User's Manual

AudioCodes One Voice™ Operations Center

EMS

Version 7.2

HD VoIP Sounds Better

AudioCodes

Table of Contents

Troubleshooting 365

Appendix 371

List of Figures

List of Tables

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: October-15-2017

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
Device	Refers to trunking gateway, MediaPack and CPE products.
Endpoints	Refers to the IP Phone series: • 400 HD Series (Lync and Skype for Business) • Lync and Skype for Business clients
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 products: • 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 and Mediant 500L E-SBC • Mediant 500 MSBR and Mediant 500L MSBR • Mediant SE SBC and Mediant VE SBC • Mediant SBA products • CloudBond and CCE Appliance products
DS3	Synonymous with the term 'T3'.
'Frame' and 'Screen'	Sometimes used interchangeably

Document Revision Record

LTRT	Description
91028	Initial document release for Version 7.2.
91029	Updates include the following: launching the EMS client; enhanced clarifications for HTTPS configuration; SBC License Pool Manager update for device management; option to cancel hanging connection attempt; new Media Transcoding Cluster (MTC) product type; Session Timeout enhancements; enhanced Actions Journal for security events and LDAP SSL enhancements.
91030	Time License; SBC License Pool Manager Enhancements; Enhanced SBA Information; Support for MP-1288 and MP-202 devices; support for Windows 10.
91031	Updates to the License Pool Manager for supporting CloudBond 365 and CCE Appliance products and for configuring unknown devices; updates to the Software Manager section for supporting rmt/rms/conf files and procedure for adding and filtering files; Updates to section for methods for connecting devices to EMS; moved SNMP Configuration section and merged device and EMS SNMP configuration to the same section; update for section Status Monitoring and Navigation Concepts for CloudBond 365 and CCE Appliance products; updates to the procedure for backing up device configuration files.
91032	Update to Section ‘Maintenance Actions’ for the Upgrade action explanation; update to Section ‘Real-Time Performance Monitoring’; update to Section ‘Single Sign-On related descriptions and for connecting to devices behind a NAT using the Single Sign-on feature.
91033	Updated to Section ‘Software Upgrade for Devices’ and EMS Firewall Configuration Schema. Updated description for automatic alarms and events clearing.
91038	Added note to indicate that the PM Polling interval is 15 minutes and cannot be changed.

Documentation Feedback

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

Related Documentation

Manual Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User’s Manual
Mediant 800B MSBR User’s Manual
Mediant 1000B Gateway and E-SBC User’s Manual
Mediant 1000B MSBR User’s Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User’s Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAM Integration Guide
Element Management System (EMS) User’s Manual
SEM User's Manual
IP Phone Management Server Administrator's Manual
IP Phone Manager Express Administrator's Manual
OVOC Security Guidelines
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 Gateway and E-SBC Performance Monitors and Alarms Guide
Mediant 800 Gateway and E-SBC Mediant Software SBC CloudBond 365 and CCE Alarms Guide
Mediant 1000B Gateway and E-SBC Performance Monitors and Alarms Guide
Mediant 2600-4000-9000-SW SBC Series Performance Monitors and Alarms Guide
Mediant 3000 with TP-6310 Performance Monitors and Alarms Guide
Mediant 3000 with TP-8410 Performance Monitors and Alarms Guide
Mediant 1000B MSBR Performance Monitors and Alarms Guide
Mediant 500/Mediant 500L and Mediant 800B MSBR Performance Monitors and Alarms Guide

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 inclusive, 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 feature-rich management framework, including fault management and security. Additionally, the REST protocol is implemented between the EMS and Endpoints (IP Phones) and between the EMS and devices for supporting specific features.

1.1 Feature Specifications

- Software Version Number: **7.2**
- Release Date: **Q1 2017**
- 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. 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 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 2013 Server. ▪ Filtering according to time range, devices and links.
Devices Maintenance Actions	▪ 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, 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	**MP-1xx:** 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. **MP-20x:**The MP-20x VoIP Gateway is an all-in-one unit featuring (depending on model) a VoIP adapter, FXS lines, FXO interfaces, Ethernet LAN interfaces (with an internal Layer-2 switch), and Ethernet WAN interface (Refer to the product documentation for detailed information.)

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Mediant 500 E-SBC **Mediant 500L E-SBC**	The Mediant 500 and Mediant 500L Enterprise Session Border Controller (E-SBC,is a member of AudioCodes family of E-SBCs, enables 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.
 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 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.
 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.

Table 1-3: Supported VoIP Equipment

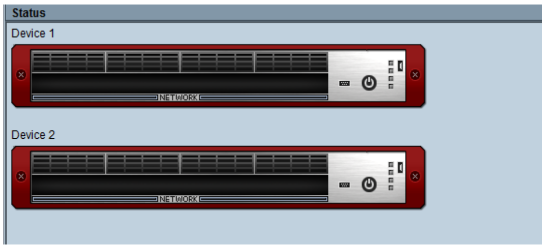
Supported VoIP Equipment	Description
 **AudioCodes Mediant Software Enterprise Session Border Controllers**	AudioCodes Mediant Software Enterprise Session Border Controllers (E-SBC) are pure-software products, enabling connectivity and security between Enterprises' and Service Providers' VoIP networks. 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.
 MP-1288	AudioCodes MediaPack 1288 (MP-1288), is a cost-effective best-of-breed, high density analog media voice-over-IP (VoIP) gateway. The device provides superior voice technology for connecting legacy telephones, fax machines and modems with IP-based telephony networks, as well as for integration with IP PBX systems. It is designed and tested to be fully interoperable with leading softswitches, unified communications (UC) servers and SIP proxies. The device is designed for carrier environments including 1+1 power supplies and 1+1 Ethernet redundancy, maintaining high voice quality to deliver reliable enterprise VoIP communications. Advanced call routing mechanisms, network voice quality monitoring and survivability capabilities (including PSTN fallback) result in minimum communications downtime.

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.
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.

Table 1-3: Supported VoIP Equipment

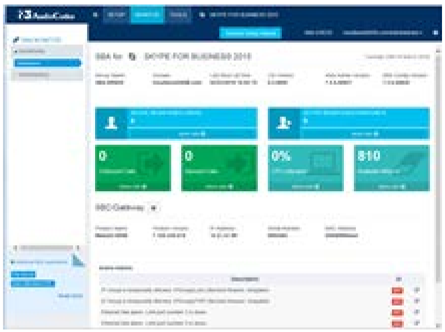
Supported VoIP Equipment	Description
Survivable Branch Appliance (SBA)  SBA for SKYPE FOR BUSINESS 2015 0 0 0% 810 SBC/Gateway	The Survivable Branch Appliance (SBA) is an AudioCodes product designed for Microsoft Lync Server which allows remote branch resiliency in a Microsoft Lync Server network (Microsoft 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

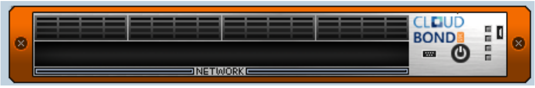
Supported VoIP Equipment	Description
     	AudioCodes AudioCodes 420HD 430HD 440HD and 450HD IPPhones are based on AudioCodes' High Definition voice technology, providing clarity and a rich audio experience in Voice-over-IP (VoIP) calls. All models include a large monochrome multi-language graphic LCD 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, Skype for Business and non-Microsoft environments.
 	AudioCodes CloudBond™ 365 is a modular, adaptable solution for the data center, customer premises or the branch. A versatile all-in-one Skype for Business appliance designed for hybrid environments, it combines the best of the Skype for Business server, the Cloud-PBX and the service provider's voice services.

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
	The AudioCodes Mediant Server CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage. Based on a powerful HP server, the AudioCodes Mediant Server CCE Appliance delivers the Cloud Connector integrated with the AudioCodes SBC for organizations or enterprise branches with up to 2500 users and supports up to 500 concurrent sessions.
	The AudioCodes Mediant 800 CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage. For organizations or enterprise branches with up to 1000 users, the AudioCodes Mediant 800 with the integrated OSN server module can host the Cloud Connector on the same self-contained appliance supporting up to 185 concurrent sessions

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 257
- 'Configuration management' on page 75
- Accounting (managed by a higher-level management system such as an NMS)
- 'Performance Management' on page 303
- 'Security Management' on page 323

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 Launching the EMS Client

This chapter describes how to launch the EMS client on your PC. The EMS platform consists of a PC client and a server platform. For detailed instructions for installing the server platform , 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 Launching the EMS Client Using the Supplied DVD

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

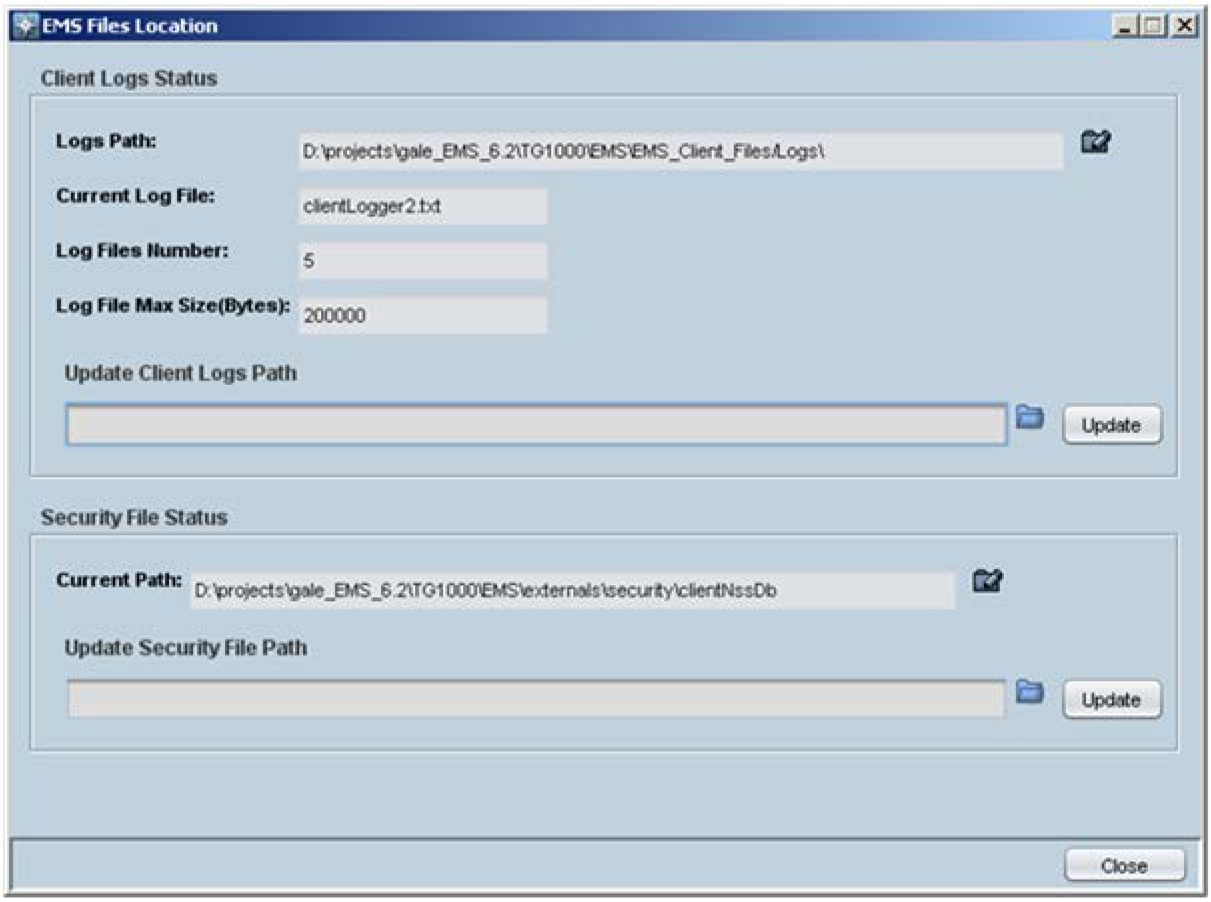
➢ **To install the EMS client from the supplied DVD:**

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; at the end of the installation process, the EMS Client icon is added to the PC 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. If for any reason for example, security or any other reason, you wish 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



Client Logs Status

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

Current Log File: clientLogger2.txt

Log Files Number: 5

Log File Max Size(Bytes): 200000

Update Client Logs Path

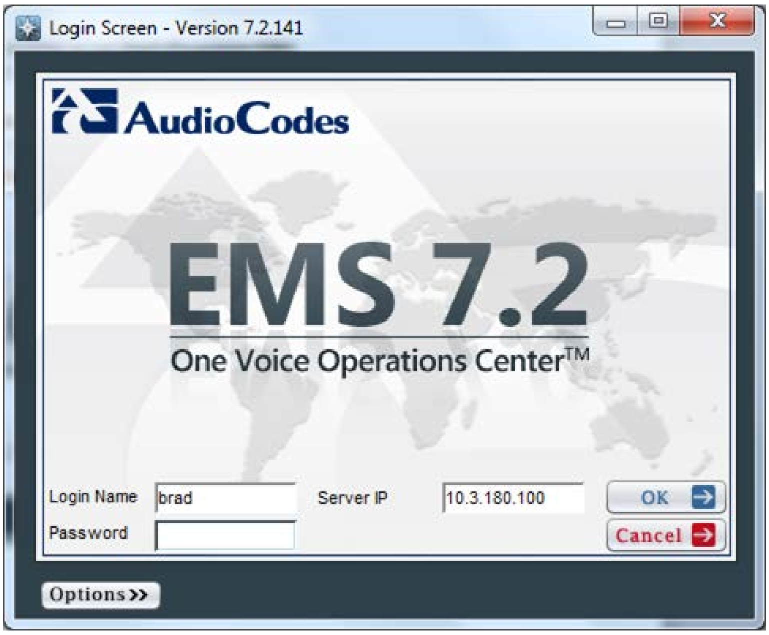
Security File Status

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

Update Security File Path

3. Double-click the EMS Client icon on your desktop, or run **start>All programs >EMS Client_Version > runClient**; the EMS Login screen is displayed.

Figure 2-2: Login Screen



Login Name: brad

Password:

Server IP: 10.3.180.100

2.2 Launching the EMS Client 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.

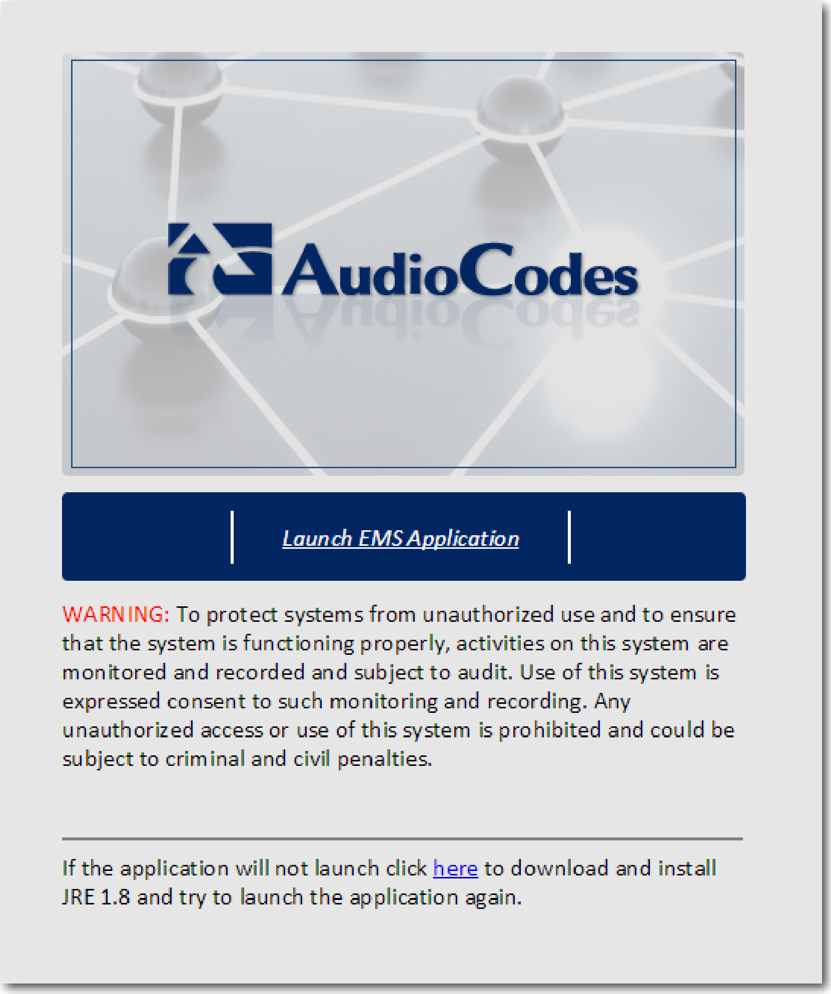
Specify the path 'http://<server_ip>; an 'EMS Login Screen' is opened.

For example: http://10.7.6.18

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

1. Open a Web browser and enter the IP address of the EMS server. For example: http://10.7.6.18

Figure 2-3: Launch EMS Application

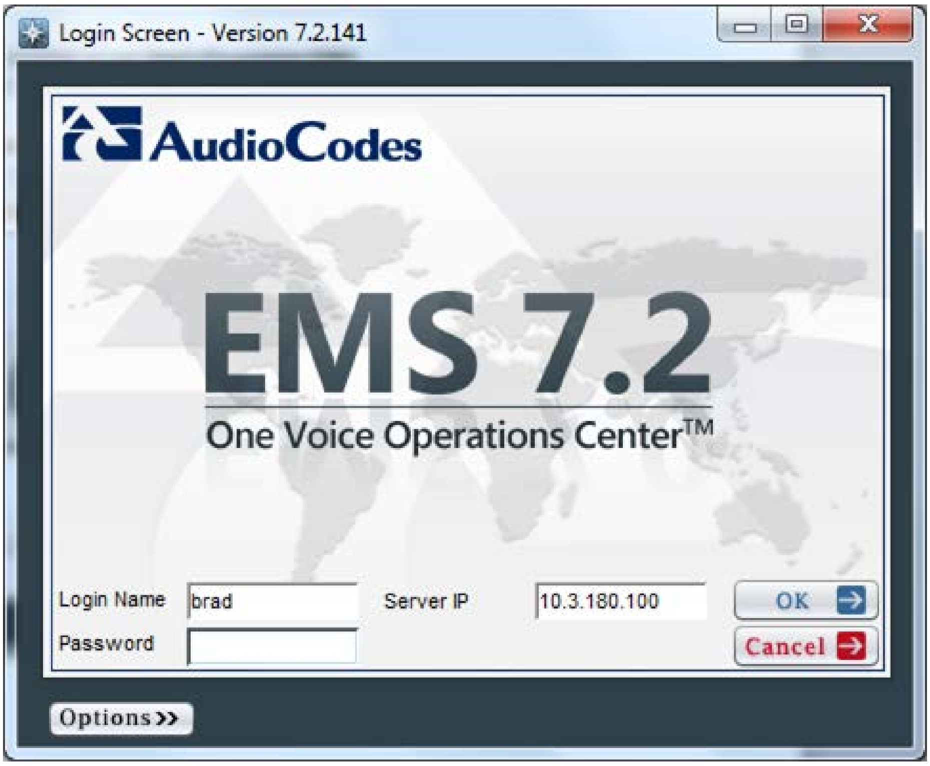


WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.

If the application will not launch click here to download and install JRE 1.8 and try to launch the application again.

2. Click the **Launch EMS Application** button The EMS Login screen is displayed.

Figure 2-4: EMS Login Screen



Login Name: brad

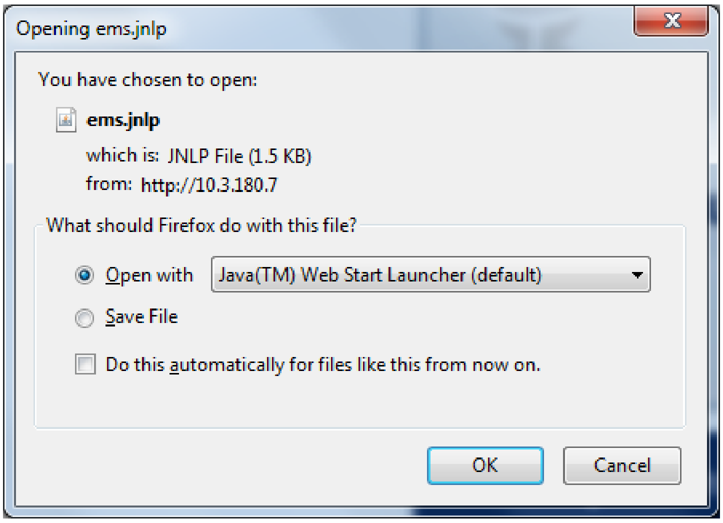
Password:

Server IP: 10.3.180.100

Note the following:

- If you are using an Internet Explorer browser, the EMS Login screen appears immediately.
- If you are using a Firefox browser, the following screen is displayed:

Figure 2-5: Launching EMS from Firefox Browser



You have chosen to open:

ems.jnlp

which is: JNLP File (1.5 KB)

from: http://10.3.180.7

What should Firefox do with this file?

● Open with Java(TM) Web Start Launcher (default)

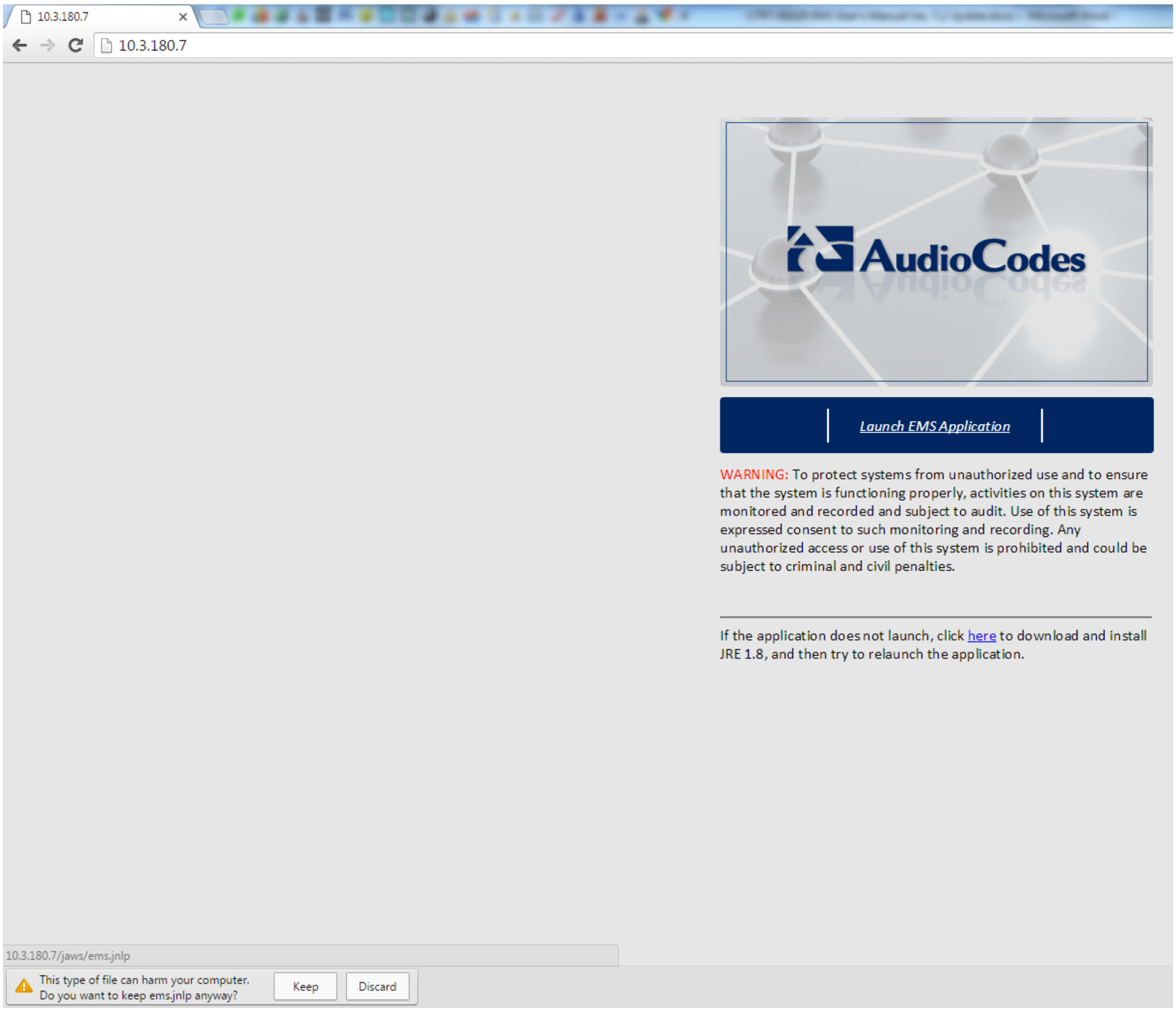
○ Save File

□ Do this automatically for files like this from now on.

- Click **OK** to open the link.

- If you are using a Chrome browser, the following screens appear:

Figure 2-6: Launching EMS from Chrome Browser (1)



10.3.180.7

Launch EMS Application

WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.

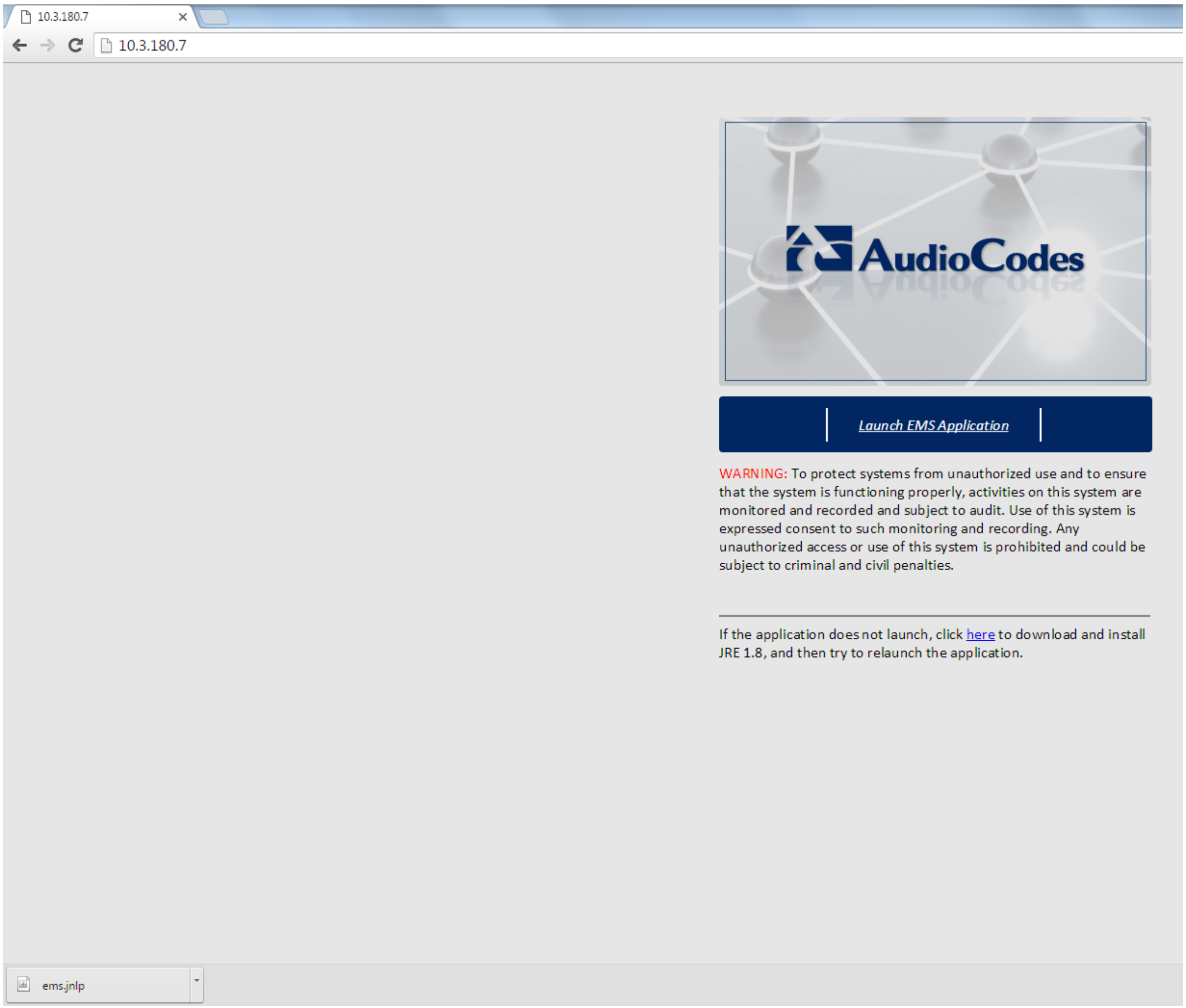
If the application does not launch, click here to download and install JRE 1.8, and then try to relaunch the application.

10.3.180.7/jaws/ems.jnlp

This type of file can harm your computer. Do you want to keep ems.jnlp anyway?

a. Click **Keep**; the following screen is displayed:

Figure 2-7: Launching EMS from Chrome Browser (2)



WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.

If the application does not launch, click here to download and install JRE 1.8, and then try to relaunch the application.

b. Right click the drop-down list arrow adjacent to the "ems.jnlp" link and click **Open**.

Note: Launching the EMS client using Java Webstart requires the pre-installation of the Java Runtime Environment Version 1.8 on your PC.

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

You can login to the EMS using one of the following methods:

- Login using a username and password (see below).
- Login using a CAC card (see below).
- Login using the Geo HA option (see Section 3.1.3 on page 47)

> **Note:** If the EMS license has expired, you will be denied connection to the EMS server. To renew your EMS license, contact your AudioCodes representitive.

3.1.1 Logging in Using Username and Password

This section describes how to login to EMS using a username and password.

➢ **To login using a username and password:**

1. 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.

2. Enter the IP address of the EMS server to which you wish to connect.
   - If your EMS server is enabled for HA, see Section 3.1.3 or click **OK**.

3.1.2 Logging in Using CAC Card

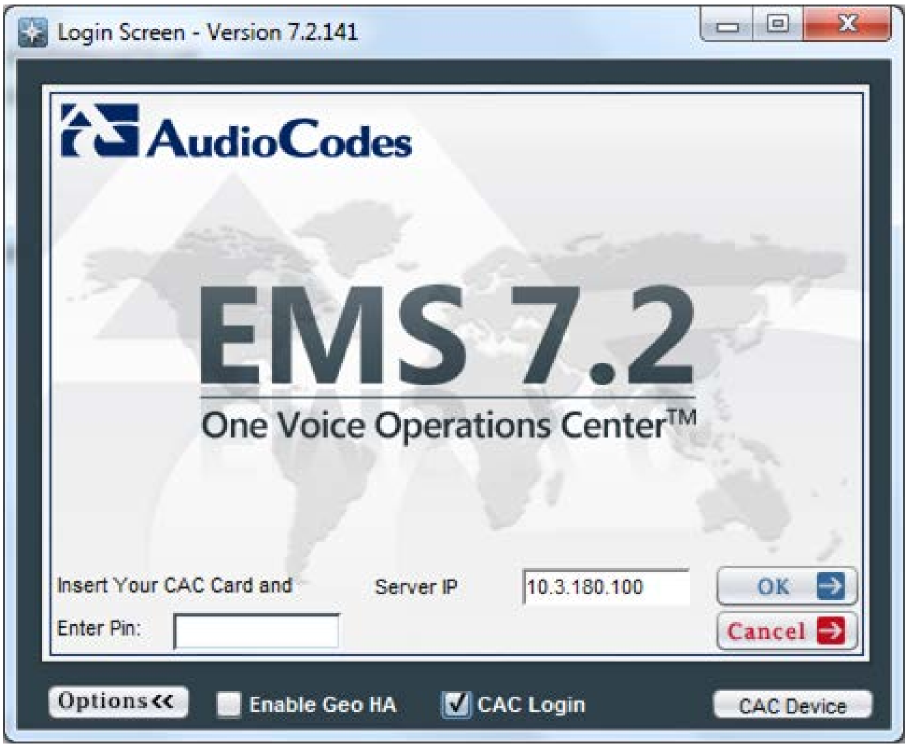
This section describes how to login to the EMS using a CAC card.

➢ **To login to the EMS using a CAC card:**

1. 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.

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

Figure 3-1: CAC Login Screen



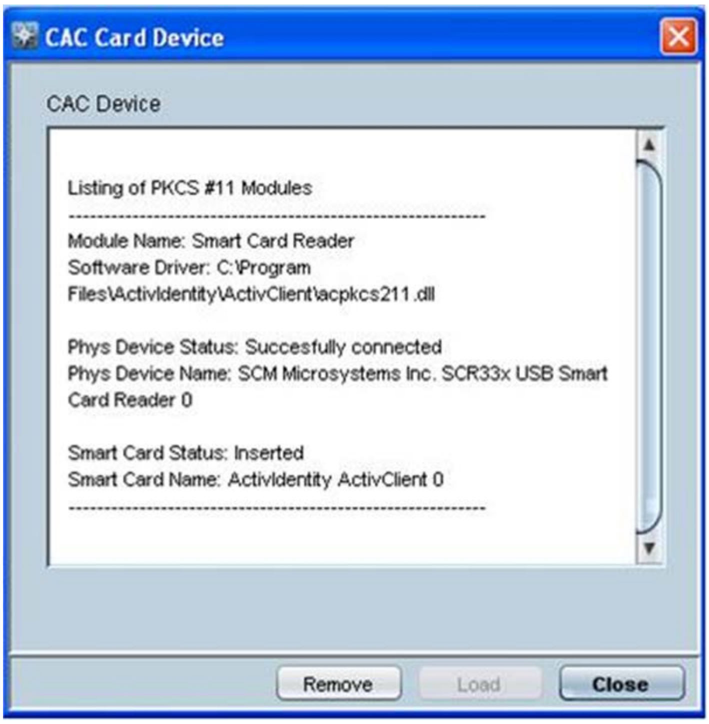
Insert Your CAC Card and Enter Pin:

Server IP 10.3.180.100

□ Enable Geo HA ☑ CAC Login

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

Figure 3-2: CAC Card Device



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

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

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

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

c. If your EMS server is enabled for HA, see Section 3.1.3 below or click **OK**.

3.1.3 Logging in Using the Geo HA option

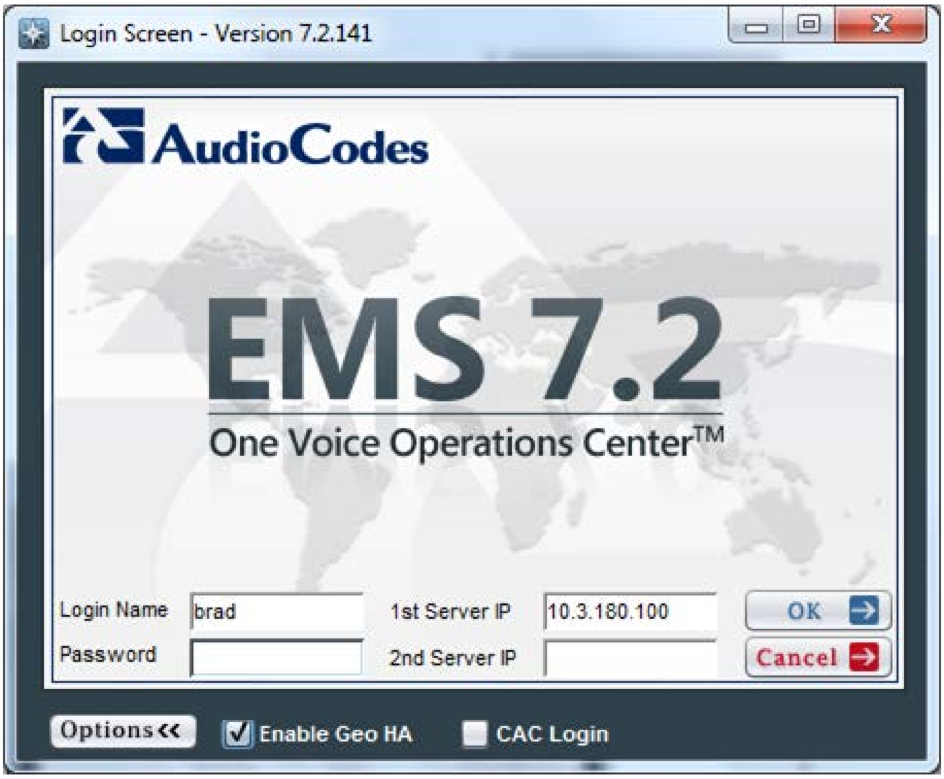
In the case the EMS application has been enabled for HA (High Availability) (via the EMS Server Manager-refer to the *EMS Server IOM*), and only when two EMS servers are located in different subnets, you can use the Geo HA option to login to the EMS client.

➢ **To login to the EMS using the Geo HA option:**

3. Select the **Enable Geo HA** checkbox.
4. 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 3-3: Geo HA Option



Login Screen - Version 7.2.141

Login Name: brad

Password:

1st Server IP: 10.3.180.100

2nd Server IP:

☑ Enable Geo HA

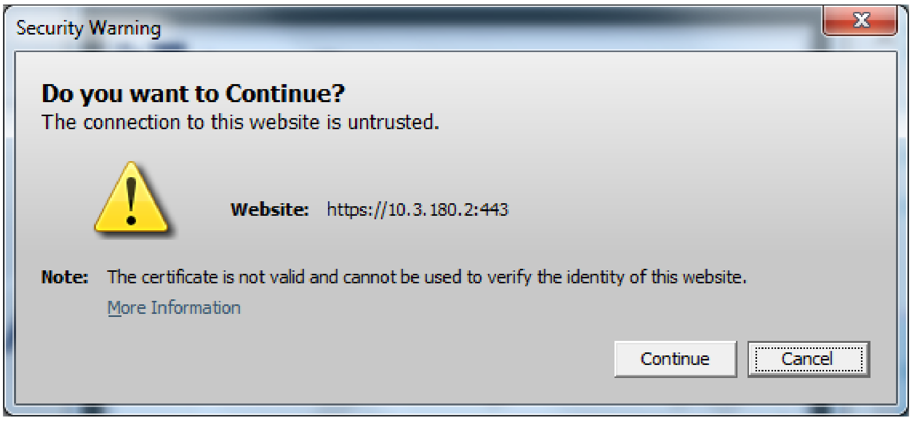
□ CAC Login

5. 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).

Note that when you click **OK**, the following screen is displayed:

Figure 3-4: Security Warning



Security Warning

Do you want to Continue?
The connection to this website is untrusted.

Website: https://10.3.180.2:443

Note: The certificate is not valid and cannot be used to verify the identity of this website.

6. Click **Continue** to open the EMS.

3.2 Getting Oriented in the EMS

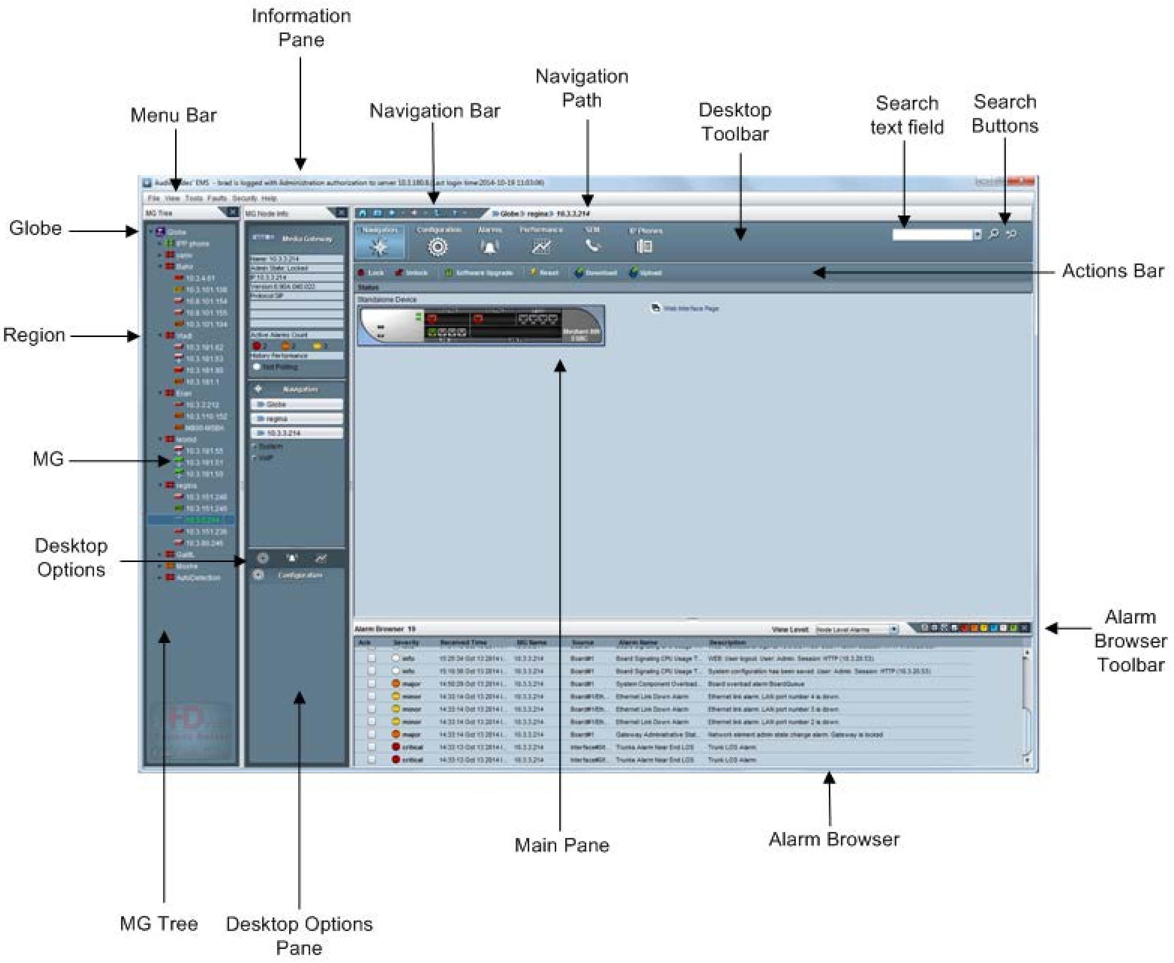
This subsection acquaints operators with the EMS. Read this section for a quick orientation to navigating in the EMS. This section explains the following:

- 'Navigating Down and Up System Hierarchy' on page 48.
- 'Selecting an Interface in the Context of an Element' on page 55 (and the concept of context-oriented screens).
- 'Using Color Coding to Assess Element Status' on page 56.

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



Alarm Browser 15 View Level: Node Level Alarms

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	○ info	15:25:34 Oct 13 2014 I...	10.3.3.214	Board#1	Board Signaling CPU Usage T...	WEB: User logout. User: Admin. Session: HTTP (10.3.20.53)
□	○ info	15:16:38 Oct 13 2014 I...	10.3.3.214	Board#1	Board Signaling CPU Usage T...	System configuration has been saved. User: Admin. Session: HTTP (10.3.20.53)
□	● major	14:50:29 Oct 13 2014 I...	10.3.3.214	Board#1	System Component Overload...	Board overload alarm BoardQueue
□	● minor	14:33:14 Oct 13 2014 I...	10.3.3.214	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.
□	● minor	14:33:14 Oct 13 2014 I...	10.3.3.214	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.
□	● minor	14:33:14 Oct 13 2014 I...	10.3.3.214	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.
□	● major	14:33:14 Oct 13 2014 I...	10.3.3.214	Board#1	Gateway Administrative Stat...	Network element admin state change alarm. Gateway is locked
□	● critical	14:33:13 Oct 13 2014 I...	10.3.3.214	Interface#0/...	Trunks Alarm Near End LOS	Trunk LOS Alarm
□	● critical	14:33:13 Oct 13 2014 I...	10.3.3.214	Interface#0/...	Trunks Alarm Near End LOS	Trunk LOS Alarm

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 257.

- **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 303.

- **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

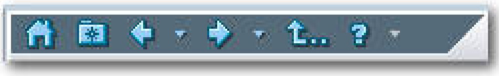


Table 3-1: Navigation Pane Description

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. 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

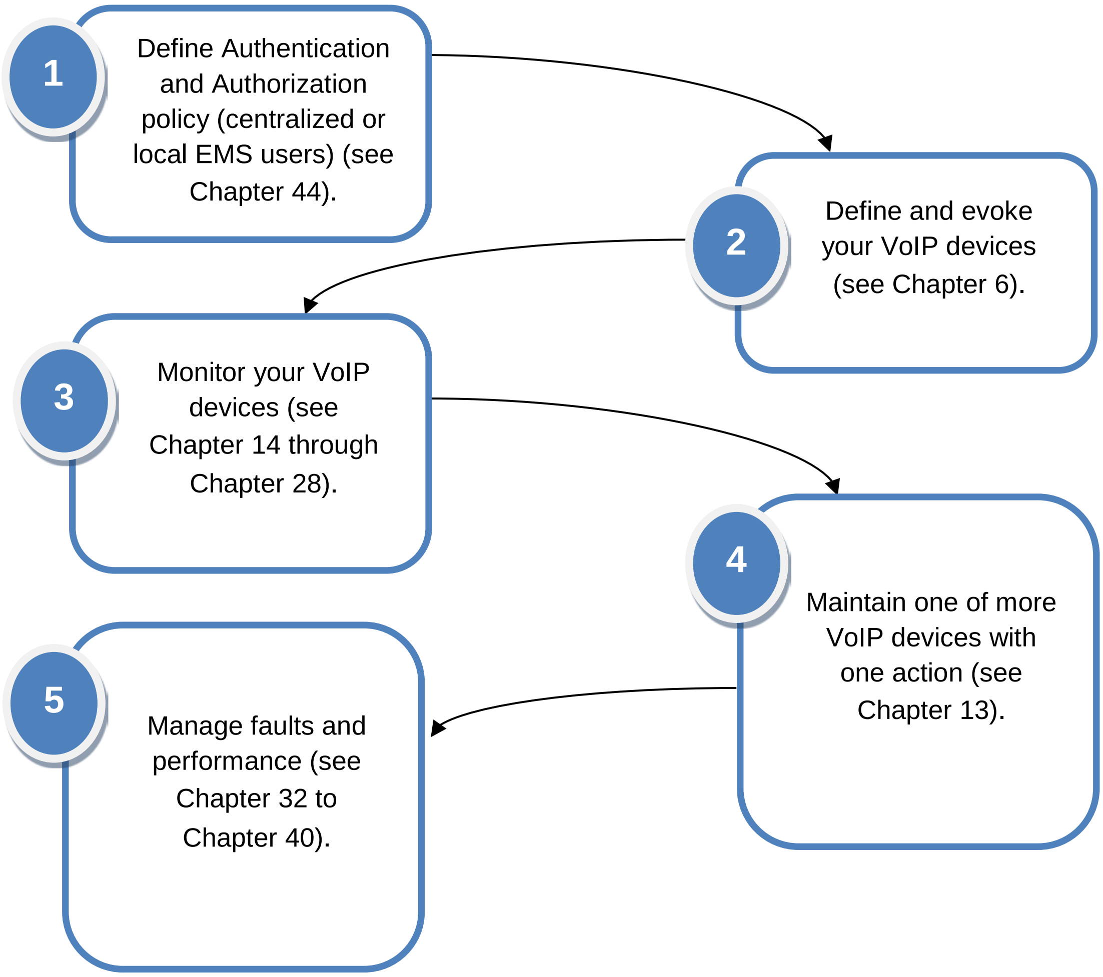
System Entity Status	Color	Region Icon	AudioCodes Device Icon
Clear (OK)	Green	🟩	🟩 🟩 🟩 124 108
Warning	Blue	🟦	🟦 🟦
Minor	Yellow	🟨	🟨 🟨
Major	Orange	🟧	🟧 🟧
Critical	Red	🟥	🟥 🟥 🟥 124 108
Shutting Down	Gray Gradient		⬛ ⬛
Locked	Gray		⬛ ⬛
Unable to Connect	Red Gradient		🟥 🟥 🟥 124 108
Unknown entity	? ?	🟪	

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

3.3 Basic Workflow

The below procedure shows the basic workflow for managing your VoIP equipment with the EMS:

Figure 22-7: Basic Workflow


1
Define Authentication and Authorization policy (centralized or local EMS users) (see Chapter 44).
2
Define and evoke your VoIP devices (see Chapter 6).
3
Monitor your VoIP devices (see Chapter 14 through Chapter 28).
4
Maintain one of more VoIP devices with one action (see Chapter 13).
5
Manage faults and performance (see Chapter 32 to Chapter 40).

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:

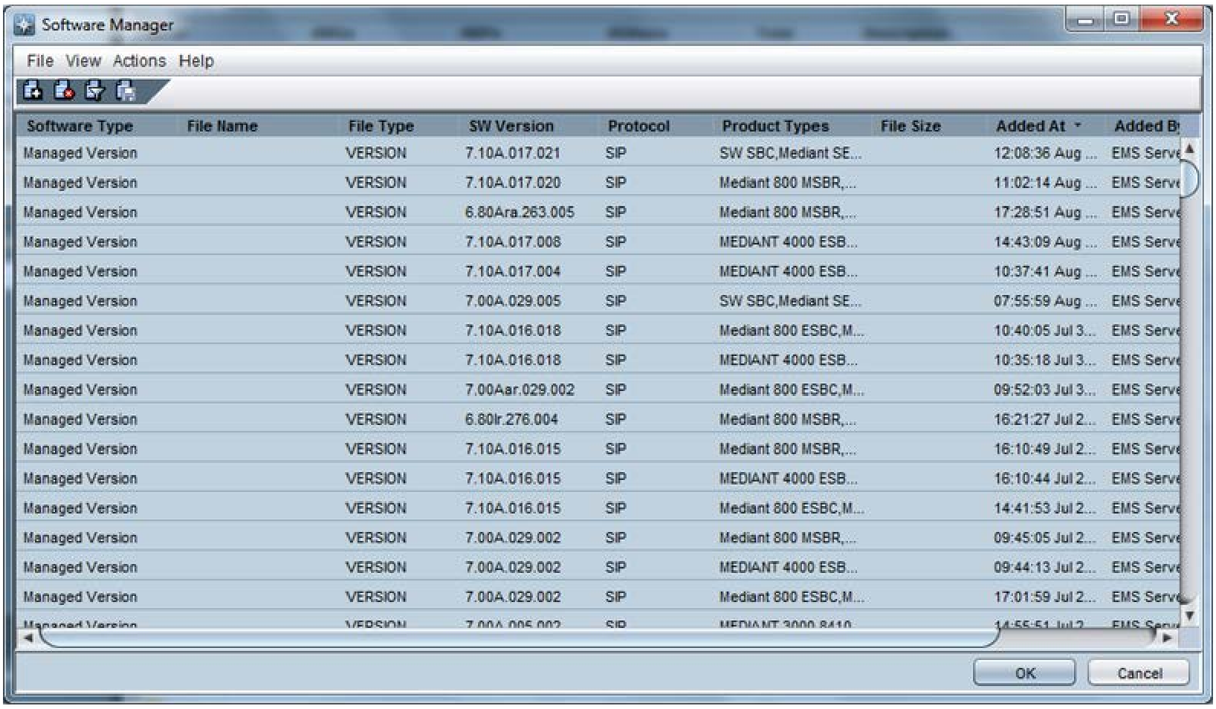
- **Software Type:**

  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, rmt/rms, tar* or *tar.gz*, *cpt, vp*, *cas, dat 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.

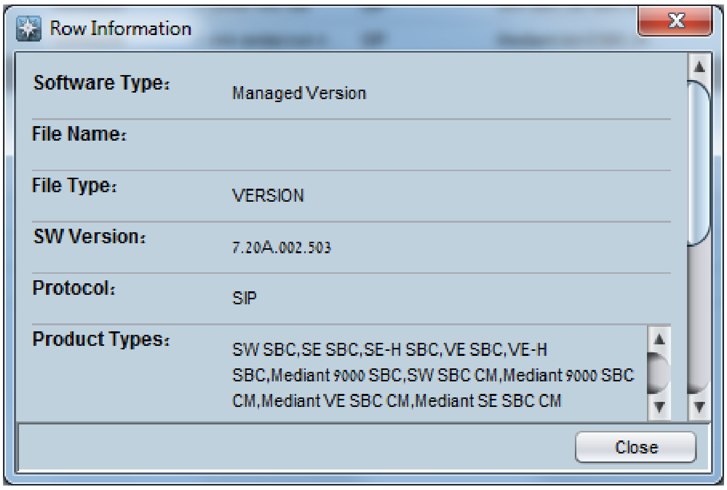
Figure 4-1: Software Manager



Software Type	File Name	File Type	SW Version	Protocol	Product Types	File Size	Added At	Added By
Managed Version		VERSION	7.10A.017.021	SIP	SW SBC,Mediant SE...		12:08:36 Aug ...	EMS Serve
Managed Version		VERSION	7.10A.017.020	SIP	Mediant 800 MSBR,...		11:02:14 Aug ...	EMS Serve
Managed Version		VERSION	6.80Ara.263.005	SIP	Mediant 800 MSBR,...		17:28:51 Aug ...	EMS Serve
Managed Version		VERSION	7.10A.017.008	SIP	MEDIANT 4000 ESB...		14:43:09 Aug ...	EMS Serve
Managed Version		VERSION	7.10A.017.004	SIP	MEDIANT 4000 ESB...		10:37:41 Aug ...	EMS Serve
Managed Version		VERSION	7.00A.029.005	SIP	SW SBC,Mediant SE...		07:55:59 Aug ...	EMS Serve
Managed Version		VERSION	7.10A.016.018	SIP	Mediant 800 ESBC,M...		10:40:05 Jul 3...	EMS Serve
Managed Version		VERSION	7.10A.016.018	SIP	MEDIANT 4000 ESB...		10:35:18 Jul 3...	EMS Serve
Managed Version		VERSION	7.00Aar.029.002	SIP	Mediant 800 ESBC,M...		09:52:03 Jul 3...	EMS Serve
Managed Version		VERSION	6.80Ir.276.004	SIP	Mediant 800 MSBR,...		16:21:27 Jul 2...	EMS Serve
Managed Version		VERSION	7.10A.016.015	SIP	Mediant 800 MSBR,...		16:10:49 Jul 2...	EMS Serve
Managed Version		VERSION	7.10A.016.015	SIP	MEDIANT 4000 ESB...		16:10:44 Jul 2...	EMS Serve
Managed Version		VERSION	7.10A.016.015	SIP	Mediant 800 ESBC,M...		14:41:53 Jul 2...	EMS Serve
Managed Version		VERSION	7.00A.029.002	SIP	Mediant 800 MSBR,...		09:45:05 Jul 2...	EMS Serve
Managed Version		VERSION	7.00A.029.002	SIP	MEDIANT 4000 ESB...		09:44:13 Jul 2...	EMS Serve
Managed Version		VERSION	7.00A.029.002	SIP	Mediant 800 ESBC,M...		17:01:59 Jul 2...	EMS Serve
Managed Version		VERSION	7.00A.005.002	SIP	MEDIANT 3000 8410		14:55:51 Jul 2	EMS Serv

To view additional details for each file, double-click an entry. A screen similar to the following screen is displayed:

Figure 4-2: Software Manager File Details



Software Type: Managed Version

File Name:

File Type: VERSION

SW Version: 7.20A.002.503

Protocol: SIP

Product Types: SW SBC,SE SBC,SE-H SBC,VE SBC,VE-H SBC,Mediant 9000 SBC,SW SBC CM,Mediant 9000 SBC CM,Mediant VE SBC CM,Mediant SE SBC CM

File types managed by the Software Manager are as follows:

- Configuration files for devices:
  - *cmp* file only
    - *cmp* file - This is the main software firmware image file for most devices (except MP-20x devices, see below). Load the file to change the software version (for example).
    - *rmt/rms* - This is the software image file for MP-20x devices.
    - Software version - automatically defined after adding the *cmp* or *rmt/rms* file
    - Major version - automatically defined after adding the *cmp* file
    - Select a product (corresponding to the *cmp or rmt/rms* file from list).
    - Select a protocol from the list e.g. SIP
  - *cmp/rmt/rms* & *ini/conf (*for MP-20x devices*)* & *ems* files

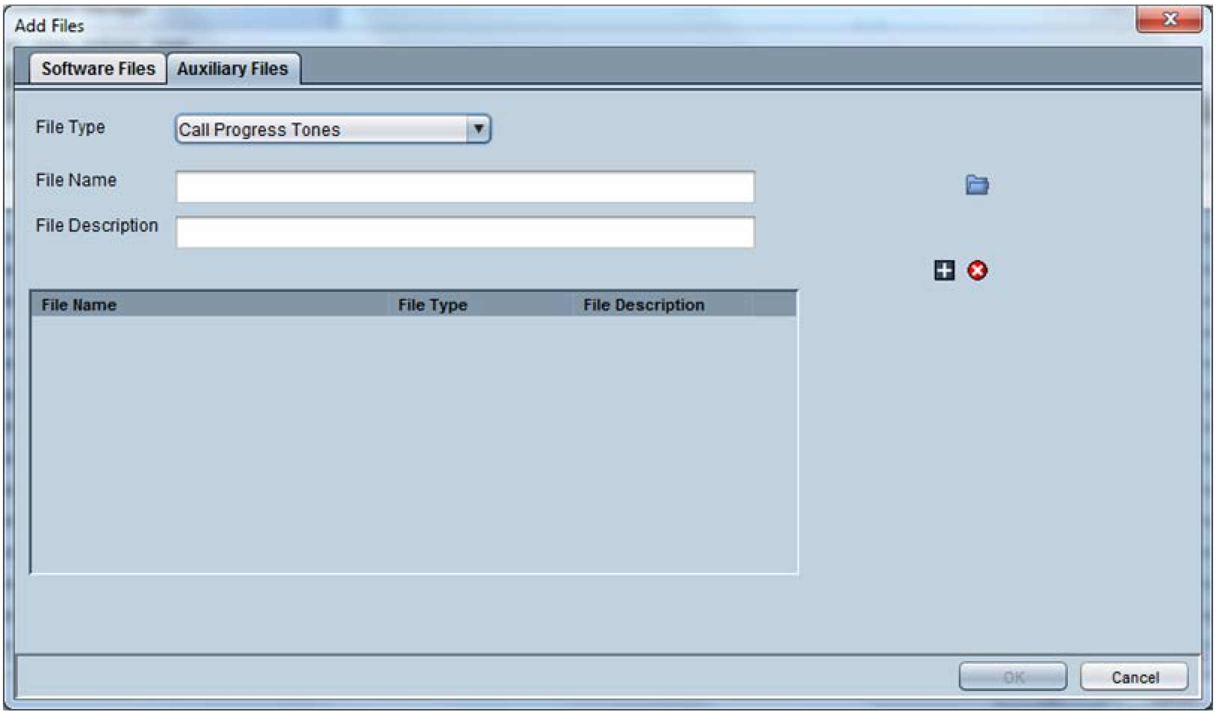
Note: This option is reserved for backward compatibility reasons, and must be used by AudioCodes FAEs only.

