active Board Status

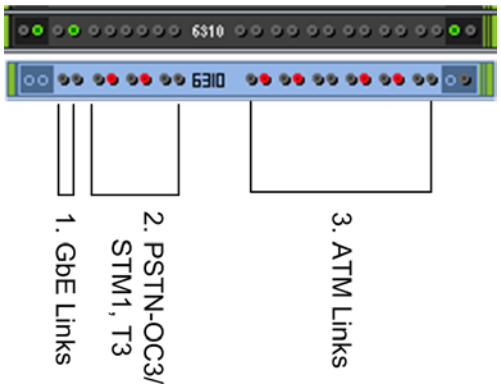
Figure 11-4: 6310 Redundant Board Status

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 11-5: 6310 Board-LED Status



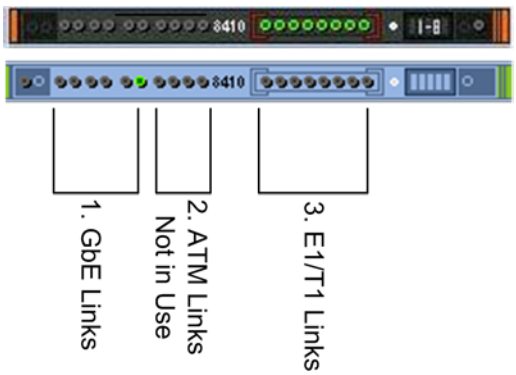
Legend

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 11-6: 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

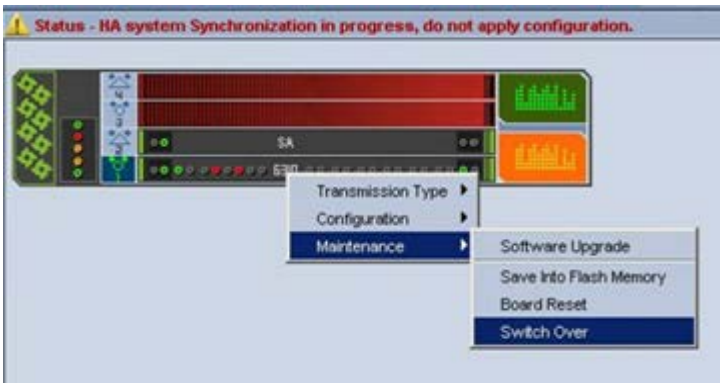
- **Power Supplies Status**

  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 11-7: Status Screen Displaying Failed Redundant Boards and Warning Notification



12.3.2 Hardware Component Status in Table View

This section describes the Hardware Component Status in Table View.

➢ **To open the Hardware Component Status in Table View:**

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

Figure 11-8: Mediant 3000 Hardware Components Status Pane

Mediant 3000 Components Status

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

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

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

  The status of the 8 fans are read as follows:

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

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

12.3.3 Mediant 3000 TP-8410 SA BITS status

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

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

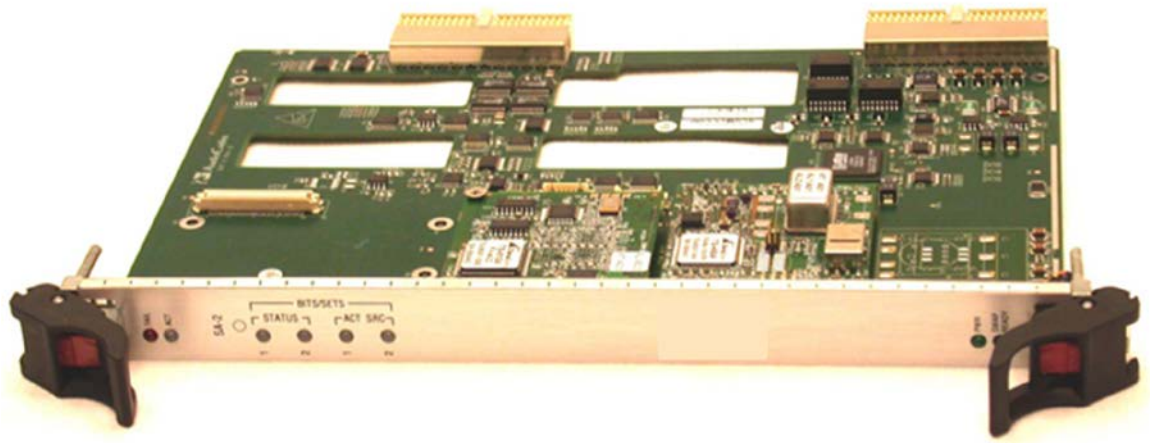
Figure 11-9: Mediant 3000 SA Board Status

The LEDs are represented as follows:

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

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

Figure 11-10: 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 11-11: Mediant 3000 SAT Status

SAT Status

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

12.4 Provisioning

For provisioning of the Mediant 3000, click the 

link in the status screen to open the device's Web server.

Refer to the *Mediant 3000 SIP User's Manual.*

Note: For devices running firmware prior to version 7.0, provisioning is performed using the EMS application. For more information, refer to the *EMS Users Manual* for previous versions.

12.4.1 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*).

12.5 Physical and Logical Components Status

12.5.1 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'.

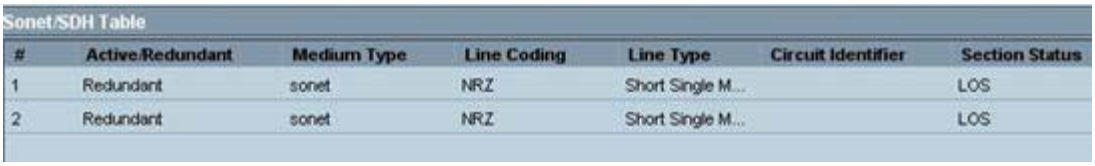
The Sonet OC3 interface on the TP-6310 board supports mapping to three DS3 channels using STS1 (*DS3 Channelization-Asynchronous DS3*).

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 167.

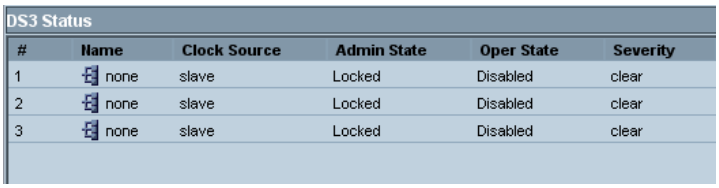
Figure 11-12: SONET / SDH Table



12.5.2 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 11-13: Provisioning a DS3 Interface



12.5.3 DS1 Interfaces

DS1 Trunks and T runks Channels Status screens are described in 'MediaPack' on page 215.

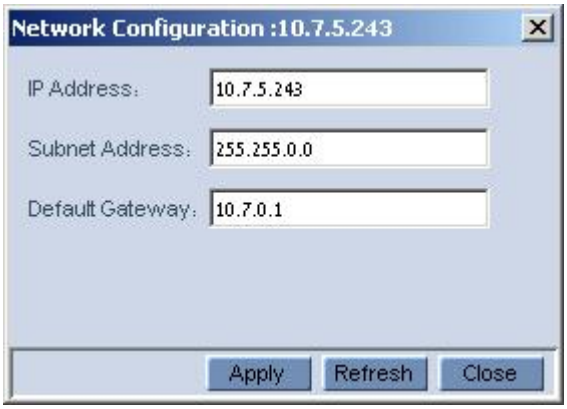
12.6 Executable Actions

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

12.6.1 Configuration Actions

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

Figure 11-14: Mediant 3000 Network Configuration



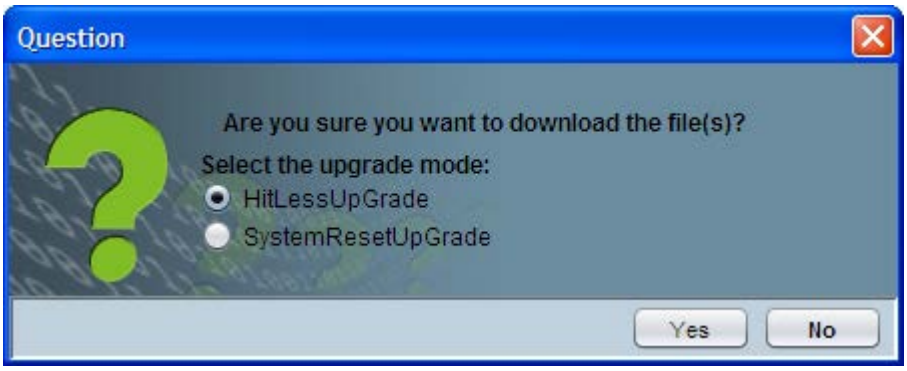
Note: Reconfiguring the network parameters might cause a loss of connection with the device. Make sure that the IP address you reconfigure is distinct from those of other devices in the tree.

12.6.2 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 the appropriate questionnaire.

Figure 11-15: Hitless Upgrade Prompt



12.6.3 Switchover

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

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

12.6.4 Reset Device

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 device 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 devices, refer 'Executable Actions on MediaPacks' on page 218.

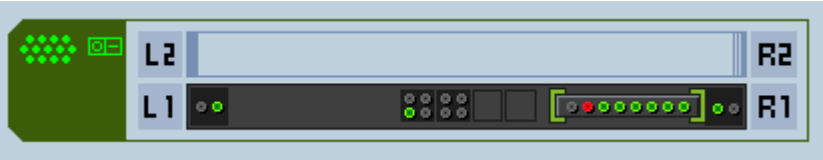
13 Mediant 2000

This section describes the management of the Mediant 2000 device.

13.1 Status Pane

The figure below shows the Mediant 2000 16-trunk Status pane. The Status pane for the 1, 2, 4 and 8-trunk devices are identical; only the number of trunks differs.

Figure 12-1: Mediant 2000 Status Pane



The Mediant 2000 Status pane graphically represents the status of the one or two-module device. 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 12-2: 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 12-3: 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 12-4: 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 device'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 device, a Reset must be performed.
- The DS1 Trunks and Trunks Channels Status screens are described in 'DS1 Interfaces' on page 188.

13.2 Provisioning

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

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

Figure 12-5: Navigation Hierarchy Links- Mediant 2000 (Part 1)

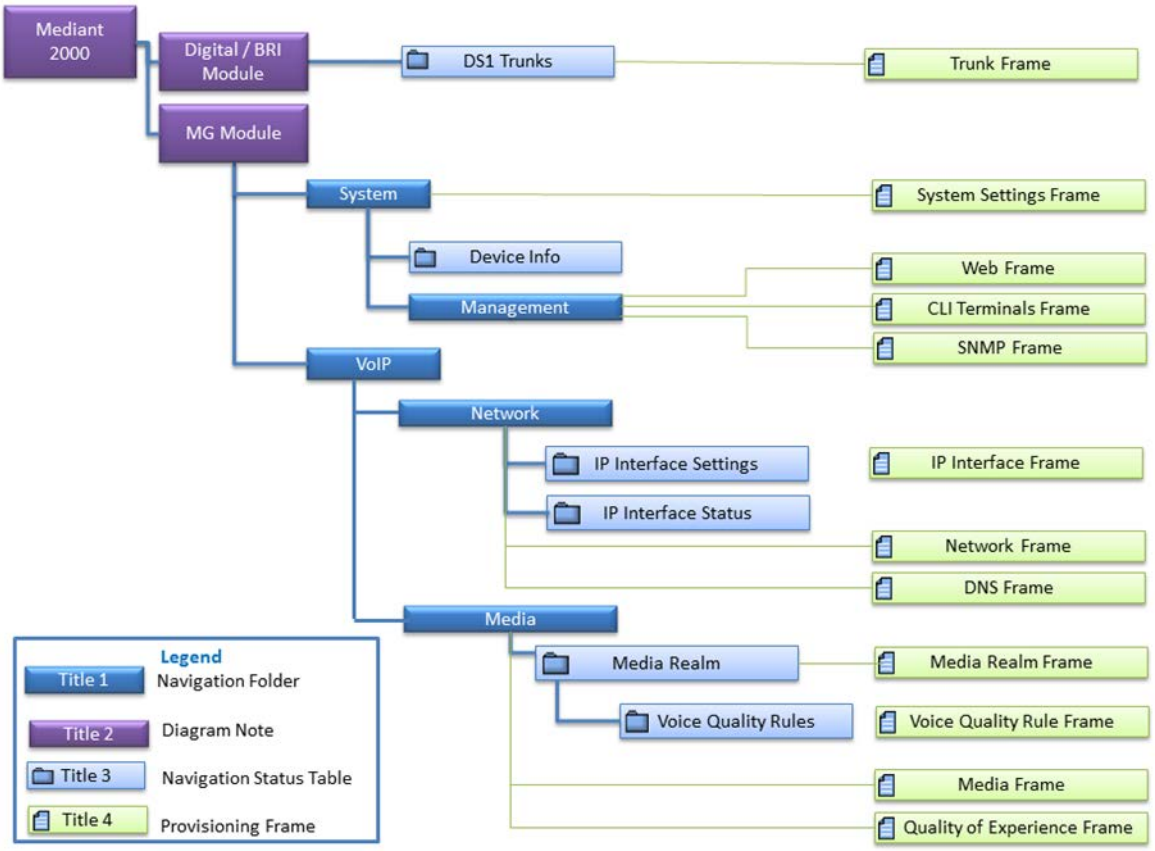


Figure 12-6: Navigation Hierarchy Links - Mediant 2000 (Part 2)

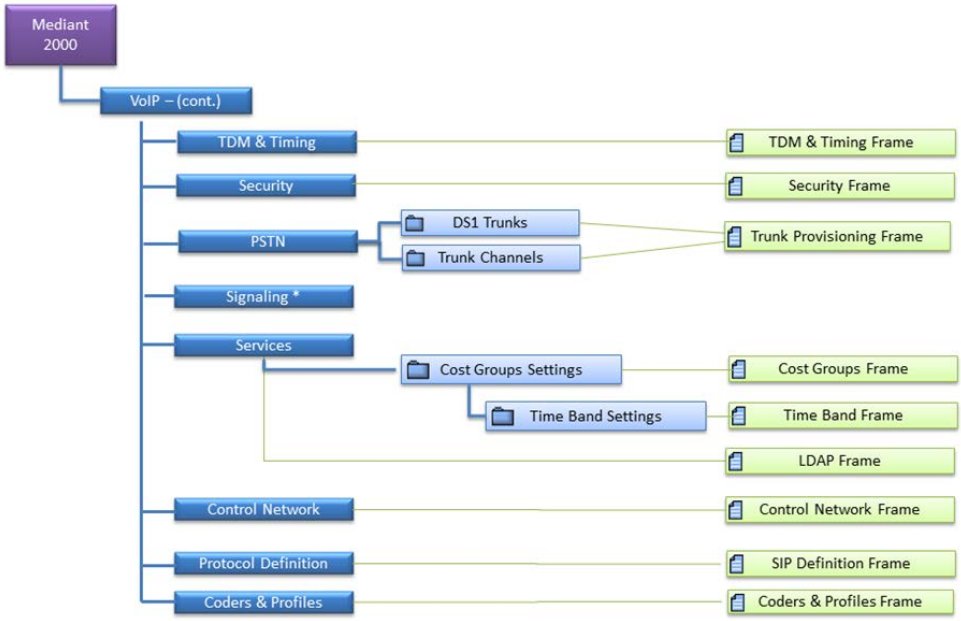
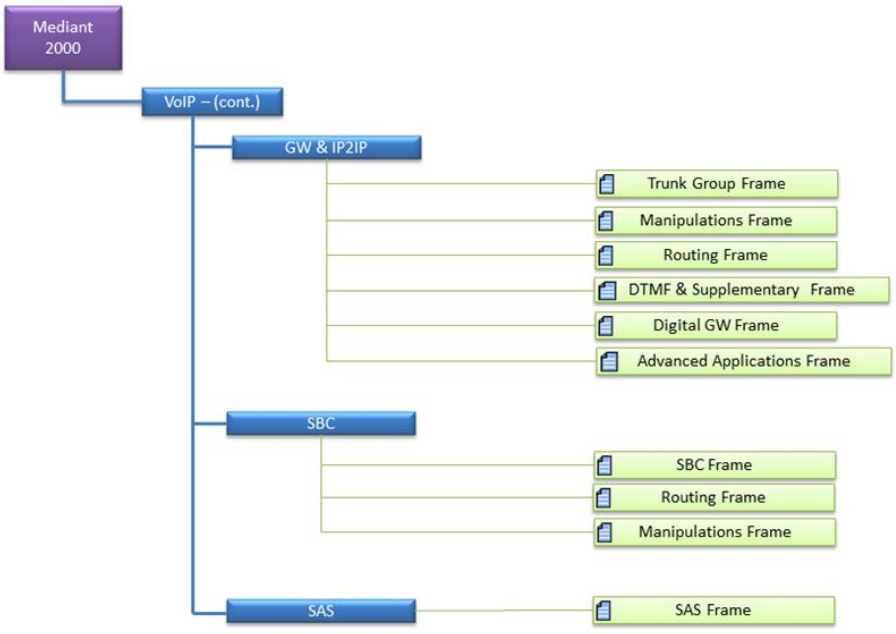


Figure 12-7: Navigation Hierarchy Links - Mediant 2000 (Part 3)



See Section 'Provisioning Concepts' on page 224 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles.

13.3 Executable Actions

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

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

This page is intentionally left blank.

14 Mediant 600 and Mediant 1000

This section describes the management of the the Mediant 1000 and Mediant 600 devices.

14.1 Mediant 1000 Status Pane

The figure below displays the Mediant 1000 status pane.

Figure 13-1: Mediant 1000 Status

Note the following:

- To define new modules, physically insert them and reset the device. 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 188.

14.2 Mediant 600 Status Pane

The Mediant 600 status pane is illustrated below.

Figure 13-2: Mediant 600 Status Pane

14.3 Provisioning

The Mediant 1000/Mediant 600 provisioning parameters are divided into sub-categories (frames). Each category is represented by links and s ub-links that are displayed in the Configuration pane.

The figure below shows the navigation hierarchy links used to provision the Mediant 600and Mediant 1000.

Figure 13-3: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 1)

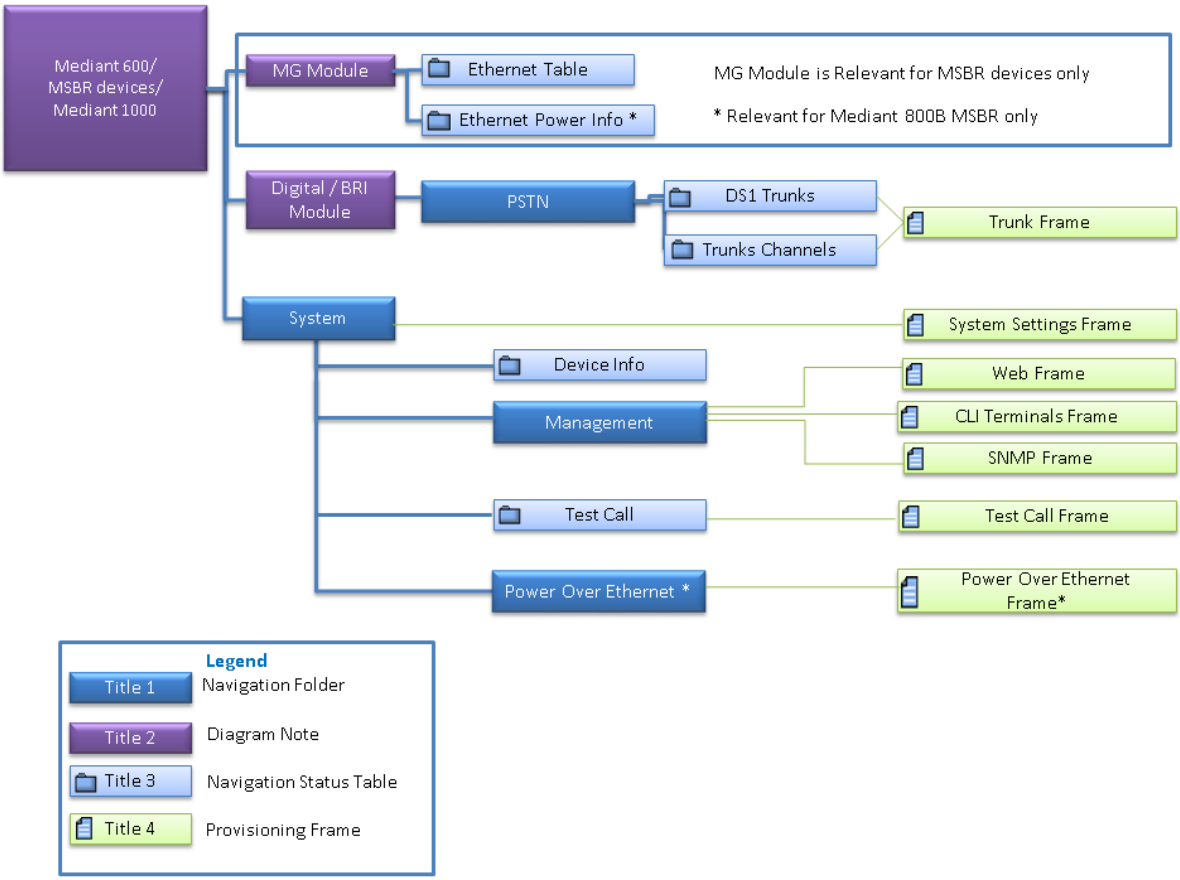


Figure 13-4: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 2)

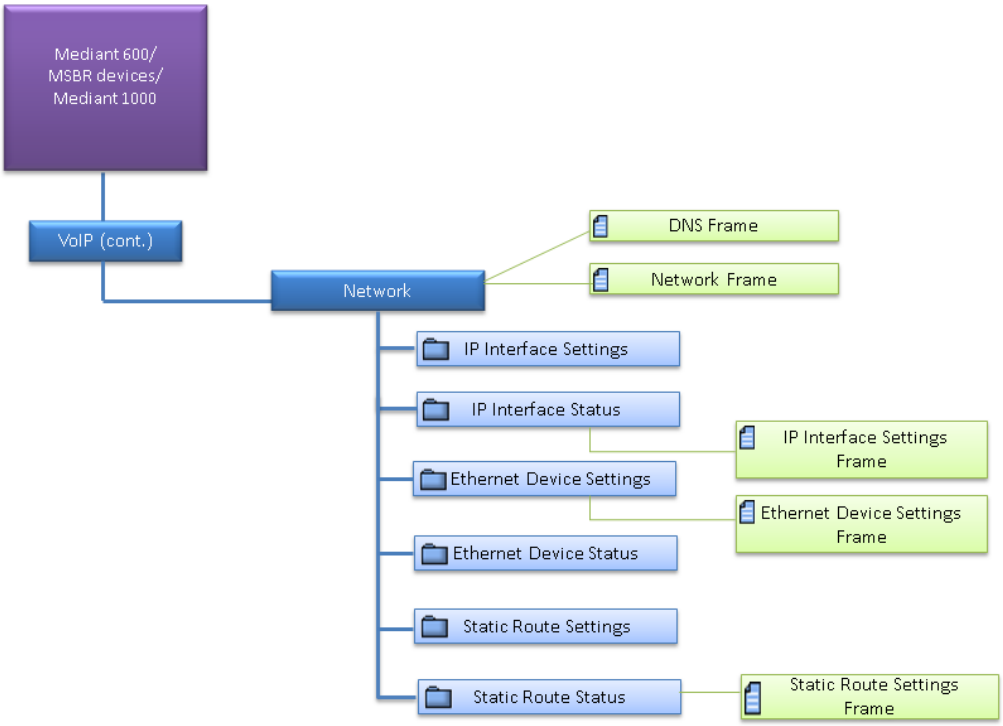


Figure 13-5: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 3)

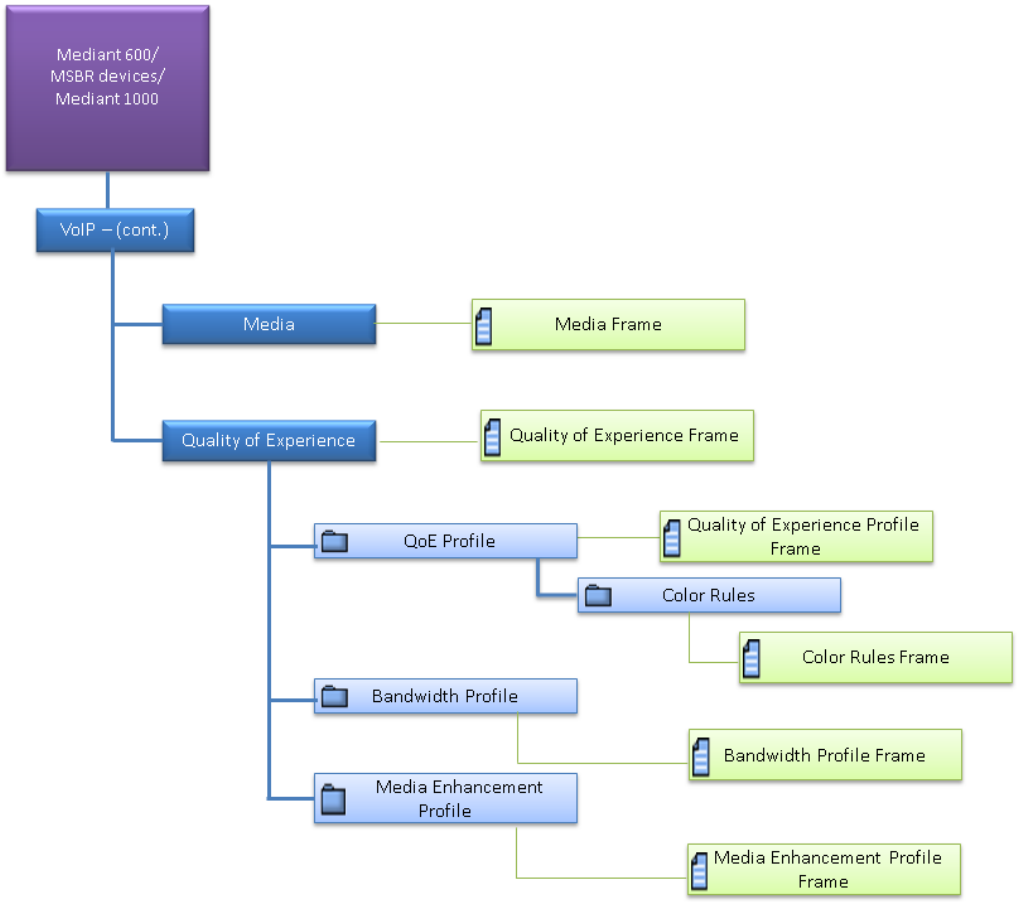


Figure 13-6: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 4)

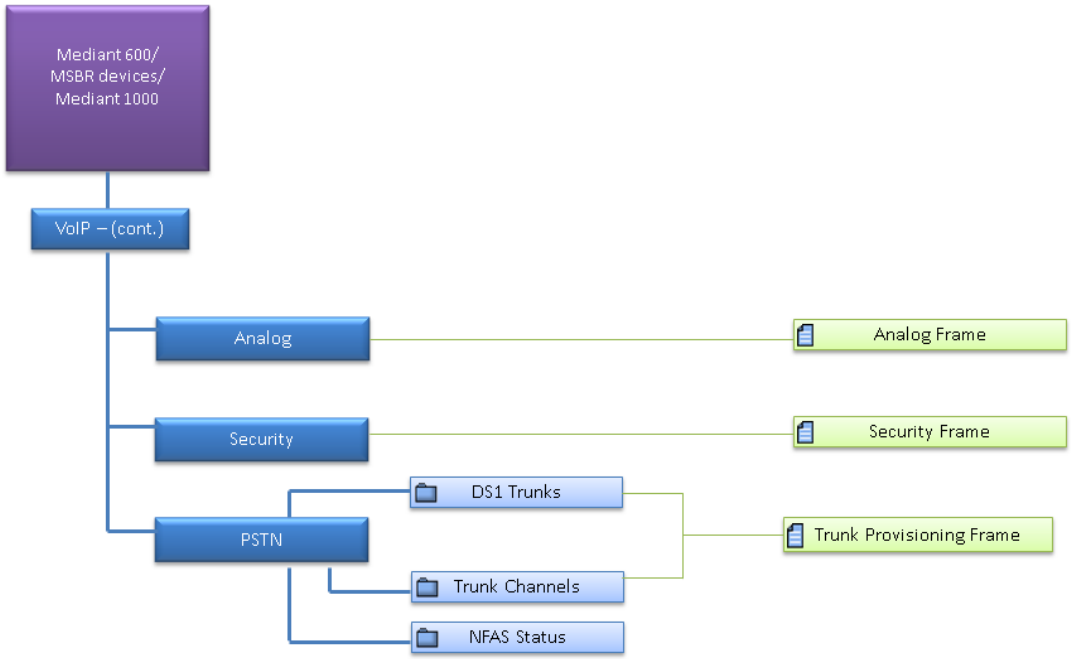


Figure 13-7: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 5)

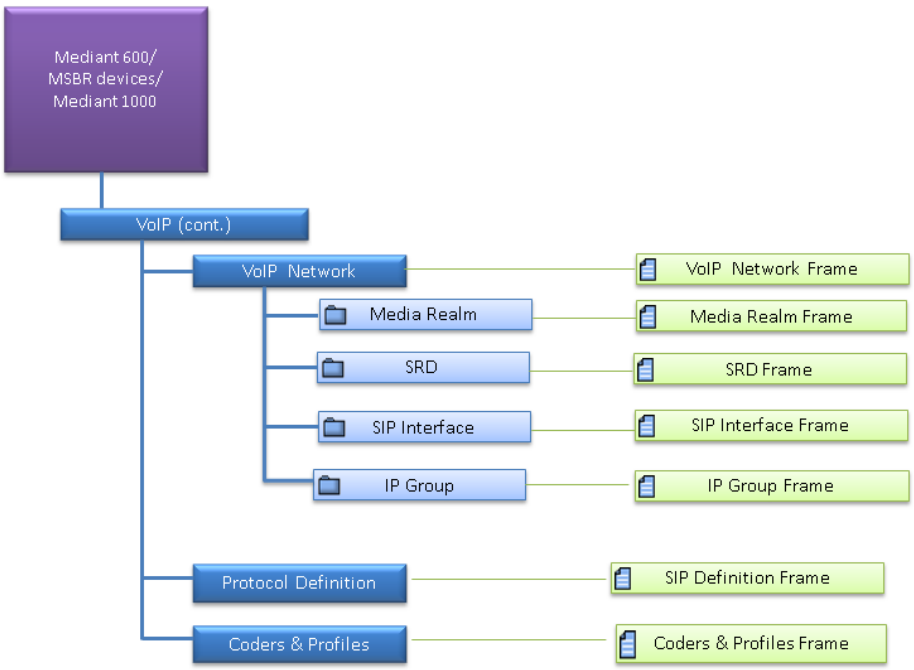


Figure 13-8: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 6)

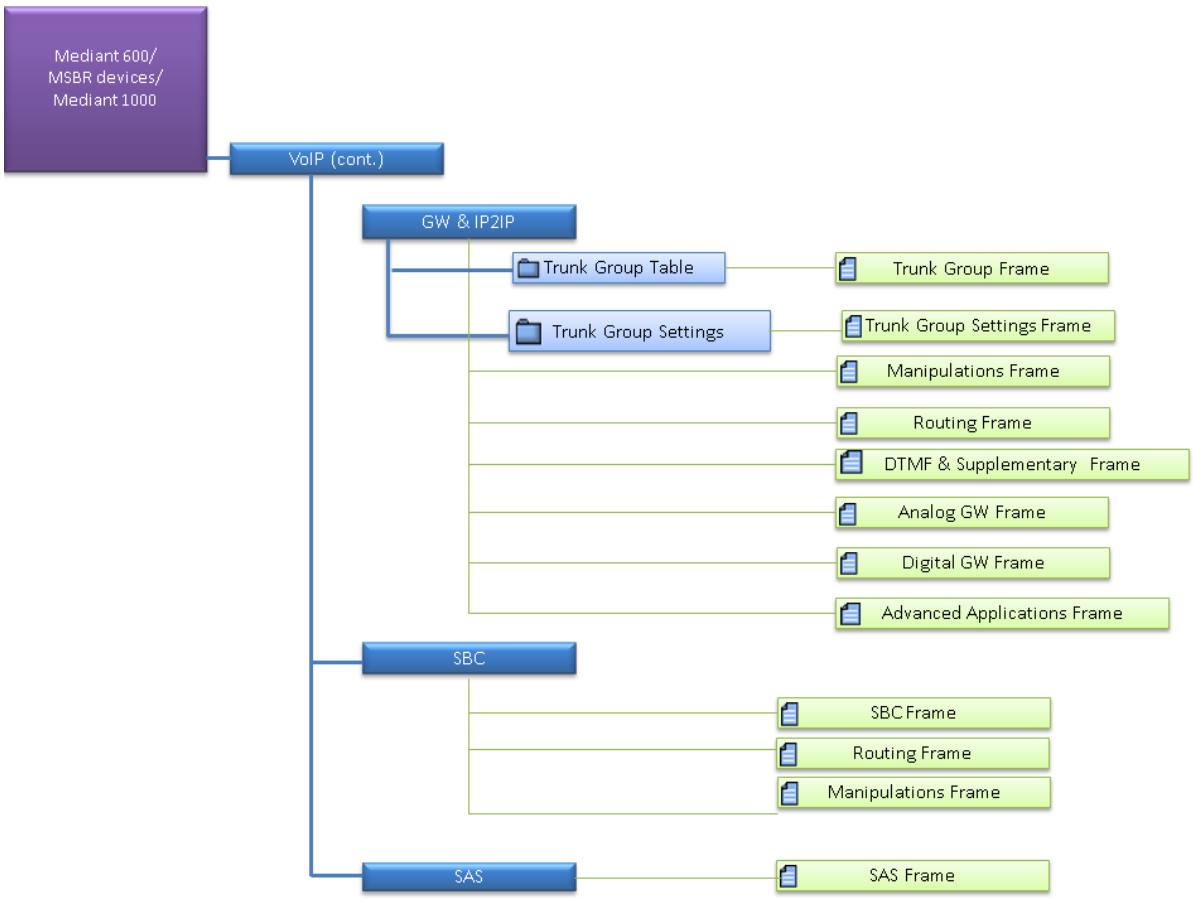
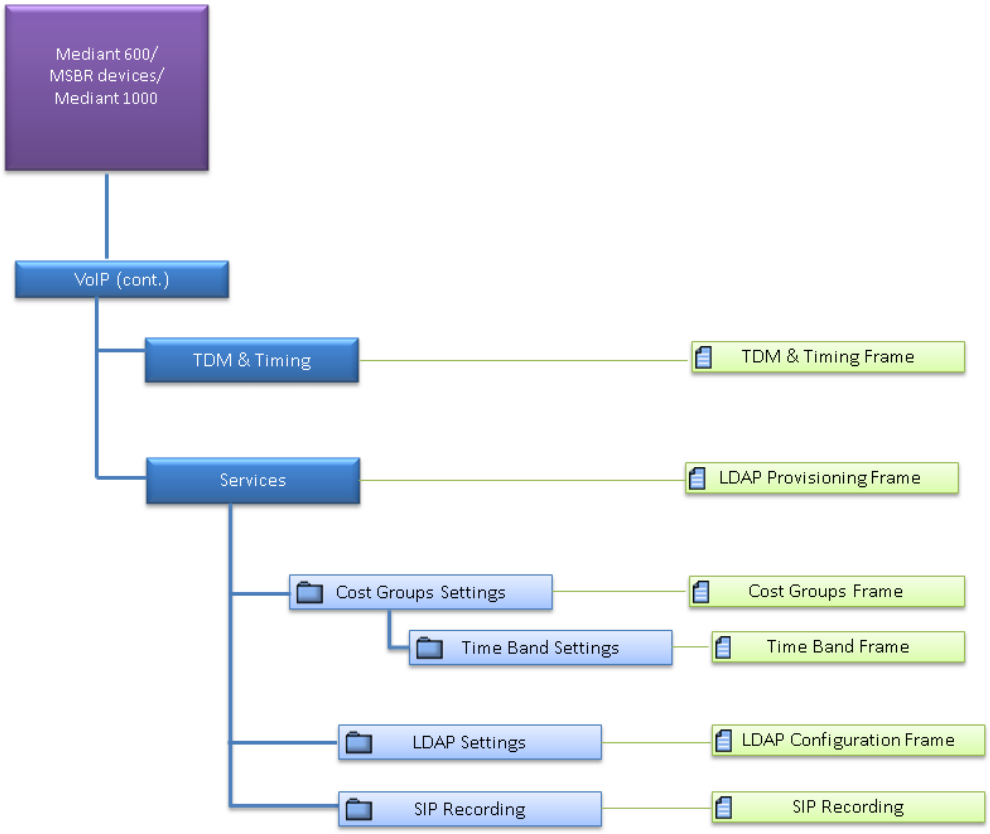


Figure 13-9: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 7)



See Section 'Provisioning Concepts' on page 224 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

14.4 Executable Actions

The following maintenance actions are specific for the Mediant 600 and Mediant 1000 devices:

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 module and reset the device.

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

For the list of common supported maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

15 Mediant Gateway and E-SBC Products

This section describes the management of the Mediant 800B and Mediant 1000B Gateway and E-SBC devices.

15.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

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

15.2 Initial Configuration

Refer to either the Mediant 800B E-SBC or the Mediant 1000B E-SBC User's manual for the initial device configuration.

15.3 Status Pane

This Status pane provides the following information:

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

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

Mediant 1000B Gateway and E-SBC Status Pane

Figure 14-1: Mediant 800B Gateway and E-SBC HA Status Pane

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

Figure 14-2: Mediant 800B E-SBC and Gateway Ethernet Links

Ethernet Links

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

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

Figure 14-3: Mediant 800B E-SBC and Gateway DS1 Trunks List

DS1 Trunks List

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

15.4 Provisioning

For provisioning of E-SBC products, click the 

link in the status screen to open the device's Web server.

Refer to the relevant *SIP User's Manual.*

Note: For devices running firmware prior to version 7.0, provisioning is performed using the EMS application. For more information, refer to the *EMS Users Manual* for previous versions.

15.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

This page is intentionally left blank.

16 Mediant MSBR Products

This section describes the management of the MSBR devices.

16.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Mediant 1000B MSBR, Mediant 800B MSBR, Mediant 500 MSBR and Mediant 500L MSBR with standalone (simplex) configuration.

16.2 Initial Configuration

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

16.3 Status Pane

This pane provides the following information:

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

The figures below display the MSBR status panes.

Figure 15-1: Mediant 500 MSBR Status Pane

Figure 15-2: Mediant 500L MSBR Status Pane

Figure 15-3: Mediant 800B MSBR Status Pane

Figure 15-4: Mediant 1000B MSBR Status Pane

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

- Double-click an FXO link to open the FXO Line Test Table.
- Double-click an FXS link to open the FXS Line Test Table.
- Double-click one of the Ethernet ports (to display the detailed status for each port). The **Ethernet Links** table is displayed:

Figure 15-5: Mediant 1000B MSBR Ethernet Links

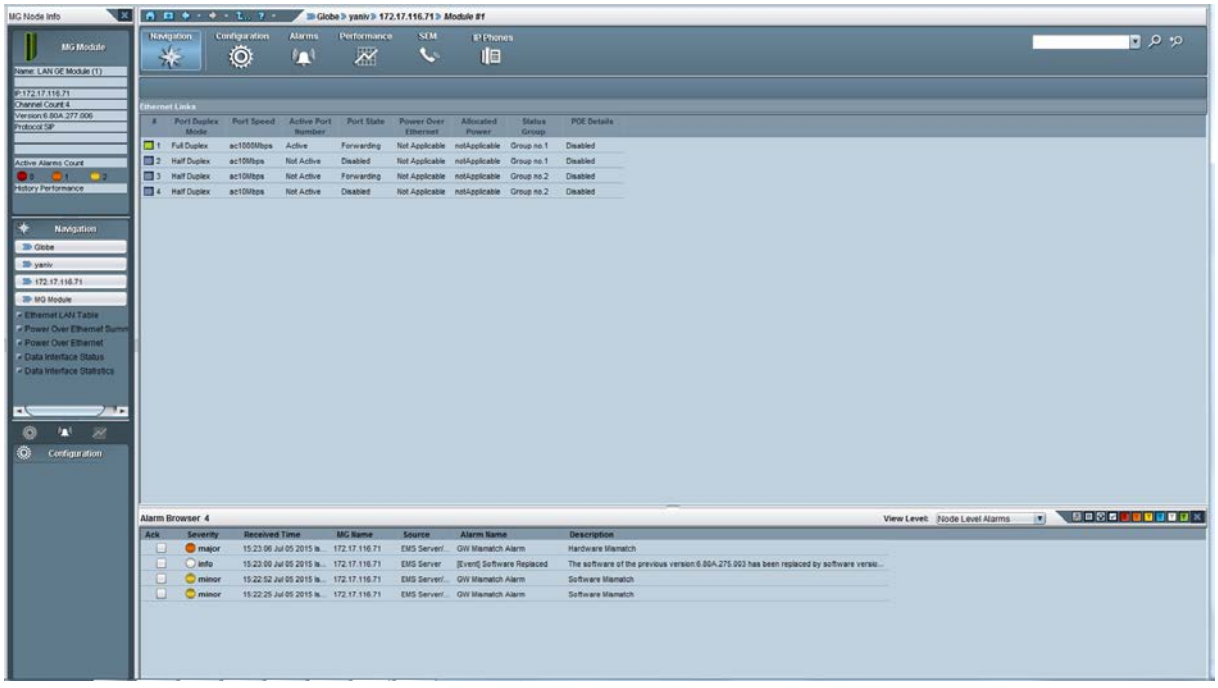
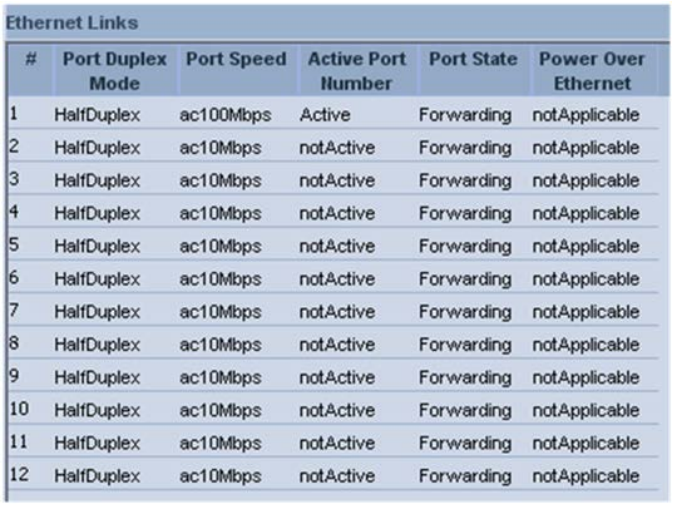


Figure 15-6: Mediant 800 MSBR Ethernet Links



Ethernet Links

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

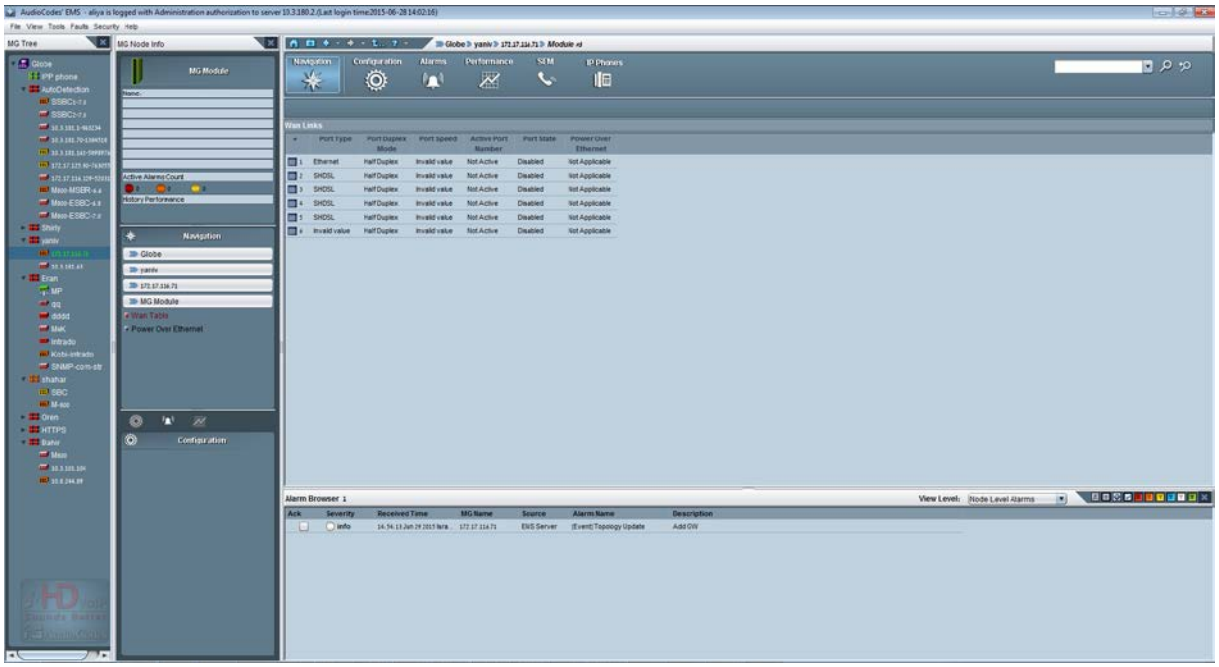
In addition, the following screens provide further information on the Ethernet Links:

- **The Power over Ethernet Summary;** this screen displays power information on the Ethernet connection (Power Budget, Power Remaining, Power Allocated).

- **Data Interface Status:** this screen displays the details for each data interface including the IP address, type of interface, Up Time, DNS Status and Operational state.
- **Data Interface Statistics:** this screen displays detailed packet data for each interface.

- Double-click the WAN link to open the WAN Links table:

Figure 15-7: WAN Links



The configured WAN links are displayed.

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

Figure 15-8: Mediant 800 MSBR DS1 Trunks List

The Information pane indicates the device's name, IP address, software version, trunks count and c ontrol 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 device.

16.4 Provisioning

The devices' 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 MSBR product's navigation hierarchy links are described in Section 14.3 on page 198.

See Section 'Provisioning Concepts' on page 224 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles..

Note: MSBR Data Routing is not provisioned via the EMS application; however, you can upload a CLI script file (containing the data configuration) to the EMS and then download it to the MSBR device (see below).

16.5 Executable Actions

By default when you select the Upload or Download actions for the MSBR device, the CLI script file is loaded to the EMS and the device respectively. This file includes the configuration of the MSBR device using its CLI interface. For both these actions, an additional action is provided to load an ini file.

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

17 MediaPack

This section describes the management of the MediaPack devices.

17.1 Status Pane

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

Figure 16-1: MediaPack Status Pane

The Status pane r epresents 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 16-1: 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 16-1: 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 device's name, IP address, software version, trunks count and c ontrol 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 r eset must be performed to apply these parameters to the device.

17.2 Line Test

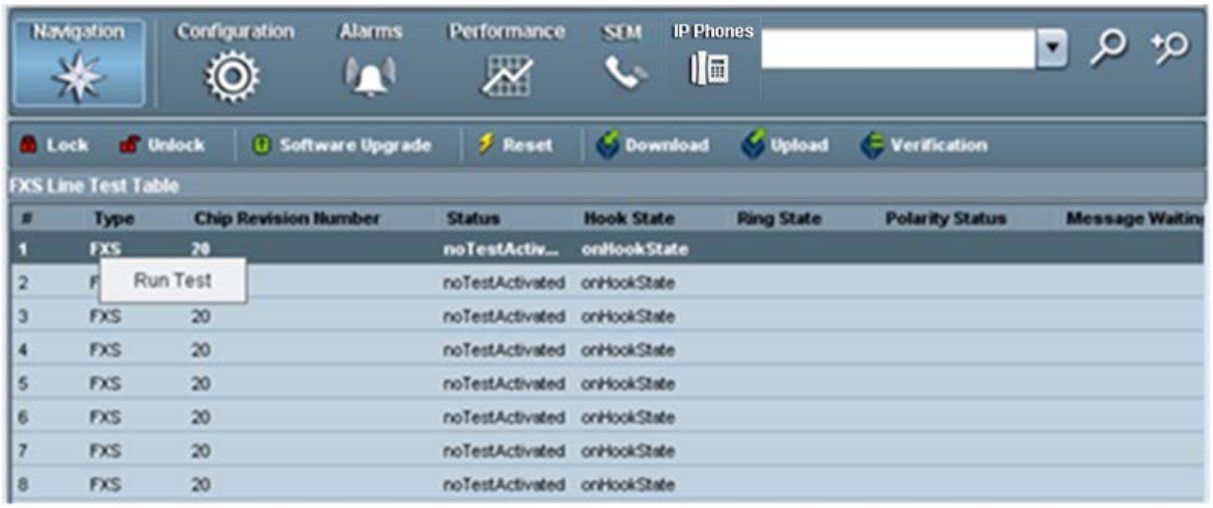
The MediaPack device supports Line Testing.