- **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 4-3: Software Manager-Adding Auxiliary Files



Add Files

Software Files | Auxiliary Files

File Type: Call Progress Tones

File Name:

File Description:

File Name	File Type	File Description

Table 4-1: Auxiliary Files

File Type	MediaPack (Analog Gateway)	CPEs	EMS Server
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	✓ (Reset)	✓ (Reset)	

File Type	MediaPack (Analog Gateway)	CPEs	EMS Server
File (All Products)			
Certificate File (LDAP server authentication and Single-Sign-On to AudioCodes device)			✓
CAS (All Digital Products)	-	✓ (Lock/Unlock Trunks)	
Dial Plan File (All Digital Products)	-	✓	
Coefficient File (Analog MP / M1K)	✓ (Reset)	-	
User Information (All Products SIP)	✓ (Reset)	✓ (Reset)	
External Coders (All Products MGCP / MEGACO)	✓ (Reset)	✓ (Reset)	
License Keys (All Products)	-	✓	
INI Stand Alone	✓	✓	
V5.2 File	-	Mediant 3000 8410 MEGACO only	
AMD Sensitivity File	-	✓	

File Type	MediaPack (Analog Gateway)	CPEs	EMS Server
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).
- **Security**
  - 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)
  - Certificate File – used for SSL authentication with an LDAP server (see Section” LDAP Server”) and for Single-Sign-On from the EMS to the AudioCodes device's embedded Web server tool (for more information on HTTPS, see Chapter 42). When this option is used, the EMS keystore is updated.
- **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**: Includes initial configuration of device 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).
  - **CONF** – Configuration file for MP-20x devices.
  - **RMT/RMS**- firmware files MP-20x gateways
  - **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 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
```

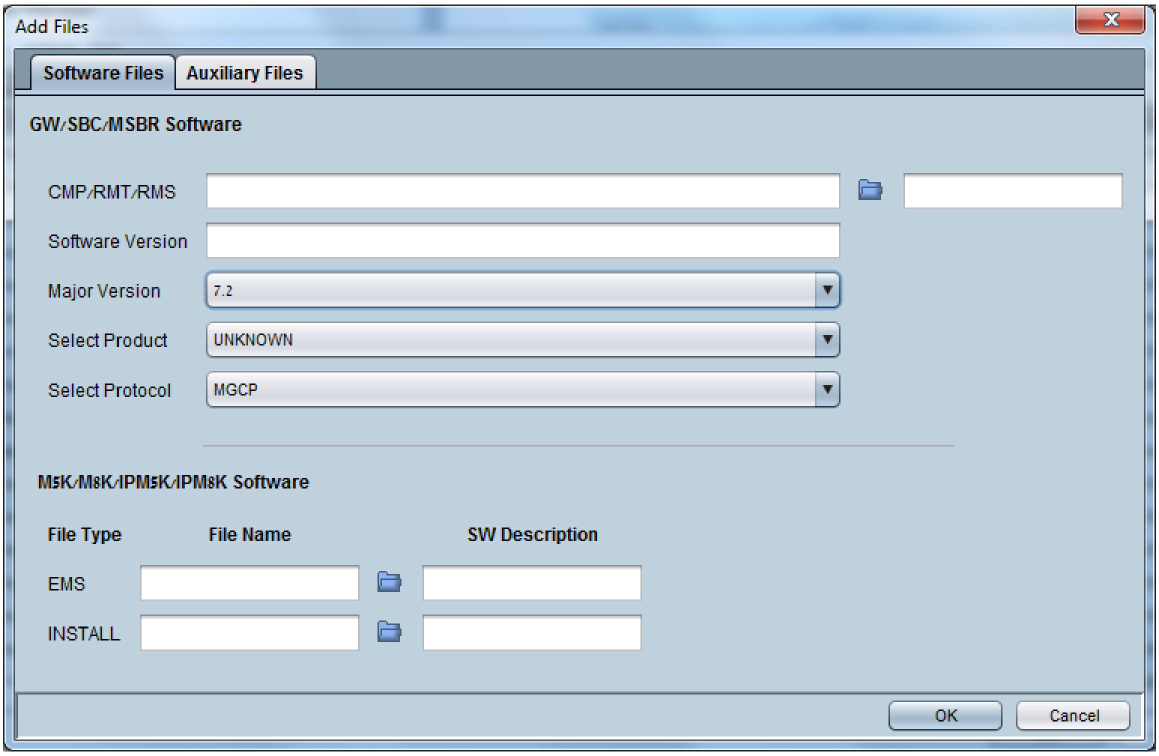
4.1 Adding a Software File

This section describes how to add a new CMP/RMT/RMD file to the Software Manager.

➢ To add new files to the Software Manager:

1. In the Software Manager toolbar, click the **Add** File icon or open the Actions menu and choose the option **Add File**; the Add Files screen (shown in the figure below) opens.

Figure 4-4: Add Software File



Add Files

Software Files | Auxiliary Files

GW/SBC/MSBR Software

CMP/RMT/RMS:

Software Version:

Major Version: 7.2

Select Product: UNKNOWN

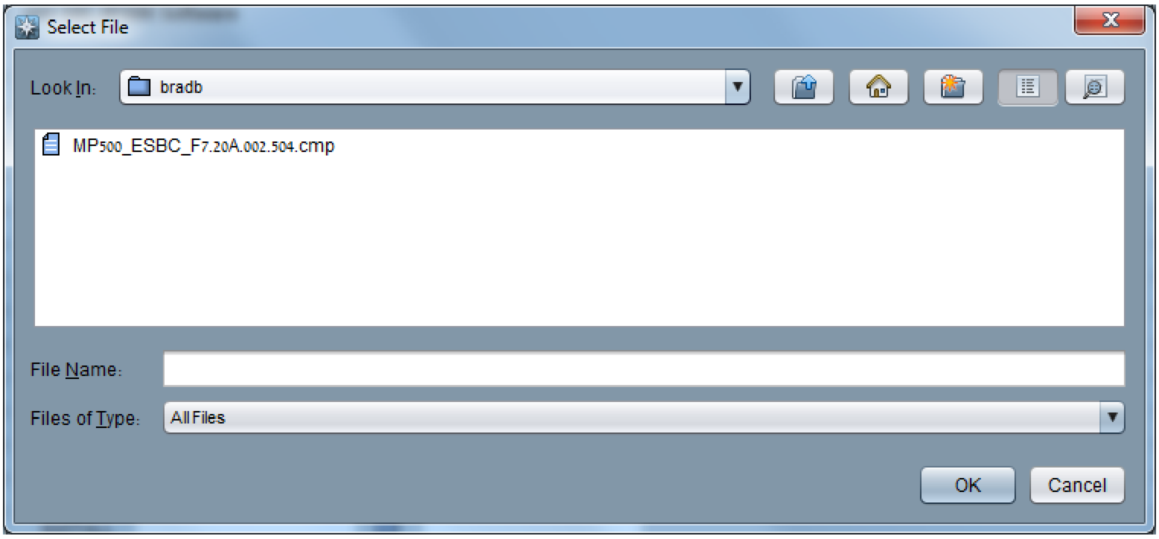
Select Protocol: MGCP

M5K/M8K/IPM5K/IPM8K Software

File Type	File Name	SW Description
EMS		
INSTALL		

2. Click the browse button to browse to the file (saved on your PC) that you wish to load to the Software Manager, select it and click **OK**.

Figure 4-5: Browse to Software File


Select File

Look In: bradb

MP500_ESBC_F7.20A.002.504.cmp

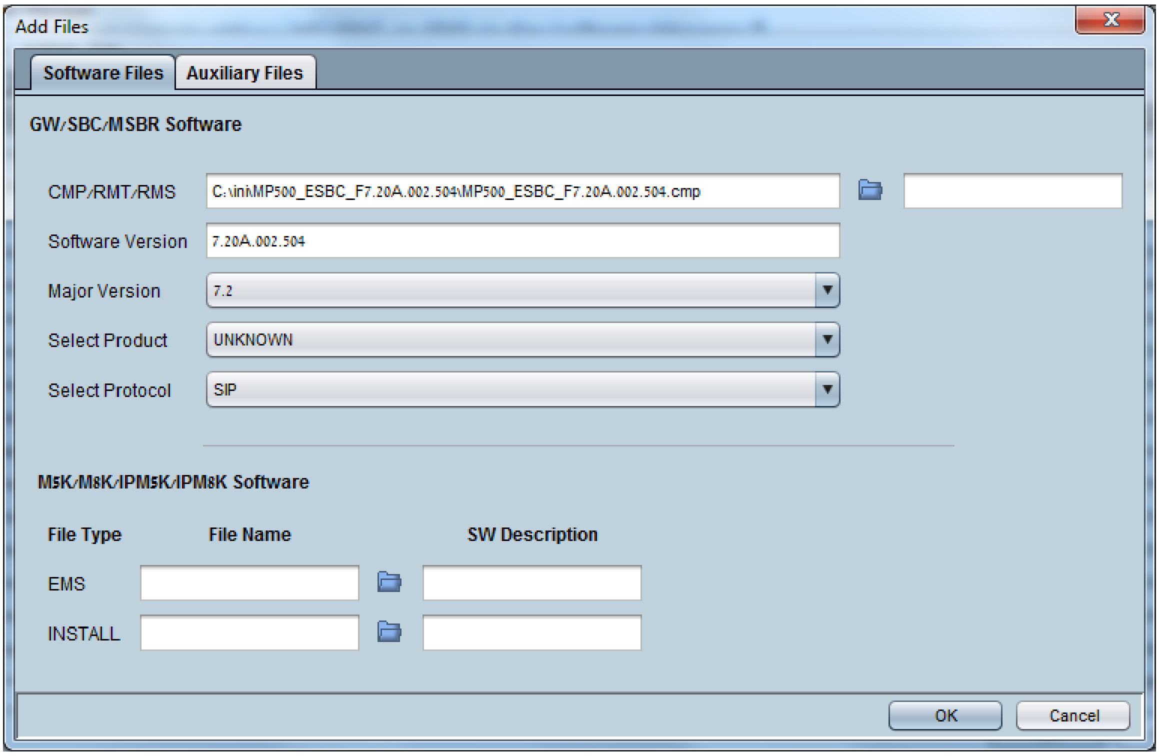
File Name:

Files of Type: All Files

The name of the file/s is displayed defined in the CMP/RMT/RMS field.

3. Click **OK**; the files that you defined are now displayed in the Software Manager.

Figure 4-6: Software File Added


Add Files

GW/SBC/MSBR Software

CMP/RMT/RMS: C:\ini\MP500_ESBC_F7.20A.002.504\MP500_ESBC_F7.20A.002.504.cmp

Software Version: 7.20A.002.504

Major Version: 7.2

Select Product: UNKNOWN

Select Protocol: SIP

M5K/M8K/IPM5K/IPM8K Software

File Type	File Name	SW Description
EMS		
INSTALL		

Note: Follow the same procedure for adding Mediant 5000/Mediant 8000 files.

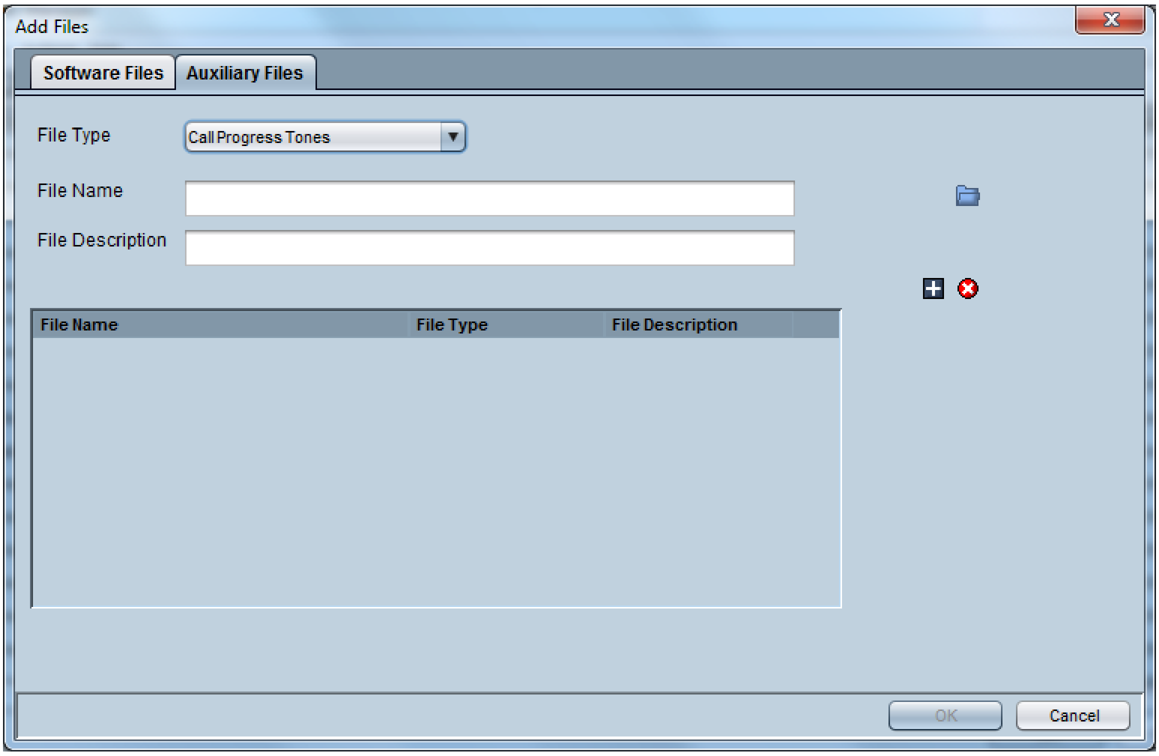
4.2 Adding an Auxiliary File

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

➢ To add a new auxiliary file to the software manager:

1. In the Software Manager toolbar, click the **Add** File icon and then select the **Auxiliary Files** tab.

Figure 4-7: Adding a New Auxiliary File



Add Files

Software Files | Auxiliary Files

File Type: Call Progress Tones ▼

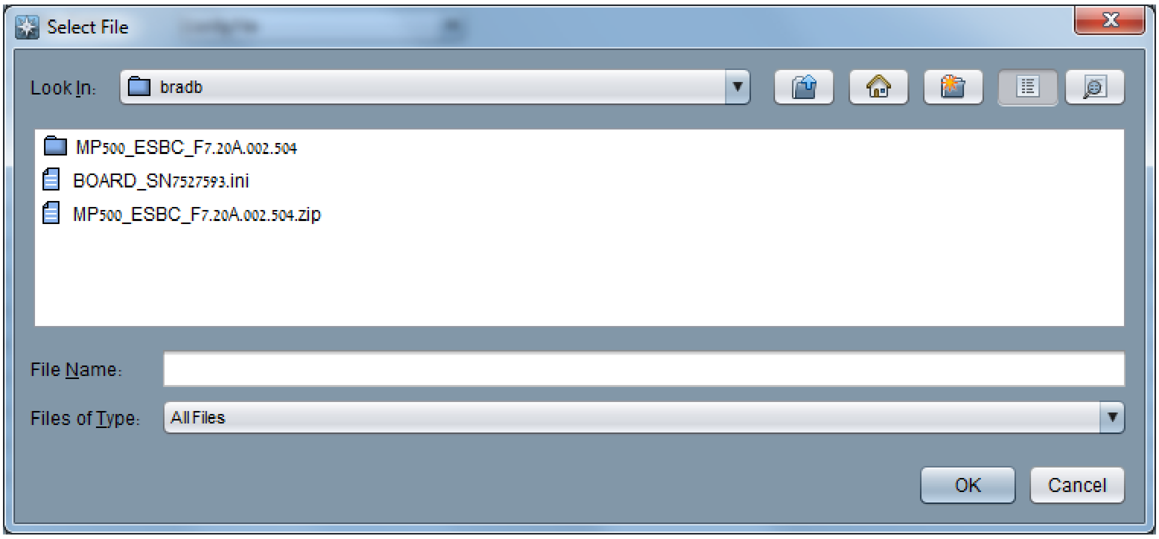
File Name:

File Description:

File Name	File Type	File Description

2. In the File Type drop-down list, select the auxiliary file type that you wish to add to the Software Manager.
3. Click the browse button to browse to the file (saved on your PC) that you wish to load to the Software Manager, select it and click **OK**.

Figure 4-8: Browse to Configuration File



Select File

Look In: bradb

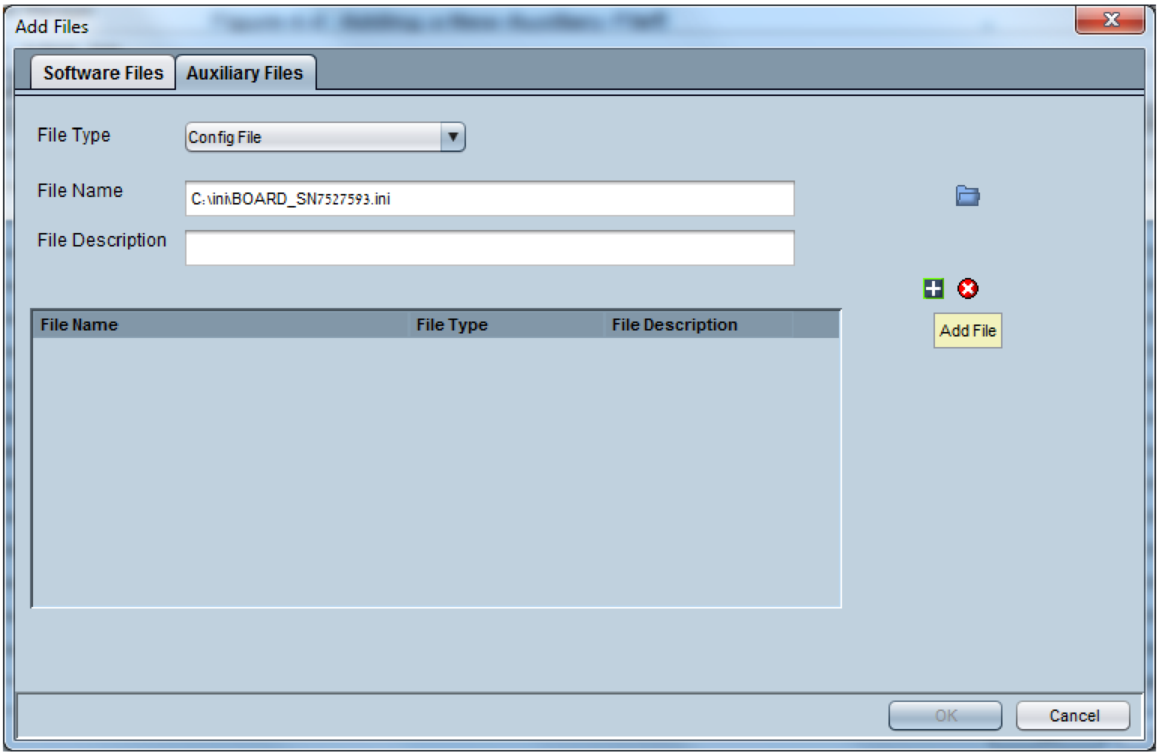
- MP500_ESBC_F7.20A.002.504
- BOARD_SN7527593.ini
- MP500_ESBC_F7.20A.002.504.zip

File Name:

Files of Type: All Files

The name of the file/s is displayed defined in the File Name field.

Figure 4-9: Adding an Auxiliary File



Add Files

File Type: Config File

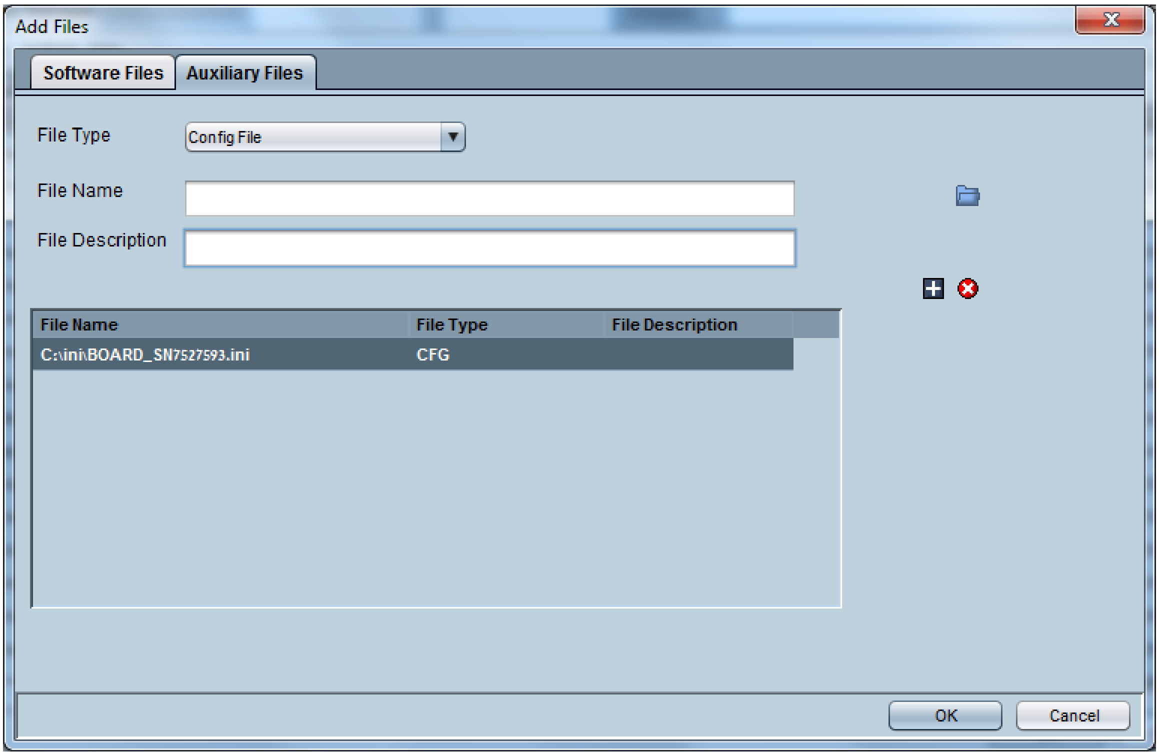
File Name: C:\ini\BOARD_SN7527593.ini

File Description:

File Name	File Type	File Description

4. Click the Add button to add the file to the Software Manager and then click **OK**.

Figure 4-10: File Added



File Type: Config File

File Name:

File Description:

File Name	File Type	File Description
C:\ini\BOARD_SN7527593.ini	CFG	

The file name is displayed in the file details pane and the file is added to the EMS..

4.3 Removing Software Files

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, 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 that is associated with the cmp file is removed with it.

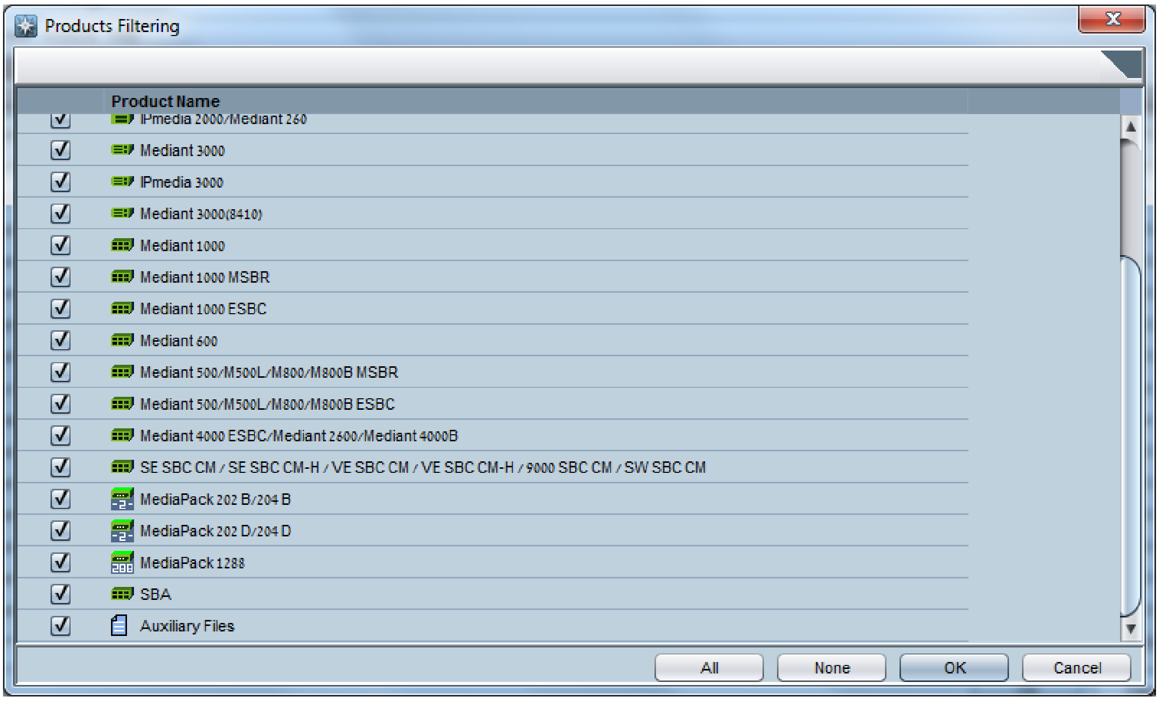
4.4 Filtering the Files Displayed in the Software Manager

You can filter the files that are displayed in the Software Manager according to product type and you can also filter whether to display Auxiliary files.

➢ **To filter the file display:**

1. In the Software Manager toolbar, select the filter icon .

Figure 4-11: Software Manager Filter



	Product Name
☑	IPmedia 2000/Mediant 260
☑	Mediant 3000
☑	IPmedia 3000
☑	Mediant 3000(8410)
☑	Mediant 1000
☑	Mediant 1000 MSBR
☑	Mediant 1000 ESBC
☑	Mediant 600
☑	Mediant 500/M500L/M800/M800B MSBR
☑	Mediant 500/M500L/M800/M800B ESBC
☑	Mediant 4000 ESBC/Mediant 2600/Mediant 4000B
☑	SE SBC CM / SE SBC CM-H / VE SBC CM / VE SBC CM-H / 9000 SBC CM / SW SBC CM
☑	MediaPack 202 B/204 B
☑	MediaPack 202 D/204 D
☑	MediaPack 1288
☑	SBA
☑	Auxiliary Files

2. Select or deselect the product types that you wish to filter.
3. Select the Auxiliary Files item if you wish to filter to view auxiliary files.
4. Select the **All** button to not view any files.
5. Select the **None** button to not filter any files.

4.5 Saving Files in Software Manager to the Network

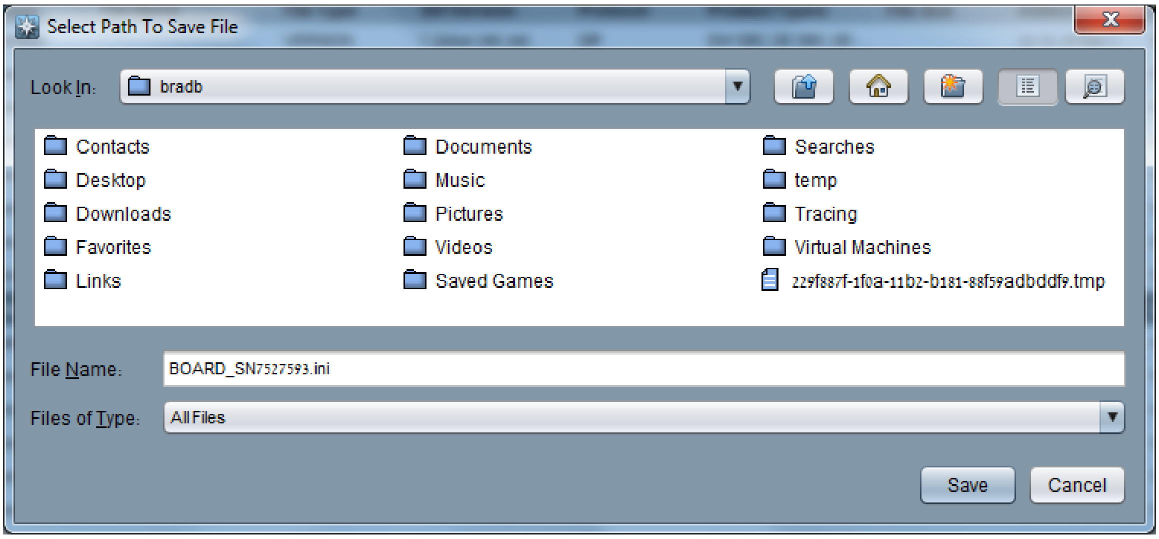
You may save files on the Software Manager to a location on your network.

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. Click the **Save File** icon, or open the Actions menu and choose the option **Save File** and click **OK**.

Figure 4-12: Select Path to Save File



Select Path To Save File

Look In: bradb

Contacts	Documents	Searches
Desktop	Music	temp
Downloads	Pictures	Tracing
Favorites	Videos	Virtual Machines
Links	Saved Games	229f887f-1f0a-11b2-b181-88f59adbddf9.tmp

File Name: BOARD_SN7527593.ini

Files of Type: All Files

2. In the File Location dialog, navigate to the required file location and click **Save**.

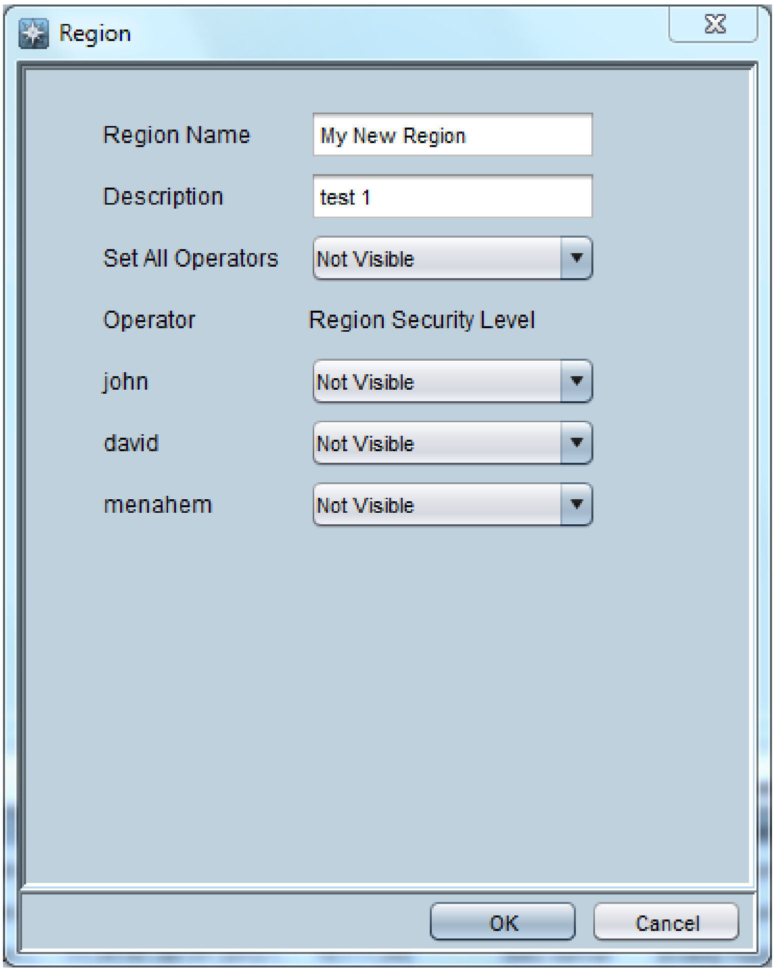
5 Configuring a Region

VoIP devices are managed in regions. The region may represent a geographic area for an enterprise or service provider. All VoIP devices are added to the EMS GW tree under the Region entity.

➤ 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



Region

Region Name: My New Region

Description: test 1

Set All Operators: Not Visible

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

2. Define the region's name and type in an optional description.
3. Set users security rights for the new region (note: 'Set All Operators' selection sets the same security level for all users).
4. Click **OK**; the requested region is added.

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.

This page is intentionally left blank.

6 Connecting Devices to the EMS

The following describes the different methods that may be used to connect devices to the EMS:

- **Full Automatic detection:** devices are automatically connected to the EMS and added to the Auto Detection region (you do not need to add devices manually to the MGs tree). If the device is the first device that is connected to the EMS using this method, then this region is automatically created. This method is predominantly used for NAT traversal, and allows SNMP communication with the devices when they are located behind NAT and the EMS is installed in the WAN. Using this method, the device initiates the connection to the EMS and sends coldStart and Keep-alive traps to the EMS. The EMS then recognizes the devices IP address and port according to its serial number (see Section 6.1).
- **Predefinition by IP address:** devices are manually added to the MGs tree under the desired Region by their IP address. Using this method, the EMS initiates the connection to the device (see Section 6.2).
- **Predefinition by Serial Number (with Auto detection):** devices are manually added to the MGs tree under the desired Region by their serial number. Using this method, the device initiates the connection to the EMS and then the devices IP address and port are recognized by the EMS according to its serial number using the auto detection process (see Section 6.2).
- **Pre-provisioning (with Auto detection):** devices are pre-provisioned with their firmware and configuration files upon initial connection to EMS. Using this method, multiple devices are manually predefined (with desired files) in the MGs tree and then the auto detection process is used to connect the devices to the EMS and provision them with their firmware and configuration files (see Section 6.3).

Note: Before connecting devices to the EMS, you need configure the device’s SNMP settings (see Section 7.1).

6.1 Connecting Devices using Full Automatic Detection

Devices can be connected to the EMS using the automatic detection mechanism. When the device is connected to the power supply in the network at the customer's premises and/or is rebooted and initialized, it is automatically detected by the EMS and added by default to the AutoDetection region in the EMS.

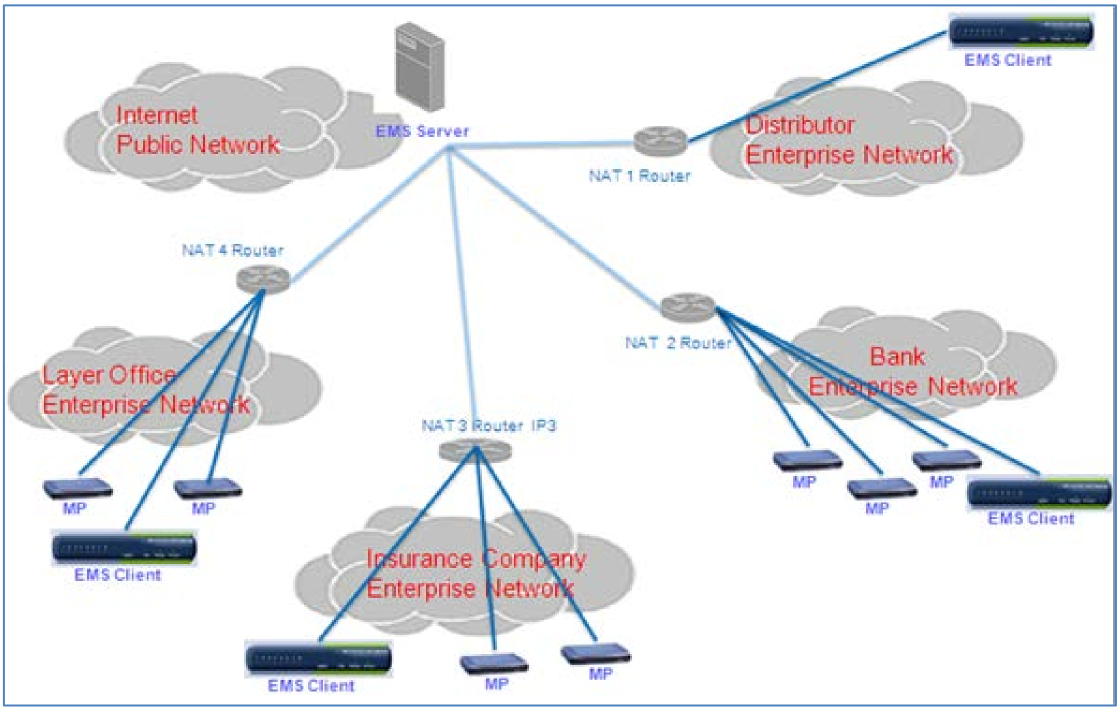
Note: You must fully configure the device's SNMP settings (see Section 7.1) for this feature to function.

When the device 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 device is alive. This can be ensured by configuring the device to send coldStart (after device reset) and Keep-alive traps (sent every 30 seconds by default) to the EMS server. This allows the EMS to perform SNMP SET and GET commands at any time. When the device is added to the EMS, EMS recognizes the device according to its **sysDesc** field and its serial number, and according to the entries in the EMS database and GWs tree. The devices default name is composed of the router's IP address and port number. Sometimes the NAT changes the IP address and port for the devices. EMS recognizes these changes after the device is reset.

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

- Each device in each LAN i.e. a Bank Enterprise Network connects to the Internet Public Network via a NAT IP address.
- Connectivity between the EMS server and the device is maintained by configuring the device to coldStart and Keep-alive traps.

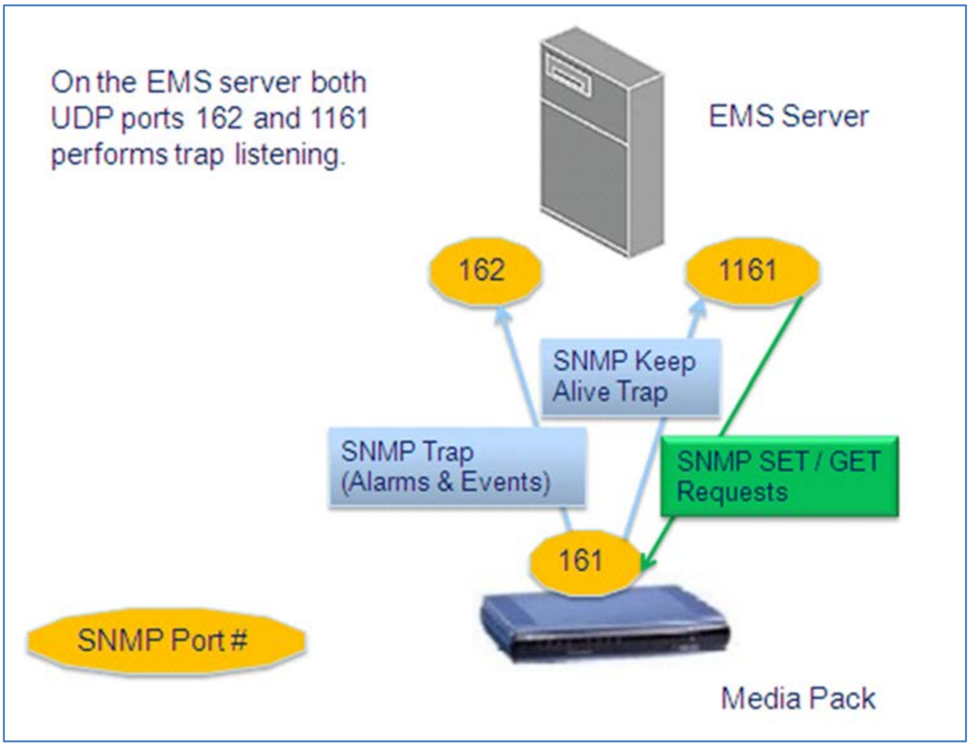
Figure 5-1: MP-NAT Configuration



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 5-2: Sending SNMP Traps to EMS Server (Behind a NAT)


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

6.1.1 Devices Behind a NAT

All gateway, SBC, MSBR and CloudBond/CCE Appliance devices can be managed by EMS behind a NAT.

6.1.2 IP Phones Behind a NAT

IP Phones residing behind a NAT whose IP addresses are internal, can be managed by the EMS via an SBC HTTP proxy. If the phones are not behind a NAT, phone-EMS communications are direct, without the requirement of an SBC HTTP proxy. If the phones are located behind a NAT and an SBC HTTP proxy is not used, then only partial management of the phones is possible; the following can be performed:

- Alarms and statuses can be sent from the phones to the IP Phone Manager i.e. the REST requests originate from the phone and the EMS functions as a REST server.
- The IP Phone Manager can perform auto-discovery of the phones for the purpose of uploading configuration and firmware files.

The following cannot be performed:

- Actions menu actions cannot be applied, for example, ‘Reset Phone’ i.e. the EMS functions as a REST client.

Note: HTTP updates can be sent from the phones to the EMS server across a NAT; however requests cannot be sent from the EMS server to the phones without the mediation of the SBC HTTP Proxy server.

6.2 Connecting Devices using Predefinition

This section describes how to connect devices to the EMS by manually predefining them in the MGs tree.

6.2.1 Predefining a Single Device

This section describes how to connect a single device. Note the following:

- 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 prepared the relevant template ini files and .cmp firmware files. You can add these files to the Software Manager in the procedure described below. See Chapter 11 ‘Interoperability Automatic Provisioning’.
- 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.
- This procedure includes the Single Sign-on setting for automatically logging into the device's embedded Web server tool from EMS; therefore ensure that you know the appropriate Web user and password. For more information, see Section 42.1.1.

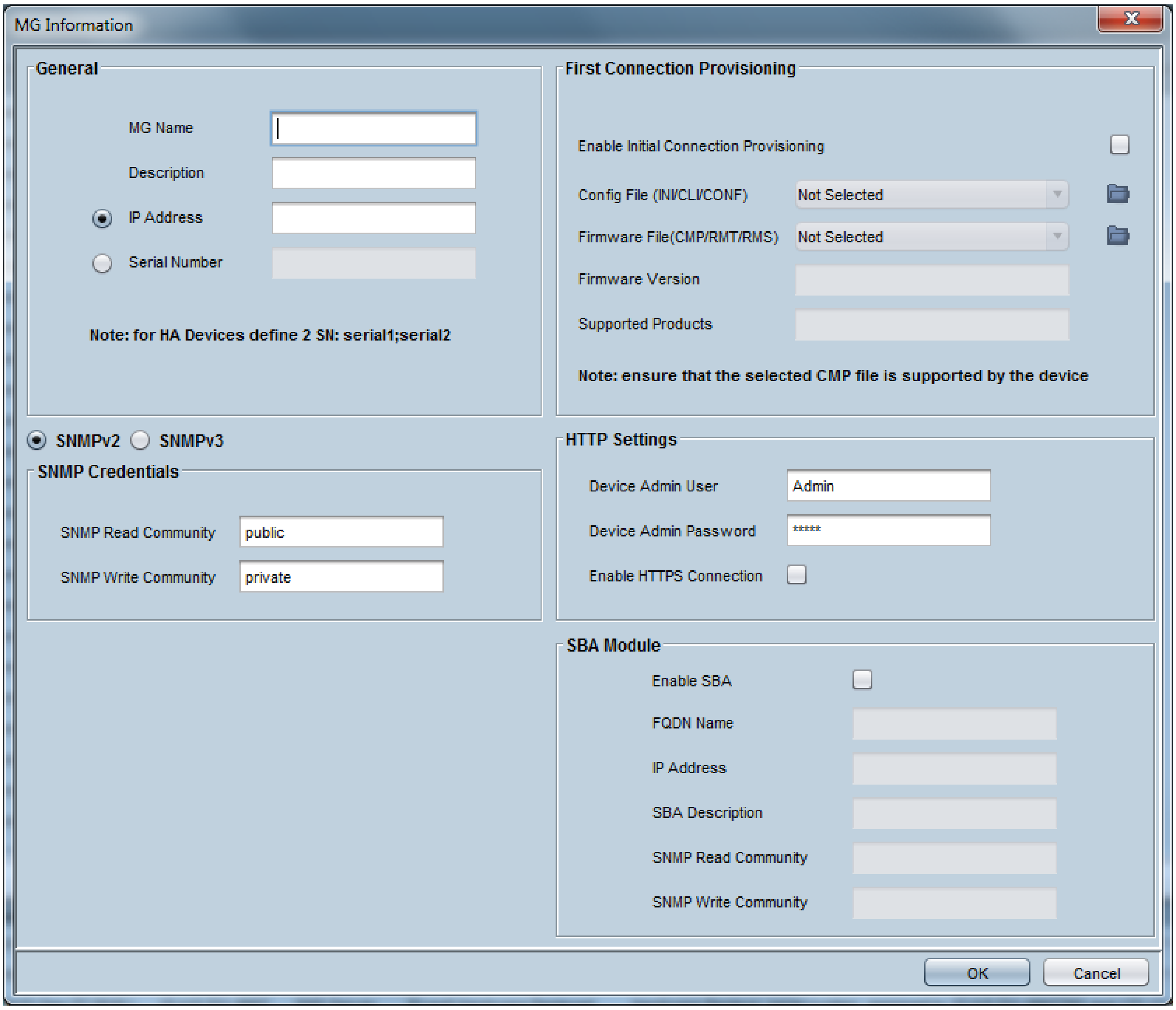
Note:

- Do not use underscores in device names (MG Name).
- References to "device" in this procedure, also includes "boards".

➢ To predefine a single device:

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 5-3: MG Information



MG Information

General

MG Name

Description

● IP Address

○ Serial Number

Note: for HA Devices define 2 SN: serial1;serial2

First Connection Provisioning

Enable Initial Connection Provisioning □

Config File (INI/CLI/CONF): Not Selected

Firmware File(CMP/RMT/RMS): Not Selected

Firmware Version

Supported Products

Note: ensure that the selected CMP file is supported by the device

● SNMPv2 ○ SNMPv3

SNMP Credentials

SNMP Read Community: public

SNMP Write Community: private

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

Enable HTTPS Connection □

SBA Module

Enable SBA □

FQDN Name

IP Address

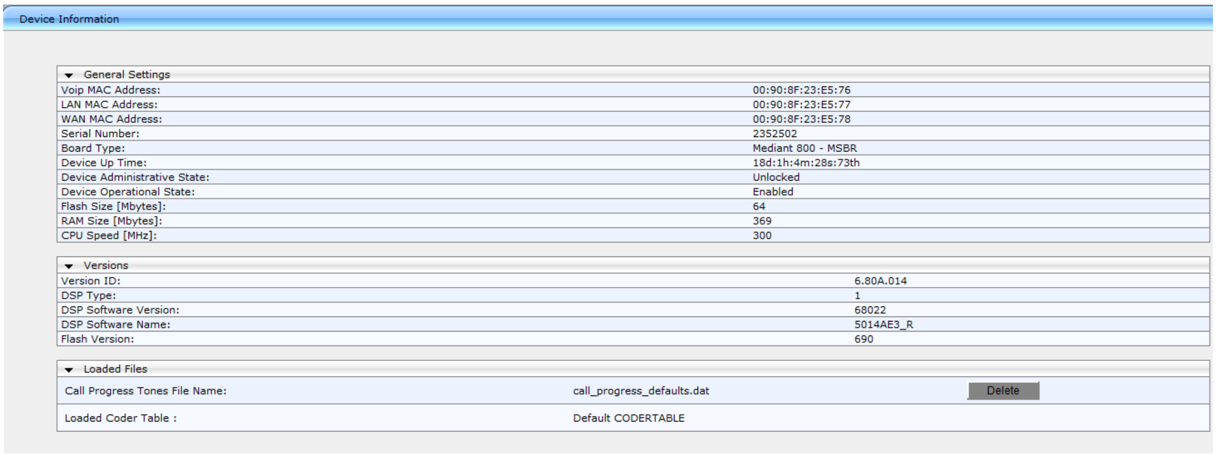
SBA Description

SNMP Read Community

SNMP Write Community

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. When this method is used, the device is immediately connected to the EMS.
    - Enter the **Serial Number** of the device. You can find the device serial number on the Web server device Information page (**Status & Diagnostics** menu> **System Status** > **Device Information**).

Figure 5-4: Device Information



Device Information

General Settings	
Voip MAC Address:	00:90:8F:23:E5:76
LAN MAC Address:	00:90:8F:23:E5:77
WAN MAC Address:	00:90:8F:23:E5:78
Serial Number:	2352502
Board Type:	Mediant 800 - MSBR
Device Up Time:	18d:1h:4m:28s:73th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [Mbytes]:	64
RAM Size [Mbytes]:	369
CPU Speed [MHz]:	300

Versions	
Version ID:	6.80A.014
DSP Type:	1
DSP Software Version:	68022
DSP Software Name:	5014AE3_R
Flash Version:	690

Loaded Files		
Call Progress Tones File Name:	call_progress_defaults.dat	Delete
Loaded Coder Table :	Default CODERTABLE	

Note: If you are connecting the device to the EMS by its serial number, you must configure the device's SNMP settings as described in Section 7.1.

4. Do one of the following:
    - If you are configuring SNMPv2, enter the device's SNMP Read (default 'public') and Write (default 'private') 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.

Note: For CloudBond 365 and CCE Appliance users: When updating SNMPv2/SNMPv3 credentials for these products, these credentials are not automatically updated in the EMS and therefore users should update the device details (MG Information) as well.

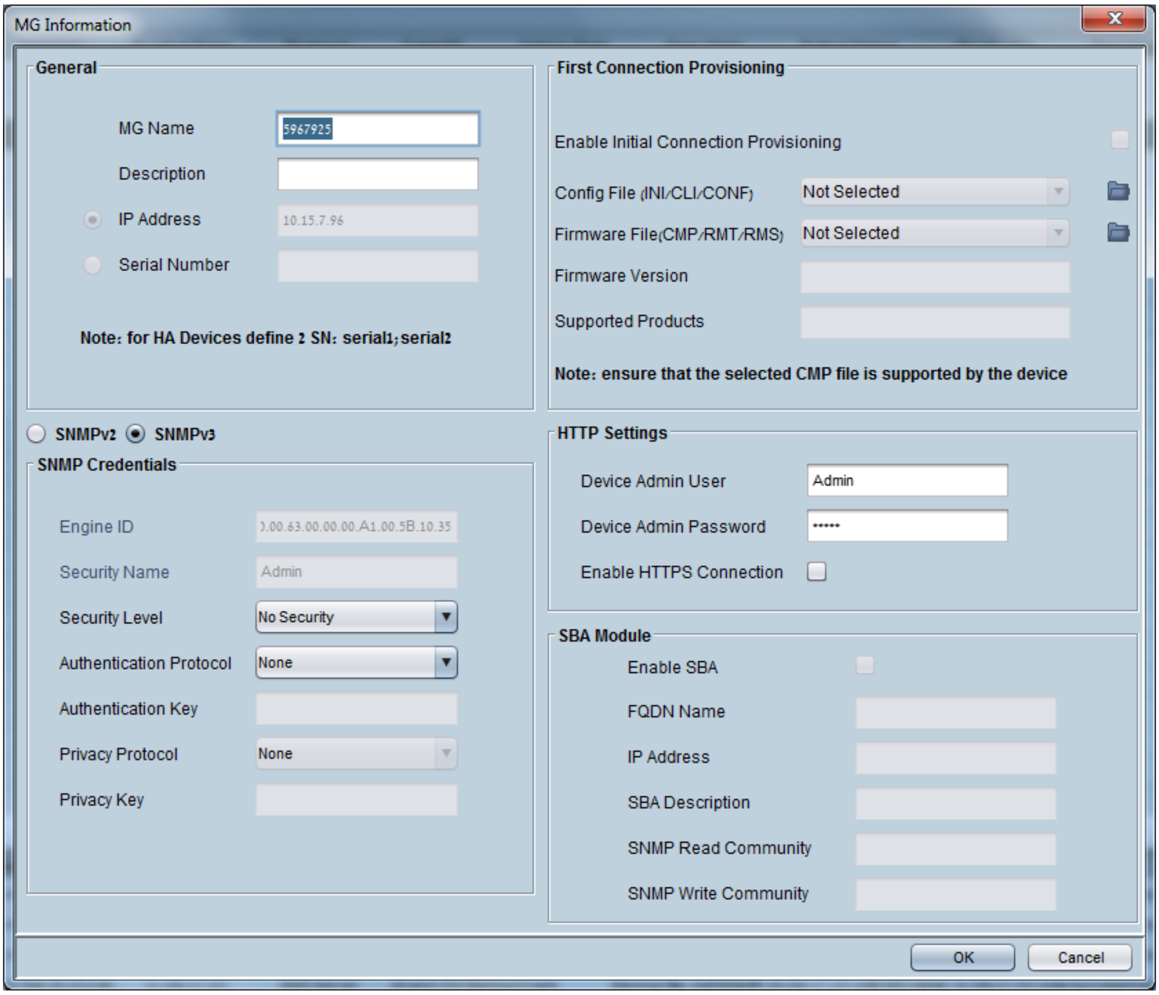
5. (Optional) In the Device Admin User field, enter the device Web server user name and in the Device Admin Password field, enter the Web server password. For example, User -"Admin", Password - "Admin".

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.

6. If you wish to secure the connection with device, select the 'Enable HTTPS Connection" option. For more information on HTTPS, see Chapter 42.

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 5-5: MG Details



MG Information

General

MG Name: 5967925

Description:

● IP Address: 10.15.7.96

○ Serial Number:

Note: for HA Devices define 2 SN: serial1;serial2

First Connection Provisioning

Enable Initial Connection Provisioning □

Config File (INI/CLI/CONF): Not Selected

Firmware File(CMP/RMT/RMS): Not Selected

Firmware Version:

Supported Products:

Note: ensure that the selected CMP file is supported by the device

○ SNMPv2 ● SNMPv3

SNMP Credentials

Engine ID:).00.63.00.00.00.A1.00.5B.10.35

Security Name: Admin

Security Level: No Security

Authentication Protocol: None

Authentication Key:

Privacy Protocol: None

Privacy Key:

HTTP Settings

Device Admin User: Admin

Device Admin Password: •••••

Enable HTTPS Connection □

SBA Module

Enable SBA □

FQDN Name:

IP Address:

SBA Description:

SNMP Read Community:

SNMP Write Community:

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

Note: To configure the EMS and device SNMP settings , see Chapter 34 on page 330.

6.2.2 Predefining Multiple Devices

This section describes how to predefine multiple devices in a single screen. The EMS supports this feature on the condition that all devices have identical SNMP settings. Additionally ensure that you know the relevant SNMPv2 or SNMPv3 credentials that were configured on the device.

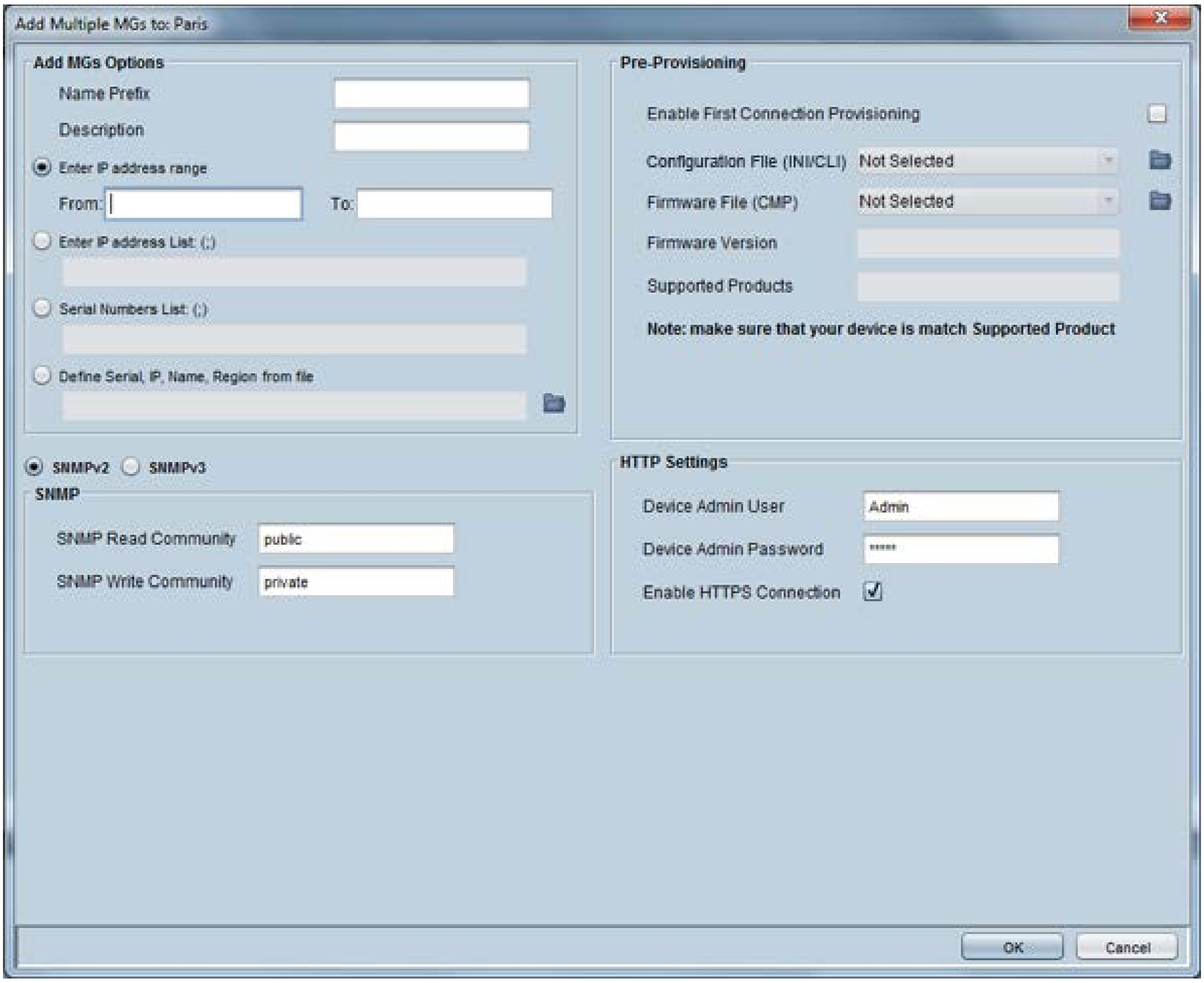
Note:

- 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 prepared the relevant template ini files and .cmp firmware files. You can add these files to the Software Manager in the procedure described below. See Chapter 11 Interoperability Automatic Provisioning.
- This procedure includes the Single Sign-on setting for automatically logging into the device's embedded Web server tool from EMS; therefore ensure that you know the appropriate Web user and password. For more information on this feature, see Section 42.1.1.
- Do not use underscores in device names (MG Name).

➢ 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 5-6: Add Multiple MGs-SNMPv2



Name Prefix
Description
● Enter IP address range
From: To:
○ Enter IP address List: (;)
○ Serial Numbers List: (;)
○ Define Serial, IP, Name, Region from file
● SNMPv2 ○ SNMPv3
SNMP Read Community: public
SNMP Write Community: private
Enable First Connection Provisioning □
Configuration File (INI/CLI): Not Selected
Firmware File (CMP): Not Selected
Firmware Version
Supported Products
Note: make sure that your device is match Supported Product
Device Admin User: Admin
Device Admin Password: *****
Enable HTTPS Connection ☑

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.

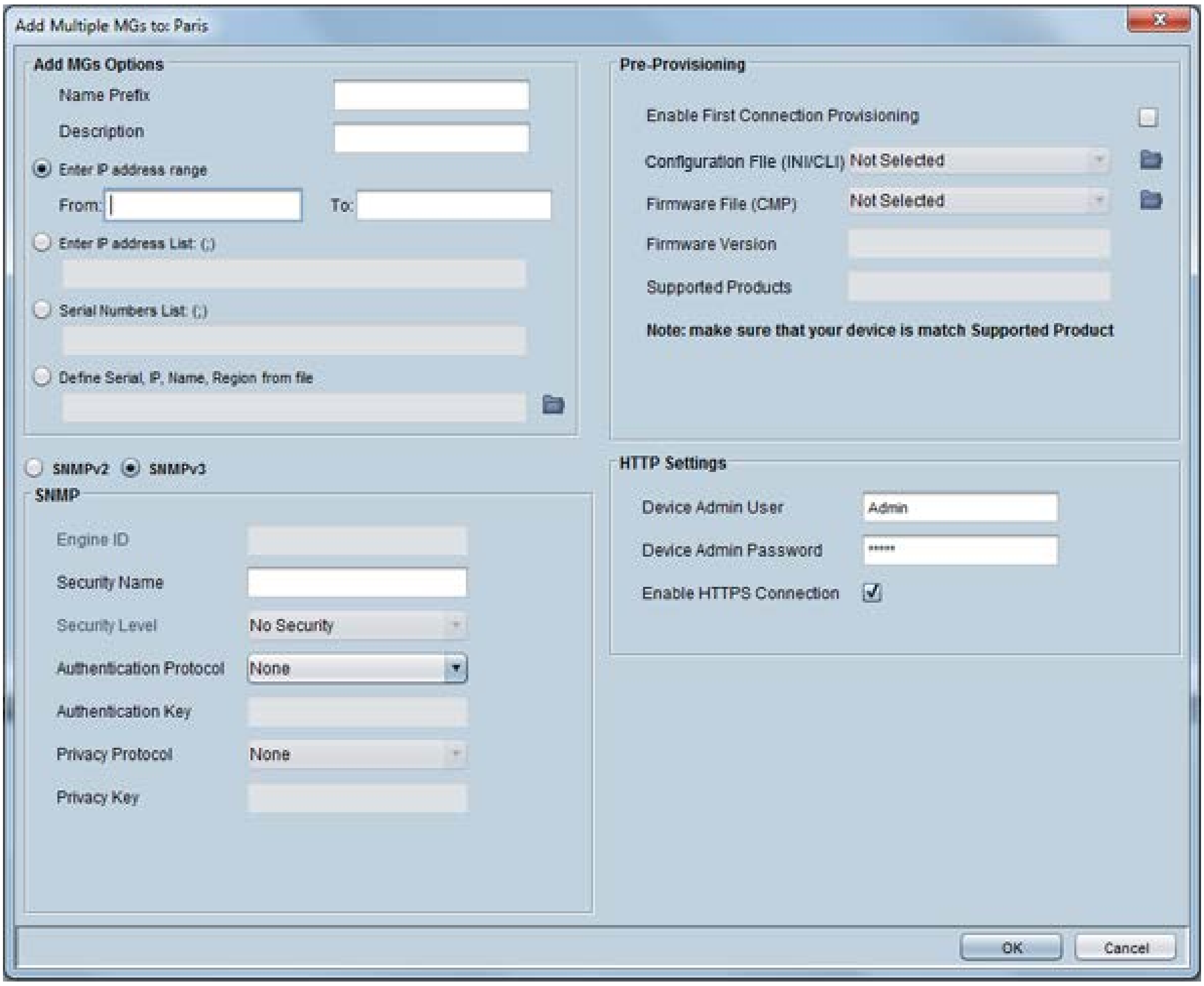
- Define multiple devices by checking the check box 'Define Serial, IP, Name, Region from file', navigate to a pre-prepared *csv* predefinition file and click **OK**. Each device must have a row in the predefinition file. If you don't know all the required information, use empty coma delimiters. The 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 Section 9.7).
- If you are connecting the device to the EMS by its serial number, you must configure the device’s SNMP settings as described in Section 7.1.

8. Do one of the following:
    - If you are configuring SNMPv2, enter the device's SNMP Read (default 'public') and Write (default 'private') 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 5-7: Add Multiple MGs-SNMPv3



Add Multiple MGs to: Paris

Add MGs Options

Name Prefix

Description

● Enter IP address range

From: To:

○ Enter IP address List: (;)

○ Serial Numbers List: (;)

○ Define Serial, IP, Name, Region from file

○ SNMPv2 ● SNMPv3

SNMP

Engine ID

Security Name

Security Level: No Security

Authentication Protocol: None

Authentication Key

Privacy Protocol: None

Privacy Key

Pre-Provisioning

Enable First Connection Provisioning □

Configuration File (INI/CLI): Not Selected

Firmware File (CMP): Not Selected

Firmware Version

Supported Products

Note: make sure that your device is match Supported Product

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

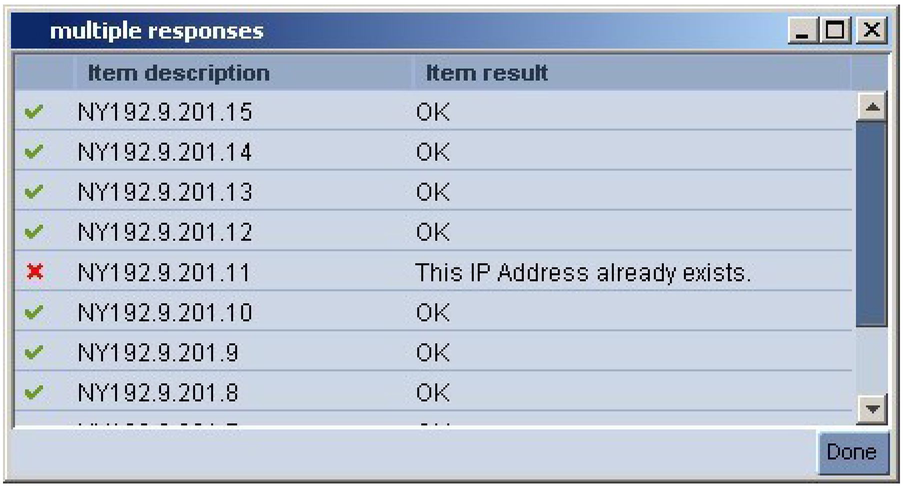
Enable HTTPS Connection ☑

9. 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).

10. If you wish to secure the connection with device, set the 'Enable HTTPS Connection' option. For more information on HTTPS, see Chapter 42.
11. Click **OK**; an Action Report is displayed, indicating the result of the add action for each device added.

Figure 5-8: Action Report for Adding Multiple Devices Result



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

6.3 Connecting Devices using Pre-Provisioning

This procedure includes the configuration of the Interoperability Automatic Provisioning feature. If you wish to provision devices using this feature, ensure you have prepared the relevant template ini files and firmware files. You can add these files to the Software Manager in the procedure described below.

Note: Before proceeding, It is recommended to read the detailed information on the Interoperability Automatic Provisioning feature in Chapter 11.

6.3.1 Pre-provisioning a Single Device

This procedure describes how to pre-provision a single device.

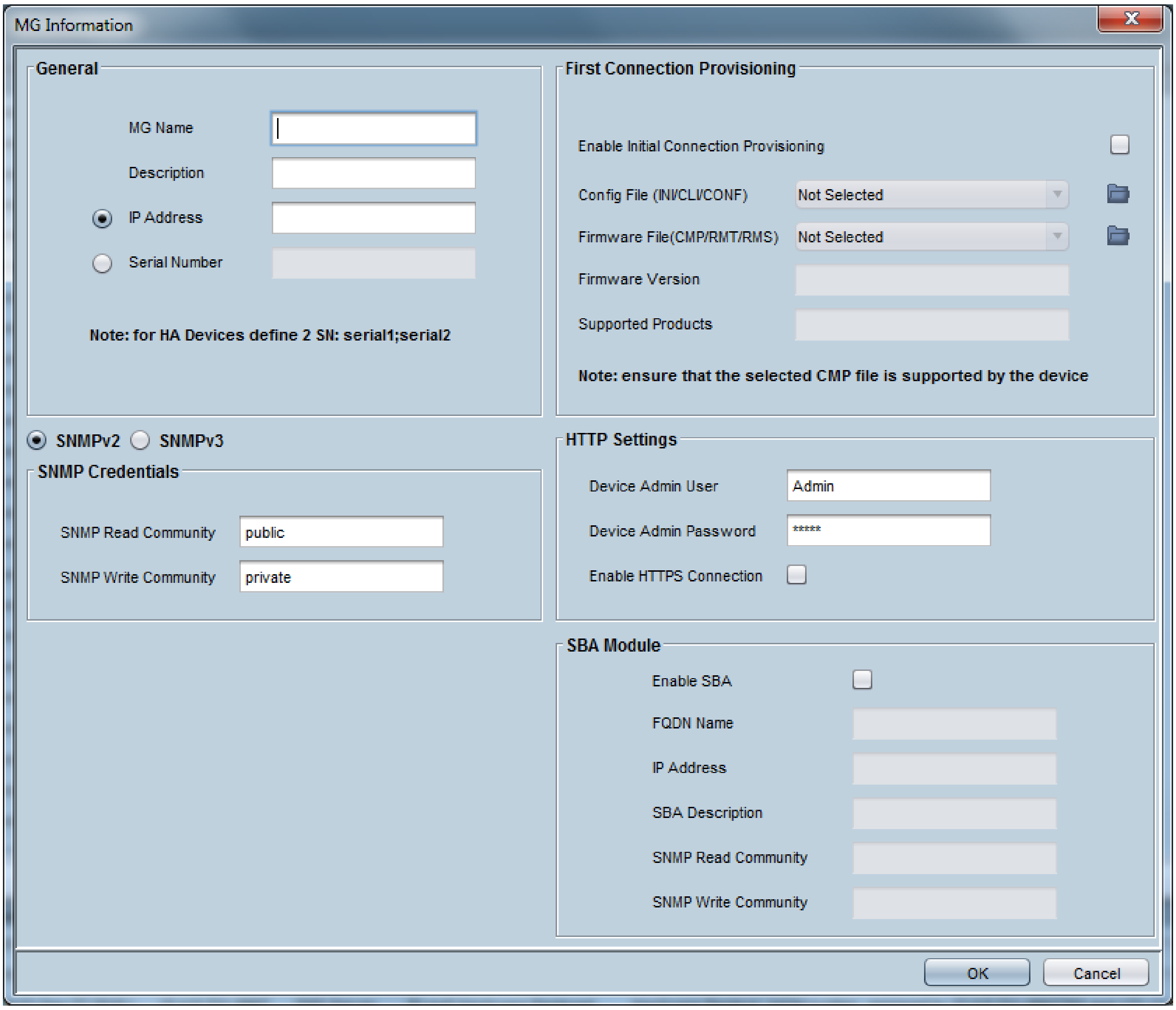
- This procedure includes the configuration of the SNMP settings for the connection between the device and the EMS; therefore ensure that you note the relevant SNMPv2 or SNMPv3 credentials.
- This procedure includes the Single-Sign-on setting for automatically logging into the device's embedded Web server tool from EMS; therefore ensure that you know the appropriate Web user and password. For information, see Section 42.1.1.

Note: Do not use underscores in device names (MG Name).

➢ **To predefine a single device:**

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 5-9: MG Information



MG Information

General

MG Name: |

Description:

● IP Address:

○ Serial Number:

Note: for HA Devices define 2 SN: serial1;serial2

First Connection Provisioning

Enable Initial Connection Provisioning □

Config File (INI/CLI/CONF): Not Selected

Firmware File(CMP/RMT/RMS): Not Selected

Firmware Version:

Supported Products:

Note: ensure that the selected CMP file is supported by the device

● SNMPv2 ○ SNMPv3

SNMP Credentials

SNMP Read Community: public

SNMP Write Community: private

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

Enable HTTPS Connection □

SBA Module

Enable SBA □

FQDN Name:

IP Address:

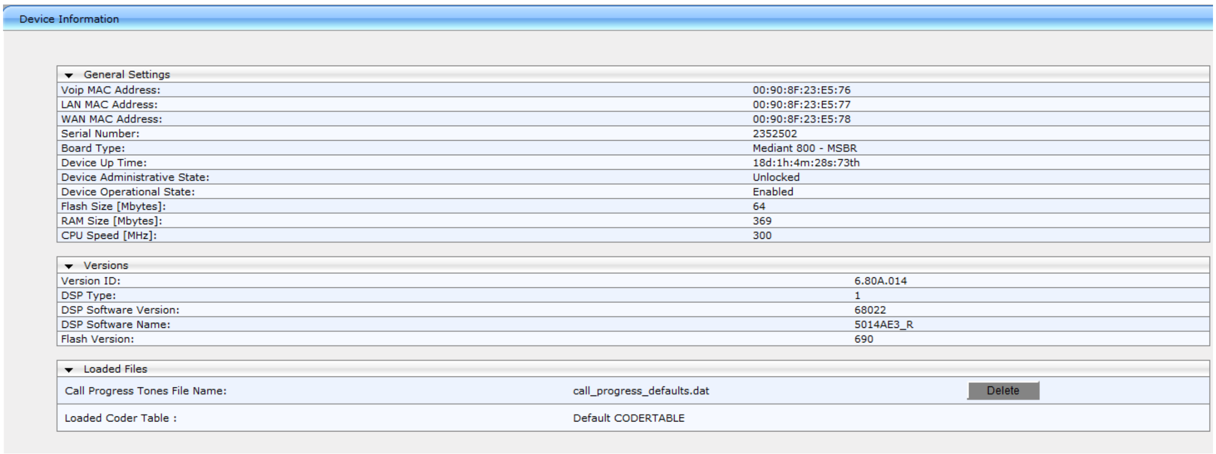
SBA Description:

SNMP Read Community:

SNMP Write Community:

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. When this method is used, the device is immediately connected to the EMS.
   - Enter the **Serial Number** of the device. You can find the device serial number on the Web server device Information page (**Status & Diagnostics** menu> **System Status** > **Device Information**).

Figure 5-10: Device Information



Device Information

General Settings

Voip MAC Address:	00:90:8F:23:E5:76
LAN MAC Address:	00:90:8F:23:E5:77
WAN MAC Address:	00:90:8F:23:E5:78
Serial Number:	2352502
Board Type:	Mediant 800 - MSBR
Device Up Time:	18d:1h:4m:28s:73th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [Mbytes]:	64
RAM Size [Mbytes]:	369
CPU Speed [MHz]:	300

Versions

Version ID:	6.80A.014
DSP Type:	1
DSP Software Version:	68022
DSP Software Name:	5014AE3_R
Flash Version:	690

Loaded Files

Call Progress Tones File Name:	call_progress_defaults.dat	Delete
Loaded Coder Table :	Default CODERTABLE	

Note: If you are connecting the device to the EMS by its serial number, you must configure the device’s SNMP settings as described in Section 7.1.

4. Do one of the following:
   - If you are configuring SNMPv2, enter the device's Read (default 'public') and Write (default 'private') 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.

Note: For CloudBond and CCE Appliance users: When updating SNMPv2/SNMPv3 credentials for these products, these credentials are not automatically updated in the EMS and therefore users should update the device details (MG Information) as well.

5. Select the 'Enable Initial Connection Provisioning' check box to enable the Interoperability Automatic Provisioning feature (see Chapter 11), and then do the following:
   - In the 'Configuration File' (ini file for gateway or SBC devices, CLI script for MSBR devices or CONF files for MP-20x devices) field, from the drop-down

list box, select the desired file, or click the button to browse to a file.

- (Optional) In the 'Firmware File' (.cmp file or rmt/rms files for MP-20x devices) field, from the drop-down list box, select the desired file or click the button to browse to a file.

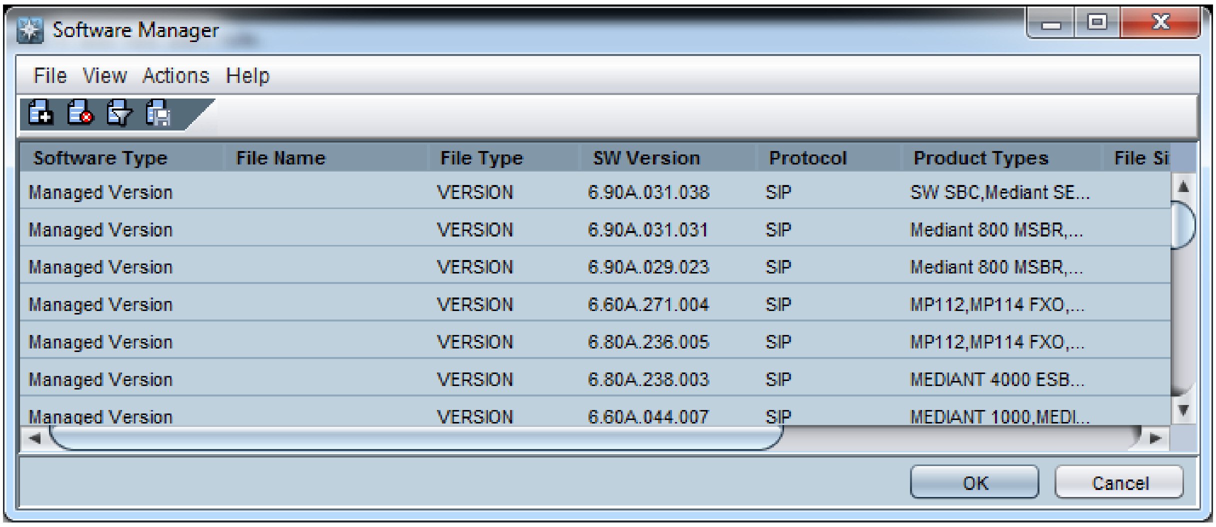
  When you choose a .cmp or rmt/rms file, the corresponding firmware version is displayed as well as the products that are supported for this file.

Notes:

- When choosing a .cmp or rmt/rms 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 CLI or conf file and can *optionally* select a .cmp or rmt/rms file.
- This feature is not supported for CloudBond and CCE Appliance devices.
- The device is automatically reset twice, once to apply the firmware and once to apply the configuration file.

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

Figure 5-11: Software Manager



Software Type	File Name	File Type	SW Version	Protocol	Product Types	File Si
Managed Version		VERSION	6.90A.031.038	SIP	SW SBC,Mediant SE...	
Managed Version		VERSION	6.90A.031.031	SIP	Mediant 800 MSBR,...	
Managed Version		VERSION	6.90A.029.023	SIP	Mediant 800 MSBR,...	
Managed Version		VERSION	6.60A.271.004	SIP	MP112,MP114 FXO,...	
Managed Version		VERSION	6.80A.236.005	SIP	MP112,MP114 FXO,...	
Managed Version		VERSION	6.80A.238.003	SIP	MEDIANT 4000 ESB...	
Managed Version		VERSION	6.60A.044.007	SIP	MEDIANT 1000,MEDI...	

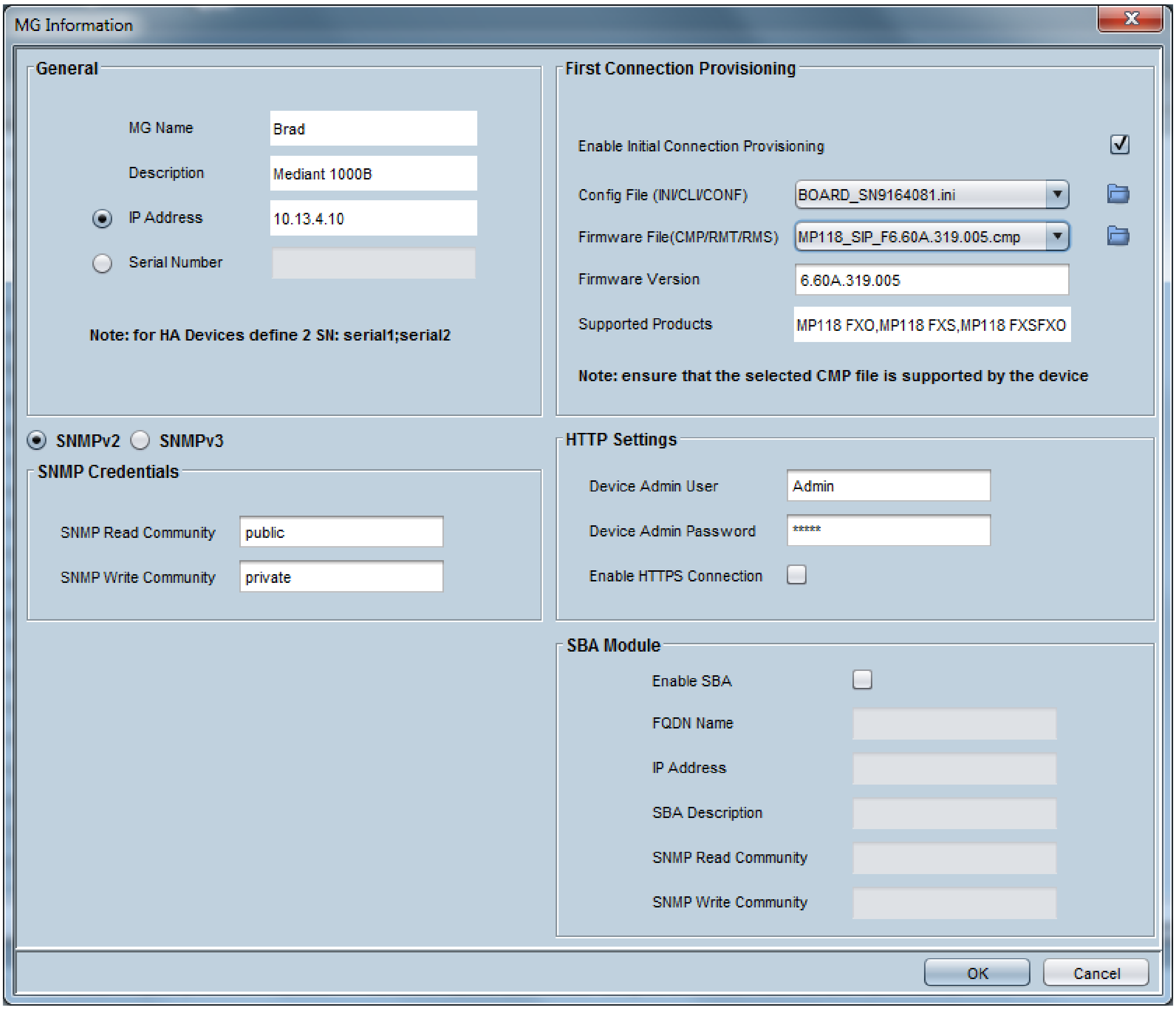
6. (Optional) In the Device Admin User field, enter the device Web server user name and in the Device Admin Password field, enter the Web server password. For example, User -"Admin", Password - "Admin".

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 the 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 Chapter 42.

   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 5-12: MG Details



General

MG Name: Brad
Description: Mediant 1000B
● IP Address: 10.13.4.10
○ Serial Number:

Note: for HA Devices define 2 SN: serial1;serial2

First Connection Provisioning

Enable Initial Connection Provisioning ☑
Config File (INI/CLI/CONF): BOARD_SN9164081.ini
Firmware File(CMP/RMT/RMS): MP118_SIP_F6.60A.319.005.cmp
Firmware Version: 6.60A.319.005
Supported Products: MP118 FXO,MP118 FXS,MP118 FXSFXO

Note: ensure that the selected CMP file is supported by the device

● SNMPv2 ○ SNMPv3

SNMP Credentials

SNMP Read Community: public
SNMP Write Community: private

HTTP Settings

Device Admin User: Admin
Device Admin Password: *****
Enable HTTPS Connection □

SBA Module

Enable SBA □
FQDN Name:
IP Address:
SBA Description:
SNMP Read Community:
SNMP Write Community:

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

6.3.2 Pre-provisioning Multiple Devices

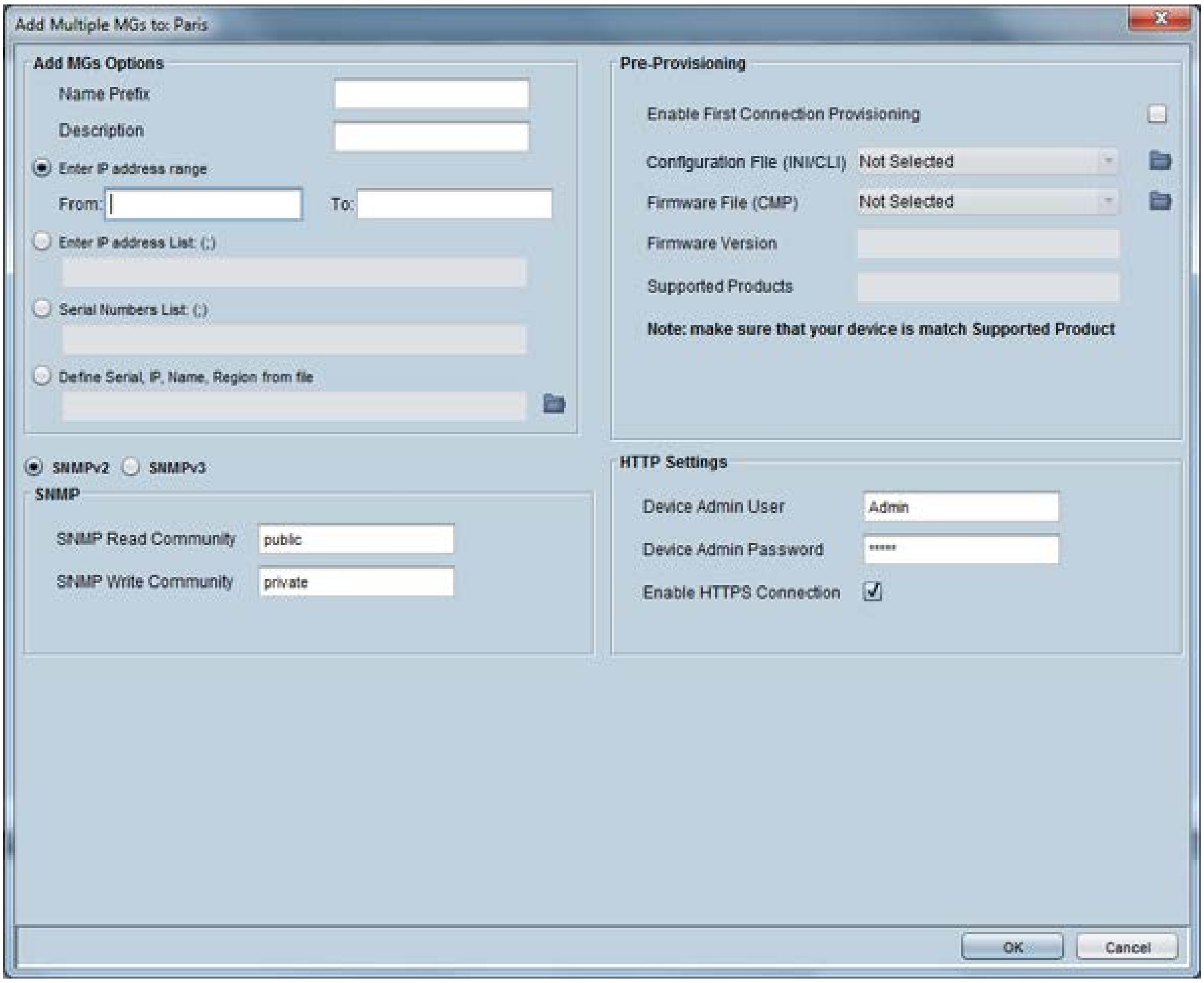
This section describes how to pre-provision multiple devices in a single screen. The EMS supports this feature on the condition that all devices have identical SNMP settings. Additionally ensure that you know the relevant SNMPv2 or SNMPv3 credentials that were configured on the device.

> **Note:**
>
> - This procedure includes the Single-Sign-On setting for automatically logging into the device's embedded Web server tool from EMS; therefore ensure that you know the Web user and password (for more information, see Section 6.2.1).
> - Do not use underscores in device names (MG Name).

➢ 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 5-13: Add Multiple MGs-SNMPv2



Add Multiple MGs to: Paris

Add MGs Options

Name Prefix

Description

● Enter IP address range

From: | To:

○ Enter IP address List: (;)

○ Serial Numbers List: (;)

○ Define Serial, IP, Name, Region from file

● SNMPv2 ○ SNMPv3

SNMP

SNMP Read Community: public

SNMP Write Community: private

Pre-Provisioning

Enable First Connection Provisioning □

Configuration File (INI/CLI): Not Selected

Firmware File (CMP): Not Selected

Firmware Version

Supported Products

Note: make sure that your device is match Supported Product

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

Enable HTTPS Connection ☑

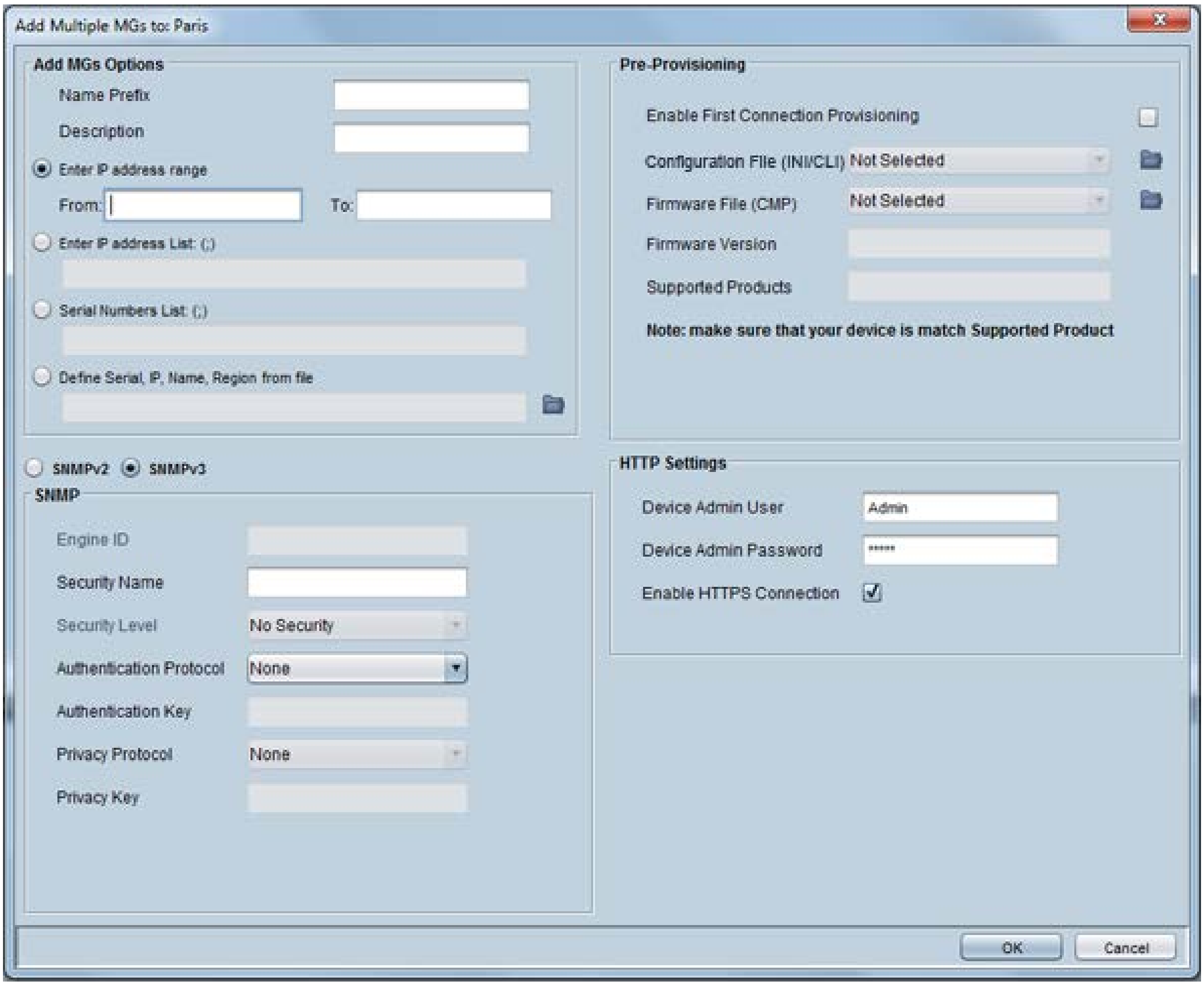
2. Enter the Name Prefix for device group e.g. type of device and Description for the group of devices.
3. Use one of the following methods to connect the multiple devices to the EMS:
   - Select the 'Enter IP address range' option, define the 'From' and 'To' fields and click OK. All devices in the defined 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 Section 9.7).
- If you are connecting the device to the EMS by its serial number, you must configure the device's SNMP settings as described in Section 7.1.

9. Do one of the following:
   - If you are configuring SNMPv2, enter the device's Read (default 'public') and Write (default 'private') 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 5-14: Add Multiple MGs-SNMPv3



Add Multiple MGs to: Paris

Add MGs Options

Name Prefix

Description

● Enter IP address range

From: To:

○ Enter IP address List: (;)

○ Serial Numbers List: (;)

○ Define Serial, IP, Name, Region from file

○ SNMPv2 ● SNMPv3

SNMP

Engine ID

Security Name

Security Level: No Security

Authentication Protocol: None

Authentication Key

Privacy Protocol: None

Privacy Key

Pre-Provisioning

Enable First Connection Provisioning □

Configuration File (INI/CLI): Not Selected

Firmware File (CMP): Not Selected

Firmware Version

Supported Products

Note: make sure that your device is match Supported Product

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

Enable HTTPS Connection ☑

10. 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, CLI script for MSBR devices or CONF files for MP-20x devices) field, from the drop-down list box, select the desired file, or click the 📁 button to browse to a file.
- (Optional) In the 'Firmware File' (.cmp file or rmt/rms files for MP-20x devices) field, from the drop-down list box, select the desired file or click the 📁 button to browse to a file.

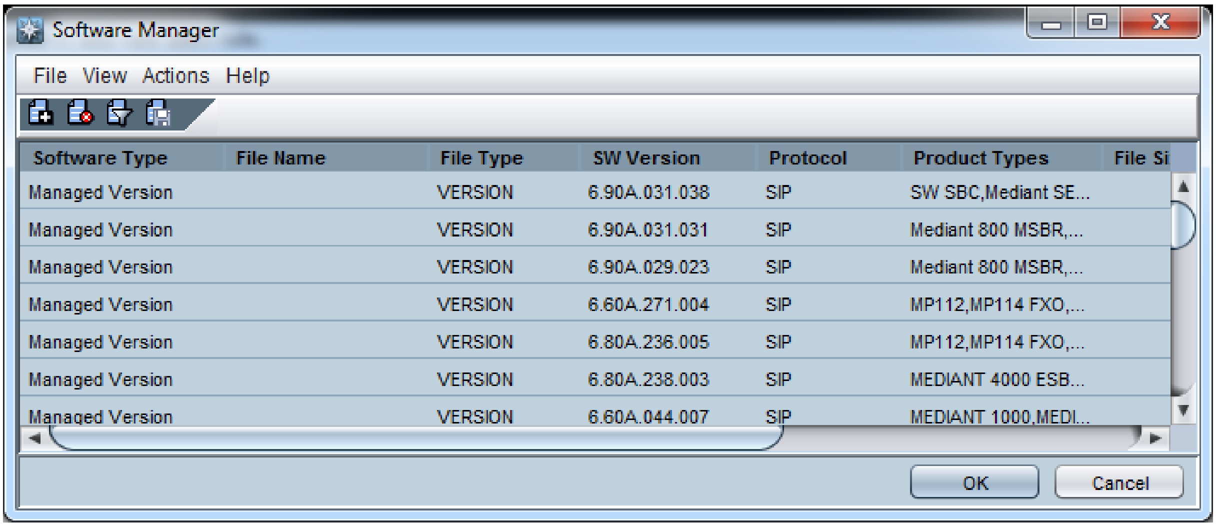
When you choose a .cmp or rmt/rms file, the corresponding firmware version is displayed as well as the products that are supported for this file.

Notes:

- When choosing a .cmp or rmt/rms 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 or conf file and can *optionally* select a .cmp or rmt/rms file.
- This feature is not supported for CloudBond devices.

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

Figure 5-15: Software Manager



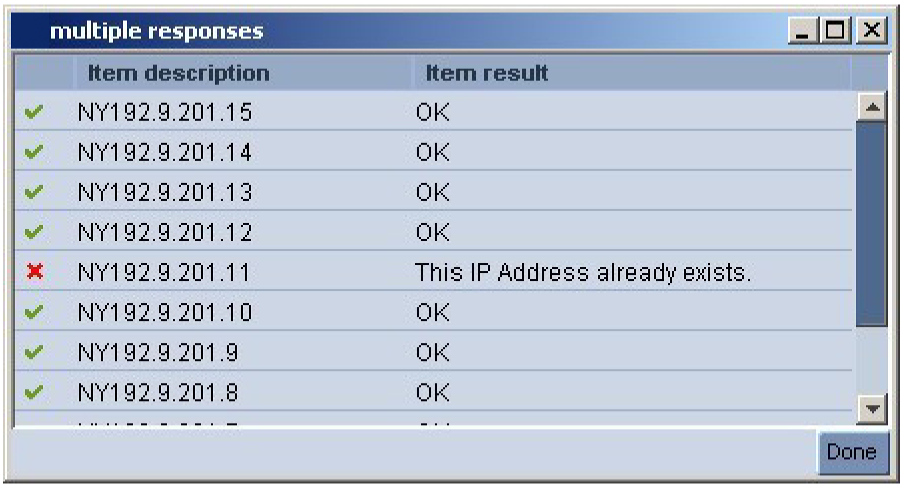
Software Type	File Name	File Type	SW Version	Protocol	Product Types	File Si
Managed Version		VERSION	6.90A.031.038	SIP	SW SBC,Mediant SE...	
Managed Version		VERSION	6.90A.031.031	SIP	Mediant 800 MSBR,...	
Managed Version		VERSION	6.90A.029.023	SIP	Mediant 800 MSBR,...	
Managed Version		VERSION	6.60A.271.004	SIP	MP112,MP114 FXO,...	
Managed Version		VERSION	6.80A.236.005	SIP	MP112,MP114 FXO,...	
Managed Version		VERSION	6.80A.238.003	SIP	MEDIANT 4000 ESB...	
Managed Version		VERSION	6.60A.044.007	SIP	MEDIANT 1000,MEDI...	

11. 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).

12. If you wish to secure the connection with device, set the 'Enable HTTPS Connection' option. For more information on HTTPS, see Chapter 42.
13. Click **OK**; an Action Report is displayed, indicating the result of the add action for each device added.

Figure 5-16: Action Report for Adding Multiple Devices Result



multiple responses

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

7 Configuring SNMP

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.

You must configure the SNMP connection on both the EMS server and on the device.

- Configuring SNMP on devices (see Section 7.1)
- Configuring SNMP on the EMS (see Section 07.2)

7.1 Configuring Device SNMP Settings

Before connecting devices to the EMS, you must configure the SNMP connection between the device and the EMS. SNMP is used for establishing the initial connection with the device and then for every day operations including maintenance actions and fault and performance management.

You need to configure the following SNMP parameters:

- The SNMP Manager: specifies the IP address of the EMS server. All traps are sent from the device to this address. For establishing the connection with the EMS, this is the destination address for the coldStart and Keep-alive traps.
- SNMP Manager Trap User: associates a SNMPv2 or SNMPv3 trap user with the EMS server destination. The Keep-alive trap indicates whether the device is configured for SNMPv2 or SNMPv3.

  The configured SNMPv2 or SNMPv3 user credentials are verified with the following default EMS configuration:

  - SNMPv2: SNMPReadCommunity string ‘public’ and SNMPWriteCommunity string ‘private’ and Trap User 'trapuser'
  - SNMPv3: User ‘OVOCUser’; Auth protocol ‘SHA’; Privacy protocol ‘AES-128’; password ‘123456789’

  SNMP parameters should be identically configured on both the device and in EMS; however if different credentials to the default values described above are configured on the device, then the device is added to the EMS as “Unknown” until these credentials are updated in the MG Information screen.

Note: If you are connecting devices to the EMS using the IP address method then you do not need to configure the above parameters for establishing an initial connection. However, if you wish to perform fault management i.e. receive traps from the device, then you also need to configure the above parameters.

When you are connecting devices to the EMS using the Auto-detection mechanism or when pre-defining a device using the serial number, you need to also configure the following parameters:

- Send Keep Alive Trap: Enables the device to send keep-alive traps to the EMS. This is used for NAT traversal, and allows SNMP communication with AudioCodes EMS management platform, located in the WAN, when the device is located behind NAT. It is needed to keep the NAT pinhole open for the SNMP messages sent from EMS to the device.
- KeepAliveTrapPort: Defines the EMS port to which the device sends keep-alive traps.

Note: The SNMP Port, SNMPManagerTrapPort, SNMPManagerTrapSendingEnable and NatBindingDefaultTimeout are configured by default on the device with the values shown below.

➢ To configure SNMP on devices:

1. Open the devices AdminPage (deviceIPaddress/AdminPage)and configure the following ini parameters:

```
SNMPPort = 161
SNMPManagerTrapPort = 162
SNMPManagerIsUsed = 1
SNMPManagerTrapSendingEnable = 1
SNMPManagerTableIP = <EMS_IP_Address>
SNMPManagerTrapUser = <SNMPv2 user community string> or <SNMPv3 user>
```

2. In the event where the device is configured behind a NAT and you have added the device to the EMS by it's serial number or using Auto-detection, you also need to configure the following:

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

3. Reset the device with burn to apply the changes.

7.2 Configuring EMS SNMP Settings

This section describes how to modify the SNMP configuration after devices are already connected to the EMS. The following topics are described:

- Configuring SNMPv3 (see Section 7.2.1)
- Modifying SNMPv2 Community Strings or SNMPv3 passwords (see Section 7.2.2)
- Configuring Additional SNMPv3 Users (see Section 7.2.3)
- SNMPv3 User Cloning (see Section 7.2.4)

7.2.1 Configuring SNMPv3

This section describes how to configure SNMPv3.

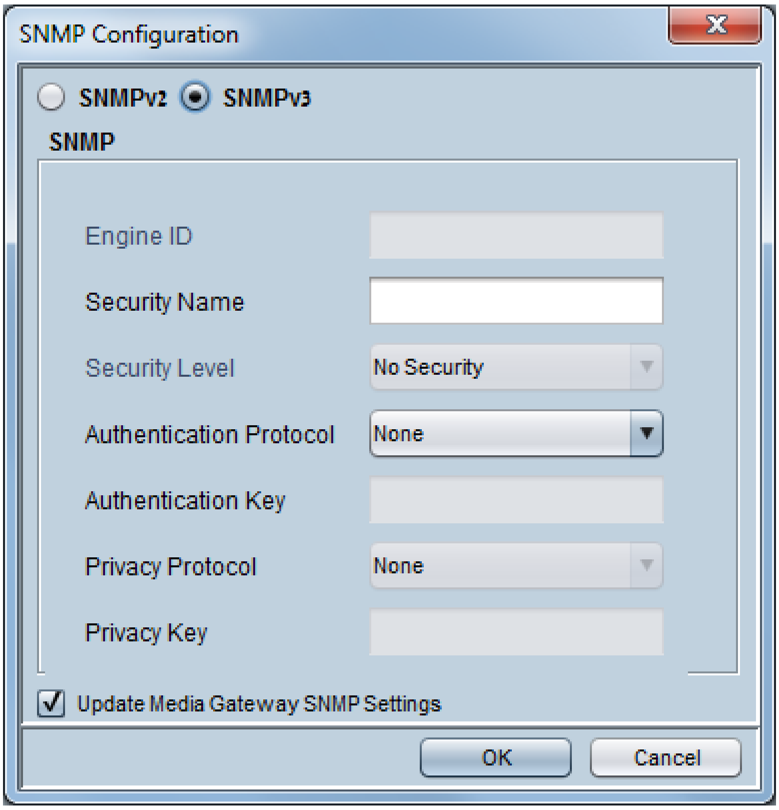
➢ **To configure the device connection with an SNMPv3 user:**

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;
5. In the Privacy Protocol field, select a Privacy Protocol from the drop-down list box;
6. 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 devices (multiple selections are relevant when all the devices are updated to the same community strings / passwords).
2. Right-click **Configuration** ► **SNMP Configuration** option. The SNMP Configuration screen is displayed.

Figure 34-1: MG Information-New SNMPv3 User



○ SNMPv2 ● SNMPv3

SNMP

Engine ID:

Security Name:

Security Level: No Security

Authentication Protocol: None

Authentication Key:

Privacy Protocol: None

Privacy Key:

☑ Update Media Gateway SNMP Settings

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.

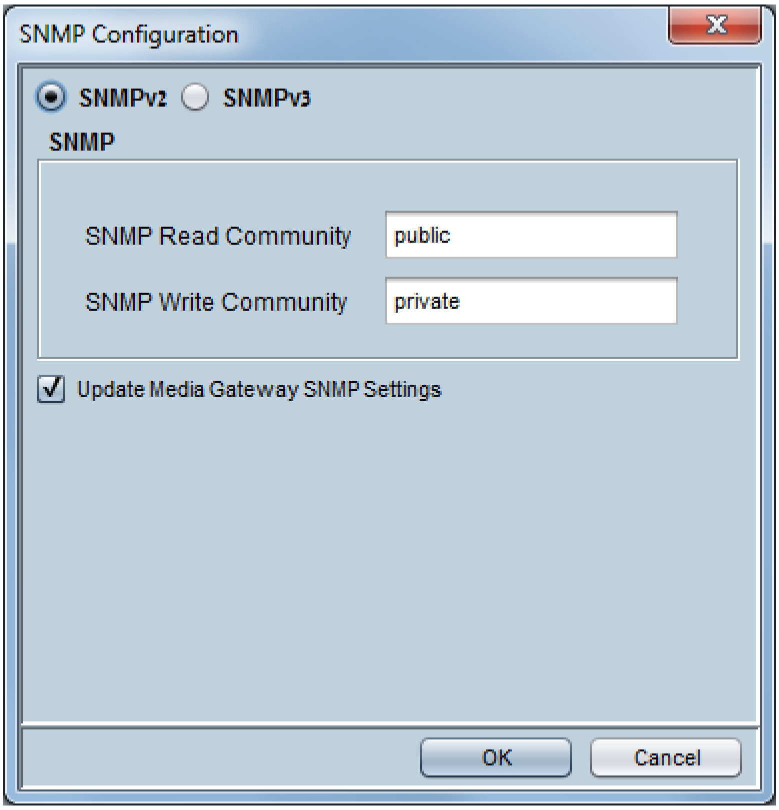
7.2.2 Modifying SNMPv2 Community Strings or SNMPv3 Passwords

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) and right-click **Configuration** ▶ **SNMP Configuration** option.

Figure 34-2: Update SNMPv2 Settings for Multiple Devices


SNMP Configuration

● SNMPv2 ○ SNMPv3

SNMP

SNMP Read Community: public

SNMP Write Community: private

☑ Update Media Gateway SNMP Settings

2. Update SNMPv2 community strings / or SNMPv3 Users passwords.
3. Select the 'Update Media Gateway SNMP Settings' check box.

7.2.3 Configuring Additional SNMPv3 Users

You can configure additional SNMPv3 users with different security permissions or for sending traps to another SNMP Trap 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.*

7.2.4 SNMPv3 User Cloning

According to the SNMPv3 standard, SNMPv3 users on the 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.

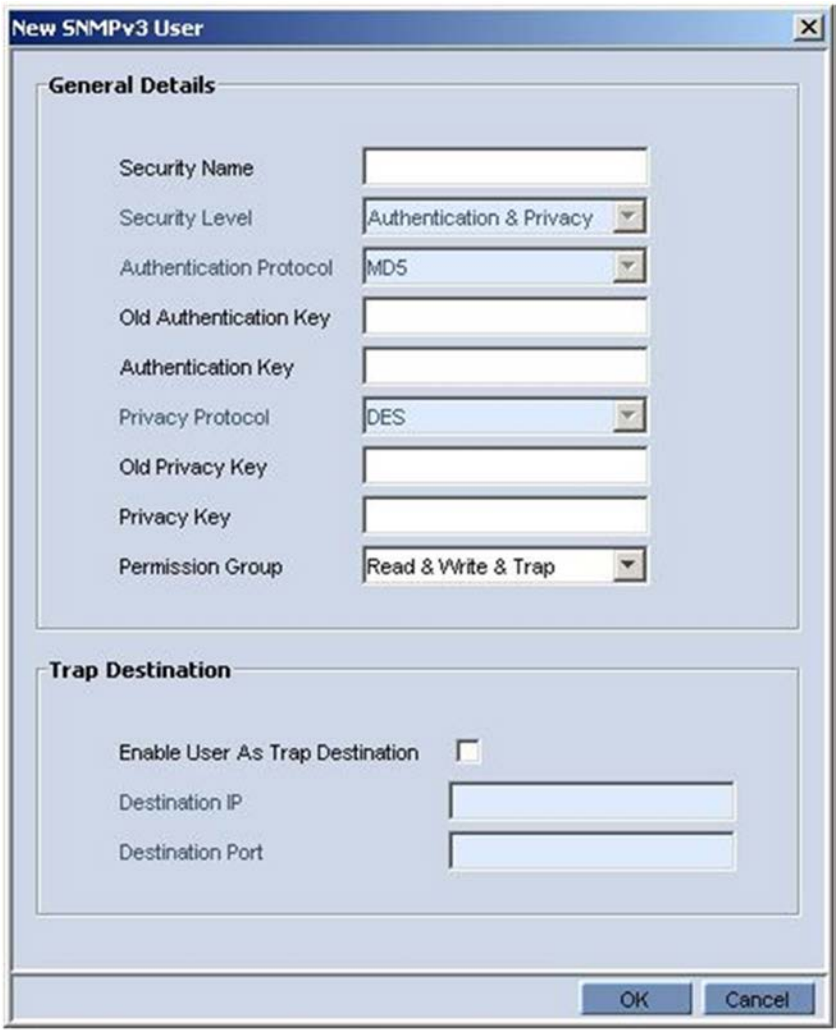
Note: The procedure below is only relevant for managed devices running firmware prior to version 7.0.

➢ 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 34-3: MG Information Screen-New SNMPv3 User



New SNMPv3 User

General Details

Security Name	
Security Level	Authentication & Privacy
Authentication Protocol	MD5
Old Authentication Key	
Authentication Key	
Privacy Protocol	DES
Old Privacy Key	
Privacy Key	
Permission Group	Read & Write & Trap

Trap Destination

Enable User As Trap Destination	□
Destination IP	
Destination Port	

This page is intentionally left blank.

8 Troubleshooting Initial Connection

This section describes issues that may arise when attempting to initially connect devices to the EMS. The following issues are described:

- Failure to Connect to a Device - all Devices
- Devices Connected to the Network
- Devices not Connected to the Network
- First-Time Connection Problems
- Mismatch Indications

8.1 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:

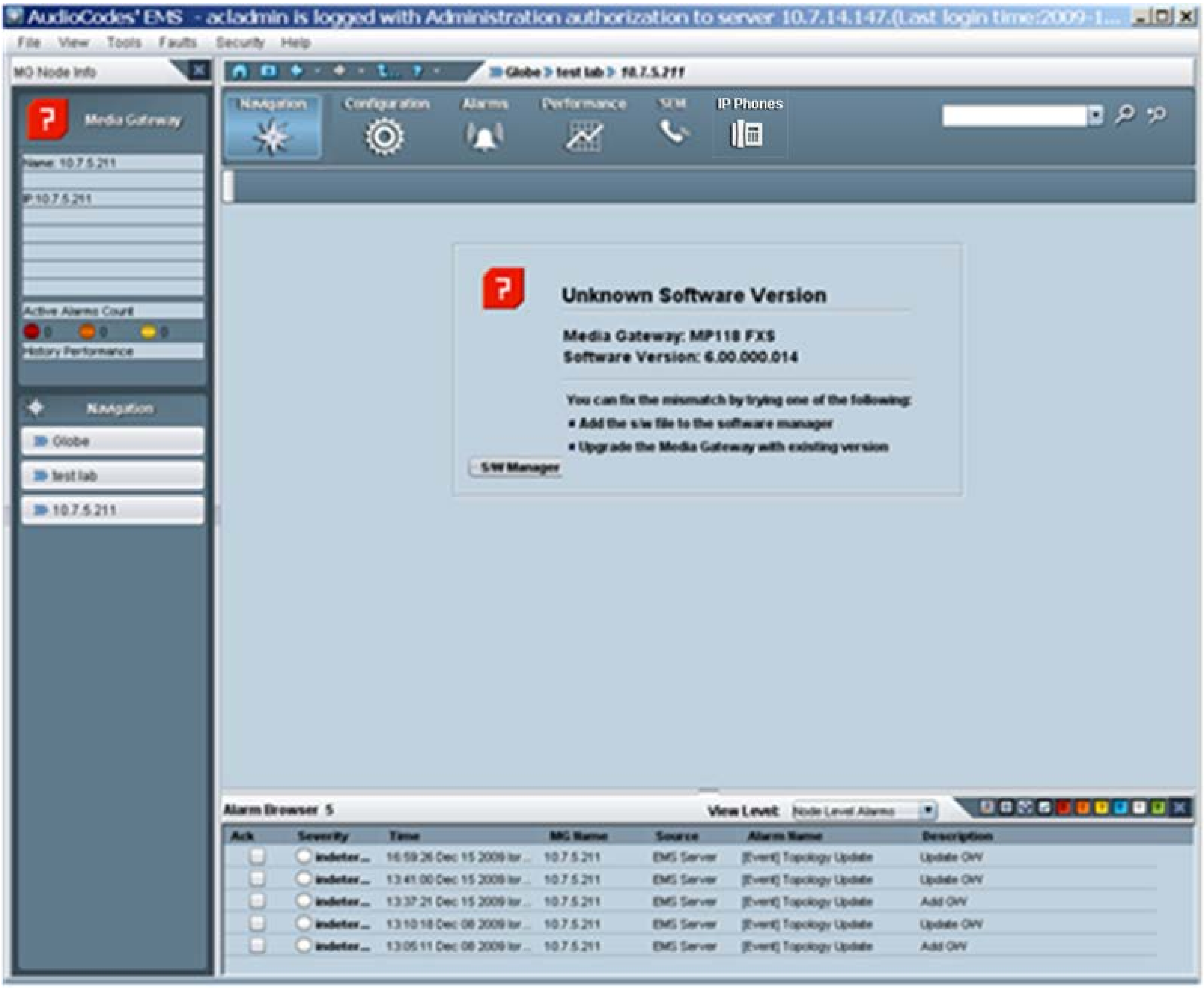
1. You've incorrectly defined the IP address of the device you're attempting to connect to (in the MG Information screen; see the figure 'Incorrectly Defined MG Information Screen', below).
2. An operational problem exists in the system (lack of communication with the server, for example).
3. A network 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 75). 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


AudioCodes' EMS - acladmin is logged with Administration authorization to server 10.7.14.147.(Last login time:2009-1...
File View Tools Faults Security Help
MG Node Info
Media Gateway
Name: 10.7.5.211
IP 10.7.5.211
Active Alarms Count
History Performance
Navigation
Globe
test lab
10.7.5.211
Globe > test lab > 10.7.5.211
Navigation
Configuration
Alarms
Performance
SEM
IP Phones
S/W Manager
View Level: Node Level Alarms

Unknown Software Version

Media Gateway: MP118 FXS
Software Version: 6.00.000.014

You can fix the mismatch by trying one of the following:
- Add the s/w file to the software manager
- Upgrade the Media Gateway with existing version

Alarm Browser 5

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	○ indeter...	16:59:26 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:41:00 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:37:21 Dec 15 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Add GW
□	○ indeter...	13:10:18 Dec 08 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Update GW
□	○ indeter...	13:05:11 Dec 08 2009 Isr...	10.7.5.211	EMS Server	[Event] Topology Update	Add GW

8.2 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 367 to resolve the issue (or contact AudioCodes).

8.3 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 367 to resolve the issue (or contact AudioCodes).

8.4 First-Time Connection Problems

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

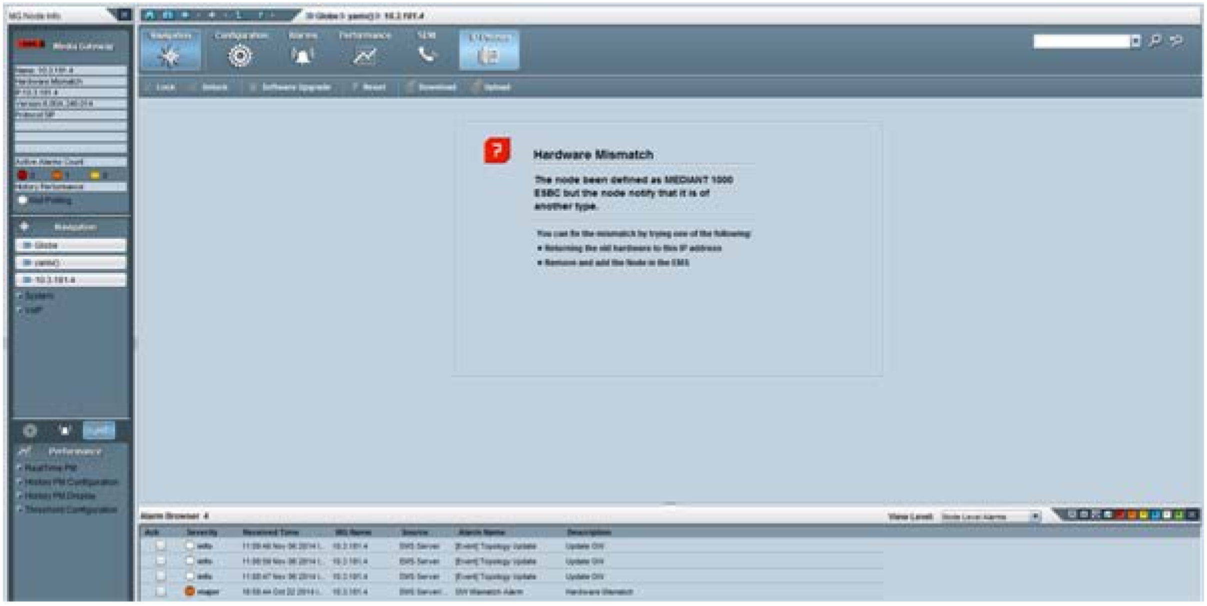
- **Unknown Hardware:** The Product Type, returned by the MIBII sysDescr value, is not recognized by the EMS. The device cannot be managed by the EMS.
- **Unknown Software**: The Software Version, returned by the MIBII sysDescr value, is not recognized by the EMS. Either add the specified version to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

8.5 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**: 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**: '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 5-2: Mediant 2000 Information pane Indicating Mismatch



Hardware Mismatch

The node been defined as MEDIANT 1000 ESBC but the node notify that it is of another type.

You can fix the mismatch by trying one of the following:

- Returning the old hardware to this IP address
- Remove and add the Node in the EMS

Alarm Browser 4

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	info	11:09:46 Nov 06 2014 I...	10.3.181.4	EMS Server	[Event] Topology Update	Update GW
□	info	11:08:58 Nov 06 2014 I...	10.3.181.4	EMS Server	[Event] Topology Update	Update GW
□	info	11:08:47 Nov 06 2014 I...	10.3.181.4	EMS Server	[Event] Topology Update	Update GW
□	major	18:58:44 Oct 22 2014 I...	10.3.181.4	EMS Server...	GW Mismatch Alarm	Hardware Mismatch

This page is intentionally left blank.

9 Managing Devices and Regions

This chapter describes basic management of devices and regions.

9.1 Searching for a Device

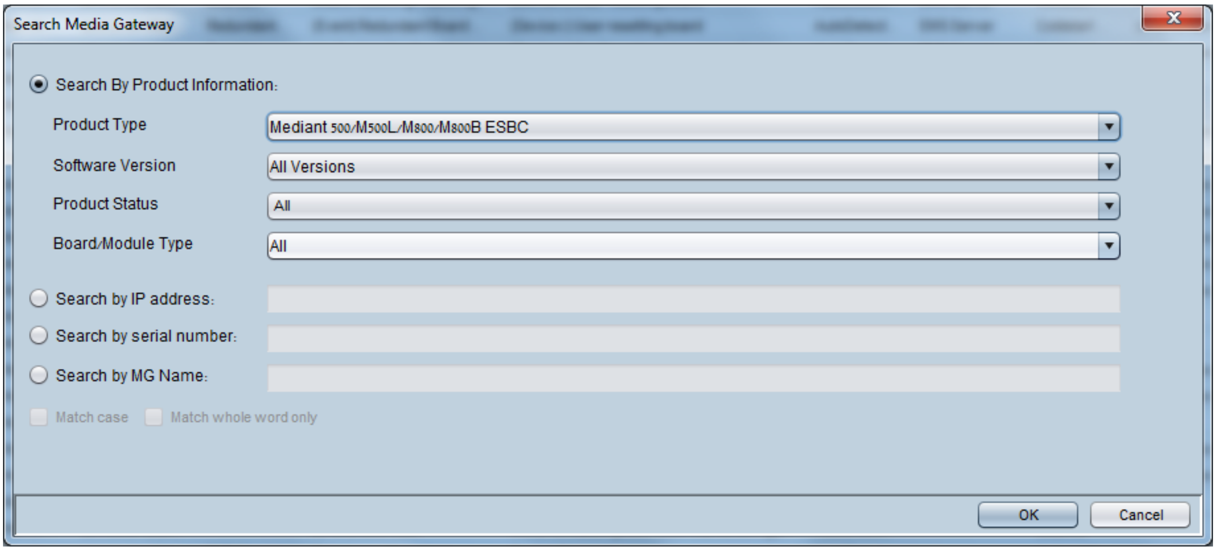
This section describes how to search for a device.

➢ 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 5-1: Search MGs



Search Media Gateway

● Search By Product Information:

Product Type: Mediant 500/M500L/M800/M800B ESBC

Software Version: All Versions

Product Status: All

Board/Module Type: All

○ Search by IP address:

○ Search by serial number:

○ Search by MG Name:

□ Match case □ Match whole word only

2. Search by Product Information: Enter the following 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.
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.

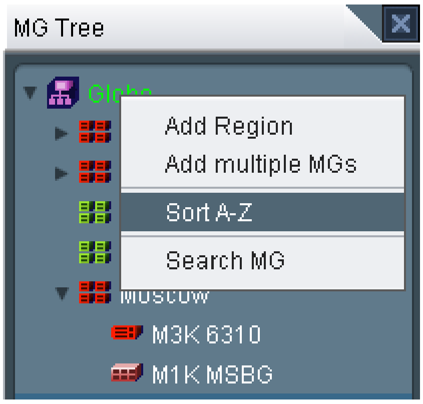
9.2 Sorting Regions and Devices

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 5-2: Sort Regions



9.3 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.

9.4 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 5-3: Moving Multiple MGs from Region to Region

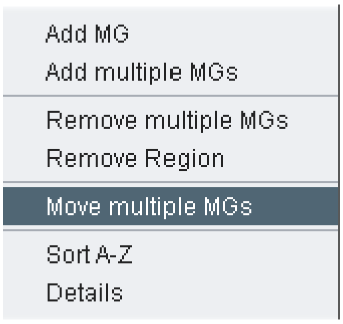
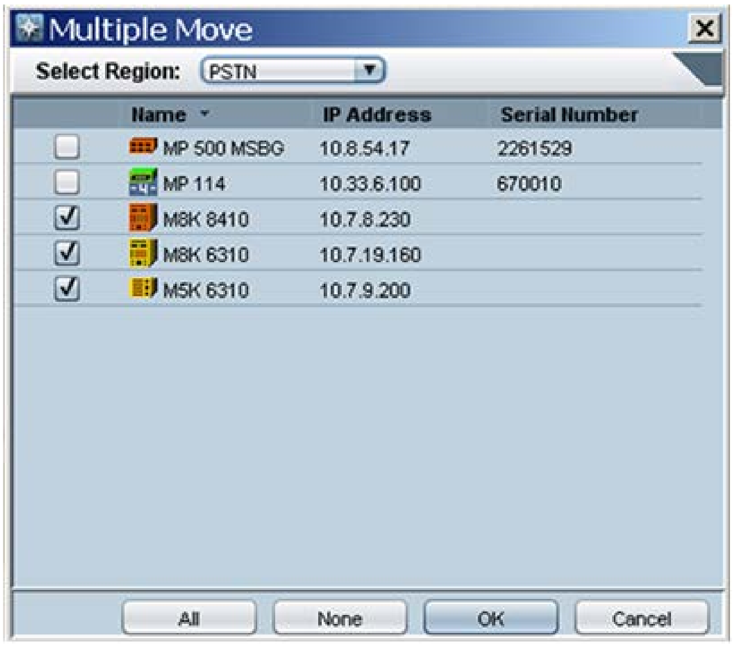


Figure 5-4: Multiple Move from Region to Region



Select Region: PSTN

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

2. In the 'Multiple Move' screen, select the 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.

9.5 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.

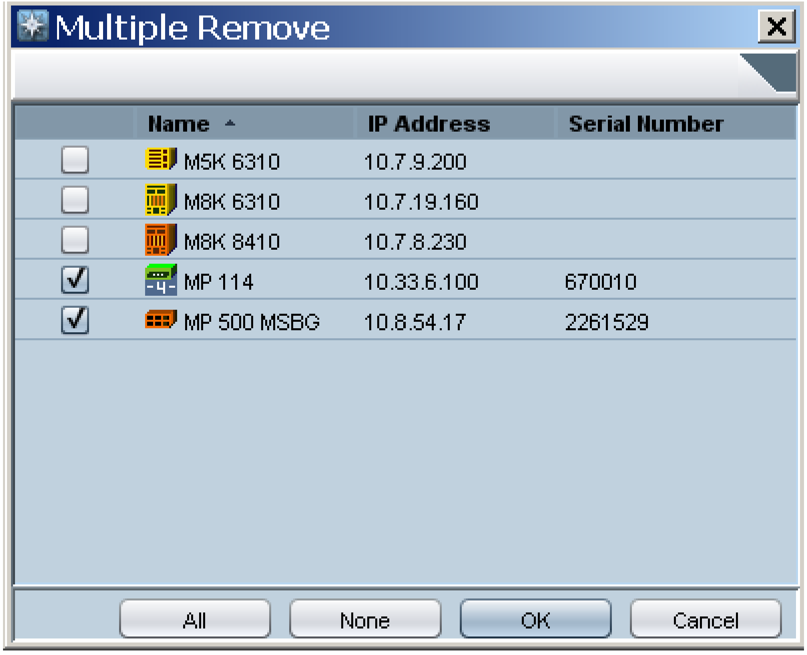
9.6 Removing Multiple Devices

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.

➢ 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 5-5: Removing Multiple Devices



Multiple Remove

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

2. 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.

9.7 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**.

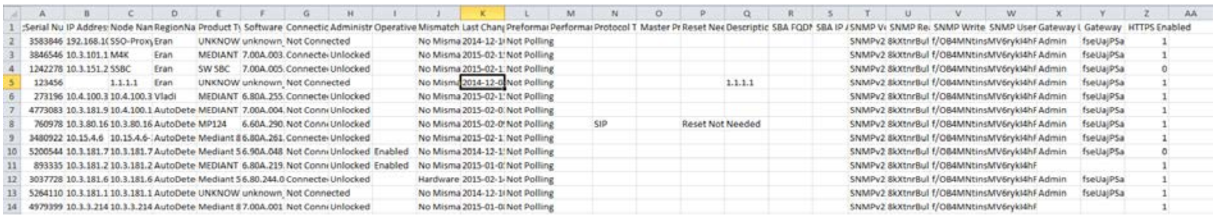
   The File is stored in the CSV format in the required location and includes the following field columns:

   - Serial Number
   - 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
- 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 5-6: Device Pre-Definition File



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1	;Serial Nu	IP Addres	Node Nan	RegionNa	Product Ty	Software	Connectic	Administr	Operative	Mismatch	Last Chang	Preformai	Performai	Protocol T	Master Pr	Reset Nee	Descriptic	SBA FQDN	SBA IP A	SNMP Ve	SNMP Re	SNMP Write	SNMP User	Gateway U	Gateway	HTTPS Enabled	
2	3583846	192.168.1(	SSO-Proxy	Eran	UNKNOW	unknown_	Not Connected			No Misma	2014-12-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
3	3846546	10.3.101.1	M4K	Eran	MEDIANT	7.00A.003.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
4	1242278	10.3.151.2	SSBC	Eran	SW SBC	7.00A.005.	Connecte	Unlocked		No Misma	2015-02-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	0	
5	123456		1.1.1.1	Eran	UNKNOW	unknown_	Not Connected			No Misma	2014-12-0	Not Polling					1.1.1.1			SNMPv2	8kXtnrBul	f/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
6	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
7	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
8	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
9	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
10	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	0	
11	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/OB4MNtinsMV6rykl4hF				1	
12	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/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
13	5264110	10.3.181.1	10.3.181.1	AutoDete	UNKNOW	unknown_	Not Connected			No Misma	2014-12-1	Not Polling								SNMPv2	8kXtnrBul	f/OB4MNtinsMV6rykl4hF		Admin	fseUajPSa	1	
14	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/OB4MNtinsMV6rykl4hF				1	

This page is intentionally left blank.

10 EMS Application Welcome Message

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

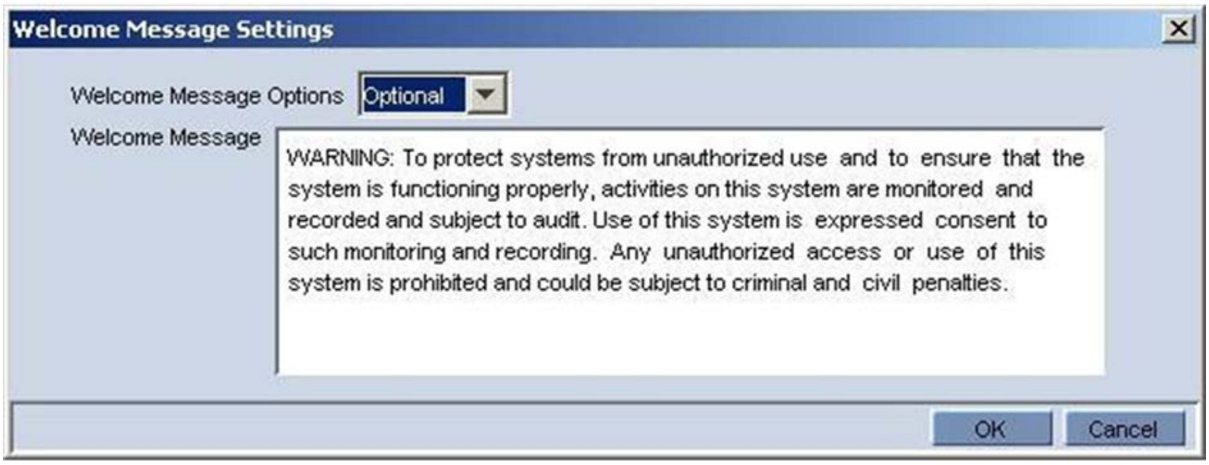
The Administrator can set a welcome message note using the Help -> Advisory Message menu.

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

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

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

Figure 5-1: Welcome Message Settings

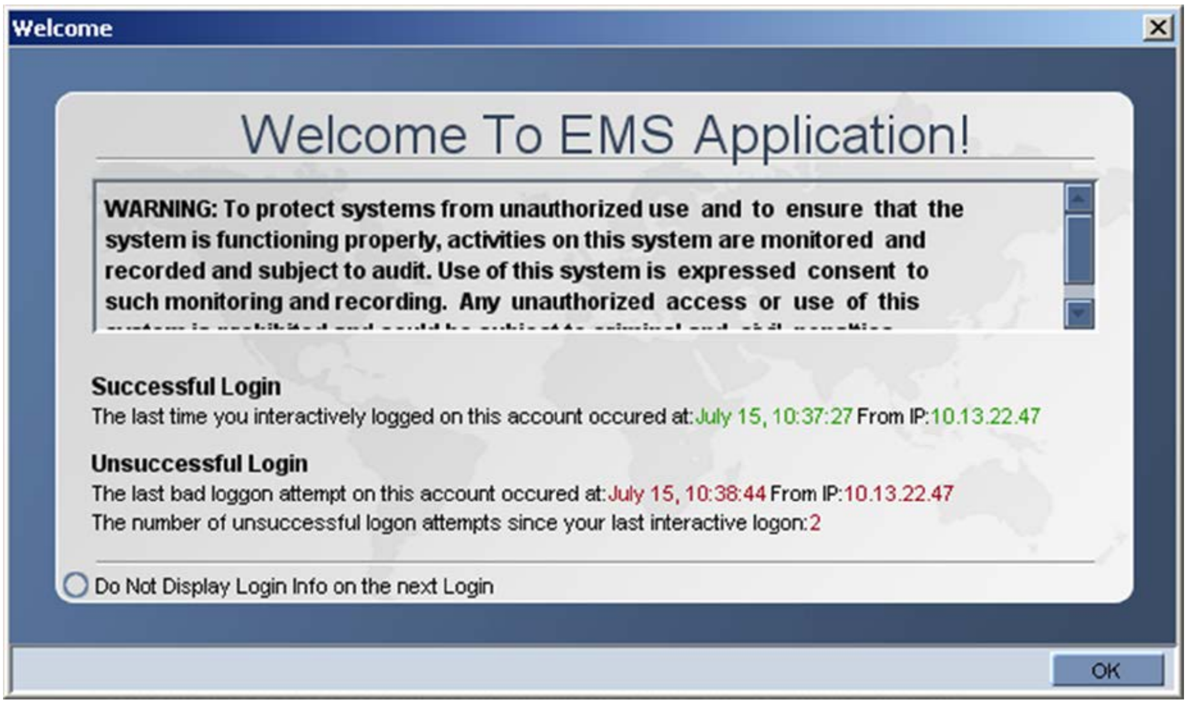


Welcome Message Settings

Welcome Message Options: Optional

Welcome Message: WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.

Figure 5-2: Welcome Message with Login Information



Welcome

Welcome To EMS Application!

WARNING: To protect systems from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this

Successful Login

The last time you interactively logged on this account occured at:July 15, 10:37:27 From IP:10.13.22.47

Unsuccessful Login

The last bad loggon attempt on this account occured at:July 15, 10:38:44 From IP:10.13.22.47

The number of unsuccessful logon attempts since your last interactive logon:2

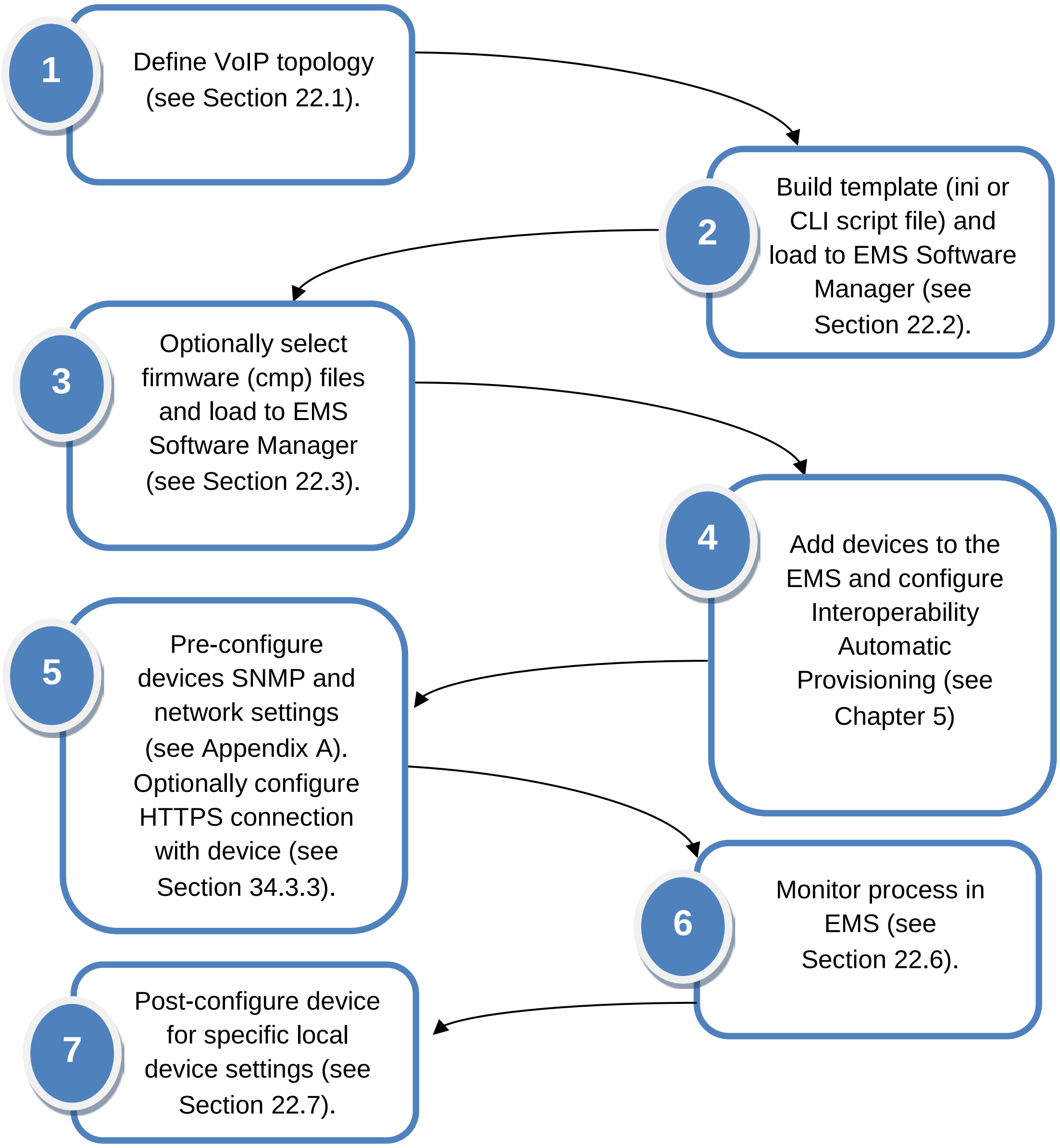
○ Do Not Display Login Info on the next Login

11 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.

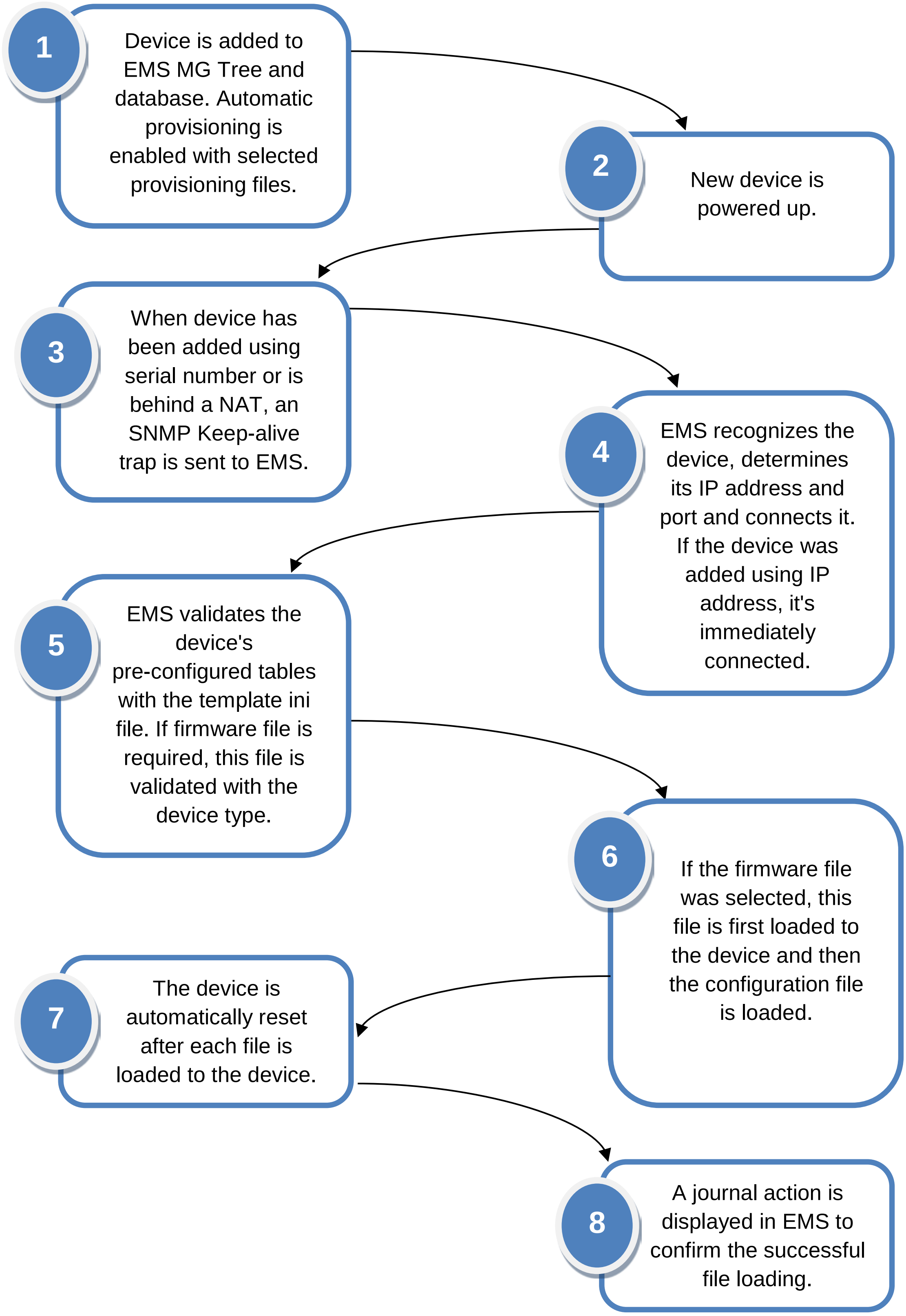
The following figure guides you step-by-step through the required actions in the Interoperability Automatic Provisioning process with the appropriate procedure references:

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


1
Define VoIP topology (see Section 22.1).
2
Build template (ini or CLI script file) and load to EMS Software Manager (see Section 22.2).
3
Optionally select firmware (cmp) files and load to EMS Software Manager (see Section 22.3).
4
Add devices to the EMS and configure Interoperability Automatic Provisioning (see Chapter 5)
5
Pre-configure devices SNMP and network settings (see Appendix A). Optionally configure HTTPS connection with device (see Section 34.3.3).
6
Monitor process in EMS (see Section 22.6).
7
Post-configure device for specific local device settings (see Section 22.7).

The following figure illustrates the Interoperability Automatic Provisioning process flow.

Figure 22-2: Interoperability Automatic Provisioning Process Flow


1
Device is added to EMS MG Tree and database. Automatic provisioning is enabled with selected provisioning files.
2
New device is powered up.
3
When device has been added using serial number or is behind a NAT, an SNMP Keep-alive trap is sent to EMS.
4
EMS recognizes the device, determines its IP address and port and connects it. If the device was added using IP address, it's immediately connected.
5
EMS validates the device's pre-configured tables with the template ini file. If firmware file is required, this file is validated with the device type.
6
If the firmware file was selected, this file is first loaded to the device and then the configuration file is loaded.
7
The device is automatically reset after each file is loaded to the device.
8
A journal action is displayed in EMS to confirm the successful file loading.

11.1 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.

11.1.1 AudioCodes Devices

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

11.1.2 SIP Trunking

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

11.1.3 Microsoft Lync Server

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

11.1.4 Contact Center

- Vendor
- Software Version
- Protocol
- Additional Notes

11.1.5 IP-PBX

- Vendor
- Software Version
- Protocol
- Additional Notes

11.1.6 Environment Setup

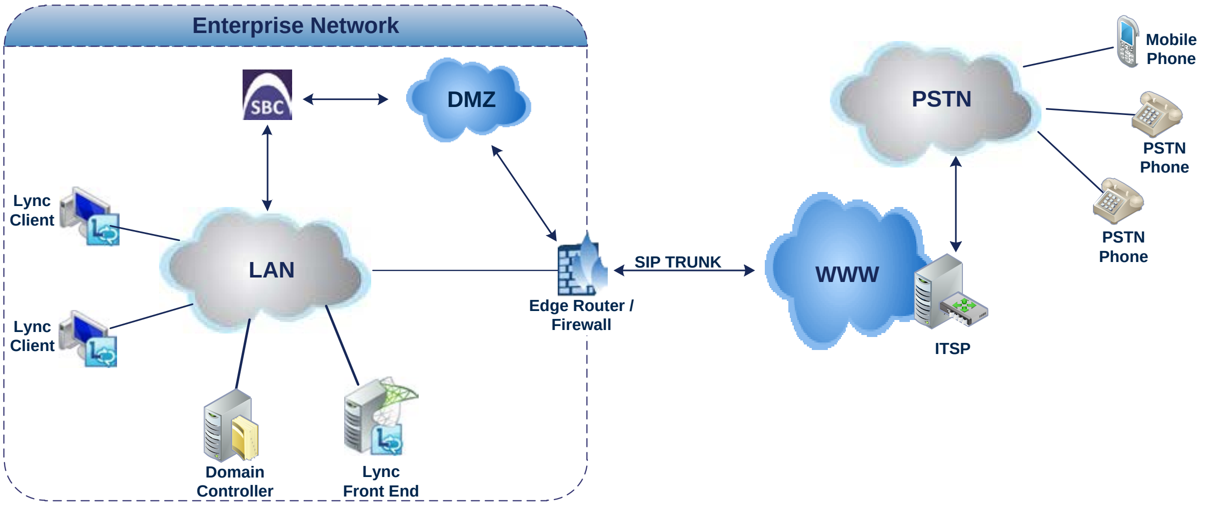
The table below illustrates an example environment setup:

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



11.2 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). 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 can 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.
- 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).

Note:

- 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.

11.3 Step 3: Selecting Firmware Files (Optional)

You can also optionally pre-provision devices with firmware files. Ensure that the selected files are for Version 7.0 firmware and later 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.

11.4 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).

11.5 Step 5: Pre-Configuring Devices

You must pre-configure the device's network (see Appendix A) and SNMP settings (see Section 7.1). 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 6.2.1 on page 81).
- 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 Appendix Custom X.509 Certificates- Supplementary Procedures in the *EMS Server IOM*).

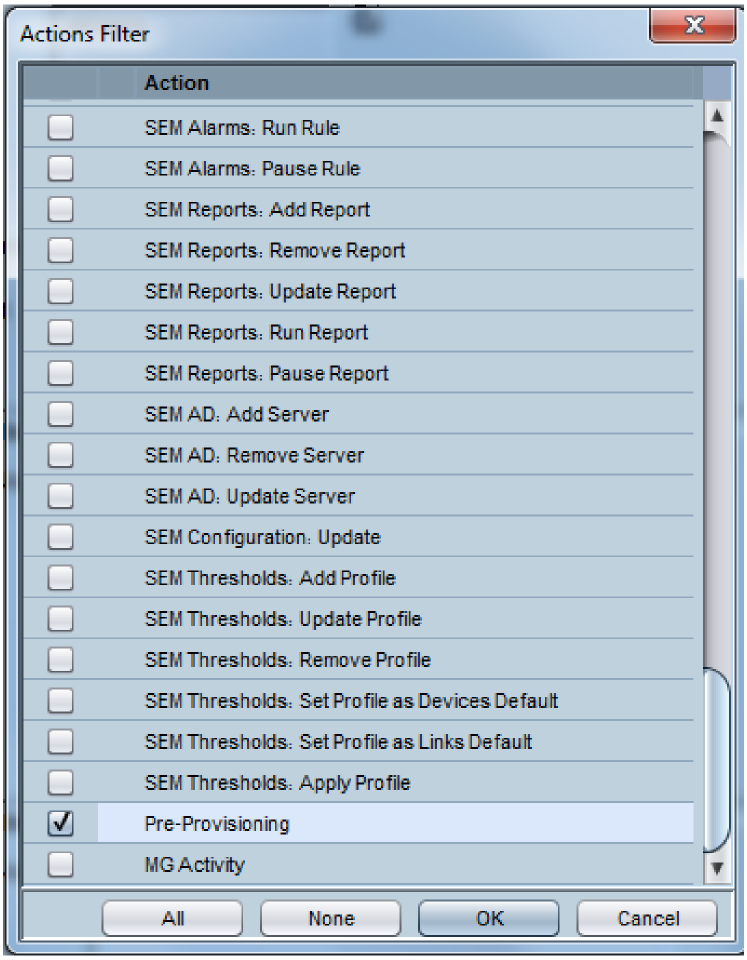
11.6 Step 6: Monitoring Interoperability Automatic Provisioning Process in EMS

Once the device is successfully fully connected to the EMS, the pre-configured configuration and optionally firmware files are loaded.

11.6.1 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

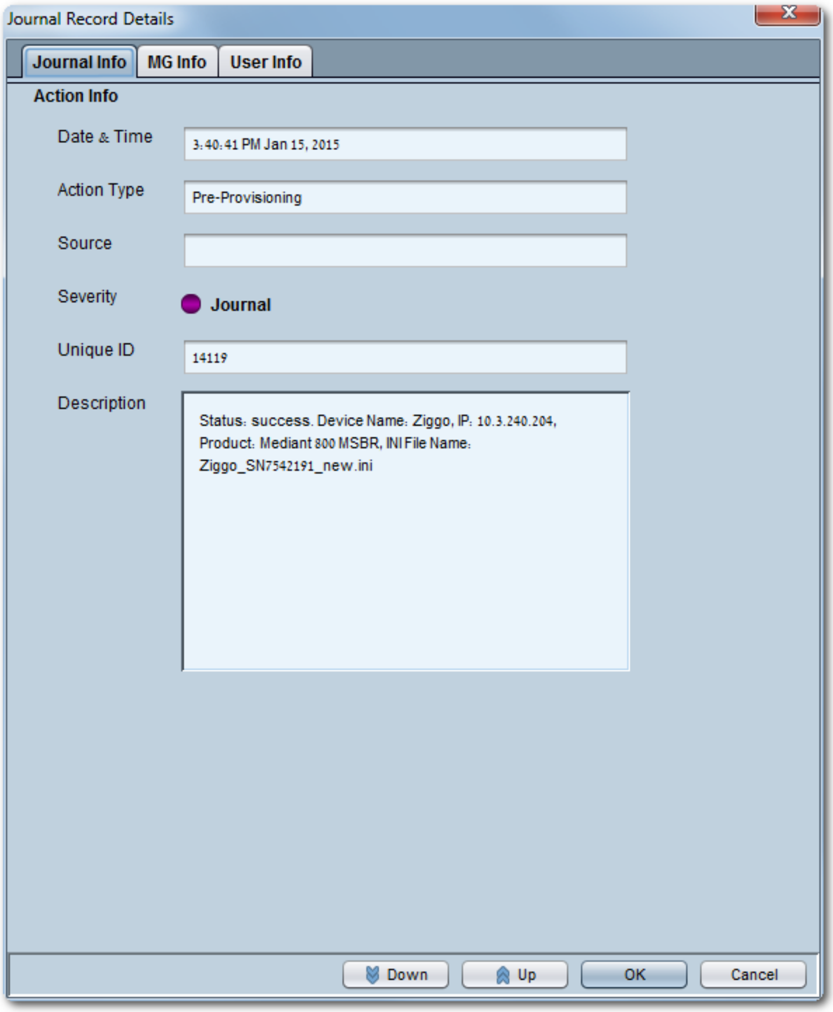


Actions Filter

	Action
□	SEM Alarms: Run Rule
□	SEM Alarms: Pause Rule
□	SEM Reports: Add Report
□	SEM Reports: Remove Report
□	SEM Reports: Update Report
□	SEM Reports: Run Report
□	SEM Reports: Pause Report
□	SEM AD: Add Server
□	SEM AD: Remove Server
□	SEM AD: Update Server
□	SEM Configuration: Update
□	SEM Thresholds: Add Profile
□	SEM Thresholds: Update Profile
□	SEM Thresholds: Remove Profile
□	SEM Thresholds: Set Profile as Devices Default
□	SEM Thresholds: Set Profile as Links Default
□	SEM Thresholds: Apply Profile
☑	Pre-Provisioning
□	MG Activity

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



Action Info

Date & Time: 3:40:41 PM Jan 15, 2015

Action Type: Pre-Provisioning

Source:

Severity: ● Journal

Unique ID: 14119

Description: Status: success. Device Name: Ziggo, IP: 10.3.240.204, Product: Mediant 800 MSBR, INI File Name: Ziggo_SN7542191_new.ini

c

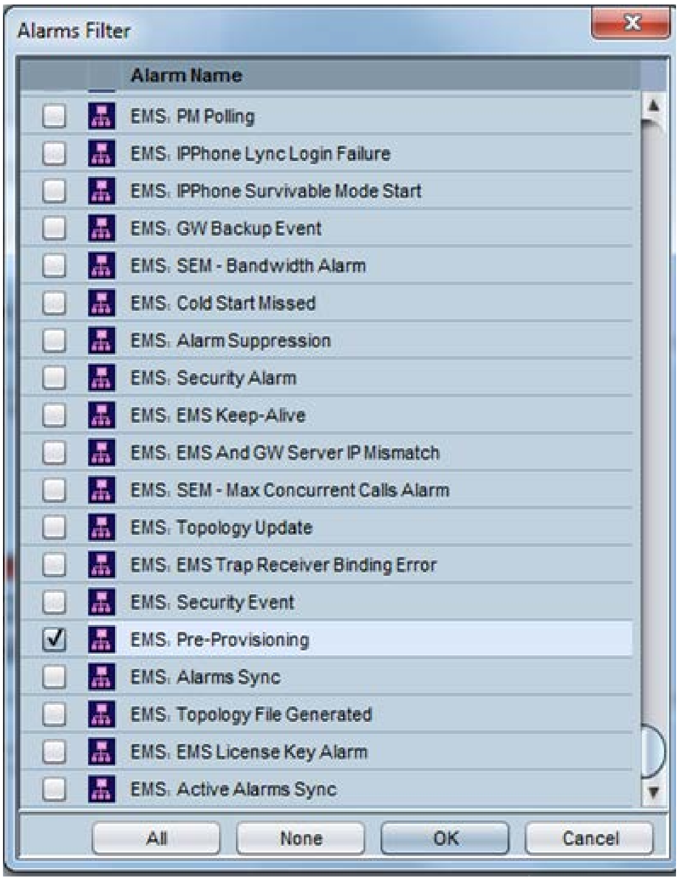
Note:

- 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 6).
- 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 Chapter 7.1).

11.6.2 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:

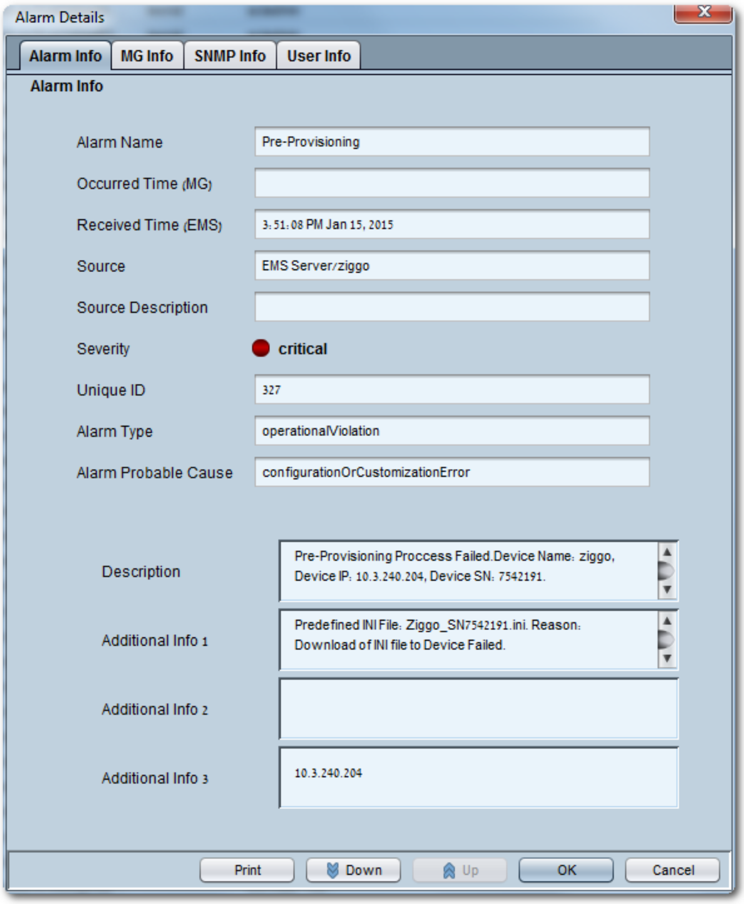
Figure 22-6: Alarms Filter



	Alarm Name
□	EMS: PM Polling
□	EMS: IPPhone Lync Login Failure
□	EMS: IPPhone Survivable Mode Start
□	EMS: GW Backup Event
□	EMS: SEM - Bandwidth Alarm
□	EMS: Cold Start Missed
□	EMS: Alarm Suppression
□	EMS: Security Alarm
□	EMS: EMS Keep-Alive
□	EMS: EMS And GW Server IP Mismatch
□	EMS: SEM - Max Concurrent Calls Alarm
□	EMS: Topology Update
□	EMS: EMS Trap Receiver Binding Error
□	EMS: Security Event
☑	EMS: Pre-Provisioning
□	EMS: Alarms Sync
□	EMS: Topology File Generated
□	EMS: EMS License Key Alarm
□	EMS: Active Alarms Sync

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



Alarm Name	Pre-Provisioning
Occurred Time (MG)	
Received Time (EMS)	3:51:08 PM Jan 15, 2015
Source	EMS Server/ziggo
Source Description	
Severity	● critical
Unique ID	327
Alarm Type	operationalViolation
Alarm Probable Cause	configurationOrCustomizationError
Description	Pre-Provisioning Proccess Failed.Device Name: ziggo, Device IP: 10.3.240.204, Device SN: 7542191.
Additional Info 1	Predefined INI File: Ziggo_SN7542191.ini. Reason: Download of INI file to Device Failed.
Additional Info 2	
Additional Info 3	10.3.240.204

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).

11.7 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.

This page is intentionally left blank.

12 License Pool Manager

The "License Pool Manager" enables operators to centrally manage and distribute session licenses for multiple devices using a flexible license pool. This feature is relevant for devices running version 7.0 and above. The operator can allocate and de-allocate the licenses for the devices in the pool according to their capacity requirements. This tool enables the following:

- Facilitates license management between devices without changing the devices' local license key.
- Facilitates the adding and removal of licenses for devices according to site requirements without the need to contact AudioCodes.

  The License Pool feature does not require a new License key file per device from AudioCodes each time the user wishes to apply different settings to each device.
- Enables service providers to manage licenses for multiple customers by using the license pool to allocate licenses between them.

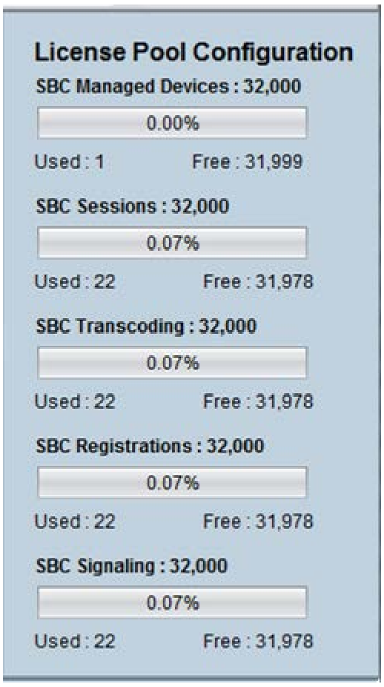
Note:

- This feature is currently not supported for multi-tenants, where each tenant is represented by an EMS region. When a service provider or integrator manages multiple customers, they need to allocate the licenses globally per EMS server installation. In a future release, support will be provided per region; including the ability to configure license sub-pools for each region.
- The License Pool Manager' is available for the EMS "Administrator" security level only.
- The Mediant 3000 and MP-1288 devices are not supported by this feature.

12.1 Licensing Capacity

The maximum license capacity for each of the License Pool session parameters is set in the OVOC Server License that is loaded to the EMS server. These limits and the percentage of utilized and free licenses for each of these license parameters are displayed in the License Pool Configuration Summary panes as shown in the figures below.

Figure 22-1: License Pool Configuration Summary Pane - SBC



License Pool Configuration

SBC Managed Devices : 32,000

0.00%

Used : 1 Free : 31,999

SBC Sessions : 32,000

0.07%

Used : 22 Free : 31,978

SBC Transcoding : 32,000

0.07%

Used : 22 Free : 31,978

SBC Registrations : 32,000

0.07%

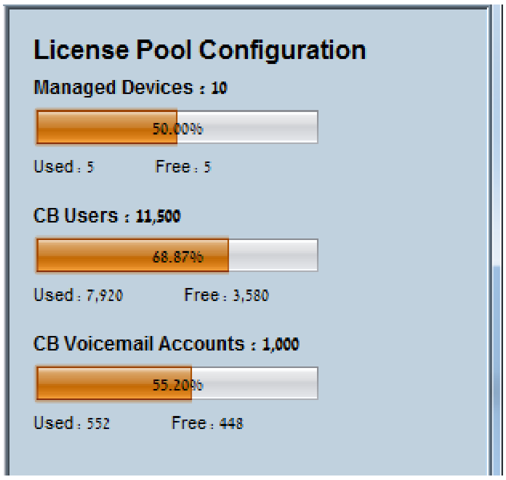
Used : 22 Free : 31,978

SBC Signaling : 32,000

0.07%

Used : 22 Free : 31,978

License Pool Configuration Summary Pane - CloudBond



License Pool Configuration

Managed Devices : 10

50.00%

Used : 5 Free : 5

CB Users : 11,500

68.87%

Used : 7,920 Free : 3,580

CB Voicemail Accounts : 1,000

55.20%

Used : 552 Free : 448

Note:

- When CloudBond/CCE Appliances are managed by the License Pool Manager, the Configuration Summary Pane displays bar graphs with the percentage of utilized and free licenses for the Number of Managed Devices and CloudBond license components.
- All of the above license parameters reflect the number of sessions that are configured per device with the exception of the 'Managed Devices' parameter which reflects the number of devices that are currently managed in the License Pool Manager.

12.2 HA Devices

For an HA device, the number of licenses required to be purchased by the customer is twice the required number of licenses per device (active device + redundant device). For example, if the License Pool Manager Server allocates 200 sessions to the active device, it also allocates 200 sessions to the redundant device. Consequently, customers must take this into consideration when ordering licenses.

Note:

- According to AudioCodes licensing policies, HA devices or boards require an equivalent number of licenses for both the active and redundant devices and boards. For more information, contact your AudioCodes representative.
- When applying a hitless license update to an HA device that exceeds the maximum number of sessions available in the License pool, service is affected. For more information, see Section 12.8.

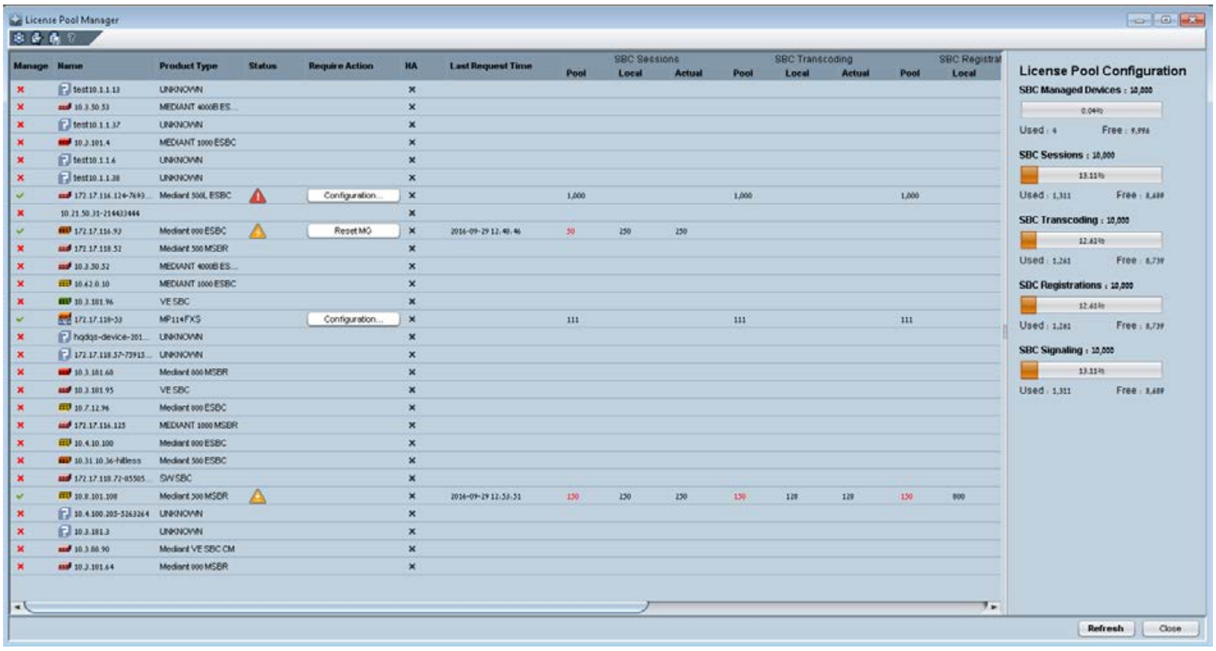
12.3 Accessing the License Pool Manager

The License Pool Manager is in the EMS Tools menu. This screen manages the allocation of pool licenses to the devices in the EMS installation.

➢ **To access the License Pool Manager:**

- In the EMS Main Menu, select **Tools** > **License Pool Manager**. The License Pool Manager screen is displayed:

Figure 22-2: License Pool Manager- SBC Devices



Manage	Name	Product Type	Status	Require Action	HA	Last Request Time	SBC Sessions Pool	SBC Sessions Local	SBC Sessions Actual	SBC Transcoding Pool	SBC Transcoding Local	SBC Transcoding Actual	SBC Registrat Pool	SBC Registrat Local
✗	test10.1.1.13	UNKNOWN			✗									
✗	10.3.50.53	MEDIANT 4000B ES...			✗									
✗	test10.1.1.37	UNKNOWN			✗									
✗	10.3.101.4	MEDIANT 1000 ESBC			✗									
✗	test10.1.1.6	UNKNOWN			✗									
✗	test10.1.1.38	UNKNOWN			✗									
✓	172.17.116.124-7693...	Mediant 500L ESBC	⚠	Configuration...	✗		1,000			1,000			1,000	
✗	10.21.50.31-214433444				✗									
✓	172.17.116.93	Mediant 800 ESBC	⚠	Reset MG	✗	2016-09-29 12:40:46	50	250	250					
✗	172.17.118.52	Mediant 500 MSBR			✗									
✗	10.3.50.52	MEDIANT 4000B ES...			✗									
✗	10.42.0.10	MEDIANT 1000 ESBC			✗									
✗	10.3.101.96	VE SBC			✗									
✓	172.17.118-53	MP114FXS		Configuration...	✗		111			111			111	
✗	hqdqs-device-201...	UNKNOWN			✗									
✗	172.17.118.57-75915...	UNKNOWN			✗									
✗	10.3.101.60	Mediant 800 MSBR			✗									