➢ **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 16-2: MediaPack Line Test



17.3 Provisioning

The devices' 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 16-3: Navigation Hierarchy Links – MediaPack (Part 1)

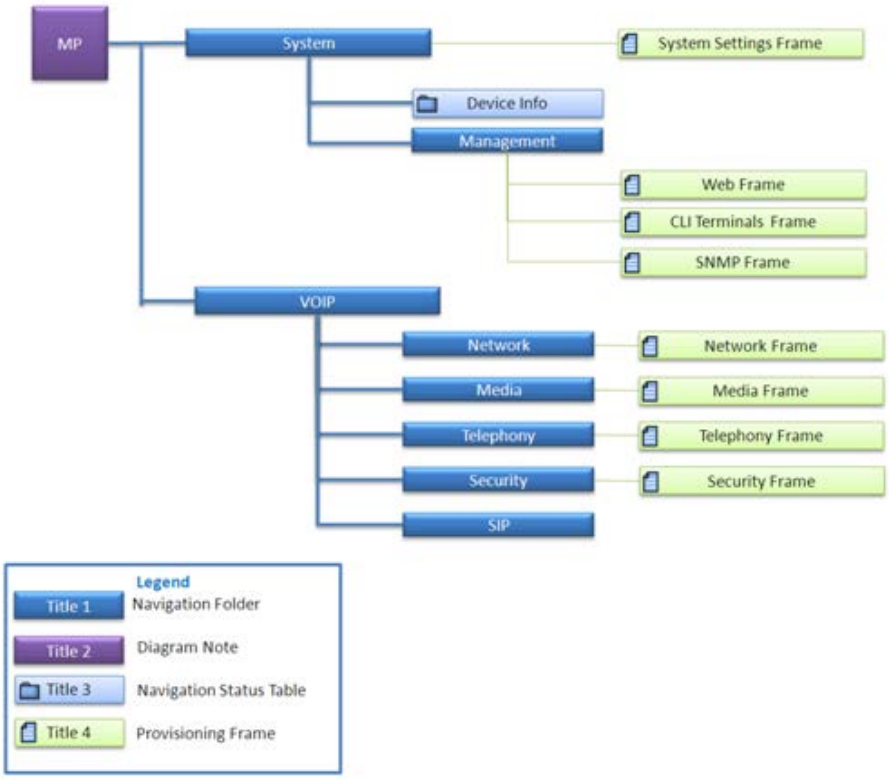
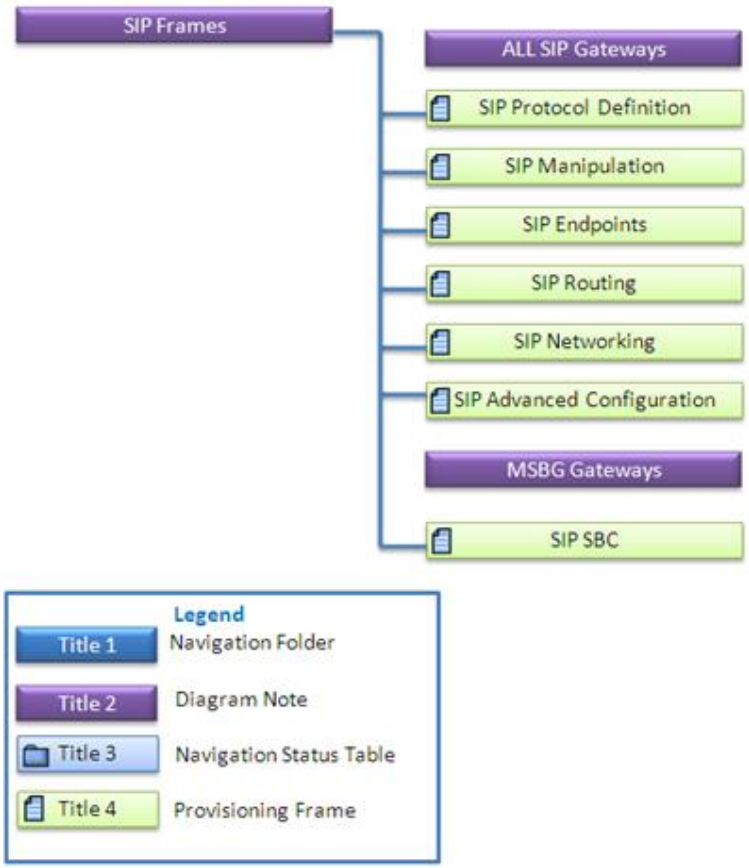


Figure 16-4: Navigation Hierarchy Links – MediaPack (Part 2)



See Section 'Provisioning Concepts' on page 224 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles on provisioning parameters.

17.4 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 227.

18 SBA

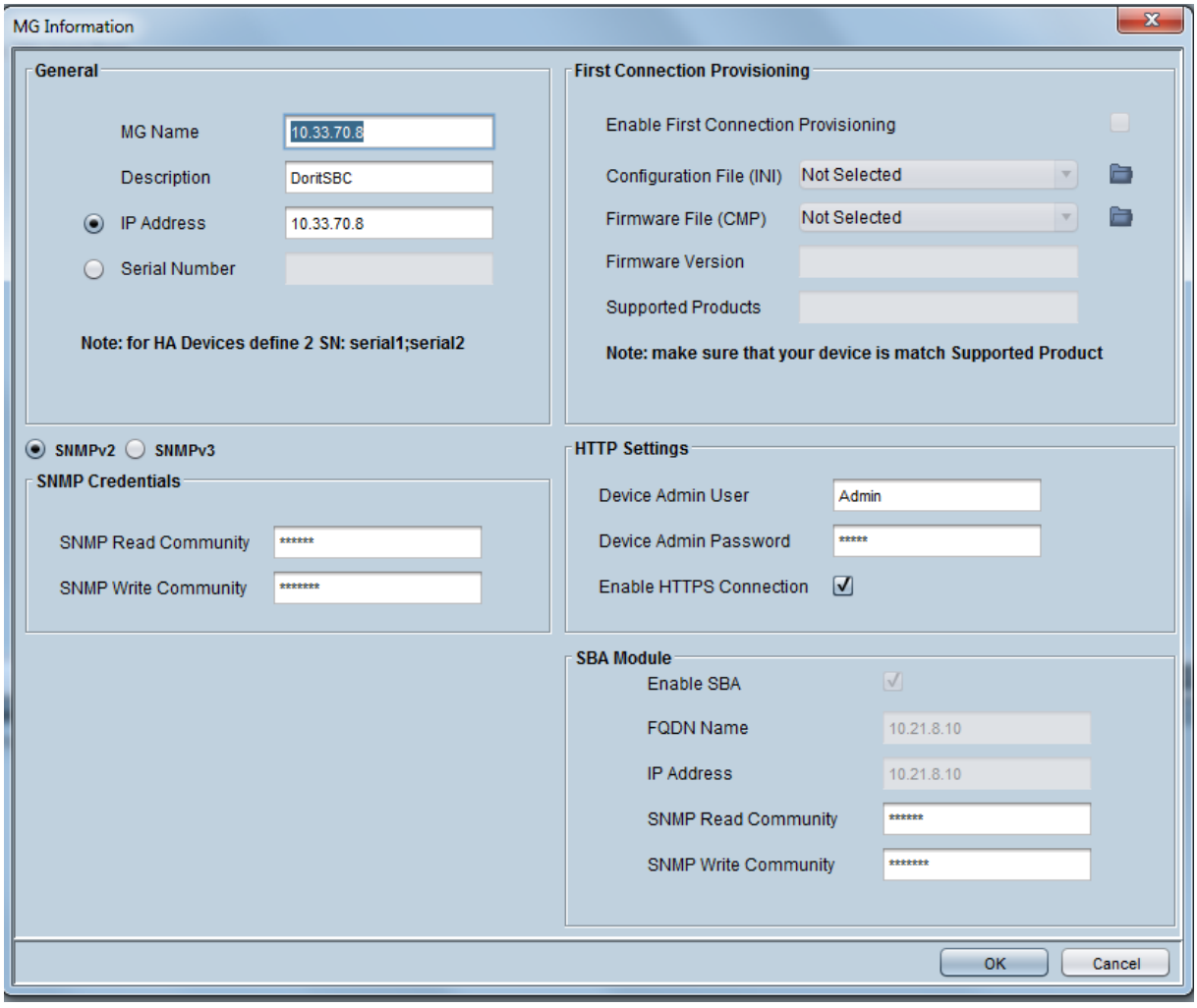
This section describes the management of the Mediant 800B or Mediant 1000B devices with SBA modules installed.

When you add the SBA to the EMS, you need to enable the module and configure the IP address of the SBA Management Interface, which you can then later access when you click the 'SBA Home Page' link on the SBA status screen (see Section 17.2.1 on page 222).

➢ To add the SBA module:

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

Figure 17-1: MG Details-Adding SBA



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

18.1 Reporting Traps from the SBA

You may wish to report SNMP information and traps from the SBA to the EMS. In this case, you must configure SNMP on both the SBA and in the EMS.

➢ **To report traps from the SBA:**

- In the SBA, configure the EMS as an external trap manager and start the SNMP service (for more information, refer to the section 'Step 17 (Optional) SNMP Setup' in the *SBA for Microsoft Lync 2010 and 2013 Installation and Maintenance Guide.*

Notes:

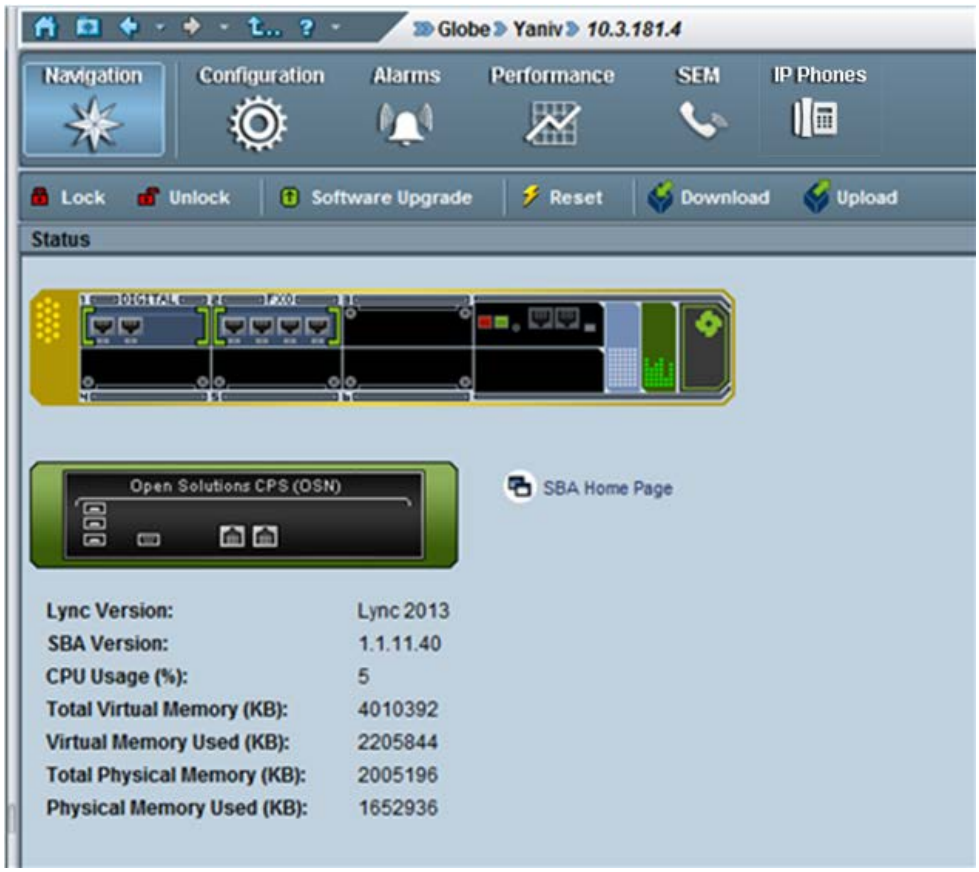
- The same community string values configured in the MG information screen (above in Figure 17-1) must be entered in the SNMP configuration on the SBA device.
- The device must be configured for SNMPv2 only.

When the above is configured, the trap 'acSBAServicesStatusAlarm' is sent to the EMS. This trap indicates the status of the following services: Front End Server, Mediation Server, Replica Server, and Centralized Logging Service for Microsoft Lync 2013 (Centralized Logging is not available for Lync 2010). For more information, refer to the appropriate product's *OAM Guide*.

18.2 SBA Status Pane

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

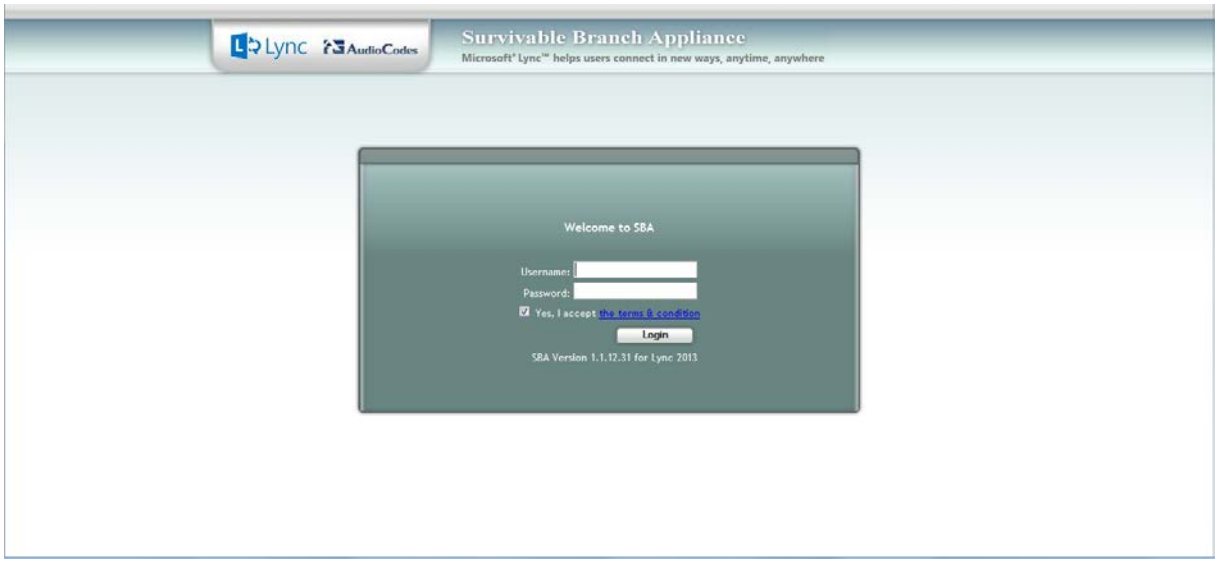
Figure 17-2: SBA Status Screen



18.2.1 SBA Management Interface Link

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

Figure 17-3: SBA Management Interface Login Screen



19 Trunks and Channels Status

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

19.1 DS1 Trunks Status and Provisioning

The Trunk List displays basic information (status and configuration) on the trunks contained in the device. 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 device must be r eset. You're not required to reset the device when making subsequent changes to 'Trunk Protocol Type'. After the device is reset, the trunks are automatically set to the Unlock state.

Table 18-1: 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 18-1: Trunk List for Mediant 2000 Module #1 or 2

DS1 Carriers List

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

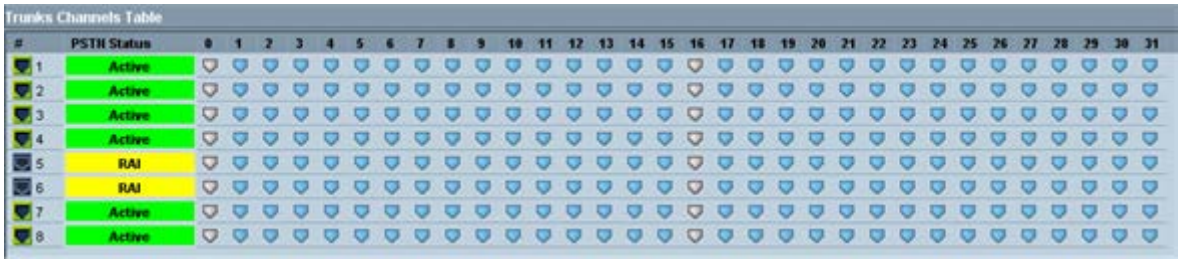
19.2 Trunk Channel Call Status

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

Table 18-2: Trunk Channel Call Status

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

Figure 18-2: 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																																

Part III

Actions and Provisioning

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

.

20 CPE Configuration and Maintenance Actions

This section describes the CPE Configuration and Maintenance actions.

20.1 Configuration Actions

All the actions described in this section are supported by right-clicking the device 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 device type and version.

Figure 19-1: Configuration Actions Menu - HA Device

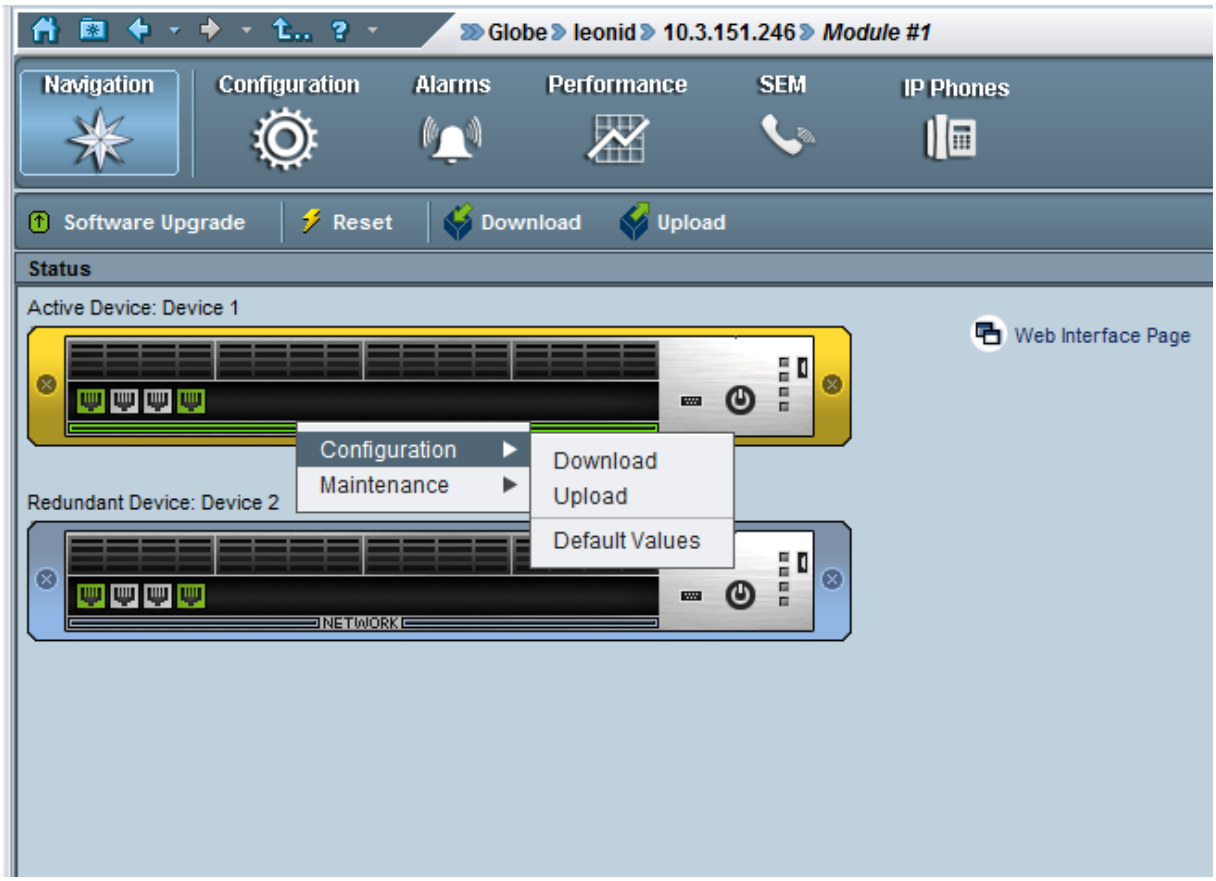
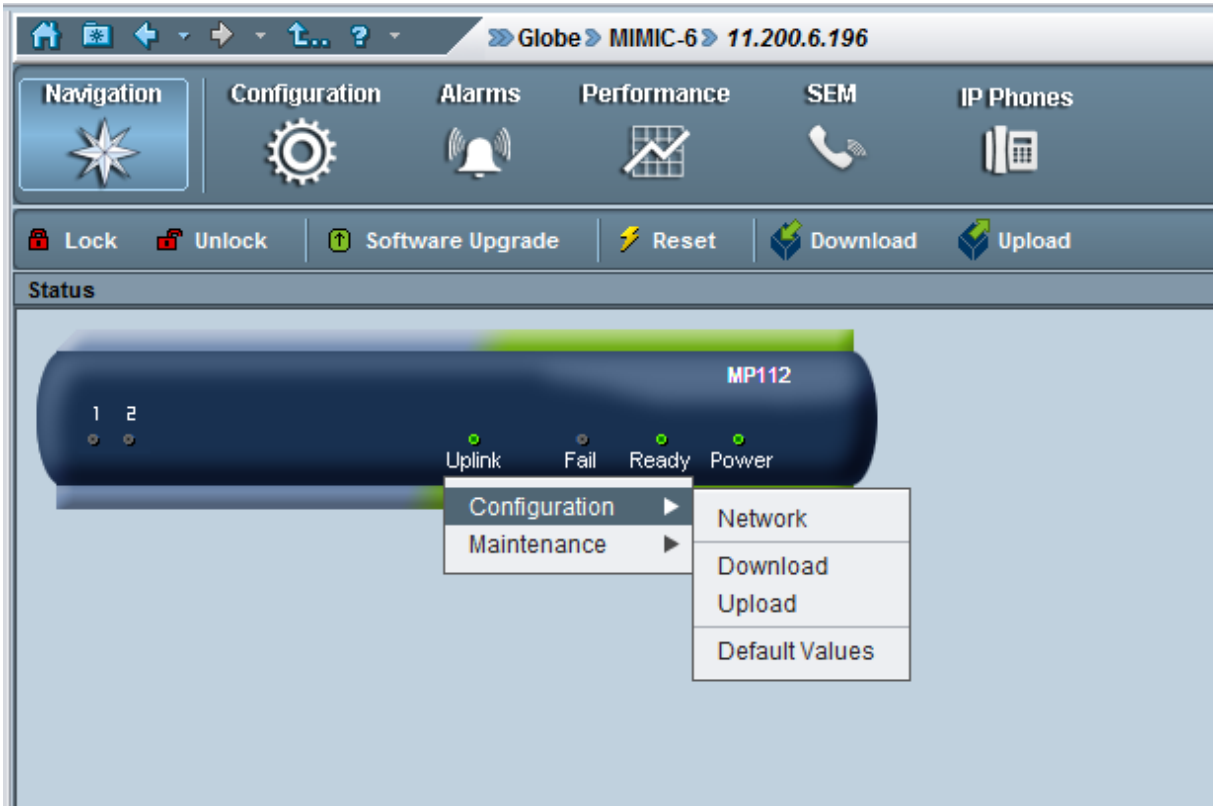


Figure 19-2: Configuration Actions Menu - MP Device



- **Network:** This operation allows modification of the device IP address, Default GW and Subnet Mask.
- **Download:** This operation loads the last saved backup configuration ini file to the device (for MSBR devices, an additional option is provided to download the CLI script file, which contains the entire device configuration including system, data and voice configuration (for more information on device backup files, see Section 21.6.2).
- **Upload:** This operation uploads the last saved backup configuration (ini or CLI script file) to the device (for more information on device backup files, see Section 21.6.2).
- **Default Values:** Removes all user-defined configurations and restores the device to its factory defaults.

20.2 Maintenance Actions

All the below actions are supported via the device 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 device type and version.

Figure 19-3: Maintenance Actions Menu - HA Device

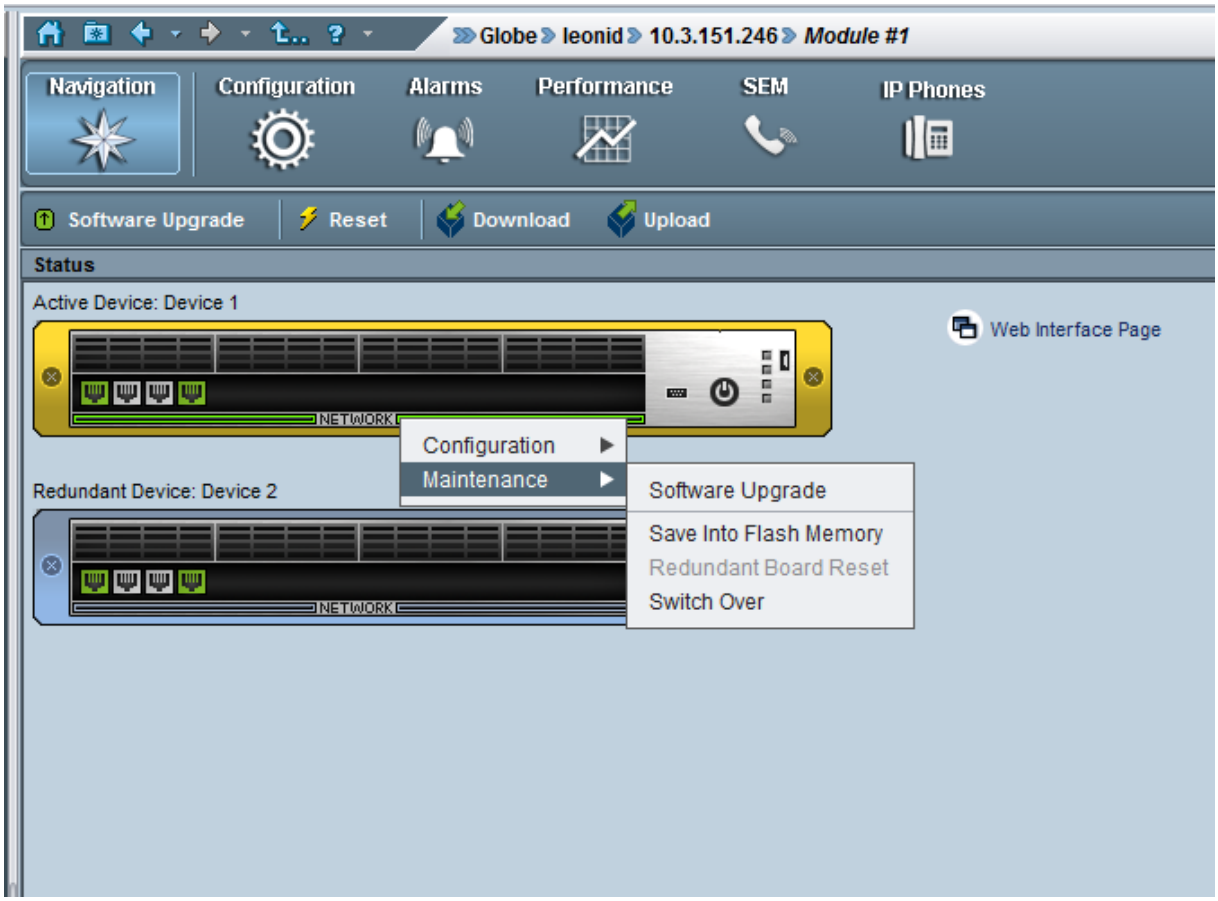
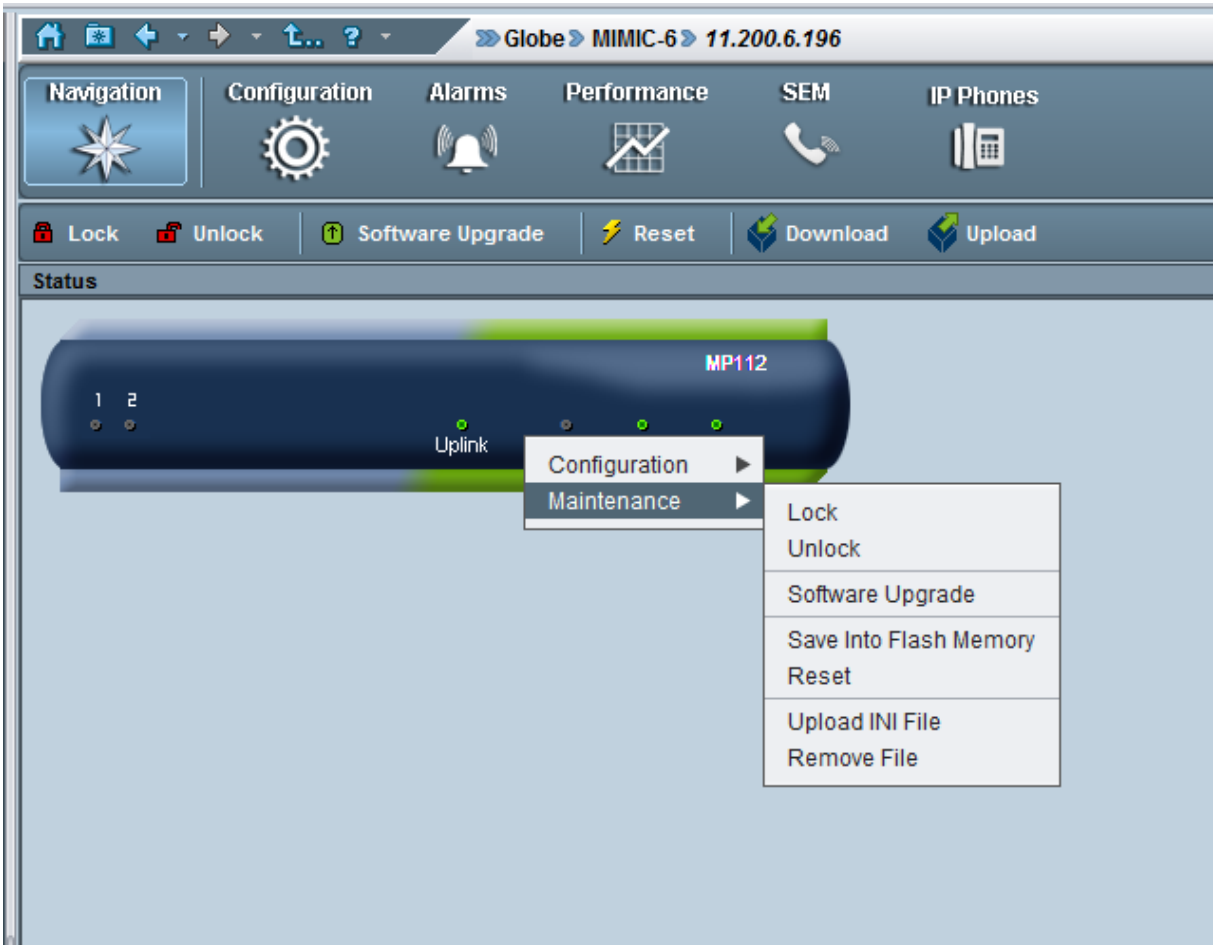


Figure 19-4: Maintenance Actions Menu - MP Device



- **Lock / Unlock:** Locking / Unlocking of the device. Locking the device, stops call control functionality and enters the device 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 device 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 device is reset.
- **Upload INI File:** This option is defined for debug purposes. The ini file received from device is used to assist AudioCodes FAE to perform problem debugging.
- **Remove File:** removed auxiliary file/s from the device. When this option is selected, the user is prompted with a list of all the files used by a specific device. The user can then select the files they wish to remove.
- **Redundant Board Reset:** Resets the redundant board.
- **Switch Over:** Switches over to the redundant board.

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 device 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 device 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 device board to the receiving end of the trunk and an RAI alarm signal is returned to the device (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).

For Performance Monitoring actions, see Section 32.4.

20.3 Performing Actions on Multiple Devices

This section describes how to perform actions on multiple devices.

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

1. In the MGs Tree Status screen, select the Region under which the devices are located.
2. Select one or more devices using the CTRL or Shift keys, or by using the mouse. Verify that all devices 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 device types and software versions, some actions in the right-click pop-up menu may be disabled. This implies that in the selected set of devices, there are one or more devices which cannot support the action that is disabled in the pop-up.

21 Provisioning Concepts

This section describes the EMS provisioning concepts.

Note: This section is relevant for the Mediant 5000 and Mediant 8000 and for CPE devices running firmware prior to version 7.0.

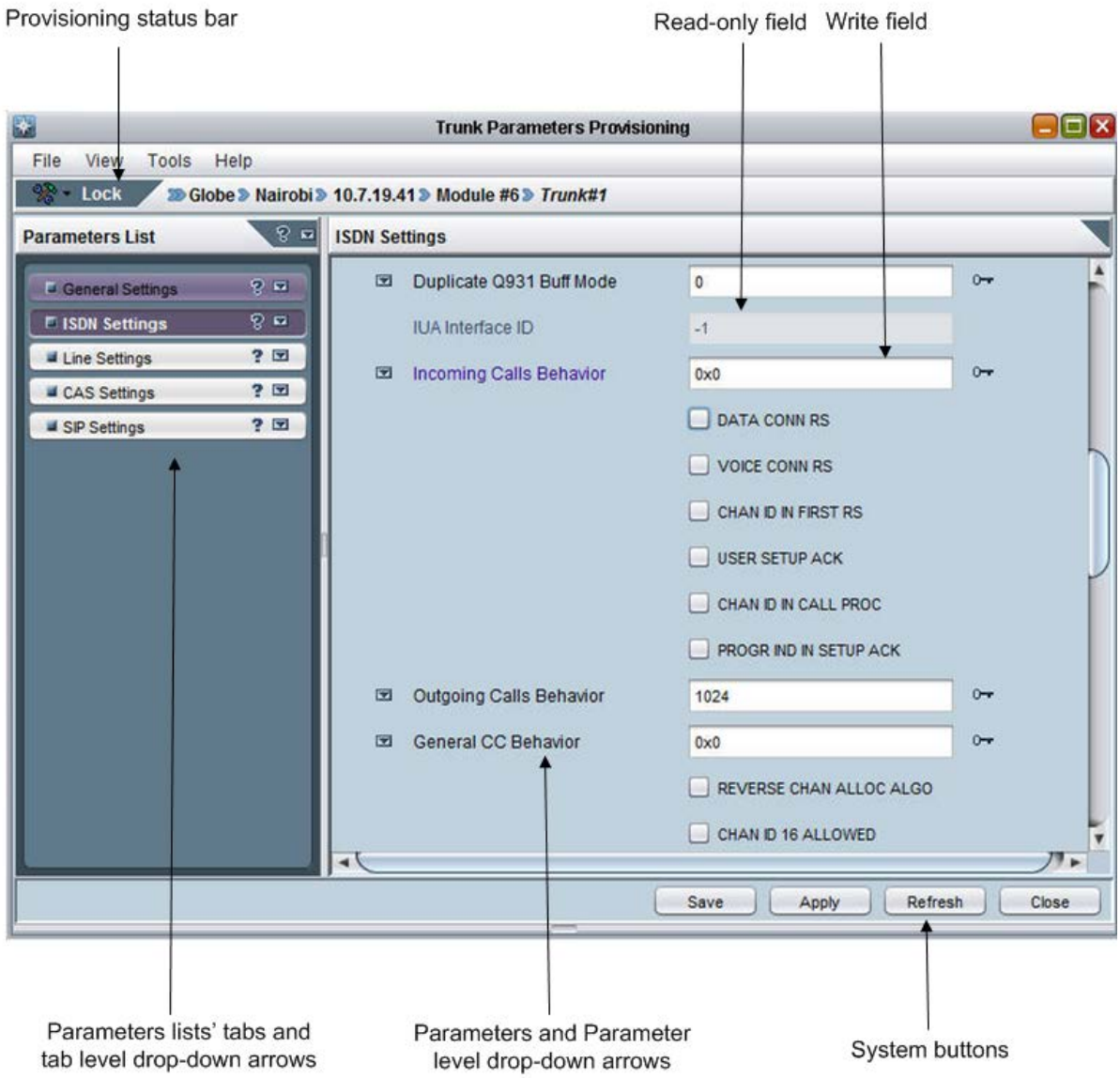
21.1 Working with the EMS's Provisioning Screens

All screens in the EMS that enable operators to provision the devices, 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 20-1: TP-6310 Board Provisioning Parameters



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

- **Provisioning Status Bar**

  This bar includes the path of the EMS-managed entity, as well as it's Administrative State (Locked/Unlocked) and it's 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 20-1: 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 device.
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 device is initiated with prior to its release.

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

- **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 20-2: 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 device, and in addition for the CPE products, saves your changes to the EMS Database.

Refresh - Read the current device setting (replace your changes with the current data). For low density devices, 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:

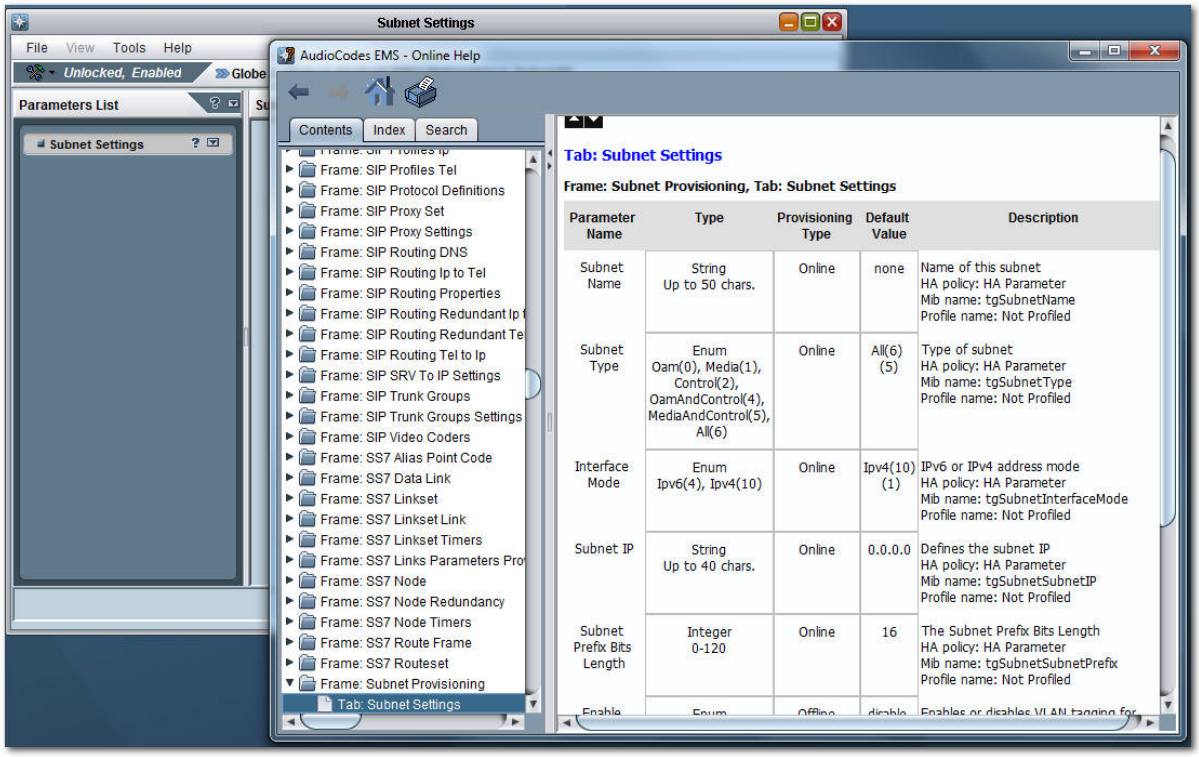
  - Right-clicking on a table row and choosing an Add / Remove / Lock / Unlock action does not then require clicking the **Apply** button; the action is executed immediately. Pressing CTRL-A enables you to select all rows in the configuration table at the same time.
  - When you finish editing a cell in 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 20-3: Online Help



21.1.1 Provisioning Procedure for Mediant 5000 and Mediant 8000

This section covers the Mediant 5000 and Mediant 8000 devices.

➢ To provision a Mediant 5000 and Mediant 8000:

1. Navigate to the element/entity you wish to provision, select it (for a device, select it in the MGs List under the region; for a board, select it in the graphic representation of the device; 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 device.
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.

21.1.2 Provisioning Procedure for CPE Products

This section describes the provisioning procedure for CPE products.

➢ **To provision these VoIP devices:**

1. Navigate to the element/entity you wish to provision, select it (for a device, select it in the MGs List under the region; for a board, select it in the graphic representation of the device; 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 device 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.

21.2 Parameters Provisioning Types

The EMS features the following provisioning parameter types:

- Instant (changes are applied to the device 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 device) 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 20-2: Indication Mapping Summary

Parameter Provisioning Type	Indication / Device Type	Description
Instant	No indication	Click Apply, OK button to load changes to the device.
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/device* containing the entity. The mode is called 'Online' because the parameter can be configured without resetting any board in the device.
- **Offline -** To configure an 'Offline' mode parameter (indicated in the EMS by the icon adjacent to the parameter), you need to lock the board/device 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/device containing the entity's parameter are dropped when you lock the board/device 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/device is required to perform the configuration.

21.3 Parameters HA Type

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

The EMS features three provisioning parameter types:

- Instant (changes are applied to the device 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 device) 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):

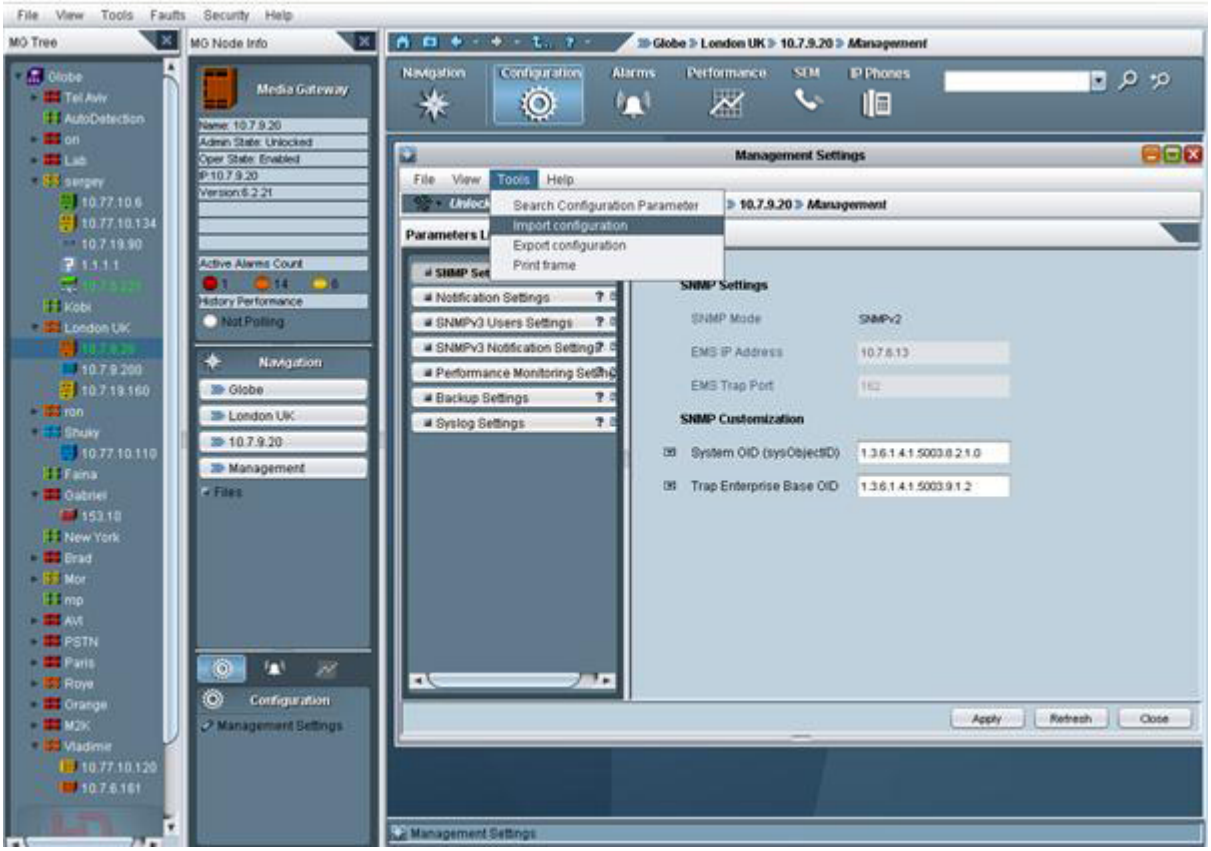
Table 20-3: Indication Mapping Summary-Parameters HA Type

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

21.4 Exporting, Importing an Entity Configuration as a File

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

Figure 20-4: 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.

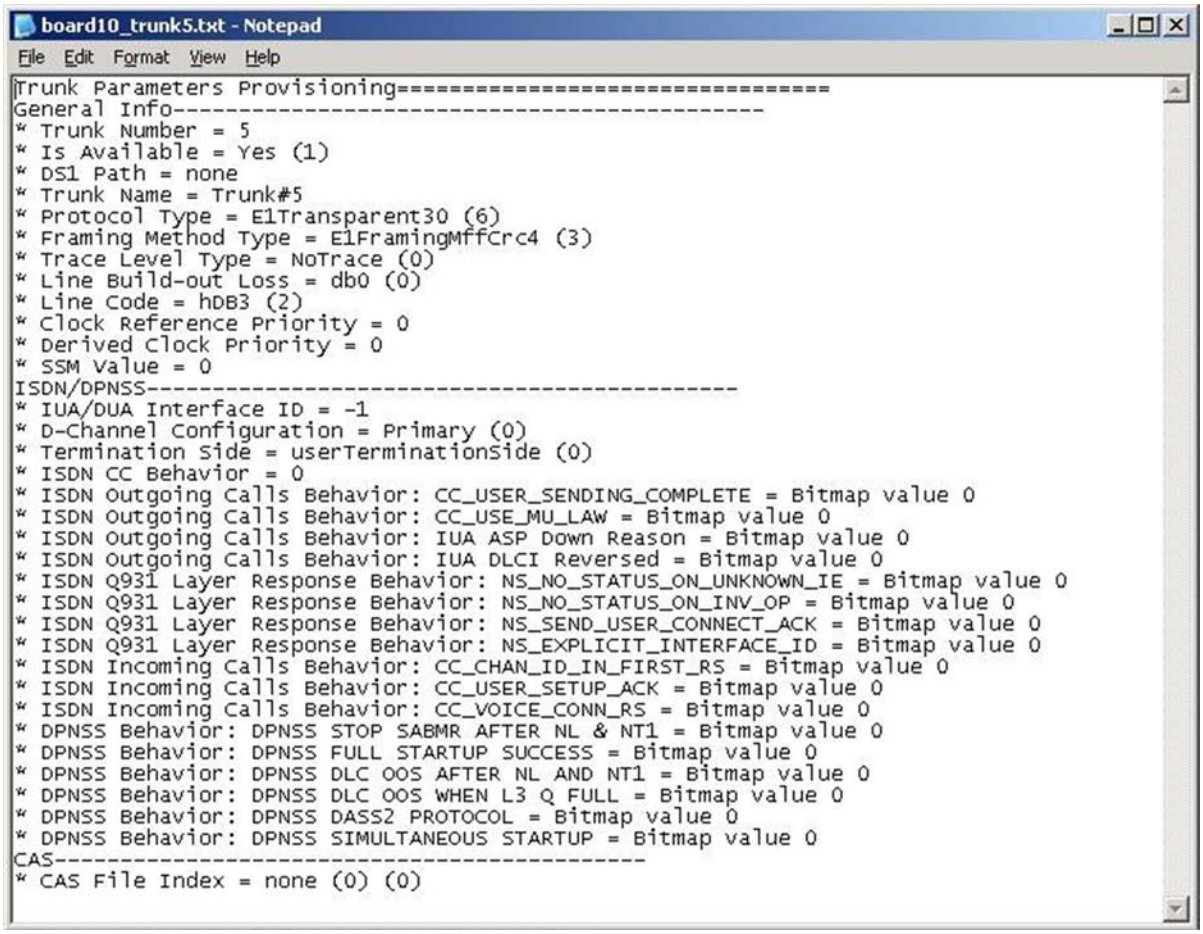
21.5 Printing an Entity's Configuration as a File

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 20-5: Trunk Print Format

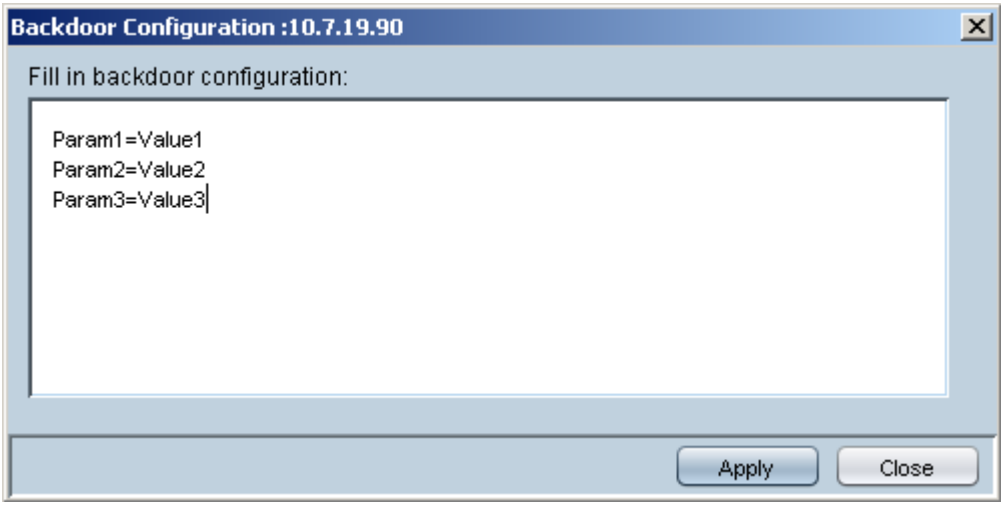


21.6 Backdoor Configuration for CPE Products

In very rare circumstances, the EMS application may not include specific provisioning parameters or tables which are supported via the device 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 device. 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 20-6: Backdoor Configuration



Notes: Backdoor parameters are downloaded directly to the device 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.