✗	10.3.101.95	VE SBC			✗									
✗	10.7.12.96	Mediant 800 ESBC			✗									
✗	172.17.116.125	MEDIANT 1000 MSBR			✗									
✗	10.4.10.100	Mediant 800 ESBC			✗									
✗	10.31.10.36-hitless	Mediant 500 ESBC			✗									
✗	172.17.118.72-85505...	SW SBC			✗									
✓	10.8.101.108	Mediant 500 MSBR	⚠		✗	2016-09-29 12:53:31	150	250	250	150	128	128	150	800
✗	10.4.100.205-5263264	UNKNOWN			✗									
✗	10.3.101.3	UNKNOWN			✗									
✗	10.3.80.90	Mediant VE SBC CM			✗									
✗	10.3.101.64	Mediant 800 MSBR			✗									

License Pool Configuration

SBC Managed Devices : 10,000
0.04%
Used : 4 Free : 9,996

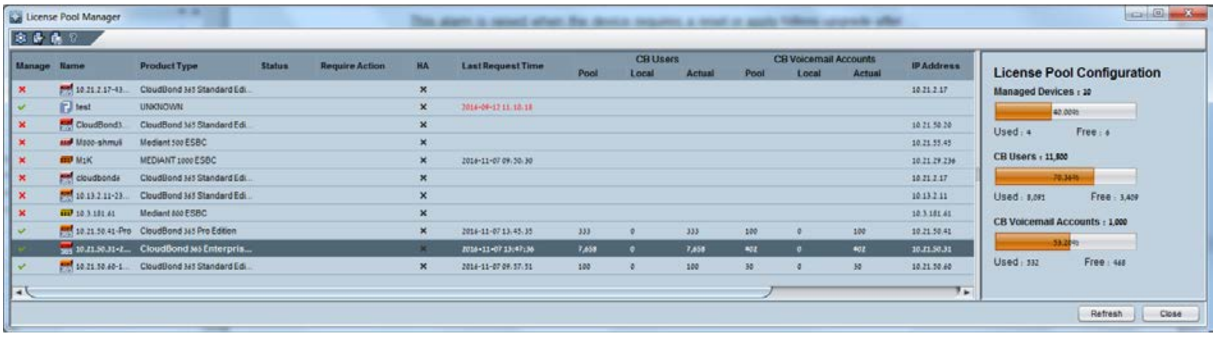
SBC Sessions : 10,000
13.11%
Used : 1,311 Free : 8,689

SBC Transcoding : 10,000
12.61%
Used : 1,261 Free : 8,739

SBC Registrations : 10,000
12.61%
Used : 1,261 Free : 8,739

SBC Signaling : 10,000
13.11%
Used : 1,311 Free : 8,689

Figure 22-3: License Pool Manager - CloudBond Devices



Manage	Name	Product Type	Status	Require Action	HA	Last Request Time	CB Users Pool	CB Users Local	CB Users Actual	CB Voicemail Accounts Pool	CB Voicemail Accounts Local	CB Voicemail Accounts Actual	IP Address
✗	10.21.2.17-43...	CloudBond 365 Standard Edi...			✗								10.21.2.17
✓	test	UNKNOWN			✗	2016-09-12 11:10:18							
✗	CloudBond3...	CloudBond 365 Standard Edi...			✗								10.21.50.20
✗	M500-shmuli	Mediant 500 ESBC			✗								10.21.55.45
✗	M1K	MEDIANT 1000 ESBC			✗	2016-11-07 09:50:30							10.21.29.236
✗	cloudbonds	CloudBond 365 Standard Edi...			✗								10.21.2.17
✗	10.13.2.11-23...	CloudBond 365 Standard Edi...			✗								10.13.2.11
✗	10.3.101.41	Mediant 800 ESBC			✗								10.3.101.41
✓	10.21.50.41-Pro	CloudBond 365 Pro Edition			✗	2016-11-07 13:45:35	333	0	333	100	0	100	10.21.50.41
✓	10.21.50.31-2...	CloudBond 365 Enterpris...			✗	2016-11-07 13:47:36	7,658	0	7,658	402	0	402	10.21.50.31
✓	10.21.50.60-1...	CloudBond 365 Standard Edi...			✗	2016-11-07 09:57:51	100	0	100	50	0	50	10.21.50.60

License Pool Configuration

Managed Devices : 10
40.00%
Used : 4 Free : 6

CB Users : 11,500
70.34%
Used : 8,091 Free : 3,409

CB Voicemail Accounts : 1,000
53.20%
Used : 532 Free : 468

The License Pool Manager displays all version 7.0 and above devices.

Note:

- Undefined devices are also displayed in the License Pool Manager. In the event where a device is connected to the EMS and it is later discovered that the device is running firmware prior to version 7.0, the device is displayed in the License Pool Manager until the operator configures the device to not be managed by the License Pool Manager (see Section 12.5 below).
- The device is identified by the License Manager by its serial number.
- The CloudBond/CCE Appliance license parameters are only displayed in the License Pool Manager if they are currently configured in the EMS license.

The operator can manage the following license parameters using the ‘License Pool’:

- The number of SBC sessions (media and signaling)
- The number of SBC Transcoding sessions
- The number of SBC Registrations (number of SIP endpoints that can register with the SBC)
- The number of SBC Signaling sessions
- The number of CB user sessions
- The number of CB PBX users
- The number of CB analog devices (for future use)
- The number of CB voicemail accounts

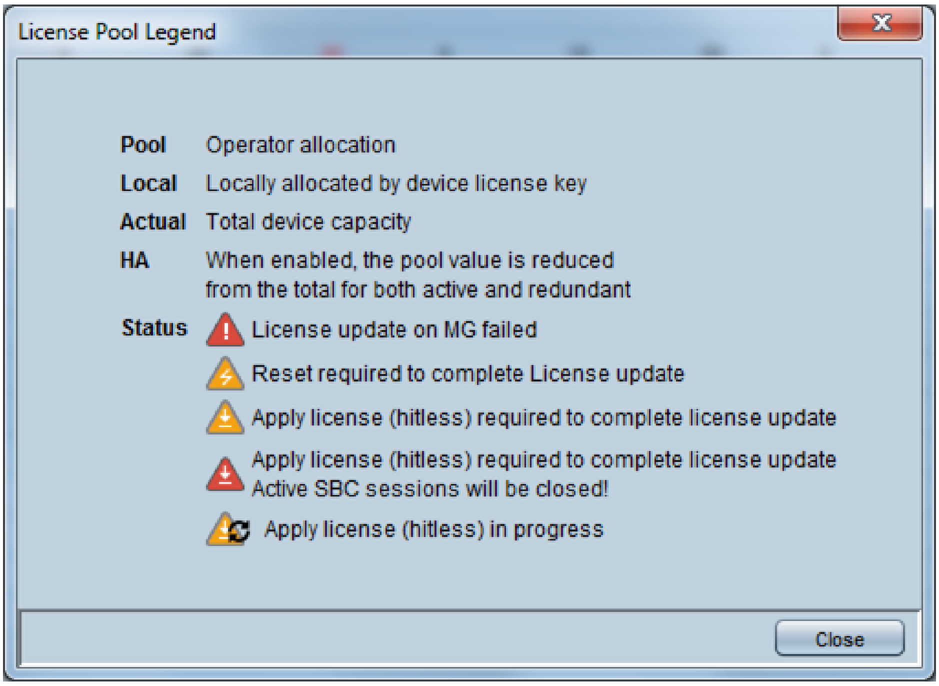
Note: In order to activate the License Pool, you must load the appropriate license to the EMS which includes the total pool numbers. Licenses are loaded to the EMS using the EMS Server Manager (refer to the *EMS Server IOM*). Once the license is loaded to the EMS, the total available licenses in the pool for each license parameter are displayed in the Summary pane (see Figure 22-2).

The License Pool Manager interface represents the license values for each of the above categories for each device as follows:

- The 'Local' value represents the base number of licenses that were previously allocated to the device using the device license key file.
- The 'Pool' value represents the incremented number of licenses that have been allocated to the device using the License Pool Manager.
- The 'Actual' value represents the actual number of licenses used by the device. Normally this value is the sum of the 'Local' and 'Pool' values.

In the Tool bar, click the **?** to open the License Pool Legend:

Figure 22-4: License Pool Legend



License Pool Legend

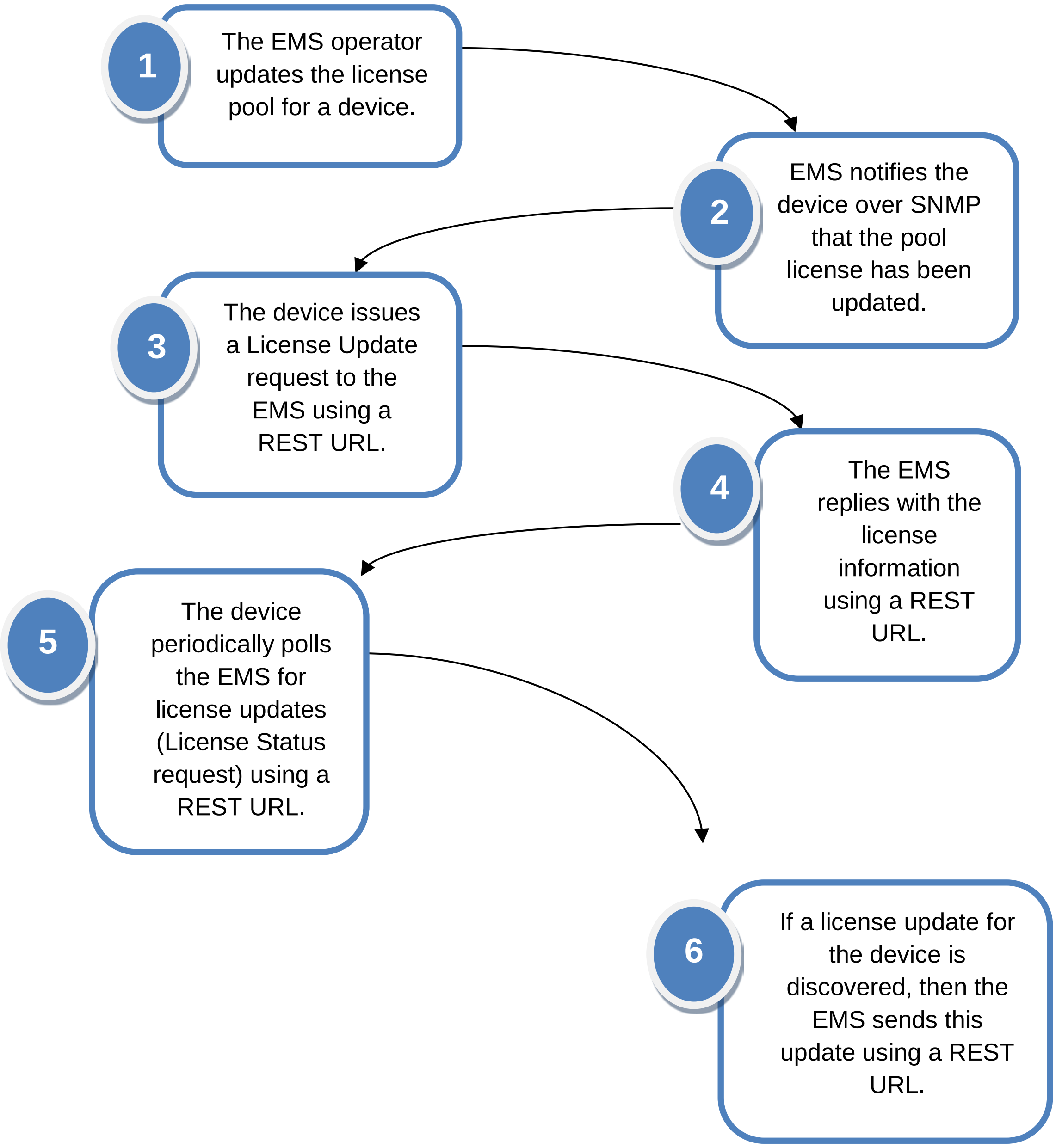
Pool	Operator allocation
Local	Locally allocated by device license key
Actual	Total device capacity
HA	When enabled, the pool value is reduced from the total for both active and redundant
Status	⚠ License update on MG failed
	⚠ Reset required to complete License update
	⚠ Apply license (hitless) required to complete license update
	⚠ Apply license (hitless) required to complete license update Active SBC sessions will be closed!
	⚠ Apply license (hitless) in progress

This dialog describes the main columns and status icons that are displayed in the License Pool Manager screen.

12.4 License Pool Update Process

The license pool update process works as shown in the figure below:

Figure 22-5: SBC License Pool Update Flow Diagram



1 The EMS operator updates the license pool for a device.

2 EMS notifies the device over SNMP that the pool license has been updated.

3 The device issues a License Update request to the EMS using a REST URL.

4 The EMS replies with the license information using a REST URL.

5 The device periodically polls the EMS for license updates (License Status request) using a REST URL.

6 If a license update for the device is discovered, then the EMS sends this update using a REST URL.

All the user actions performed in the SBC License Pool Manager are displayed in the Actions Journal and the relevant alarms are displayed in the Alarms Browser (see Section 12.12 on page 153.

12.4.1 REST Connection

When an operator modifies a device's license, they initially send an update message to the device over SNMP. The device replies with a request for the new license and the EMS then sends the license; these requests are performed using REST URLs.

The device polls the License Pool Manager for license updates (License Status request) using a REST URL every 12 hours, upon reset or for HA systems - upon a switchover and synchronization (by new active device). If a license update for the device is discovered, then the EMS sends this update using a REST URL.

The device license is valid for seven days. The validity time limit for the license is reset each time a successful REST connection is established between the device and the License Pool Manager. If the device cannot connect to the License Pool Manager for seven days, then the device license expires and resets with its initial, "local" license. This mechanism prevents the misuse of the issued licenses. Consequently, it is recommended to use EMS HA schemes as described in the *EMS IOM* manual.

Note:

- Communication between the device and the EMS License Manager is over SNMP and REST with an HTTPS connection.
- License Pool configuration updates are offline and therefore require a device reset or Hitless Upgrade (for HA devices) for the changes to take effect.

12.4.2 REST User

You need to create a designated REST user for the EMS to be able to authenticate the devices REST requests. The credentials of this user are sent from the EMS to the device in the SNMP message in the initial update sent to the device. This REST user is used for all subsequent REST license update and license status update requests sent from the device.

Note:

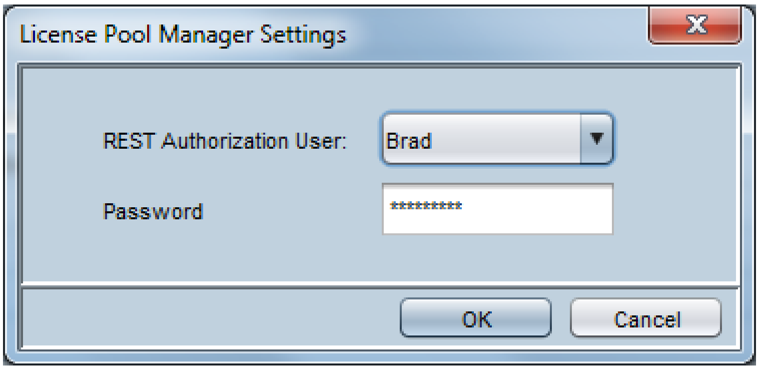
- The configured REST user cannot be deleted.
- When a device managed by the License Pool is not connected to the network when the REST user password is changed, as soon as the device is back in service, you must update the device with the new password ("Update MG") and verify in the User's list that the REST user is not suspended.

➢ **To configure the REST user:**

1. In the EMS Menu, choose **Security** > **User's List**.
2. Click the Add New User icon to create a designated REST user as follows:
   - Set the 'Security Level' field to "Administrator Super User" or "Administration".
   - Set the 'Password Validity Max Period (Days)' to "0".
   - Ensure that the 'Suspend User' check box is not selected.

   For more information, see Section 44.1.7.
3. In the License Pool Manager Toolbar, click the **Settings** icon ⚙; the following dialog is displayed:

Figure 22-6: License Pool Manager Settings


License Pool Manager Settings

REST Authorization User: Brad

Password **********

4. Configure the credentials of the REST user.

Note: The License Pool Manager is available for the EMS Administrator level only.

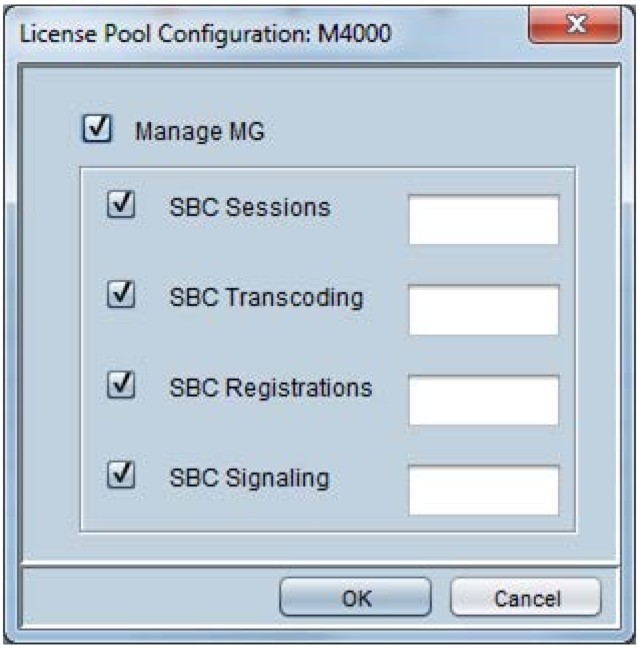
12.5 Configuring the License Pool Manager

This section describes how to enable devices to be configured with licenses and how to allocate the licenses to each device.

➢ **To configure the license pool:**

1. Right-click a device and select **Configuration** or double-click a device; the following screens are displayed:

Figure 22-7: SBC Session License Configuration



License Pool Configuration: M4000

☑ Manage MG

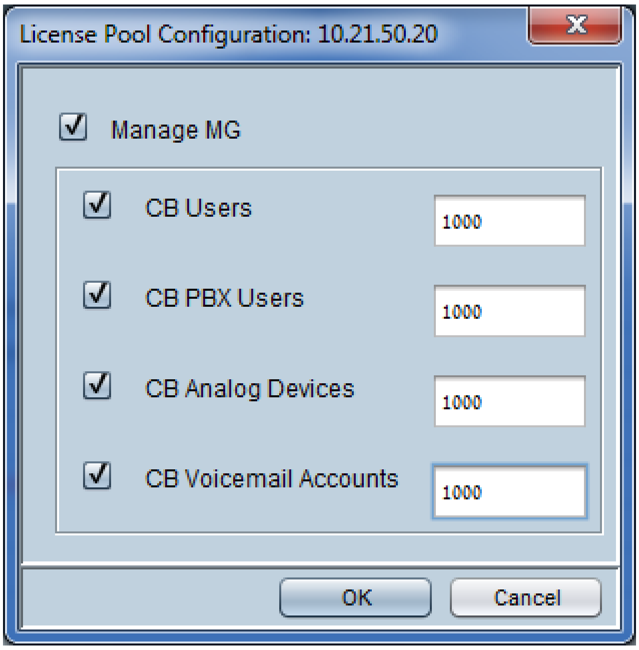
☑ SBC Sessions

☑ SBC Transcoding

☑ SBC Registrations

☑ SBC Signaling

Figure 22-8: CloudBond Session License Configuration



License Pool Configuration: 10.21.50.20

☑ Manage MG

☑ CB Users 1000

☑ CB PBX Users 1000

☑ CB Analog Devices 1000

☑ CB Voicemail Accounts 1000

2. Select the 'Manage MG' check box to manage the device using the SBC License Pool Manager.

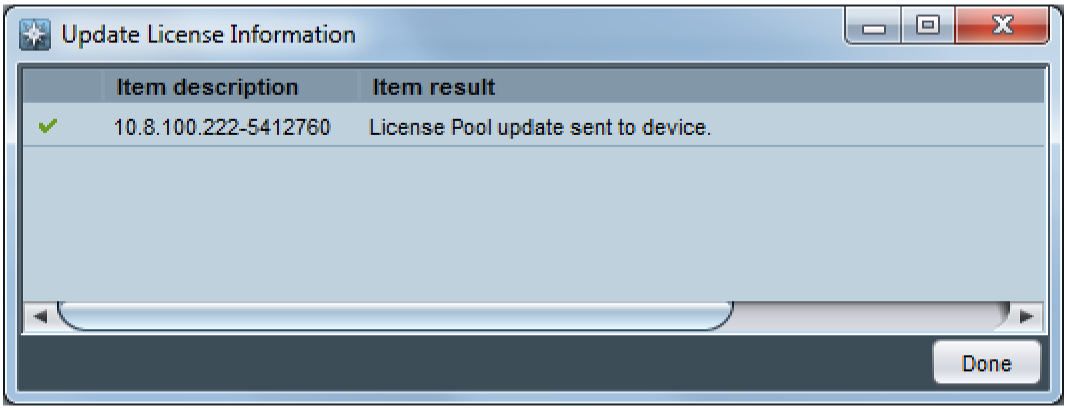
3. Select the desired license sessions checkbox, and then then in the adjacent text box, enter the required number of sessions:
   - SBC license sessions:
     - SBC Sessions.
     - SBC Transcoding
     - SBC Registrations
     - SBC Signaling
   - CloudBond 365 and CCE Appliance license sessions:
     - CB Users
     - CB PBX Users
     - CB Analog Devices
     - CB Voicemail Accounts

Note:

- When a device is removed from the EMS, the 'Manage MG' check box is cleared i.e. restored to its default value.
- If you select multiple devices, the number of licenses displayed in the dialog represents the values for the selected row entry. Once you update the dialog and click OK, the configuration for the selected devices is updated.

4. Right-click the desired device and select the **Update MG** option. An SNMP message is sent to the device to indicate that the license has been updated:

Figure 22-9: Update License Information



Update License Information

	Item description	Item result
✓	10.8.100.222-5412760	License Pool update sent to device.

5. If you received a notification to reset the device ⚠, right-click the device to reset for the SBC license to apply the update.

12.6 Maintenance Actions

The following table describes the right-click maintenance actions that can be applied to the managed device

Table 37-1: Maintenance Actions

Action	Description
Configuration	Opens the License Pool Configuration dialog.
Update MG	The device license has expired. Right-click the device and choose **Update MG**. This action reestablishes the REST connection with the device and sends the latest license.
Reset MG	Resets the device to apply the license update.
Apply License	Applies the new license to an HA supported device. When this action is performed, the device performs a hitless upgrade using the HA switchover mechanism.
Refresh License	Refreshes the configured license session values according to the current active sessions/users on the device.

⚠ **Note:** The Reset MG, Apply License and Refresh and Apply License (Apply hitless license) actions are not applicable for CloudBond and CCE Appliance products.

12.7 License Update Statuses

This following table shows the different license update statuses that are sent from the device. The related tooltips are also displayed over each device entry.

Table 37-2: SBC License Pool Statuses (sent from device)

Status Column Icon	Description
⚠	The License update process on the device was not successful.
⚠	Device reset is required to apply the license update.
⚠	Apply license (hitless) for HA devices is required to complete the license update.
⚠	Apply license (hitless) for HA devices is required to complete the license update. The number of Active sessions/users on the device is higher than what was allocated to the device.

Status Column Icon	Description
⚠	The hitless license update is in progress on the HA device. License configuration is not permitted during this time.

Note:

- When the configured license pool value exceeds the device capacity, the exceeding value is displayed in red.
- When the device license has expired, the last request time is displayed in red.

12.8 Recommended Actions

The table below summarizes the recommended actions that may be indicated in the 'Require Action' column. Each required action is identified by the appropriate action button.

Table 37-3: SBC License Manager - Actions

Required Action	Description	Status Icon or Text Indicator
Reset	The device must be reset to apply the license. Right-click the device and choose **Reset MG**.	⚠
Apply **(Apply License)**	Hitless license update should be applied for HA devices. Right-click the device and choose **Apply License**.	⚠
	Hitless license update should be applied for HA devices. Note however, the number of Active sessions/users on the device is higher than what was allocated to the device. Therefore, you should run the **Refresh License** action until you see that all Active license values are displayed with the new reduced values. Otherwise, when choosing **Apply License**, some of the users/sessions will be disconnected. When you are ready, right-click the device and choose **Apply License**.	⚠

Required Action	Description	Status Icon or Text Indicator
Configuration	The configured license pool value exceeds the device capacity. Do one of the following: • Apply the new license (**Reset MG** or **Apply License**; the device sets its SBC capacity to maximum and disregards the excess configured sessions. • Right-click the device and choose **Configuration** or double-click the device to open the License Pool Configuration dialog and configure a new value which falls within the device's session capacity and then reapply the new license: **Reset MG** or **Apply License**.	The exceeding value is displayed in red.
	The device failed to update the license, therefore verify the license configuration and modify as required.	⚠
Update	The device license has expired. Right-click the device and choose **Update MG**. This action reestablishes the REST connection with the device and sends the latest license.	The last request time is displayed in red.

Note:

- Running a Hitless license downgrade on an HA device when the current number of active SBC sessions/users on the device is higher than what was allocated to the device can lead to disruption of service. To avoid this disruption you can either run the 'Refresh License' action as described above or wait until the number of current SBC sessions/users is aligned to the configured value.
- If you downgrade the Transcoding session license and therefore the number of active transcoding sessions/users is higher than what was allocated to the device, then service is not affected i.e. there is no forceful closure of excess call sessions. However, no new call sessions can be established until the number of current Transcoding sessions is less than equal to the limit defined in the new session license.

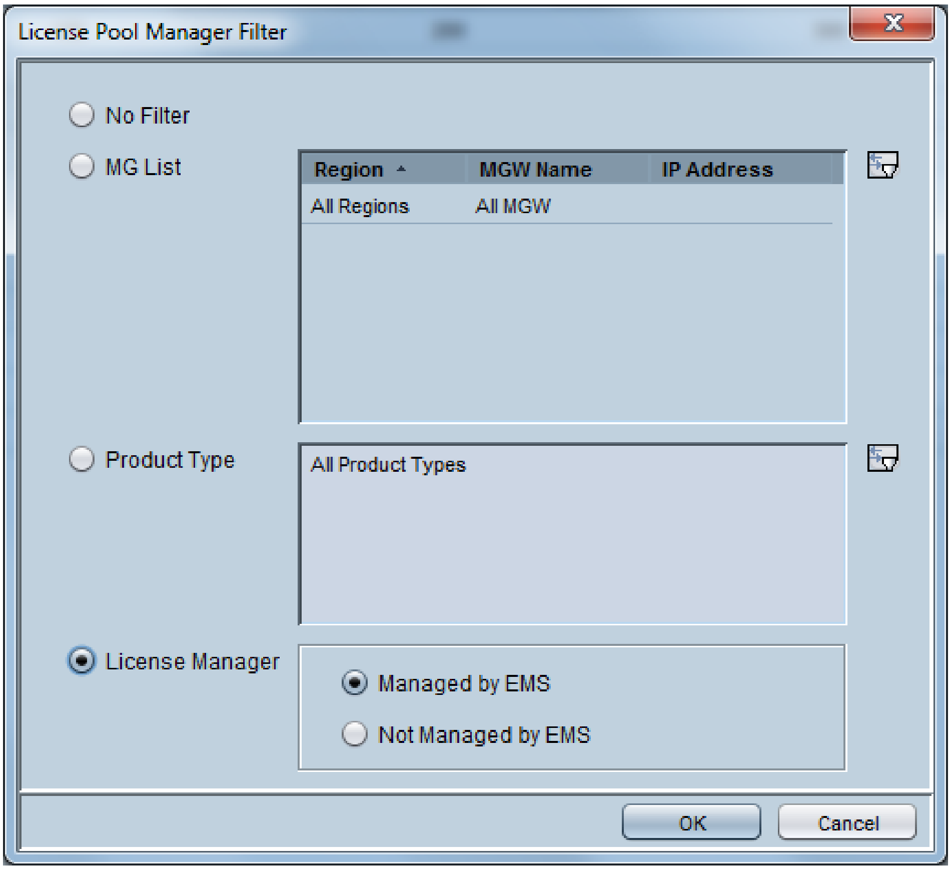
12.9 Filtering the SBC License Pool Manager

You can filter the display of the SBC License Pool Manager to display specific devices or to display only those devices that are managed by the SBC License Pool Manager.

➢ To filter the License Manager view:

1. In the SBC License Pool Manager toolbar, select the **Filter** icon ; the following dialog is displayed:

Figure 22-10: License Pool Manager Filter



License Pool Manager Filter

○ No Filter

○ MG List

Region	MGW Name	IP Address
All Regions	All MGW	

○ Product Type

All Product Types

● License Manager

● Managed by EMS

○ Not Managed by EMS

2. Set one or more of the following filter criteria:
    - **MG List:** Select a specific region or define specific devices. Use the Browse button to browse for specific devices.
    - **Product Type:** Use the browse button to select a specific product type.
    - **License Manager:** Select one of the following options:
        - **Managed by EMS:** filters the SBC License Pool Manager to display only those devices that have been enabled for management ('MG Enable').
        - **Not Managed by EMS:** filters the SBC License Pool Manager to display only those devices that have not been enabled for management.

Note: When a device is configured as unmanaged and there are active licensed sessions for this device, the device automatically performs a reset or hitless upgrade.

12.10 Saving License Pool Manager Configuration

The License Pool Manager can be saved in a *.csv file (Comma Separated File). The saved *.csv file can be viewed in Microsoft™ Excel™ with all Excel features (statistics, graphs) enabled.

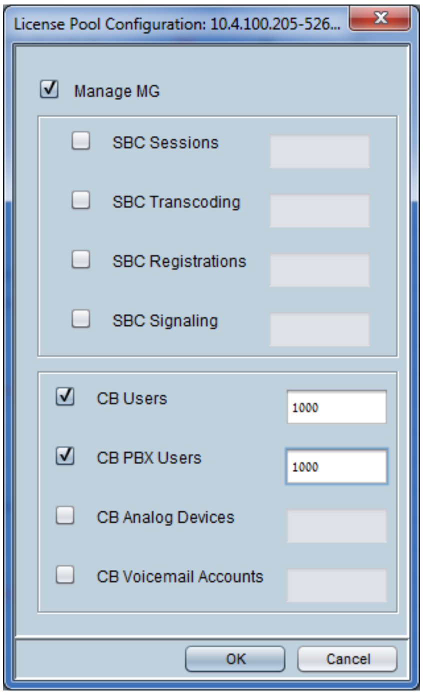
➢ To save the License Pool Manager configuration:

- In the License Pool Manager toolbar, select the **Save** option .

12.11 Configuring License Pool Parameters for Unknown Devices

When a device is not fully connected to the EMS (it has not yet received an SNMP keep-alive or Coldstart trap from the device), it is defined as an Unknown device until it's fully connected to the EMS. At this stage, it is not fully recognized by EMS. For such devices, you can configure all license pool parameters for both the SBC and CloudBond 365/CCE Appliance applications as shown in the figure below:

Figure 22-11:License Pool Configuration for Unknown Devices



License Pool Configuration: 10.4.100.205-526...

☑ Manage MG

☐ SBC Sessions

☐ SBC Transcoding

☐ SBC Registrations

☐ SBC Signaling

☑ CB Users: 1000

☑ CB PBX Users: 1000

☐ CB Analog Devices

☐ CB Voicemail Accounts

Once the Unknown device is fully connected to the EMS, and therefore is recognized as either an SBC or a CloudBond/CCE Appliance, the License Pool Configuration dialog is separated for SBC and CloudBond/CCE Appliance parameters.

12.11.1 Applying License

When licenses are applied to the CloudBond/CCE Appliance device (Update MG action), and an SNMP update is sent to the device, this automatically triggers the device to reset and therefore you do not need to reset the device from the License Pool Manager.

12.12 License Pool Manager Alarms

This section describes the SBC License Pool Manager related alarms that are sent from the device (for more information, refer to the relevant device *Performance Monitors and Alarm Guides*).

- **acLicensePoolInfraAlarm:**
  - The device was unable to establish an HTTPS REST connection with the EMS SBC License Pool Manager server after successive attempts (critical).
  - The device license has expired (critical).
  - The last attempt to establish an HTTPS REST connection with the SBC License Pool Manager server was not successful (major)
  - The device is no longer managed by the SBC License Pool Manager (major).
- **acLicensePoolOverAllocationAlarm:**

The device received a license from the License Pool Manager that exceeds the maximum SBC session capacity that can be supported by the device (warning). Two warning messages are received; one warning message after the license configuration has been applied (as described in Section 12.5) and one warning message after the device has been reset or hitless upgrade was performed.

- **acLicensePoolApplicationAlarm:**

This alarm is raised when the device requires a reset or apply hitless upgrade after receiving a new license (major).

This page is intentionally left blank.

Part II

Status Monitoring and Navigation Concepts

This section describes the various status monitoring and navigation concepts.

13 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 status view is selected, it's automatically updated (refreshed) every 20 seconds.

Following are the EMS status components:

- 'Regions List' on page 157
- 'MGs List' on page 158

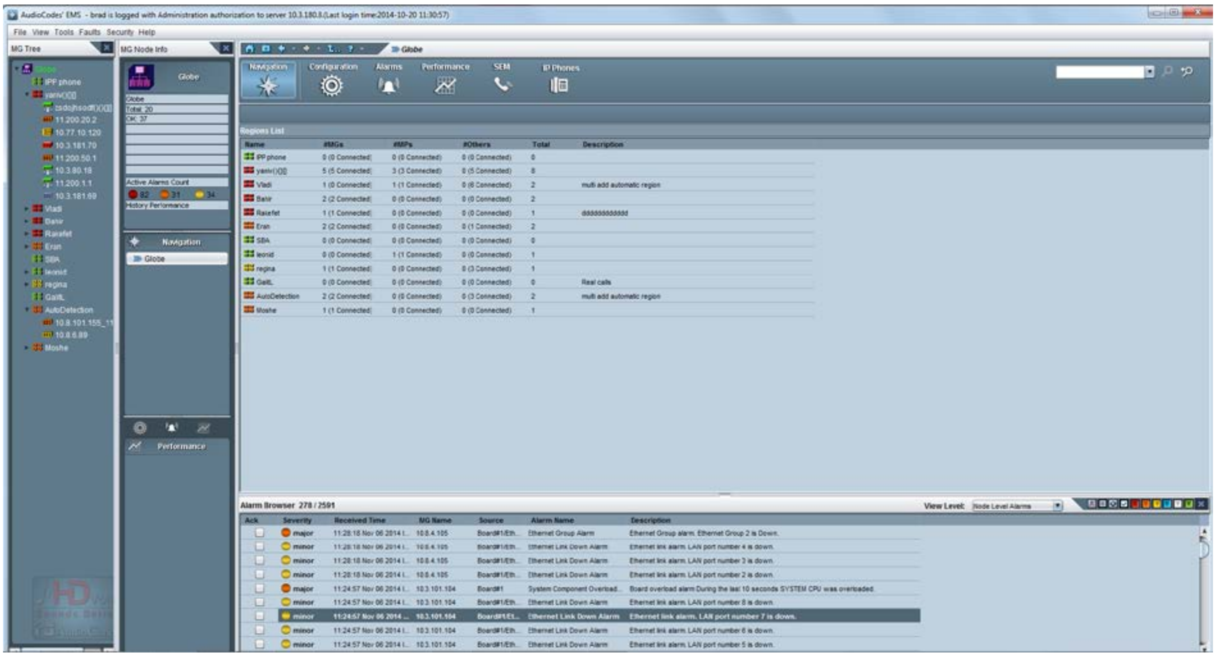
13.1 Regions List

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



Regions List

Name	#MGs	#MPs	#Others	Total	Description
IPP phone	0 (0 Connected)	0 (0 Connected)	0 (0 Connected)	0	
yaniv()()[]	5 (5 Connected)	3 (3 Connected)	0 (5 Connected)	8	
Vladi	1 (0 Connected)	1 (1 Connected)	0 (6 Connected)	2	multi add automatic region
Bahr	2 (2 Connected)	0 (0 Connected)	0 (0 Connected)	2	
Raiefet	1 (1 Connected)	0 (0 Connected)	0 (0 Connected)	1	dddddddddddd
Eran	2 (2 Connected)	0 (0 Connected)	0 (1 Connected)	2	
SBA	0 (0 Connected)	0 (0 Connected)	0 (0 Connected)	0	
leonid	0 (0 Connected)	1 (1 Connected)	0 (0 Connected)	1	
regina	1 (1 Connected)	0 (0 Connected)	0 (3 Connected)	1	
GaliL	0 (0 Connected)	0 (0 Connected)	0 (0 Connected)	0	Real calls
AutoDetection	2 (2 Connected)	0 (0 Connected)	0 (3 Connected)	2	multi add automatic region
Moshe	1 (1 Connected)	0 (0 Connected)	0 (0 Connected)	1	

Alarm Browser 278 / 2591

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	major	11:28:18 Nov 06 2014 I...	10.8.4.105	Board#1/Eth...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 2 is Down.
□	minor	11:28:18 Nov 06 2014 I...	10.8.4.105	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.
□	minor	11:28:18 Nov 06 2014 I...	10.8.4.105	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.
□	minor	11:28:18 Nov 06 2014 I...	10.8.4.105	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.
□	major	11:24:57 Nov 06 2014 I...	10.3.101.104	Board#1	System Component Overload...	Board overload alarm During the last 10 seconds SYSTEM CPU was overloaded
□	minor	11:24:57 Nov 06 2014 I...	10.3.101.104	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 8 is down.
□	minor	11:24:57 Nov 06 2014 ...	10.3.101.104	Board#1/Et...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 7 is down.
□	minor	11:24:57 Nov 06 2014 I...	10.3.101.104	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 6 is down.
□	minor	11:24:57 Nov 06 2014 I...	10.3.101.104	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 5 is down.

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.

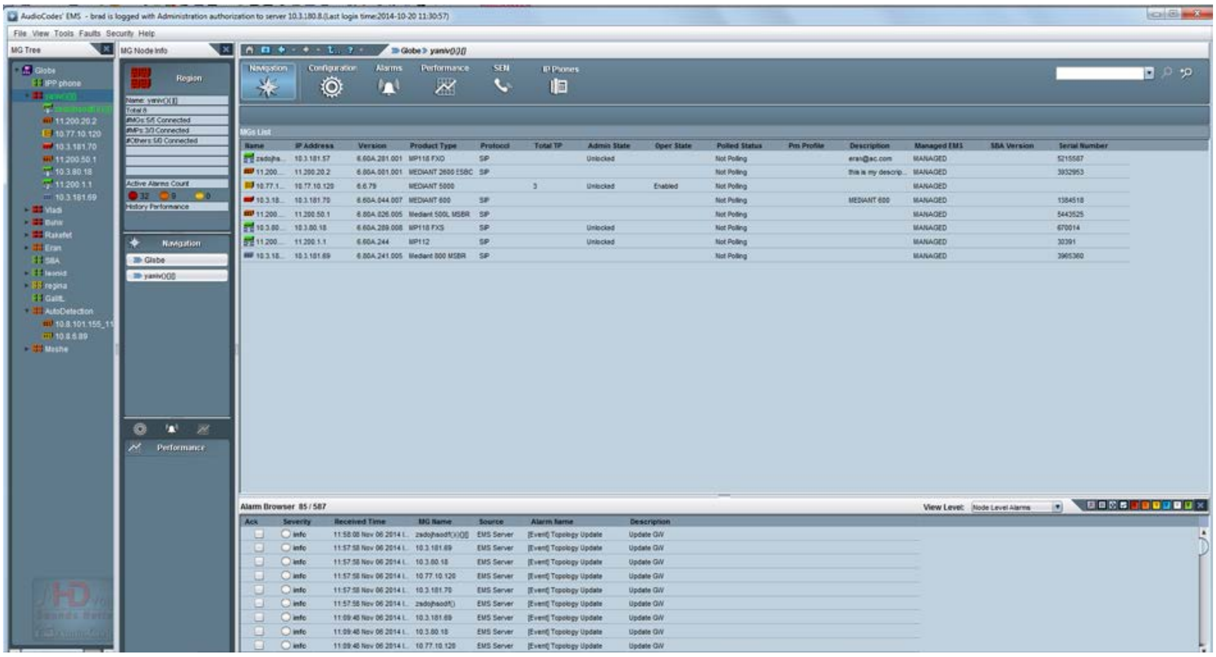
13.2 MGs List

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. 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.
3. Double-click a device in the MGs List; the Main Screen displays the Status pane.
4. Click the **Up** button on the Gateway level screens to return to the MGs List in the Main Screen.

Figure 6-2: MGs List



Name	IP Address	Version	Product Type	Protocol	Total TP	Admin State	Oper State	Polled Status	Pm Profile	Description	Managed EMS	SBA Version	Serial Number
zadojha...	10.3.181.57	6.60A.281.001	MP118 FXO	SIP		Unlocked		Not Polling		eran@ac.com	MANAGED		5215567
11.200...	11.200.20.2	6.80A.001.001	MEDIANT 2600 ESBC	SIP				Not Polling		this is my descrip...	MANAGED		3932953
10.77.1...	10.77.10.120	6.6.79	MEDIANT 5000		3	Unlocked	Enabled	Not Polling			MANAGED		
10.3.18...	10.3.181.70	6.60A.044.007	MEDIANT 600	SIP				Not Polling		MEDIANT 600	MANAGED		1384518
11.200...	11.200.50.1	6.60A.026.005	Mediant 500L MSBR	SIP				Not Polling			MANAGED		5443525
10.3.80...	10.3.80.18	6.60A.289.008	MP118 FXS	SIP		Unlocked		Not Polling			MANAGED		670014
11.200...	11.200.1.1	6.60A.244	MP112	SIP		Unlocked		Not Polling			MANAGED		30391
10.3.18...	10.3.181.69	6.80A.241.005	Mediant 800 MSBR	SIP				Not Polling			MANAGED		3965360

Alarm Browser 85 / 587

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	○ info	11:58:08 Nov 06 2014 I...	zadojhaodf()()[][]	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:57:58 Nov 06 2014 I...	10.3.181.69	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:57:58 Nov 06 2014 I...	10.3.80.18	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:57:58 Nov 06 2014 I...	10.77.10.120	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:57:58 Nov 06 2014 I...	10.3.181.70	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:57:58 Nov 06 2014 I...	zadojhaodf()	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:09:48 Nov 06 2014 I...	10.3.181.69	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:09:48 Nov 06 2014 I...	10.3.80.18	EMS Server	[Event] Topology Update	Update GW
□	○ info	11:09:48 Nov 06 2014 I...	10.77.10.120	EMS Server	[Event] Topology Update	Update GW

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)
- 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

13.3 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.

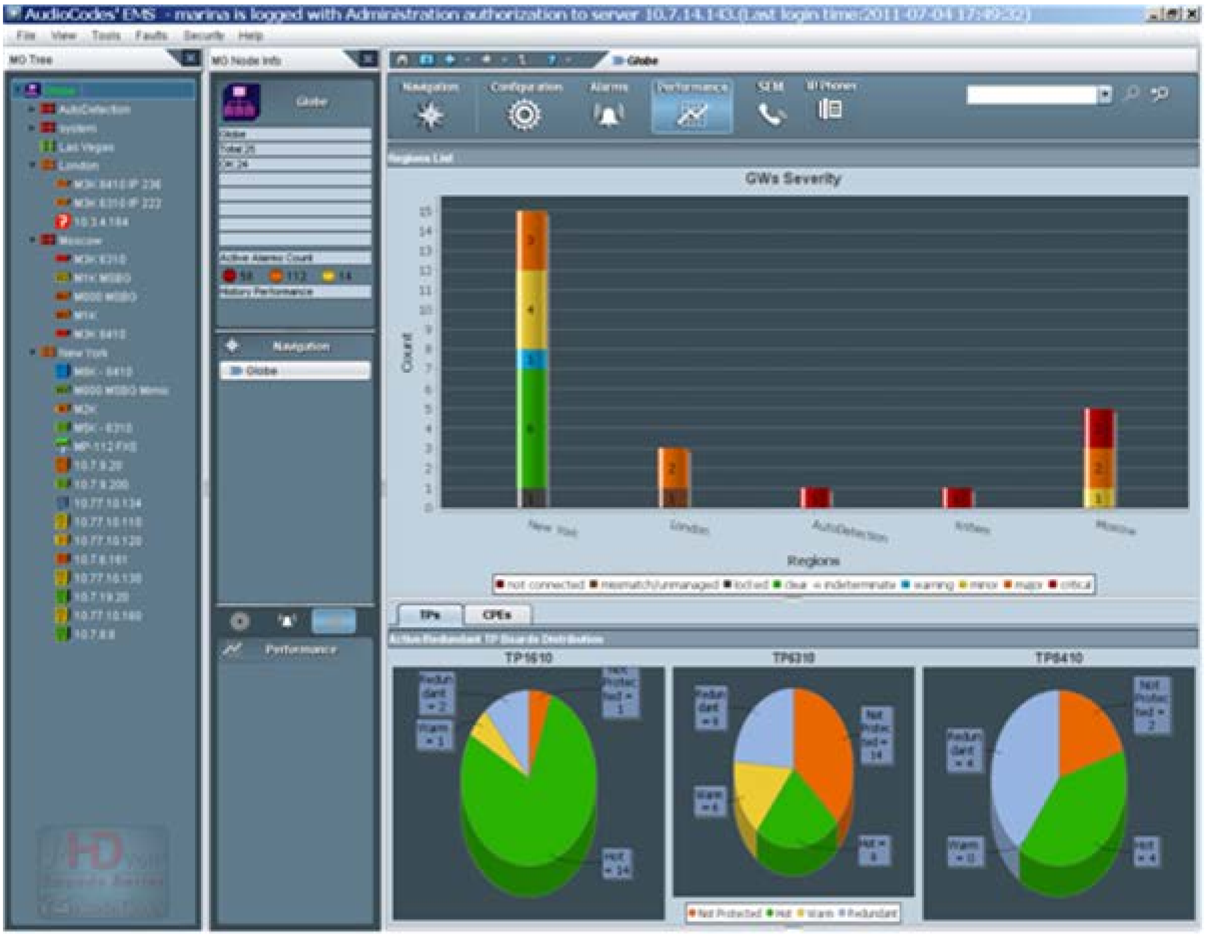
          When devices cannot be categorized into one of the above states, they are collectively represented as a separate bar graph with the label 'Unknown'.

- 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 3000chassis). 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:

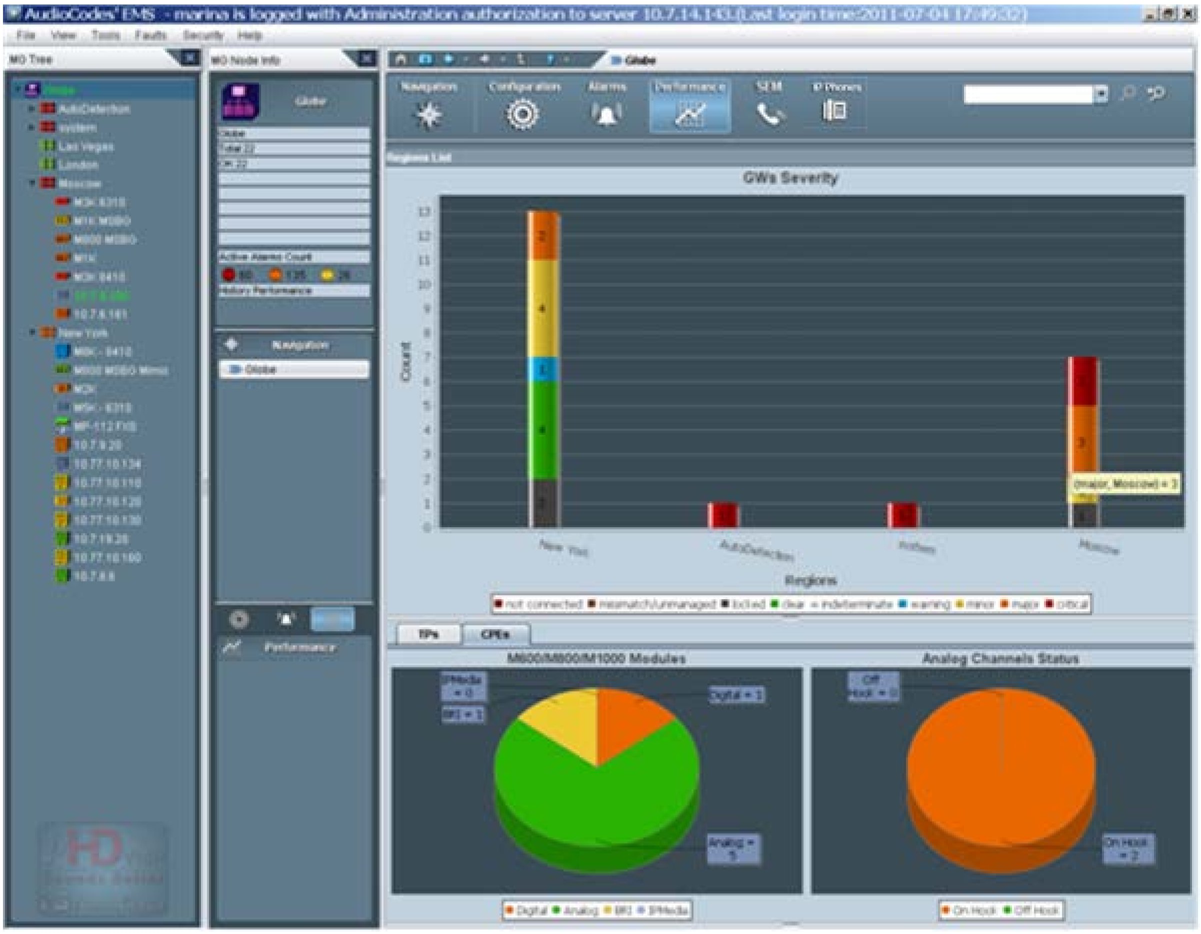
- Globe level – TPs
- Globe level – CPEs
- Region Level – TPs
- Region Level – CPEs

Figure 6-3: Globe Level - TPs



AudioCodes' EMS - marina is logged with Administration authorization to server 10.7.14.143.(Last login time:2011-07-04 17:49:32)

Figure 6-4: Globe Level – CPEs



AudioCodes' EMS - marina is logged with Administration authorization to server 10.7.14.143.(Last login time:2011-07-04 17:49:32)

Figure 6-5: Region Level – TPs

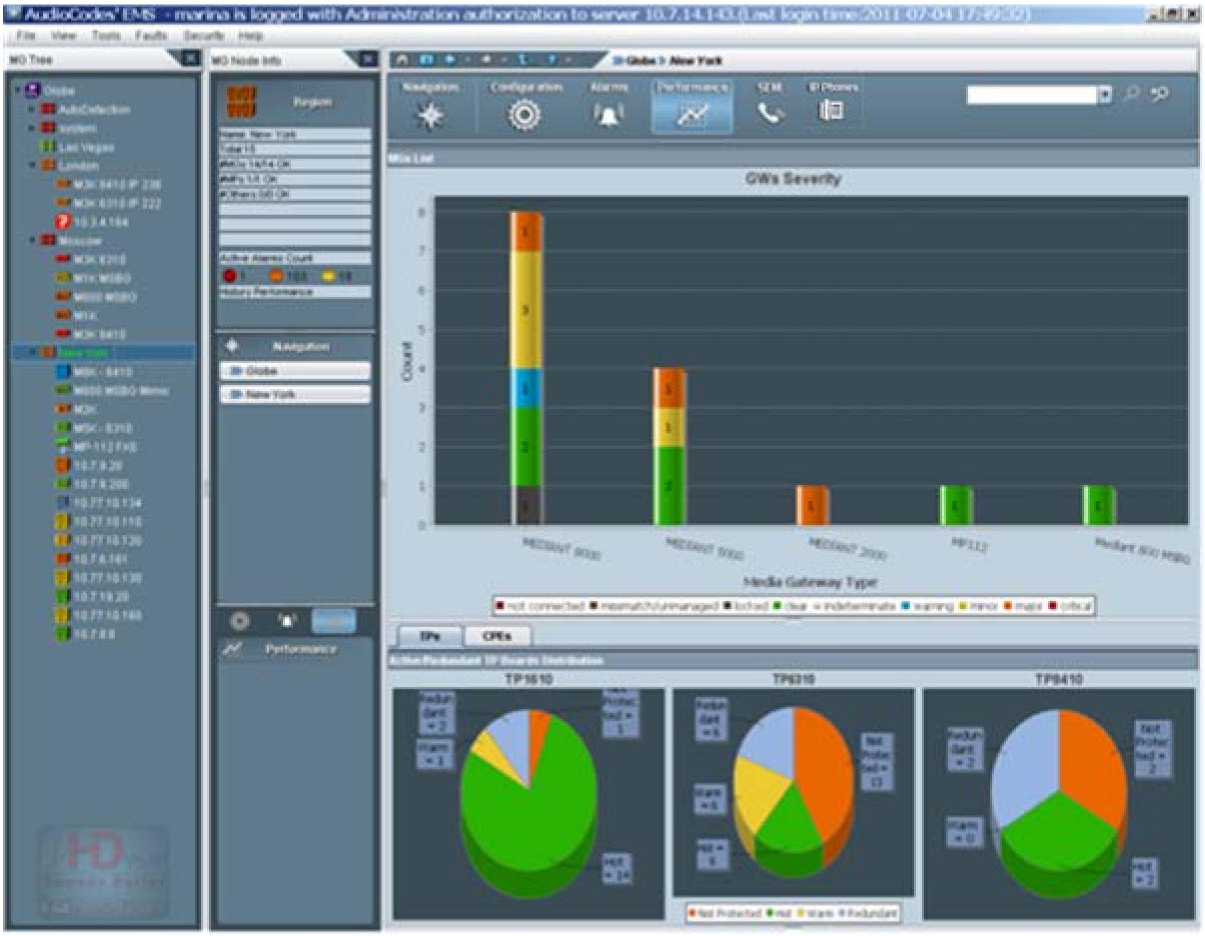
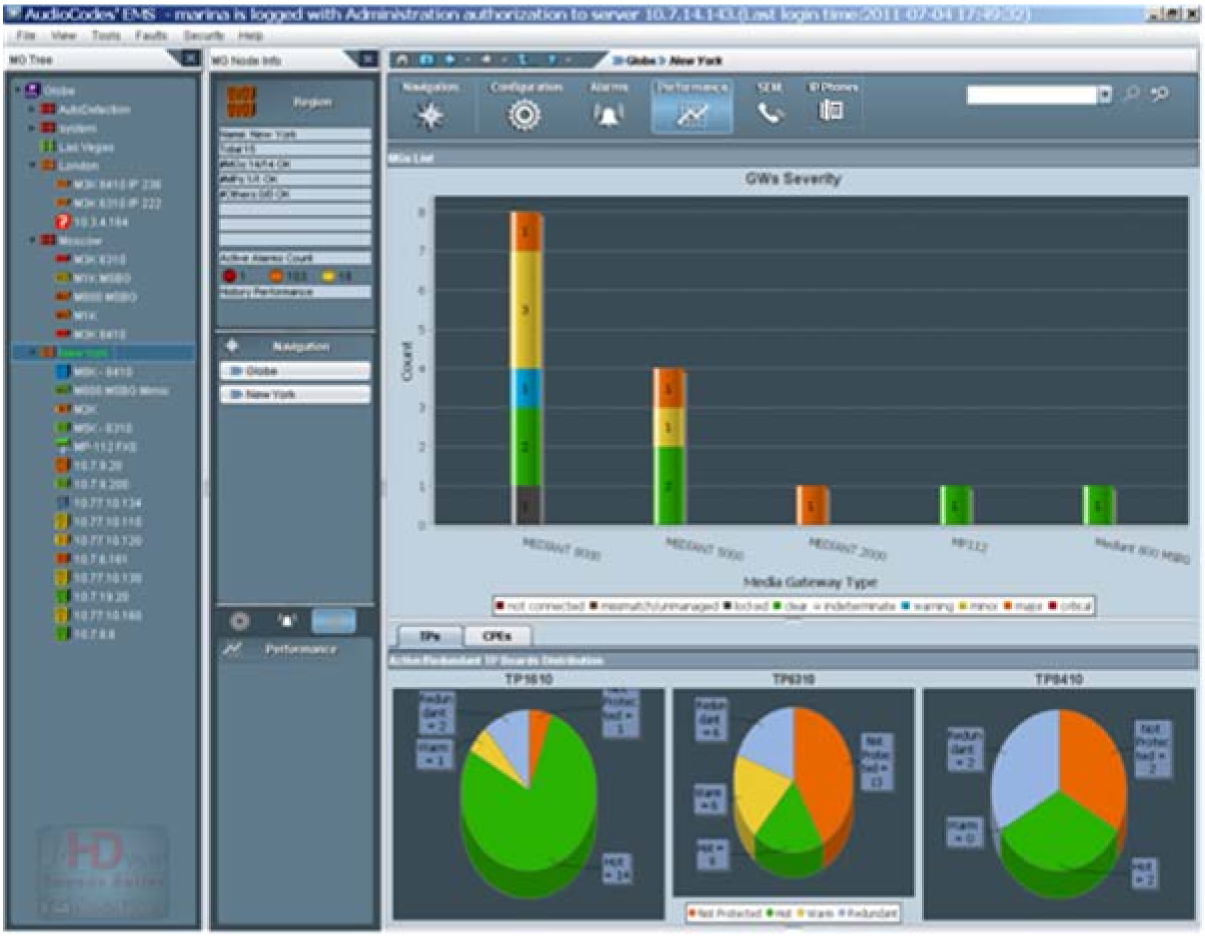


Figure 6-6: Region Level – CPEs



AudioCodes' EMS - marina is logged with Administration authorization to server 10.7.14.143 (Last login time:2011-07-04 17:49:32)
File View Tools Faults Security Help
MG Tree
MG Node Info
Globe > New York
Globe
AutoDetection
System
Las Vegas
London
Moscow
New York
Region
Name: New York
Total 15
Active Alarms Count
History Performance
Navigation
Globe
New York
Performance
Navigation Configuration Alarms Performance SEM IP Phones
MGs List
GWs Severity
Count
MEDIANT 8000
MEDIANT 5000
MEDIANT 2000
MP112
Mediant 800 MSBG
Media Gateway Type
not connected mismatch/unmanaged locked clear indeterminate warning minor major critical
TPs
CPEs
Active/Redundant TP Boards Distribution
TP1610
TP6310
TP8410
Not Protected Hot Warm Redundant

13.4 Device Level Status Pane

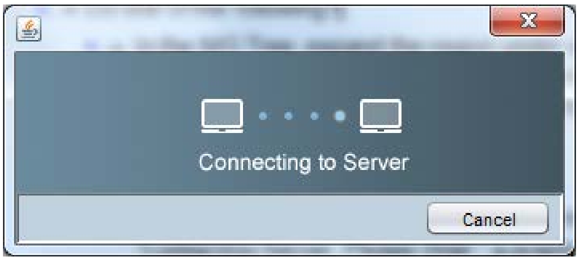
This section describes how to access the device level status pane.

➢ **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 “Connecting to Server;" (see figure below). Once a successful connection has been established, a graphical representation of the device is displayed.

     -OR-
   - In the MGs List, double-click a device; a message appears indicating “Connecting to Server" (see figure below). Once a successful connection has been established, a graphical representation of the device is displayed.
2. Click the **Up** button in the board-level screens to navigate back up a level.

Figure 6-7: Connecting to Server



Connecting to Server

Note: If the attempt to connect to the device is hanging, you can optionally click the **Cancel** button to cancel the action.

This page is intentionally left blank.

14 Mediant 9000

This section describes the management of the Mediant 9000 device.

14.1 Supported Configuration

The EMS supports the following product configuration:

- Standalone (Simplex) Mediant 9000
- High Availability-HA (1+ 1) Mediant 9000
- Media Transcoding Cluster (MTC) (Mediant 9000 configured with a transcoding cluster).

14.2 Initial Configuration

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

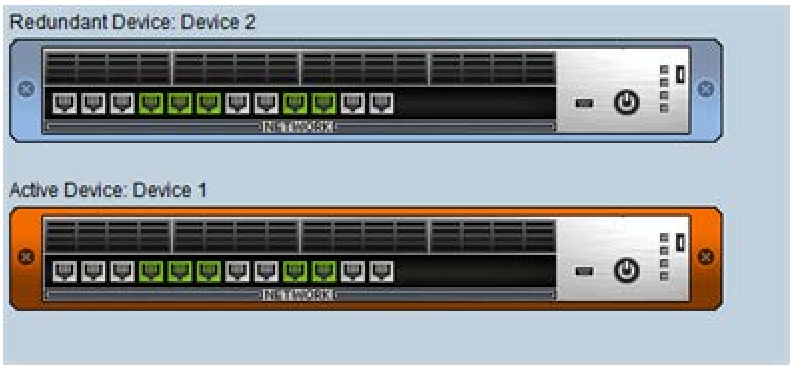
14.3 Status Pane

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

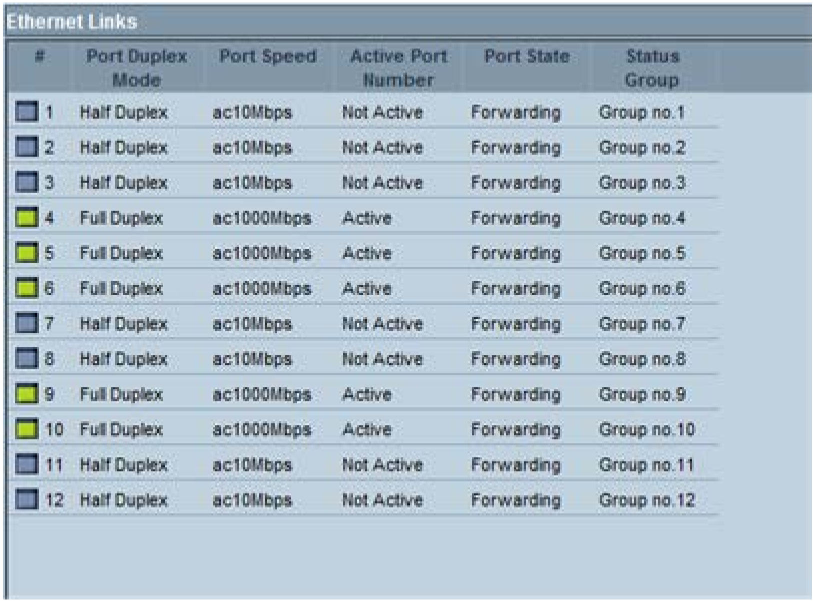


Gigabit Ethernet port status icons:

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

Double-click one of the Ethernet ports (to display the detailed status for each port); the Ethernet Links Table screen is displayed:

Figure 8-2: Ethernet Table-Mediant 9000 SBC

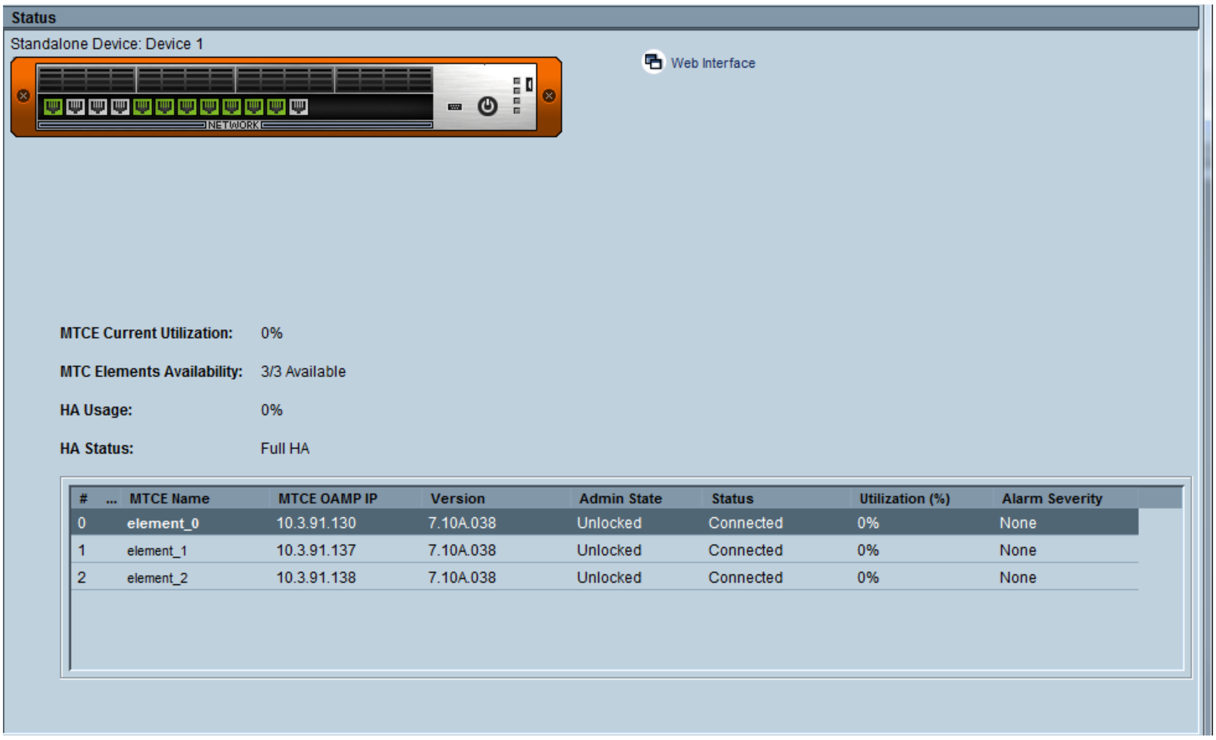


Ethernet Links

#	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

The following screen shows the Media Transcoding Cluster Status screen.

Figure 8-3: MTC Status Screen



Status

Standalone Device: Device 1

MTCE Current Utilization: 0%

MTC Elements Availability: 3/3 Available

HA Usage: 0%

HA Status: Full HA

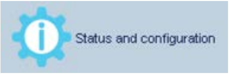
#	...	MTCE Name	MTCE OAMP IP	Version	Admin State	Status	Utilization (%)	Alarm Severity
0		**element_0**	10.3.91.130	7.10A.038	Unlocked	Connected	0%	None
1		element_1	10.3.91.137	7.10A.038	Unlocked	Connected	0%	None
2		element_2	10.3.91.138	7.10A.038	Unlocked	Connected	0%	None

The following table describes the MTC statistics displayed in the above screen.

Table 16-1: MTC Status Data

Field	Description
MTC Current Utilization	Displays the percentage of currently used DSP resources in the Media Transcoding Cluster (i.e., of all Media Transcoders).
Media Elements Availability	Displays the number of Media Transcoders, out of all the configured Media Transcoders in the Media Transcoders table, available for processing transcoding sessions. A Media Transcoder is available if it's in "connected" status. The status is displayed in the following syntax: "<available>/<total> Available".
HA Usage	Displays the percentage threshold of utilized DSP resources. If the Media Transcoding Cluster is configured to operate in Best Effort mode, the current utilization might increase to over 100%, indicating that there is no guarantee for HA redundancy for all the transcoding sessions.
HA Status	Displays the HA status: ▪ "Full HA": Sufficient DSP resources exist to ensure HA for active transcoding sessions if a Media Transcoder fails. ▪ "Partial HA": Sufficient DSP resources exist only for some of the active transcoding sessions if a Media Transcoder fails. This can occur, for example, if a Media Transcoder is undergoing a software upgrade when another Media Transcoder fails. ▪ "No HA": No resources for HA and therefore, if a Media Transcoder fails, all its active transcoding sessions are terminated.

14.4 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.

14.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 229.

This page is intentionally left blank.

15 Mediant Software SBC Products

This section describes the management of the Mediant Software SBC.

15.1 Supported Configuration

The EMS supports the following product configurations:

- Mediant SE SBC Standalone (Simplex)
- Mediant SE-H SBC (High Availability-HA (1+ 1)
- Mediant VE SBC Standalone (Simplex)
- Mediant VE-H SBC (High Availability-HA (1+ 1)
- Mediant VE SBC with Media Transcoder Cluster (MTC) configuration

15.2 Initial Configuration

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

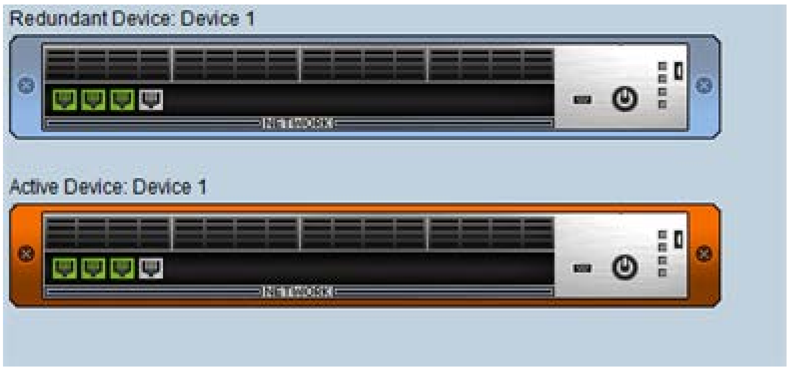
15.3 Status Pane

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

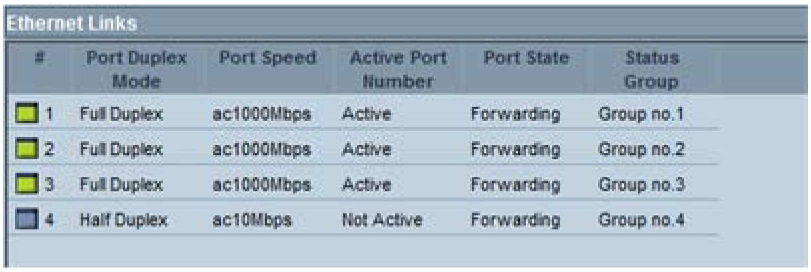


Gigabit Ethernet port status icons:

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

Double-click one of the Ethernet ports (to display the detailed status for each port); the Ethernet Links Table screen is displayed:

Figure 9-2: Ethernet Table-Software SBC



Ethernet Links

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

15.4 Provisioning

For provisioning of the Mediant *Software* SBC, click the ⓘ Status and configuration 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.

15.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 229.

16 Mediant 2600 E-SBC and Mediant 4000 SBC

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

16.1 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

16.2 Initial Configuration

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

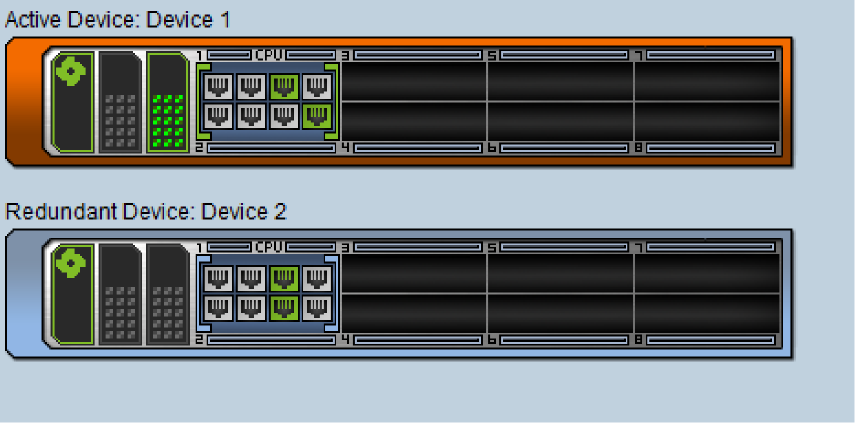
16.3 Status Pane

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.

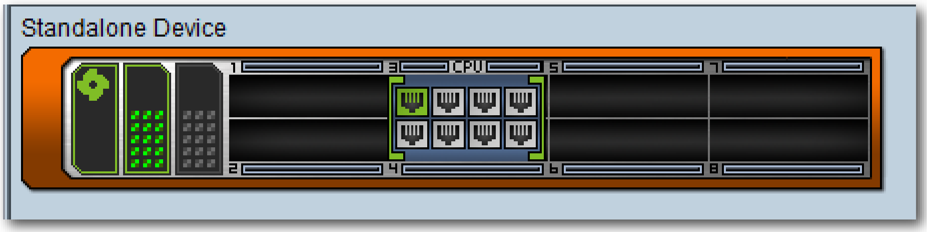
16.3.1 Hardware Component Status in Table View

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
- **Gigabit Ethernet port status icons:**
  - 🟩 (green): Ethernet link is working
  - ⬜ (gray): Ethernet link is not connected

  Double-click one of the Ethernet ports (to display the detailed status for each port); the Ethernet Links Table screen is displayed:

16.4 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.

16.5 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 229.

17 Mediant 3000

This section describes the management of the Mediant 3000 device.

17.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

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

17.2 Initial Configuration

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

17.3 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

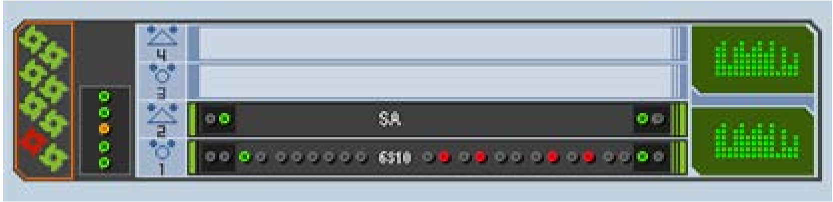
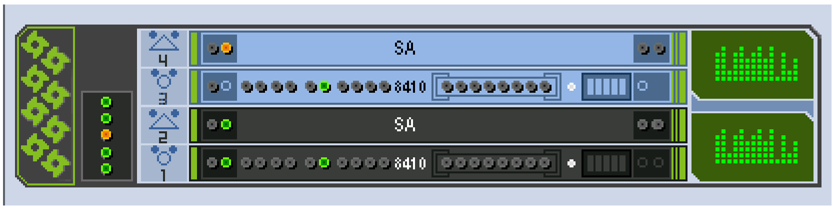


Figure 11-2: Mediant 3000 8410 Status Pane



17.3.1 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

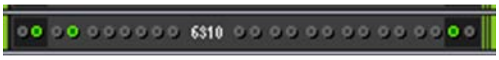
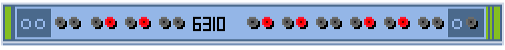


Figure 11-4: 6310 Redundant Board Status

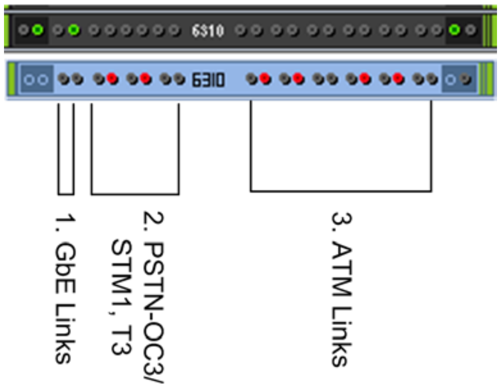


Background color: Dark Gray = Active board; Blue = Redundant board

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



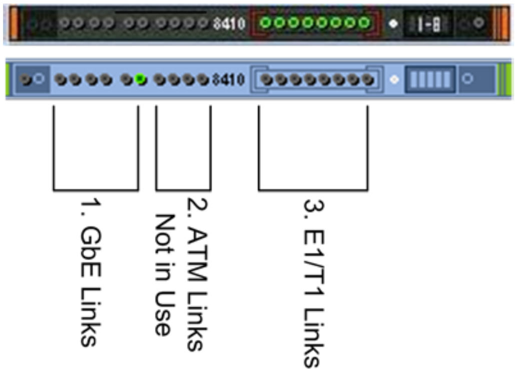
Legend

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

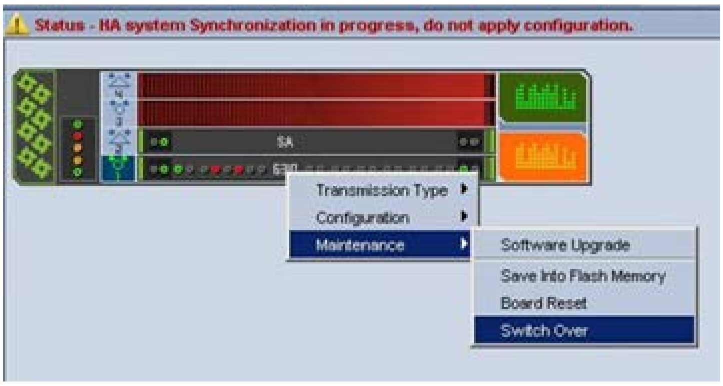
- **Power Supplies Status**

  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



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

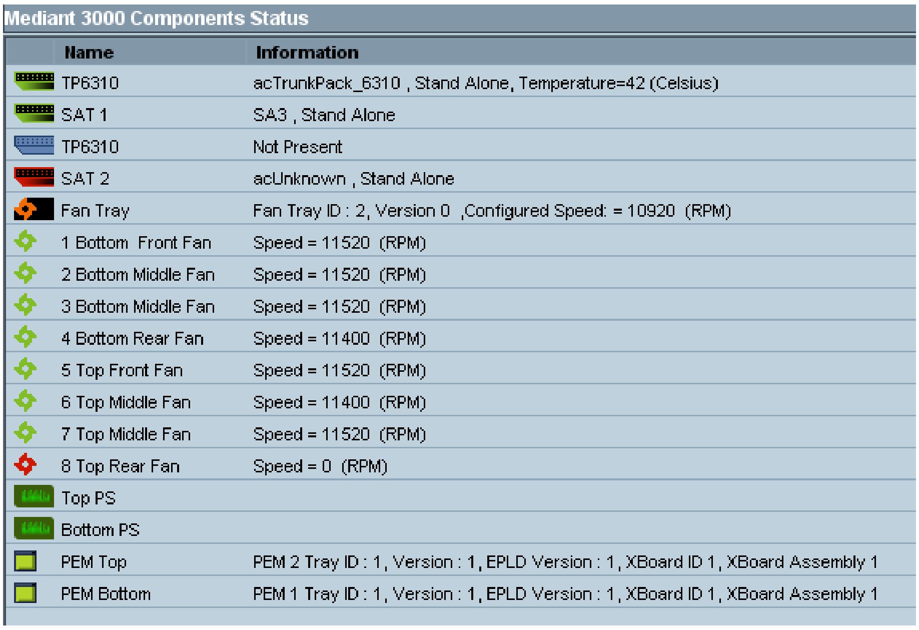
17.3.2 Hardware Component Status in Table View

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

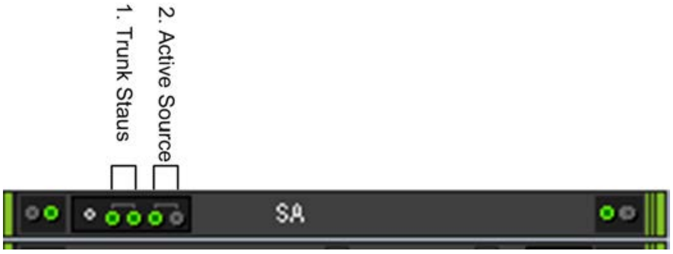
  - Status: Color convention: Gray = Doesn't Exist; Red = Minor severity, power cable is missing; Green = Clear Severity
  - Information : PEM ID and version

17.3.3 Mediant 3000 TP-8410 SA BITS status

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

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

Figure 11-9: Mediant 3000 SA Board Status

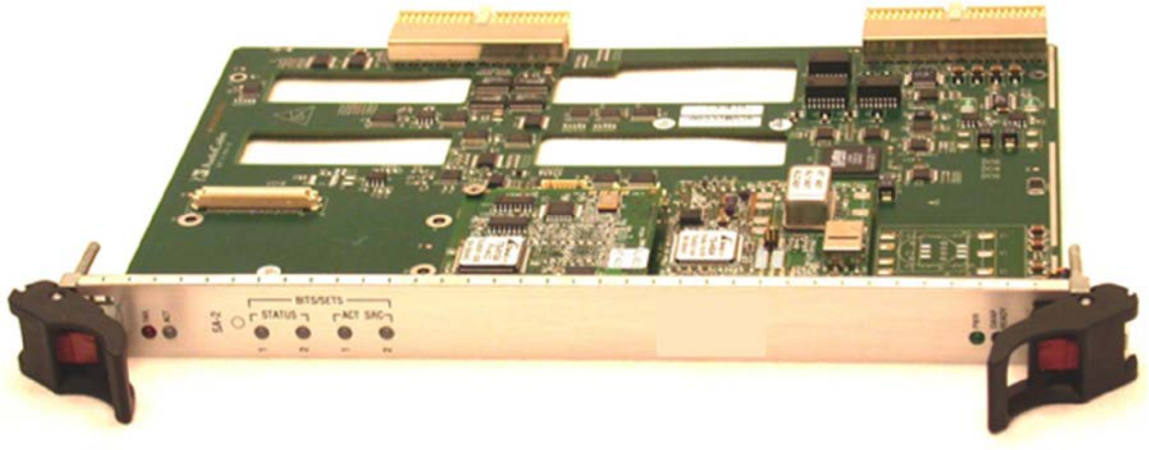


The LEDs are represented as follows:

- 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.

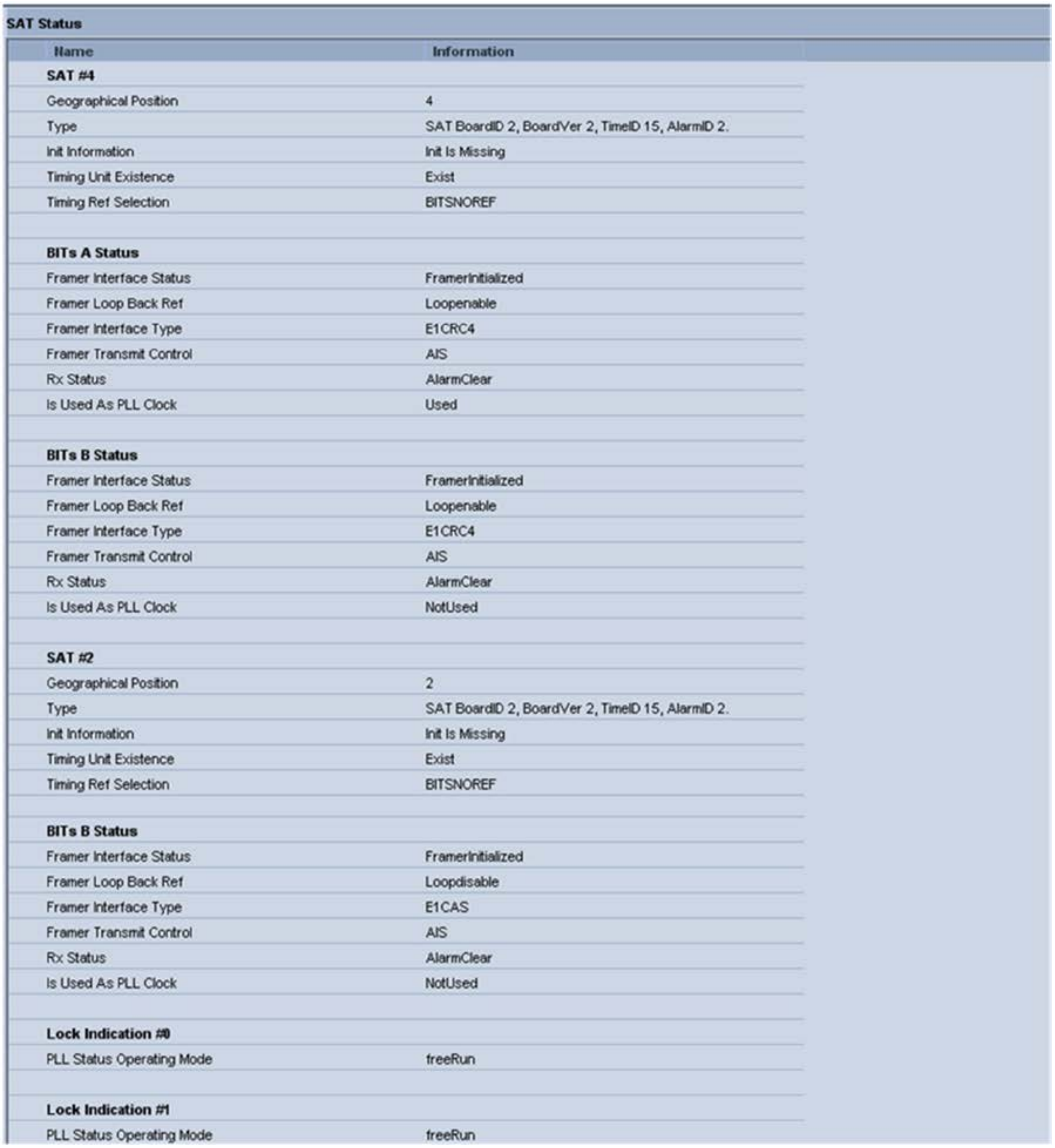
Green represents OK status, Red represents an alarm (problem), Grey -represents OFF

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

17.4 Provisioning

For provisioning of the Mediant 3000, click the Status and configuration 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.

17.5 Physical and Logical Components Status

17.5.1 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'.

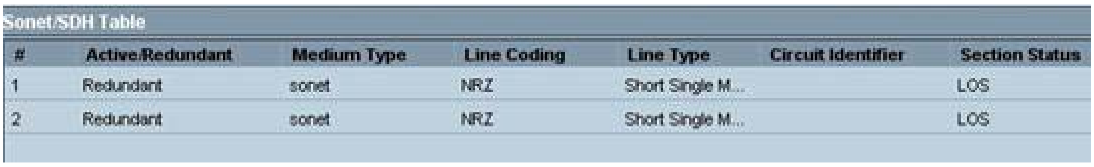
The Sonet OC3 interface on the TP-6310 board supports mapping to three DS3 channels using STS1 (*DS3 Channelization-Asynchronous DS3*).

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



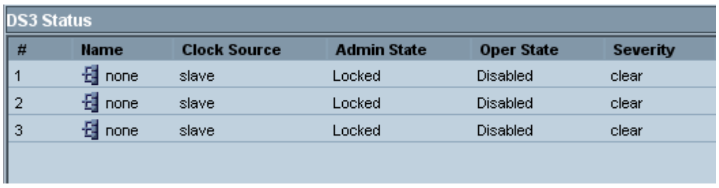
Sonet/SDH Table

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

17.5.2 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



DS3 Status

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

17.5.3 DS1 Interfaces

DS1 Trunks and Trunks Channels Status screens are described in 'MediaPack' on page 213.

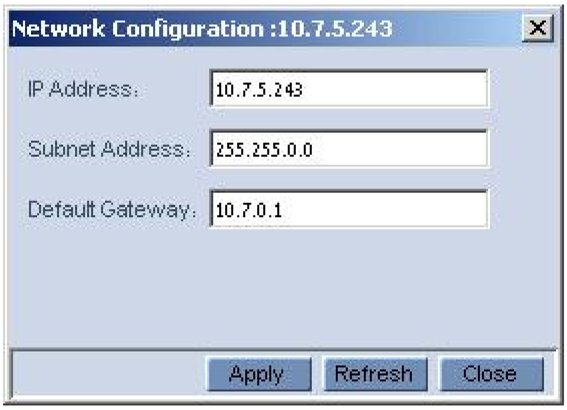
17.6 Executable Actions

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

17.6.1 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



Network Configuration :10.7.5.243

IP Address: 10.7.5.243

Subnet Address: 255.255.0.0

Default Gateway: 10.7.0.1

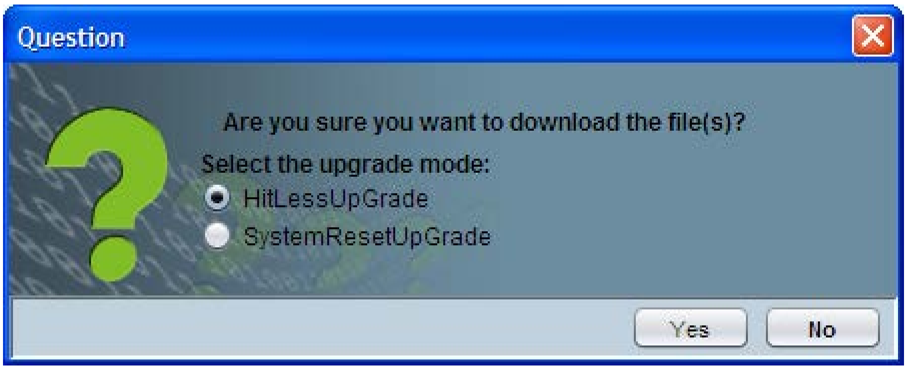
Note: Reconfiguring the network parameters might cause a loss of connection with the device. Make sure that the IP address you reconfigure is distinct from those of other devices in the tree.

17.6.2 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



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

Select the upgrade mode:

● HitLessUpGrade

○ SystemResetUpGrade

17.6.3 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.

17.6.4 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.

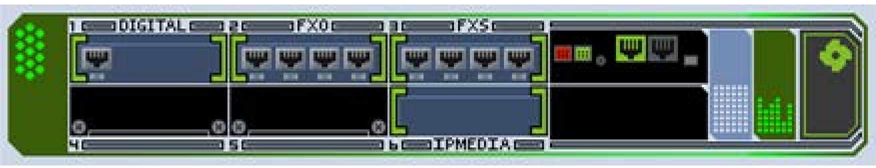
18 Mediant 600 and Mediant 1000

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

18.1 Mediant 1000 Status Pane

The figure below displays the Mediant 1000 status pane.

Figure 13-1: Mediant 1000 Status



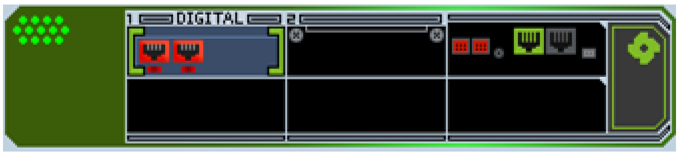
Note the following:

- 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 186.

18.2 Mediant 600 Status Pane

The Mediant 600 status pane is illustrated below.

Figure 13-2: Mediant 600 Status Pane



18.3 Provisioning

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

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

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

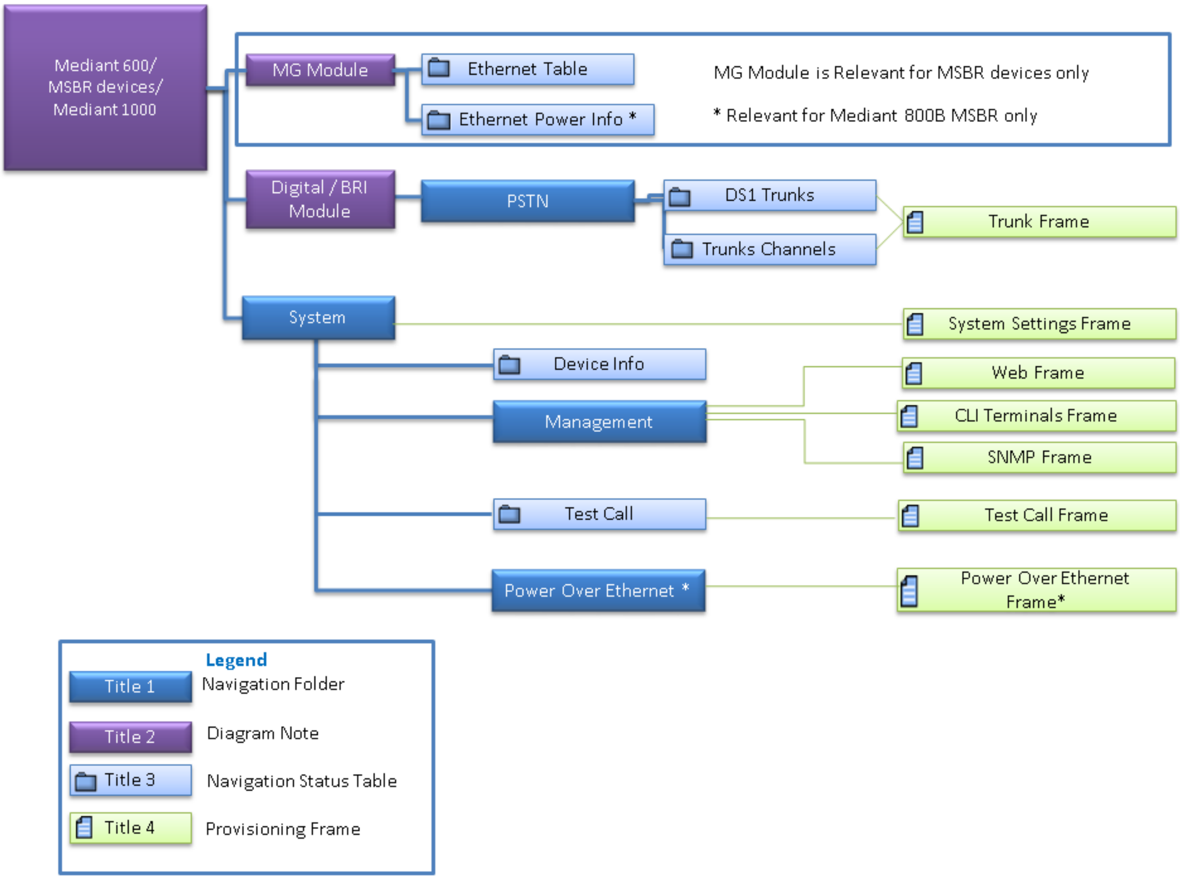


Figure 13-4: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 2)

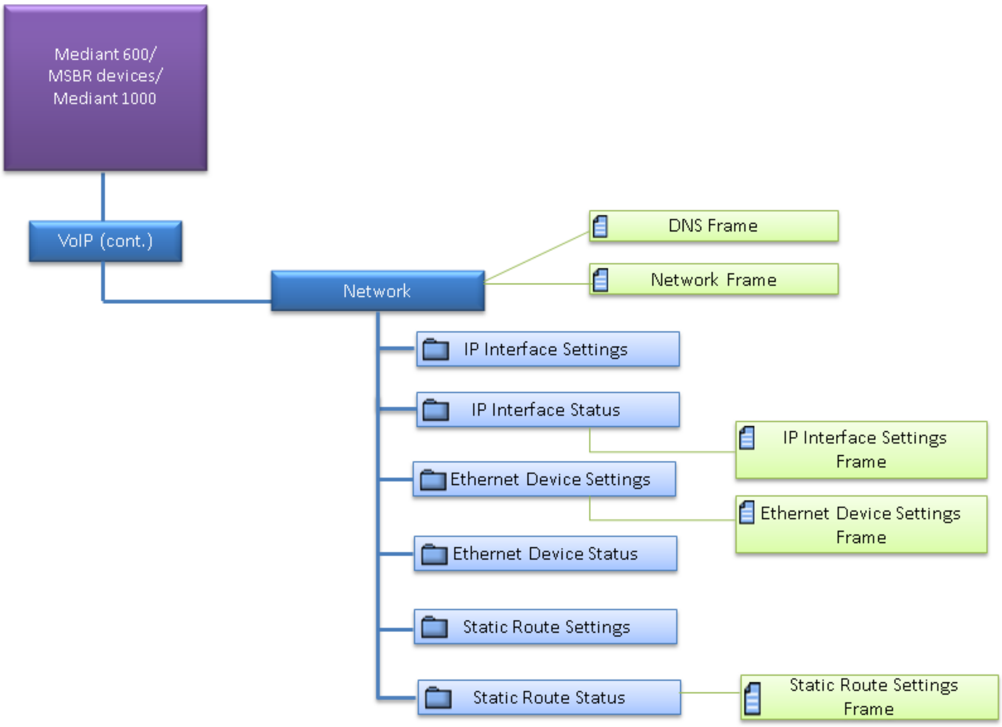


Figure 13-5: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 3)

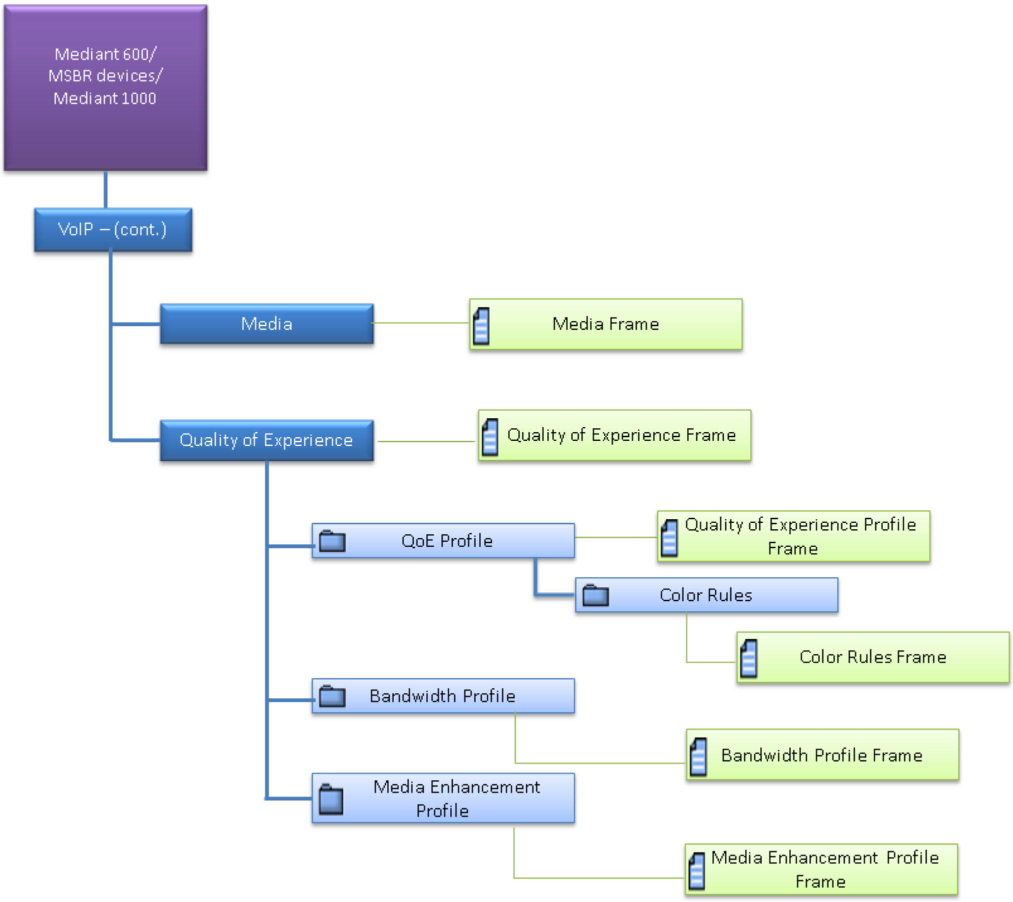


Figure 13-6: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 4)

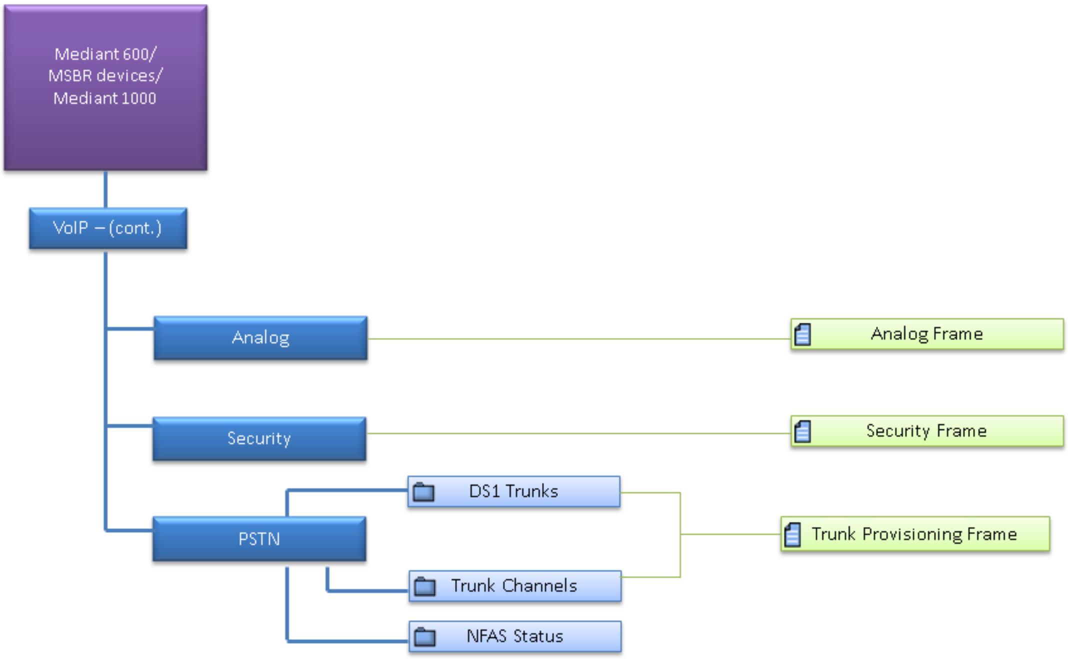


Figure 13-7: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 5)

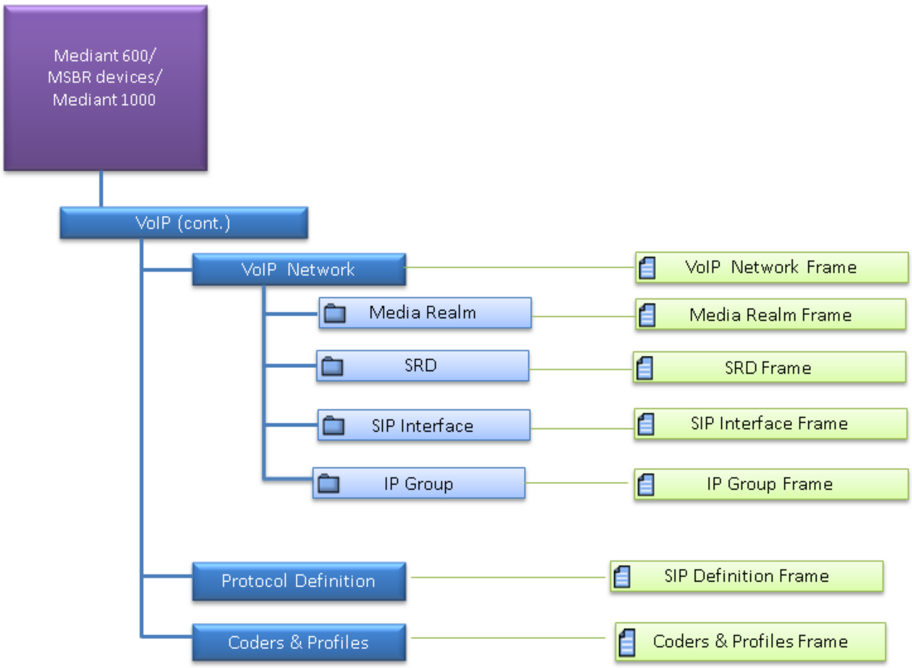


Figure 13-8: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 6)

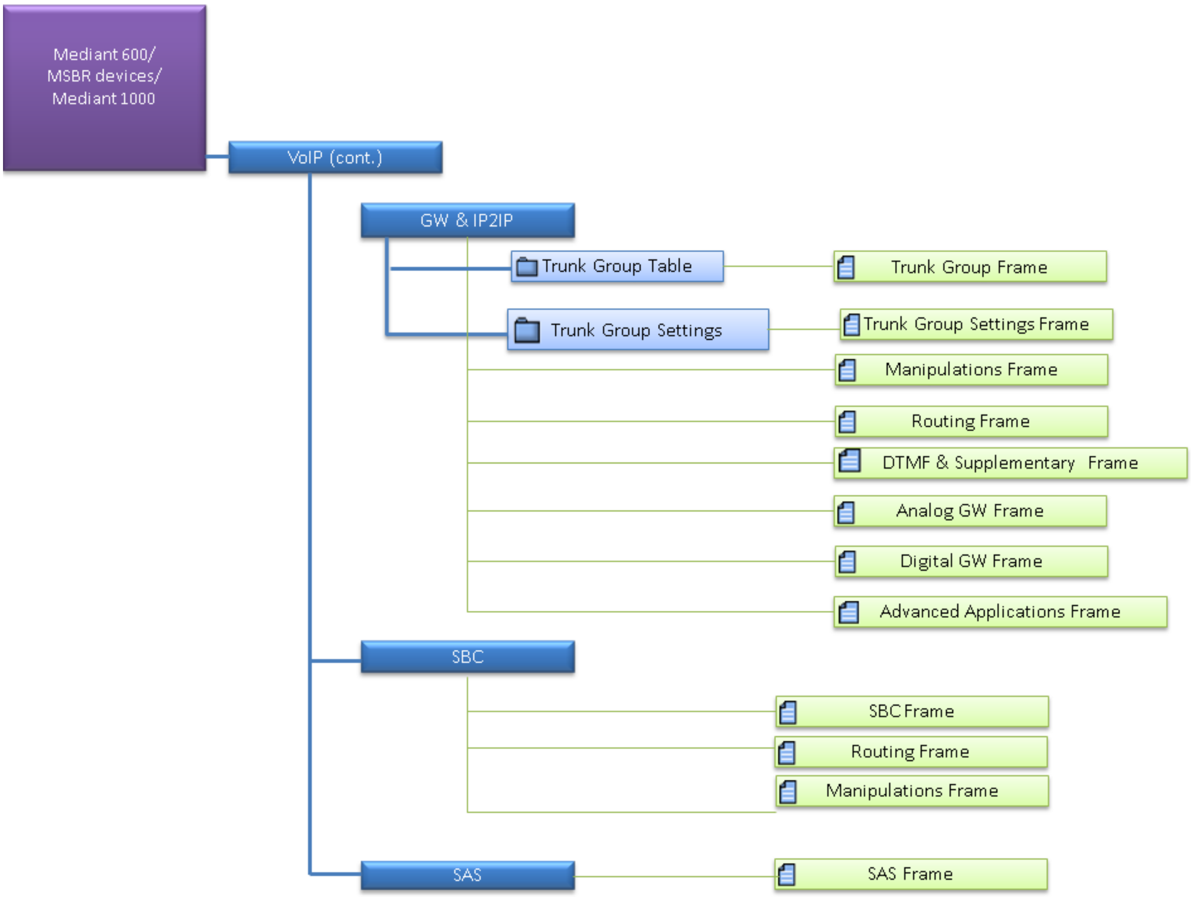
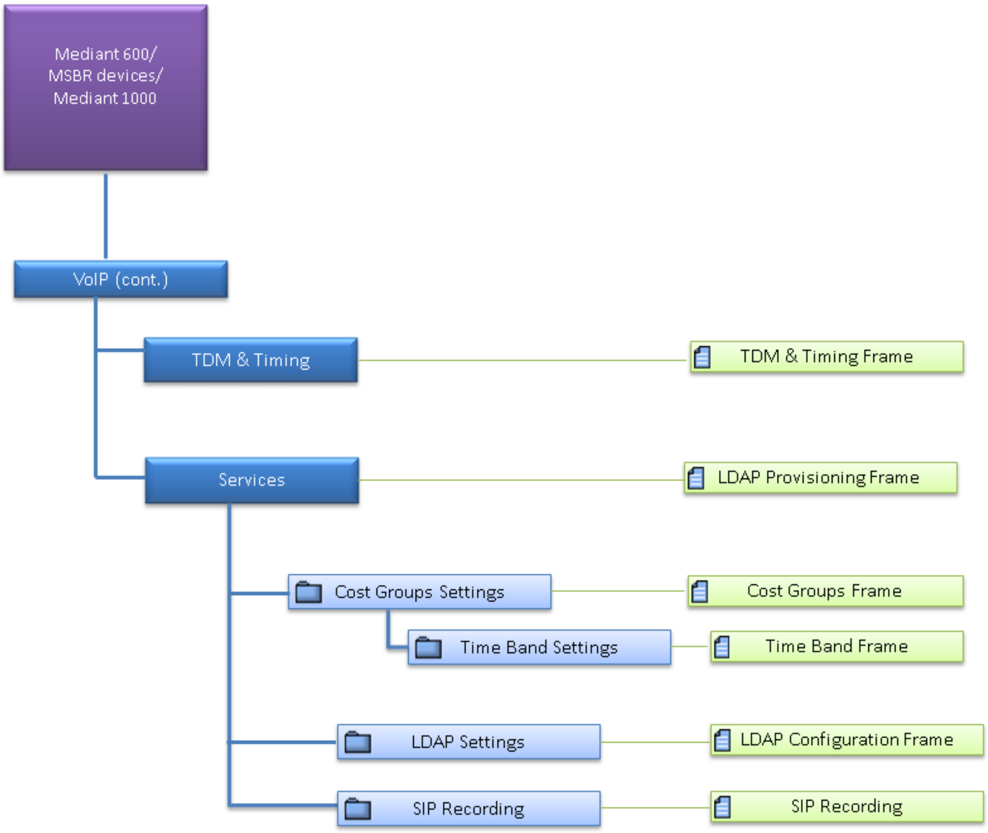


Figure 13-9: Navigation Hierarchy Links - Mediant 600, MSBR Products and Mediant 1000 (Part 7)



See Section 'Provisioning Concepts' on page 226 to learn about provisioning parameter types, how to work with table status columns and how to create and apply profiles.

18.4 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 229.

19 Mediant Gateway and E-SBC Products

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

19.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

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

19.2 Initial Configuration

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

19.3 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.

Figure 13-1: Mediant 1000B Gateway and E-SBC Status Pane

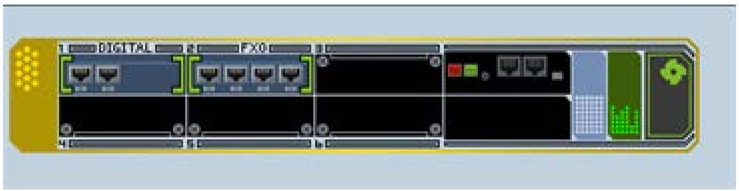
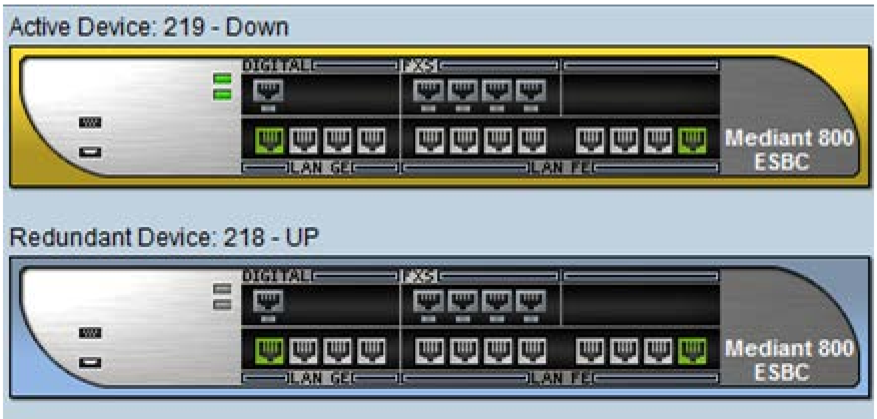


Figure 14-2: Mediant 800B Gateway and E-SBC HA Status Pane



Active Device: 219 - Down

Redundant Device: 218 - UP

Figure 13-3: Mediant 500L Gateway and E-SBC Status Pane

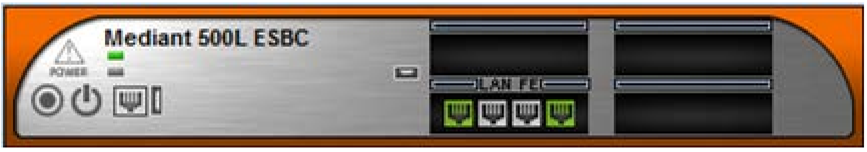
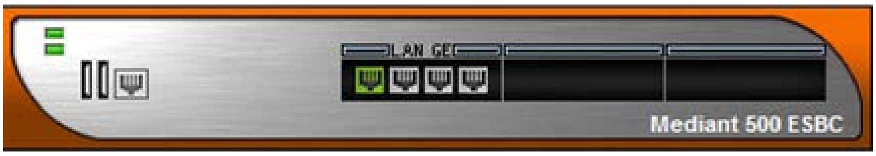
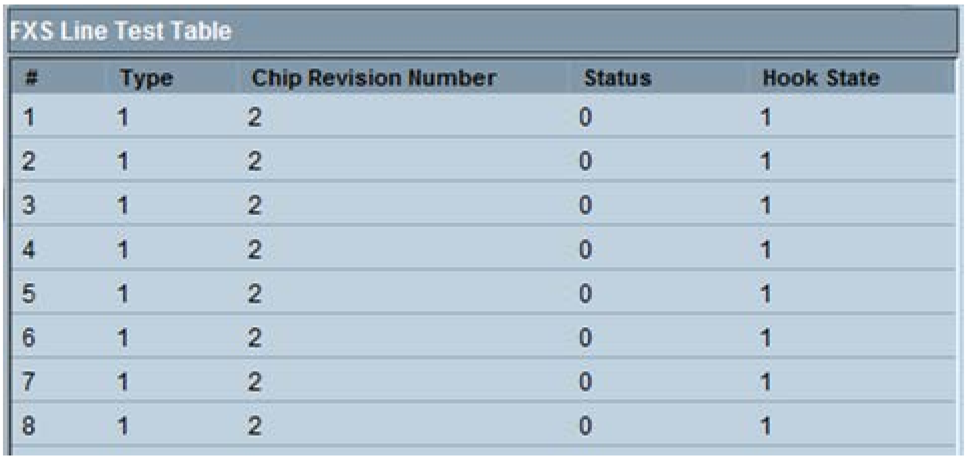


Figure 13-4: Mediant 500 E-SBC Status Pane



- The ▤ LEDs indicate the status of the power and reboot/initialization of the device.
- Double-click an FXO/FXS link to open the FXO/FXS Line Test Table.

Figure 13-5: FXS Line Test Table



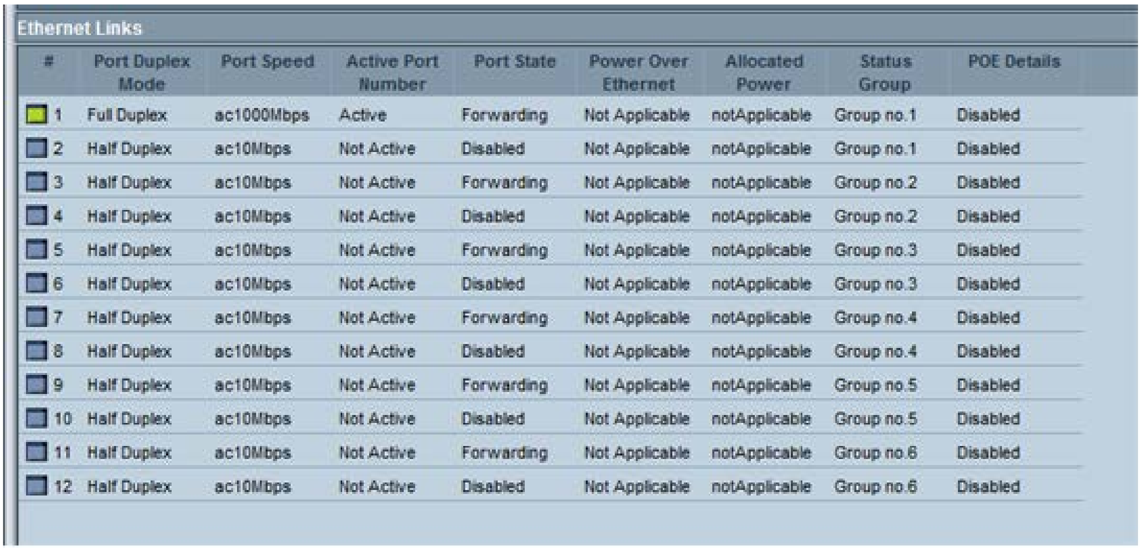
FXS Line Test Table

#	Type	Chip Revision Number	Status	Hook State
1	1	2	0	1
2	1	2	0	1
3	1	2	0	1
4	1	2	0	1
5	1	2	0	1
6	1	2	0	1
7	1	2	0	1
8	1	2	0	1

- Gigabit Ethernet port status icons:
  - 🟩 (green): Ethernet link is working
  - ▨ (gray): Ethernet link is not connected

Double-click one of the Ethernet ports (to display the detailed status for each port); the Ethernet Links Table screen is displayed:

Figure 14-6: Mediant 800B E-SBC and Gateway Ethernet Links

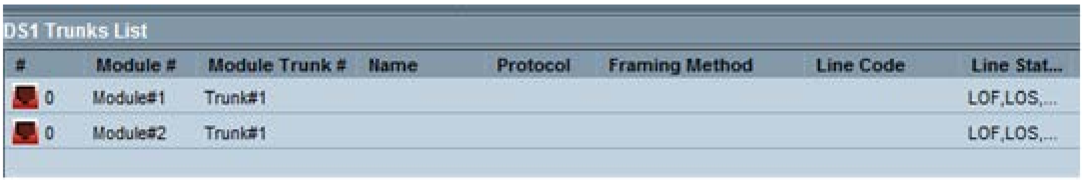


Ethernet Links

#	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 (labeled 'Digital') to open the DS1 Trunks List.

Figure 14-7: 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,...

19.4 Provisioning

For provisioning of E-SBC products, click the Status and configuration 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.

19.5 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 229.

This page is intentionally left blank.

20 CloudBond 365

This chapter describes the management of the CloudBond 365 products.

20.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- CloudBond 365 Standard Edition (Mediant 800B platform)
- CloudBond 365 Standard Plus Edition (Mediant 800B platform)
- CloudBond 365 Pro Edition (Mediant Server platform)
- CloudBond 365 Enterprise Edition (Mediant Server platform)
- CloudBond 365 Virtualized Edition (Mediant Server platform)

20.2 Initial Configuration

Refer to either the CloudBond documentation for the initial device configuration.

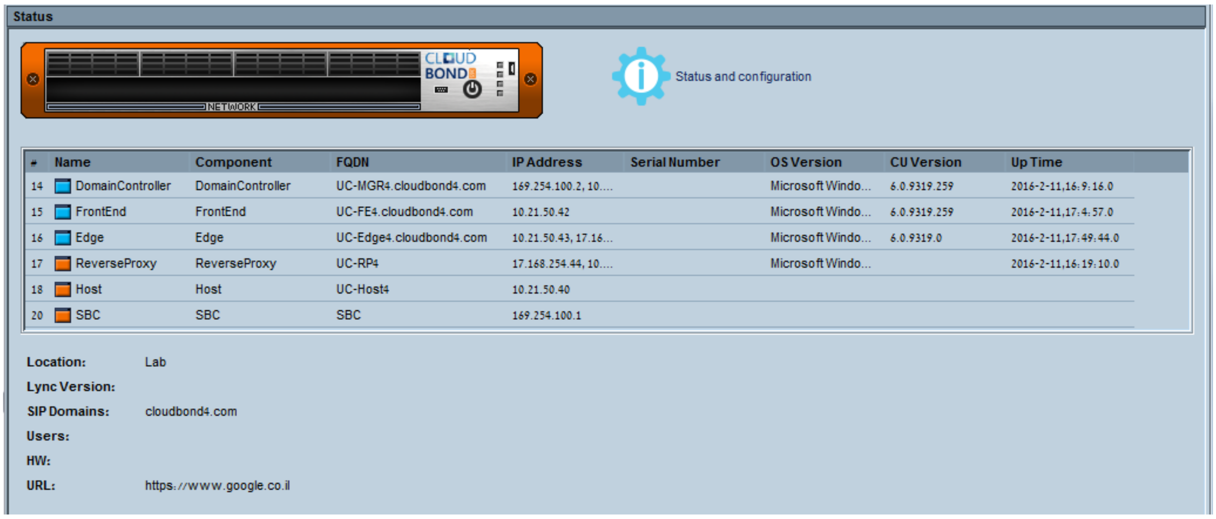
20.3 Status Pane

This Status pane provides the following information:

- Device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

The figures below display the CloudBond 365 Enterprise Edition Status pane.

Figure 13-1: CloudBond 365 Pro Edition



#	Name	Component	FQDN	IP Address	Serial Number	OS Version	CU Version	Up Time
14	DomainController	DomainController	UC-MGR4.cloudbond4.com	169.254.100.2, 10....		Microsoft Windo...	6.0.9319.259	2016-2-11,16:9:16.0
15	FrontEnd	FrontEnd	UC-FE4.cloudbond4.com	10.21.50.42		Microsoft Windo...	6.0.9319.259	2016-2-11,17:4:57.0
16	Edge	Edge	UC-Edge4.cloudbond4.com	10.21.50.43, 17.16...		Microsoft Windo...	6.0.9319.0	2016-2-11,17:49:44.0
17	ReverseProxy	ReverseProxy	UC-RP4	17.168.254.44, 10....		Microsoft Windo...		2016-2-11,16:19:10.0
18	Host	Host	UC-Host4	10.21.50.40				
20	SBC	SBC	SBC	169.254.100.1				

Location: Lab

Lync Version:

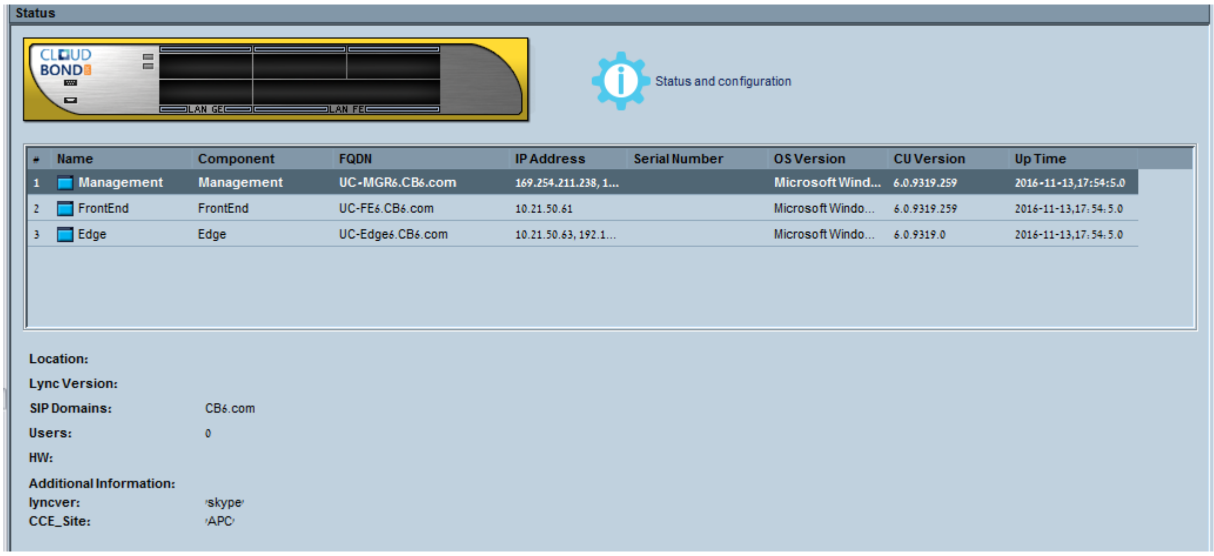
SIP Domains: cloudbond4.com

Users:

HW:

URL: https://www.google.co.il

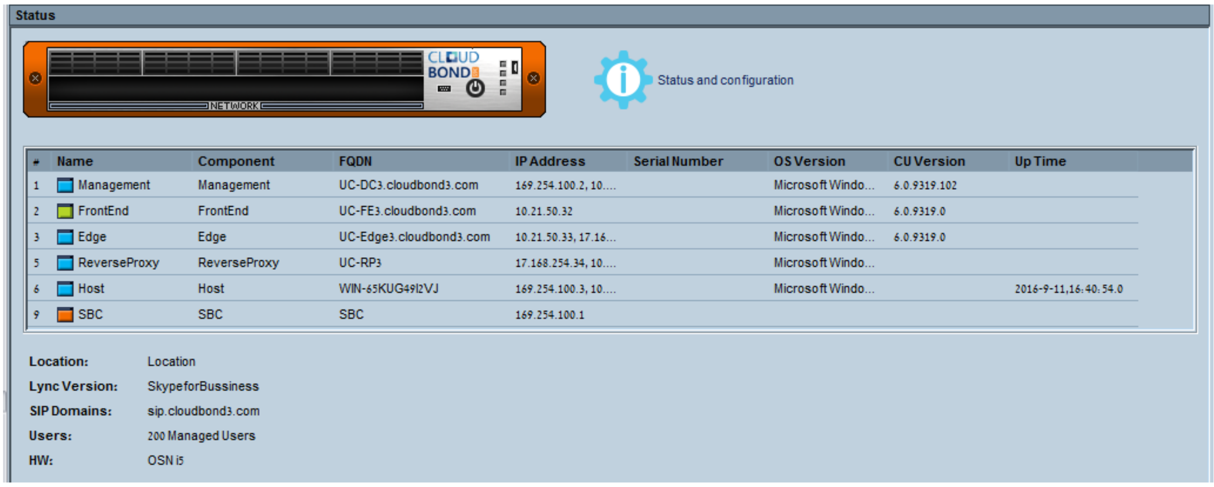
Figure 13-2: CloudBond 365 Standard Edition



#	Name	Component	FQDN	IP Address	Serial Number	OS Version	CU Version	Up Time
1	Management	Management	UC-MGR6.CB6.com	169.254.211.238, 1...		Microsoft Wind...	6.0.9319.259	2016-11-13,17:54:5.0
2	FrontEnd	FrontEnd	UC-FE6.CB6.com	10.21.50.61		Microsoft Windo...	6.0.9319.259	2016-11-13,17:54:5.0
3	Edge	Edge	UC-Edge6.CB6.com	10.21.50.63, 192.1...		Microsoft Windo...	6.0.9319.0	2016-11-13,17:54:5.0

Location:	
Lync Version:	
SIP Domains:	CB6.com
Users:	0
HW:	
Additional Information:	
lyncver:	'skype'
CCE_Site:	'APC'

Figure 13-3: CloudBond 365 Enterprise Edition



#	Name	Component	FQDN	IP Address	Serial Number	OS Version	CU Version	Up Time
1	Management	Management	UC-DC3.cloudbond3.com	169.254.100.2, 10....		Microsoft Windo...	6.0.9319.102	
2	FrontEnd	FrontEnd	UC-FE3.cloudbond3.com	10.21.50.32		Microsoft Windo...	6.0.9319.0	
3	Edge	Edge	UC-Edge3.cloudbond3.com	10.21.50.33, 17.16...		Microsoft Windo...	6.0.9319.0	
5	ReverseProxy	ReverseProxy	UC-RP3	17.168.254.34, 10....		Microsoft Windo...		
6	Host	Host	WIN-65KUG49I2VJ	169.254.100.3, 10....		Microsoft Windo...		2016-9-11,16:40:54.0
9	SBC	SBC	SBC	169.254.100.1				

Location:	Location
Lync Version:	SkypeforBussiness
SIP Domains:	sip.cloudbond3.com
Users:	200 Managed Users
HW:	OSN i5

- The CloudBond server components are represented by Blue icons.
- The Software SBC server components are represented by Orange icons.

The following table describes the components that are displayed:

Table 20-1: CloudBond 365 Componet Statuses

Detail	Description
Name	The name of the Microsoft Windows (Skype for Business Server) component.
Component	The type of the Microsoft Windows (Skype for Business Server) component.
FQDN	The components FQDN in the Enterprise’s network.
IP Address	The IP address of the component.
Serial Number	The serial number of the component.
OS Version	The Microsoft Windows Operating system of the component.
CU Version	The Microsoft Windows Cumulative Update version.
Up Time	The time that the component is active.

20.4 Provisioning

For provisioning of CloudBond 365 products, click the link in the status screen to open the device's Web server.

Refer to the relevant *CloudBond/CCE Appliance Manual.*

Note: Single Sign-on is not supported for CloudBond and CCE Appliance products. Consequently when you click the above link, the CloudBond or CCE Appliance Login screen is displayed.

20.5 Executable Actions

Executable actions are not supported for this product series.

This page is intentionally left blank.

21 CCE Appliance

This chapter describes the management of the CCE Appliance products.

21.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Mediant 800 CCE Appliance
- Mediant Server CCE Appliance

21.2 Initial Configuration

Refer to either the CloudBond documentation for the initial device configuration.

21.3 Status Pane

This Status pane provides the following information:

- Device active / redundant alarm status color coding.
- Commands supported: Switchover; Reset whole chassis or Reset Redundant chassis.

Figure 13-1: Mediant 800 CCE Appliance

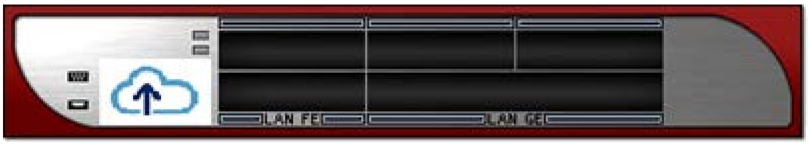
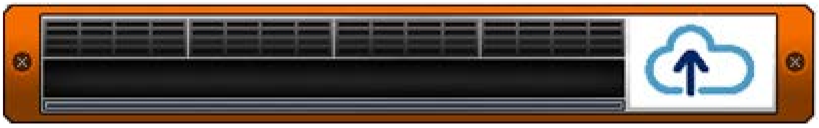


Figure 13-2: Mediant Server CCE Appliance



- The CCE Appliance components are represented by Blue icons.
- The Software SBC server components are represented by Orange icons.

The following table describes the components that are displayed:

Table 21-1: CCE Appliance Components

Detail	Description
Name	The name of the Microsoft Windows (Skype for Business Server) component.
Component	The type of the Microsoft Windows (Skype for Business Server) component.
FQDN	The components FQDN in the Enterprise’s network.
IP Address	The IP address of the component.

Detail	Description
Serial Number	The serial number of the component.
OS Version	The Microsoft Windows Operating system of the component.
CU Version	The Microsoft Windows Cumulative Update version.
Up Time	The time that the component is active.

21.4 Provisioning

For provisioning the CCE Appliance devices, click the ⓘ Status and configuration link in the status screen to open the device's Web server.

Refer to the relevant *CCE Appliance Manual.*

⚠ **Note:** Single Sign-on is not supported for CCE Appliance products. Consequently when you click the above link, the CCE Appliance Login screen is displayed.

21.5 Executable Actions

Executable actions are not supported for this product series.

22 Mediant MSBR Products

This section describes the management of the MSBR devices.

22.1 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.

22.2 Initial Configuration

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

22.3 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

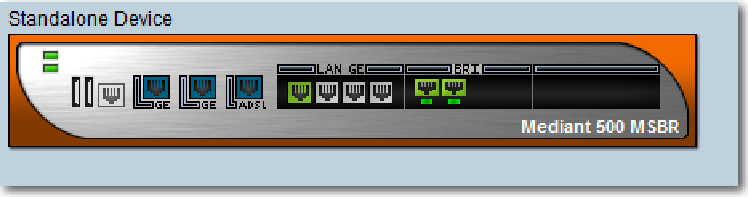


Figure 15-2: Mediant 500L MSBR Status Pane

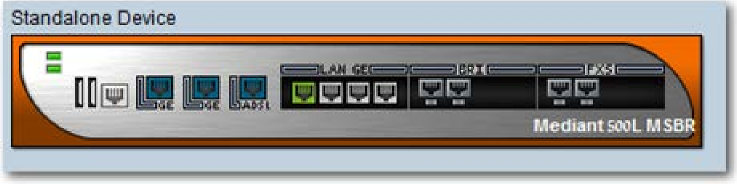


Figure 15-3: Mediant 800B MSBR Status Pane

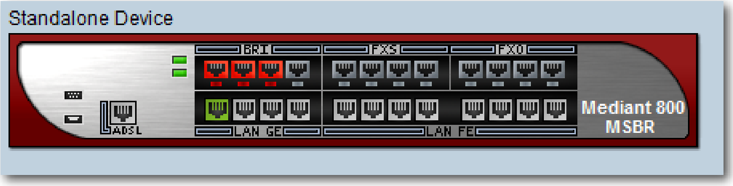
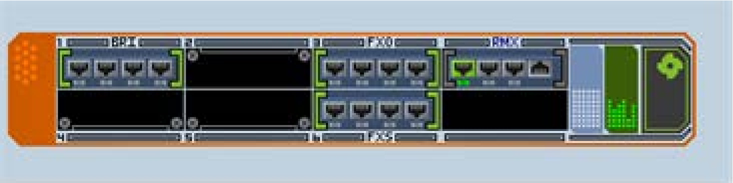


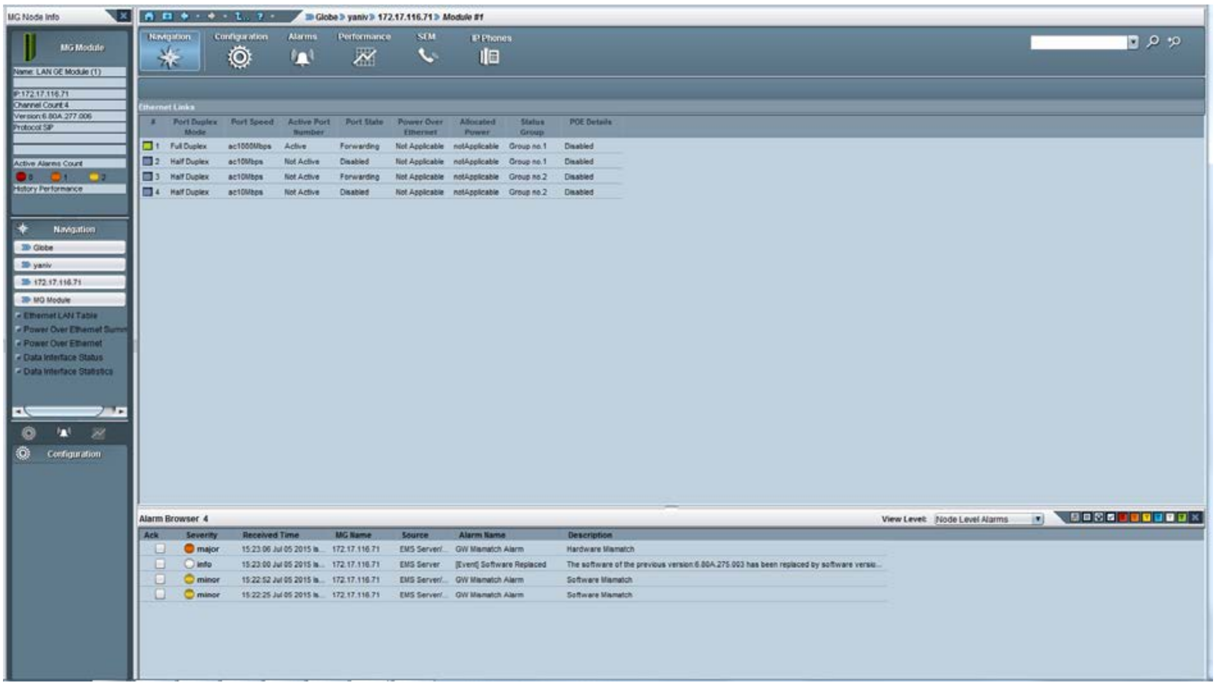
Figure 15-4: Mediant 1000B MSBR Status Pane



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



Name: LAN GE Module (1)
IP:172.17.116.71
Channel Count:4
Version:6.80A.277.006
Protocol:SIP
Active Alarms Count
● 0 ● 1 ● 2
History Performance

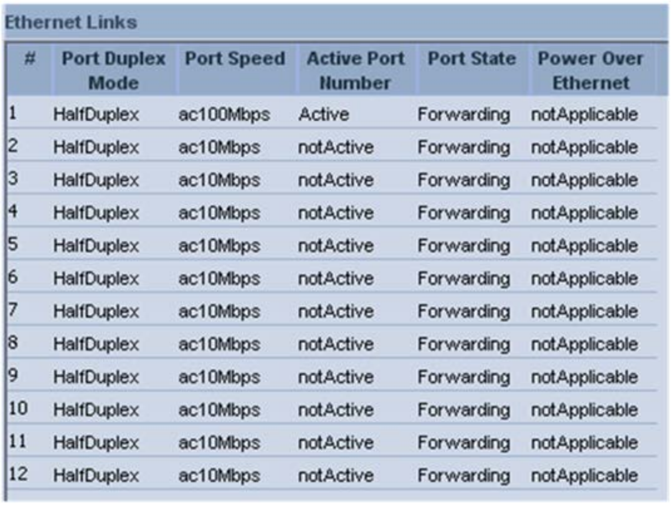
Ethernet Links

#	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

Alarm Browser 4

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	● major	15:23:06 Jul 05 2015 is...	172.17.116.71	EMS Server/...	GW Mismatch Alarm	Hardware Mismatch
□	○ info	15:23:00 Jul 05 2015 is...	172.17.116.71	EMS Server	[Event] Software Replaced	The software of the previous version:6.80A.275.003 has been replaced by software versio...
□	● minor	15:22:52 Jul 05 2015 is...	172.17.116.71	EMS Server/...	GW Mismatch Alarm	Software Mismatch