21.7 Searching for a Provisioned Parameter

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

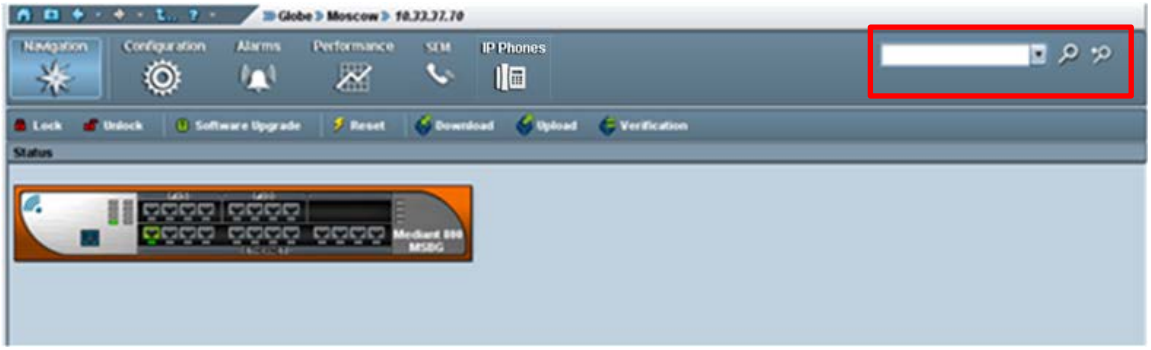
The search option is context sensitive according to the selected device. The search options are always visible in the right-hand corner of the EMS toolbar. In addition, the Advanced Search Configuration dialog can be opened from the EMS Tools menu.

Note: The search option is only available for the Mediant 8000 and Mediant 5000 and CPE devices running firmware prior to version 7.0.

➢ To perform a Basic Search:

1. Type the required string or its substring, or alternatively select one of the previously searched strings and then click the 'Search' button; the Search Result screen opens, displaying a list of parameters addressing the defined search criteria.

Figure 20-7: 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 required) by selecting 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' checkbox 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 defined search criteria.

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 20-8: Advanced Search Configuration Parameter Dialog

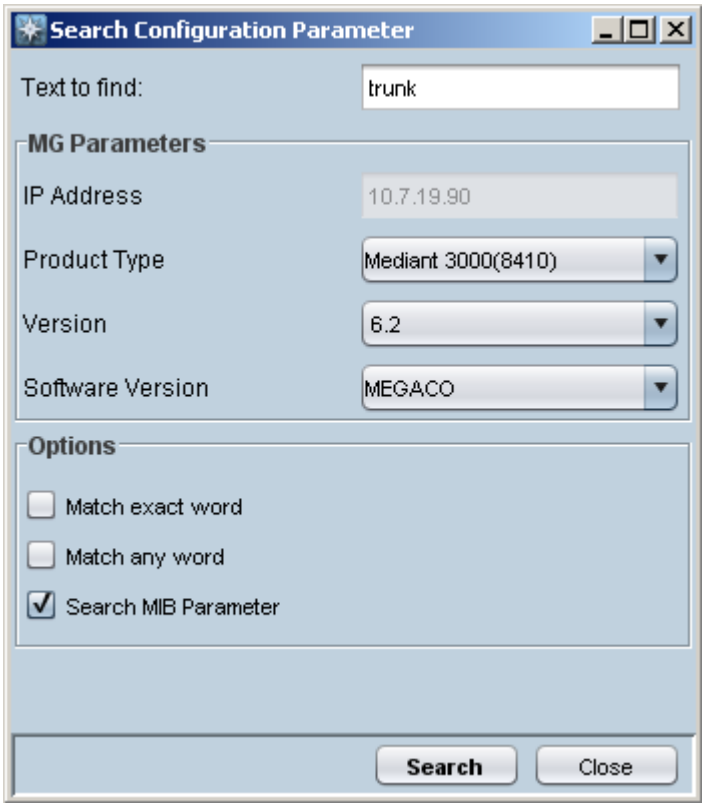
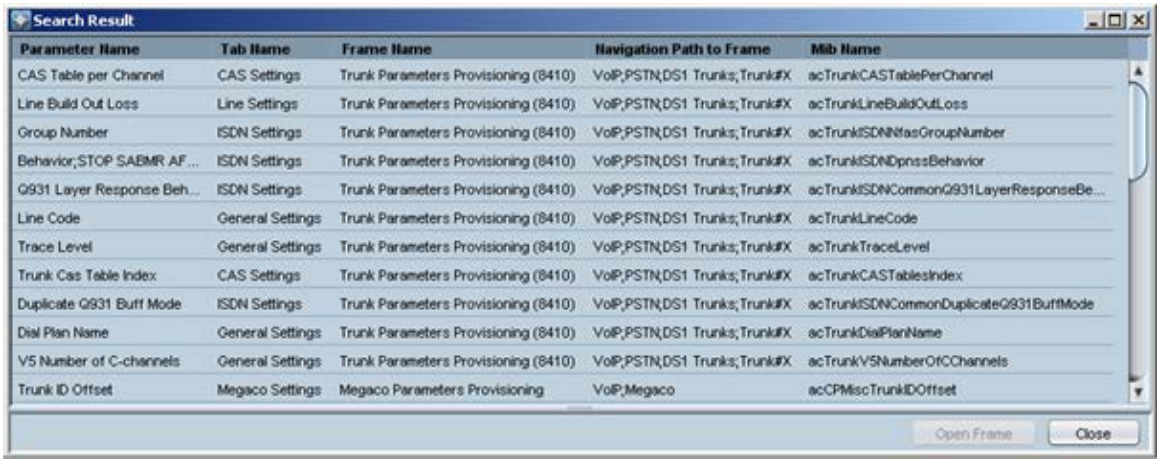


Figure 20-9: Advanced Search Configuration Results Dialog

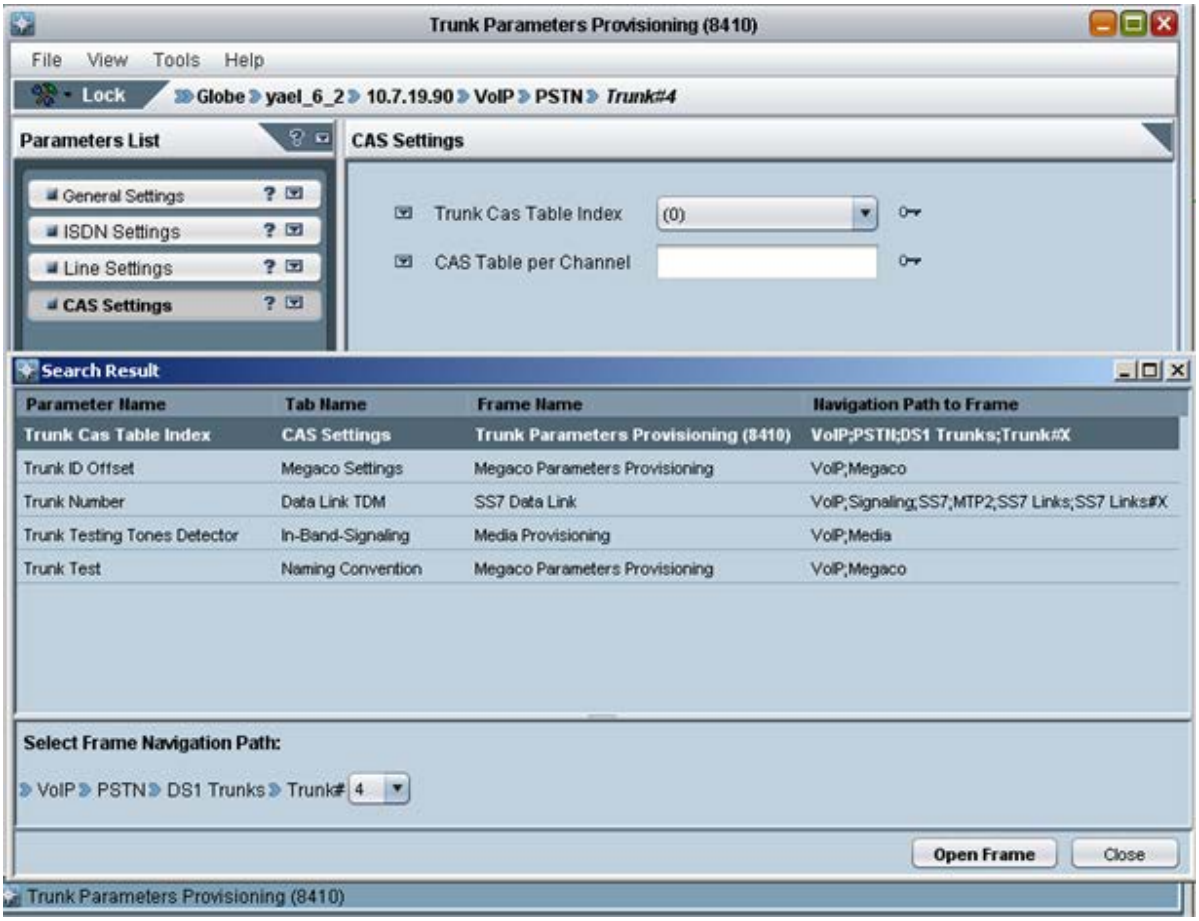


21.7.1 Search Results

When you select the relevant entry, the navigation path to this parameter is displayed in the lower pane. Clicking the 'Open Frame' button opens the provisioning frame for the selected entry.

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

Figure 20-10: Advanced Search Results screen and related Provisioning screen



22 Device Installation, Software Upgrade and Regional Files Distribution

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

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

For the Mediant 5000 / Mediant 8000, online software upgrade is supported (the device 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 device.

22.1 Software Manager

See Section 'Software Manager' on page 61.

22.2 Software Upgrade for CPE and Boards

This section describes the software upgrade for CPEs and boards.

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

1. Either select the device 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 device are displayed.
3. Wait for the operation result prompt; in both cases, the EMS opens the Software Manager with a subset of software files which can be loaded to the selected entities.

Notes:

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

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

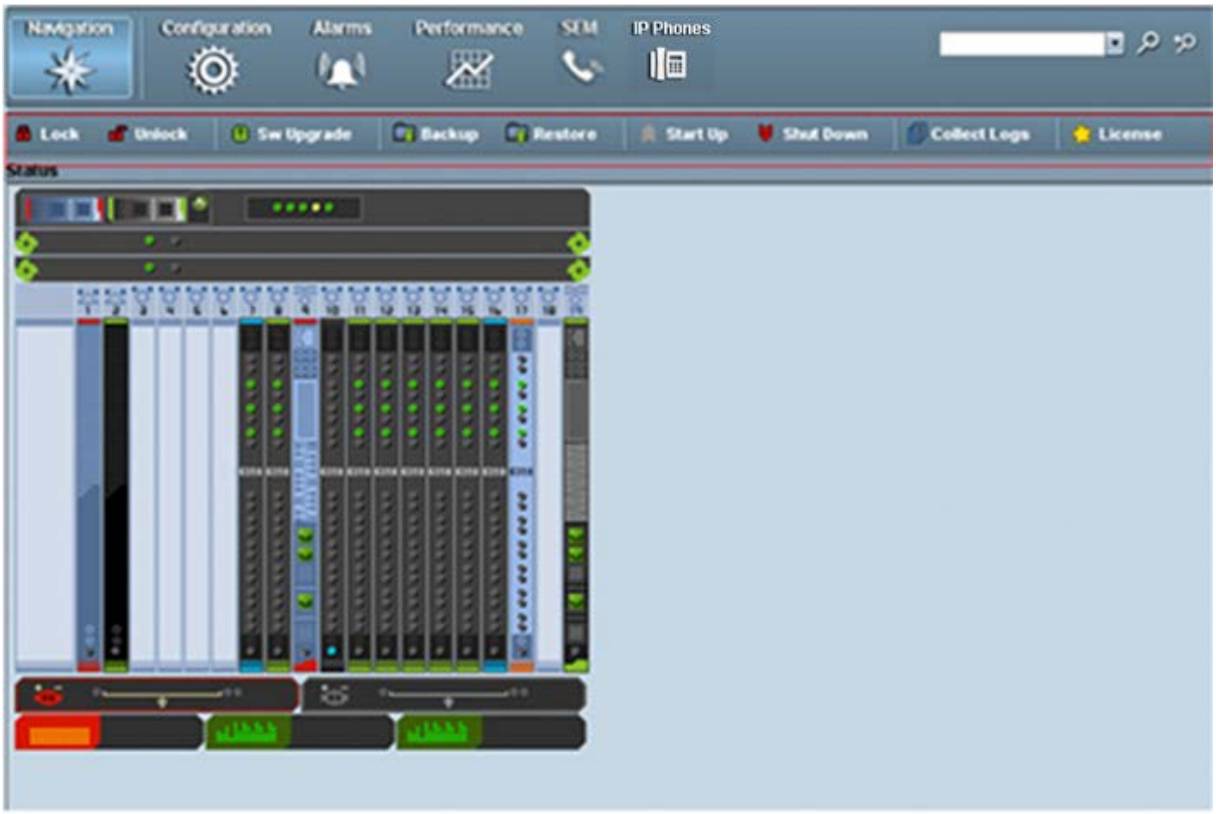
22.3 Mediant 5000/Mediant 8000 Maintenance Actions

This section refers to the Mediant 5000 and Mediant 8000. 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 device on which maintenance action is required.
2. In the Actions bar, click the relevant maintenance action. For example, **Lock** to lock the device.

Figure 21-1: 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 and Mediant 8000 have an FTP server.

22.3.1 Locking and / Unlocking the Device

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 device 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 device board returns to service its **Operational State** is enabled.

Notes: It may take some time for the operability state of an MO to change – e.g., it takes a few minutes for a device 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 device board returns to service its **Operational State** is enabled.

22.3.2 License Key Update

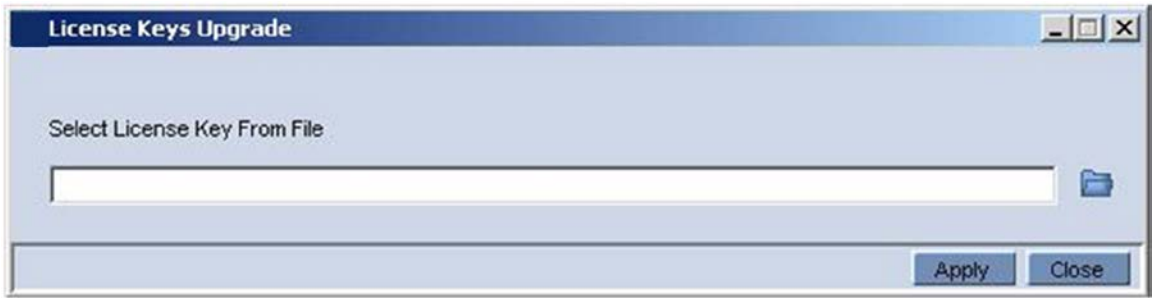
You can update the License Key for multiple TP boards managed in the same device using a single file which includes all the corresponding Keys.

➢ **To update the License Key:**

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

   The License Keys Upgrade dialog opens.

Figure 21-2: 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.

22.3.3 Online Software Upgrade Wizard

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

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

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

After upgrading each major system component (e.g., the SC or device 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 device to the pre-upgrade software version and configuration in the event of a problem.

The device continues its uninterrupted operation during the software upgrade of the SC and ES boards. However, certain calls can be affected when upgrading device boards, depending on the upgrade mode used. To minimize impact on device 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 device boards. The following options are available:
     - **Hitless Upgrade** – Gateway boards are upgraded via a switchover between normal and redundant boards of board activity; all established calls are preserved.
     - **Graceful Shutdown** – Gateway boards are upgraded sequentially; the mechanism minimizes the number of calls impacted.
   - **VoIP Board Upgrade Mode** – different levels of user involvement when upgrading boards; the following options are available:
     - **Non-Interactive** - the upgrade process moves to the next Gateway board without involvement on the part of the user; the user is informed when all boards complete the upgrade.
     - **Pause after the first gateway board** – allows a pause after the first board is upgraded so that the user can test the system and ensure that the upgrade to the board was successful before upgrading the remaining boards

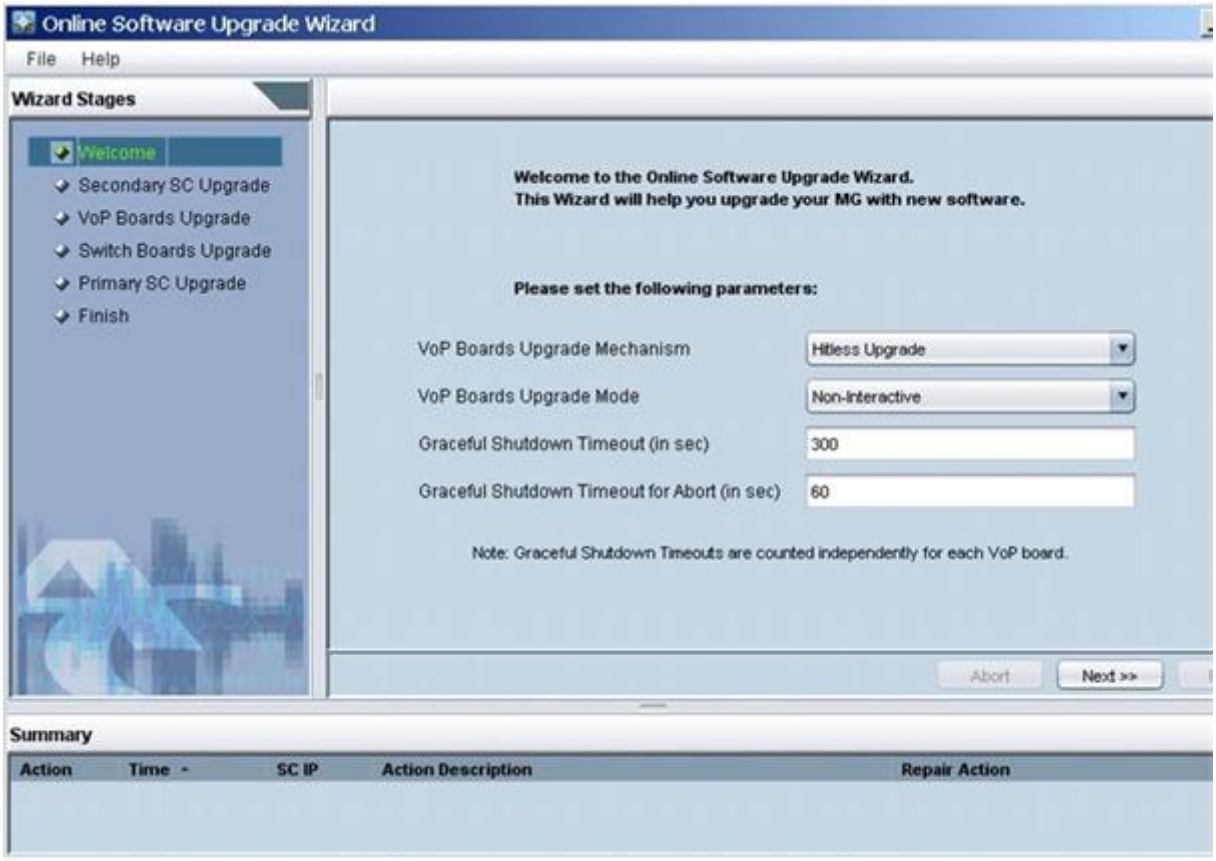
- **Pause after each gateway board** - allows a pause after each board is upgraded. The user controls the start time of each board upgrade. This option further minimizes the number of calls impacted by the upgrade.

- **Graceful Shutdown Period (sec)** – the period of time allowed for calls to end before each board is upgraded. Inapplicable when a board is upgraded with the Hitless Upgrade option. During the time period, the board accepts no new calls. At the end of the time period, all remaining calls are dropped.
- **Graceful Shutdown Period for Abort (sec)** – the time period used during a rollback sequence after the user clicks the **Abort** button.

Notes:

- Set parameter 'Graceful Shutdown Period' to 0 since it directly impacts the total time of the upgrade process and new calls are not established on the specific board during this time.
- Even though you choose 'Hitless Upgrade' as the upgrade mechanism, some boards may be upgraded with the Graceful Shutdown mechanism). Therefore set a proper value for the Graceful Shutdown Period and estimate the worst-case required upgrade maintenance time.
- The rollback sequence always uses the 'Graceful Shutdown' mechanism, so always set a proper value for the Graceful Shutdown Period for the 'Abort' parameter.

Figure 21-3: Welcome to the Online Software Upgrade Wizard

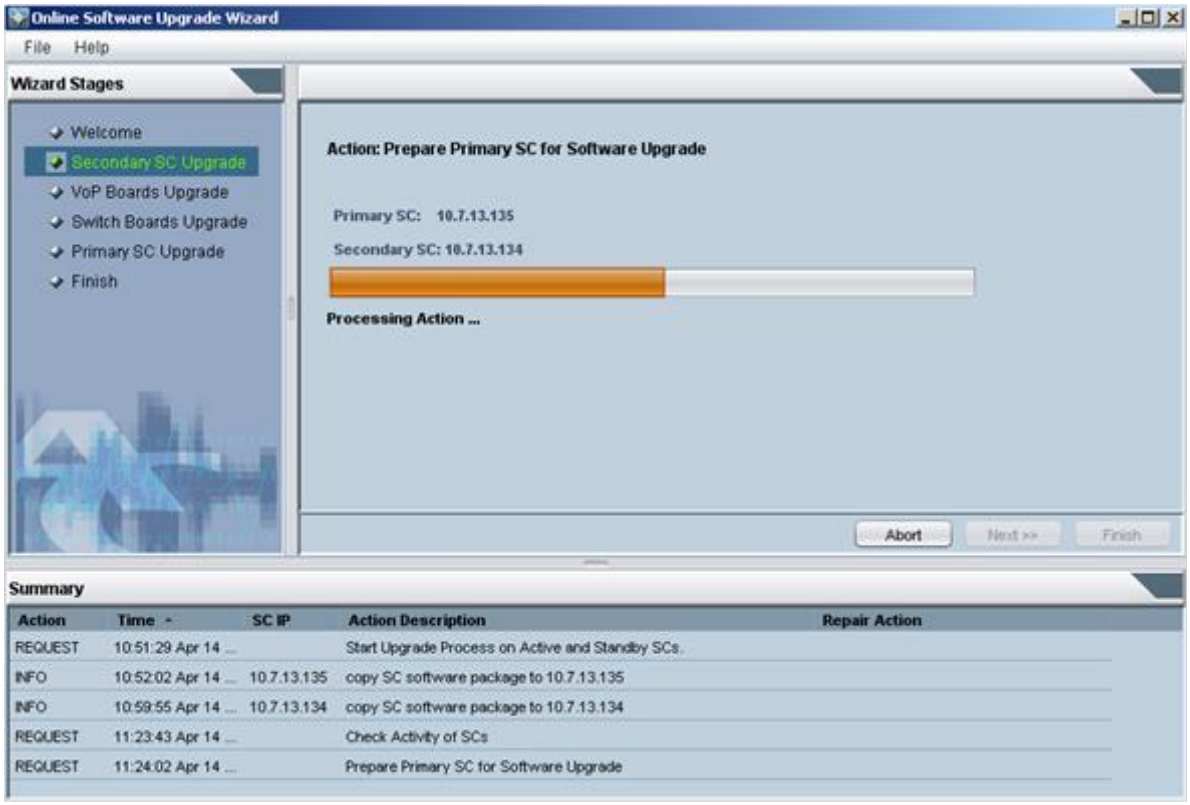


2. Secondary SC Update

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 21-4: 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**

22.3.3.1 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 device 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 device) 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.

22.3.3.2 Troubleshooting

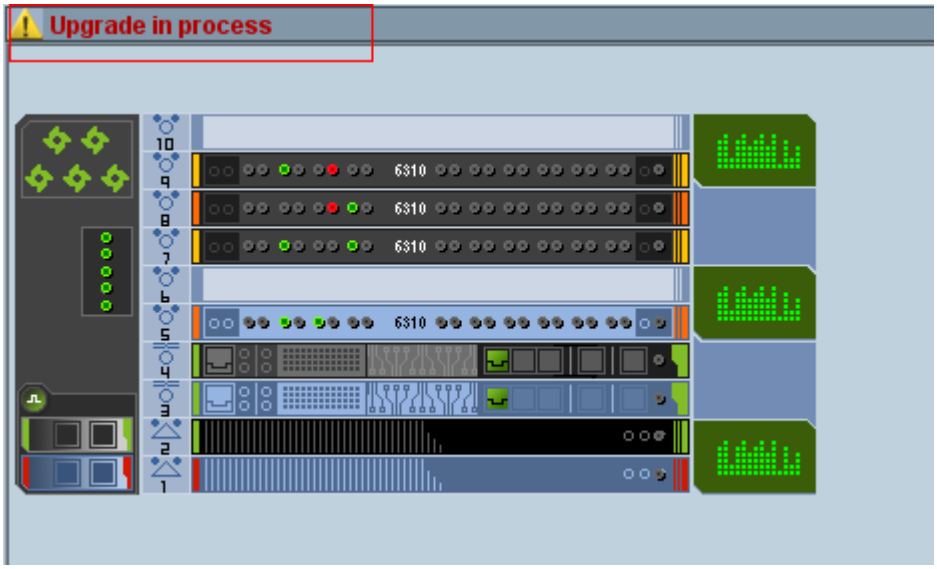
If you experience an unexpected network or software problem during online software upgrade (e.g., if the PC, on which the EMS client runs, crashes or the network connection to the device is lost) you have several options to continue the upgrade session from the same stage. If your network fails, a 'Connect' 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 21-5: Upgrade Indicator



22.3.4 Backing Up and Restoring the Device

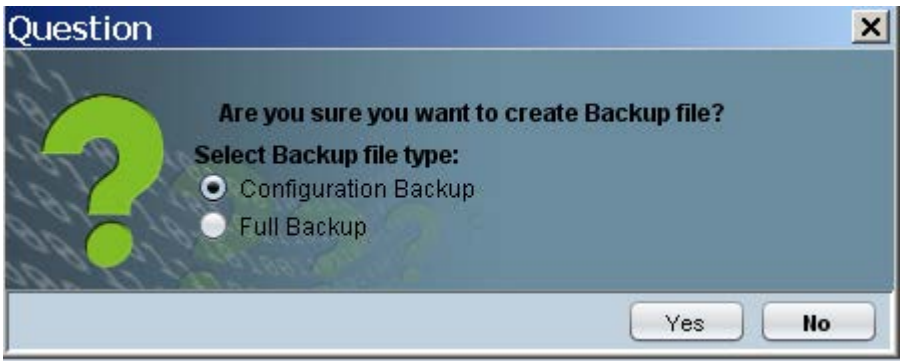
This section describes how to backup and restore the device.

➢ To back up the device:

1. From the 'Maintenance Actions' popup menu, select **Back Up**.
2. Click **OK**.

   Note that you cannot start up an already started device.
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 21-6: Create Backup File Prompt



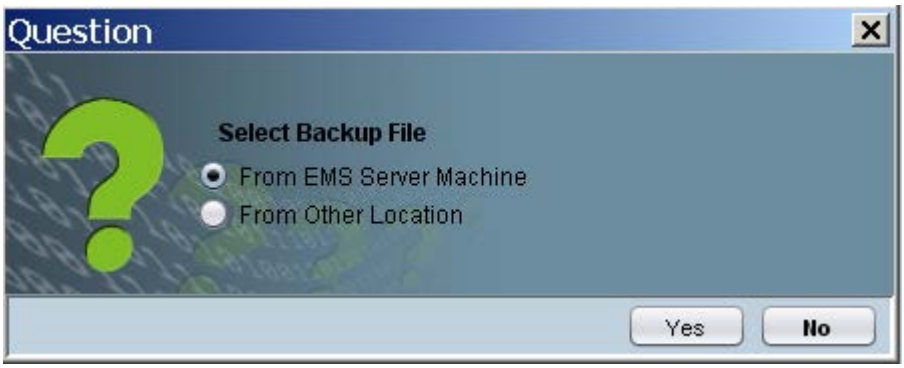
➢ To restore the device:

1. Lock the device.
2. From the 'Maintenance Actions' pop-up menu, select the **Restore** option. The user is prompted with the Note below.

Figure 21-7: Restore Device 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 21-8: Select Backup File Prompt



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

22.4 Mediant 5000, Mediant 8000 Startup and Shutdown

This section refers to the Mediant 5000 and Mediant 8000.

➢ To reset the device 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 device.

22.5 Collecting Log Files (Mediant 5000 and Mediant 8000)

This section describes how to collect log files.

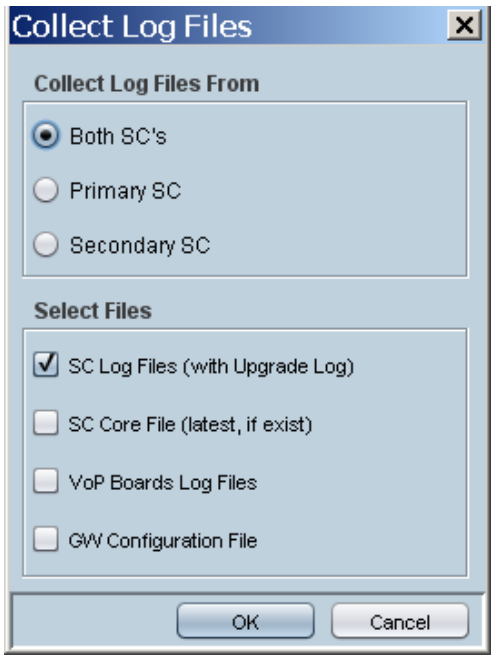
➢ To collect MG logs:

1. In the Actions bar, select **Collect Log Files** menu.
2. Select the SCs and Logs you wish to collect (see figure below), and clicking **OK** button.

The Log c ollection process is started, and the user is displayed with the waiting indicator. Upon log collection finish, the user is prompted with the file chooser to select a location for log file placement. The entire report is packaged as a TAR file, named according to following convention:

```
<GW_Name>_<GW_Global_IP>_report.tar
```

Figure 21-9: Collecting Log Files



22.6 Backup Files

This section describes how to backup device configurations.

22.6.1 Mediant 5000 and Mediant 8000 Devices

EMS can collect backup files (.bk files) that were created and locally stored on the device and store them on the EMS server machine, thereby enabling a centralized backup files location for all managed devices.

Upon file collection from the device, 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

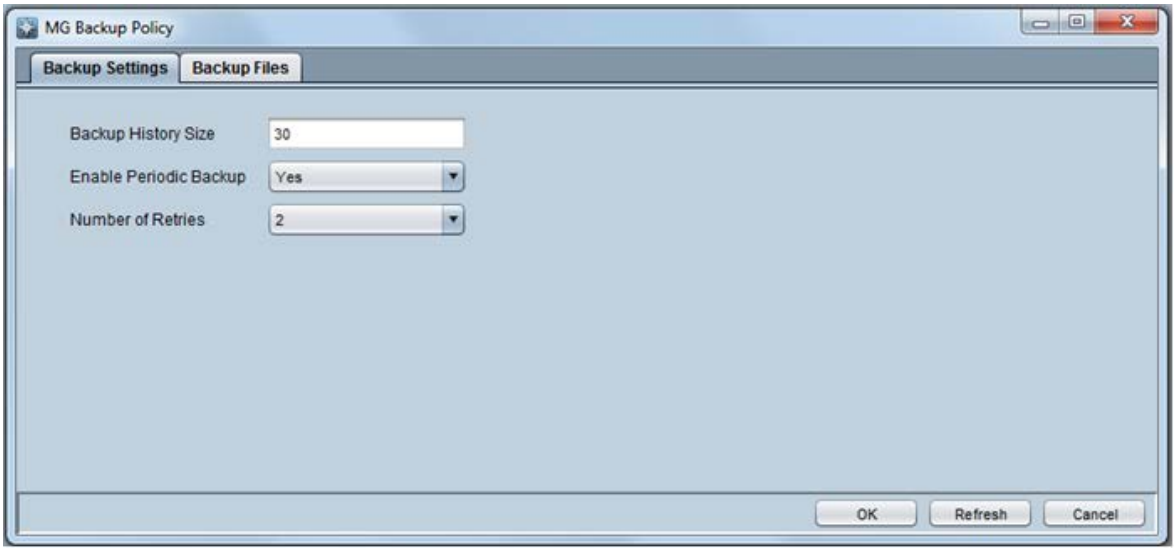
device backup files are located in the EMS Server machine under ACEMS/NBIF/mgBackup folder. File can be accessed and transferred using SSH, and SFTP.

Note: For Mediant 5000 and Mediant 8000 devices, the EMS periodically checks each of the devices and when a new backup file is created on the device, copies the file to the EMS server database. You can define different backup file creation rules for each device.

➢ To backup Mediant 5000 and Mediant 8000 devices:

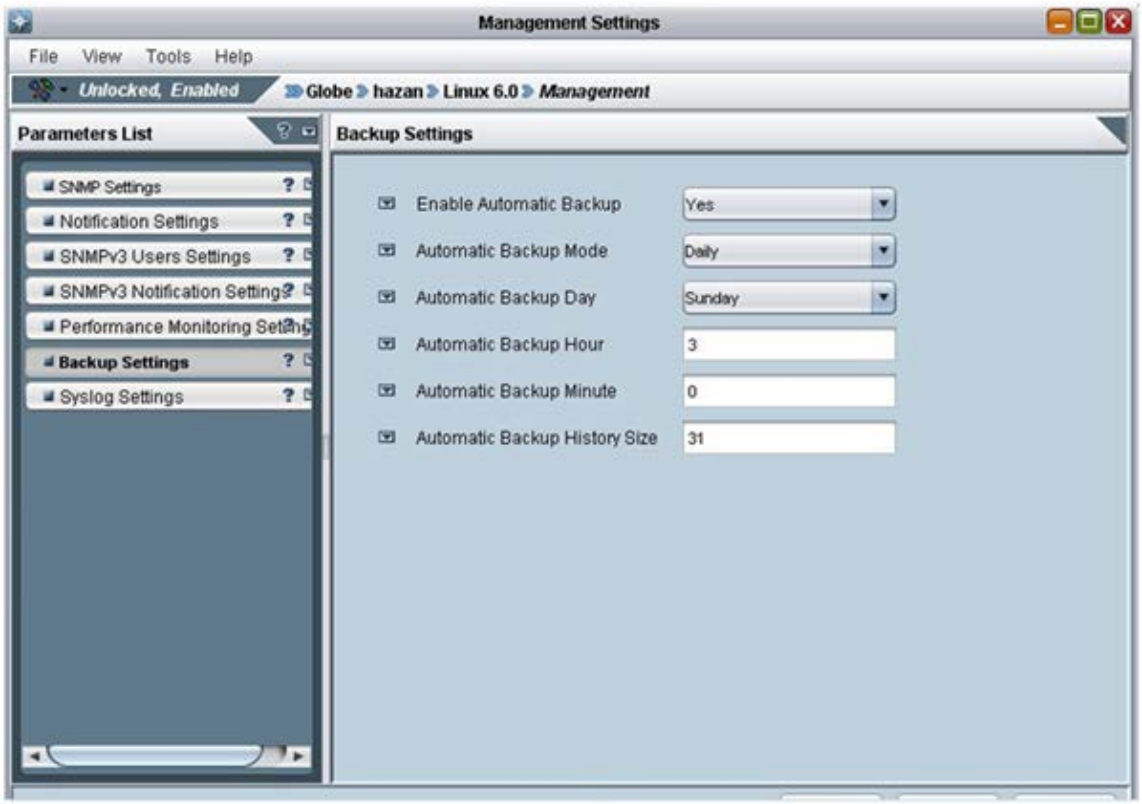
1. From the EMS menu, choose **Tools** > **MG Backup Settings**; the MG Backup Policy **Backup Settings** tab is displayed:

Figure 21-10: Backup Settings



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 devices. Default and maximum value -10.
3. Enable or disable Periodic Backup collection.
4. Define the number of retries that must be made on each connection to the device. Default-2.
5. To provision backup creation policy for each individual devices, open the device Provisioning Frame, Automatic Backup Tab. For more information, refer to the *Mediant 5000 / Mediant 8000 IOM Guide*.

Figure 21-11: Automatic Backup Setup



➢ **To view Mediant 5000 and Mediant 8000 backup files:**

1. From the EMS menu, choose **Tools** > **Backup Files**; the MG Backup Policy **Backup Files** tab is displayed with a listing of the device backup files *bk* files for the Mediant 5000 and Mediant 8000 devices.

22.6.2 CPE Devices

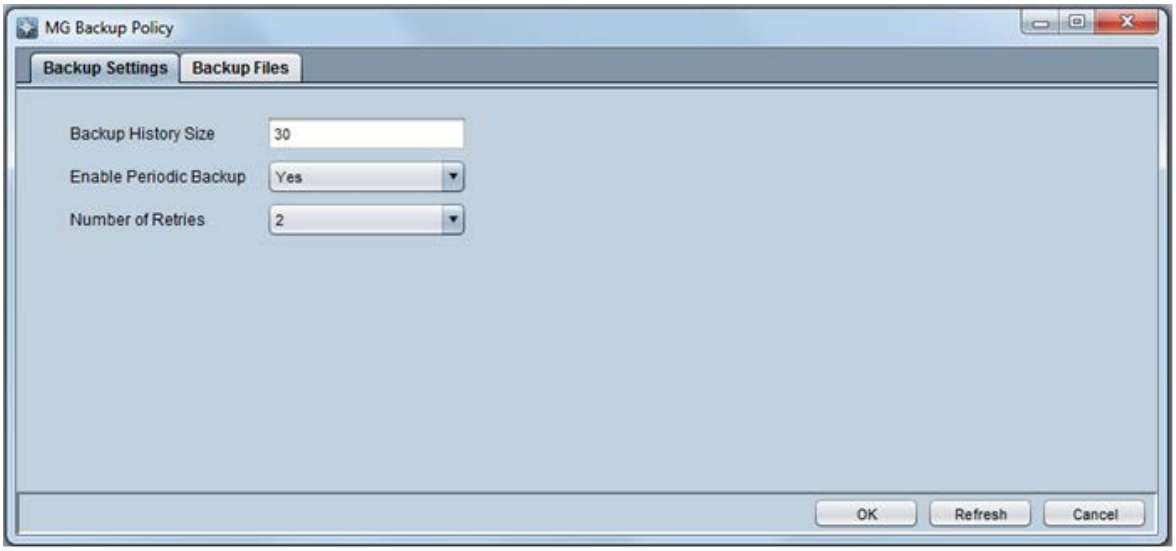
The EMS automatically backs up de vice configurations to ini or CLI script (MSBR device) files according to EMS server application time (device configuration is not saved to the EMS database). The ini files are updated according to the backup settings (described below).

CPE ini and CLI script files are saved on the EMS server machine in the /data/NBIF/mgBackup/ folder. These files can be ac cessed and t ransferred using SSH, and SFTP.

➢ **To configuration the backup file settings:**

1. From the EMS menu, choose **Tools** > **MG Backup Settings**; the MG Backup Policy **Backup Settings** tab is displayed:

Figure 21-12: Backup Settings

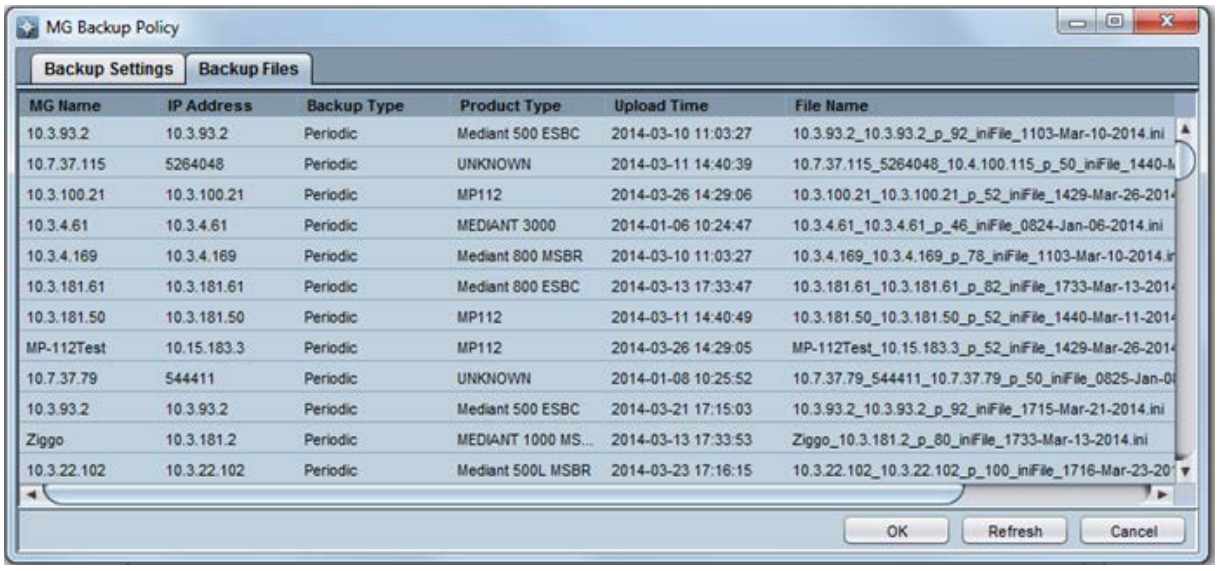


2. Set the 'Backup History Size' parameter. This parameter determines the number of latest backup files that will be stored for each one of the managed devices. Default and maximum value -10.
3. Enable or disable Periodic Backup collection.
4. Define the number of retries that must be made on each connection to the device. Default-2.

➢ To view CPE backup files:

1. From the EMS menu, choose **Tools** > **Backup Files**; the MG Backup Policy **Backup Files** tab is displayed with a listing of the device backup files (*ini* and *CLI script (*MSBR devices*)* files) for CPE devices.

Figure 21-13: Backup Files-CPE INI Files



2. To upload a ini or CLI script file to your PC, select the file, right-click, and then choose **Save As**.

3. To delete the ini or CLI script file/s, select the file/s, right-click and then choose **Delete File(s)**.

This page is intentionally left blank.

Part IV

Fault and Performance Management

This section describes fault and performance management.

23 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 device IP address, User name or Action Type, Alarm Name, Source or Free text in Description Fields.

Figure 23-1: Alarm Browser in Main Screen

This page is intentionally left blank.

24 Alarm Browser

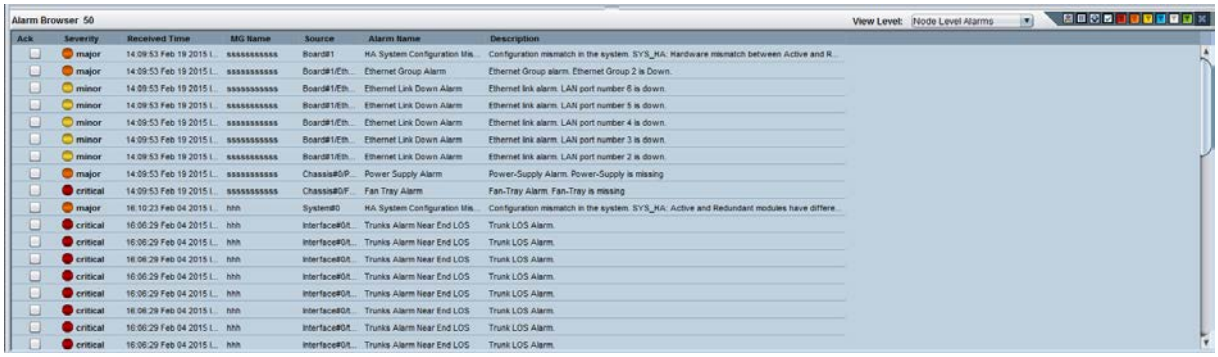
The EMS's fault management functionality manages and displays all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system.

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 devices 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 device 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 device 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 Paris region-context alarms displayed in the Alarm Browser.

Figure 24-1: Alarms Browser



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.
- **Occurred Time** - indicates the time that the alarm occurred on the device (Day of the Week, Month, Date in the Month, Hours: Minutes: Seconds, Time Zone, Year.
- **Received Time** – indicates the time that the alarm was received by the EMS server (Day of the Week, Month, Date in the Month, Hours: Minutes: Seconds, Time Zone, Year). Note that the Time value that is displayed in the Alarm Browser is based on the time setting of the 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 Name** (short description of the alarm)
- **Events** are indicated by the label [Event] which makes it easy for the user to sort between alarms and events.
- **Description** (elaborated alarm details)

Notes:

- By default, alarms are listed in the Alarm Browser in chronological order. The most recently received alarms appear at the **top** of the list, with the oldest alarms at the **bottom**.
- The same NTP server should be configured on the device and the EMS server to ensure acccurate time indications in the alarm details. For more information, refer to the *EMS Server IOM Manual* and the *User's Manual* for the relevant device.

24.1 Filtering Alarms

The Alarm Browser lists all the currently active alarms in the EMS for a c ontext selected in the Navigation module. When selecting the root (Globe) of the managed devices 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 devices under that region. Available contexts are categorized 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 24-1: Alarm Browser Buttons

Alarm Severity Filtration Toolbar	Purpose (When Clicking on a Button on the Toolbar)
	Opens the graphical display for the current alarms for this device. For more information, see page 287.
	Opens the Actions Journal. For more information, see Section Viewing Operator Actions in the Actions Journal on page 373.
	Enables Audio Indication on receipt of alarm. 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; a different sound is played for each severity type.
	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.

Alarm Severity Filtration Toolbar	Purpose (When Clicking on a Button on the Toolbar)
	Filters the active Alarm Browser window by displaying Clear Alarms.
	Close Alarm Browser

Notes: By default, all Alarm Severity Filtration buttons are selected, meaning that both acknowledged and unacknowledged alarms of all severities are displayed by default. After clicking a button, the arrow (↓) ceases to be displayed on that button, meaning that alarms have been filtered for that severity level.

24.2 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.