□	● minor	15:22:25 Jul 05 2015 is...	172.17.116.71	EMS Server/...	GW Mismatch Alarm	Software Mismatch

Figure 15-6: Mediant 800 MSBR Ethernet Links



Ethernet Links

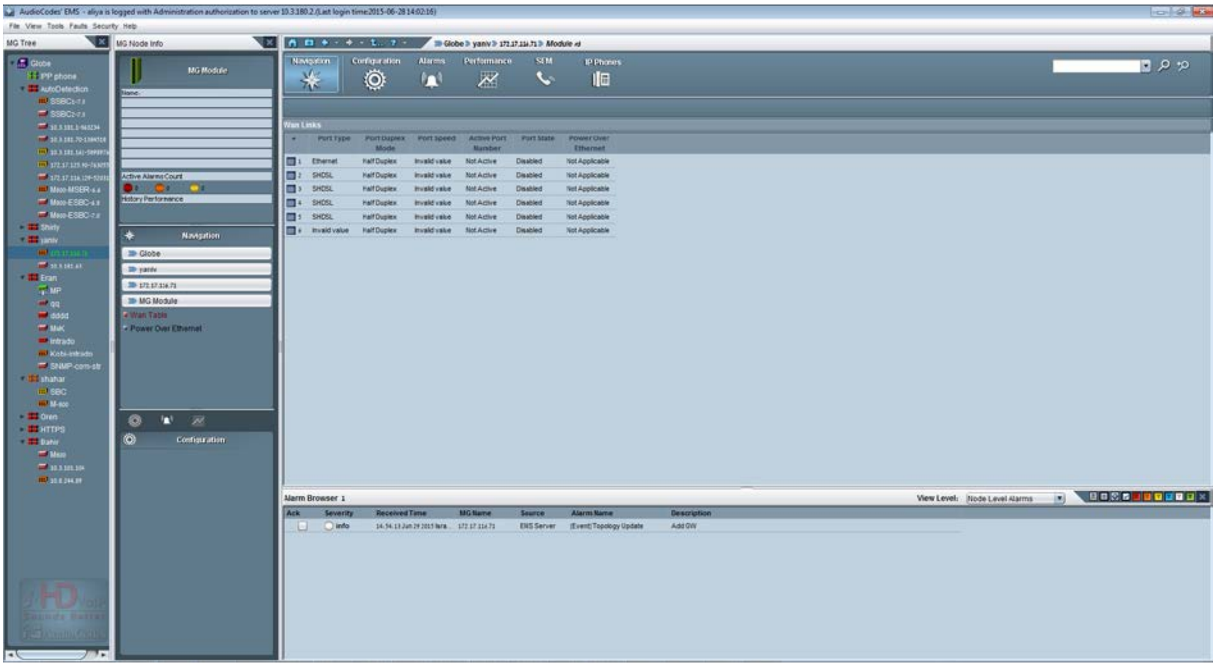
#	Port Duplex Mode	Port Speed	Active Port Number	Port State	Power Over Ethernet
1	HalfDuplex	ac100Mbps	Active	Forwarding	notApplicable
2	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
3	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
4	HalfDuplex	ac10Mbps	notActive	Forwarding	notApplicable
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



Wan Links

#	Port Type	Port Duplex Mode	Port Speed	Active Port Number	Port State	Power Over Ethernet
1	Ethernet	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable
2	SHDSL	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable
3	SHDSL	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable
4	SHDSL	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable
5	SHDSL	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable
6	Invalid value	Half Duplex	Invalid value	Not Active	Disabled	Not Applicable

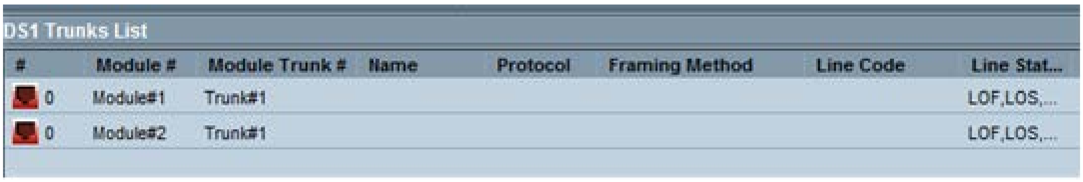
Alarm Browser 1 View Level: Node Level Alarms

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	○ info	14:54:13 Jun 29 2015 Isra...	172.17.114.71	EMS Server	[Event] Topology Update	Add GW

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



DS1 Trunks List

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

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

22.4 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 18.3 on page 190.

See Section 'Provisioning Concepts' on page 226 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 to the EMS and then download it to the MSBR device (see below).

22.5 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 229.

This page is intentionally left blank.

23 MP-1288

23.1 Supported Configuration

EMS supports the following product configuration described in this chapter:

- Standalone (Simplex) MP-1288

23.2 Initial Configuration

Refer to the MP-1288 High-Density Analog Media Gateway User's Manual for the initial device configuration.

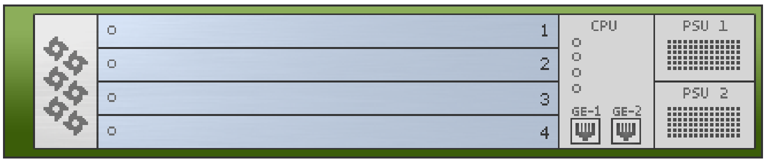
23.3 Status Pane

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 figure below display the MP-1288 status pane.

Figure 15-1: MP-1288 Status Pane



This page is intentionally left blank.

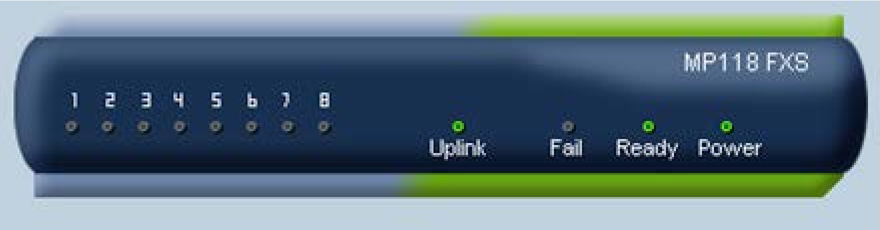
24 MP-11x and MP-124

This section describes the management of the MediaPack devices.

24.1 Status Pane

The figure below shows an example of the MP-118 Status pane. The Status pane for the 4-channel, 8-channel, and 24-channel devices are identical (except for the number of channels).

Figure 16-1: MP-11x Status Pane



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

Table 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 control protocol type. It also includes hardware, software or configuration mismatch information, in case any problem is detected. 'Reset Needed' indicates that the operator changed offline parameters and that a reset must be performed to apply these parameters to the device.

24.1.1 Line Test

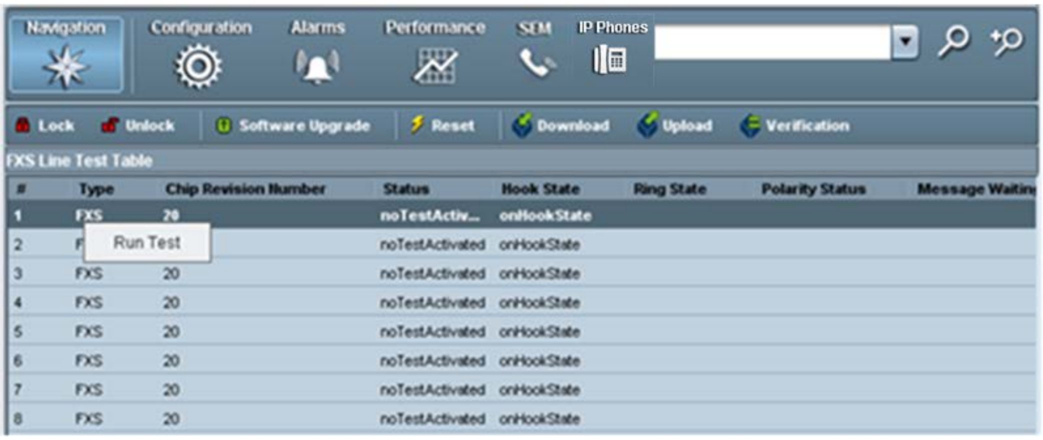
The MediaPack device supports Line Testing.

➢ **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



FXS Line Test Table

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

24.1.2 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)

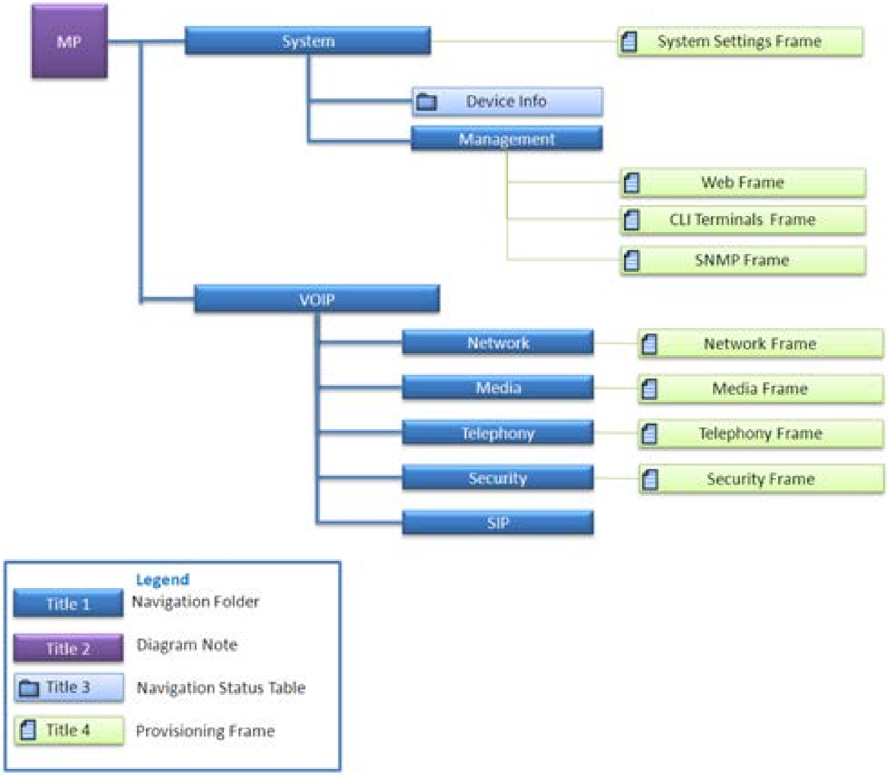
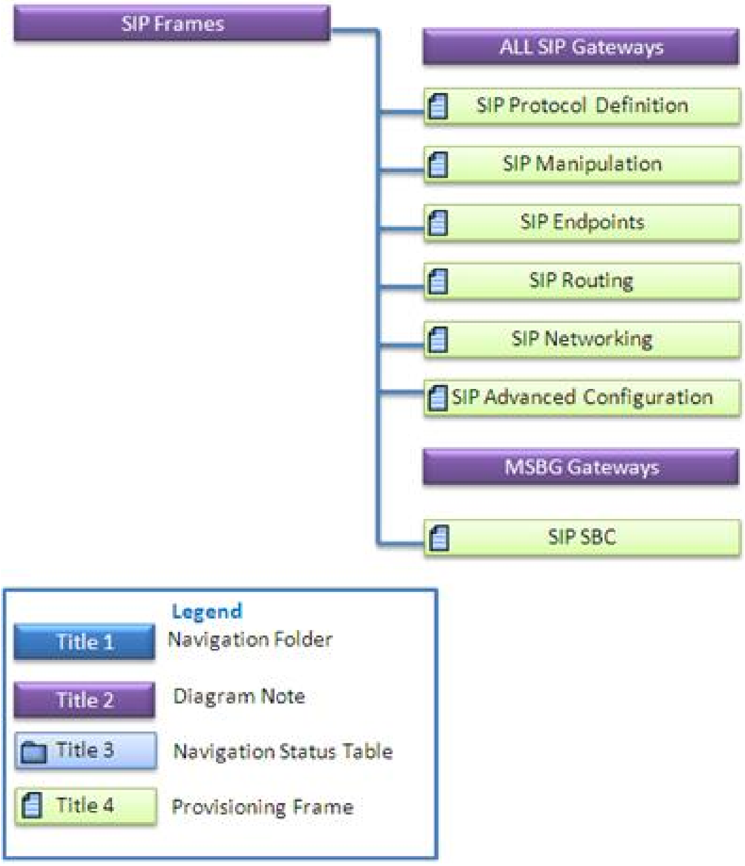


Figure 16-4: Navigation Hierarchy Links – MediaPack (Part 2)



See Section 'Provisioning Concepts' on page 226 to learn about parameter provisioning types, how to work with table status columns and how to create and apply profiles on provisioning parameters.

24.1.3 Executable Actions

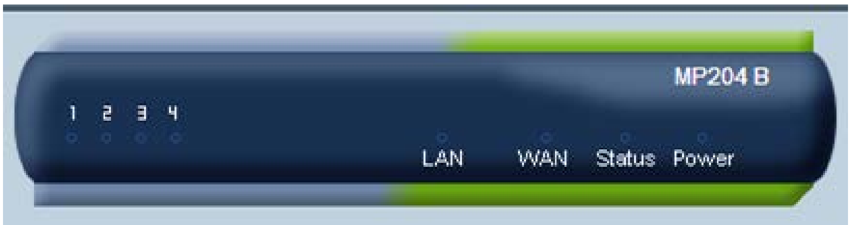
For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 229.

25 MP-20x

25.1 Status Pane

The figure below shows an example of the MP-204 Status pane. The Status pane for the other MP-20x modules are identical (except for the number of channels).

Figure 16-1: MP-20x Status Pane



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

Table 16-1: MP-20x Status LEDs

LED	Type	Color	State	Definition	EMS Representation
POWER	Device Status	**Green**	On	Power received by MP-20x	Power LED is *green*
		-	Off	MP-20x has been powered off	
STATUS		**Green**	On	System start-up successful	Status LED is *green*
		Red	On	Reboot (automatic, by default)	The entire MP is *red*
PHONE 1- 4	Telephone Interface	**Green**	Type 1 Blinking	Idle Proxy register ok	Channel LED is *green*
			On	Off-hook	Channel LED is *green*
			Type 2 Blinking	Phone ringing	Channel LED is *green*
			Type 3 Blinking	Upgrade in process (all LEDs including STATUS LED)	Channel LED is *green*
		Red	On	Idle Proxy register failed	Channel LED is *red*
		-	Off	On-hook and not ringing, not using Proxy	Channel LED is *red*
LAN / WAN	Ethernet Link	**Yellow**	Steady On	Connected at 10 Mbps	LAN LED is *yellow*.
			Steady On	Connected at 100 Mbps	LAN LED is *yellow*.

LED	Type	Color	State	Definition	EMS Representation
	Status		Blinking	Activity - there is traffic on 10/100 Mbps	LAN LED is *yellow*.
		Green	Steady On	Connected at 1000 Mbps	LAN LED is *green*.
			Blinking	Activity - there is traffic on 1000 Mbps	LAN LED is *green.*
		-	Off	Disconnected	LAN LED is *green.*

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

25.2 Provisioning

For provisioning the MP-2xx products, click the link in the status screen to open the device's Web server.

For information, refer to the MP-20x *User's Manual.*

25.3 Executable Actions

For the list of common supported configuration and maintenance actions, see Section 'CPE Configuration and Maintenance Actions' on page 229.

26 SBA

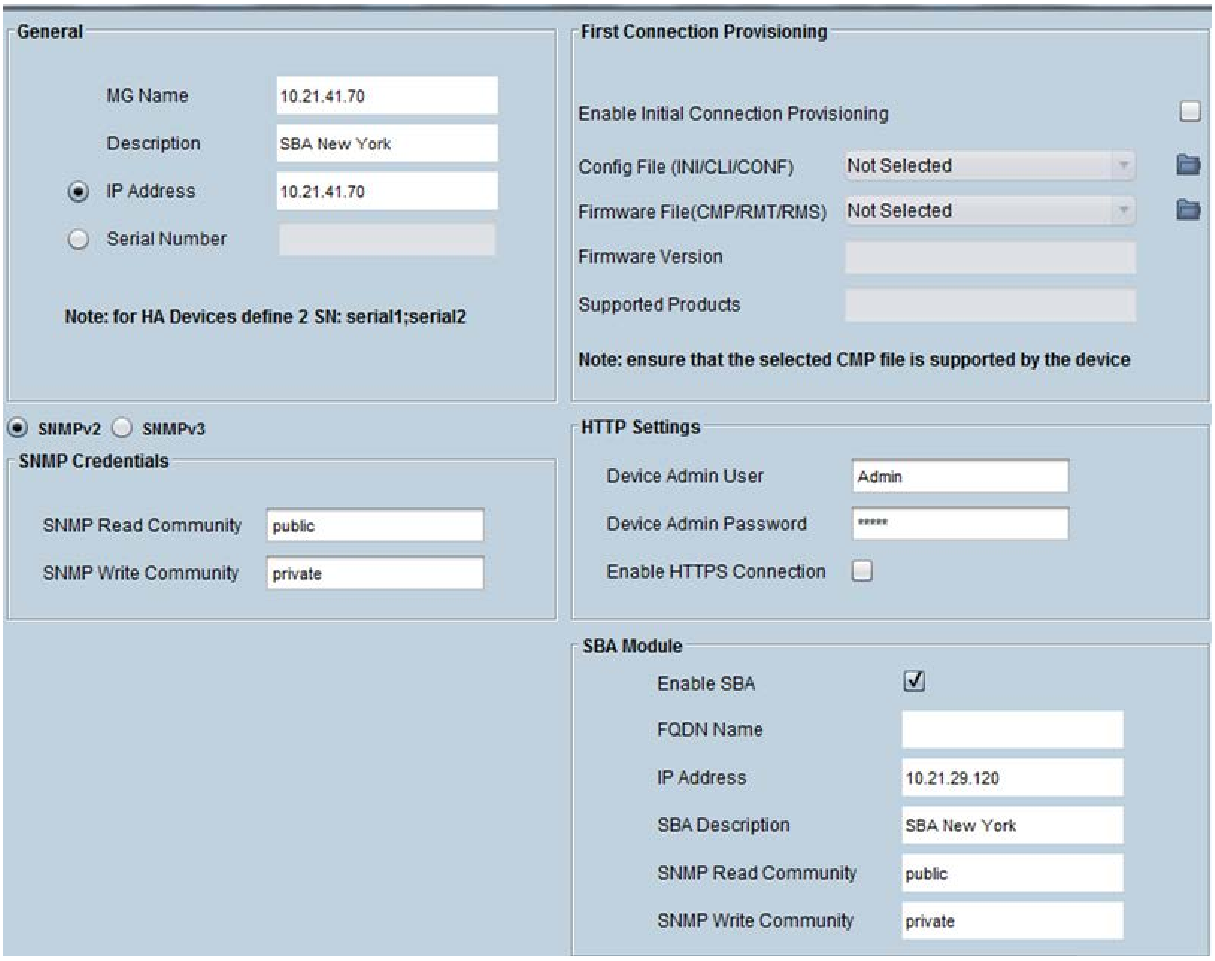
This section describes the management of the Mediant 800B or Mediant 1000B devices with SBA modules installed.

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 224).

➢ 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



General

MG Name: 10.21.41.70

Description: SBA New York

● IP Address: 10.21.41.70

○ Serial Number:

Note: for HA Devices define 2 SN: serial1;serial2

First Connection Provisioning

Enable Initial Connection Provisioning □

Config File (INI/CLI/CONF): Not Selected

Firmware File(CMP/RMT/RMS): Not Selected

Firmware Version:

Supported Products:

Note: ensure that the selected CMP file is supported by the device

● SNMPv2 ○ SNMPv3

SNMP Credentials

SNMP Read Community: public

SNMP Write Community: private

HTTP Settings

Device Admin User: Admin

Device Admin Password: *****

Enable HTTPS Connection □

SBA Module

Enable SBA ☑

FQDN Name:

IP Address: 10.21.29.120

SBA Description: SBA New York

SNMP Read Community: public

SNMP Write Community: private

2. In the SBA Module pane, select the 'Enable SBA' check box.
3. Enter the P address of the SBA Management Interface (the IP address that you configured in the SBA Management interface).
4. Enter a description for the SBA module. This text is displayed in the Additional Info of the 'SBA Services' and 'Gateway Connection' alarms.

26.1 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.*

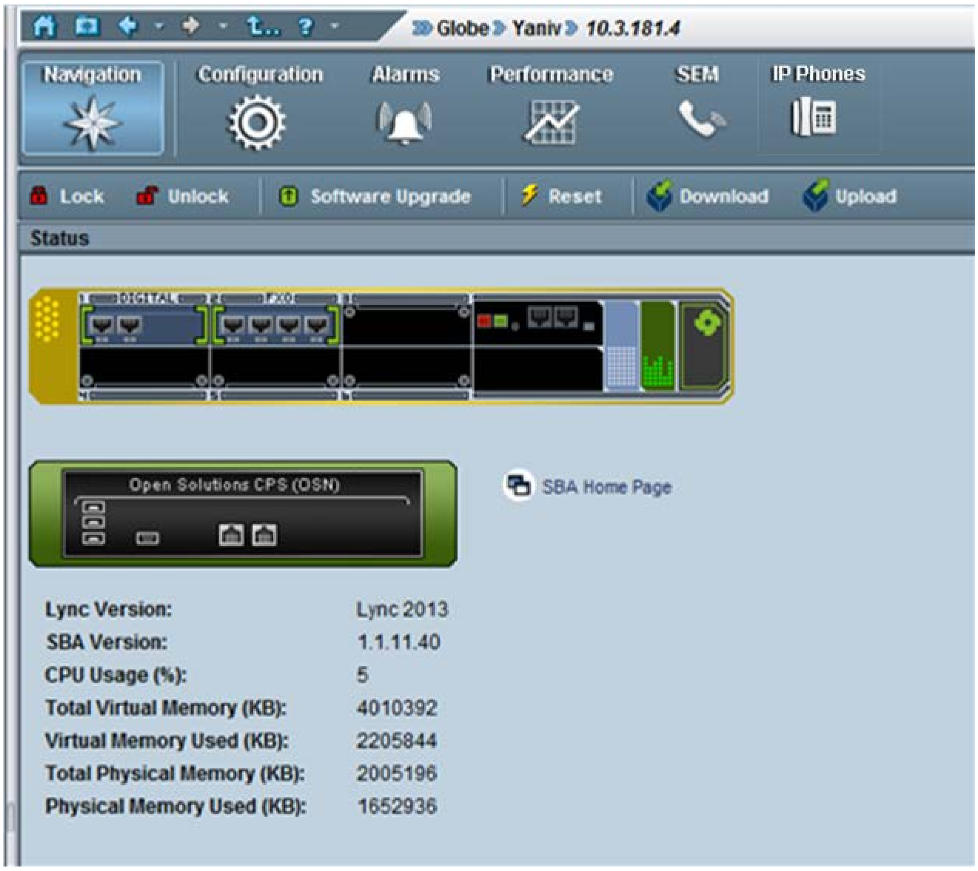
> **Note:**
>
> - The same community string values configured in the MG information screen (above in Figure 17-1) must be entered in the SNMP configuration on the SBA device.
> - The device must be configured for SNMPv2 only.

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 *Alarm and Performance Monitoring Guide*.

26.2 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

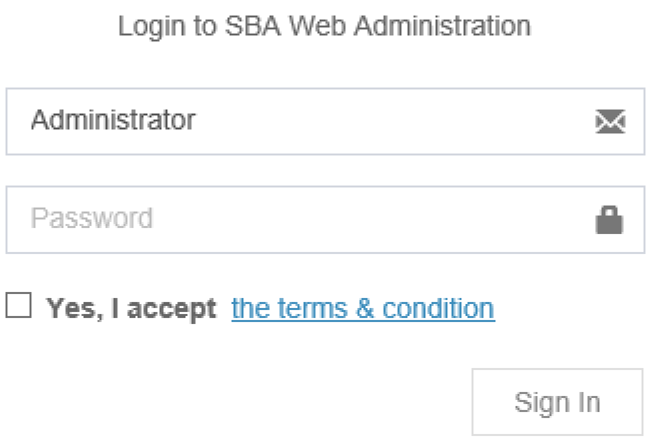


Lync Version:	Lync 2013
SBA Version:	1.1.11.40
CPU Usage (%):	5
Total Virtual Memory (KB):	4010392
Virtual Memory Used (KB):	2205844
Total Physical Memory (KB):	2005196
Physical Memory Used (KB):	1652936

26.2.1 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



Login to SBA Web Administration

Administrator

Password

□ Yes, I accept the terms & condition

Sign In

27 Trunks and Channels Status

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

27.1 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 reset. 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)

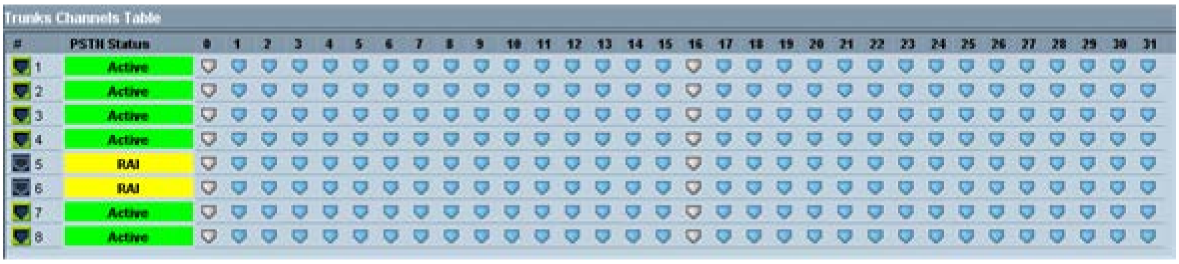
27.2 Trunk Channel Call Status

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 18-1: 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.

.

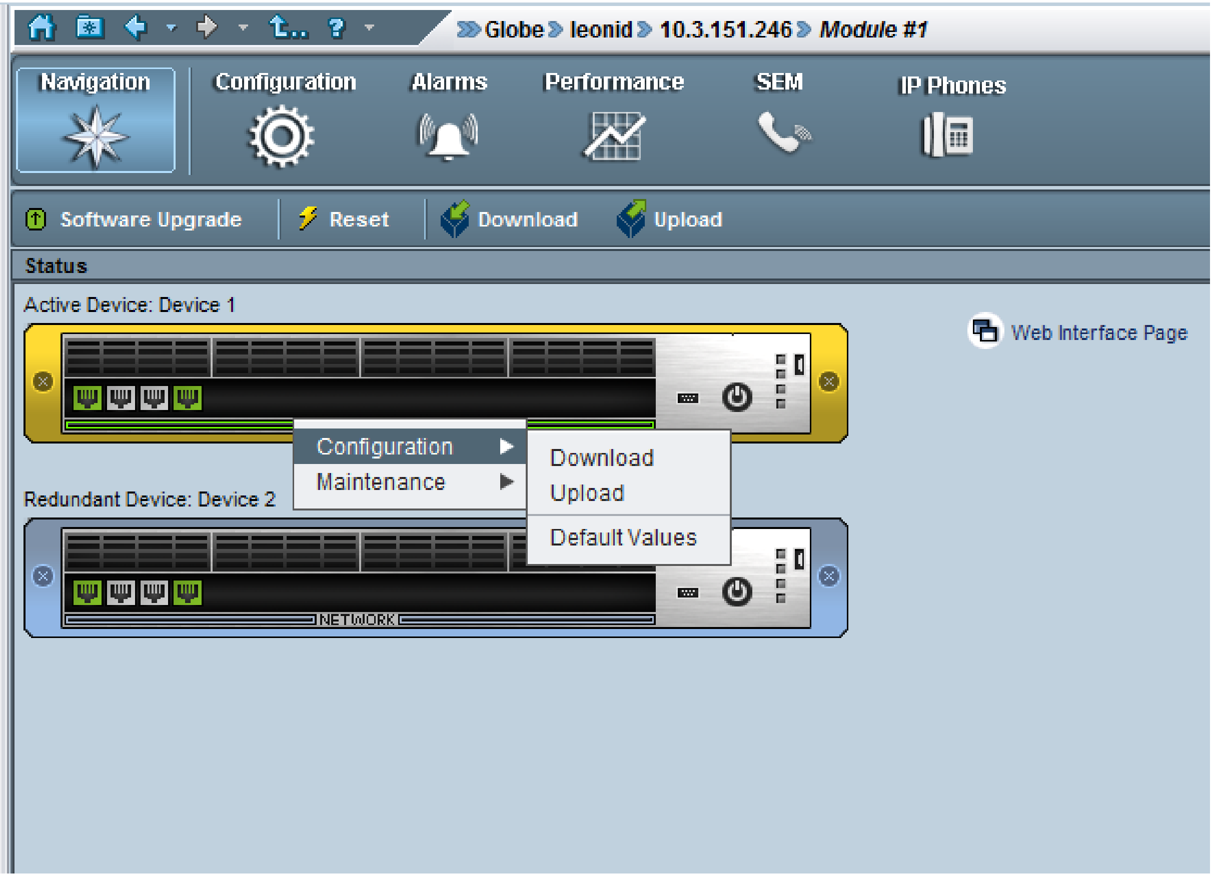
28 CPE Configuration and Maintenance Actions

This section describes the CPE Configuration and Maintenance actions.

28.1 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



- **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 or CLI script file (MSBR devices) to the device. In addition, an option is provided to include the download of auxiliary files.

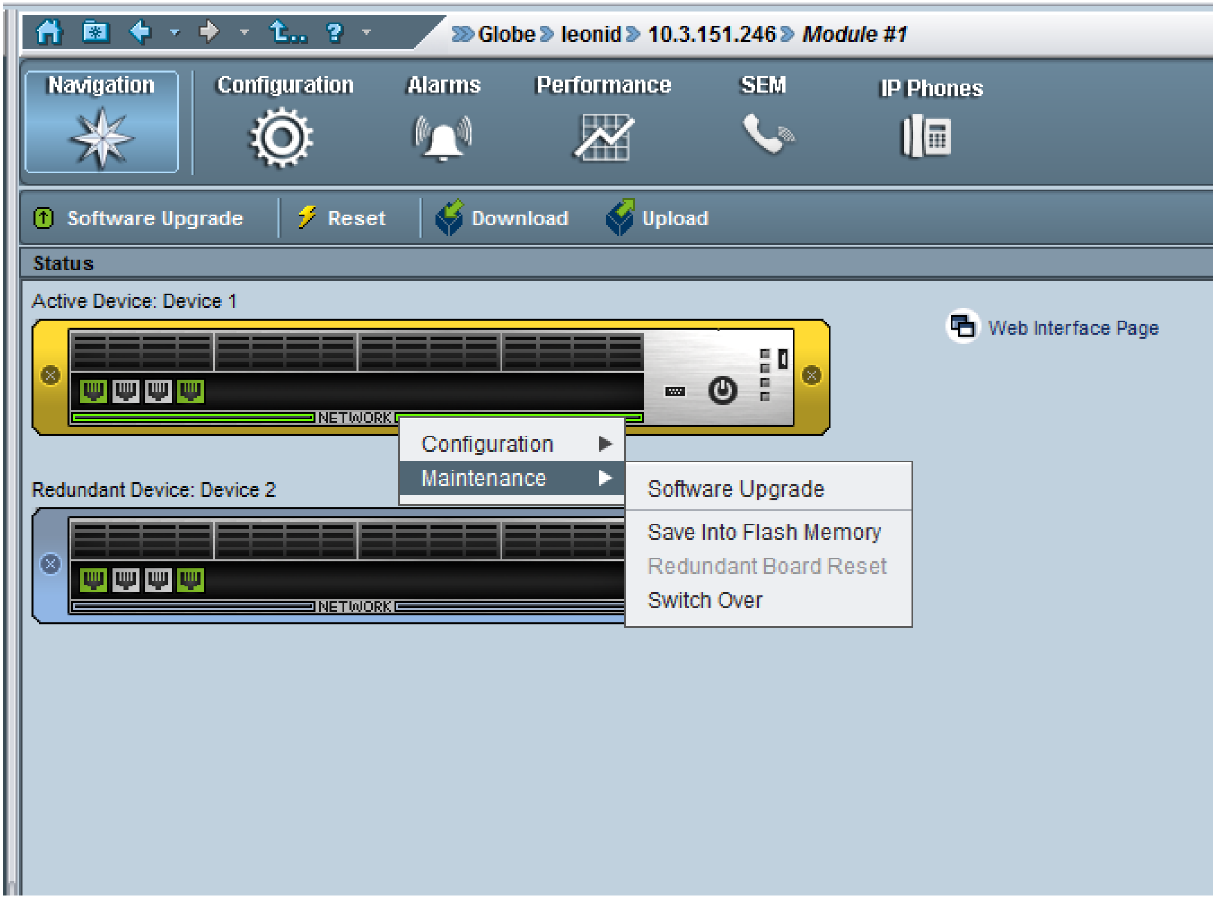
  You can download an ini file or CLI script file to a device prior to firmware download (software upgrade) to eliminate the process of validating the ini file with the device's existing configuration .

  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.

28.2 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 19-2: Maintenance Actions Menu - HA 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. This option enables you to download firmware and configuration/auxiliary files to the device. When you select this option, the Software Manager opens and you can then choose which files to upgrade to the device. If you are downloading an ini file, the following options are available:
    - 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
- **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 Configuration File:** This option enables you to upload a device ini or CLI script file for debug purposes. The configuration file received from the device is used to assist AudioCodes FAE for 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.

28.3 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.

29 Provisioning Concepts

This section describes the EMS provisioning concepts.

Note: This section is relevant for CPE devices running firmware prior to version 7.0.

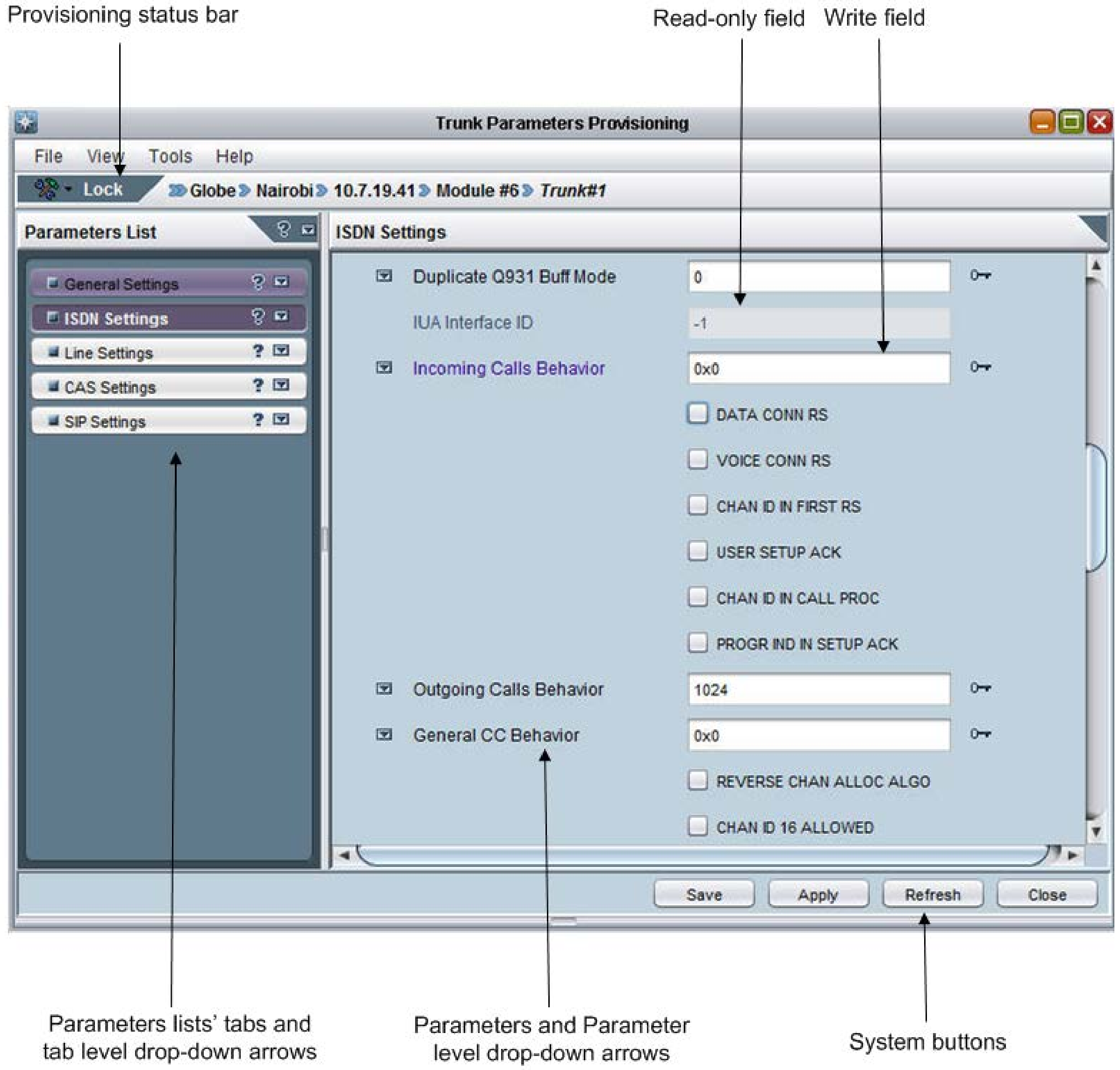
29.1 Working with the EMS's Provisioning Screens

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



Duplicate Q931 Buff Mode: 0

IUA Interface ID: -1

Incoming Calls Behavior: 0x0

□ DATA CONN RS

□ VOICE CONN RS

□ CHAN ID IN FIRST RS

□ USER SETUP ACK

□ CHAN ID IN CALL PROC

□ PROGR IND IN SETUP ACK

Outgoing Calls Behavior: 1024

General CC Behavior: 0x0

□ REVERSE CHAN ALLOC ALGO

□ CHAN ID 16 ALLOWED

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

- **Provisioning Status Bar**

  This bar includes the path of the EMS-managed entity.

  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:

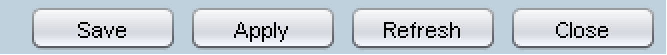
  - Undo modification/s
  - Factory default value - displays the values that the device is initiated with prior to its release.

  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:

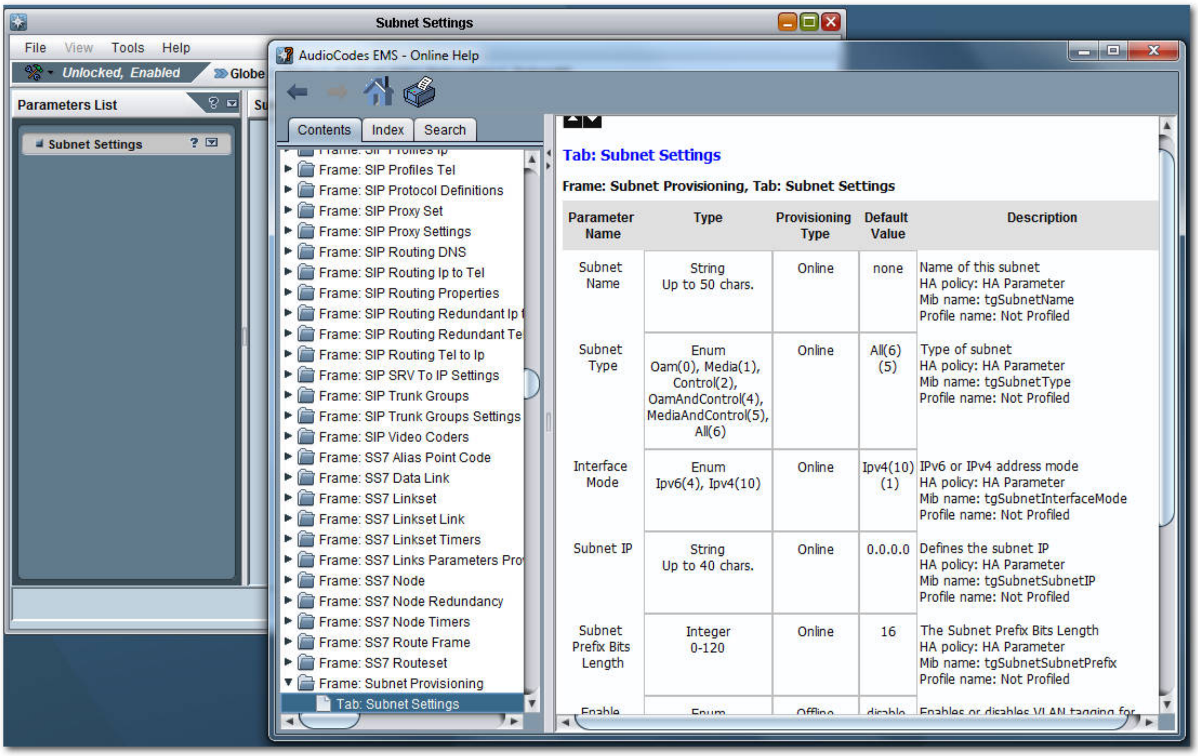
  - Right-clicking on a table row and choosing an Add / Remove / Lock / Unlock action does not then require clicking the **Apply** button; the action is executed immediately. Pressing CTRL-A enables you to select all rows in the configuration table at the same time.
  - When you finish editing a cell in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


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

Tab: Subnet Settings

Frame: Subnet Provisioning, Tab: Subnet Settings

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

29.1.1 Provisioning Procedure

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.

29.2 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

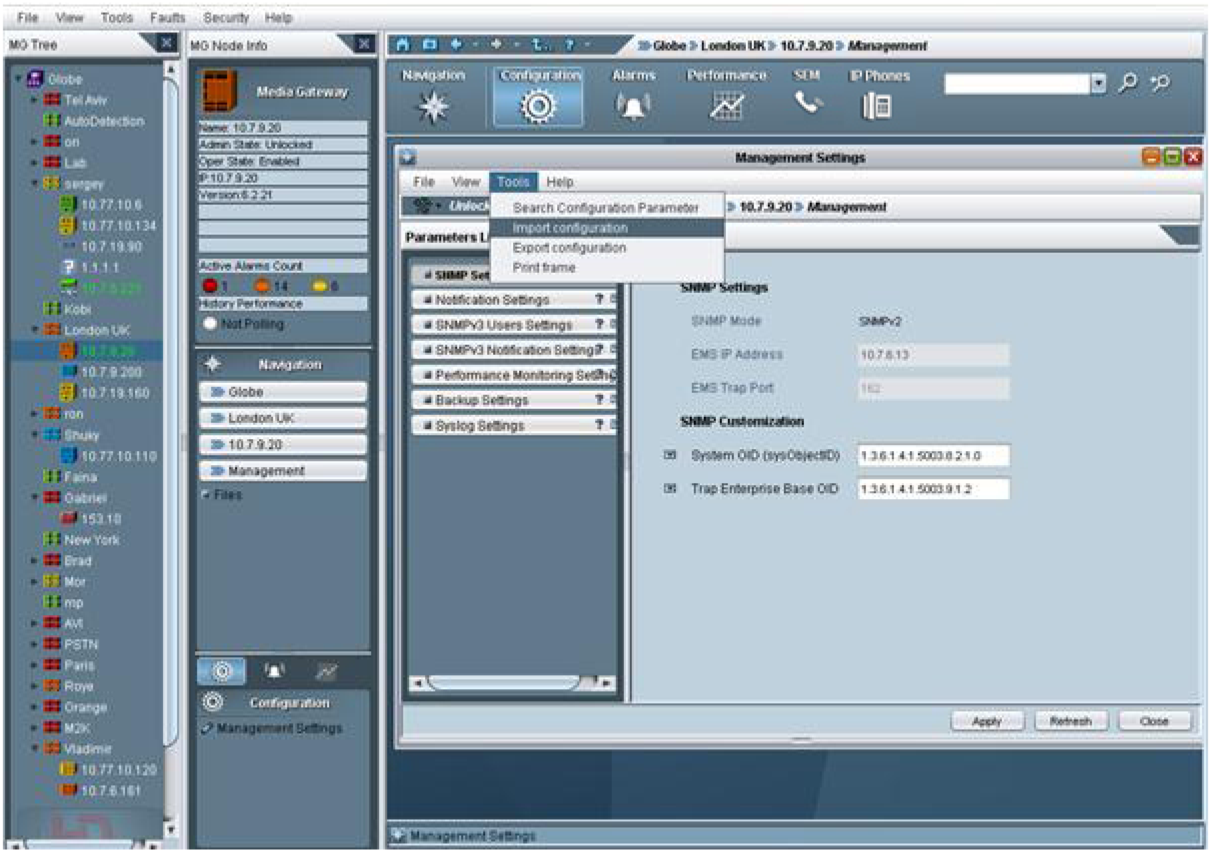
Parameter Provisioning Type	Indication / Device Type	Description
Instant	No indication	Click Apply, OK button to load changes to the device.
Online	🔑	Lock / Unlock modified entity (trunk, for example)
Offline	🔑 Trunking Gateway	Lock/Unlock the physical entity within/under which the managed entity is 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.

29.3 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



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

SNMP Settings

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

SNMP Customization

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

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

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

The entity into which the file is imported can be in another EMS system or in the same EMS system.

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

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

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

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

➢ To import the .xml file into an entity:

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

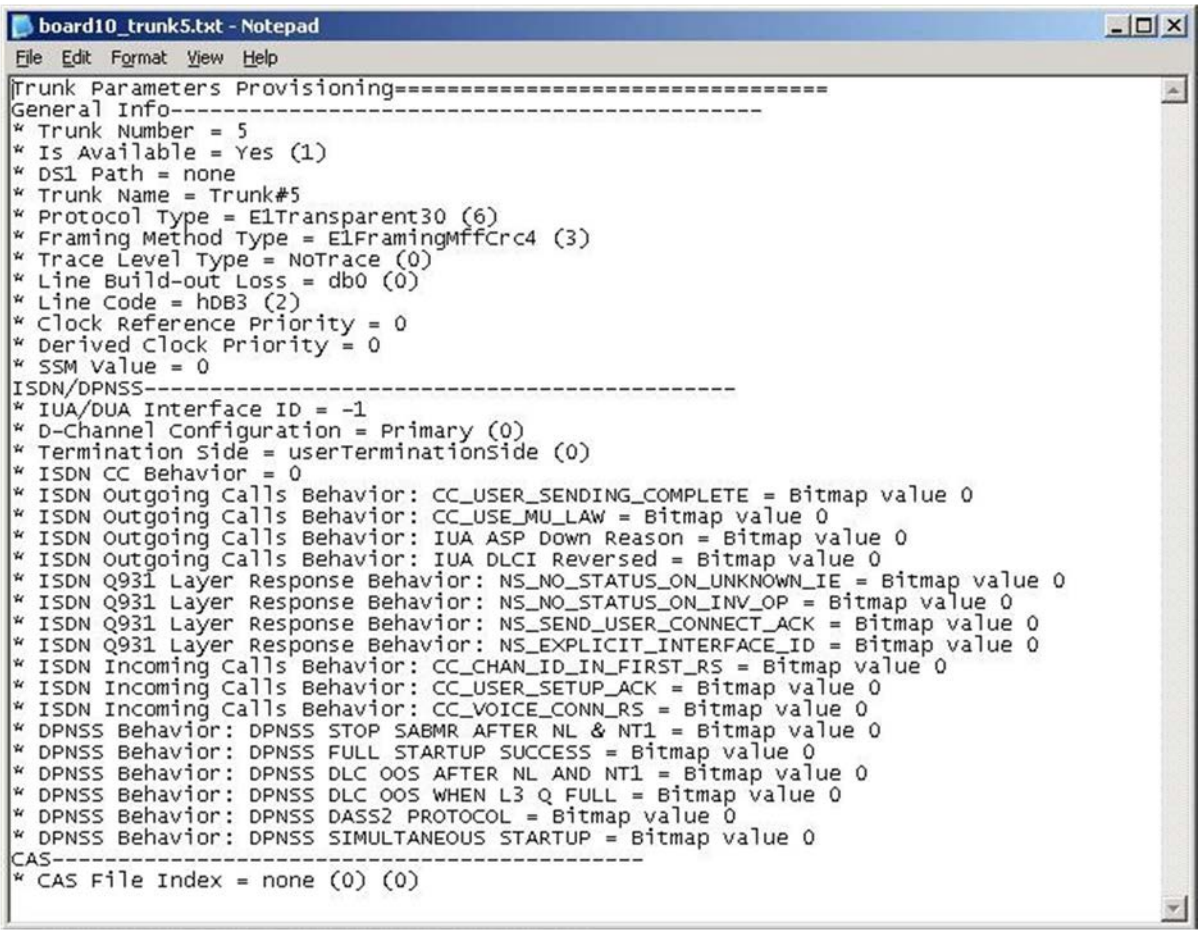
29.4 Printing an Entity's Configuration as a File

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



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

29.5 Backdoor Configuration for CPE Products

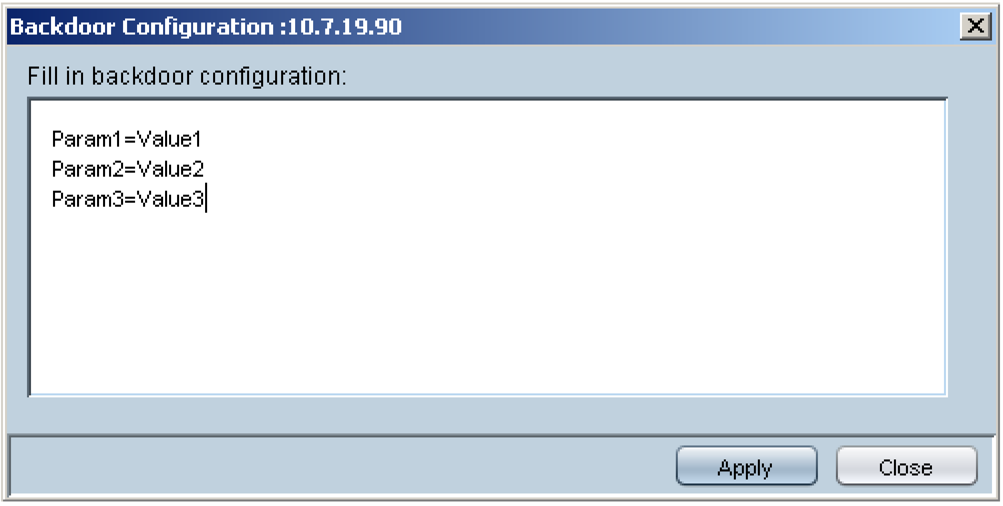
In very rare circumstances, the EMS application may not include specific provisioning parameters or tables which are supported via the device ini file provisioning. In these cases, the user should use the Backdoor Configuration screen and inform an AudioCodes FAE engineer to open a trouble ticket in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



Backdoor Configuration :10.7.19.90

Fill in backdoor configuration:

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

Note: 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.

29.6 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.

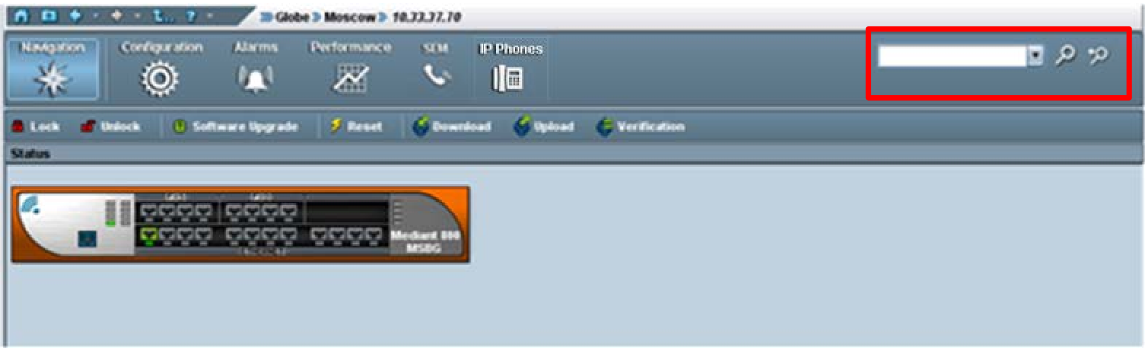
The search option is context sensitive according to the selected device. The search options are always visible in the right-hand corner of the EMS toolbar. In addition, the Advanced Search Configuration dialog can be opened from the EMS Tools menu.

> **Note:** The search option is only available for 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

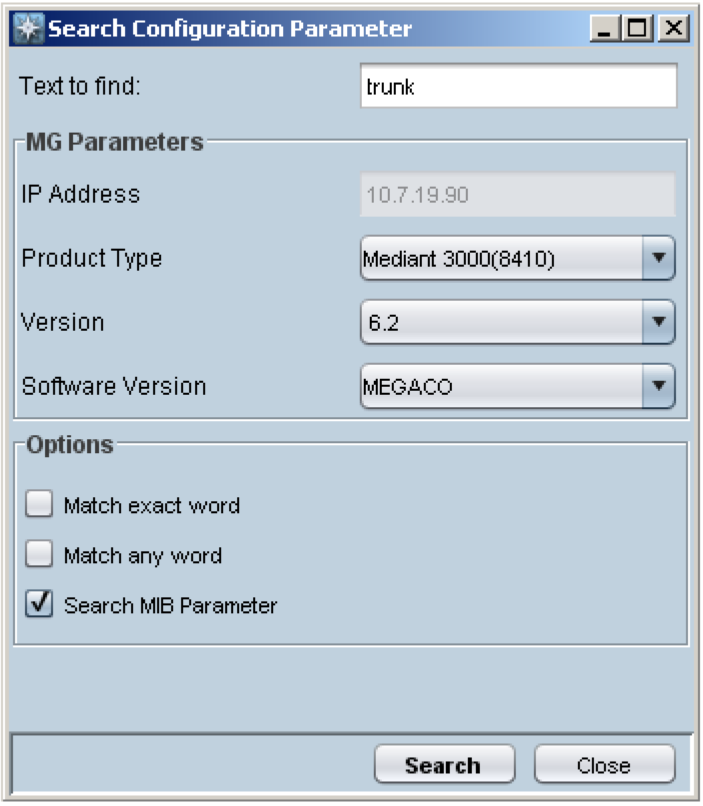


➢ To perform an Advanced Search:

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



Text to find: trunk

IP Address: 10.7.19.90

Product Type: Mediant 3000(8410)

Version: 6.2

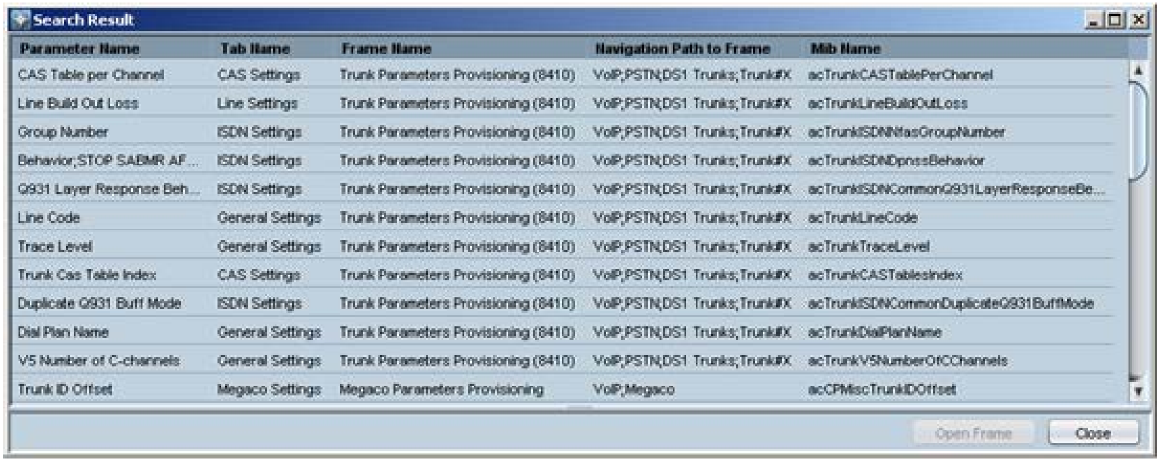
Software Version: MEGACO

□ Match exact word

□ Match any word

☑ Search MIB Parameter

Figure 20-9: Advanced Search Configuration Results Dialog



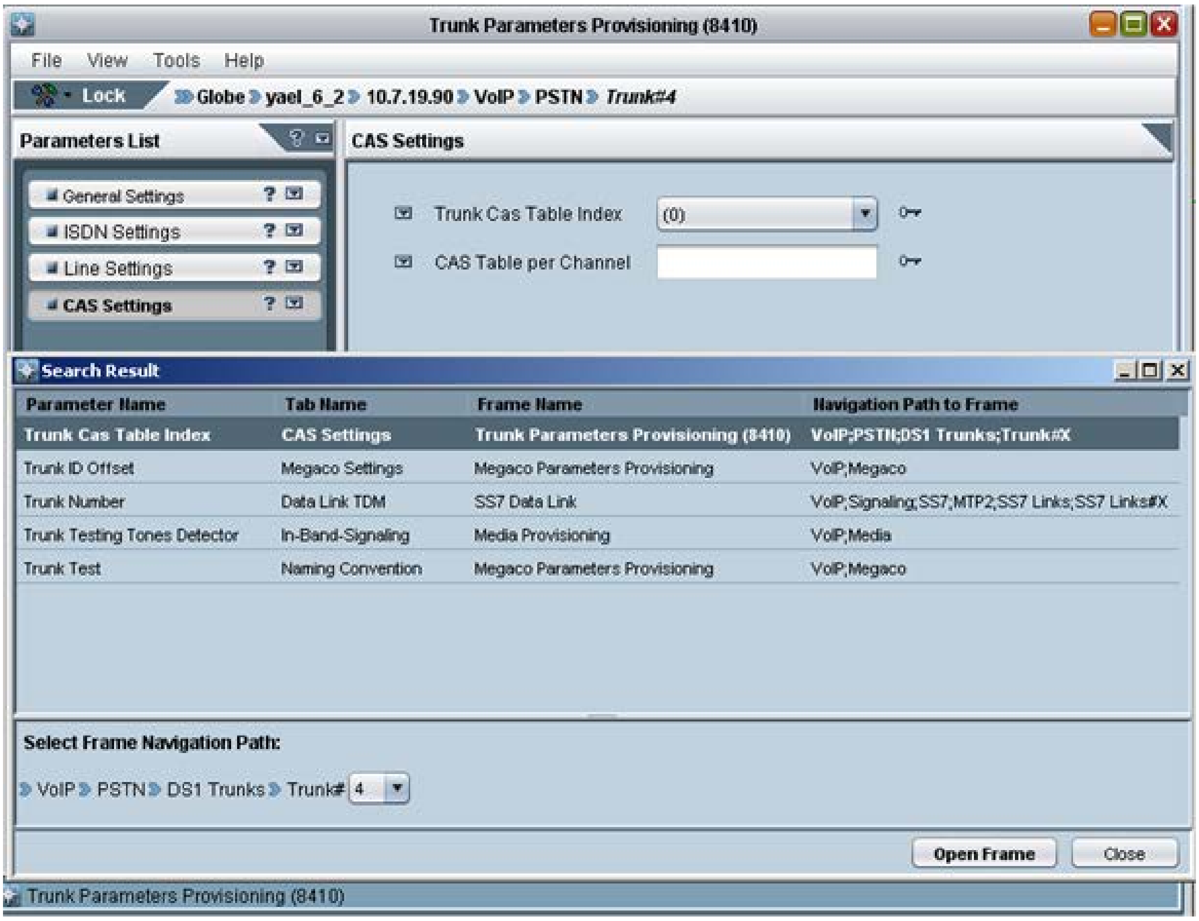
Parameter Name	Tab Name	Frame Name	Navigation Path to Frame	Mib Name
CAS Table per Channel	CAS Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkCASTablePerChannel
Line Build Out Loss	Line Settings	Trunk Parameters Provisioning (8410)	VoIP;PSTN;DS1 Trunks;Trunk#X	acTrunkLineBuildOutLoss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

29.6.1 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



Trunk Cas Table Index (0)
CAS Table per Channel

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

Select Frame Navigation Path:

VoIP › PSTN › DS1 Trunks › Trunk# 4

30 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.

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.

30.1 Software Manager

See Section 'Software Manager' on page 59.

30.2 Software Upgrade for Devices

This section describes the software upgrade for devices.

➢ **To load software to devices:**

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.
- This procedure is relevant for the device and TP boards.

The software distribution process is performed via HTTP/S. The default password received by the VoIP device at AudioCodes is used to connect the HTTP/S server. For more information on HTTPS security, see Chapter 42.

30.3 Backup Files

You can configure the EMS to automatically (daily) back up device configurations (ini, CONF or CLI script files) according to EMS server application time (device configuration is not saved to the EMS database).

These files are saved on the EMS server machine in the /data/NBIF/mgBackup/ folder. These files can be accessed and transferred using SSH, and SFTP.

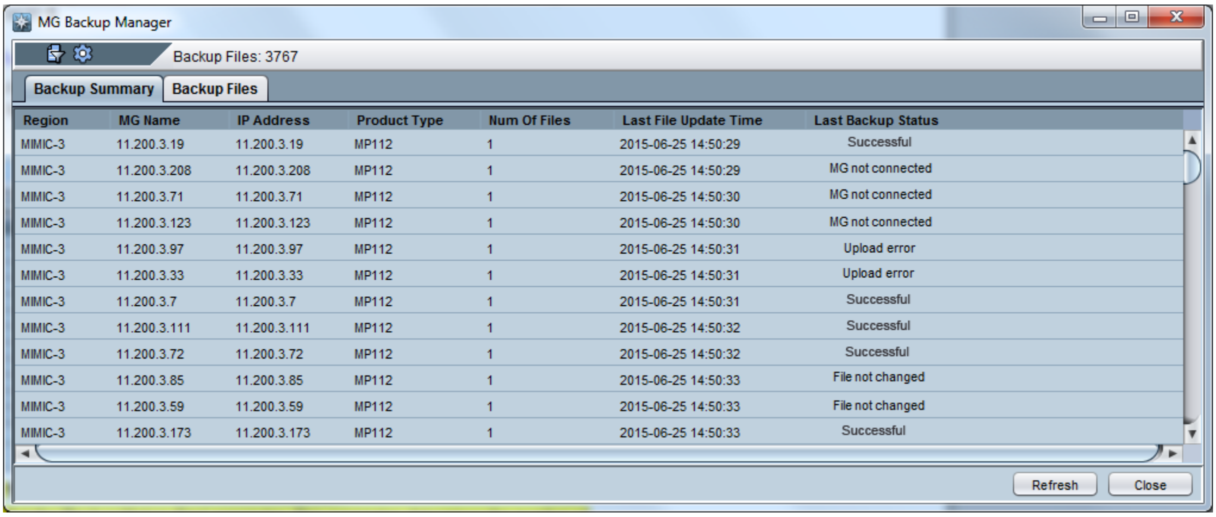
Backup files are managed by the MG Backup Manager tool. This screen displays the following:

- **Backup Summary:** displays a summary for all files that have been backed up to the EMS for each device.
- **Backup Files** tab: displays a full listing of all backup files that have been saved to the MG Backup Manager for all devices.

➢ To open the MG Backup Manager tool:

1. In the EMS Main Menu, choose **Tools** > **MG Backup Manager**; the MG Backup Manager **Summary** tab is displayed:

Figure 21-1: MG Backup Manager-Backup Summary tab



Region	MG Name	IP Address	Product Type	Num Of Files	Last File Update Time	Last Backup Status
MIMIC-3	11.200.3.19	11.200.3.19	MP112	1	2015-06-25 14:50:29	Successful
MIMIC-3	11.200.3.208	11.200.3.208	MP112	1	2015-06-25 14:50:29	MG not connected
MIMIC-3	11.200.3.71	11.200.3.71	MP112	1	2015-06-25 14:50:30	MG not connected
MIMIC-3	11.200.3.123	11.200.3.123	MP112	1	2015-06-25 14:50:30	MG not connected
MIMIC-3	11.200.3.97	11.200.3.97	MP112	1	2015-06-25 14:50:31	Upload error
MIMIC-3	11.200.3.33	11.200.3.33	MP112	1	2015-06-25 14:50:31	Upload error
MIMIC-3	11.200.3.7	11.200.3.7	MP112	1	2015-06-25 14:50:31	Successful
MIMIC-3	11.200.3.111	11.200.3.111	MP112	1	2015-06-25 14:50:32	Successful
MIMIC-3	11.200.3.72	11.200.3.72	MP112	1	2015-06-25 14:50:32	Successful
MIMIC-3	11.200.3.85	11.200.3.85	MP112	1	2015-06-25 14:50:33	File not changed
MIMIC-3	11.200.3.59	11.200.3.59	MP112	1	2015-06-25 14:50:33	File not changed
MIMIC-3	11.200.3.173	11.200.3.173	MP112	1	2015-06-25 14:50:33	Successful

Each entry in the summary displays the following information:

- The Region and Product Type of the device
- The device name, IP address and product type
- The number of files that have been backed up from the device to the EMS.
- The date of the last backup file.
- The last backup status e.g. Successful.

In the Tool bar, you can configure the Backup Settings and filter the files that are displayed.

In the Information pane, the total number of backup files displayed in the MG Backup Manager is indicated along with the total number of files that have been saved to the EMS database. In this example, 5000 files is the maximum number of files that can be displayed in the MG Backup Manager out of a total number of 56335 files that have been backed up from devices.

2. To view detailed information of the latest file backed up from the device, right-click an entry and choose **Show Files**.
3. To upload the latest configuration file from the device, right-click an entry and choose **Upload INI/CONF** or **Upload CLI**.
4. To restore or download the latest backup file to the device, right-click an entry and choose **download latest INI/CONF** or **download latest CLI**.

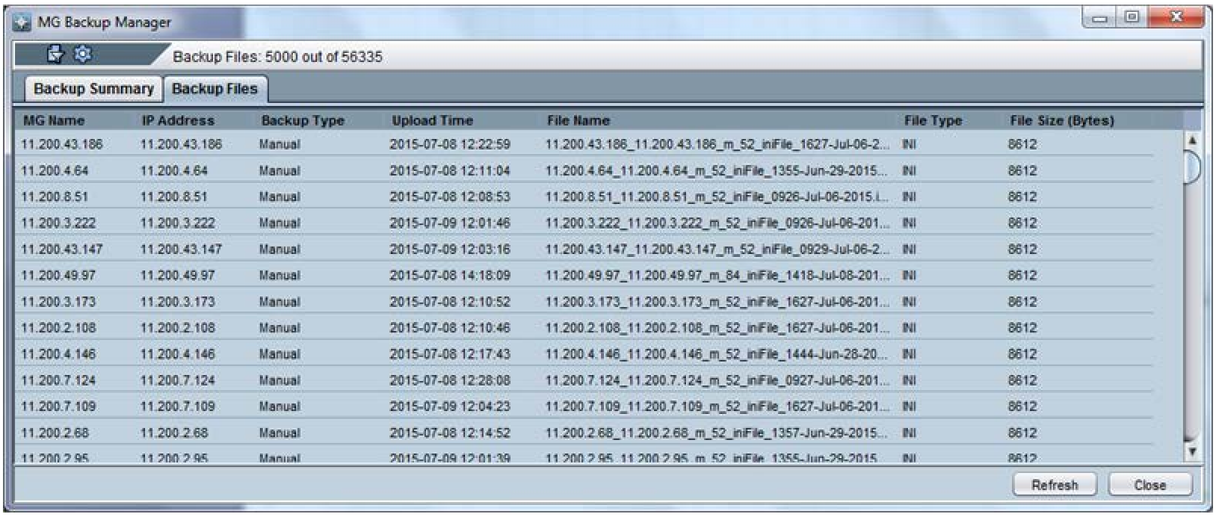
30.3.1 Viewing Backup Files

In the Information pane, the total number of backup files displayed in the MG Backup Manager is indicated along with the total number of files that have been saved to the EMS database. In this example, 5000 files is the maximum number of files that can be displayed in the MG Backup Manager out of a total number of 56335 files that have been backed up from devices.

➢ To view a full listing of all backup files:

1. In the MG Backup Policy screen; select the **Backup Files** tab. This tab displays a full listing of all files that have been backed up to the device *ini* and *CLI script (*MSBR devices files) for CPE devices.

Figure 21-2: Backup Files



Backup Files: 5000 out of 56335

MG Name	IP Address	Backup Type	Upload Time	File Name	File Type	File Size (Bytes)
11.200.43.186	11.200.43.186	Manual	2015-07-08 12:22:59	11.200.43.186_11.200.43.186_m_52_iniFile_1627-Jul-06-2...	INI	8612
11.200.4.64	11.200.4.64	Manual	2015-07-08 12:11:04	11.200.4.64_11.200.4.64_m_52_iniFile_1355-Jun-29-2015...	INI	8612
11.200.8.51	11.200.8.51	Manual	2015-07-08 12:08:53	11.200.8.51_11.200.8.51_m_52_iniFile_0926-Jul-06-2015.i...	INI	8612
11.200.3.222	11.200.3.222	Manual	2015-07-09 12:01:46	11.200.3.222_11.200.3.222_m_52_iniFile_0926-Jul-06-201...	INI	8612
11.200.43.147	11.200.43.147	Manual	2015-07-09 12:03:16	11.200.43.147_11.200.43.147_m_52_iniFile_0929-Jul-06-2...	INI	8612
11.200.49.97	11.200.49.97	Manual	2015-07-08 14:18:09	11.200.49.97_11.200.49.97_m_84_iniFile_1418-Jul-08-201...	INI	8612
11.200.3.173	11.200.3.173	Manual	2015-07-08 12:10:52	11.200.3.173_11.200.3.173_m_52_iniFile_1627-Jul-06-201...	INI	8612
11.200.2.108	11.200.2.108	Manual	2015-07-08 12:10:46	11.200.2.108_11.200.2.108_m_52_iniFile_1627-Jul-06-201...	INI	8612
11.200.4.146	11.200.4.146	Manual	2015-07-08 12:17:43	11.200.4.146_11.200.4.146_m_52_iniFile_1444-Jun-28-20...	INI	8612
11.200.7.124	11.200.7.124	Manual	2015-07-08 12:28:08	11.200.7.124_11.200.7.124_m_52_iniFile_0927-Jul-06-201...	INI	8612
11.200.7.109	11.200.7.109	Manual	2015-07-09 12:04:23	11.200.7.109_11.200.7.109_m_52_iniFile_1627-Jul-06-201...	INI	8612
11.200.2.68	11.200.2.68	Manual	2015-07-08 12:14:52	11.200.2.68_11.200.2.68_m_52_iniFile_1357-Jun-29-2015...	INI	8612
11.200.2.95	11.200.2.95	Manual	2015-07-09 12:01:39	11.200.2.95_11.200.2.95_m_52_iniFile_1355-Jun-29-2015	INI	8612

2. To upload an ini or CLI script file to your PC, select the file, right-click, and then choose **Save As**.
3. To delete the selected ini or CLI script file/s, select the file/s, right-click and then choose **Delete File(s)**.
4. To download the configuration file to the device, right-click and then choose **Download**.

30.3.2 Enabling Backup of Device Configuration Files

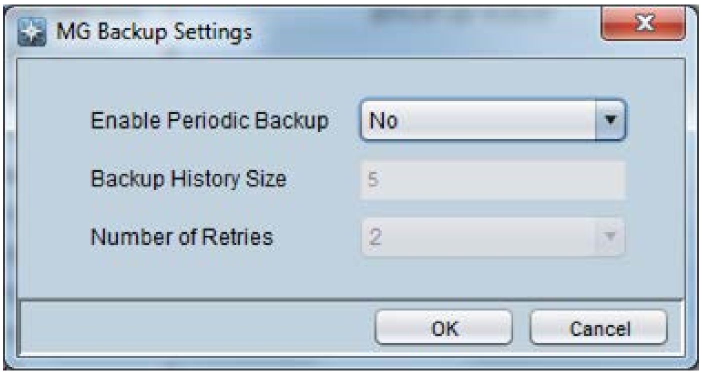
This section describes how to enable the EMS to backup device configuration files, set how many backup files you wish to store and how many retries for each connection attempt with the device.

When this feature is enabled all device configuration files (INI, CONF and CLI) are backed up to the MG Backup Manager from all managed devices on a daily basis.

➢ To configure the EMS backup file settings:

1. In the MG Backup Manager Tool bar, click the Settings icon ⚙ ; the **MG Backup Settings window** is displayed:

Figure 21-3: Backup Settings



MG Backup Settings

Enable Periodic Backup: No

Backup History Size: 5

Number of Retries: 2

2. Enable or disable Periodic Backup collection.
   - When enabled, backup is performed daily
   - When disabled, you can perform manual backup immediately after configuration changes (by performing one of the right-click actions from the Backup Summary view as described above).
3. 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.
4. Define the number of retries that must be made on each connection to the device. Default-2.

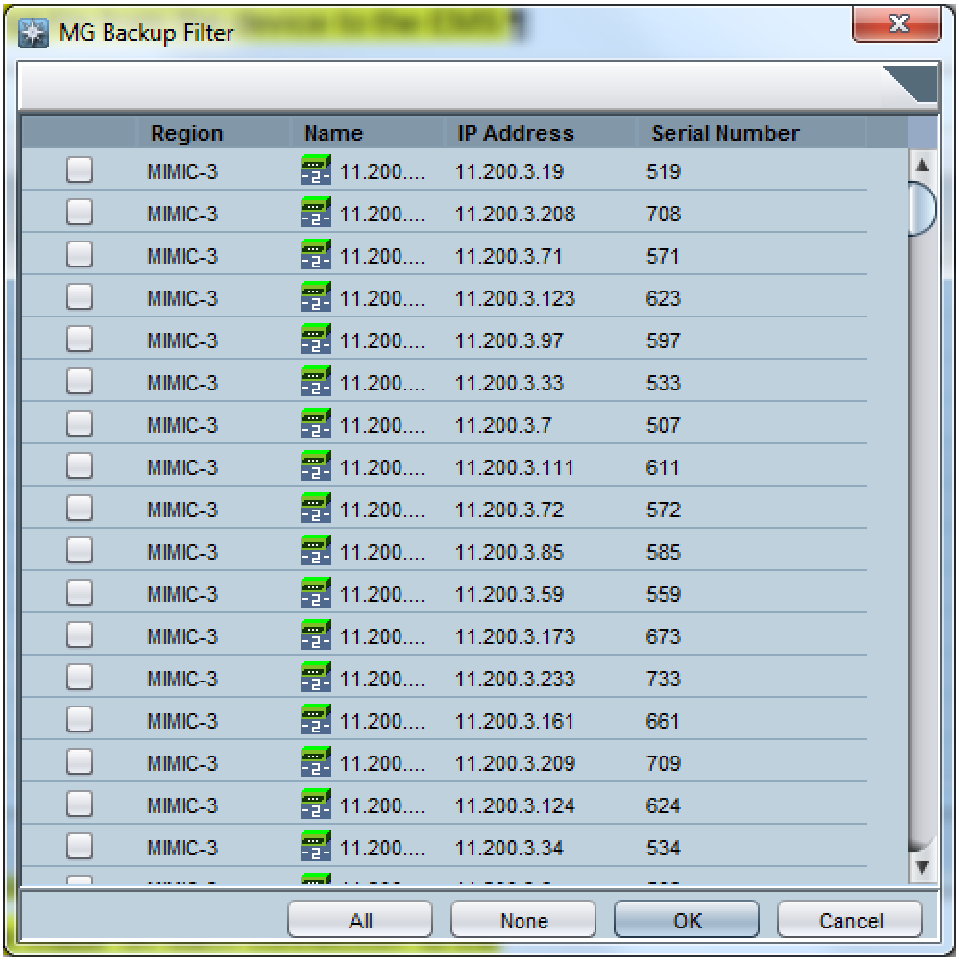
30.3.3 Filtering the Backup Data Display

You can filter which devices you wish to display in the MG Backup Manager. Once you select the filter criteria, the Backup Summary and the Backup Files tab displays backup data for these selected devices.

➢ To filter the files displayed in the Backup Files tab:

1. In the MG Backup Manager Toolbar, select the icon ; the MG Backup Filter is displayed:

Figure 21-4: MG Backup Filter



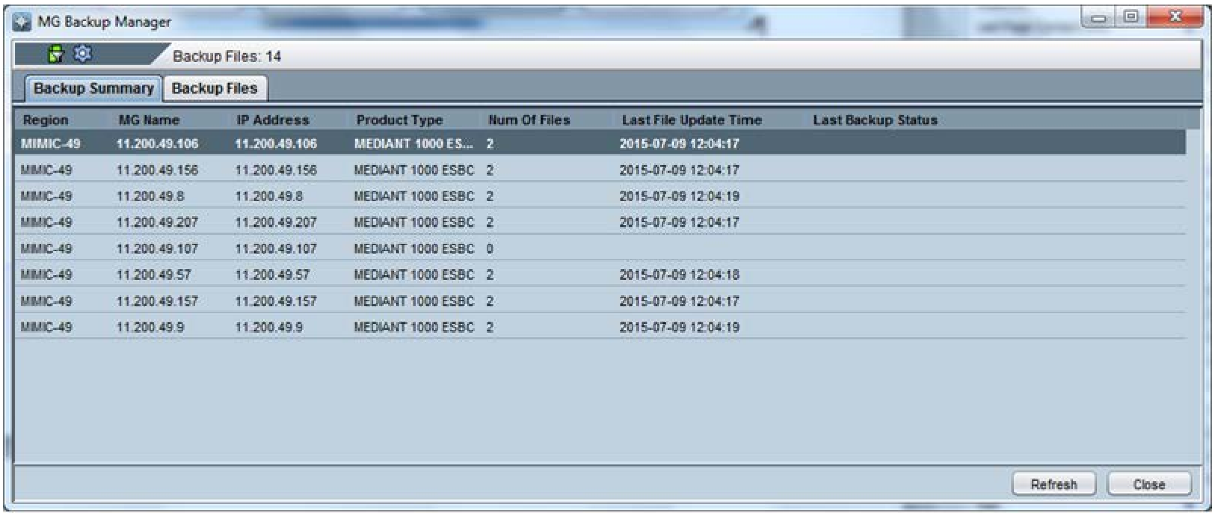
	Region	Name	IP Address	Serial Number
☐	MIMIC-3	11.200....	11.200.3.19	519
☐	MIMIC-3	11.200....	11.200.3.208	708
☐	MIMIC-3	11.200....	11.200.3.71	571
☐	MIMIC-3	11.200....	11.200.3.123	623
☐	MIMIC-3	11.200....	11.200.3.97	597