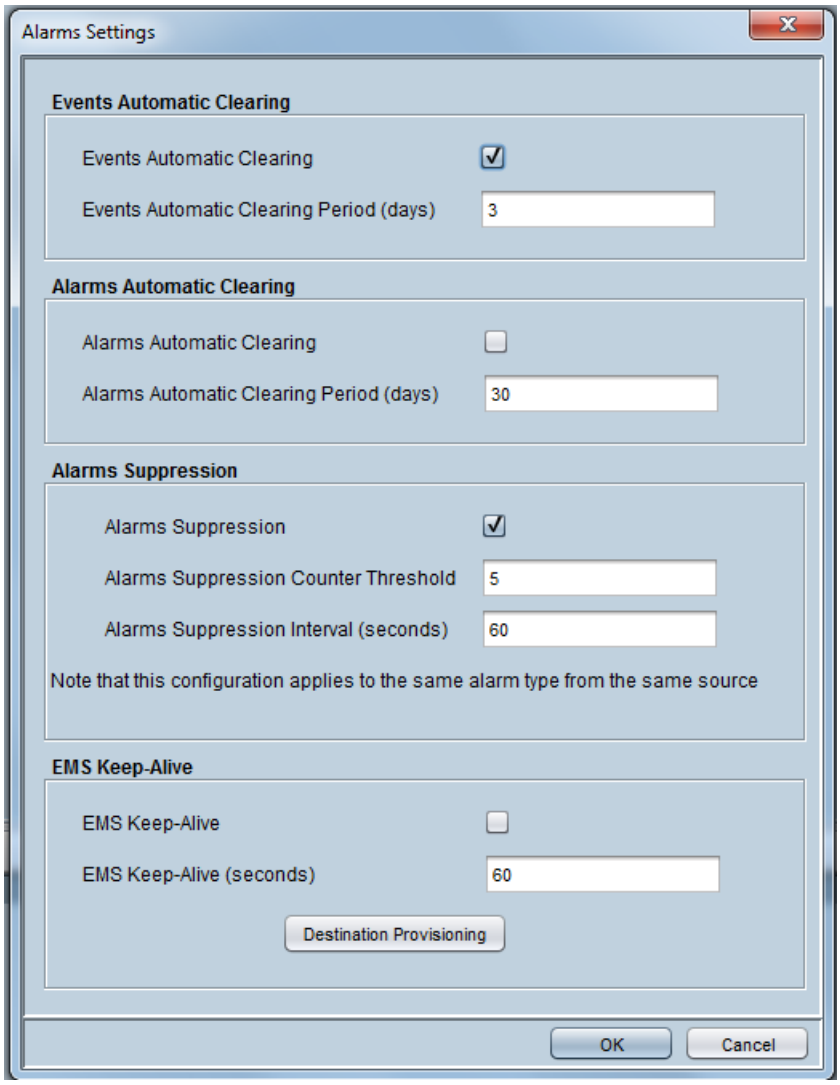
24.3 Alarm and Event Management

The Alarm Settings screen provides several options for you to configure which alarms and events are displayed in the Alarms Browser.

➢ To manage alarms and events displayed in the EMS:

1. In the EMS Main menu, choose **Faults** -> **Alarm Settings**. The Alarms Settings screen is displayed:

Figure 24-2: Alarm and Event Auto - Clearing Settings



This screen provides the following configuration options:

- Alarms and Event Clearing (see page 276)
- Alarms Suppression (see page 277)
- HA Alarms Forwarding (see page 278)

24.3.1 Alarms and Event Clearing

The Alarm Browser for each device is cleared of 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 device 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.

The default application settings ensure that events are cleared by the EMS application after three days, while alarms are not cleared (only by the device itself). If you wish the EMS to perform automatic alarms clearing, select the 'Alarms Automatic Clearing' check box 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'.

24.3.2 Alarm Suppression Mechanism

When the EMS server recognizes that there are greater than a threshold-defined number of alarms of the same type and from the same source that are generated in a threshold-defined time, an 'Alarm Suppression' alarm is generated. At this point, these alarms are not added to the database and are not forwarded to configured destinations.

When the 'Alarms Suppression' check box is selected, you can configure a counter threshold (default - 10 alarms) and interval (default - 10 seconds). For example, if there are 10 alarms generated from 'Board#1/EthernetLink#2 in 10 seconds, then alarms from this source are suppressed and the 'Suppression' alarm is generated. This alarm is cleared when in the subsequent 10 second interval, less than 10 alarms are sent from this source. At this point, updating to the EMS database is resumed (the last received alarm is updated).

During the time that the Suppression alarm is active, the EMS server updates the database with a single alarm (with updated unique ID) database every minute, until the alarm is cleared.

Notes:

- This feature applies for alarms of the same type and from the same source.
- When forwarding traps, you can determine whether the Suppression alarm is forwarded (see 'Trap Forwarding' on page 303).

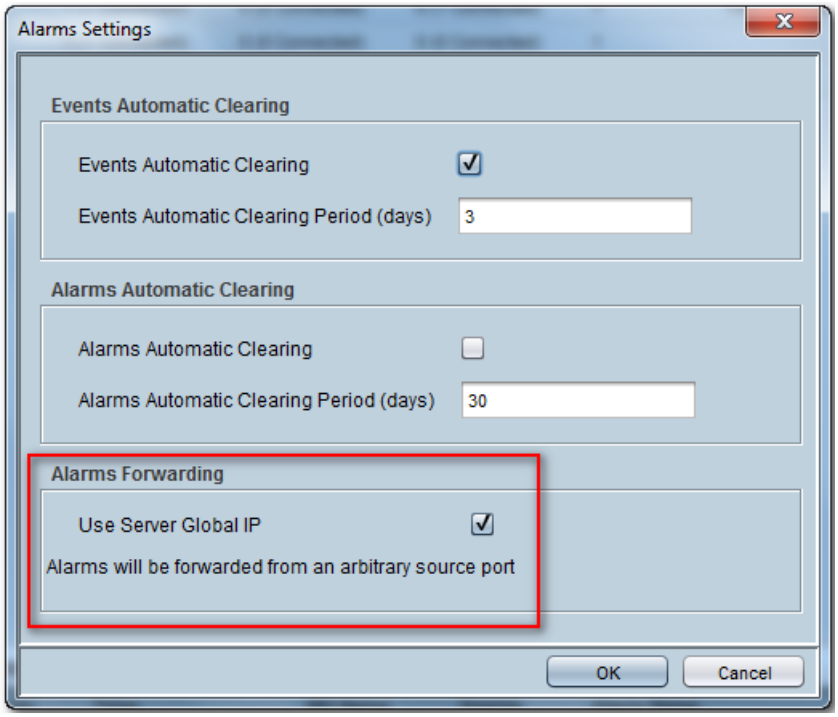
24.3.3 HA Alarms Forwarding

You can forward alarms from the EMS HA server that is configured with a global IP address.

Whenever a trap is forwarded from the EMS, it's source IP address is shown as the Global IP address of the EMS server that is configured in the Primary HA Server Installation setup (for more information, refer to the *EMS Server IOM manual*).

Notes: This option only appears when the EMS server is configured for HA using a global IP address.

Figure 24-3: HA Alarms Forwarding



24.3.4 EMS Keep-alive

You can configure the EMS to generate SNMP Keep-alive traps toward 3rd-party applications, such as a Syslog server.

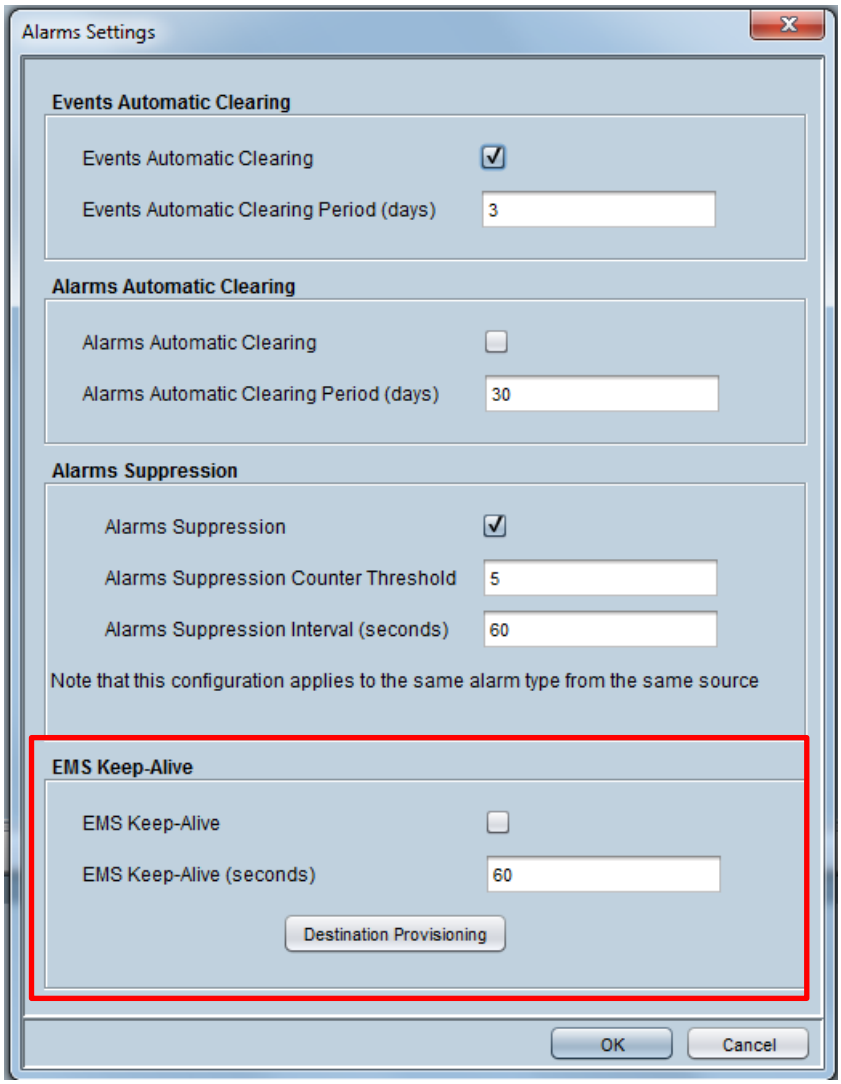
When the "EMS Keep-Alive" check box is checked, this trap is sent from the EMS to a configured destination according to a configured interval (default 60 seconds).

You can send the Keep-alive trap to the desired destination (according to an existing configured forwarding destination rule). This trap can be sent to either the SNMP, Syslog or Mail server destination.

➢ **To configure EMS Keep-alive:**

1. In the EMS menu, choose **Faults** > **Alarm Settings**.

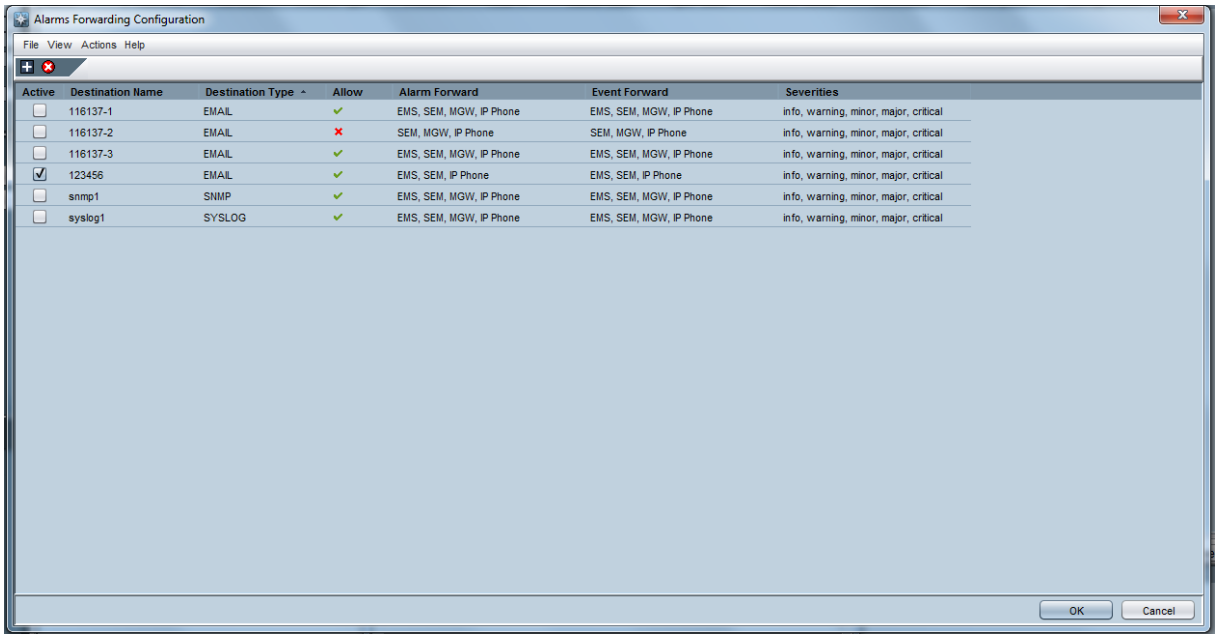
Figure 24-4: EMS Keep-alive



2. Select the EMS Keep-Alive check box.

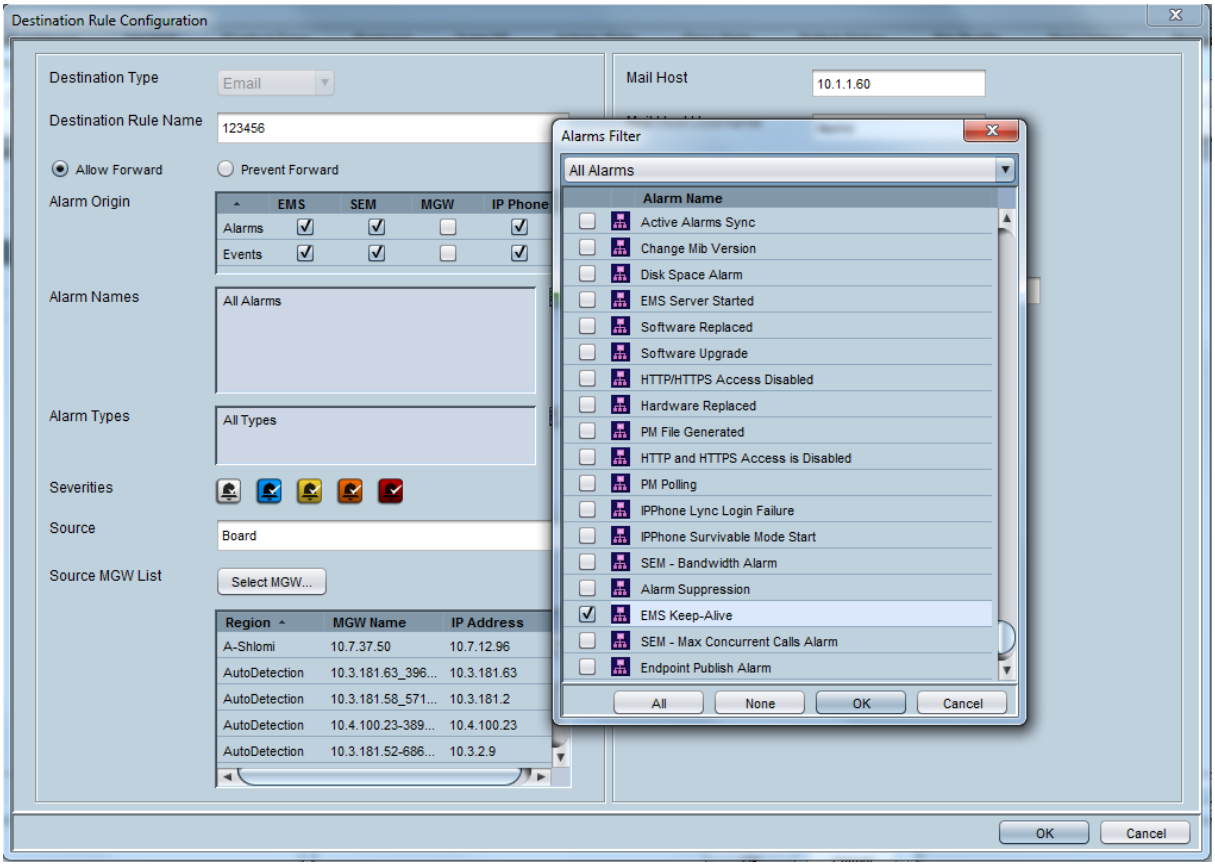
3. Click the Destination Provisioning button; the Alarm Forwarding Configuration window is displayed

Figure 24-5: Alarm Forwarding Configuration



4. Select the Active check box for the destination that you wish to forward the EMS Keep-alive trap.
5. Double-click the destination rule to open the Destination Rule Configuration window.

Figure 24-6: Destination Rule Configuration



6. In the Alarm Names pane, click the Alarms Filter and ensure that the "EMS Keep-Alive" alarm is selected.

24.4 Changing the Alarms Browser Views

This section describes how to change the Alarms Browser Views.

24.4.1 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:

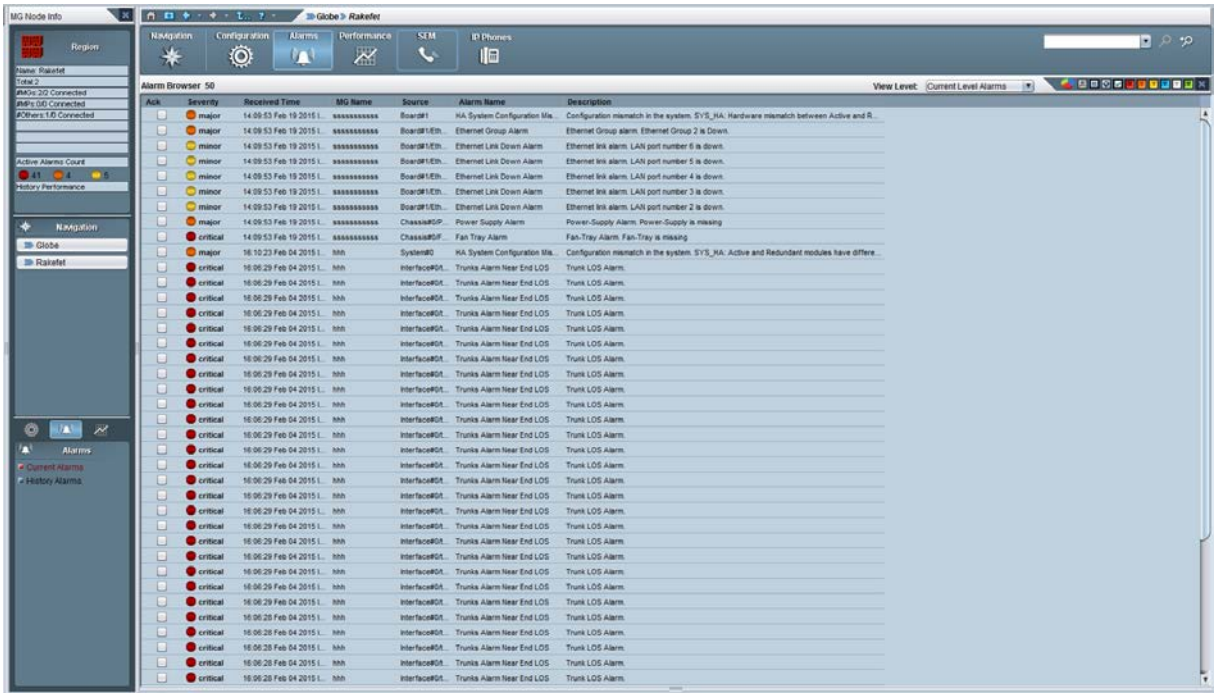
- **Current Level Alarms (default)** - users view alarms filtered according to the context they're viewing in the status pane
- **Node Level Alarms** – users always view all alarms received from the node they're viewing, regardless of the lower level context (board, trunk) they've accessed.
- **Region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

24.4.2 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 / Mediant 8000 devices). 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 24-7: Alarm Browser Column View

Figure 24-8: Current Alarms



24.5 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 284.

24.6 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 373.

24.7 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.

24.8 Alarms and Events Filtering and 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]

24.9 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**.

25 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 device location, physical attributes of failed entity.

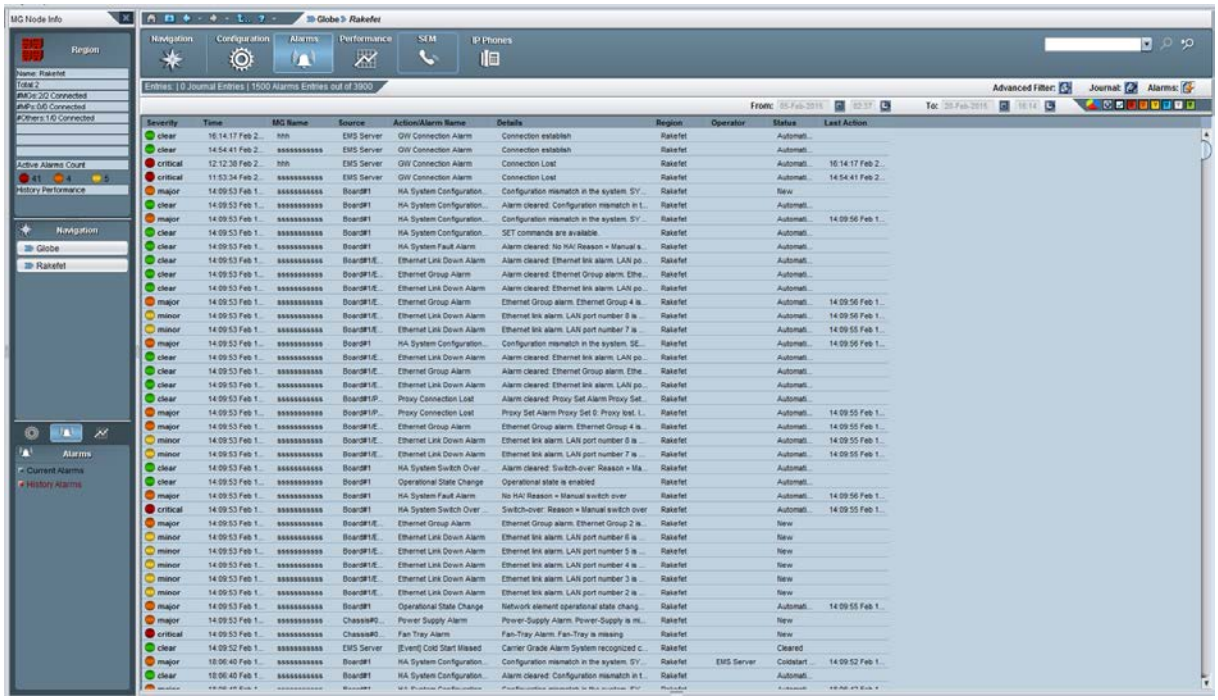
Open the Alarms History screen from the Alarms module by clicking the 'History Alarms' option. The Alarms History screen is context-sensitive like the Alarm Browser; the context is displayed in the title of the screen.

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 25-1: 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**.

26 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.

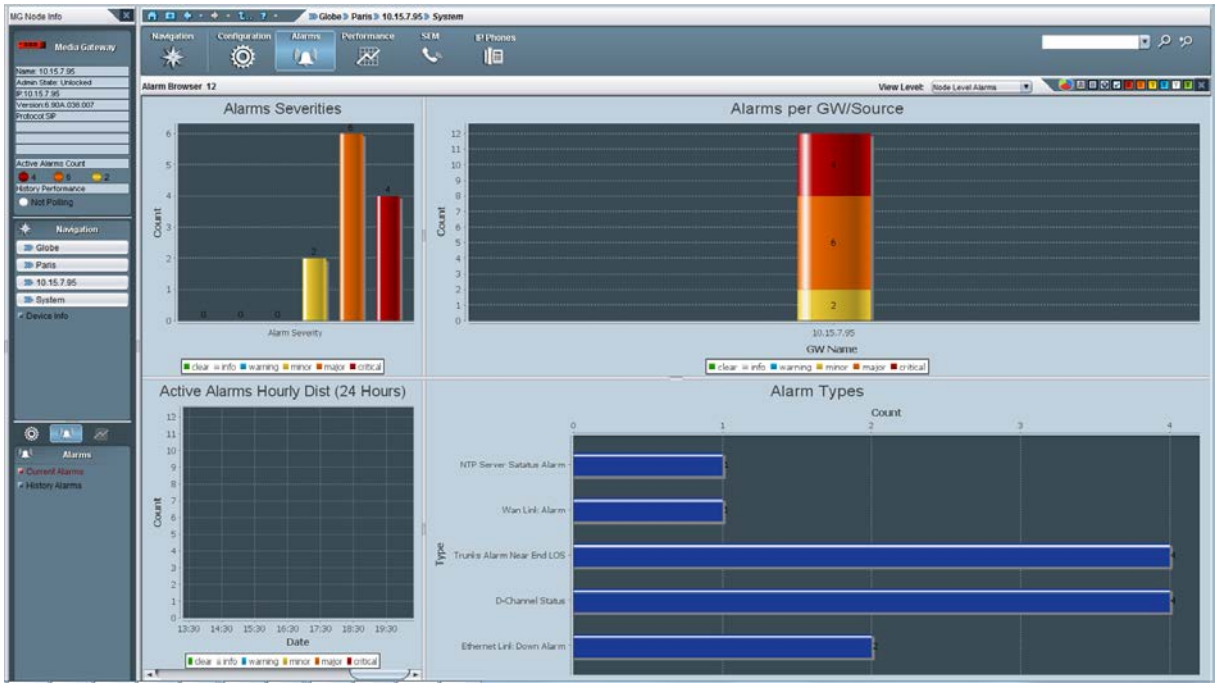
The following graphs are displayed:

- 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 device (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 device:

Figure 26-1: Current Alarms Graph



The following screen illustrates the History Alarms graph for the device:

Figure 26-2: History Alarms Graph

27 Using Alarm Filters

This section describes how to use the alarm filters.

27.1 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 27-1: Alarms History Screen: Defining Time Filtration using Calendar

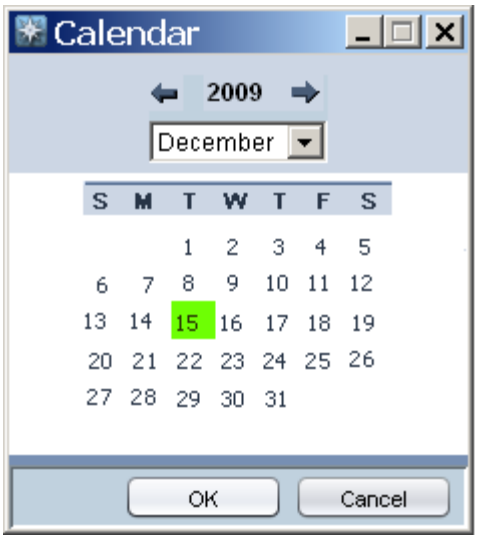
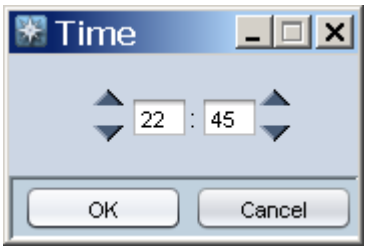


Figure 27-2: Alarms History Screen: Defining Time Filtration using Hour & Minutes



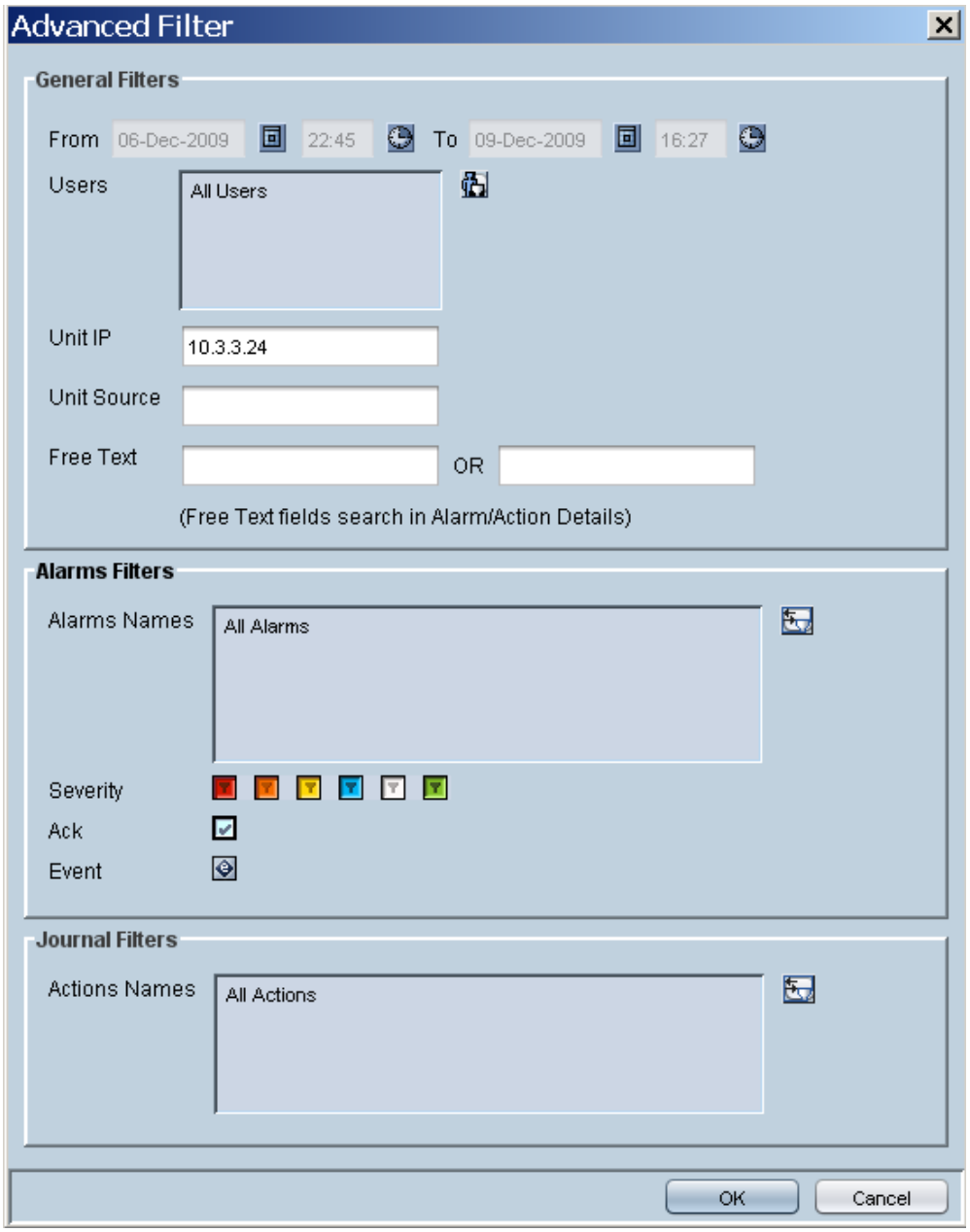
27.2 Using Advanced Filters

You can use the 'Advanced Filter' screen to define queries to search for EMS and device 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 device.

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 27-3: 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

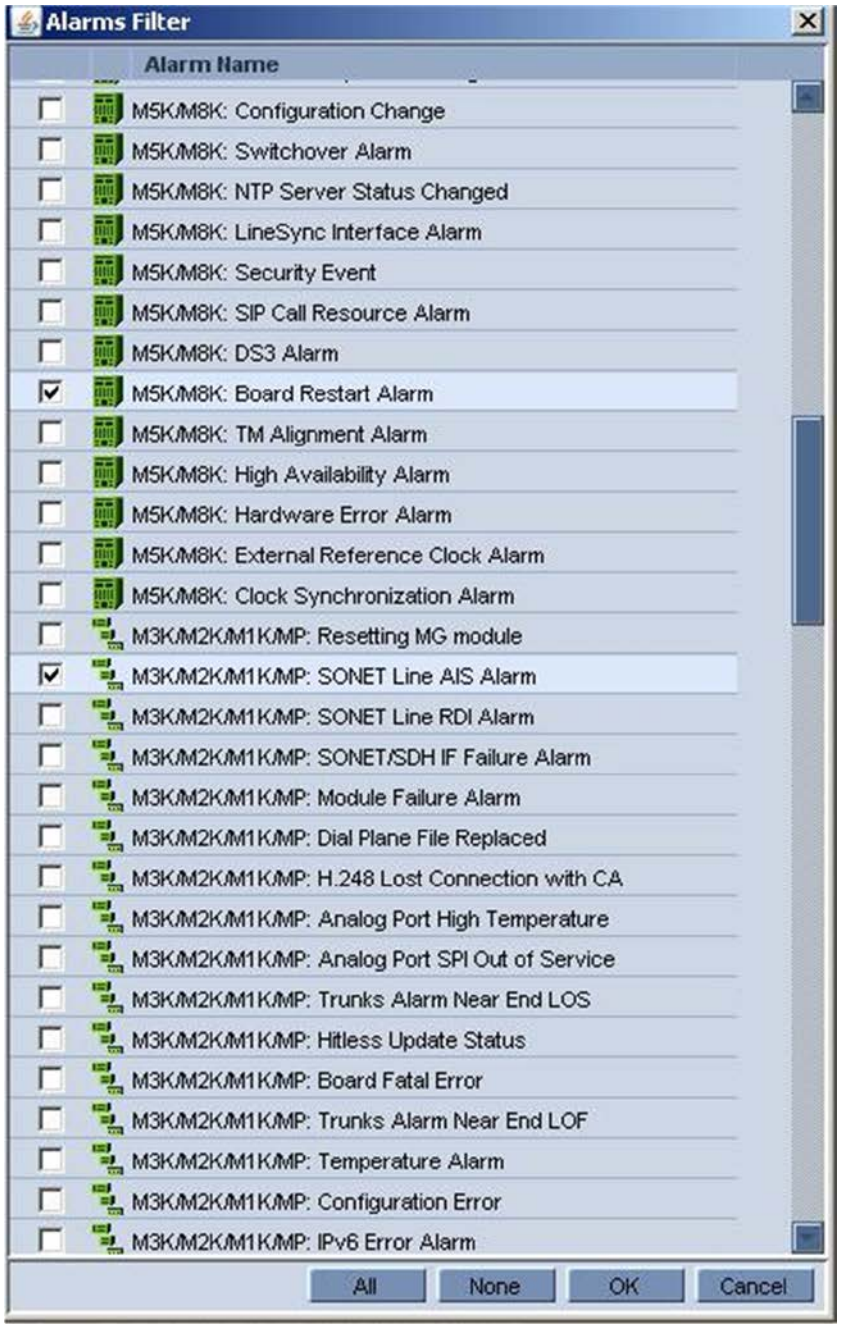
- **Journal Filters**

  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 27-4: Alarms Filter



28 Defining Complex Queries using a Combination of Filters

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

28.1 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 device, 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 device 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

29 Viewing, Interpreting an Alarm's Details

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

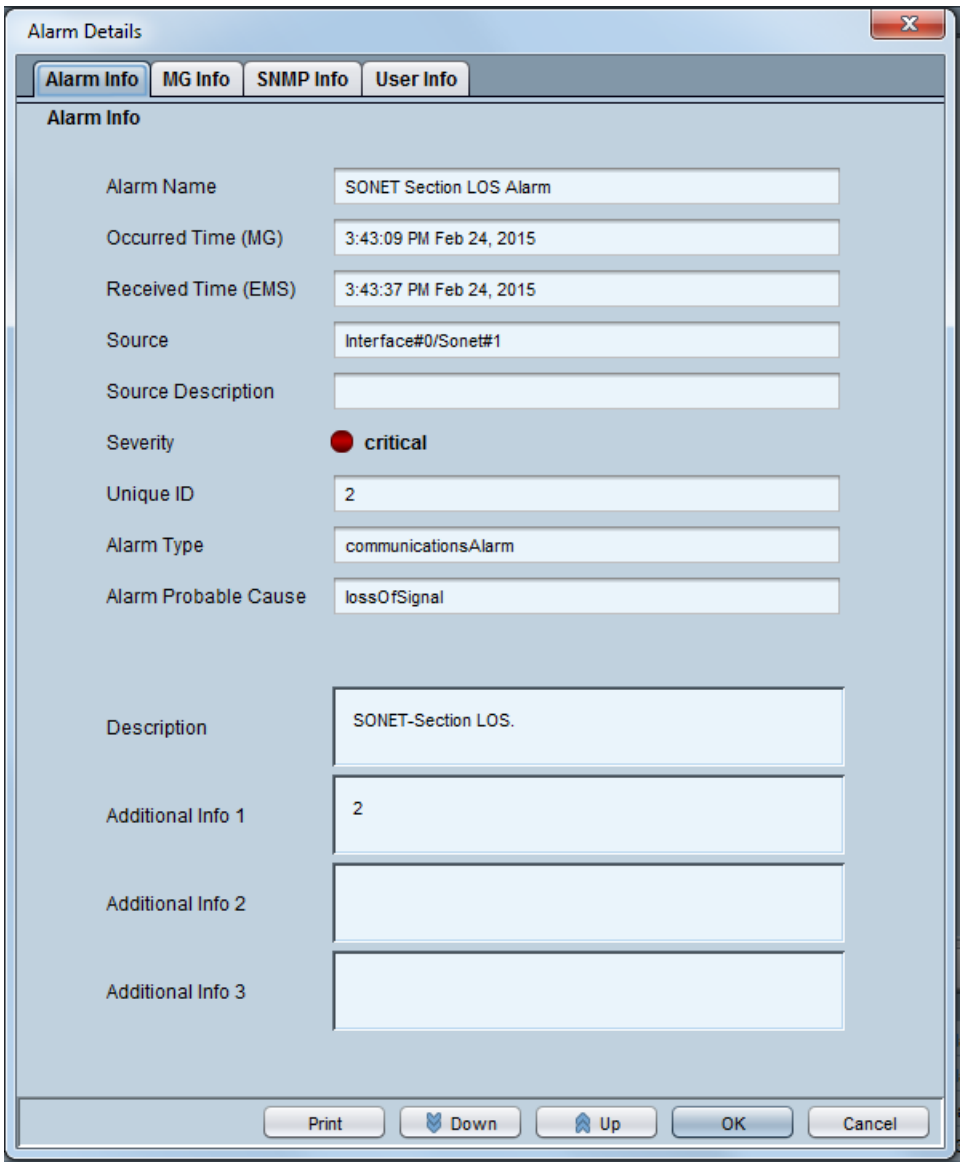
➢ **To view/interpret an alarm's details, do one of the following:**

- 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 29-1: 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 device, 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).

29.1 Alarm Info Tab

The Alarm Info tab features the following fields:

- **Title** – The name of the alarm, provided in the Alarm Browser.
- **Occurred Time** – indicates the time that the alarm occurred on the device (Day of the Week, Month, Date in the Month, Hours:Minutes:Seconds, Time Zone, Year.
- **Received Time** – indicates the time that the alarm was received by the EMS server (for more information, see page 271).
- **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 device for alarm clearing and correlation purposes.
- **Alarm Type** – The alarm type can be one of the following:
  - Communication (inter-process communication alarm)
  - Quality of Service (indicates degradation in service performance)
  - Processing Error (used for internal software errors)
  - Equipment Alarm (indicates a hardware failure)
  - Environmental alarm (used to indicate environmental errors such as temperature, power, etc.)

Notes: The parameter 'Alarm Type' is based on ITU X.733, X736 standards.

- **Probable Cause** – the probable cause of the alarm, which may be one of the following reasons:
  - Degraded Signal for Trunk Alarm
  - Communications Protocol Error for a V5.2 Alarm
  - Underlying Resource Unavailable for a Change in a Managed Entity's Administrative State or Operational State
  - Configuration Or Customization Error for Configuration Error Alarm
  - Heating Vent Cooling System Problem for Fan or Temperature Alarm
  - Temperature Unacceptable for Temperature Alarm
  - Power Problem for Voltage Alarm

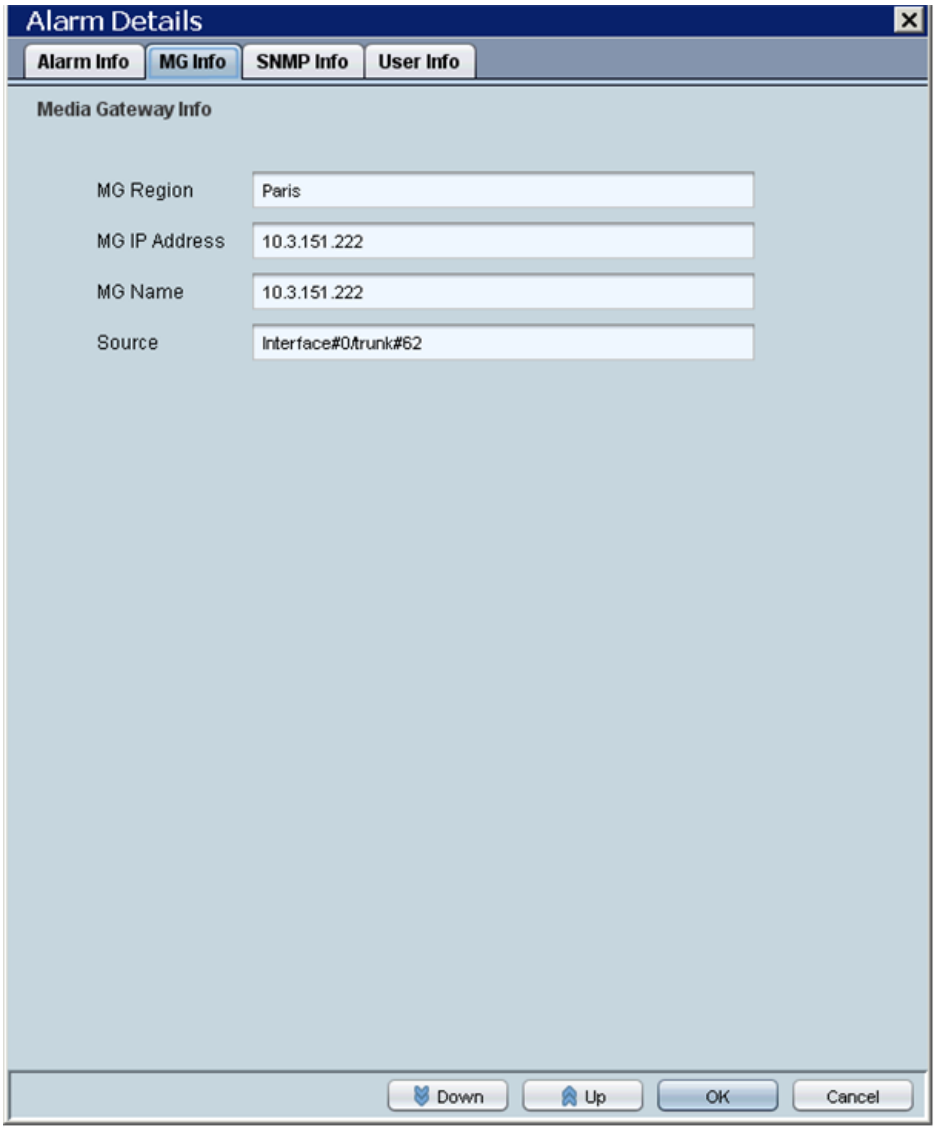
Notes: The parameter 'Alarm Type' is based on ITU X.733, X736 standards.

- **Description** – Textual description of the alarm, received as part of the alarm information
- **Additional Info 1-3** – These three fields are provided as part of the alarm information, supplying additional information on the alarm.

29.2 Alarm Details - Tab MG Info

This section describes the MG Info tab.

Figure 29-2: Alarm Details-MG Info



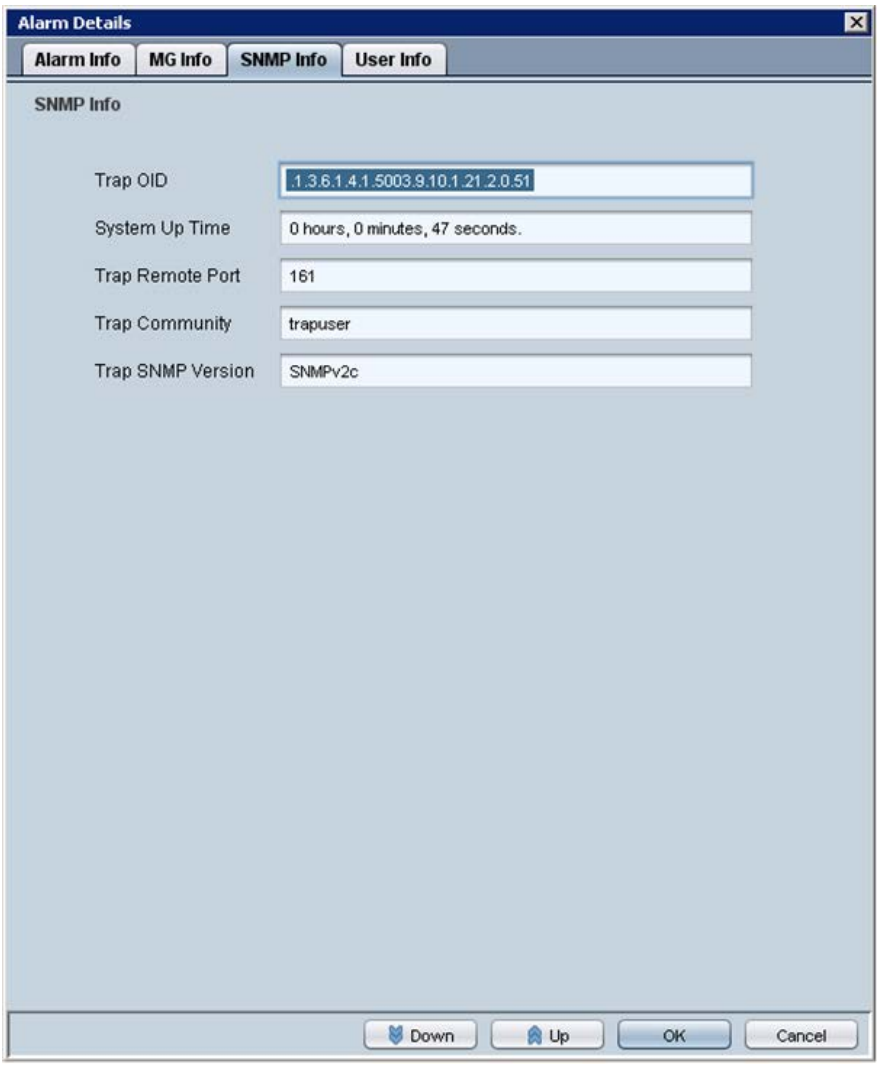
The **MG Info** tab features the following fields:

- **MG Region** – The name of the region in which the device is located.
- **MG IP Address** – The IP address of the device that originated the alarm.
- **MG Name** – Name of the device that originated the alarm.
- **Source** – The exact alarm source, in format 'board#3/trunk#7'.

29.3 Alarm Details > Tab SNMP Info

This section describes the SNMP Info tab.

Figure 29-3: Alarm Details-SNMP Info



The **SNMP Info** tab features the following fields:

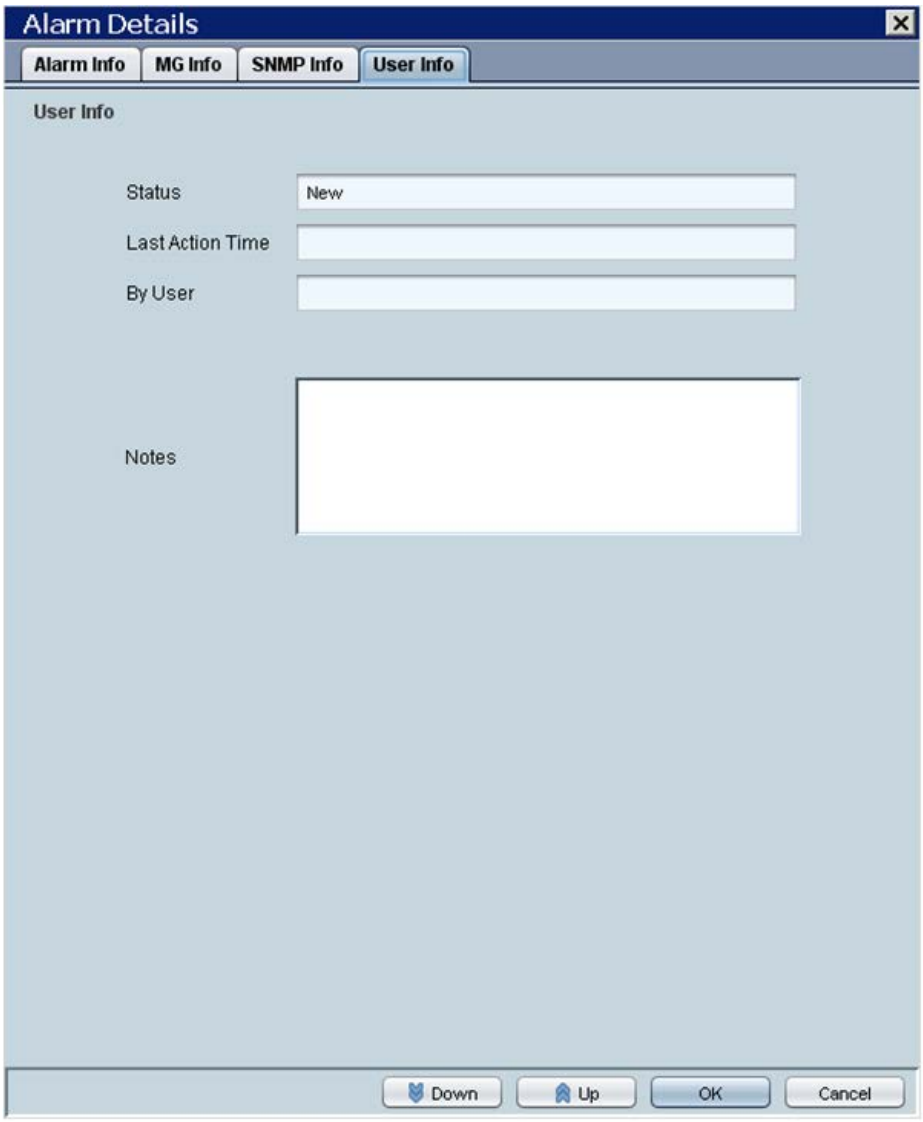
- **Trap OID** – Trap Object Identifier, as defined in the MIB.
- **System Up Time** – The time elapsed since the last system reset.
- **Trap Remote Port** – The EMS UDP remote port at which the trap was received.
- **Trap Community** – Trap Community String received as part of the Notification message

- **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

29.4 Alarm Details > Tab User Info

This section describes the User Info tab.

Figure 29-4: Alarm Details-User Info



The **User Info** tab features the following fields:

- **Status** – This field can be one of the following values:
  - 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 device; the alarm condition no longer exists.
  - ColdStart Cleared (The device 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.

30 Trap Forwarding

All the alarms and events issues by devices 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.

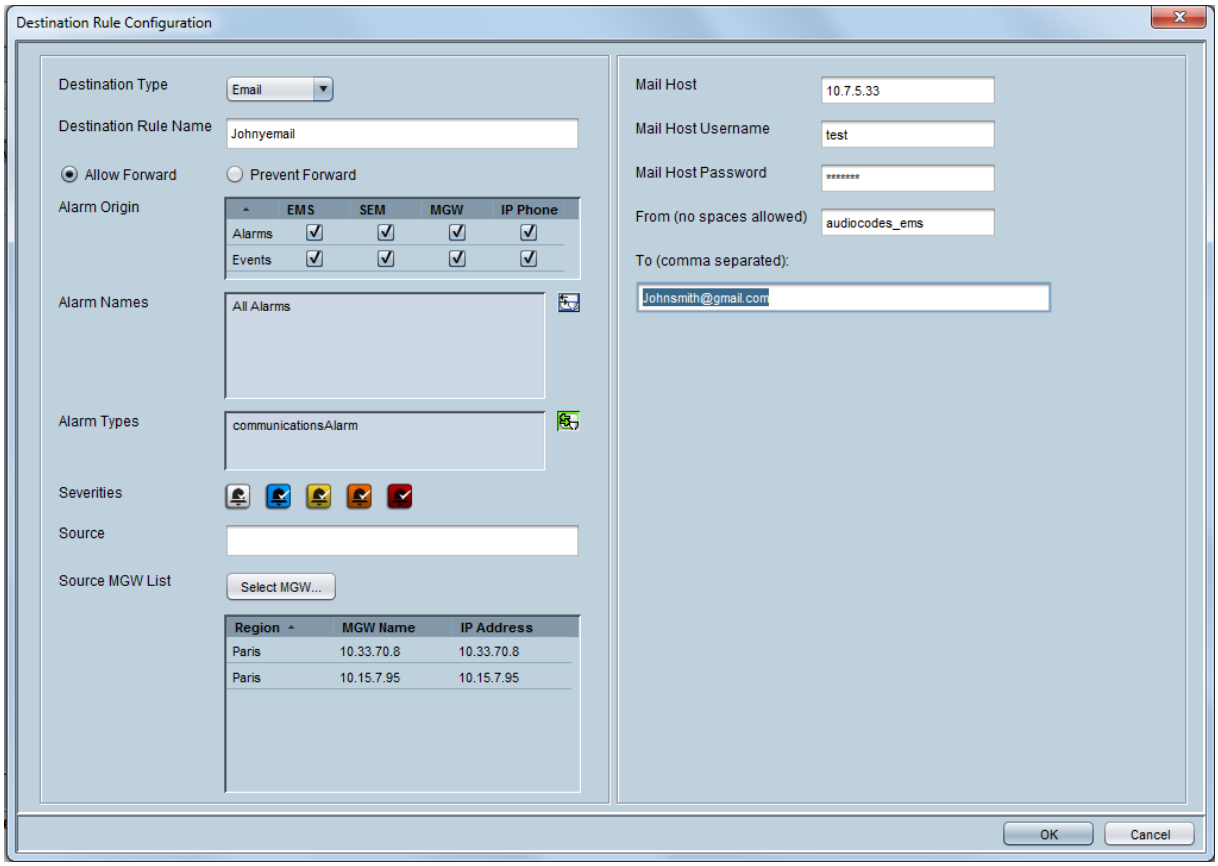
30.1 Trap Forwarding in Mail Format

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**.

Figure 30-1: Trap Forwarding-Email



4. In the left-hand pane, provision the following parameters for defining the destination rule:
   - 'Destination Rule Name' as you wish it to appear in the summary screen.
   - 'Allow Forward' or 'Prevent Forward': allow or prevent the forwarding of specific alarms according to the filtering criteria specified in the 'Destination Rule' Configuration window. When you select the 'Prevent Forward' or 'Allow Forward' buttons, and then specify additional filter criteria (as described in this step), then alarms are forwarded according to the specified filter criteria. For example, when you select 'Prevent Forward', and then select the 'Minor Alarms' severity icon, then minor alarms are not forwarded (according to the entities selected in the 'Alarm Origin' table). Alternatively, when you select

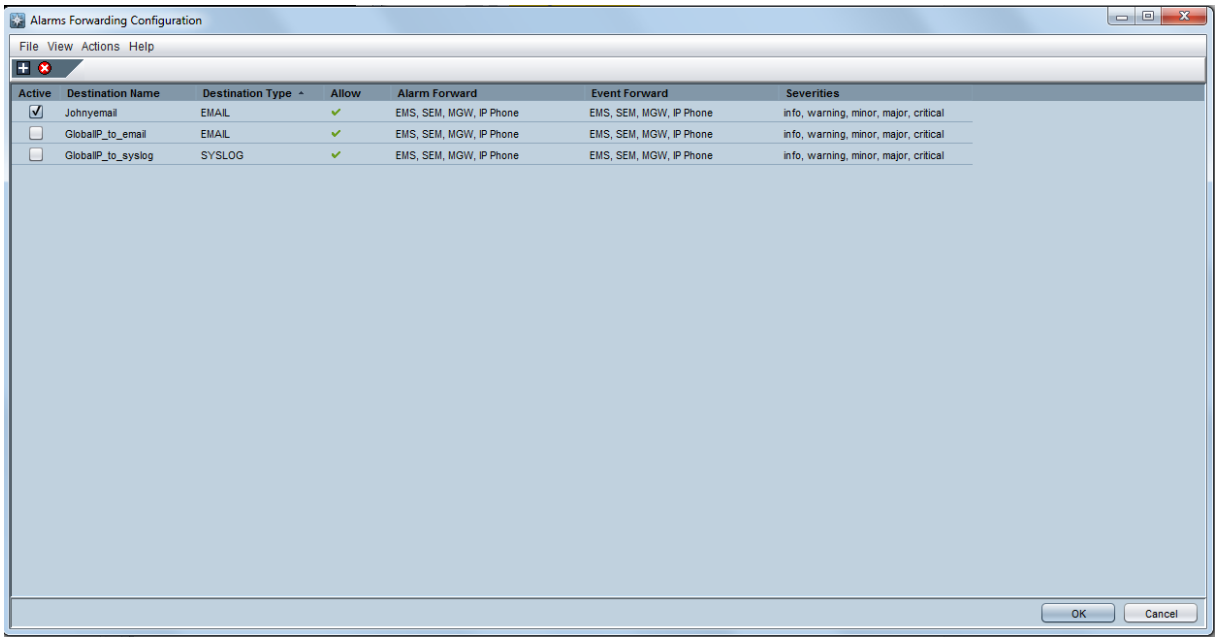
'Prevent Forward', and then in the 'Source' field, you specify 'Board#1/EthernetLink#2', then whenever LAN port #2 is down, an Ethernet link alarm is not forwarded.

- Select the subset of alarms and events to forward from the following subset (by default, all the alarms and events are selected):
  - EMS Alarms
  - EMS Events
  - SEM Alarms
  - SEM Events
  - MGW Alarms
  - MGW Events
  - IP Phone Events
  - IP Phone Alarms
- Alarm Names: allows the user to forward alarms according to specific alarm names. For example, setting this filter to forward the 'Power Supply' alarm.
- Alarm Types: allows the user to forward alarms according to specific alarm types. For example, forwarding only 'communications-related' alarms.
- 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.
- Source: allows the user to forward alarms according to the alarm source as displayed in the Alarm Browser 'Source' field. For example, 'EMS server' or a specific device board number.

5. Source MGW List: Select the devices from which you wish to forward alarms and events. The selected devices are displayed in the dialog box below. 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' field, enter the **list of email addresses** (coma separated) to which you wish to send mail.
6. Click **OK**.

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

Figure 30-2: 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
```

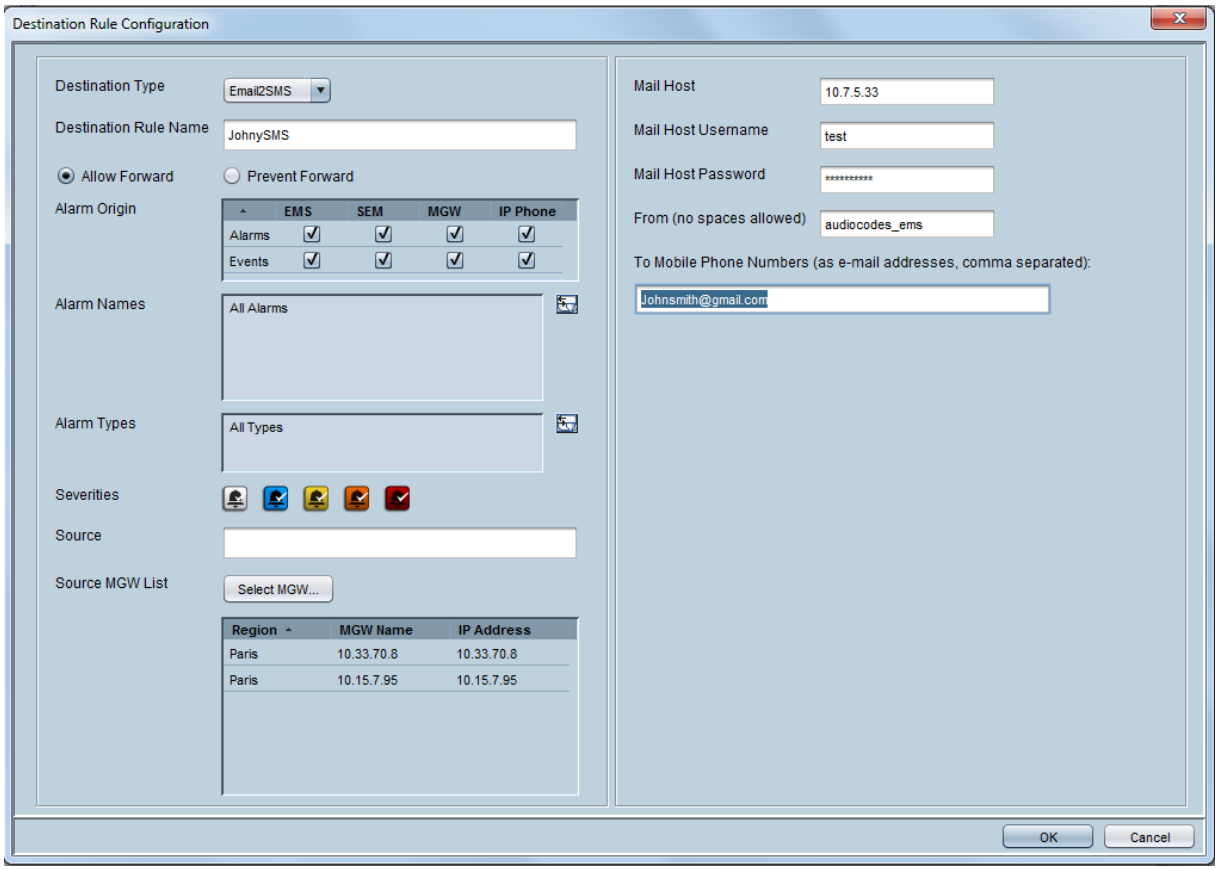
30.2 Trap Forwarding in Mail2SMS Format

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, configure the destination rule as described above in Section 30.1 on page 304.
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.

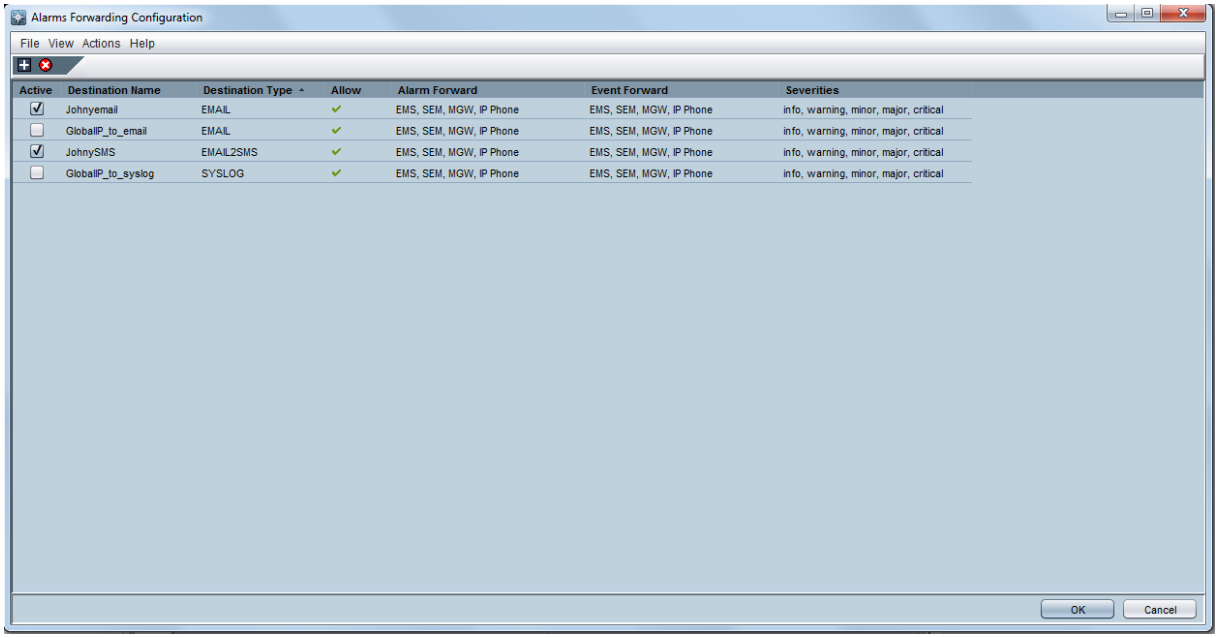
Figure 30-3: Trap Forwarding-SMS



6. Click **OK.**

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

Figure 30-4: Trap Forwarding Summary-Mail2SMS



Notes: CLEAR alarms for selected subset of the alarms are always forwarded.

- Select the devices from which you wish to forward alarms and events.

30.3 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:**

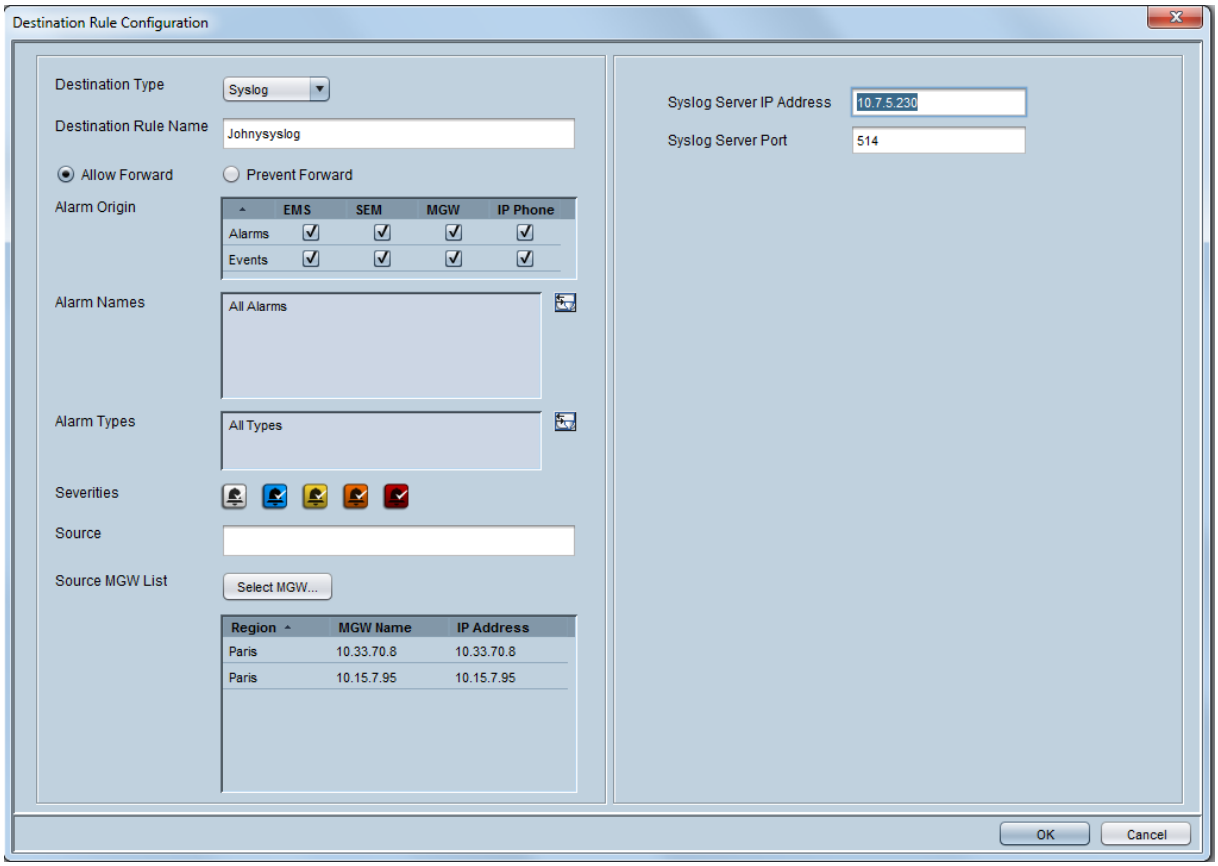
1. Open the **Faults** > **Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Syslog**.
4. In the left-hand pane, configure the destination rule as described above in Section 30.2 on page 304.

Note: CLEAR alarms for selected subset of the alarms are always forwarded.

Select the devices 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.

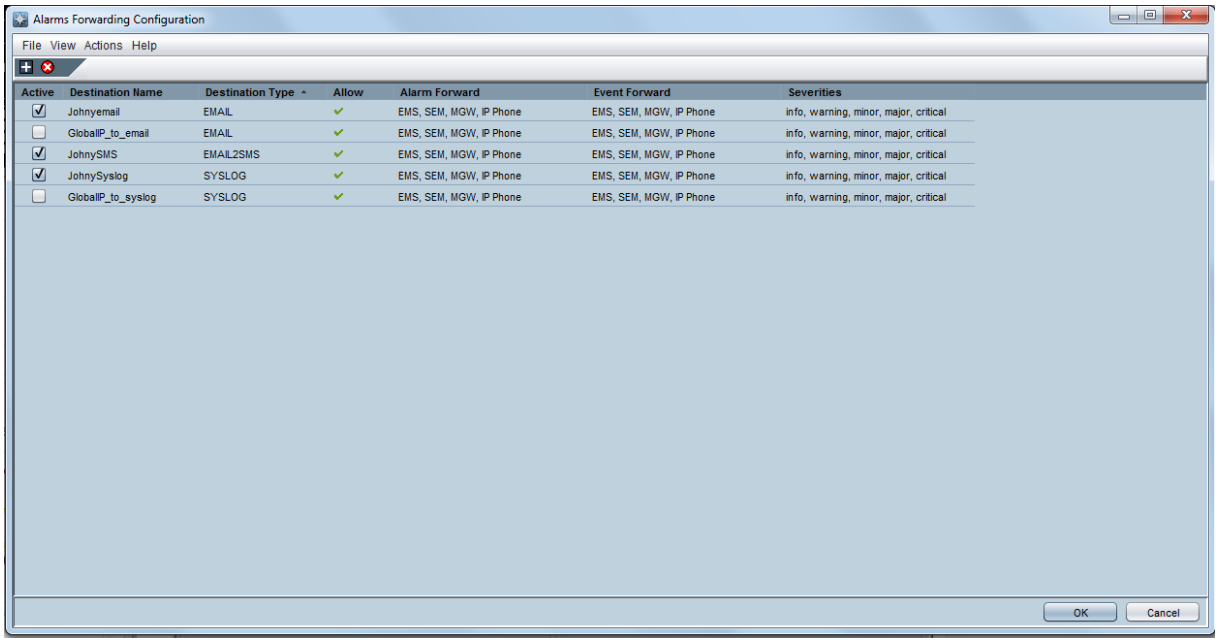
Figure 30-5: Trap Forwarding-Syslog



6. Click **OK.**

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

Figure 30-6: 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 30-1: 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>
```

In the event where the alarm is forwarded from the source global IP address in a HA configuration (see Section 24.3.3 on page 278) then the Node IP is the global IP address.

This page is intentionally left blank.

31 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.

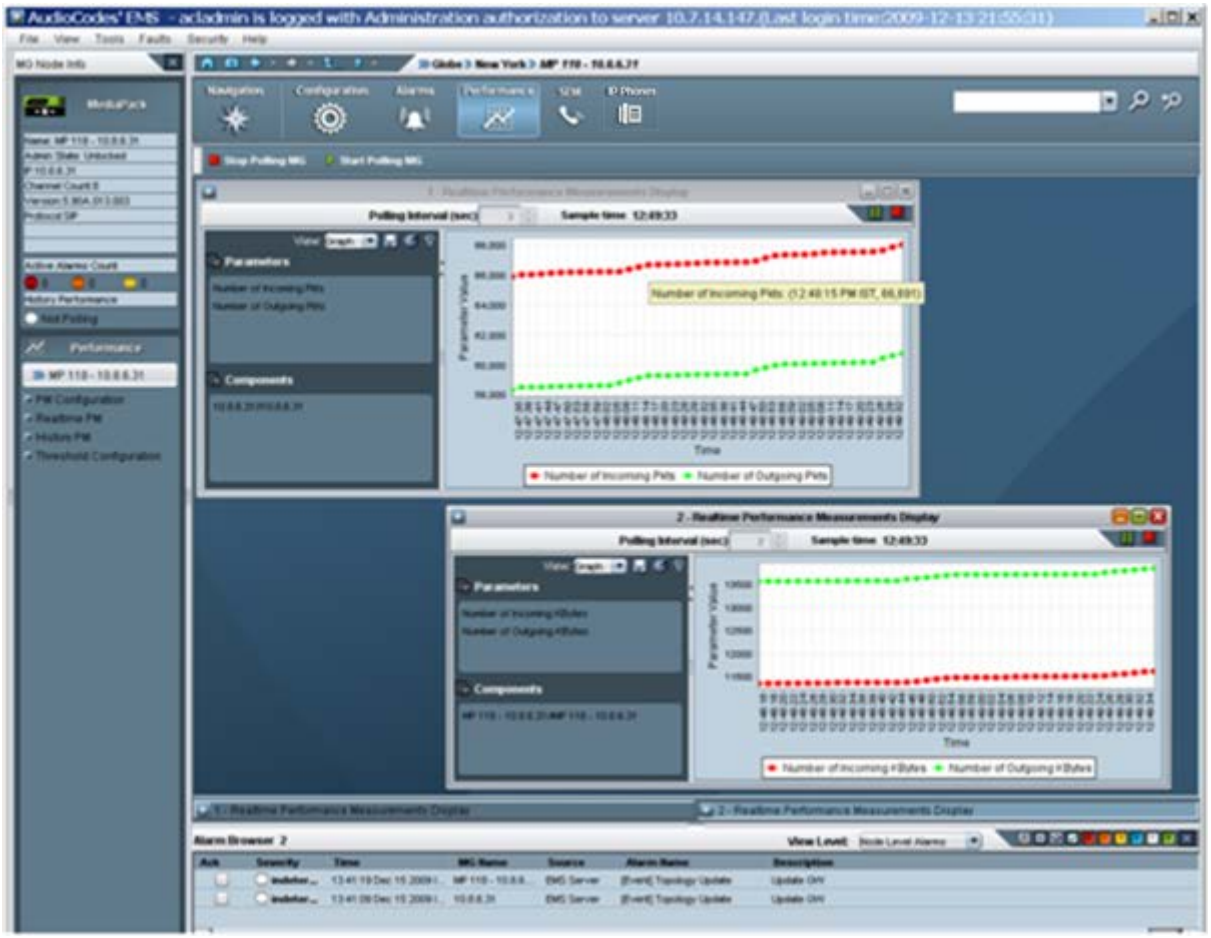
This page is intentionally left blank.

32 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.

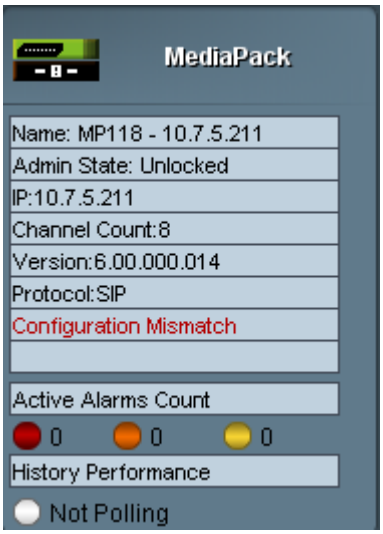
The EMS's Performance Management is composed of real-time and historical data monitoring. Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. Historical data can be used for long-term network analysis and planning. For the exact list of all the Performance Monitoring parameters supported for each one of the devices, refer to the relevant product *OAM Guide*.

Figure 32-1: 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 device / managed object.

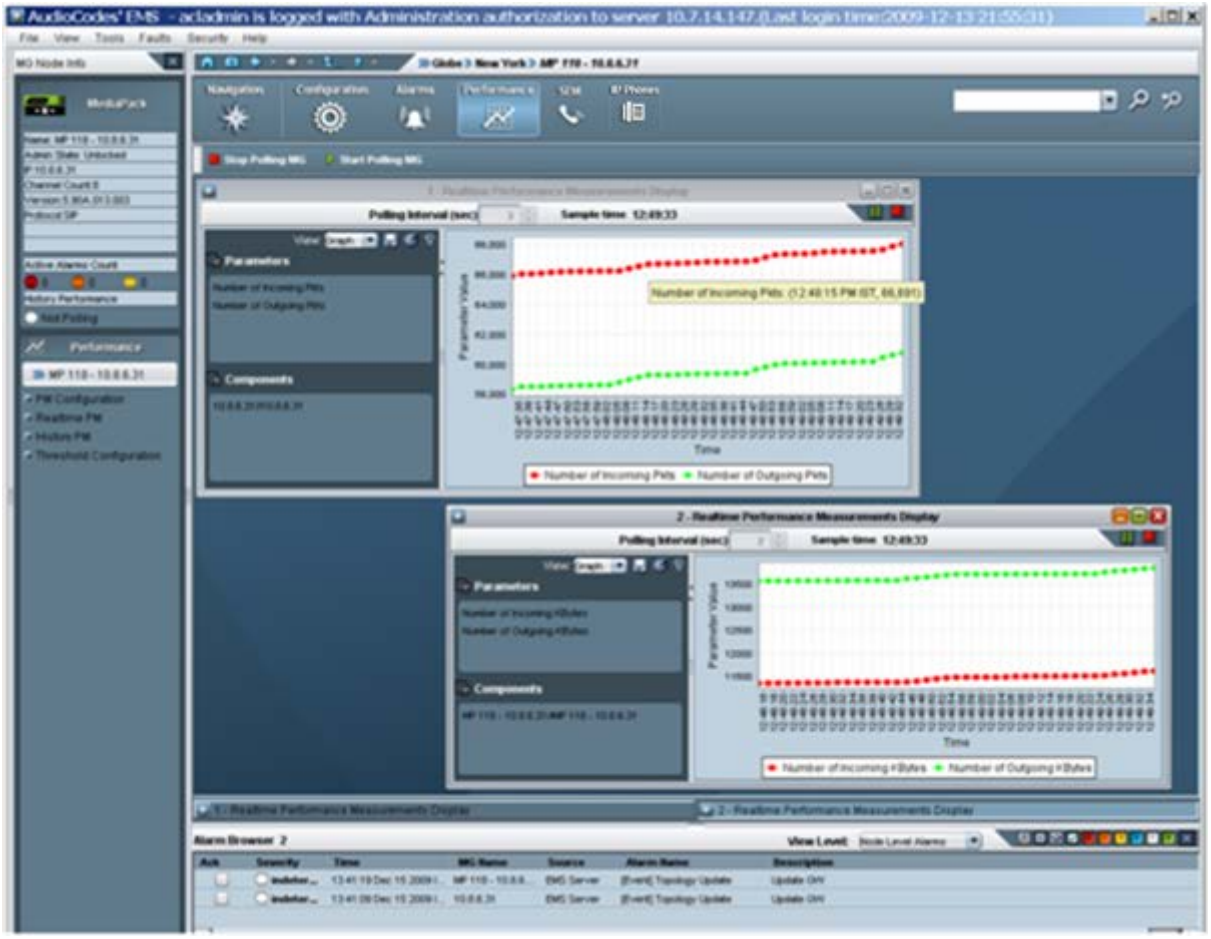
Figure 32-2: Performance Monitoring Icon in the Info Pane



32.1 Real-Time Performance Monitoring

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

Figure 32-3: Real-time PMs



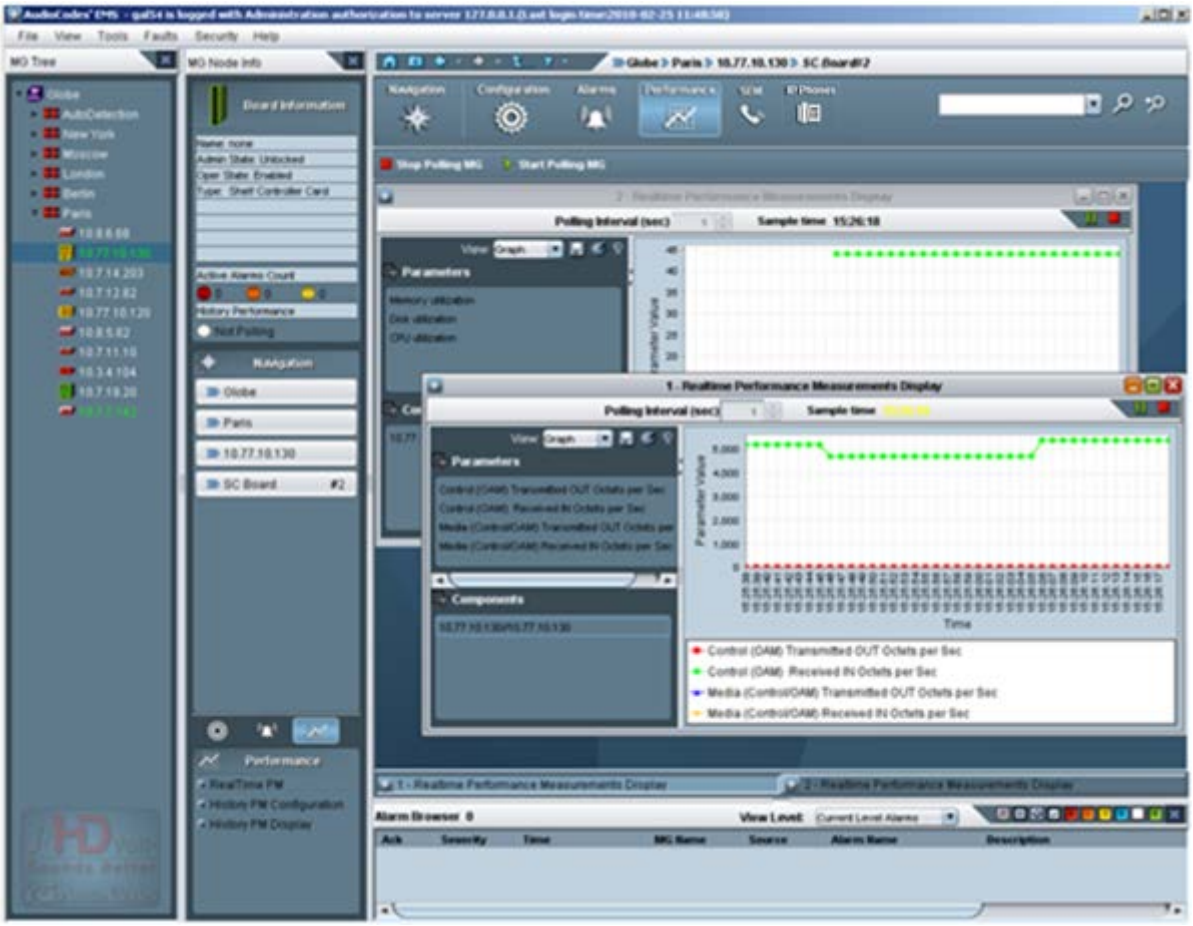
➢ **To select an entity to poll:**

1. Select the relevant device entity for which you wish to display Real Time PMs. For example, select the device 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.

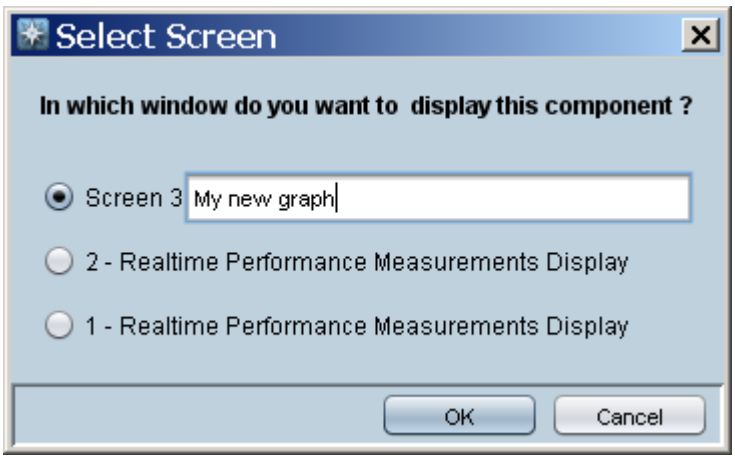
2. To define additional real-time performance monitoring windows, in the Performance pane, select **RealTime PM**.

Figure 32-4: 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 32-5: Selecting the Frame to Display the Graph of the Entity's Performance



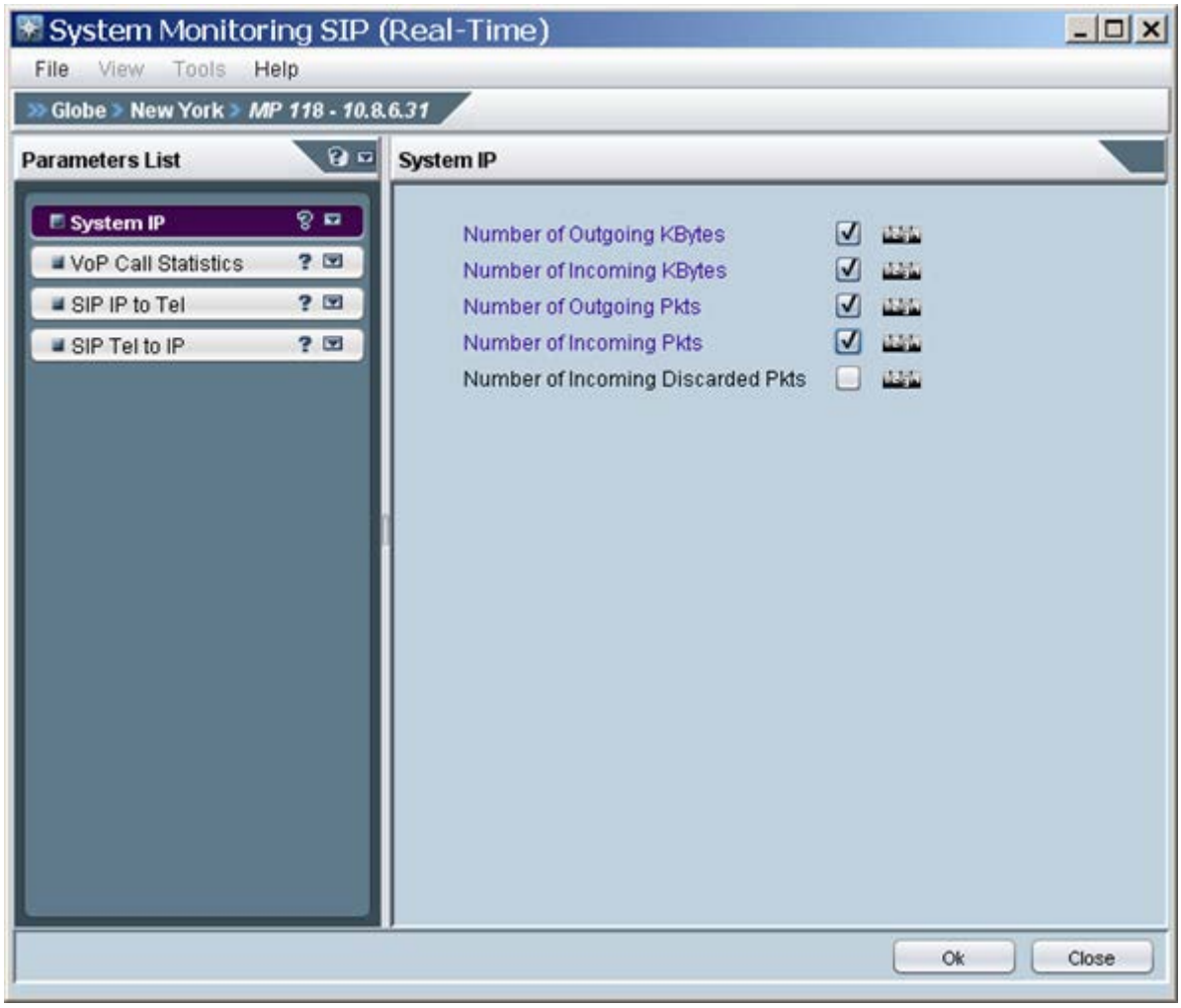
Users can open up to five separate real-time graphs in the same client application. There are two graph types that operators can use: Line Graph and Table View. In most cases, Line Graph is recommended when only a few parameters are compared. Table View is recommended when extensive data is displayed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

In each Line Graph, you can simultaneously view up to 10 parameters of the same entity (device, board and trunk) or compare the same parameters over different entities (different boards / trunks of the same or different devices). 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 .

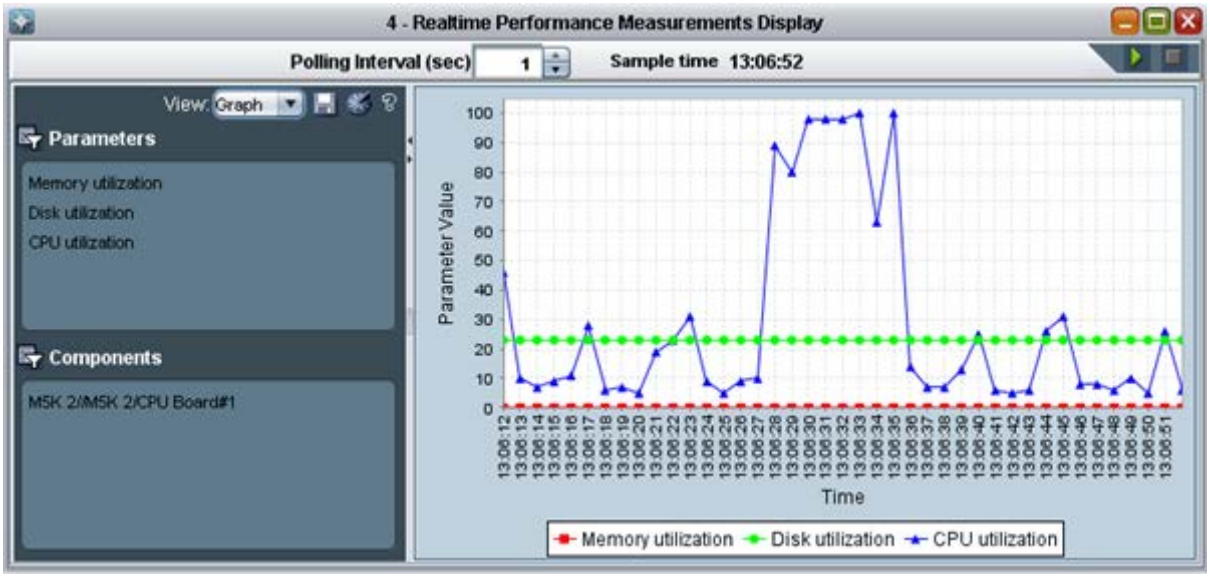
Figure 32-6: Parameter Type - Counters



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 32-7: Graph Comparing CPU, Disk and Memory Utilization of SC Boards in Devices



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.

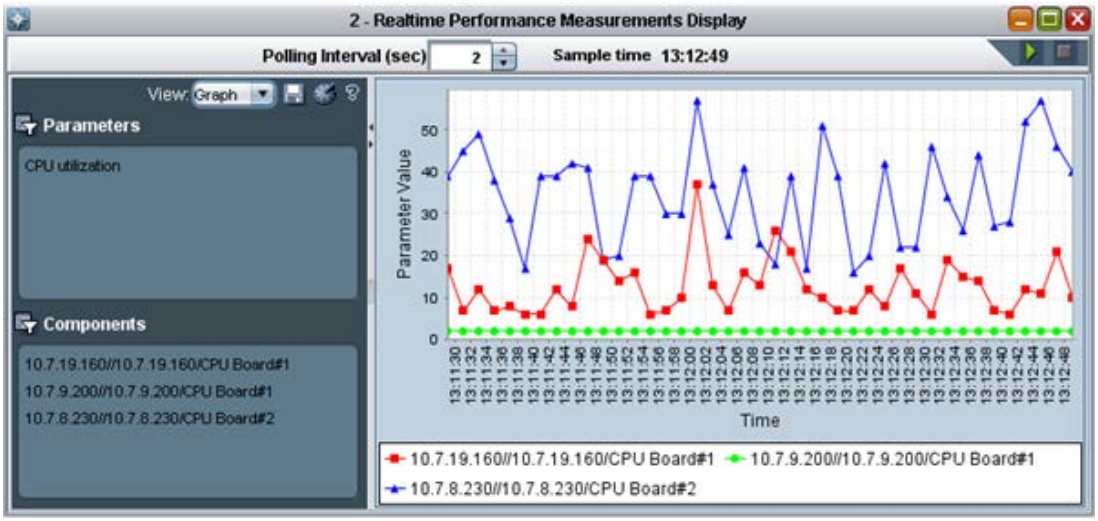
  At each stage, you can position your cursor over the nodes in the graph and view - in the tool tip - the precise information you require (the exact value of the parameter at the monitored point in time).

  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):

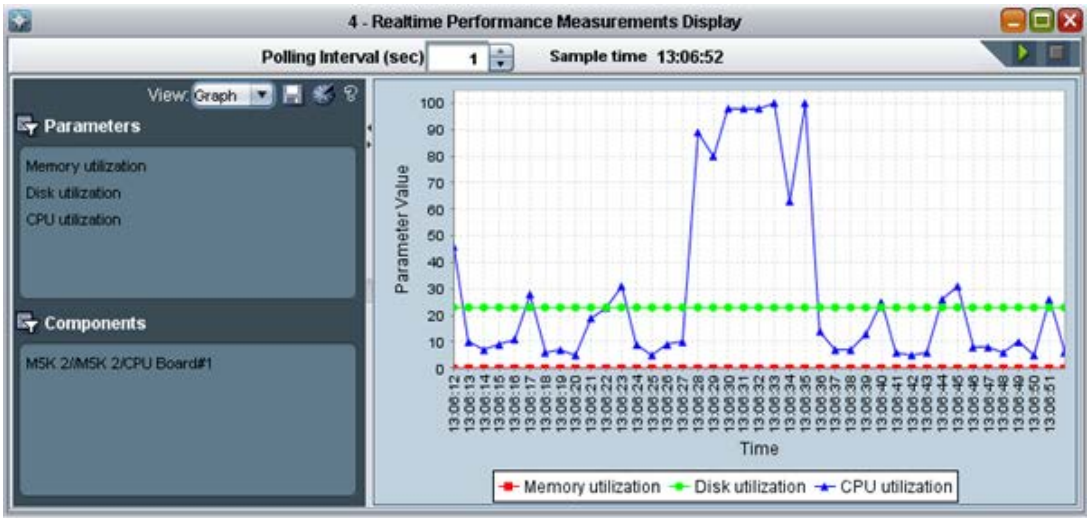
  - Compare CPU utilization of System Controller boards in the devices.

Figure 32-8: Graph Comparing CPU Utilization of SC Boards in Devices



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

Figure 32-9: View CPU, Memory and Disk Utilization of Mediant 5000 SC Board 1



32.2 Background (History) Performance Monitoring

There are two main functions of the history data monitoring: Configure the EMS to collect the data and to view the collected data. Both options are available by clicking PM icon below.

This section describes the following:

- Defining Performance Monitoring Profiles

Notes: Before collecting History Performance measurements, you must define a PM profile. For more information, see 'Configuring Background Monitoring' on page 323 below.

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

32.2.1 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 device board, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, click **History PM Configuration**.

   Note that each device and control protocol features a different set of available parameters. The figure below shows the device background monitoring provisioning parameters.

Figure 32-10: MG History PMs-Mediant 5000/Mediant 8000

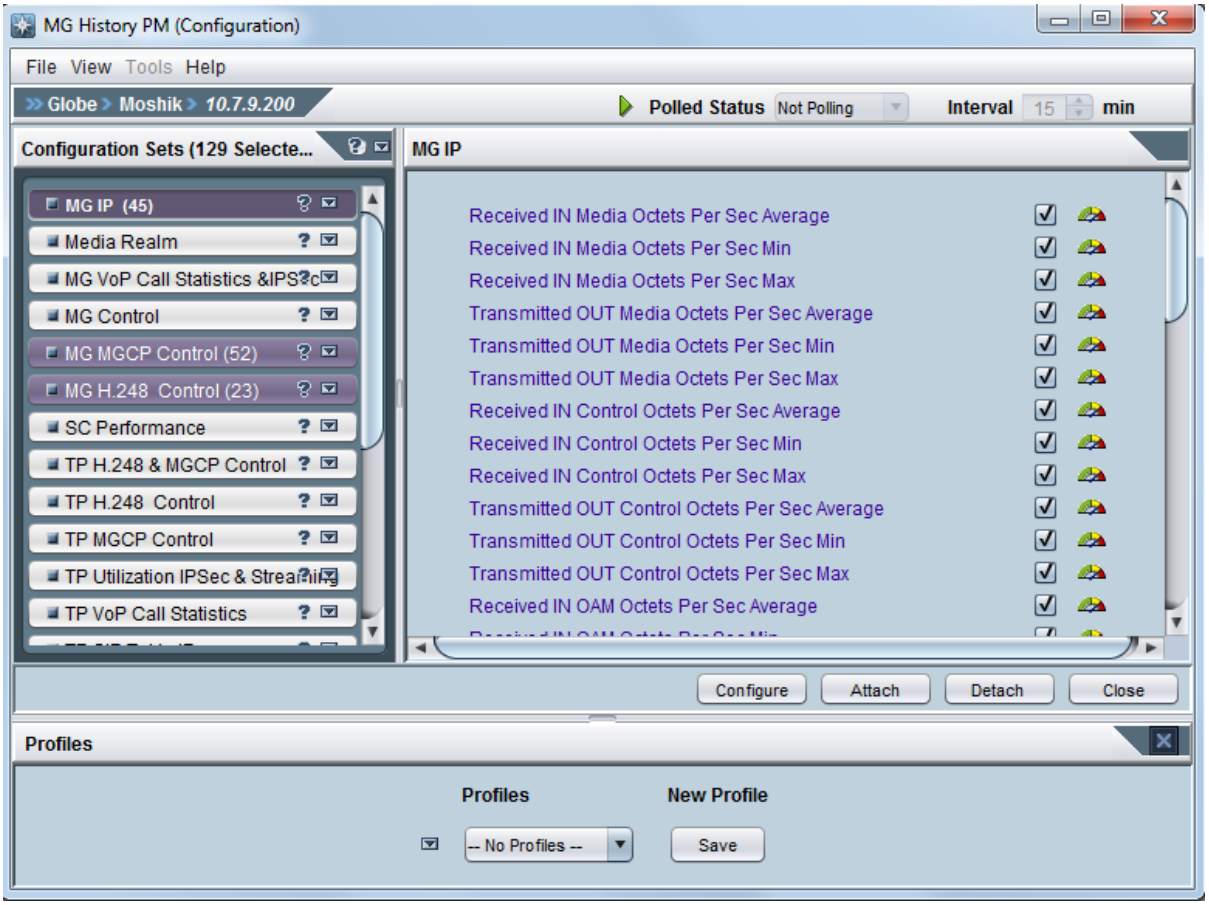
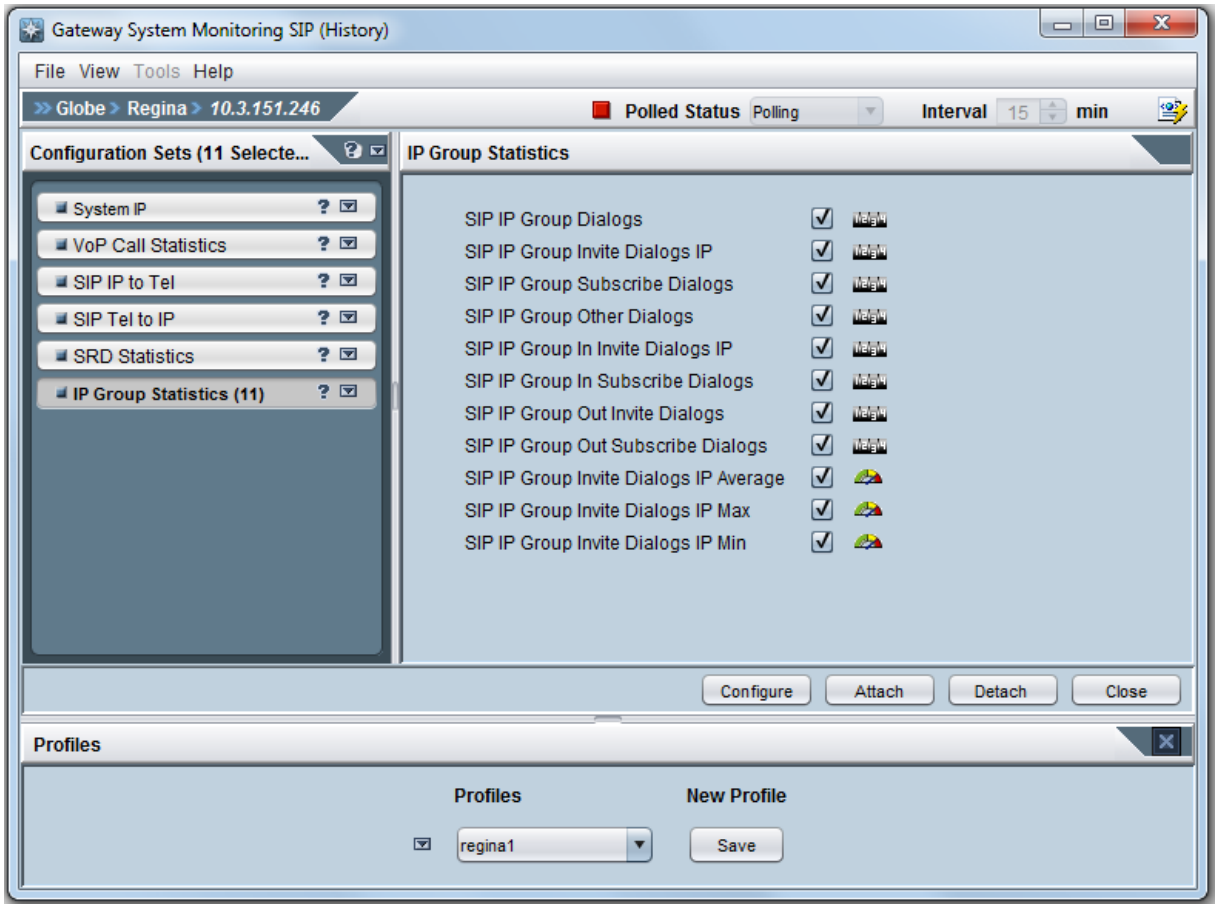


Figure 32-11: Gateway System Monitoring SIP (History)



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 device entities are polled. For example, trunk performance parameters are polled for all trunks of the selected device. Note too that the same background configuration screen opens from every device entity.
5. To change the polling interval or the PM profile, or to stop polling, click the **polling state** button.

32.2.2 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 and Mediant 8000, 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 device name in the EMS, the device'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:

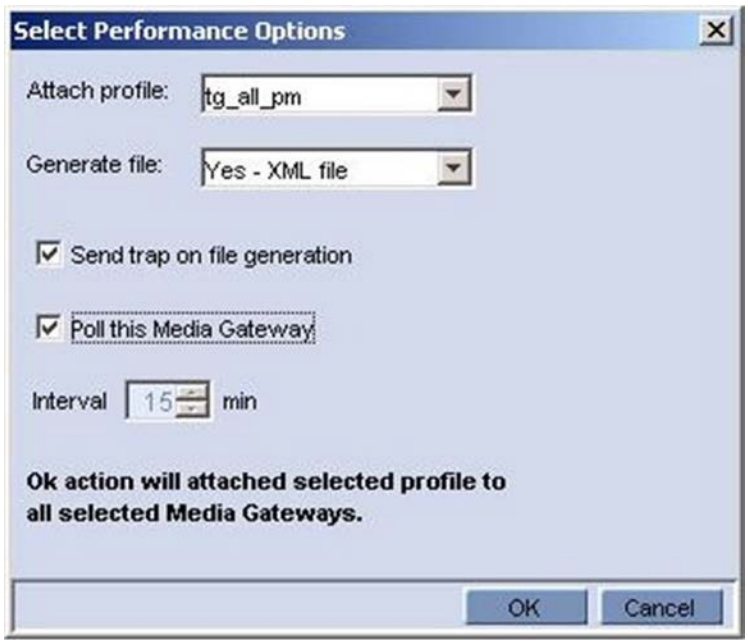
```
ACEMS/NBIF/pmFiles
```

Users should forward the trap to the NMS (Network Management System) (see Section 'Trap Forwarding to NB IF' on page 302).

➢ **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 32-12: Background Monitoring - Generate File Options



Notes: A performance data file cannot be created unless the device is polled (see section 'Configuring Background Monitoring' on page 323.

- 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 device).

An unknown value can be received from the device 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*.

32.2.3 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 device board, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, select **History PM Display**.
3. Continue (if required) to select entities to be added to the same screen. All entities must be of the same type (trunks, or System Controller boards, or devices 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.

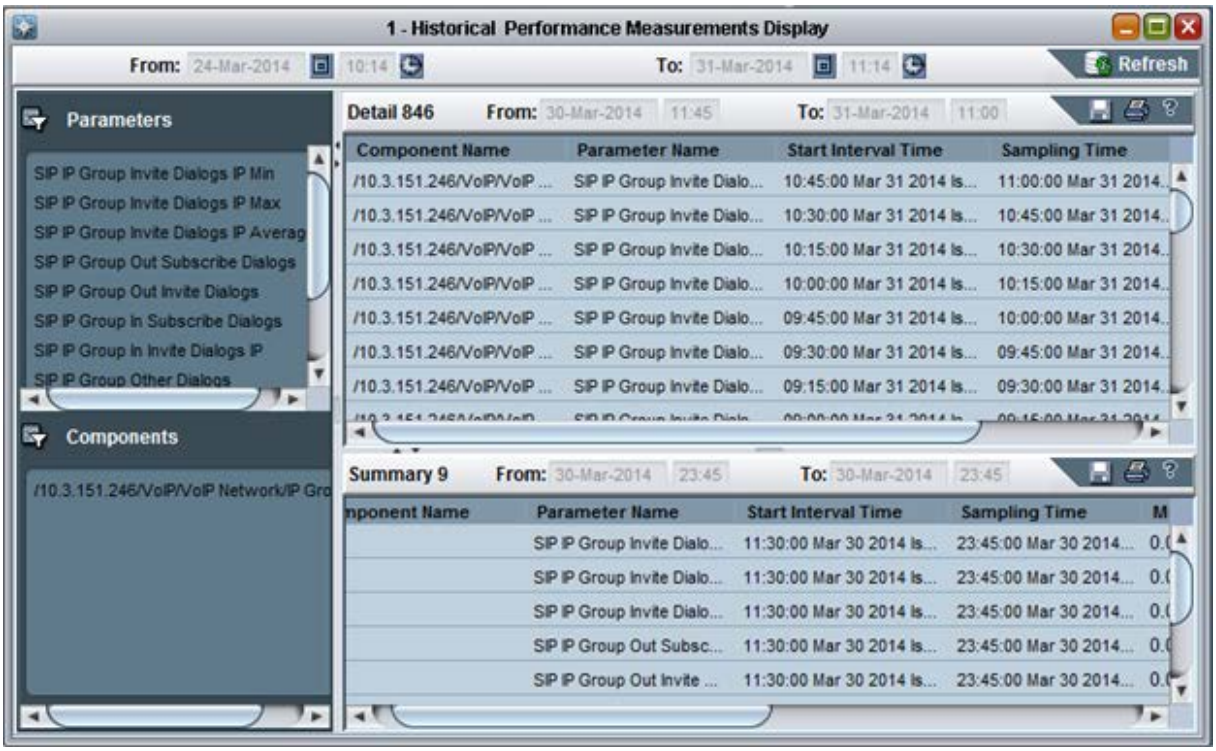
   Each time a sample is taken from the device, it is stored in the detailed table, where the entity name and index, parameter name, start, stop polling time and parameter value are specified.

   After every 24 hours of sampled data, the detailed table is summarized. For each entity and parameter, the following data is collected:

   - **Start Interval Time**-The time when the polling was started.
   - **Samling Time**-The time at the end of the sampling period
   - **Min Value**, **Avg Value** and **Max Value**-The minimum, average and maximum sampling values respectively collected during the sampling period
   - **Min Value Time** and **Max Value Time**-The respective times when the minimum value and the maximum values were recorded during the sampling period. For example, if the Start Interval Time was 14:15:00 and the Sampling Time was 14:30:00, the Min. Value Time occurred at 14:25:00 and the Max. Value Time occurred at 14:28:00.

   Detailed data is stored for a period of 7 days (in intervals of 15 minutes). Summary data is stored for 30 days (in intervals of 24 hours). Data storage time is dependent on available disk space.

Figure 32-13: 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.

32.2.4 Prinitng Historical Data PM Reports

Once you view the sample polled data, you can also print the displayed data by clicking the **Print** icon.

➢ To print historical data PM reports:

- In the Historical Performance Measurements Display, click the **Print** icon  ; the Print dialog is displayed.

  An example of the printed output is displayed below:

Figure 32-14: Historical Data PM Report

Component Name	Parameter Name	Start Interval Time	Sampling Time	Parameter Value
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	TransmittedOUTContro...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	Received IN Control Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0

32.3 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 drops 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.

32.3.1 Configuring Performance Monitoring Threshold Values for CPE Products

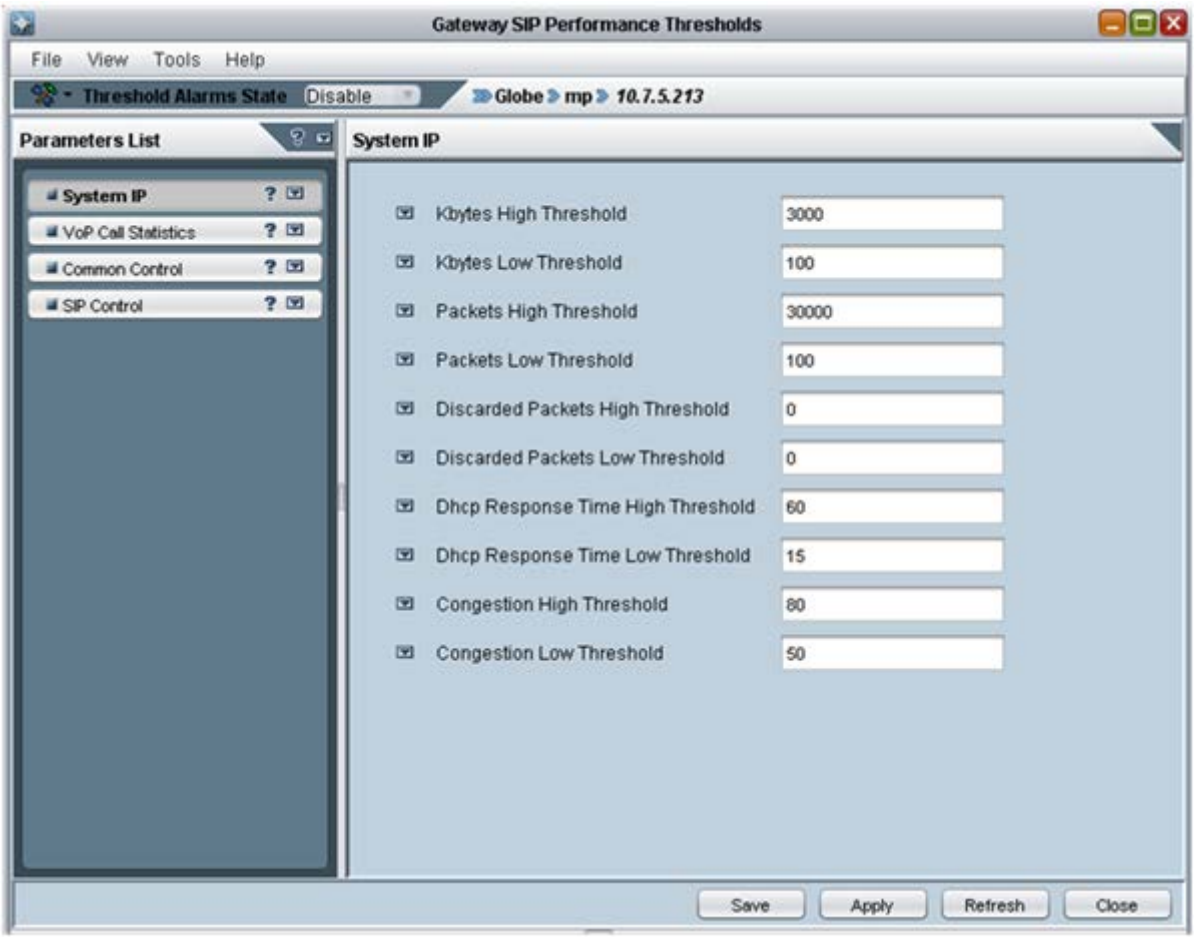
This section describes how to configure performance monitoring thresholds for CPE Products.

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

1. Select the device for which you wish to display Historical PMs, and then in the Desktop toolbar, click **Performance**.
2. In the Performance pane, click **Threshold Configuration**; the Gateway Performance Thresholds provisioning screen opens.

   The provisioning screen differs between device types and control protocols. The following screen displays an example of the MediaPack Performance Monitoring screen.

Figure 32-15: 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 device sends a Threshold Cross Alarm when a pre-defined threshold is crossed and a corresponding clear alarm when the measured value returns to normal.

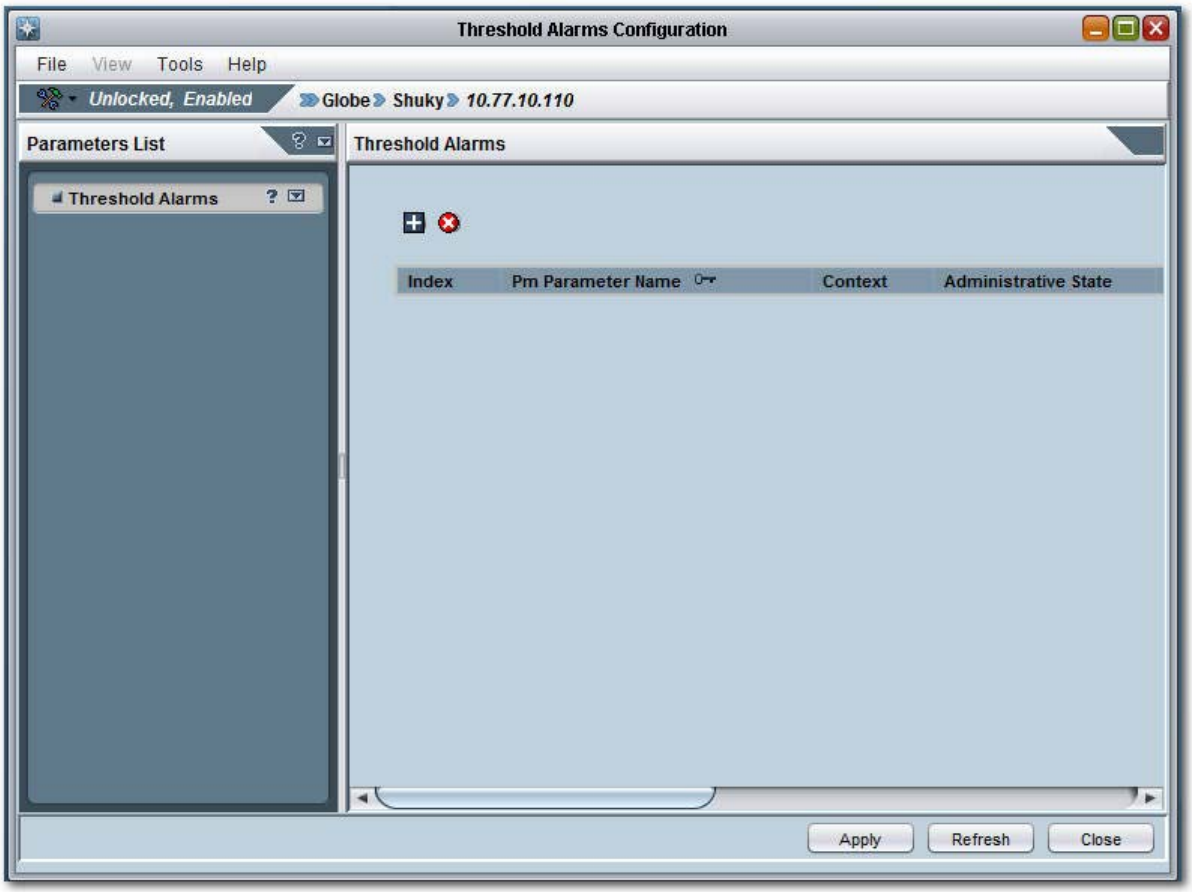
32.3.2 Configuring Performance Monitoring Threshold Values for Mediant 5000 and Mediant 8000

The feature is applicable for History PMs only, for both Counters and G auge PM types. Up to 100 entries can be configured in the PM thresholds table.

➢ **To provision the device 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 32-16: Threshold Alarms Configuration Frame



3. Click the  button to define a new threshold; the Threshold Alarm Parameters Frame is displayed.
4. Select one parameter at a time. Repeat this process as desired until the maximal threshold table size (100) is reached. For each parameter, in the Threshold Alarms Details pane, the user can define alarm severity, alarm customized text, and the low and high thresholds. For Board level parameters, it's possible to define threshold per board with different parameters.

Figure 32-17: Threshold Alarms Parameters-MG VoP Statistics and IPsec

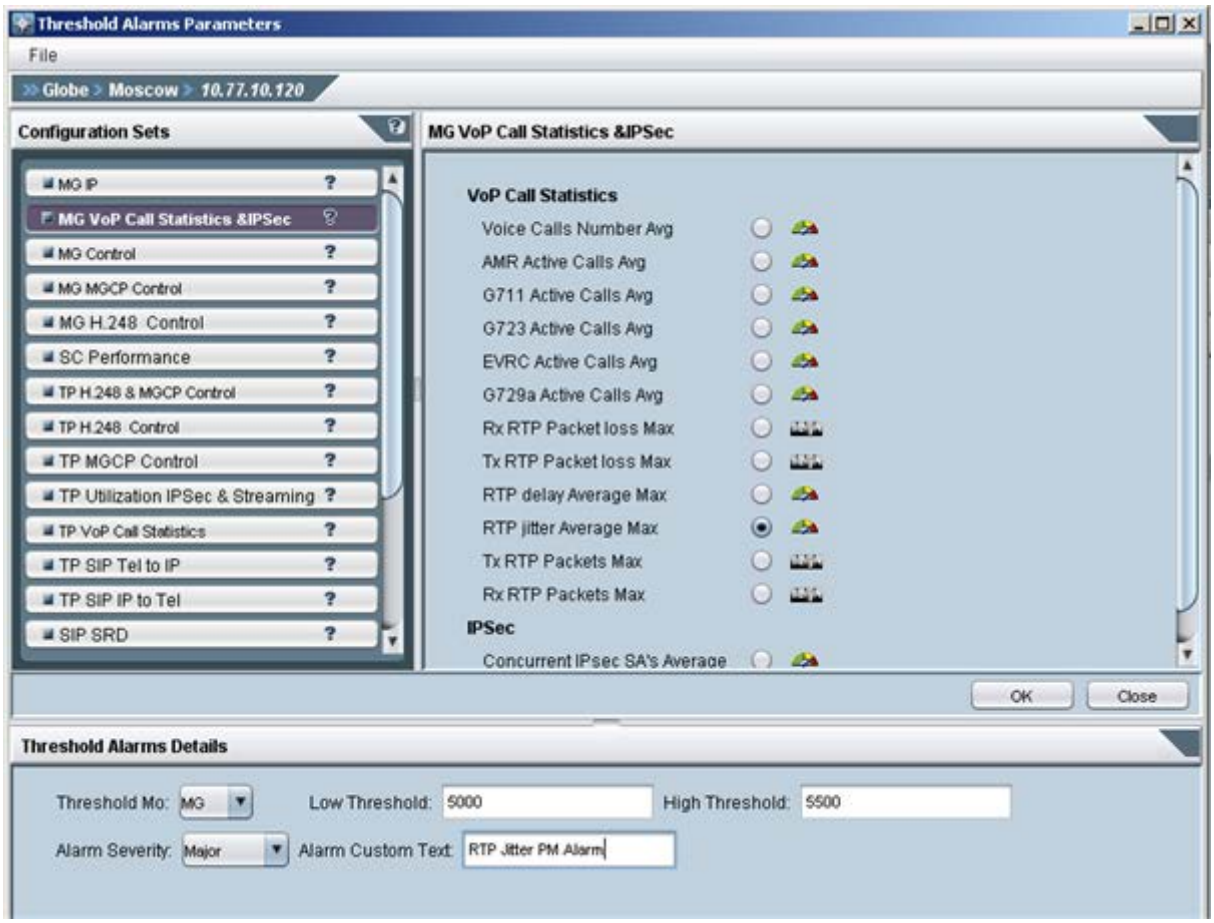
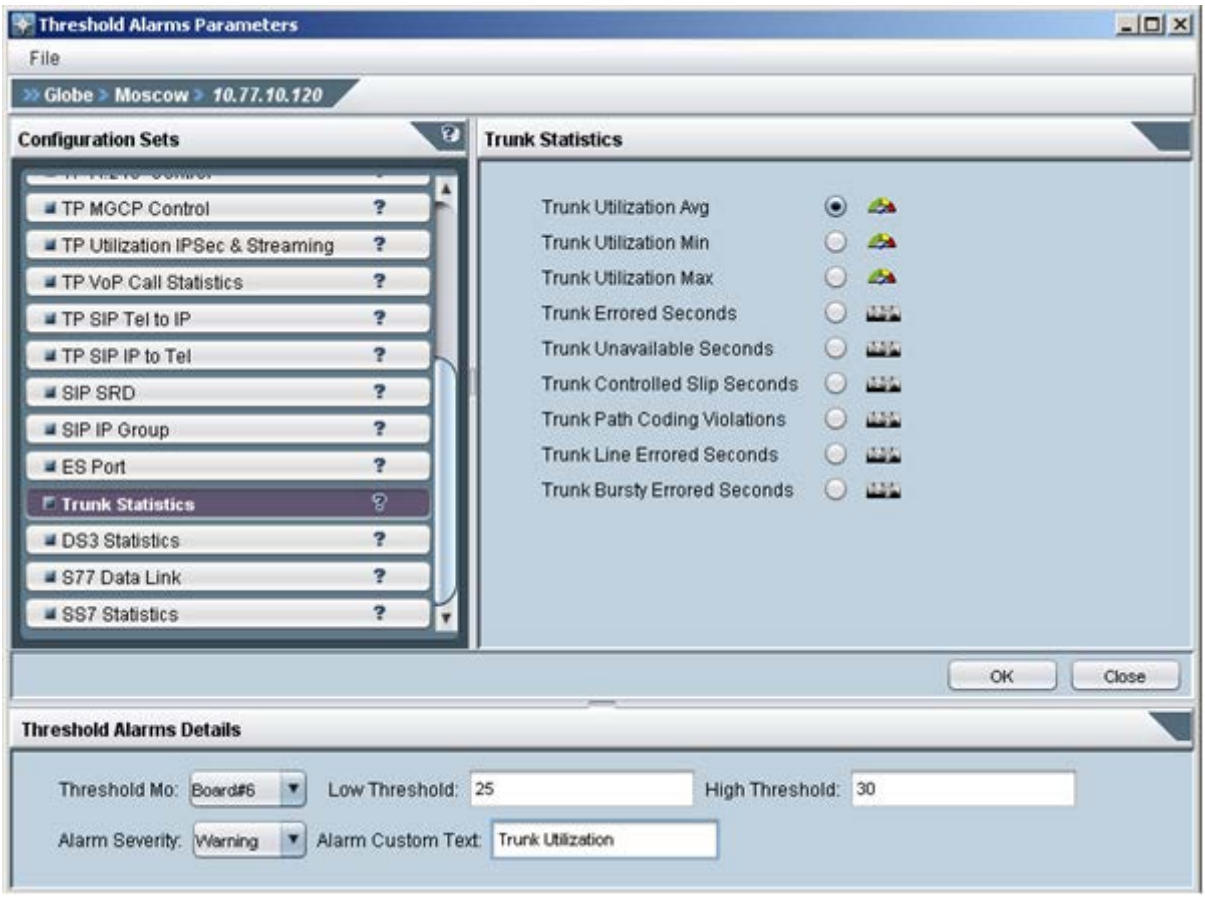
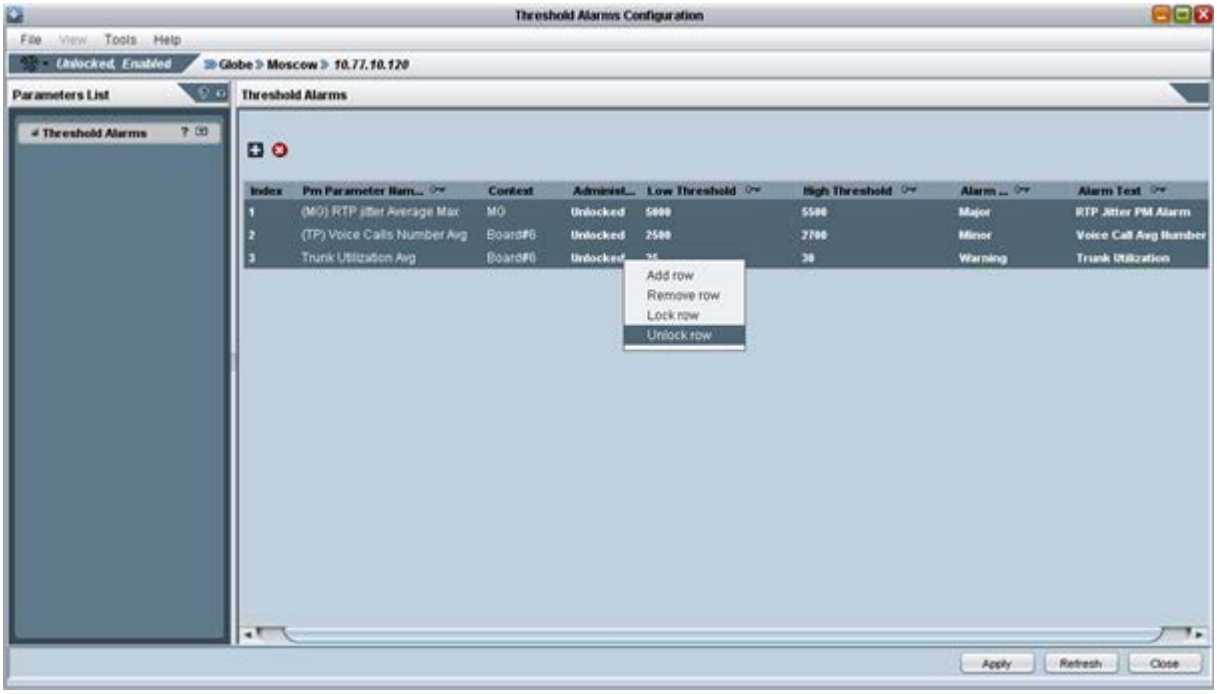


Figure 32-18: Threshold Alarms Parameters-Trunk Statistics



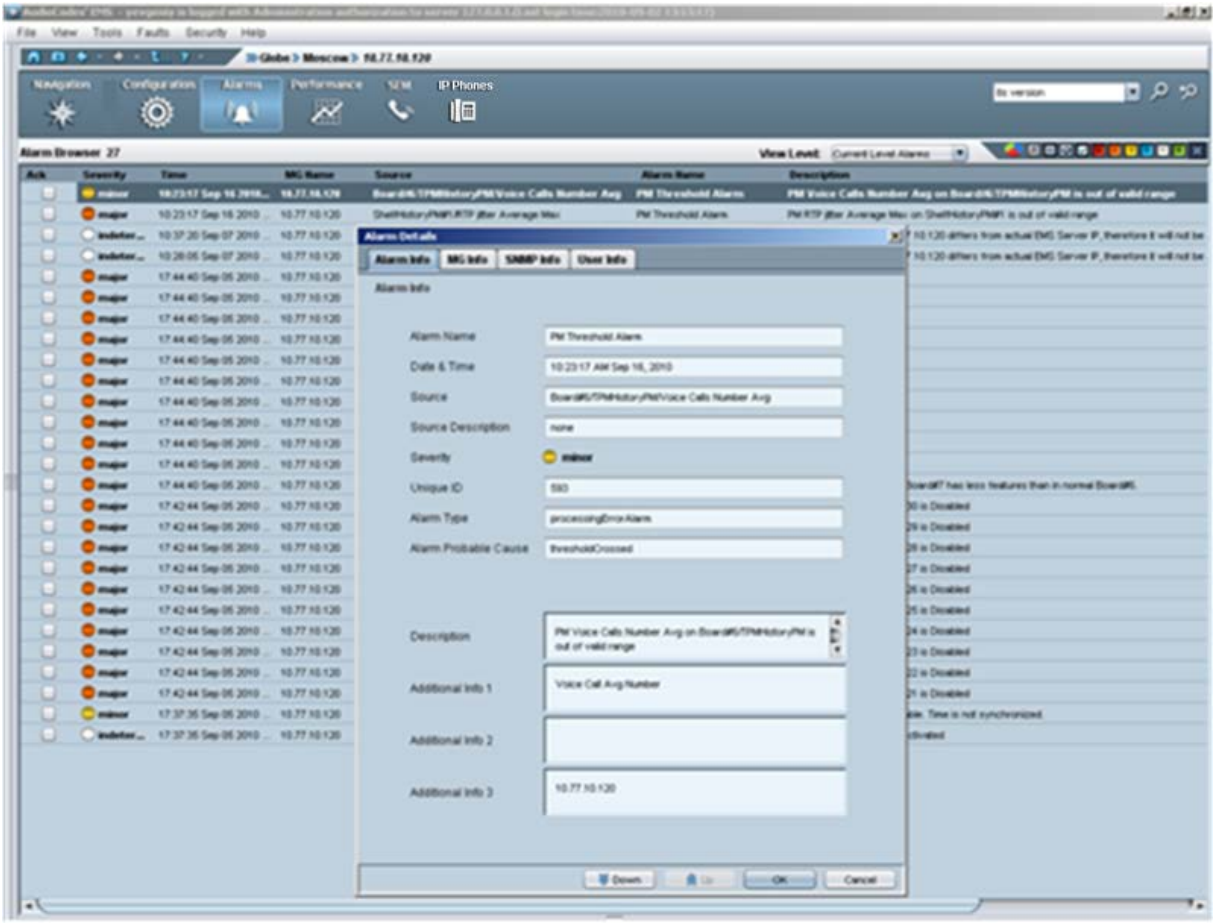
5. When all the required thresholds are defined, the user should perform **Unlock** to unlock all the rows in the Thresholds table. Once all the entries are Unlocked, the device starts to collect measurements.

Figure 32-19: Threshold Alarms Configuration



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

Figure 32-20: Threshold Alarm Details



32.4 Performance Monitoring Actions on Devices

This section describes performance monitoring actions on devices.

Figure 32-21: Performance Monitoring Actions on Devices

Users can perform the following actions on single or multiple devices:

- Attach or detach an MG profile.
- Start or stop MG polling.

Notes: For 'Display Real-Time and Historical PMs' and for 'Attach / Detach Profile', all the devices that you select must be of the same type, for example, either MediaPacks, or Mediant 2000, or Mediant 5000.

This page is intentionally left blank.

Part V

Security Management

This section describes the security features implemented on the EMS.

33 Overview

This section describes the following EMS Security Management features:

- Network Communication Security (see Chapter 34).
- EMS Application Security (see Chapter 35).
- Local EMS Users Authentication and Authorization (see Chapter 35.3).
- Centralized EMS Users Authentication and Authorization via RADIUS, TACACS+ and LDAP servers (see Chapter 35).
- EMS User Activities Journal (see Chapter 36).
- EMS server machine (refer to the *EMS Server IO&M Manual*).
- 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.

34 Network Communication Security

Network communication between the EMS and it's managed components is performed using SNMP and HTTP protocols. This is implemented as follows:

- SNMP: SNMP (SNMPv2c and SNMPv3) is used for the following:
  - Provisioning (for devices running firmware version 7.0 or below).
  - Maintenance actions and fault and performance management.
- HTTP: HTTP/S is used for the following:
  - Installing and upgrading software
  - Downloading auxiliary files
  - Connecting to the device's embedded Web interface, the SEM and IP Phone Manager interfaces and JAWS and NBIF clients.
  - For REST communication between the EMS and devices and endpoints.

34.1 SNMP Management

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

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.

34.1.1 Configuring SNMP

This section describes how to configure the SNMP connection with the device.

34.1.1.1 Configuring SNMPv3

This section describes how to configure SNMPv3.

➢ **To configure the device connection with an SNMPv3 user:**

1. Right-click the device 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.

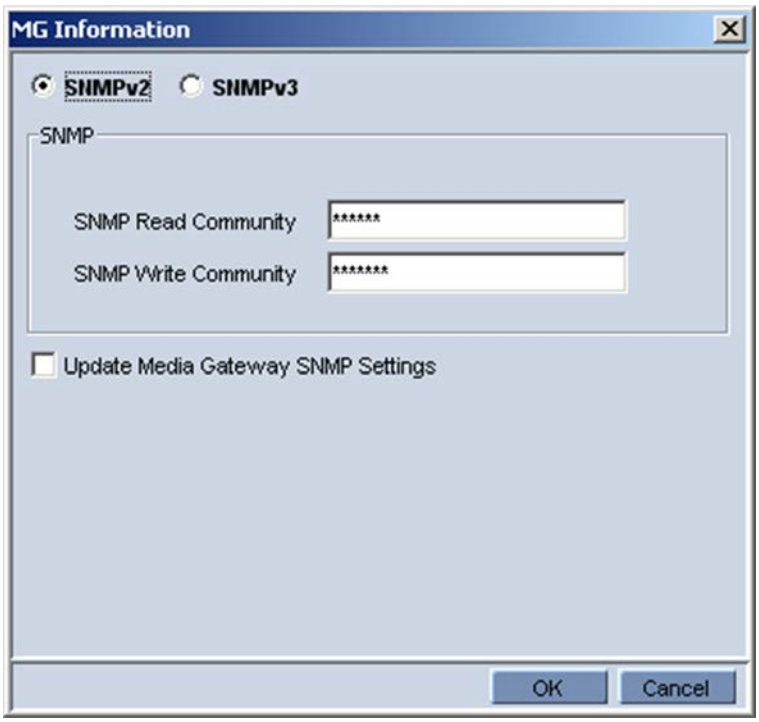
➢ To switch MG & EMS communication from one SNMP version to another via EMS:

1. In the Region Status screen, select one or more CPEs (multiple selections are relevant when all the devices 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 device. 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 device using the SNMPv2 user privileges. SNMPv3 user privileges are used the next time you connect to the device. Sometimes this operation might take up to three minutes.

Figure 34-1: MG Information-New SNMPv3 User



34.1.1.2 Modifying SNMPv2 Community Strings or SNMPv3 Passwords

This section describes how to modify SNMPv2 Community Strings or SNMPv3 passwords.

➢ **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 devices 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 Media Gateway SNMP Settings' check box.

34.1.2 Configuring Additional SNMPv3 Users

You can configure additional SNMPv3 users with different security permissions or for sending traps to another SNMP Trsp Manager such as an NMS.

For managing devices running firmware versions 7.0 or later, you must use the device's Web server to configure additional SNMP users. In the device's Web server, configure the following:

- In the SNMPv3 Users table, add the new SNMPv3 user (ensure that "SNMPUsers_Group" is set to **Trap**).
- In the SNMP Trap Destinations table, assign the new trap user to the EMS server entry or add a new entry for an additional SNMP trap manager and assign the new user to this trap manager.

For more information, refer to the relevant device's *SIP User's Manual.*

34.1.2.1 User Cloning

According to the SNMPv3 standard, SNMPv3 users on t he SNMP agent (on the device) cannot be directly added via the SNMP protocol e.g. SNMP Manager (EMS). Instead new users must be added via User Cloning. The SNMP Manager then creates a new user based on the original SNMPv3 user permission levels.

Note: The procedure below is only relevant for managed devices running firmware prior to version 7.0.

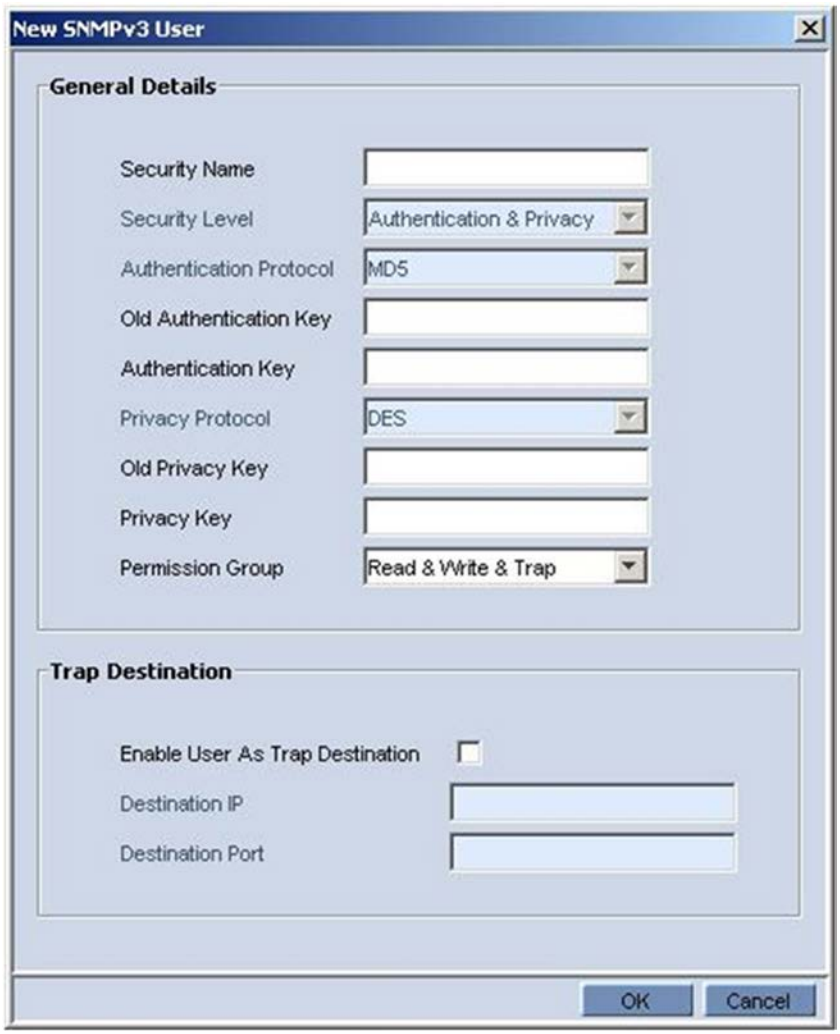
➢ **To clone SNMPv3 users:**

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 defined destination, check the **Enable User as Trap Destination** option to provision Trap a destination IP and Port. The 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 34-2: MG Information Screen-New SNMPv3 User



34.2 Configuring HTTPS

Note the following when configuring HTTPS connections:

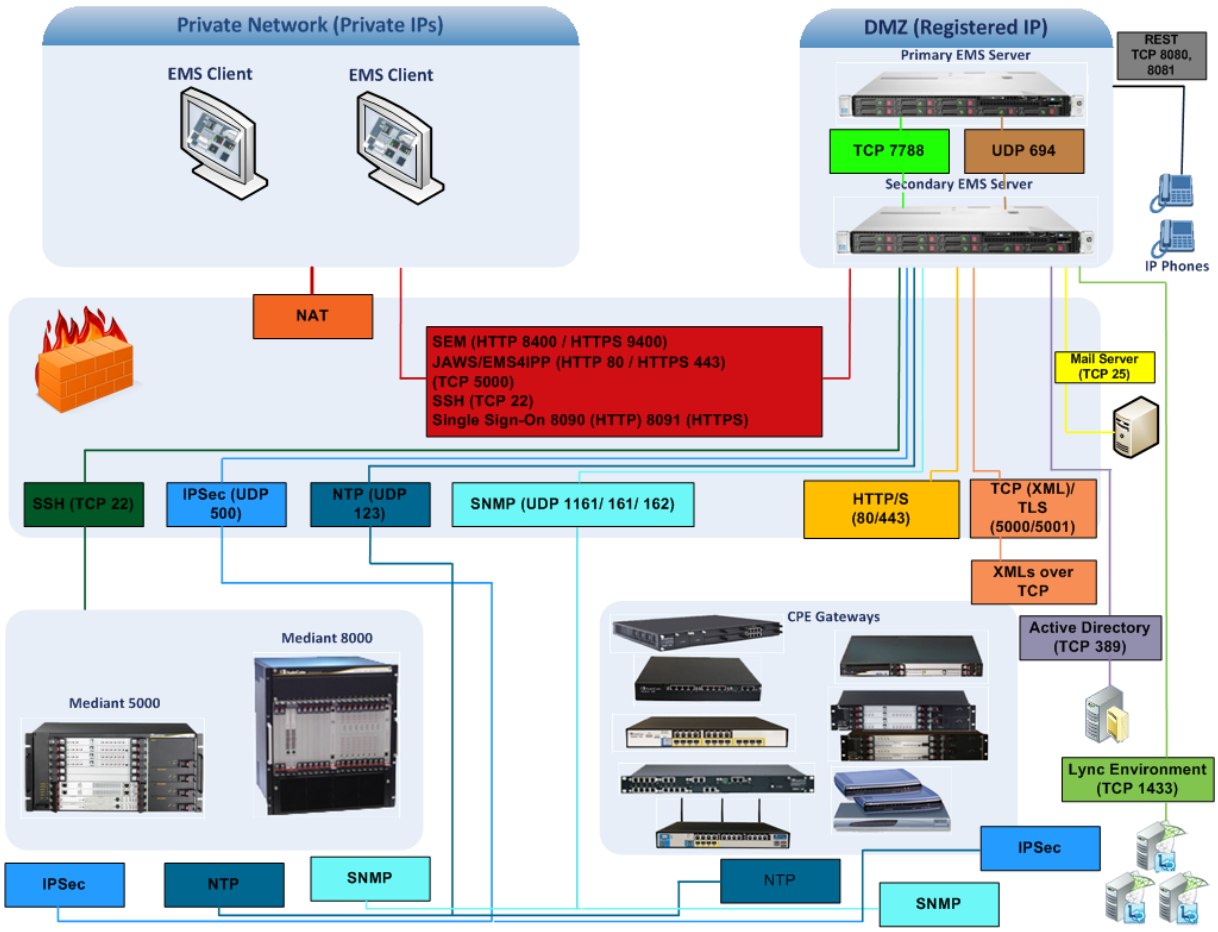
- If you wish to secure the connection between the EMS and the device over HTTPS, then when you add the device to the EMS, you must enable HTTPS ("Enable HTTPS Connection") (see Section 5.3.3 on page 82). In addition, you must also configure HTTPS on the device side (refer to the *EMS Server IOM manual*).
- When you wish to open the SEM, IP Phone Manager BIF or JAWS interfaces over an HTTPS connection, refer to the *EMS Server IOM.*

34.3 Firewall Settings

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-device 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 devices (see the figure below).

Figure 34-3: EMS Firewall Configuration Schema



Note: For detailed information on EMS firewall settings, refer to the *EMS Server IOM* manual.

34.4 Mediant 5000 and Mediant 8000 Security Management

EMS <-> device 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-device secure communication:

1. Right-click the device 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:

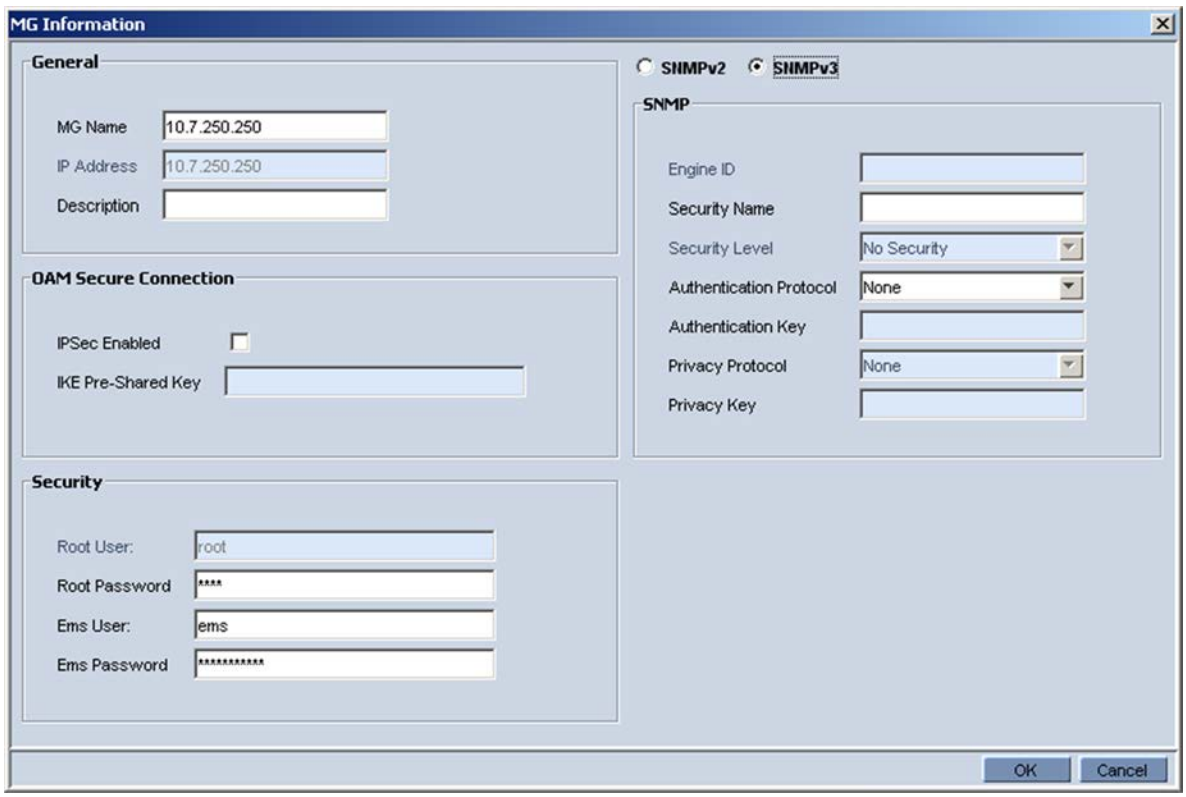
   - It is recommended to select the **IPSec Enabled** checkbox and enter the 'Pre-shared Key' string. This configuration can be performed either during the device definition stage or later. The Pre-shared Key string defined in the EMS and in the device must be identical.

   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 device definition stage or later. The Pre-shared Key string defined in the EMS and in the device 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 34-4: MG Information - Secured Connection Enabled



This page is intentionally left blank.

35 EMS Application Security

EMS Operator's Authentication and Authorization can be performed using either local EMS users management tools, or by using a centralized database. These options are described as follows:

- Local User Management:

  By default, the EMS application manages its users in the local EMS server where the EMS user and password are saved in the EMS database (see Section 35.3 on page 357).

- Centralized User Management via an external database:

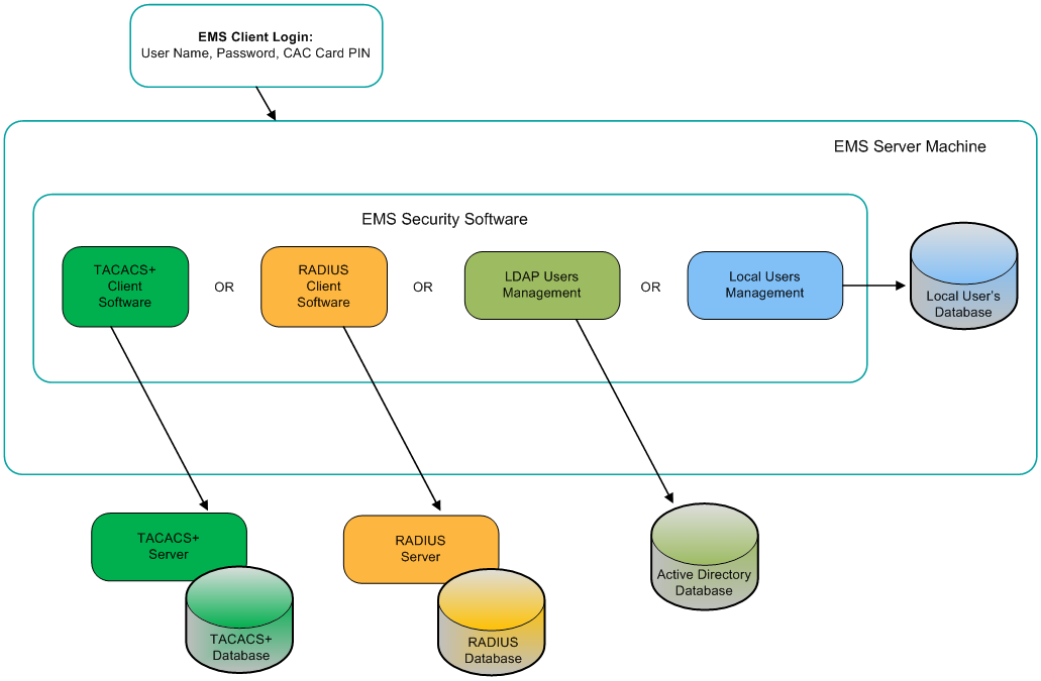
  When you choose these options, usernames, passwords and access level attributes are stored externally on these platforms. In this case, the EMS server doesn't store the username and password (these users are not displayed in the EMS users list) and instead forwards them to the pre-configured external user database.

  The following external user databases are supported:

  - Remote Authentication Dial-In User Service (RADIUS) (see Section 35.2.1 on page 353).
  - Terminal Access Controller Access-Control System Plus (TACACS+) (see Section 35.2.2 on page 355).
  - Lightweight Directory Access Protocol (LDAP) server (see Section 35.2.3 on page 356).

The figure below shows the different user management options.

Figure 35-1: Centralized User Management



Users can identify themselves with a Login user name and Password or by using Common Access Card (CAC) card (see below).

35.1 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.

35.2 Centralized EMS Users Authentication and Authorization

Customers may select an option for EMS Application Users Authentication and Authorization using centralized Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) servers. For detailed information in reference to RADIUS or TACACS+ servers provisioning in the EMS, refer to Section 'Security' in the *EMS OAM Integration Guide*.

35.2.1 RADIUS Server

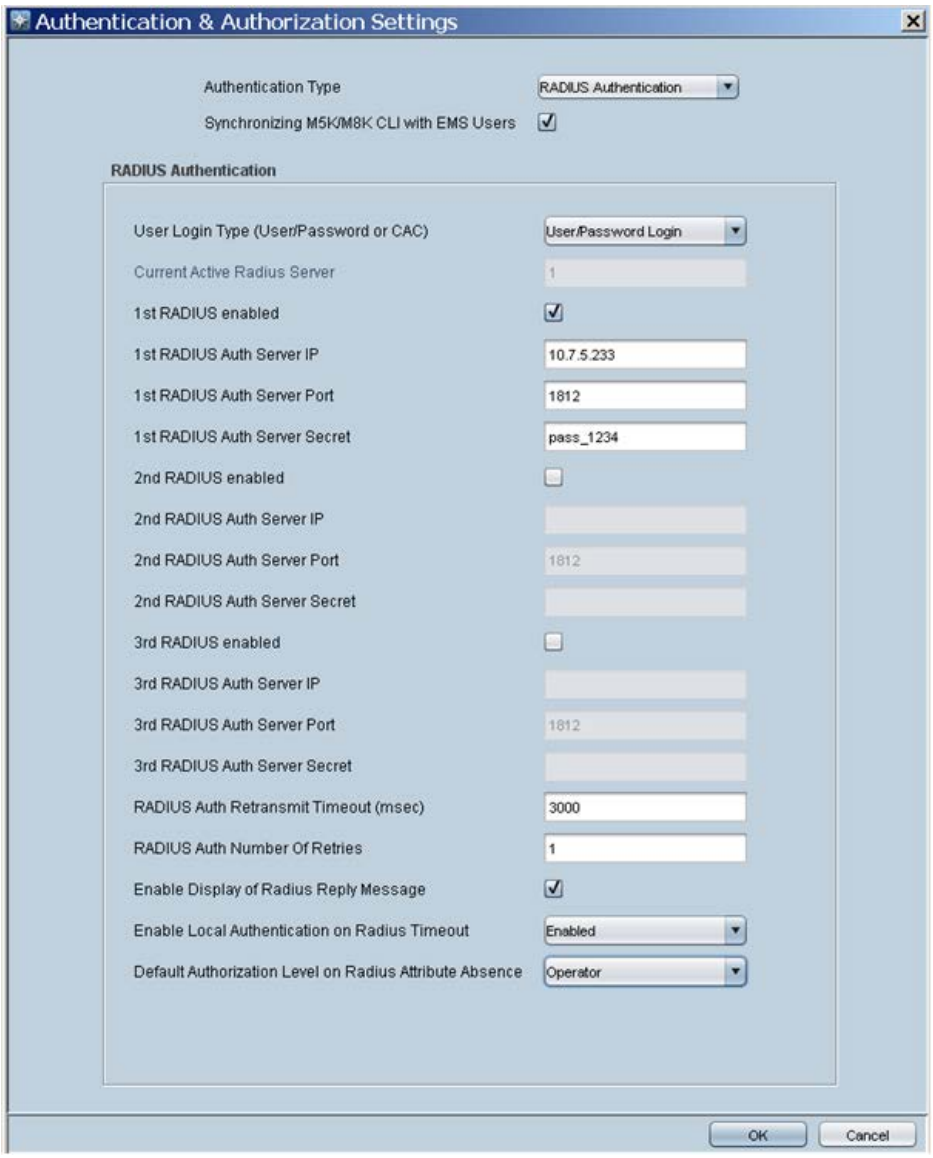
This section describes how to configure centralized EMS users Authentication and Authorization using a RADIUS server.

Note: There is a fallback option to save the user and password locally in the event that these servers do not respond ('Enable Local Authentication on Radius Timeout').

➢ **To configure using a RADIUS server.**

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the RADIUS Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **RADIUS Authentication**.

Figure 35-2: RADIUS Authentication and Authorization



3. Configure parameters as shown in the screen above.

35.2.2 TACACS+ Server

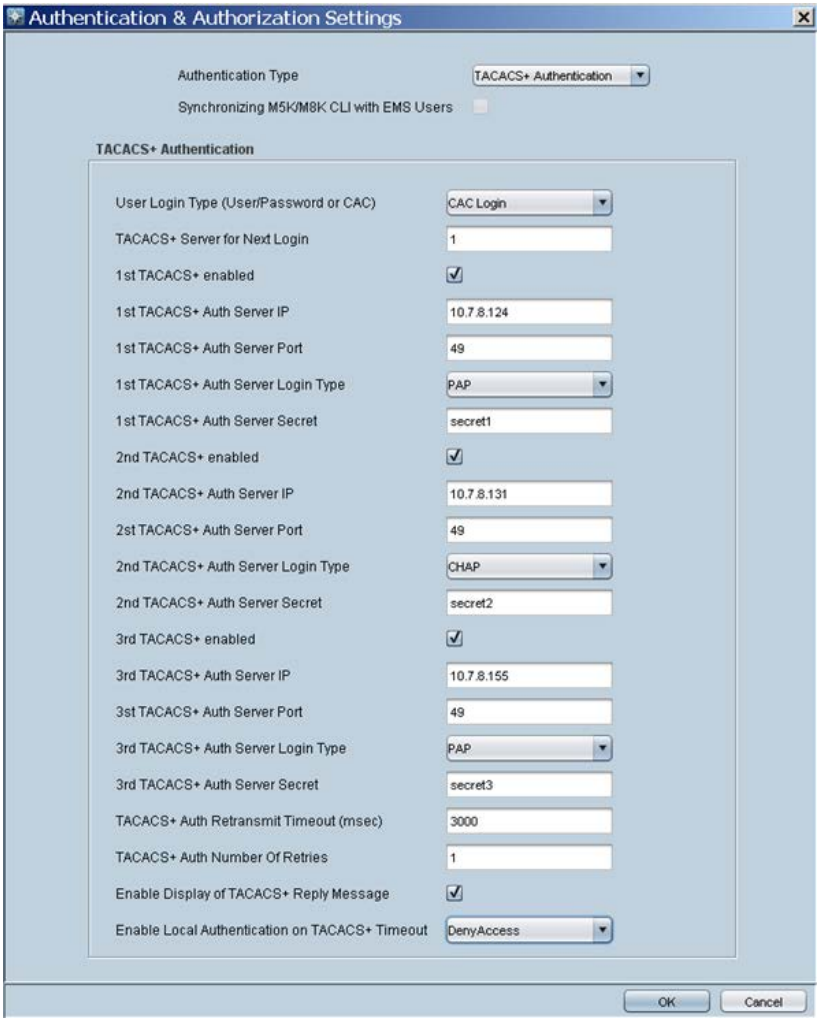
This section describes how to configure centralized EMS users Authentication and Authorization using a TACACS+ server.

Note: There is a fallback option to save the user and password locally in the event that these servers do not respond ('Enable Local Authentication on TACACS+ Timeout').

➢ To configure using a TACACS+ server.

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the TACACS+ Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **TACACS+ Authentication**.

Figure 35-3: TACACS Authentication and Authorization



3. Configure parameters as shown in the screen above.

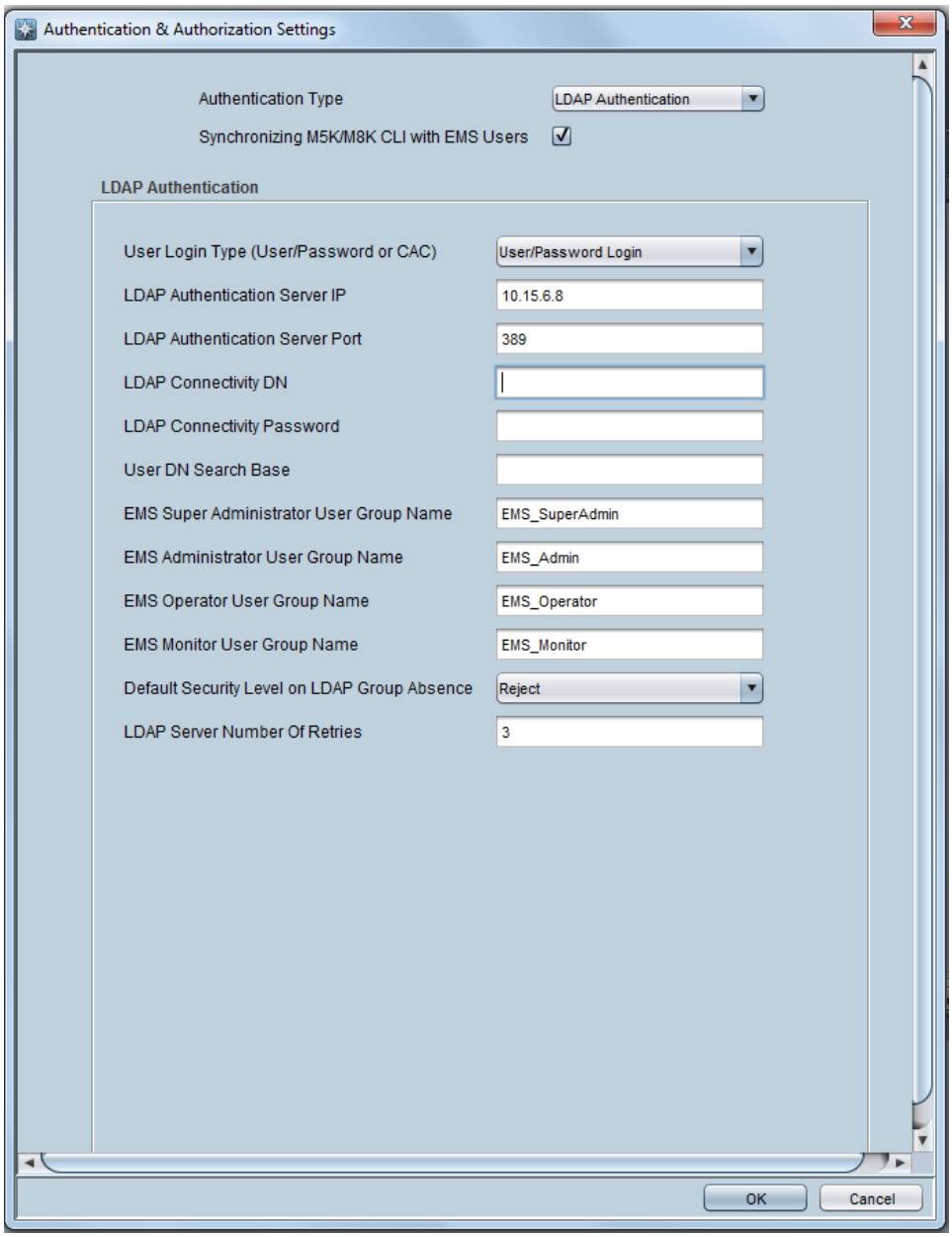
35.2.3 LDAP Server

This section describes how to configure centralized EMS users Authentication and Authorization using an LDAP server.

➢ To configure using an LDAP server.

1. In the EMS menu, choose **Security** > **Authentication & Authorization**; the LDAP Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **LDAP Authentication**.

Figure 35-4: LDAP Authentication and Authorization



3. Configure the LDAP Authentication Server IP.
4. Configure other parameters as required.

35.3 Local Users Management in the EMS Application

This section describes how to provision and operate EMS users stored locally in the EMS application. All the user operations can be performed by the user with the Administrator security level.

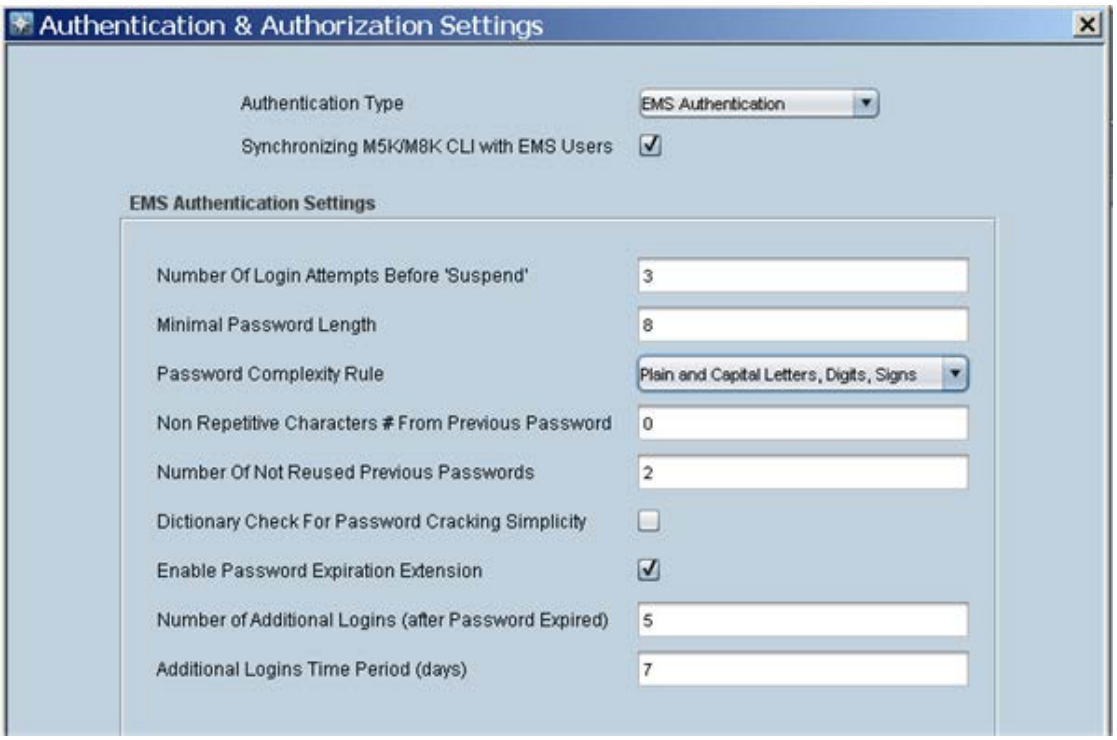
The local EMS's users management feature enables the operator with the Administrator security level to exert control over other operators' access to system resources. This ensures that sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be d isrupted by inexpert operators. In addition, the Administrator can set different user permissions for different regions. This feature has been implemented for Enterprise and Service provider environments who need to allow specific users to view only a subset of the sites, as well as to provide them with different security level per sites (regions).

User management is performed in the Security Menu, 'Users List' window. This window lists local EMS users and enables you to perform user management actions such as adding or removing a user. The EMS's user management feature enables the operator with the Administrator security level to exert control over other operators' access to system resources. In this way, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators.

➢ To manage EMS users using EMS:

1. In the Main EMS menu, choose **Security** ▶ **Authentication and Authorization**.
2. From the 'Authentication Type' drop-down list, select **EMS Authentication**.

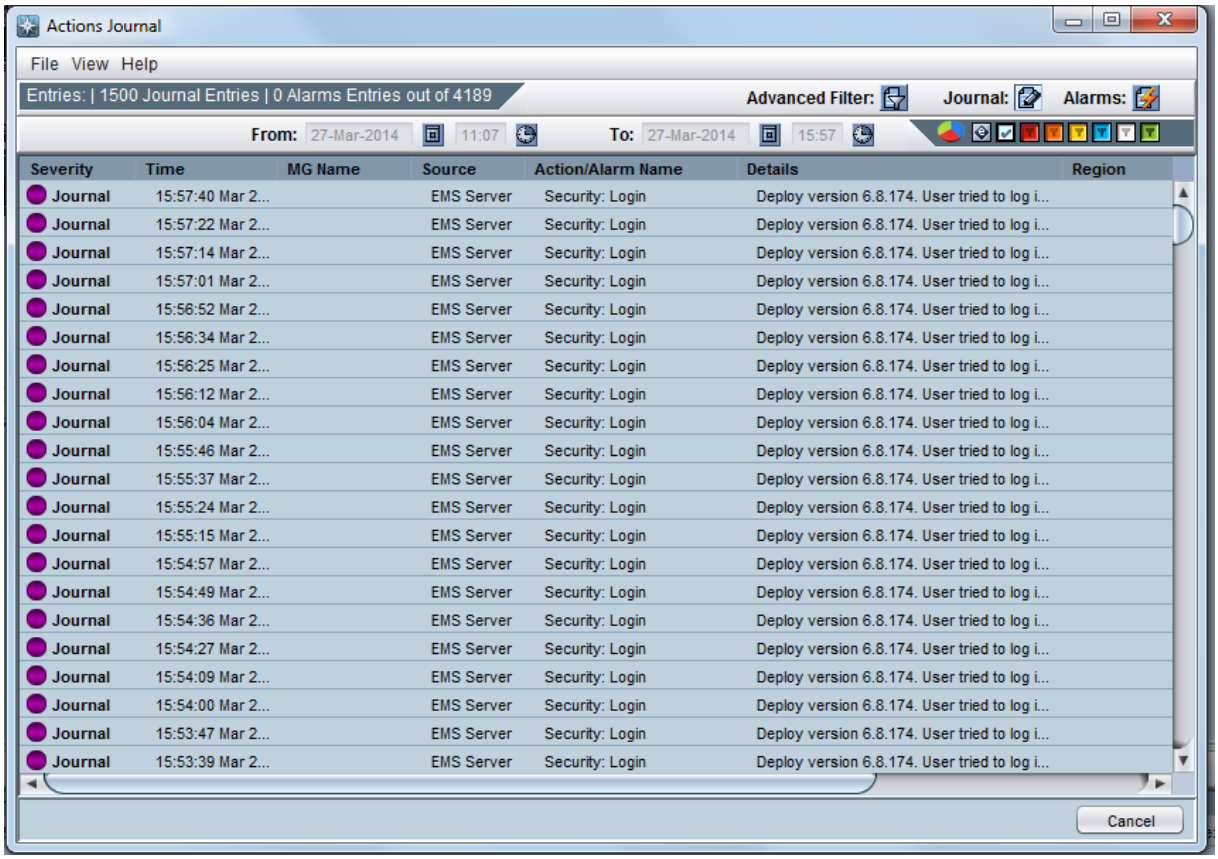
Figure 35-5: EMS Authentication Settings



35.3.1 Actions Journal-Security Items

The Actions Journal displays all logged operator actions, enabling the Administrator to verify appropriate operator access to system resources and providing the Administrator with the means to retroactively analyze actions previously carried out by operators. The Actions Journal screen is context sensitive and therefore when accessed from the Security menu, option 'Actions Journal', displays all login related events. For more information, see Chapter 36 on page 373.

Figure 35-6: Actions Journal-Security Items



35.3.2 Synchronizing EMS and Mediant 5000 / 8000 CLI users

When selecting this option, EMS automatically updates each one of the managed devices 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.

35.3.3 Provisioning Password Aging Rules

This section describes the EMS user password aging rules. Some of the rules are configured per EMS application and are applicable for all the users. Another subset of settings can be configured for each user. For more information on the user specific configuration, see the 'User Details Screen' descriptions.

The provisioning rules below are applicable for the entire EMS application and all its users.

To provision password aging rules:

- In the Authorization and Authentication Settings window, set the following parameters:
  - Number of Login Attempts before the EMS application suspends the user

    Once the number of login attempts as defined by this parameter is reached, the user is blocked from logging into EMS and can only be unblocked by the Administrator. Default-3 attempts.
  - Minimal Password Length: Default= 8 characters. The maximum supported value is 30 characters.
  - Password Complexity Rule- the following options are supported:
  - ♦ No complexity rules are applied (default)
  - ♦ Use Plain or Capital letters, Digits and Special Characters
  - ♦ Use Plain and Capital letters, Digits and Special Characters
  - Non Repetitive Characters # From Previous Password: Default=0, where all the characters can be reused for more than one password. The maximum supported value is 10.
  - Number of Not Reused Previous Passwords: Default=5. Possible values are 0-10.
  - Dictionary Check For Password Cracking Simplicity: when this option is enabled, the EMS server performs a password weakness check on the EMS user password. By default, this feature is disabled.

Note: All the parameters provisioned in this window are applicable for all the users and all the devices in the EMS application.

35.3.4 Provisioning Password Expiration Extension Period

This section describes how to provision the password expiration extension period.

To provision password expiration extension period:

1. In the Authorization and Authentication Settings window, select the **Enable Password Expiration Extension** checkbox, and set the following parameters:
2. **Number of Additional Logins** – defines the number of logins user can perform after his password already expired. Valid range: 1-10. Default: disabled.
3. **Additional Logins time period (days)** – defines the period (in days) during which user can perform the defined above number of additional logins. Valid range: 1-60. Default: disabled.

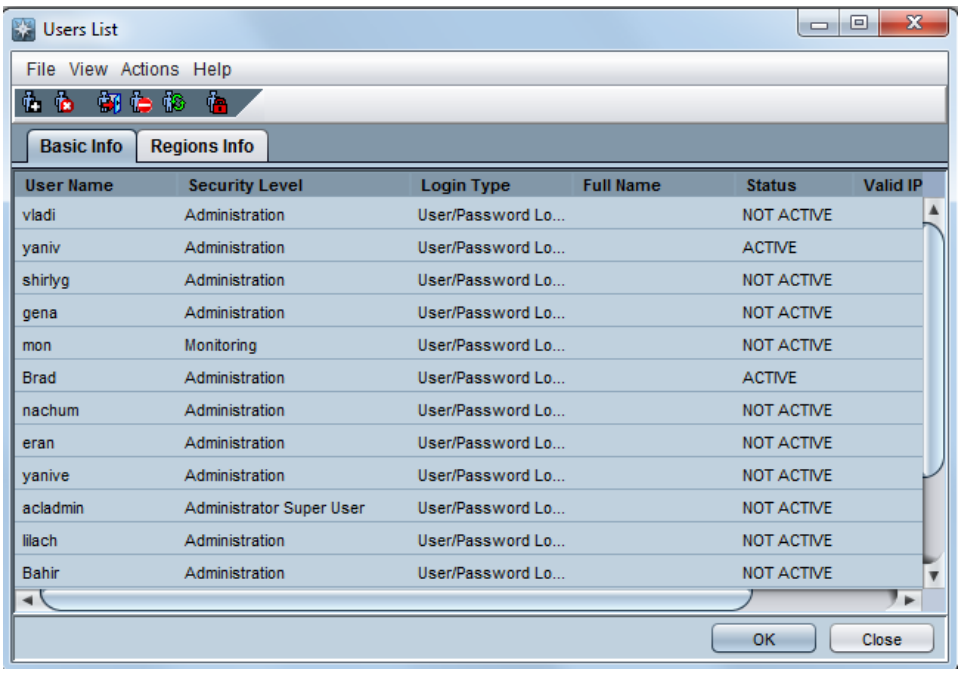
35.4 Managing the Users List

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

To open the Users List:

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

Figure 35-7: Users List



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.

35.4.1 Adding an Operator

This section describes how to add an EMS Operator.

➢ **To add an operator, do one of the following:**

- In the menu bar, choose **Actions > Add User**.

  -OR-

- Click the button **Add User** on the Users List toolbar; the User Details screen opens.

Figure 35-8: User Details screen - Basic Info

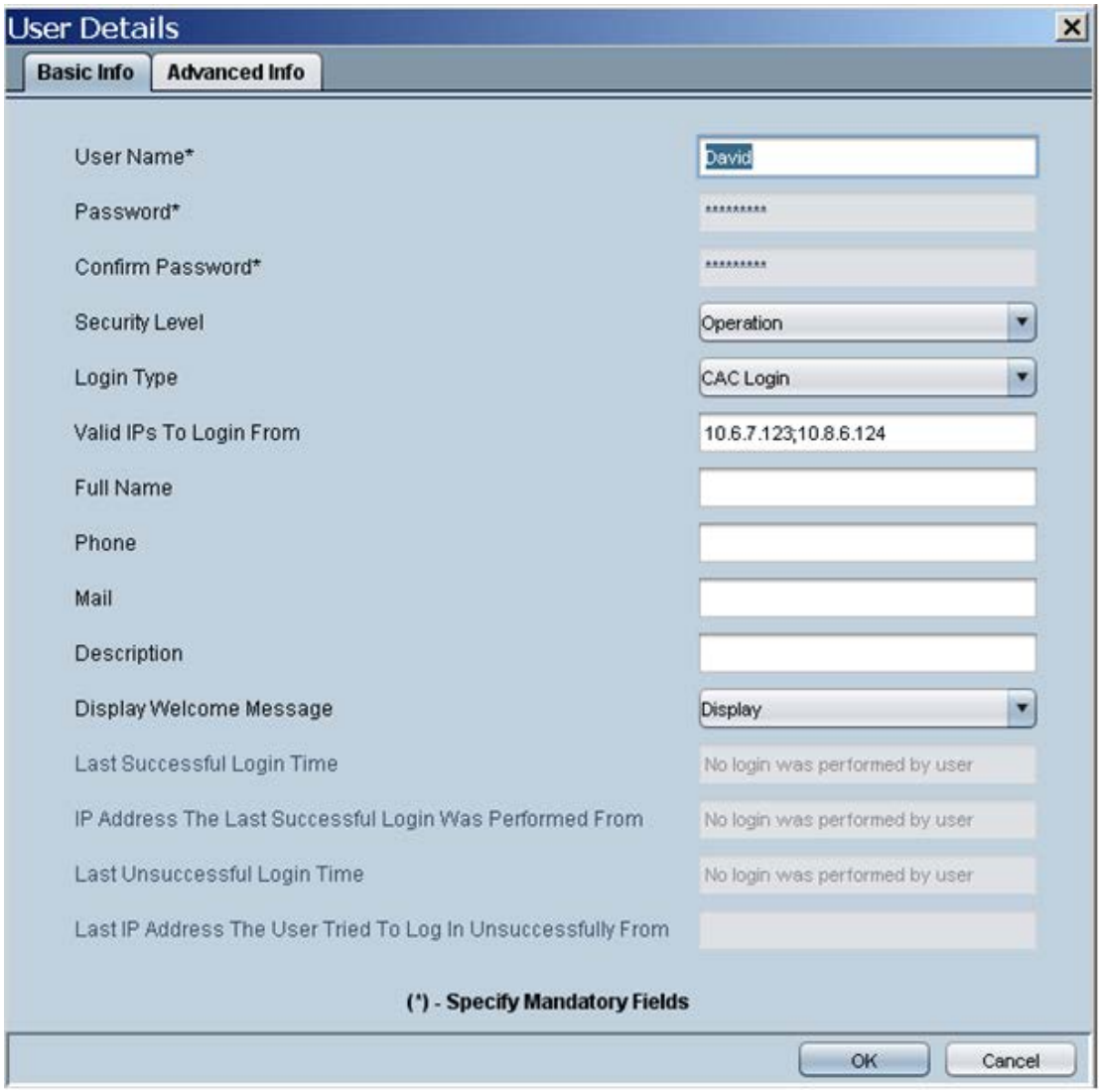
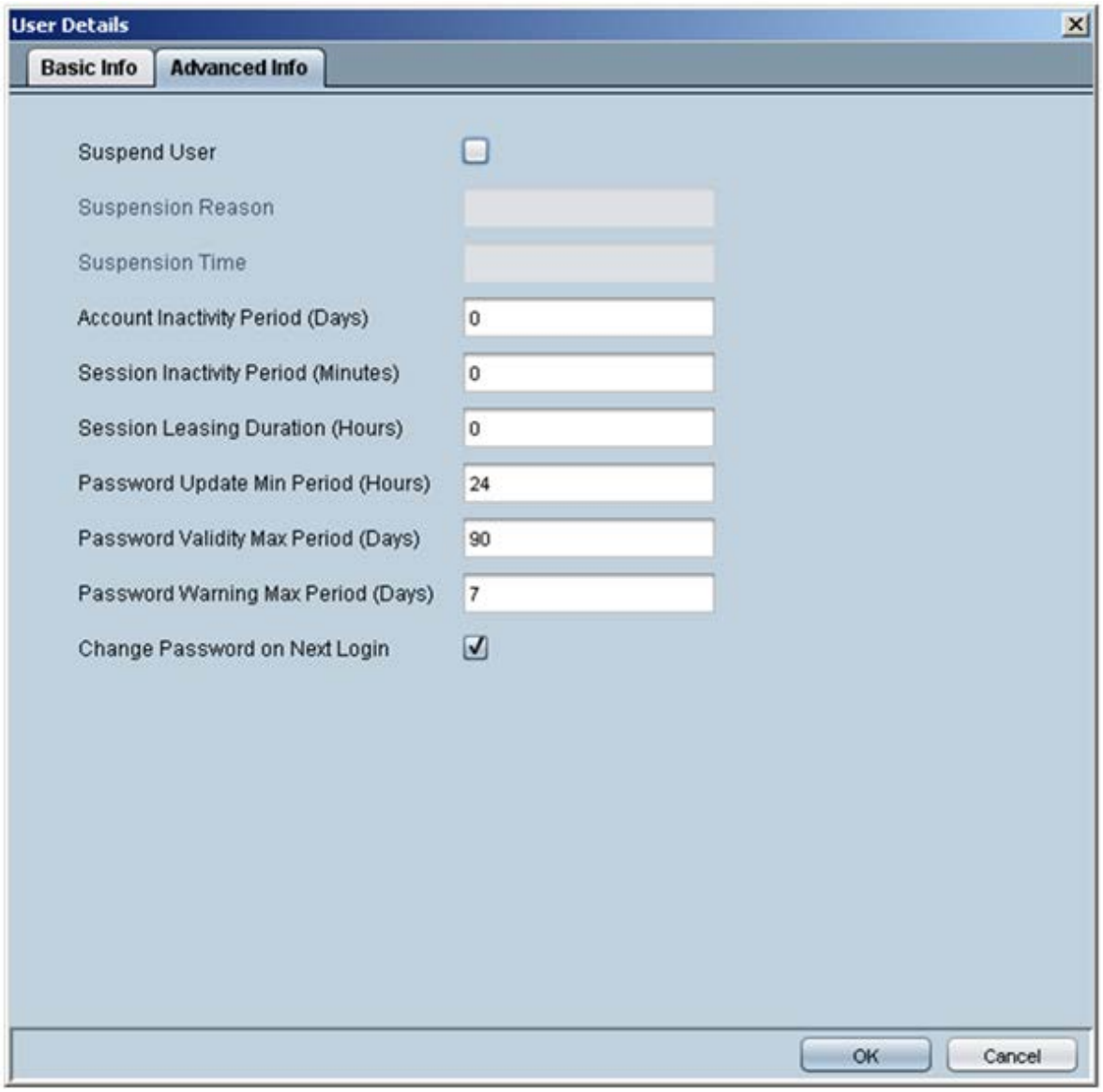


Figure 35-9: User Details screen - Advanced Info



- 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 341, 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.

35.4.1.1 Basic Info

- Changing a user's password: To modify a user's password, change the 'Password' and 'Confirm Password' fields. Both fields should have the same values.
- Security Level: EMS operators can be assigned one of the following security levels:
  - Not visible – this level is relevant only when defining different security levels per Region. When some Regions are defined as 'Not Visible' for the specific user, they will not be able to see these Regions and their devices in the EMS Tree.
  - Monitoring (viewing only)
  - Operation (viewing and all system provisioning operations on devices)
  - Administration (viewing, all system provisioning operations on devices, and operator security management described in this section).
  - Administrator Super User (viewing, all system provisioning operations on devices, 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.

35.4.1.2 Login Information

- Display Welcome Message

  In cases where the Welcome Message Option in the Help -> Welcome Message screen is set to 'Optional' or 'Disable', the Administrator can Enable / Disable the Welcome Message for each one of the specific users. A summary of the different definitions is summarized in the table below.

Table 35-1: 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.

35.4.1.3 Advanced Info

Suspend Information

- User suspension information: Suspension Status, Suspension Reason and Suspension Time.

Account / Session Security Settings

- **Account Inactivity Period (Days)**: User accounts are suspended in case the user did not login to the EMS application during a specified period of time (according to the parameter Account Inactivity Period). Default value= 0 where this feature is disabled and User Accounts are never suspended due to account inactivity. Maximal available value is 10.000 days.
- **Session Inactivity Period (Minutes)**: After the defined period of time (according to parameter Session Inactivity Period (minutes), the operator is notified that the session is 'Locked' and is prompted to enter their password to re-enter the EMS application. When set to the default configuration (0), no session inactivity timeout is applied. The Session inactivity period is a security mechanism designed to prevent unauthorized users from using the application while the authorized user is away from their computer.
- **Session Leasing Duration (Hours)**: After the defined period of time, the user is notified that the session is finished and is prompted to enter their password to work with the EMS. When defined as '0' (default configuration), no leasing time is applied. Leasing time is a security mechanism to permit the operator to log in to a time duration that is equivalent to one shift (i.e., 8 hours).

Password Settings

- **Password Update Minimum Period (Hours)**: A user password cannot be changed more than once within the time specified by this parameter. Default-24 hours.
- **Password Validity Maximum Period (Days)**: A user password must be changed within a specific number of days since the last password change as defined by this parameter. Default-90 days.
- **Password Warning Max Period (Days)**: The user receives a warning message a specified number of days prior to the password expiration date. Default-7 days.
- **Force Password Change on the next login**: A user password must be changed on the next Login attempt, before the previously defined password expiration time has expired. Active users are not required to Logout the application until their session has ended.

35.4.1.4 Regions Info

- The **Regions Info** tab includes the currently defined regions in the EMS and the security level for each region. The security level can be defined per region only for users with the 'Basic' security permissions 'Operator' or 'Monitoring'. For each one of the regions, the administrator can choose one of the following permissions:
  - Operator
  - Monitoring
  - Not visible
- The Region security level cannot be set to a higher security level than the 'Basic' user security level. For example, if the 'Basic' security level is set to 'Monitoring', it cannot be set to 'Operator' in any of the regions.

Note: For the 'Super-Admin' & 'Admin' levels, there is no option to define the security level per region, since these users are system level users.

- **Global Users Permissions:**

  Users with 'Super Administrator' or 'Administrator' permissions can perform the following EMS actions:

  - Users Management – view, define, edit users and user permissions. Perform actions related to the Users.
  - View Users Actions Journal
  - Perform Software and / or Auxiliary Files definition in the Software Manager (while the download to the device can be performed also by Regional Users)
  - Add / Remove Region (device), Move device from one Region to Another.
  - Provision Trap Forwarding Rules

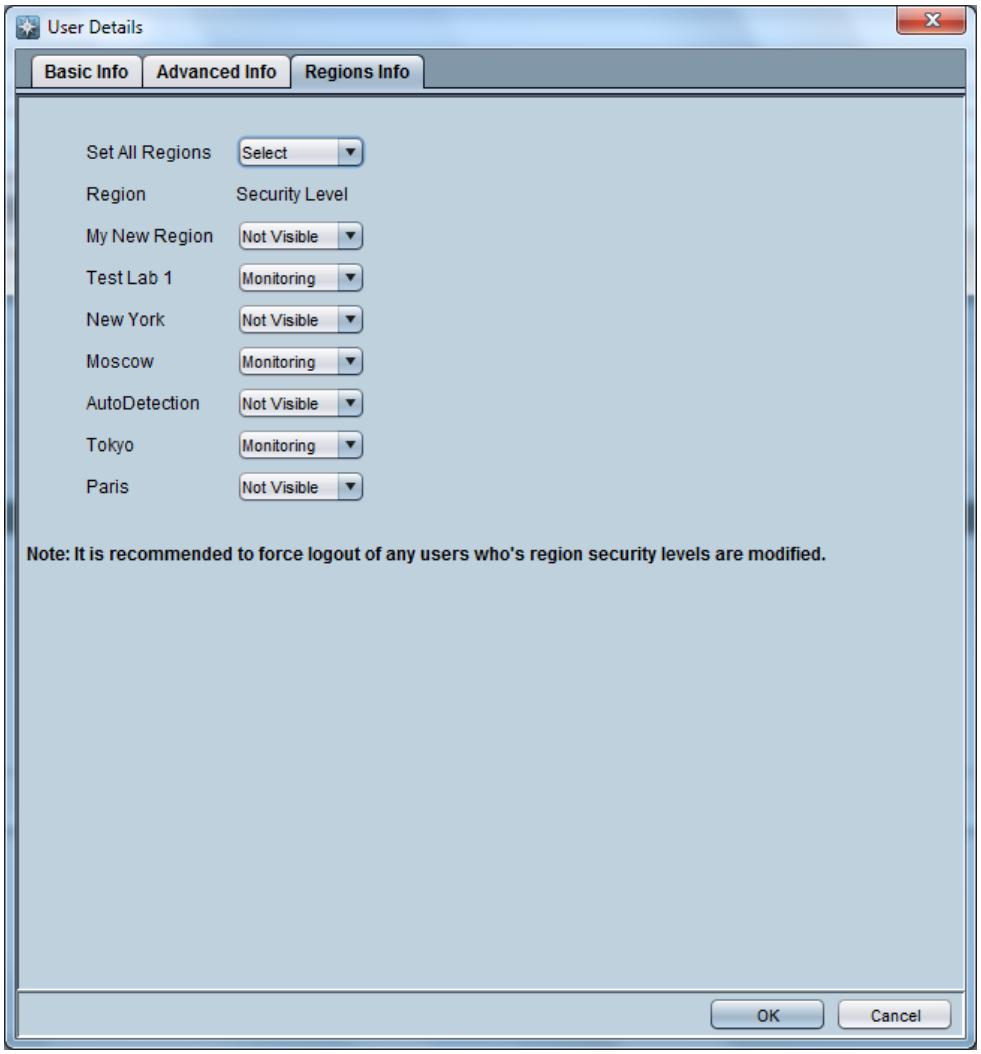
Note: These actions are not supported at the Regions level.

- **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 devices, 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 35-10: User Details - Regions Info



35.4.2 Modifying Operator Details

This section describes how to modify EMS Operator details.

➢ **To modify operator details:**

1. Double-click the name of the operator listed in the left column under Login; the User Details screen opens.

   The User Details screen is identical to that displayed in the figure 'Adding an Operator' (see Section 'Adding an Operator' on page 361) with the difference that fields are configured and the first field Login Name is disabled (read-only and non-configurable).

   The field 'Security Level' enables the Administrators to set access rights for each operator: Administrator Super User, Administration, Operation and Monitoring.

   If the user is an active user (logged in), changing the security level automatically logs the user out.
2. Click **OK** to send the modified user data to the server.

35.4.2.1 Removing an Operator

This section describes how to remove an EMS Operator.

➢ **To remove an operator:**

1. In the Users List screen, select the row of the operator to remove. Multiple rows can be selected to be removed.
2. Click the **Remove User** button or open the 'Action' menu and choose option **Remove User**. All selected rows are removed from the User Security Management screen.
3. Click **OK** to send your changes to the server.

Note: At least one user with the security level of Administrator Super User should always be defined in the EMS system. Attempted removal of the last user with the security level of Administrator Super User will fail.

35.4.2.2 Forcing the Logout of a Currently Active Operator

This section describes how to force the logout of a currently active Operator.

➢ To force the logout of a currently active operator:

1. In the 'Users List' screen, select the row of the operator who is to be logged out. Multiple users can be selected for logout.
2. Click the icon **Logout User** or open the 'Actions' menu and choose option **Logout User**; all selected rows now indicate 'NOT ACTIVE'.
3. Click **OK** to send your changes to the server.

35.4.2.3 Suspending an Operator

This section describes how to suspend an EMS operator.

➢ To suspend an operator:

1. In the 'Users List' screen, select the row of the operator who is to be suspended. Multiple users can be selected for suspension.
2. Click the icon **Suspend User** or open the 'Actions' menu and choose option **Suspend User** or double-click the user's row and select the check box **Suspended**; all selected rows now indicate 'SUSPENDED'.
3. Open the 'User Details' screen (double-click the row of the user) and enter the reason for the suspension of that user in the field 'Suspension Reason'.
4. Click **OK** to send your changes to the server.

   All active users are automatically logged out before suspension

Note: A user with the security level of Administrator or Administrator Super User cannot be suspended.

35.4.2.4 Releasing an Operator from Suspension

This section describes how to release an EMS operator from suspension.

➢ **To release an operator from suspension:**

1. In the Users List screen, select the row of the (suspended) operator who is to be released from suspension. Multiple users can be selected for release from suspension.
2. Click the icon **Release User from Suspension** or open the 'Actions' menu and choose option **Release User from Suspension**, or double-click the user's row and clear the checkbox **Suspended**; all selected rows now indicate 'NOT ACTIVE'.
3. Click **OK** to send your changes to the server.

35.4.2.5 Canceling Changes Made to the Users List

This section describes how to cancel changes made to the users list.

➢ **To cancel changes made to the Users List screen:**

- Click the **Cancel** button (not the **OK** button); all changes you made are canceled.

35.4.2.6 Changing an Operator's Password

The following describes the conditions for changing an EMS operator's password:

Password management rules are defined both per EMS application and per specific operator. These rules are configured by the EMS Administrator.

➢ **To change an operator's password:**

1. Operators can change their own password. In the 'Security' menu, choose option **Change Password**; the 'Change Password' screen opens (see the figure below).

Figure 35-11: Change Password

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

This page is intentionally left blank.

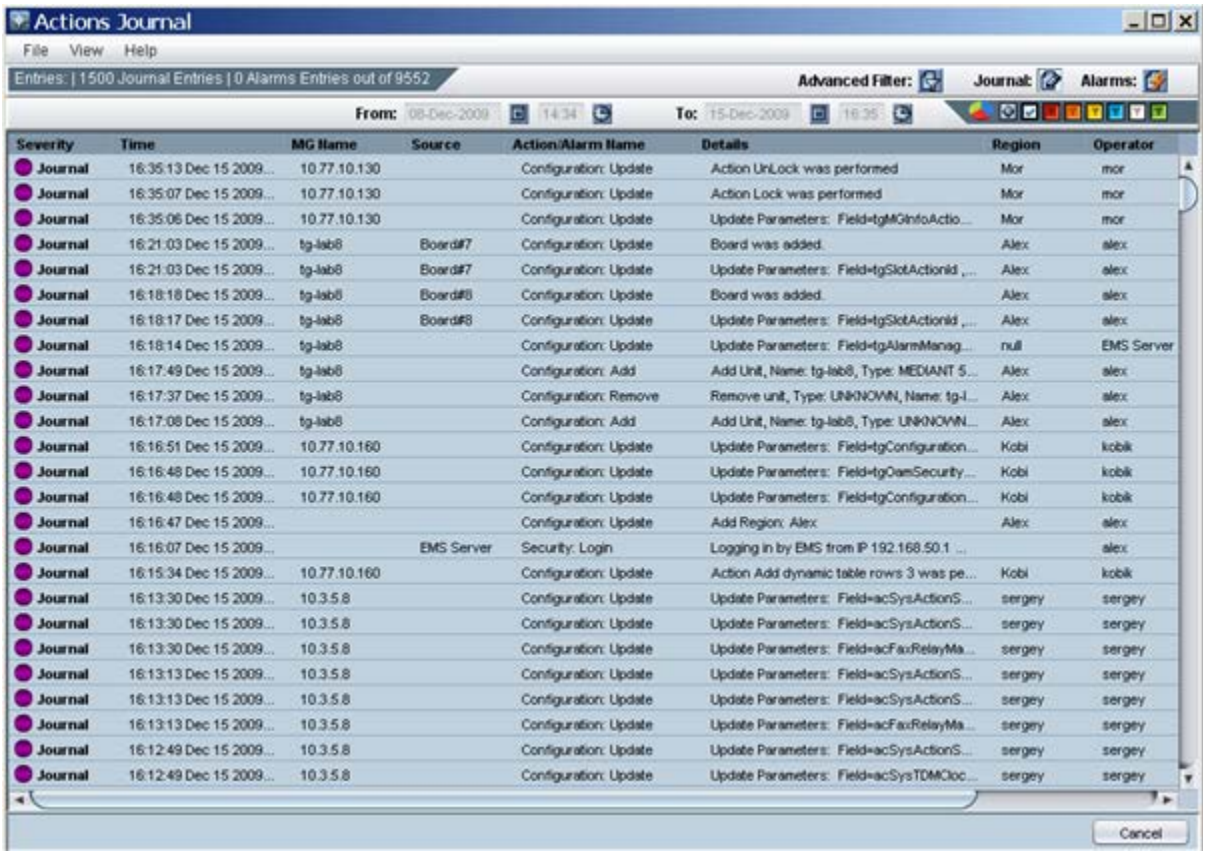
36 Viewing Operator Actions in the Actions Journal

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 36-1: 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 36-2: Journal Actions

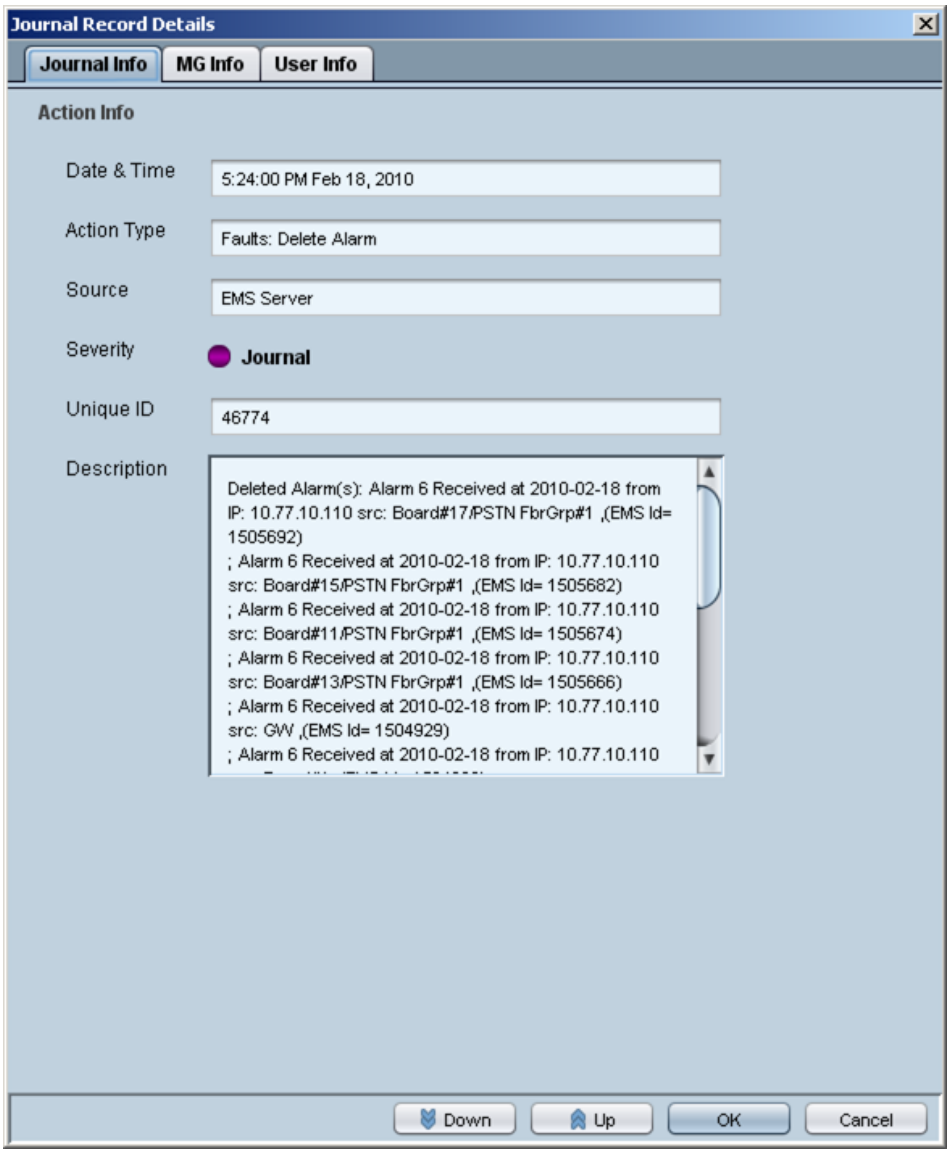
- **Details** - a precisely detailed description of the action, for example, parameter names and values for a Configuration Update action.
- **Operator** - the name of the operator who performed the action.
- **Region** - the region in which the device resides.

36.1 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:

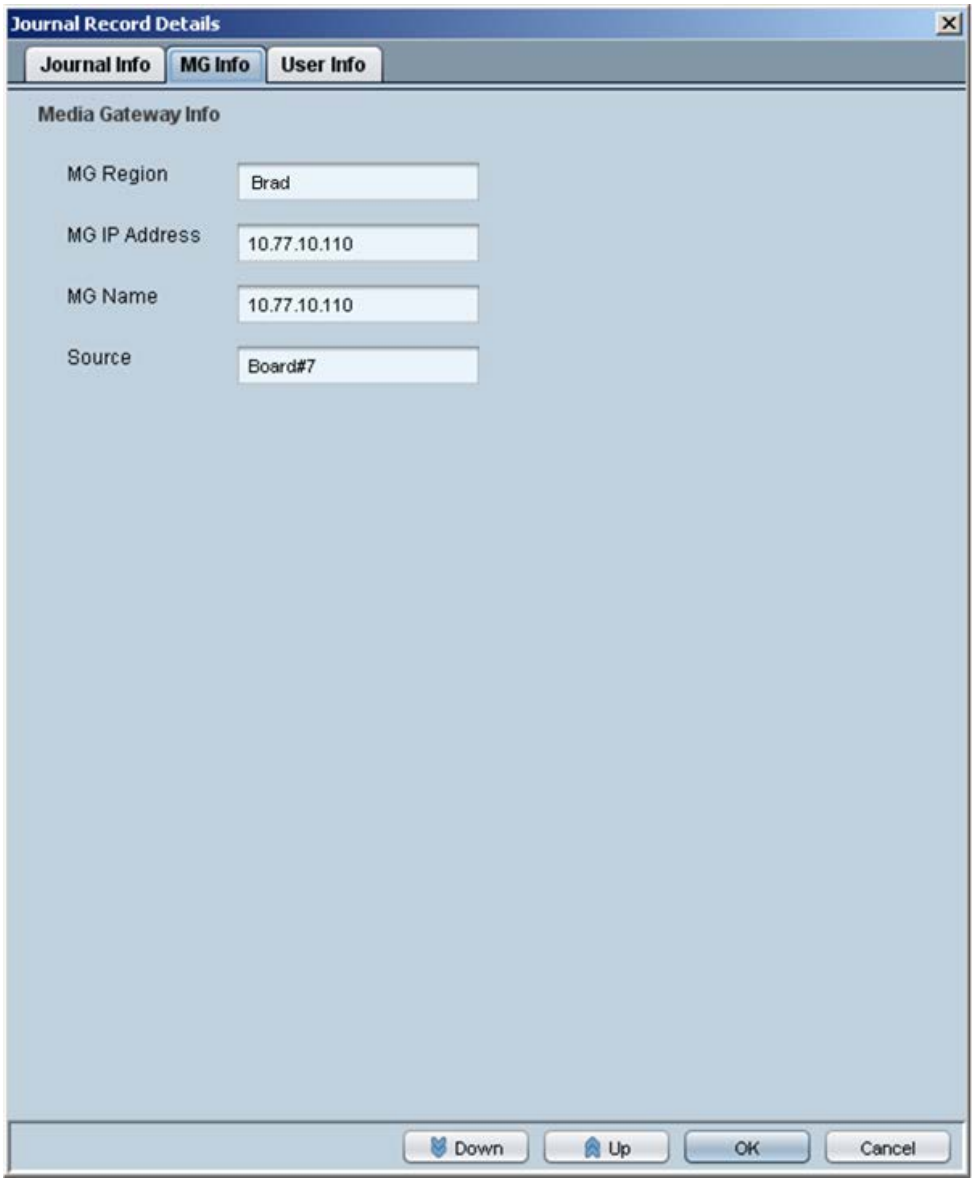
- Journal Info

Figure 36-3: Journal Record Details - Journal Information



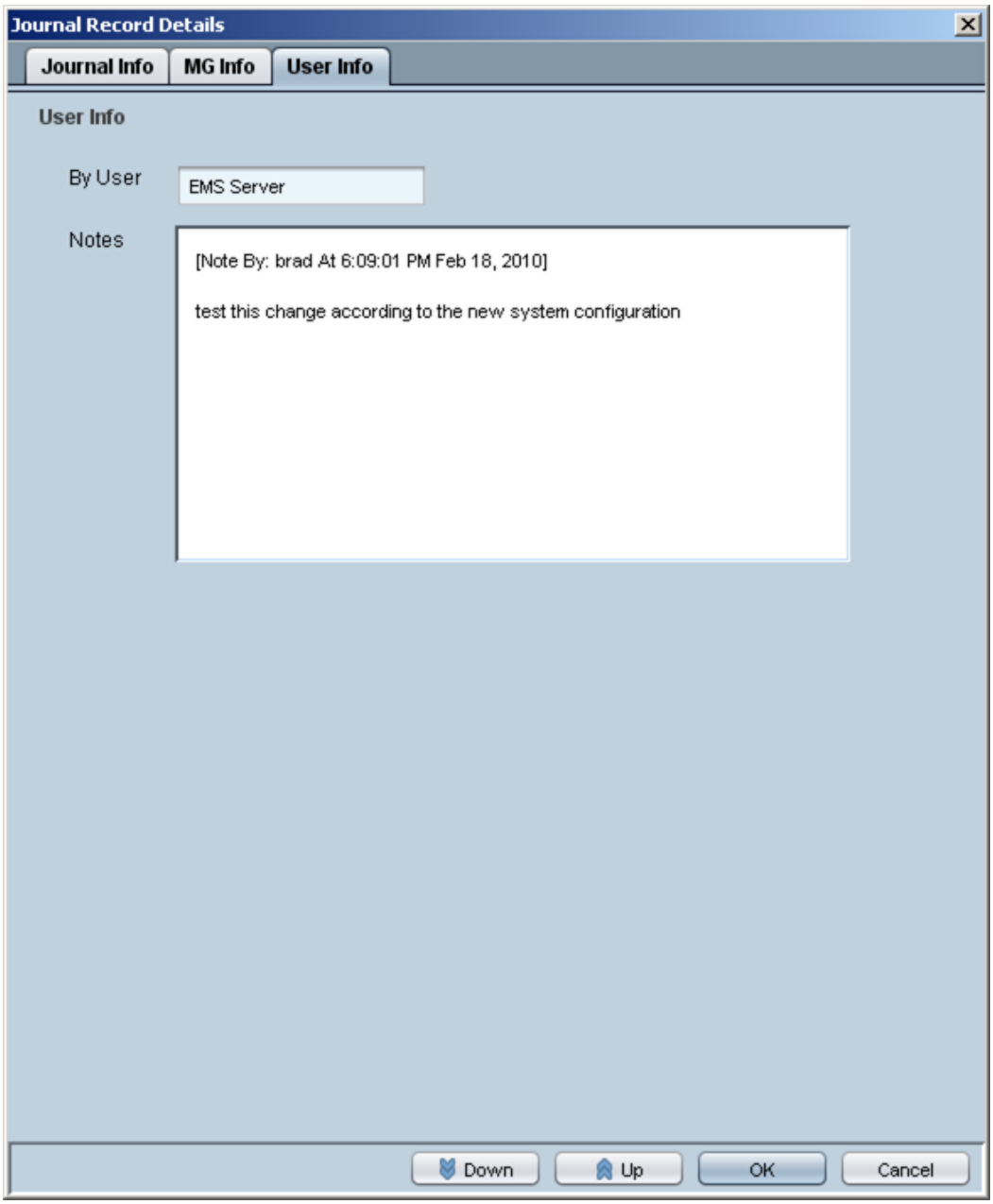
- MG Info

Figure 36-4: Journal Record Details - Media Gateway Information



- User Info

Figure 36-5: Journal Record Details - User Info

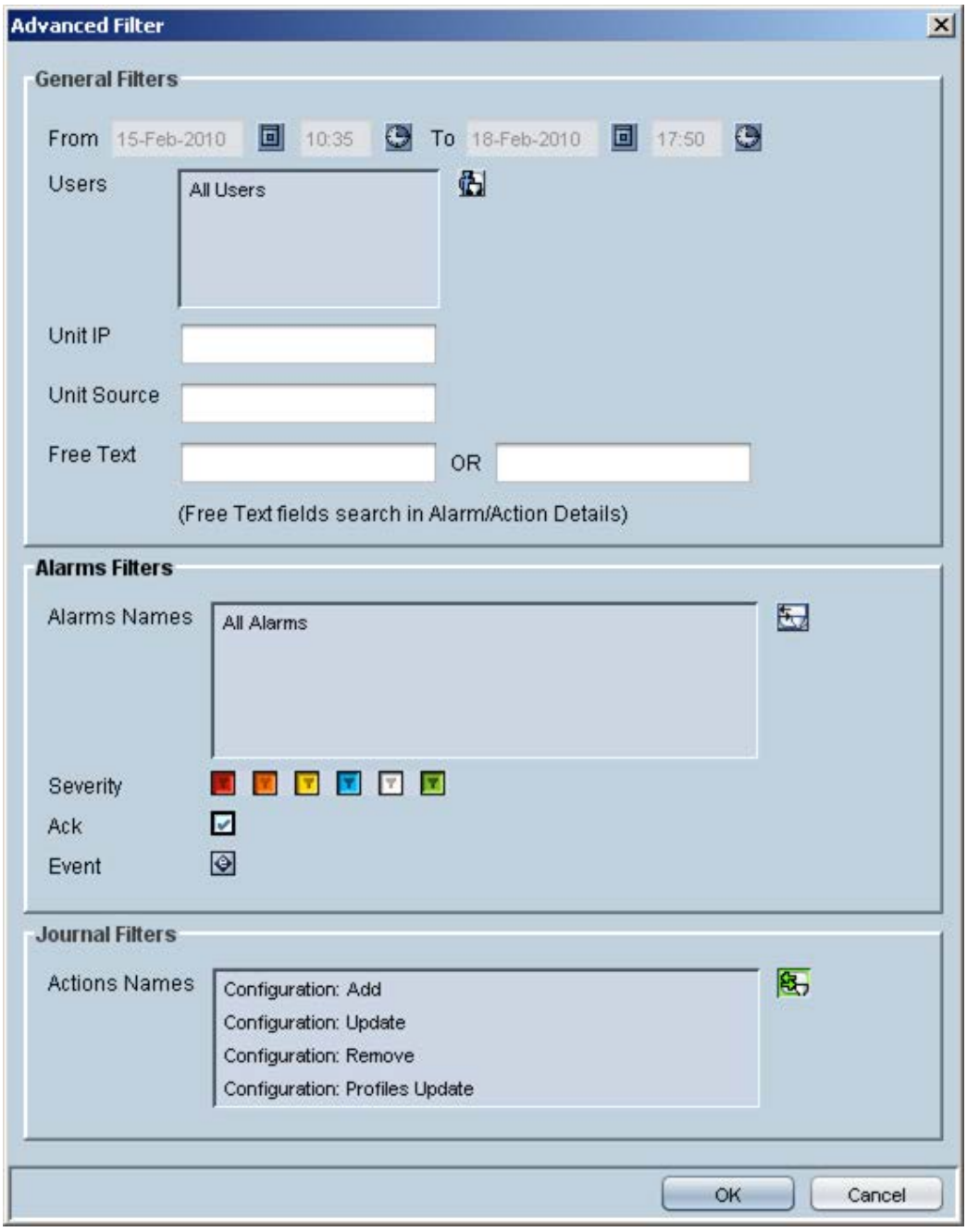


Users can insert data to be saved, together with the journal record in the Journal.

36.2 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 36-6: 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 269)
- **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)

36.2.1 Example of Filter Use

This section describes how to find all parameters that were modified in September 2006 in Board#8 of a specific device. 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 device 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.

36.3 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).

Part VI

Troubleshooting

This section describes the various EMS troubleshooting scenarios.

37 Failure to Connect to a Device - all Devices

This section describes the various scenarios that may cause a failure to connect to a device.

Failure to connect to a device can occur in one of the following circumstances:

- When attempting to connect to a device for the first time
- When attempting to connect to a device after already having established a connection but in the interim the device'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 device icon, shown in the figure 'Failure to Connect to a device 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:

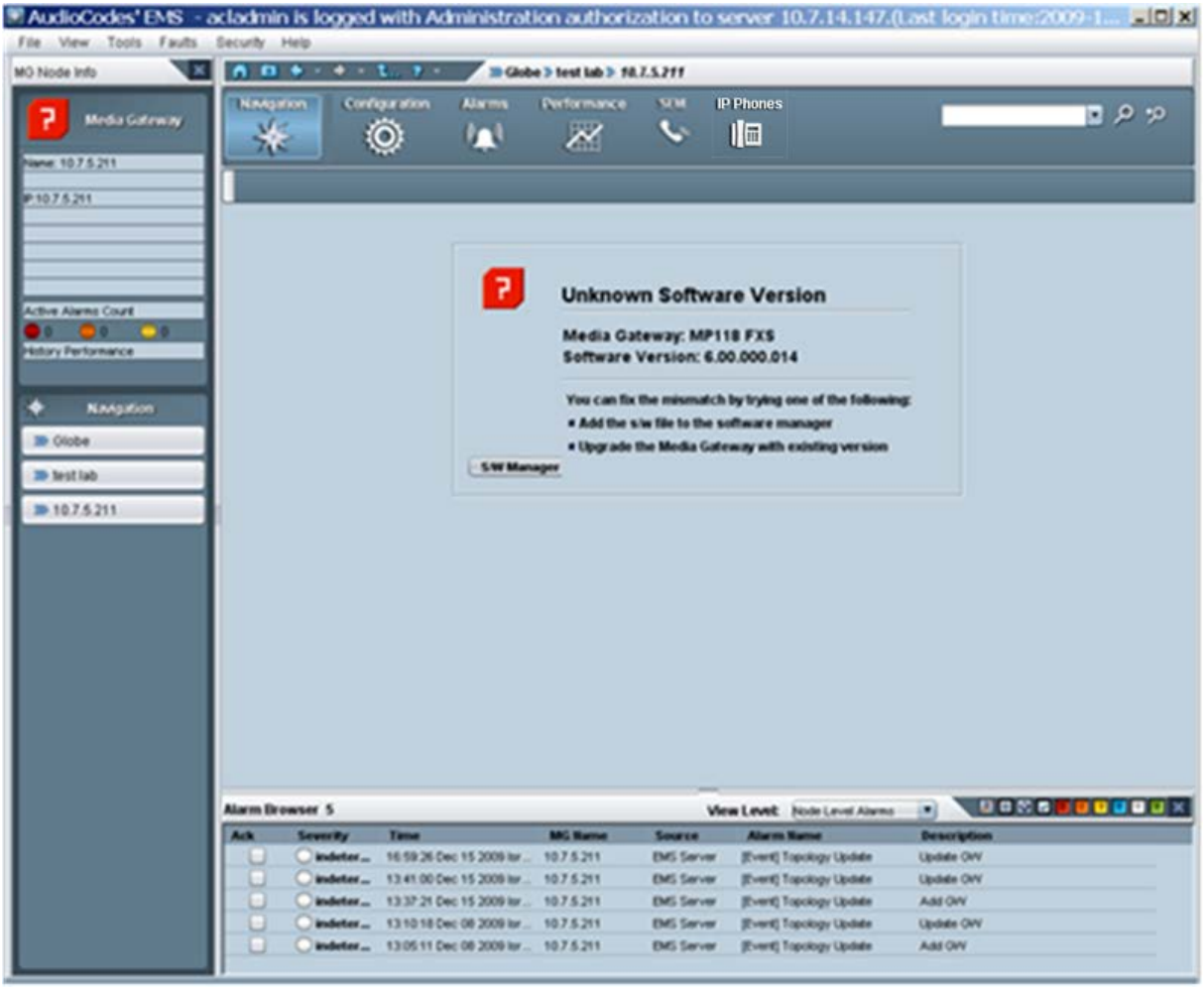
1. You've incorrectly defined the IP address of the device you're attempting to connect to (in the MG Information screen; see the figure 'Incorrectly Defined MG Information Screen', below).
2. An operational problem exists in the system (lack of communication with the server, for example).
3. A network problem prevents the EMS server from connecting to the device. Ping the device'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 37-1: Possible First-Time Connection Problems: How to Verify Them, How to Fix Them

Possible Problem	How to Verify It	How to Fix It
Wrong device IP address defined in EMS	In the MG Tree, right-click the device and choose option **Details**; verify that the device IP address is correct.	▪ Delete the device (right-click the question-mark icon and choose the option **Remove MG**). ▪ Add a new device (see Section 'Defining VoIP Devices, Managing the MG Tree' on page 73). Define the MG Information fields ensuring that the IP address for the device 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 device 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 device 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 device is not connected to the Network	In the cmd window (**Start > Run**), ping the device to verify that it is responding.	If the device isn't responding to the ping, check if there is a network problem or if the device is not operating.
The device version is not defined in the EMS Software Manager	A message notifying you that the current device 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 device of one of the EMS- supported versions.
The device 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 device).	Contact Customer Support.

Figure 37-1: Incorrectly Defined MG Information Screen



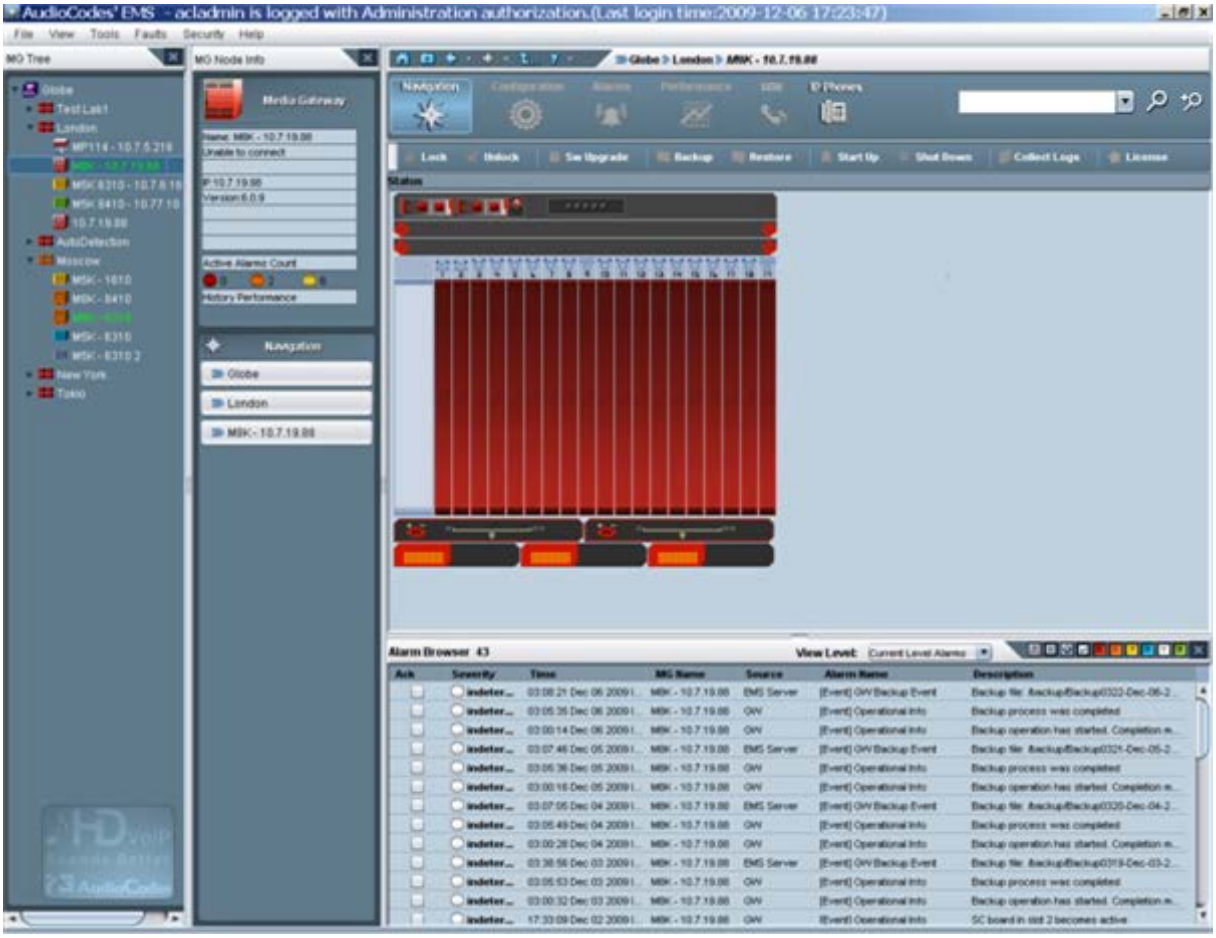
37.1 Failure to Reconnect to a Previously-Connected Device whose Operation was Interrupted

This section describes the various scenarios that may cause a failure to reconnect to a previously-connected device whose operation was interrupted.

There are three EMS GUI indications as to a failure to reconnect to a device that was previously connected but whose operation has been subsequently interrupted:

- A red icon of a device is displayed under the Region and in the Status pane (when the Region is selected).
- A device 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 37-2: Failure to Reconnect to a Device 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 37-2: 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 / device communication.	Refresh by pressing F5 or View > Refresh. If the EMS cannot reestablish connection with the device, ping the device 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 device again. (SNMP error 22 – Timeout) will be constantly received.	Verify in the EMS's Users Journal that the device Community Strings (SNMPv2) or SNMPv3 parameters were changed. Verify that the device 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 device is not responding to ping requests.	Refer to the sections on troubleshooting the device.

Notes:

- A device (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 device, as was the case with a first-time connection failure.

37.2 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

Part VII

Appendix

This section describes various miscellaneous procedures.

A Prepare Devices for Interoperability Automatic Provisioning

The Interoperability Automatic Provisioning feature requires pre-configuration of the device for successful implementation. The following topics are described:

- Configuring the device's network connectivity (see below).
- Configuring the device to send Keep-alive traps to the EMS (see Section A.2) according to the following.
  - Devices added using serial number:

    If you added the devices to the EMS using its serial number, you need to configure the device so that a Keep-alive trap can be send from the device to the EMS when the device is powered up.
  - Devices added using IP address:

    If you have added the device to the EMS using an IP address and/or the device is located behind a NAT then you need to configure the device to send a keep alive trap in order to support the auto-detection mechanism. For more information on the auto-detection mechanism, see Section 5.3.2.
- Configuring the device's SNMP settings (see Section A.3).

A.1 Configuring Device's Network Connectivity

Before you can provision your device using the Interoperability Automatic Provisioning feature, you need to do the following:

- Connect the device to the Enterprise Network:

The device is shipped with a factory default IP address for operations, administration, maintenance, and provisioning (OAMP), through its VoIP LAN interface. You need to change this default IP address with an OAMP address that is in the same subnet as the EMS (for more information, refer to the relevant *SIP User's Manual).*

- Configure all other required interfaces in the IP interface table:

The Interoperability Automatic Provisioning feature requires each device to have a completely pre-configured IP Interface table. In addition, each device IP Interface table must be configured with the structure as the template ini file. Specifically, it must be configured using the same index numbers with the same Application Types and Interface Names assigned to each respective index. During the Interoperability Automatic Provisioning validation process with the device, each index entry is validated with the equivalent entry in the template file (see example file extract on page A.1.1).

Notes:

- The reason for the above requirement is that the SIP Interface and Media Realm tables configure the 'Interface Name' therefore if two different devices have different IP Interface index numbers configured, then if attempt is made to apply the template SIP configuration to these devices, the process will fail. For example, if device A is configured with index 0 OAM interface 'OAM' and index 1 Media and Control interface 'NET1', and device B is configured the opposite with index 0 'NET1' and index 1 'OAM', then the 'Interface Name' of the OAM interface 'OAM' cannot be referenced by the template file's SIP Interface and Media Realm tables to index 0 for one device and index 1for the other device. Likewise, 'NET1' cannot be referenced to index 0 for one device and index 1 for the other device.
- If any device's IP interface table does not meet these requirements, the Interoperability Automatic Provisioning process fails and a consequent alarm is sent to the EMS (see Section 22.6).
- The Interoperability Automatic Provisioning feature can read the values from the device's IP Interface configuration and integrate these values into the provisioned configuration; however, it cannot change existing values or add index entries.

- The following networking-related configuration tables are not provided in the initial template production file and are instead read directly from the device during the Interoperability Automatic Provisioning process (see Section A.1.3). Consequently, you must pre-configure these tables (see Section A.1.2):
  - Ethernet Device Table
  - Ethernet Group Table
  - Physical Ports Table
  - Static RouteTable
  - QoS Settings

Note: If you have loaded a CLI script file for an MSBR device, then you do not need to pre-configure the IP Interface table and the other networking tables as described above.

A.1.1 Configuring IP Network Interfaces

This section shows an example configuration of the following network interfaces:

- OAMP Interface to connect to EMS.
- Media and Control interface for the WANSP network toward SIP Trunk.

Note: Before performing this configuration, open your template file and note the index configuration; the index structure must be identical to the template file as explained on page 391. In addition, see page 395 for details on the template file.

➢ **To configure the IP network interfaces:**

1. Access the device's Web-based Management tool.
2. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
3. Configure the entries similar to the example below:

Table A-1: Configuring IP Interfaces-Example

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Device
0	OAMP + Media + Control	(IPv4 Manual)	10.15.17.10	16 (subnet mask in bits for 255.255.0.0)	10.15.0.1	Voice	10.15.25.1	0.0.0.0	vlan 1
1	(Media + Control)	(IPv4 Manual)	195.189.192.156	25 (for 255.255.255.128	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2

4. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).
5. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
6. Click the **Reset** button.

A.1.2 Configure Other Networking Tables

Using the device's Web-based Management tool, configure the other networking-related configuration tables; use the table below as a guide.

Table A-2: Configuring Other Networking Tables

Configuration Table	Navigation Paths
Ethernet Device Table[1]	**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**
Ethernet Group Table	**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Group Table**
Physical Ports Table	**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Table**
Static Route Table (Optional)	**Configuration** tab > **VoIP** menu > **Network** > **Static Route Table**
OoS Settings (Optional)	**Configuration** tab > **VoIP** menu > **Network** > **QoS Settings**

For more information, refer to the relevant *SIP User's Manual.*

[1] It is mandatory to configure this table.

A.1.3 Networking Configuration and the Template File

The template ini file includes the configuration that you wish to apply to all the devices that you wish to provision. The template ini file that is loaded to the EMS Software Manager (before it is applied to the device) includes a full production configuration with all device configuration tables except for the following tables which receive their production configuration during the Interoperability Automatic Provisioning process:

- IP InterfaceTable[2]-the entries in this table are validated with the device's preconfigured IP Interface table as described in Section A.1. Once successfully validated, the entire table is read from the device, set to the template ini file and then resent to the device.
- Device Table; Ethernet Group Table; Physical Ports Table; Static Route Table and QoS Settings - these tables are read directly from the device, set to the template ini file and then resent to device.

The Interface Table ini file configuration extract below (based on t he example configuration above A.1.1) shows the validated values in blue (these values are validated with the device and therefore must be identical for all devices). The values in red indicate those values that are not validated and only read from the device once the blue parameters are successfully validated.

```
The table below shows the above data after it is written to the
ini file Interface table:
[ \InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;

InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";

InterfaceTable 1 = 5, 10, 195.189.192.156, 25, 195.189.192.129,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";
```

[2] If the EMS is configured for HA, the entry ApplicationType 99 is removed from the IP Interface table during the Zero Touch process.

A.2 Configuring the Device to Send SNMP Keep-alive Messages

This section describes how to configure the device to send SNMP Keep-alive messages to the EMS according to the following:

- **Device added using serial number:**

  Configuring the device using the Automatic provisioning feature requires the connection between the EMS server and the device to be active. This can be ensured by configuring the device to send Keep-alive traps to the EMS server. EMS recognizes the device according to the sysDesc field and serial number on the device itself, and according to the entries in the EMS database and MG tree.

  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 keep alive trap to the EMS. When the keep alive trap is received, the EMS first verifies that it's AudioCodes' device, then connects the device and loads the configuration or firmware file according to the configuration performed in Chapter 5.

- **Device added using IP address:**

  If you have added the device to the EMS using an IP address and/or the device is located behind a NAT, perform the procedure below to configure the device to send a keep alive trap in order to support the auto-detection mechanism (for more information on auto-detection, see Section 5.3.2).

Notes:

- For more information on EMS port settings, refer to the *EMS Server IOM* manual.
- Ensure that your template file is also configured as described in this procedure to maintain the SNMP Keep-alive mechanism after the template file has been loaded to the device.

➢ **To prepare the devices for sending Keep-alive traps to the EMS:**

1. Create a new text file using a text-based editor (e.g., Notepad).
2. Include the following ini file parameters:

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

3. Save the ini file and close it.
4. Load the ini file to the device using WEB “incremental” procedure. (**Maintenance** menu > **Software Update** > **Load Auxiliary Files** > **INI** file (incremental).

A.3 Configuring SNMP Settings

This section describes how to configure device SNMP settings.

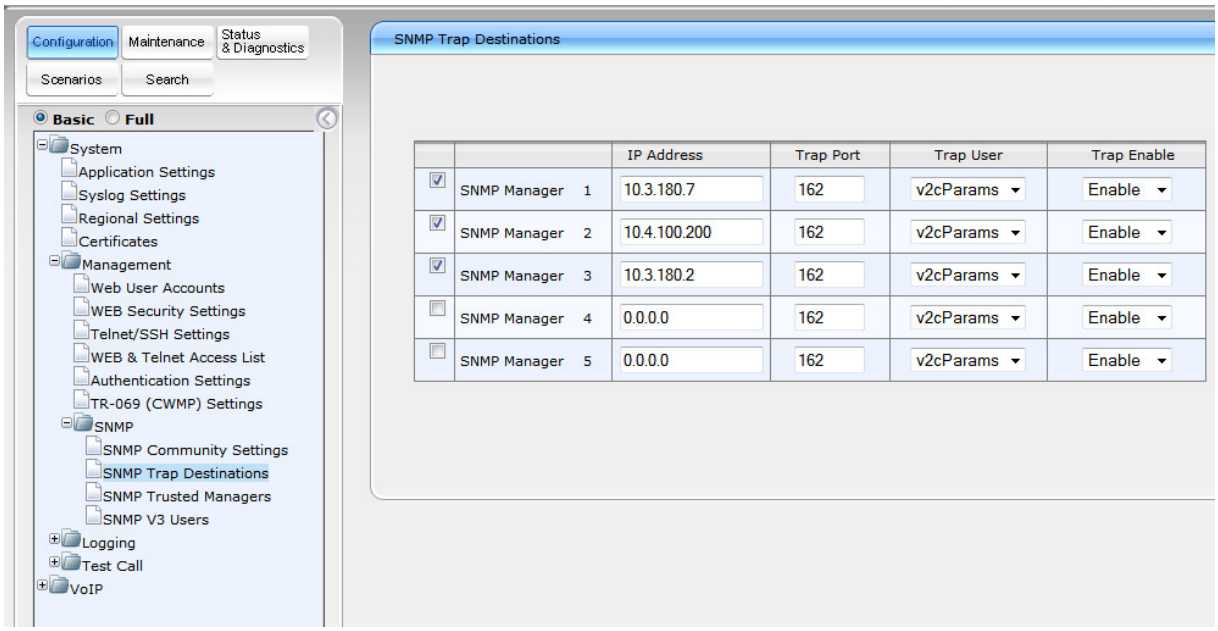
Notes:

- SNMPv2 or SNMPv3 user settings on the device should be identical to the EMS configuration (see Chapter 5).
- Ensure that your template file is also configured as described in this procedure to maintain an SNMP connection after the template file has been loaded to the device.
- If you have configured the EMS for HA with the Geo HA model, then you need to configure both the Primary and Secondary servers as separate trap destinations.

➢ To configure device SNMP settings:

1. Access the device's Web-based Management tool.
2. Open the SNMP Trap Destinations page (**Configuration** menu > **Management** > **SNMP** > **SNMP Trap Destinations**).

Figure A-1: SNMP Trap Destinations



3. Configure the EMS server as a trap destination:
   - Select the check box adjacent to the SNMP Manager that you wish to configure as the EMS server.
   - In the 'IP Address' field, enter the IP address of the EMS server.
   - In the 'Trap Port' field, enter **162**.
   - From the 'Trap User 'drop-down list, select v2cParams (SNMPv2) or v3cParams (SNMPv3) trap user (according to the definition in Chapter 5).

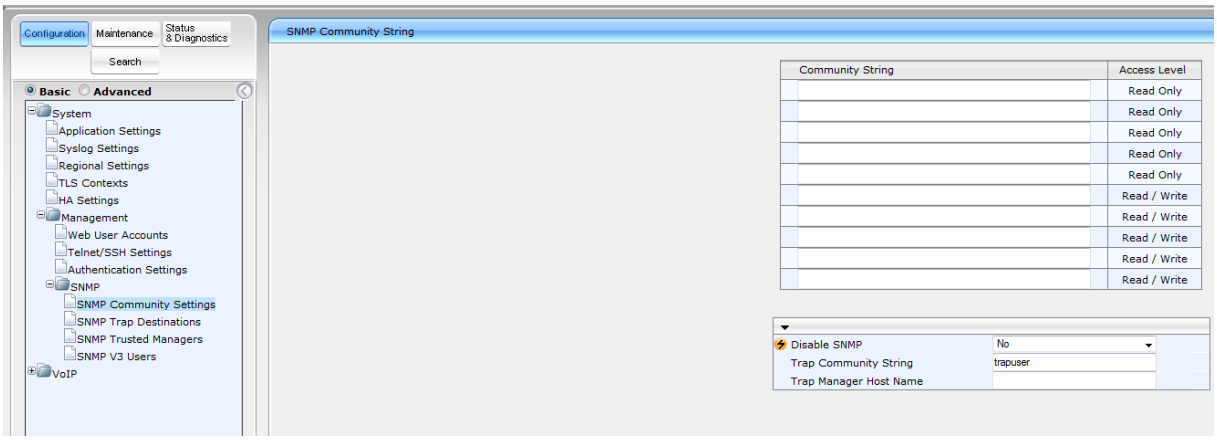
- From the 'Trap Enable' field drop-down list, select **Enable**.

Table A-3: SNMP Trap Destinations Parameters Description

Parameter	Description
Web: SNMP Manager **[SNMPManagerIsUsed_x]**	Enables the SNMP Manager to receive traps and checks the validity of the configured destination (IP address and port number). ▪ **[0]** (check box cleared) = (Default) Disables SNMP Manager ▪ **[1]** (check box selected) = Enables SNMP Manager
Web: IP Address **[SNMPManagerTableIP_x]**	Defines the IP address (in dotted-decimal notation, e.g., 108.10.1.255) of the remote host used as the SNMP Manager. The device sends SNMP traps to this IP address.
Trap Port **[SNMPManagerTrapPort_x]**	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid value range is 100 to 4000. The default is 162.
Web: Trap User **[SNMPManagerTrapUser]**	Associates a trap user with the trap destination. This determines the trap format, authentication level, and encryption level. ▪ v2cParams (default) = SNMPv2 user community string (see below). ▪ SNMPv3 user configured in 'Configuring SNMP V3 Users' (see below)
Trap Enable **[SNMPManagerTrapSendingEnable_x]**	Activates the sending of traps to the SNMP Manager. ▪ **[0]** Disable ▪ **[1]** Enable (Default)

7. Do one of the following:
   - If you are using SNMPv2, open the SNMP Community Settings page (**Configuration** menu > **Management** > **SNMP** > **SNMP Community Settings**).

Figure A-2: SNMPv2 Users Page

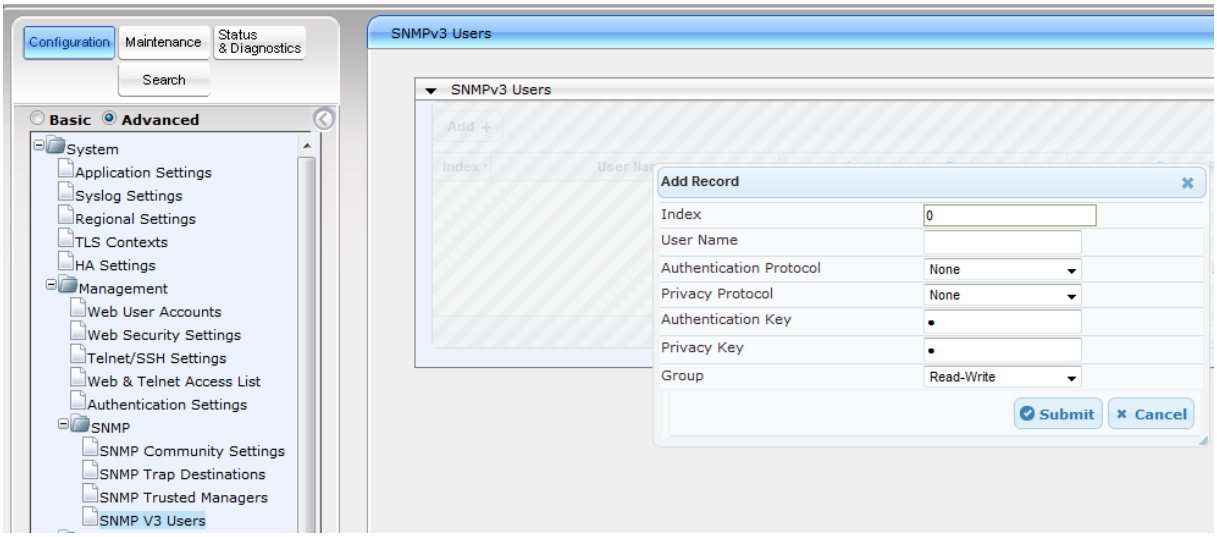


a. Enter the Trap Community String value that you configured in Chapter 5.

b. Enter the Trap Manager Host Name that you configured in Step 2.

- If you are using SNMPv3, open the SNMPv3 Users page (**Configuration** menu > **Management** > **SNMP** > **SNMP V3 Users**).

Figure A-3: SNMPv3 Users Page



c. Configure identical SNMPv3 Users settings that you configured in Chapter 5.

The page is intentionally left blank.

B Example AudioCodes Template INI File

An example AudioCodes template ini configuration file for an E-SBC device is shown below:

Note: To load and save an ini file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

```
;**************
;** Ini File **
;**************

;Board: Mediant 500
;HW Board Type: 69  FK Board Type: 77
;Serial Number: 4965606
;Slot Number: 1
;Software Version: 7.00A.003.005
;DSP Software Version: 5014AE3_R => 700.26
;Board IP Address: 10.15.17.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 50
;Num of physical LAN ports: 4
;Profile: NONE
;;Key features:;Board Type: Mediant 500 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) POC ;Channel Type: RTP DspCh=50 ;Coders: G723
G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB ;QOE
features: VoiceQualityMonitoring MediaEnhancement ;DSP Voice features:
IpmDetector RTCP-XR AMRPolicyManagement ;FXSPorts=3 ;FXOPorts=1
;BRITrunks=12 ;DATA features: ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;Control Protocols: MGCP MEGACO
H323 SIP TPNCP SASurvivability SBC=50 MSFT CLI TRANSCODING=50 FEU=600
TestCall=5 EMS ;Default features:;Coders: G711 G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;---------------------------------------------
;      2 : FXS         : 3
;      3 : FXO         : 1
;---------------------------------------------


[SYSTEM Params]

;NTPServerIP_abs is hidden but has non-default value
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.25.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
```

```
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

ENABLEMEDIASECURITY = 1

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value

[SIP Params]

MEDIACHANNELS = 30
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
```

```
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0;

[ \DeviceTable ]


[ InterfaceTable ]
```

```
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.0.1, "IP-PBX-NET",
0.0.0.0, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.156, 25, 195.189.192.129, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]


[ DspTemplates ]

;
;  *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 100, 6990, 1, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 100, 7990, 0, "", "";

[ \CpMediaRealm ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$PQhaCXJxcXBzIHQkLi0pfSkpfH5lZDdqYDcwNm9uY2xpa2c+VVABBgZXAFBZDF1aDlpeW
EVIREYWERdEGUAbGk0=", 1, 0, 2, 15, 60, 200,
"aa867960f2679a68cdaddce1808a0fe9";
WebUsers 1 = "User",
"$1$NQBQVQ5bCFoJWwkJcHJ6IHJzJ3Esei57fih/fTRpYDI3YzM0b2A4amg8O2sDBFZWUVJfV
V4KCVhbX1sLFEZBFUQ=", 1, 0, 2, 15, 60, 50,
"524240a38badac0f83f1041546a47901";

[ \WebUsers ]


[ TLSContexts ]
```

```
FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, , , 2560, 0;

[ \TLSContexts ]


[ IpProfile ]
```

```
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag;
IpProfile 1 = "IPProfile_IP-PBX-NET", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "",
-1, -1, 0, 1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1,
0, 3, 2, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -
1, 0, "";
```

```
IpProfile 2 = "IPProfile_WANSP", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2,
0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -
1, 1, 2, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 3,
0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0,
"";

[ \IpProfile ]


[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode,
SRD_SBCRegisteredUsersClassificationMethod, SRD_SBCRoutingPolicyName;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, -1, "Default_SBCRoutingPolicy";

[ \SRD ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "SIPInterface_IP-PBX-NET", "Voice", 2, 0, 0, 5067,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1,
0;
SIPInterface 1 = "SIPInterface_WANSP", "WANSP", 2, 5060, 0, 0,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1,
0;

[ \SIPInterface ]


[ ProxySet ]
```

```
FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "ProxySet_IP-PBX-NET", 1, 60, 1, 1, "DefaultSRD", 0,
"default", 1, -1, "", "", "SIPInterface_IP-PBX", "", "", "", "";
ProxySet 1 = "ProxySet_WANSP", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1,
"", "", "SIPInterface_WANSP", "", "", "", "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 0 = 0, "IPGroup_IP-PBX-NET", "ProxySet_IP-PBX-NET", "vendor.com",
"", -1, 0, "DefaultSRD", "MRLan", 1, "IPProfile_IP-PBX-NET", -1, 1, 2, 0,
0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "",
0, 0, -1, 0;
IPGroup 1 = 0, "IPGroup_WANSP", "ProxySet_WANSP", "vendor.com", "", -1,
0, "DefaultSRD", "MRWan", 1, "IPProfile_WANSP", -1, -1, 4, 0, 0, "", 0, -
1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1,
0;

[ \IPGroup ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FE15.IP-PBX-NET.local.com:5061", 2;
ProxyIp 1 = "1", 0, "vendor.com:5060", 0;

[ \ProxyIp ]


[ Account ]
```

```
FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "IPGroup_IP-PBX-NET", "IPGroup_WANSP", "441423514022",
"$1$tIWHhYONjw==", "audiocodes.com", 1, "441423514022", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS Termination", "Default_SBCRoutingPolicy",
"IPGroup_IP-PBX-NET", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "",
"internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "IP-PBX-NET to ITSP", "Default_SBCRoutingPolicy",
"IPGroup_IP-PBX-NET", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0,
"IPGroup_WANSP", "SIPInterface_WANSP", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to IP-PBX-NET", "Default_SBCRoutingPolicy",
"IPGroup_WANSP", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "IPGroup_IP-
PBX-NET", "SIPInterface_IP-PBX-NET", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0, "";

[ \CodersGroup0 ]


[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 1, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 1, "";

[ \CodersGroup1 ]


[ CodersGroup2 ]
```

```
FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";

[ \AllowedCodersGroup2 ]


[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]
```

This page is intentionally left blank.

AudioCodes One Voice Operations Center

Element Management System (EMS)

User's Manual

www.audiocodes.com