☐	MIMIC-3	11.200....	11.200.3.33	533
☐	MIMIC-3	11.200....	11.200.3.7	507
☐	MIMIC-3	11.200....	11.200.3.111	611
☐	MIMIC-3	11.200....	11.200.3.72	572
☐	MIMIC-3	11.200....	11.200.3.85	585
☐	MIMIC-3	11.200....	11.200.3.59	559
☐	MIMIC-3	11.200....	11.200.3.173	673
☐	MIMIC-3	11.200....	11.200.3.233	733
☐	MIMIC-3	11.200....	11.200.3.161	661
☐	MIMIC-3	11.200....	11.200.3.209	709
☐	MIMIC-3	11.200....	11.200.3.124	624
☐	MIMIC-3	11.200....	11.200.3.34	534

2. Select the checkboxes adjacent to those devices that you wish to filter to view.

   After you set the required criteria, in the **Backup Summary** tab, a summary of files that have been backed up for the selected devices is displayed. In the **Backup Files** tab, a full listing of all files that have been backed up to the EMS for the selected devices is displayed.

   In the example below, the **Summary** tab shows that eight devices have been selected using the MG Backup Filter and a total of 14 files have been backed up to the EMS from these devices.

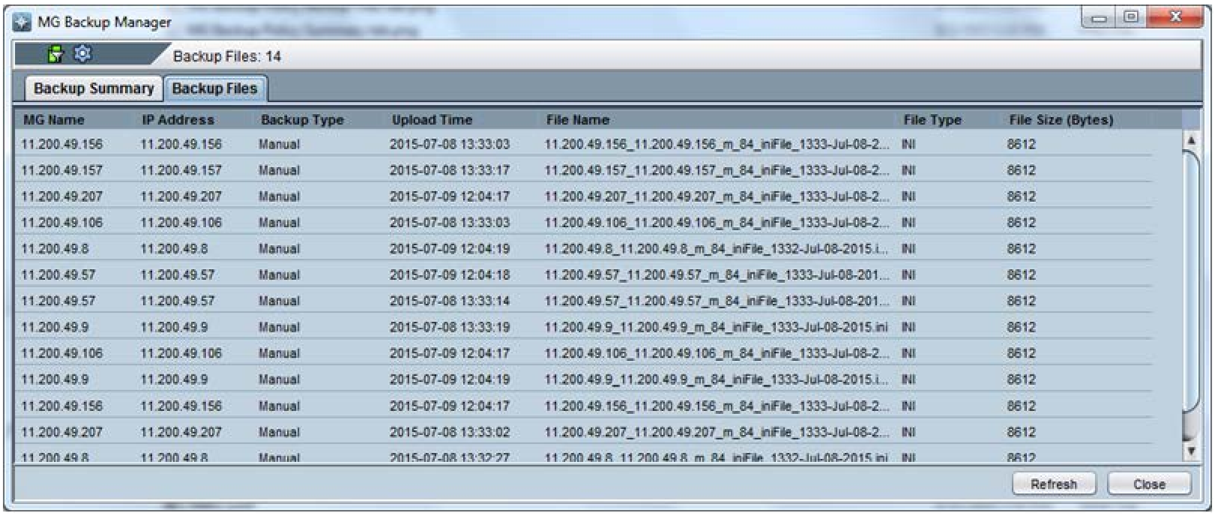
Figure 21-5: Backup Summary with Filter Settings



Region	MG Name	IP Address	Product Type	Num Of Files	Last File Update Time	Last Backup Status
MIMIC-49	11.200.49.106	11.200.49.106	MEDIANT 1000 ES...	2	2015-07-09 12:04:17	
MIMIC-49	11.200.49.156	11.200.49.156	MEDIANT 1000 ESBC	2	2015-07-09 12:04:17	
MIMIC-49	11.200.49.8	11.200.49.8	MEDIANT 1000 ESBC	2	2015-07-09 12:04:19	
MIMIC-49	11.200.49.207	11.200.49.207	MEDIANT 1000 ESBC	2	2015-07-09 12:04:17	
MIMIC-49	11.200.49.107	11.200.49.107	MEDIANT 1000 ESBC	0		
MIMIC-49	11.200.49.57	11.200.49.57	MEDIANT 1000 ESBC	2	2015-07-09 12:04:18	
MIMIC-49	11.200.49.157	11.200.49.157	MEDIANT 1000 ESBC	2	2015-07-09 12:04:17	
MIMIC-49	11.200.49.9	11.200.49.9	MEDIANT 1000 ESBC	2	2015-07-09 12:04:19	

The figure below lists the details of each of the 14 files that have been backed up to the EMS for these eight devices.

Figure 21-6: Backup Files with Filter Settings



MG Name	IP Address	Backup Type	Upload Time	File Name	File Type	File Size (Bytes)
11.200.49.156	11.200.49.156	Manual	2015-07-08 13:33:03	11.200.49.156_11.200.49.156_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.157	11.200.49.157	Manual	2015-07-08 13:33:17	11.200.49.157_11.200.49.157_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.207	11.200.49.207	Manual	2015-07-09 12:04:17	11.200.49.207_11.200.49.207_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.106	11.200.49.106	Manual	2015-07-08 13:33:03	11.200.49.106_11.200.49.106_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.8	11.200.49.8	Manual	2015-07-09 12:04:19	11.200.49.8_11.200.49.8_m_84_iniFile_1332-Jul-08-2015.i...	INI	8612
11.200.49.57	11.200.49.57	Manual	2015-07-09 12:04:18	11.200.49.57_11.200.49.57_m_84_iniFile_1333-Jul-08-201...	INI	8612
11.200.49.57	11.200.49.57	Manual	2015-07-08 13:33:14	11.200.49.57_11.200.49.57_m_84_iniFile_1333-Jul-08-201...	INI	8612
11.200.49.9	11.200.49.9	Manual	2015-07-08 13:33:19	11.200.49.9_11.200.49.9_m_84_iniFile_1333-Jul-08-2015.ini	INI	8612
11.200.49.106	11.200.49.106	Manual	2015-07-09 12:04:17	11.200.49.106_11.200.49.106_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.9	11.200.49.9	Manual	2015-07-09 12:04:19	11.200.49.9_11.200.49.9_m_84_iniFile_1333-Jul-08-2015.i...	INI	8612
11.200.49.156	11.200.49.156	Manual	2015-07-09 12:04:17	11.200.49.156_11.200.49.156_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.207	11.200.49.207	Manual	2015-07-08 13:33:02	11.200.49.207_11.200.49.207_m_84_iniFile_1333-Jul-08-2...	INI	8612
11.200.49.8	11.200.49.8	Manual	2015-07-08 13:32:27	11.200.49.8_11.200.49.8_m_84_iniFile_1332-Jul-08-2015.ini	INI	8612

Part IV

Fault and Performance Management

This section describes fault and performance management.

31 Introduction

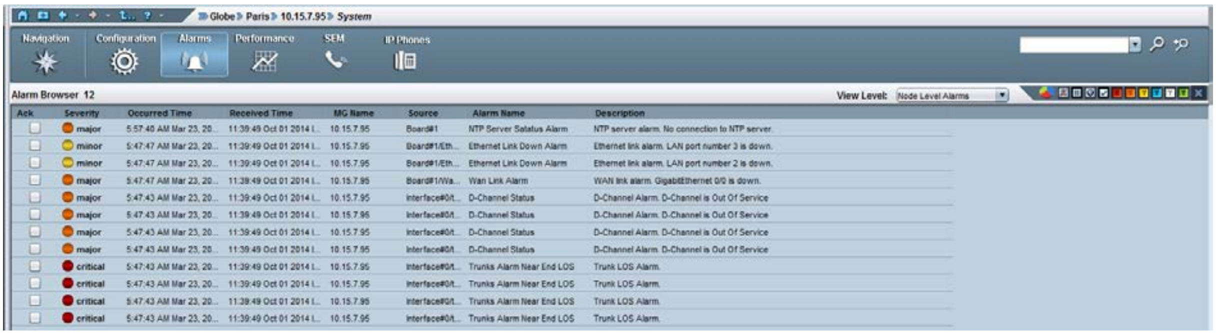
After service is provisioned for a subscriber under a given QoS level, the service provider must ensure that the purchased level of service is delivered. In the domain of the EMS, this process involves high-level fault and performance management of the managed entities. This section describes the fault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



Alarm Browser 12

View Level: Node Level Alarms

Ack	Severity	Occurred Time	Received Time	MG Name	Source	Alarm Name	Description
□	● major	5:57:40 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Board#1	NTP Server Salatus Alarm	NTP server alarm. No connection to NTP server.
□	● minor	5:47:47 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.
□	● minor	5:47:47 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.
□	● major	5:47:47 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Board#1/Wa...	Wan Link Alarm	WAN link alarm. GigabitEthernet 0/0 is down.
□	● major	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	D-Channel Status	D-Channel Alarm. D-Channel is Out Of Service
□	● major	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	D-Channel Status	D-Channel Alarm. D-Channel is Out Of Service
□	● major	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	D-Channel Status	D-Channel Alarm. D-Channel is Out Of Service
□	● major	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	D-Channel Status	D-Channel Alarm. D-Channel is Out Of Service
□	● critical	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	5:47:43 AM Mar 23, 20...	11:39:49 Oct 01 2014 I...	10.15.7.95	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.

This page is intentionally left blank.

32 Alarm Browser

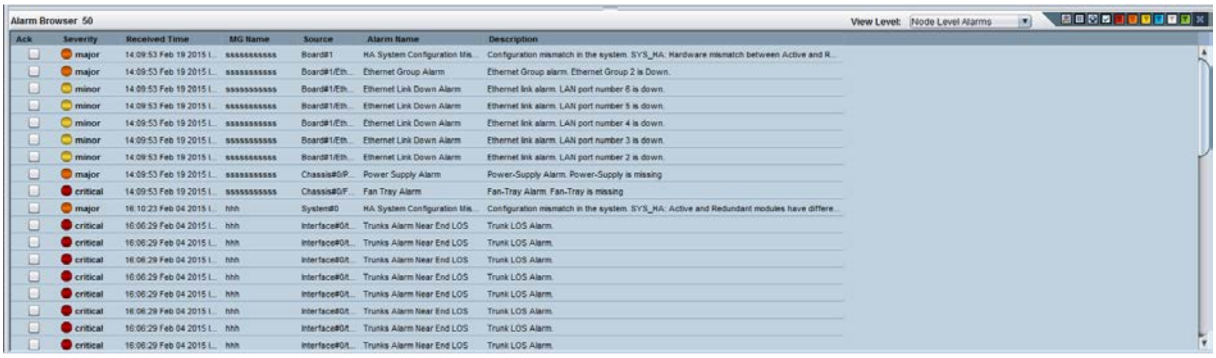
The EMS's fault management functionality manages and displays all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system.

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



Alarm Browser 50

View Level: Node Level Alarms

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
☐	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1	HA System Configuration Mis...	Configuration mismatch in the system. SYS_HA: Hardware mismatch between Active and R...
☐	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 2 is Down.
☐	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 6 is down.
☐	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 5 is down.
☐	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.
☐	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.
☐	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.
☐	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Chassis#0/P...	Power Supply Alarm	Power-Supply Alarm. Power-Supply is missing
☐	● critical	14:09:53 Feb 19 2015 I...	sssssssssss	Chassis#0/F...	Fan Tray Alarm	Fan-Tray Alarm. Fan-Tray is missing
☐	● major	16:10:23 Feb 04 2015 I...	hhh	System#0	HA System Configuration Mis...	Configuration mismatch in the system. SYS_HA: Active and Redundant modules have differe...
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
☐	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.

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 Nam**e (short description of the alarm)
- **Events** are indicated by the label [Event] which makes it easy for the user to sort between alarms and events.
- **Description** (elaborated alarm details)

Notes:

- By default, alarms are listed in the Alarm Browser in chronological order. The most recently received alarms appear at the **top** of the list, with the oldest alarms at the **bottom**.
- 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.

32.1 Filtering Alarms

The Alarm Browser lists all the currently active alarms in the EMS for a context selected in the Navigation module. When selecting the root (Globe) of the managed 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.
- **Device** - all the alarms of the device and it's hardware modules
- **TP Board and its subcomponents** (Trunk, SS7, MTP2), SAT, 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 275.
📝	Opens the Actions Journal. For more information, see Section Viewing Operator Actions in the Actions Journal on page 357.
🔇	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.
e	Filters the active Alarm Browser window by only displaying alarms (events are not displayed)
✓	Filters the active Alarm Browser window by displaying only Unacknowledged Alarms (acknowledged alarms are not displayed)
🟥	Filters the active Alarm Browser window by displaying Critical Alarms.
🟧	Filters the active Alarm Browser window by displaying Major Alarms.
🟨	Filters the active Alarm Browser window by displaying Minor Alarms.
🟦	Filters the active Alarm Browser window by displaying Warning Alarms
⬜	Filters the active Alarm Browser window by displaying Info Alarms.

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.

32.2 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.

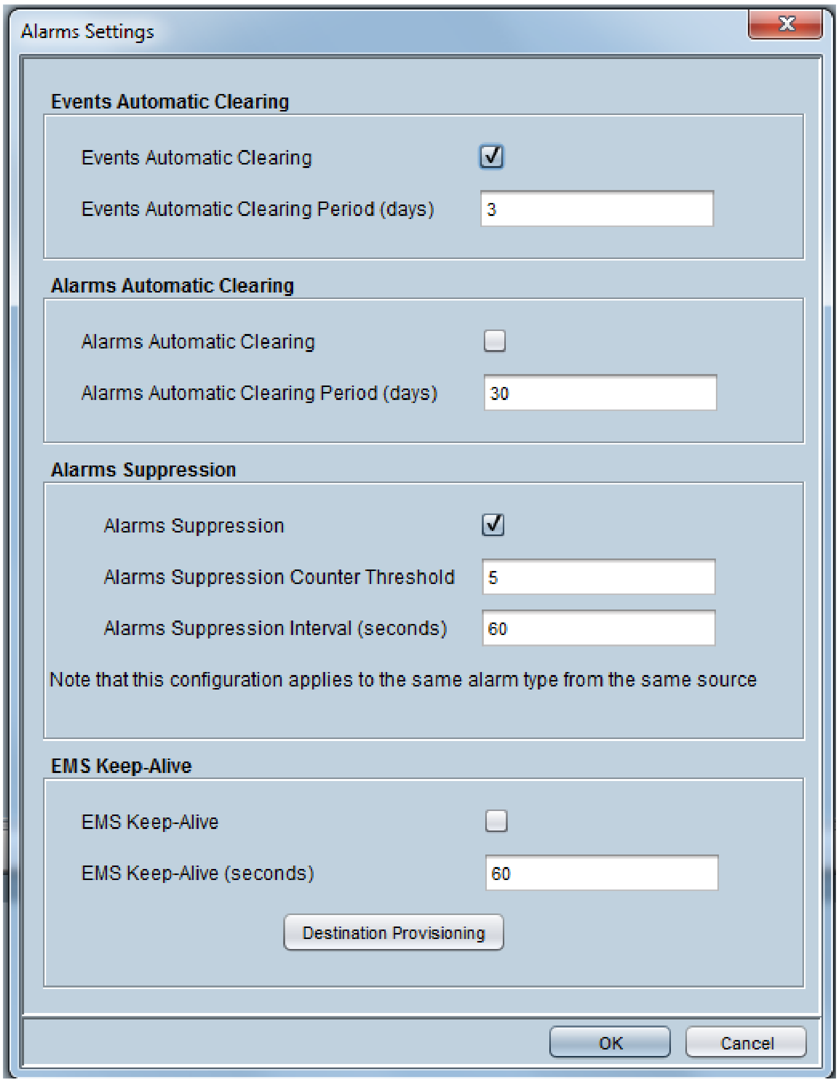
32.3 Alarm and Event Management

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



Alarms Settings

Events Automatic Clearing

Events Automatic Clearing ☑

Events Automatic Clearing Period (days) 3

Alarms Automatic Clearing

Alarms Automatic Clearing □

Alarms Automatic Clearing Period (days) 30

Alarms Suppression

Alarms Suppression ☑

Alarms Suppression Counter Threshold 5

Alarms Suppression Interval (seconds) 60

Note that this configuration applies to the same alarm type from the same source

EMS Keep-Alive

EMS Keep-Alive □

EMS Keep-Alive (seconds) 60

This screen provides the following configuration options:

- Automatic Alarms Clearing
- Automatic Events Clearing**Error! Reference source not found.**
- Alarm Suppression Mechanism
- HA Alarms Forwarding

32.3.1 Automatic Alarms Clearing

The Alarm Browser for each device is cleared of all the current alarms 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 the same device. This feature prevents irrelevant alarms from congesting the Alarms Browser. Operators only view the list of the currently active alarms.

In addition, the operator can also configure the automatic clearing of alarms from the Alarms Browser (disabled by default). When the Automatic Clearing feature is enabled, alarms are cleared by default every 30 days.

When the EMS application performs automatic clearing, it moves the cleared Alarms to the Alarm History view with the text indication 'Automatic Cleared'.

32.3.2 Automatic Events Clearing

Events are informative messages for EMS and device actions (usually with low severity). Device events (originating from the device) are automatically cleared from the device’s Alarm Browser upon GW startup (cold start event); however, device events originating in the EMS (e.g. adding a gateway) are not cleared upon device reset. As a consequence, the EMS employs a mechanism to automatically clear these events from the Alarm Browser (by default this feature is enabled and events are cleared every three days). This feature prevents irrelevant events from congesting the Alarms Browser.

When automatic clearing is performed, the cleared Events are moved to the Alarm History view with the text indication 'Automatic Cleared'.

32.3.3 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 291).

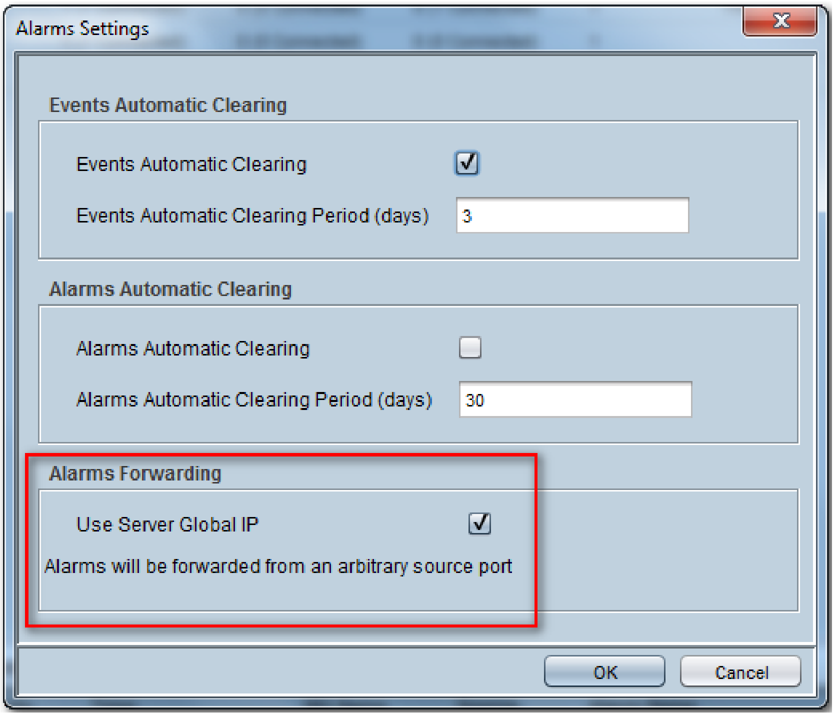
32.3.4 HA Alarms Forwarding

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



Alarms Settings

Events Automatic Clearing

Events Automatic Clearing ☑

Events Automatic Clearing Period (days) 3

Alarms Automatic Clearing

Alarms Automatic Clearing □

Alarms Automatic Clearing Period (days) 30

Alarms Forwarding

Use Server Global IP ☑

Alarms will be forwarded from an arbitrary source port

32.3.5 EMS Keep-alive

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

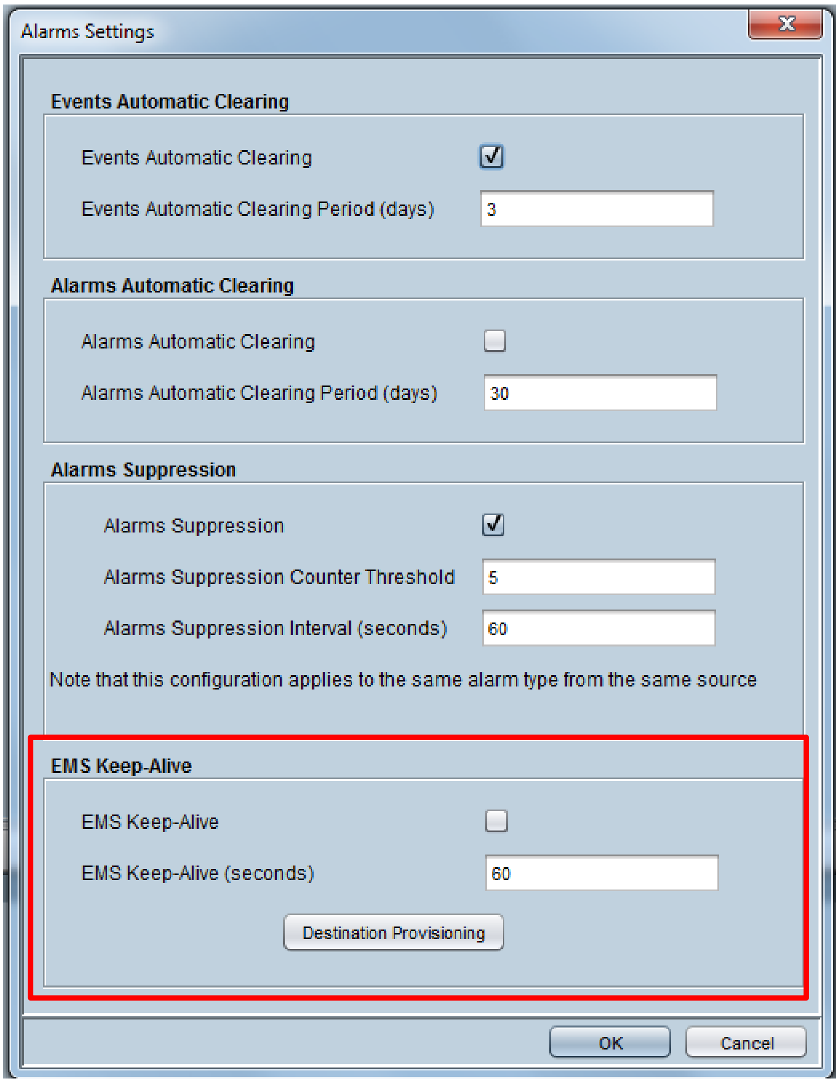
When the “EMS Keep-Alive” check box is checked, this trap is sent from the EMS to a configured destination according to a configured interval (default 60 seconds).

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



Alarms Settings

Events Automatic Clearing

Events Automatic Clearing ☑

Events Automatic Clearing Period (days) 3

Alarms Automatic Clearing

Alarms Automatic Clearing ☐

Alarms Automatic Clearing Period (days) 30

Alarms Suppression

Alarms Suppression ☑

Alarms Suppression Counter Threshold 5

Alarms Suppression Interval (seconds) 60

Note that this configuration applies to the same alarm type from the same source

EMS Keep-Alive

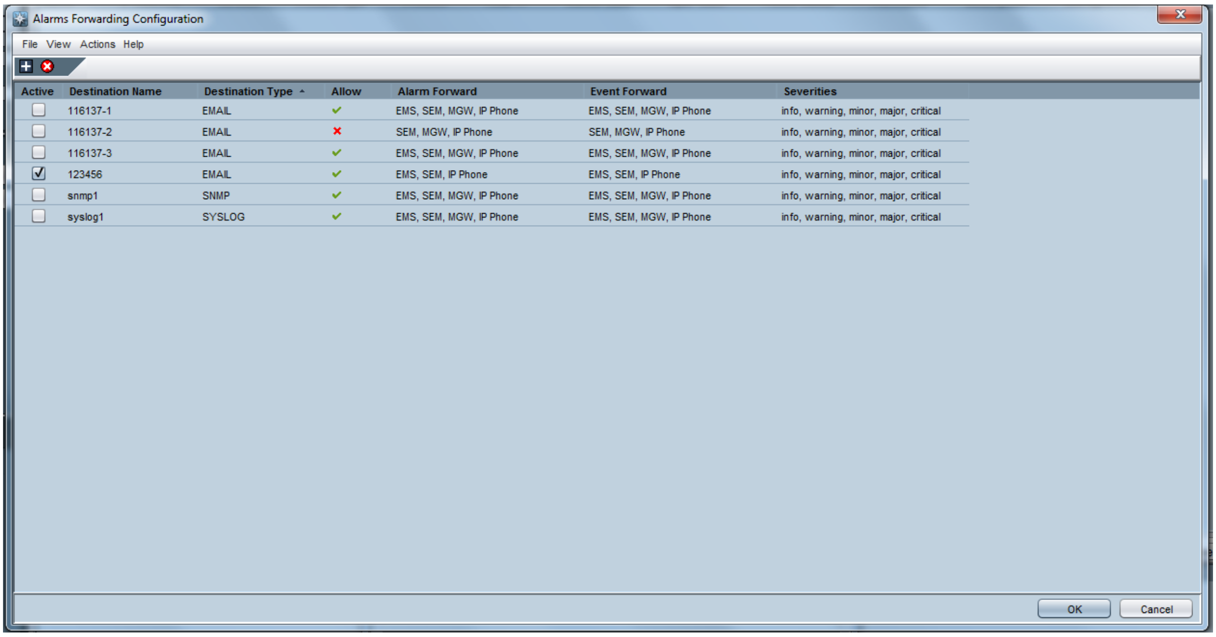
EMS Keep-Alive ☐

EMS Keep-Alive (seconds) 60

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

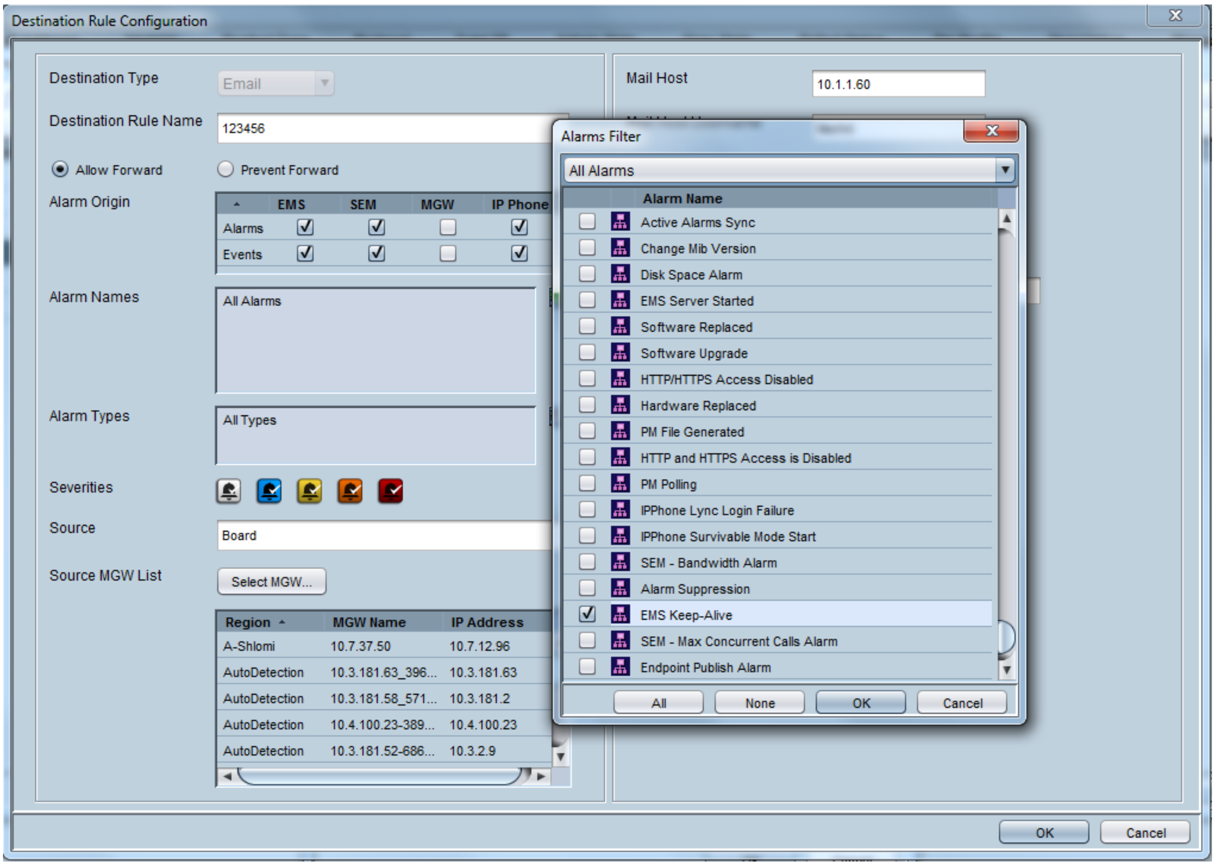


Active	Destination Name	Destination Type	Allow	Alarm Forward	Event Forward	Severities
□	116137-1	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	116137-2	EMAIL	✗	SEM, MGW, IP Phone	SEM, MGW, IP Phone	info, warning, minor, major, critical
□	116137-3	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
☑	123456	EMAIL	✓	EMS, SEM, IP Phone	EMS, SEM, IP Phone	info, warning, minor, major, critical
□	snmp1	SNMP	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	syslog1	SYSLOG	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical

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



Destination Rule Configuration

Destination Type: Email

Destination Rule Name: 123456

● Allow Forward ○ Prevent Forward

Alarm Origin

	EMS	SEM	MGW	IP Phone
Alarms	☑	☑	□	☑
Events	☑	☑	□	☑

Alarm Names: All Alarms

Alarm Types: All Types

Severities

Source: Board

Source MGW List

Region	MGW Name	IP Address
A-Shlomi	10.7.37.50	10.7.12.96
AutoDetection	10.3.181.63_396...	10.3.181.63
AutoDetection	10.3.181.58_571...	10.3.181.2
AutoDetection	10.4.100.23-389...	10.4.100.23
AutoDetection	10.3.181.52-686...	10.3.2.9

Mail Host: 10.1.1.60

Alarms Filter

All Alarms

	Alarm Name
□	Active Alarms Sync
□	Change Mib Version
□	Disk Space Alarm
□	EMS Server Started
□	Software Replaced
□	Software Upgrade
□	HTTP/HTTPS Access Disabled
□	Hardware Replaced
□	PM File Generated
□	HTTP and HTTPS Access is Disabled
□	PM Polling
□	IPPhone Lync Login Failure
□	IPPhone Survivable Mode Start
□	SEM - Bandwidth Alarm
□	Alarm Suppression
☑	EMS Keep-Alive
□	SEM - Max Concurrent Calls Alarm
□	Endpoint Publish Alarm

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

32.4 Changing the Alarms Browser Views

This section describes how to change the Alarms Browser Views.

32.4.1 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.

32.4.2 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 . 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

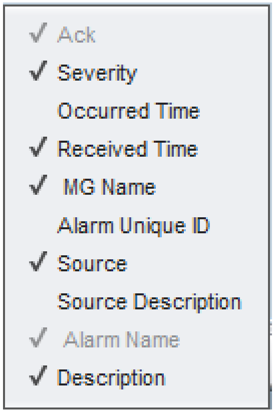
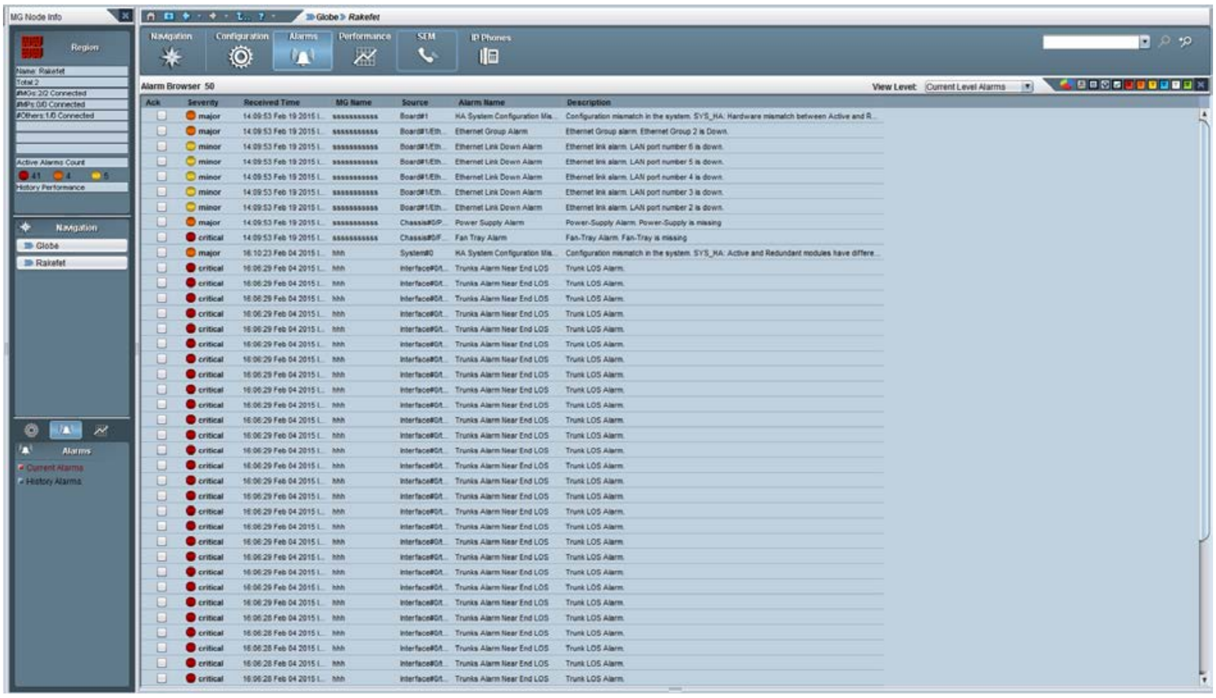


Figure 24-8: Current Alarms



Name: Rakefet
Total 2
#MGs: 2/2 Connected
#MPs: 0/0 Connected
#Others: 1/0 Connected

Active Alarms Count
● 41 ● 4 ● 5
History Performance

Alarm Browser 50

Ack	Severity	Received Time	MG Name	Source	Alarm Name	Description
□	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1	HA System Configuration Mis...	Configuration mismatch in the system. SYS_HA: Hardware mismatch between Active and R...
□	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 2 is Down.
□	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 6 is down.
□	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 5 is down.
□	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is down.
□	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is down.
□	● minor	14:09:53 Feb 19 2015 I...	sssssssssss	Board#1/Eth...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is down.
□	● major	14:09:53 Feb 19 2015 I...	sssssssssss	Chassis#0/P...	Power Supply Alarm	Power-Supply Alarm. Power-Supply is missing
□	● critical	14:09:53 Feb 19 2015 I...	sssssssssss	Chassis#0/F...	Fan Tray Alarm	Fan-Tray Alarm. Fan-Tray is missing
□	● major	16:10:23 Feb 04 2015 I...	hhh	System#0	HA System Configuration Mis...	Configuration mismatch in the system. SYS_HA: Active and Redundant modules have differe...
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:29 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:28 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:28 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:28 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:28 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.
□	● critical	16:06:28 Feb 04 2015 I...	hhh	Interface#0/t...	Trunks Alarm Near End LOS	Trunk LOS Alarm.

32.5 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 273.

32.6 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 357.

32.7 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.

32.8 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]

32.9 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**.

This page is intentionally left blank.

33 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.

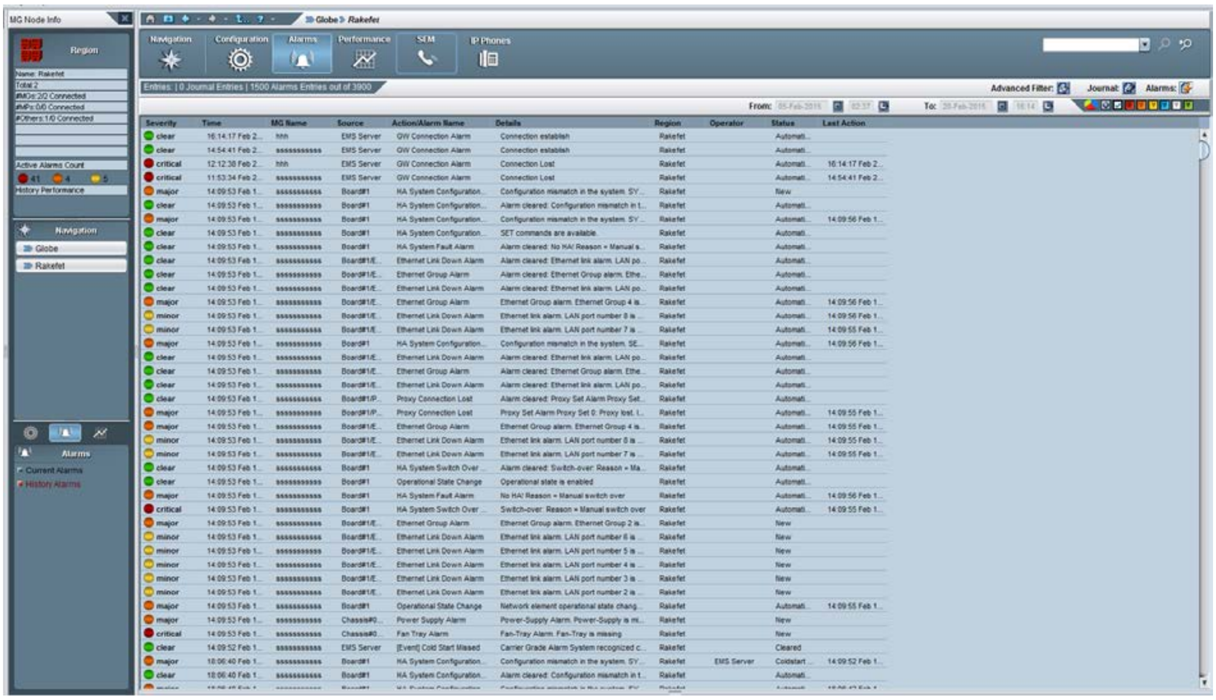
Open the Alarms History screen from the Alarms module by clicking the 'History Alarms' option. The Alarms History screen is context-sensitive like the Alarm Browser; the context is displayed in the title of the screen.

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



Entries: | 0 Journal Entries | 1500 Alarms Entries out of 3900

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator	Status	Last Action
clear	16:14:17 Feb 2...	hhh	EMS Server	GW Connection Alarm	Connection establish	Rakefet		Automati...	
clear	14:54:41 Feb 2...	sssssssssss	EMS Server	GW Connection Alarm	Connection establish	Rakefet		Automati...	
critical	12:12:38 Feb 2...	hhh	EMS Server	GW Connection Alarm	Connection Lost	Rakefet		Automati...	16:14:17 Feb 2...
critical	11:53:34 Feb 2...	sssssssssss	EMS Server	GW Connection Alarm	Connection Lost	Rakefet		Automati...	14:54:41 Feb 2...
major	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Configuration mismatch in the system. SY...	Rakefet		New	
clear	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Alarm cleared: Configuration mismatch in t...	Rakefet		Automati...	
major	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Configuration mismatch in the system. SY...	Rakefet		Automati...	14:09:56 Feb 1...
clear	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Configuration...	SET commands are available.	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Fault Alarm	Alarm cleared: No HA! Reason = Manual s...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN po...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Group Alarm	Alarm cleared: Ethernet Group alarm. Ethe...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN po...	Rakefet		Automati...	
major	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 4 is...	Rakefet		Automati...	14:09:56 Feb 1...
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 8 is ...	Rakefet		Automati...	14:09:56 Feb 1...
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 7 is ...	Rakefet		Automati...	14:09:55 Feb 1...
major	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Configuration mismatch in the system. SE...	Rakefet		Automati...	14:09:56 Feb 1...
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN po...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Group Alarm	Alarm cleared: Ethernet Group alarm. Ethe...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Alarm cleared: Ethernet link alarm. LAN po...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1/P...	Proxy Connection Lost	Alarm cleared: Proxy Set Alarm Proxy Set...	Rakefet		Automati...	
major	14:09:53 Feb 1...	sssssssssss	Board#1/P...	Proxy Connection Lost	Proxy Set Alarm Proxy Set 0: Proxy lost. I...	Rakefet		Automati...	14:09:55 Feb 1...
major	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 4 is...	Rakefet		Automati...	14:09:55 Feb 1...
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 8 is ...	Rakefet		Automati...	14:09:55 Feb 1...
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 7 is ...	Rakefet		Automati...	14:09:55 Feb 1...
clear	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Switch Over ...	Alarm cleared: Switch-over: Reason = Ma...	Rakefet		Automati...	
clear	14:09:53 Feb 1...	sssssssssss	Board#1	Operational State Change	Operational state is enabled	Rakefet		Automati...	
major	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Fault Alarm	No HA! Reason = Manual switch over	Rakefet		Automati...	14:09:56 Feb 1...
critical	14:09:53 Feb 1...	sssssssssss	Board#1	HA System Switch Over ...	Switch-over: Reason = Manual switch over	Rakefet		Automati...	14:09:55 Feb 1...
major	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Group Alarm	Ethernet Group alarm. Ethernet Group 2 is...	Rakefet		New	
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 6 is ...	Rakefet		New	
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 5 is ...	Rakefet		New	
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 4 is ...	Rakefet		New	
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 3 is ...	Rakefet		New	
minor	14:09:53 Feb 1...	sssssssssss	Board#1/E...	Ethernet Link Down Alarm	Ethernet link alarm. LAN port number 2 is ...	Rakefet		New	
major	14:09:53 Feb 1...	sssssssssss	Board#1	Operational State Change	Network element operational state chang...	Rakefet		Automati...	14:09:55 Feb 1...
major	14:09:53 Feb 1...	sssssssssss	Chassis#0...	Power Supply Alarm	Power-Supply Alarm. Power-Supply is mi...	Rakefet		New	
critical	14:09:53 Feb 1...	sssssssssss	Chassis#0...	Fan Tray Alarm	Fan-Tray Alarm. Fan-Tray is missing	Rakefet		New	
clear	14:09:52 Feb 1...	sssssssssss	EMS Server	[Event] Cold Start Missed	Carrier Grade Alarm System recognized c...	Rakefet		Cleared	
major	18:06:40 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Configuration mismatch in the system. SY...	Rakefet	EMS Server	Coldstart ...	14:09:52 Feb 1...
clear	18:06:40 Feb 1...	sssssssssss	Board#1	HA System Configuration...	Alarm cleared: Configuration mismatch in t...	Rakefet		Automati...	

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**.

34 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.

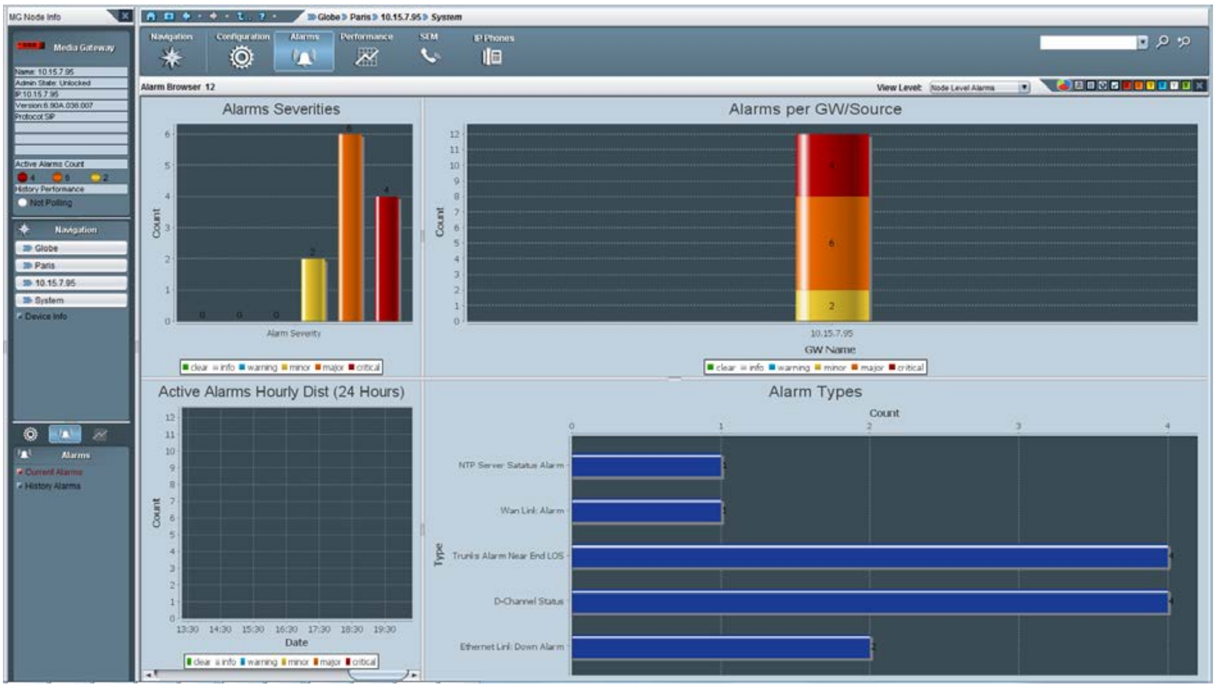
The following graphs are displayed:

- 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

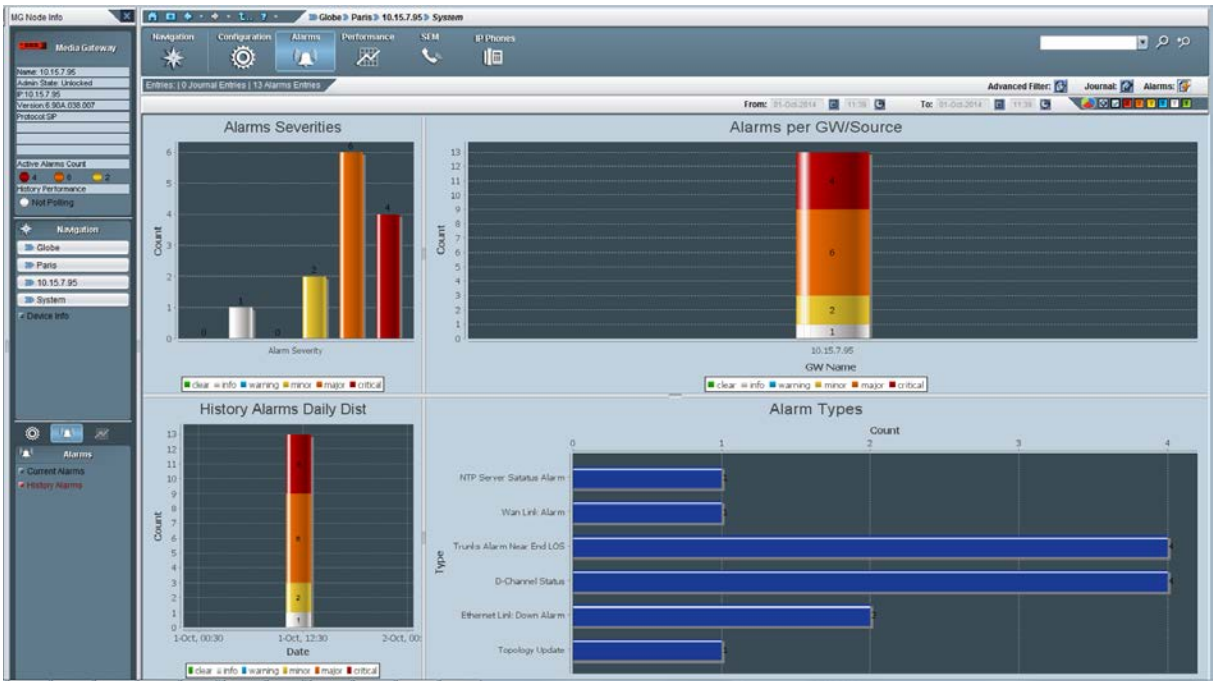


Name: 10.15.7.95
Admin State: Unlocked
IP:10.15.7.95
Version:6.90A.038.007
Protocol:SIP

Alarm Browser 12

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

Figure 26-2: History Alarms Graph



Name: 10.15.7.95
Admin State: Unlocked
IP:10.15.7.95
Version:6.90A.038.007
Protocol:SIP
Active Alarms Count
History Performance
Not Polling

Entries: | 0 Journal Entries | 13 Alarms Entries

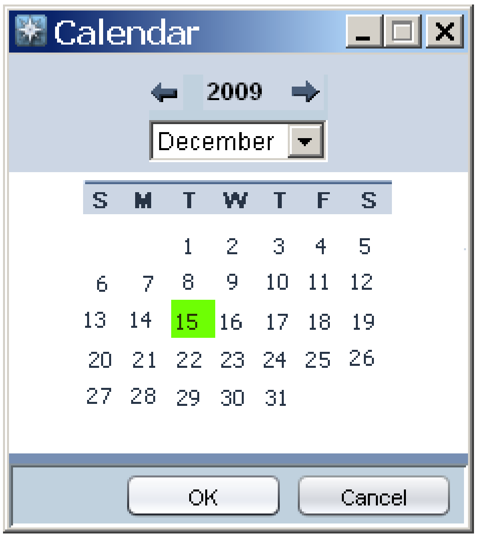
35 Using Alarm Filters

This section describes how to use the alarm filters.

35.1 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

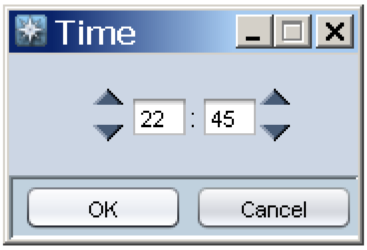


2009

December

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

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



22 : 45

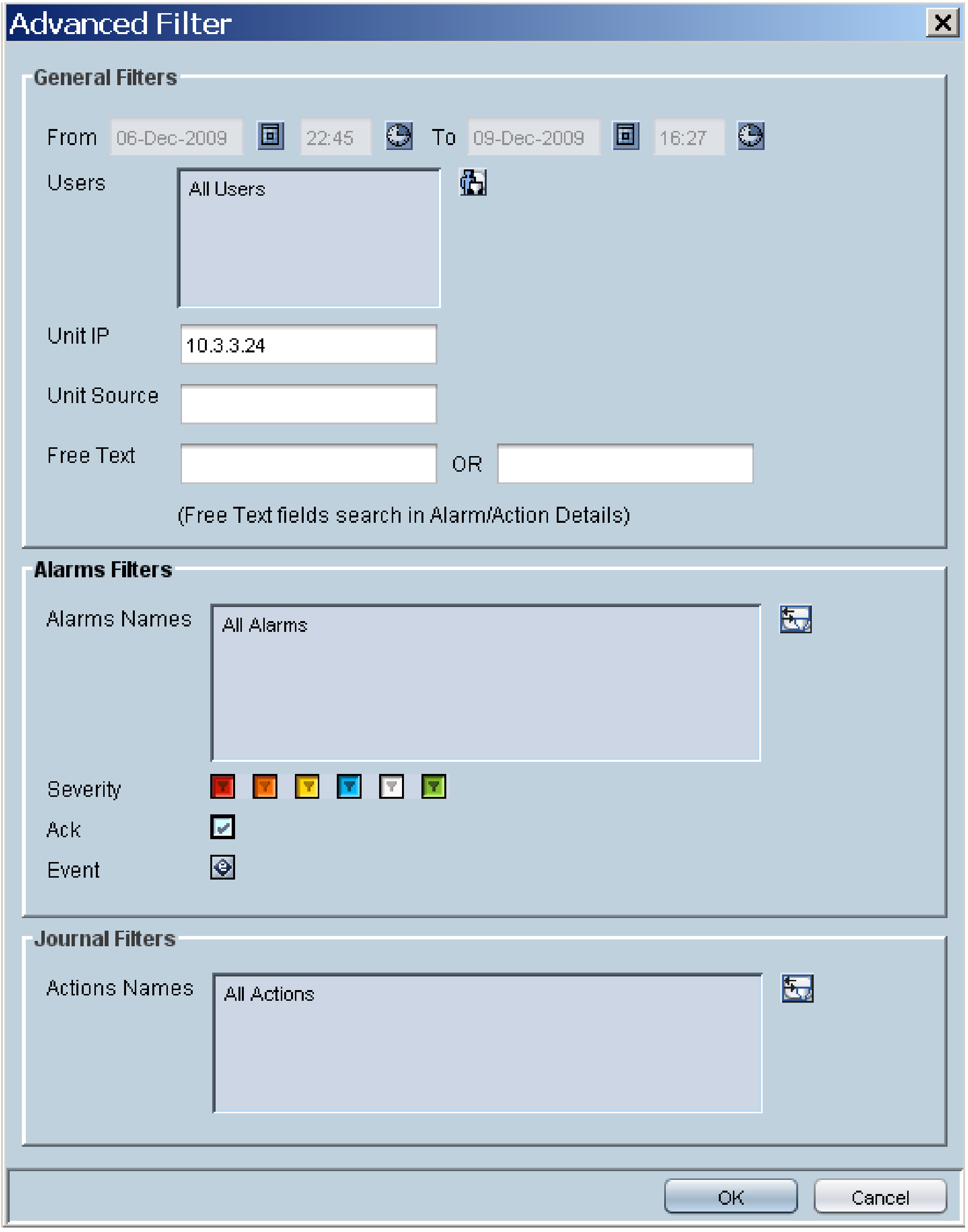
35.2 Using Advanced Filters

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



From 06-Dec-2009 22:45 To 09-Dec-2009 16:27

Users: All Users

Unit IP: 10.3.3.24

Unit Source:

Free Text: OR

(Free Text fields search in Alarm/Action Details)

Alarms Names: All Alarms

Severity

Ack

Event

Actions Names: All Actions

- **General Filters**

  To configure general filters, click the General Filters icon in the General Filters pane. You can configure the following filters:

  - Date and Time Filter
  - Users Filter. An operator can select a user or a set of users whose actions the operator needs to view.
  - Unit IP
  - Unit Source
  - Free Text 1 (searched in the Details filed)

- **Alarms Filters**

  To configure alarm filters, click the Alarms Filters icon in the Alarms Filters pane. You can configure the following filters:

  - Includes the lists of Alarms / Events per MG type.
  - Alarm Severity
  - Alarm Ack Status
  - Events

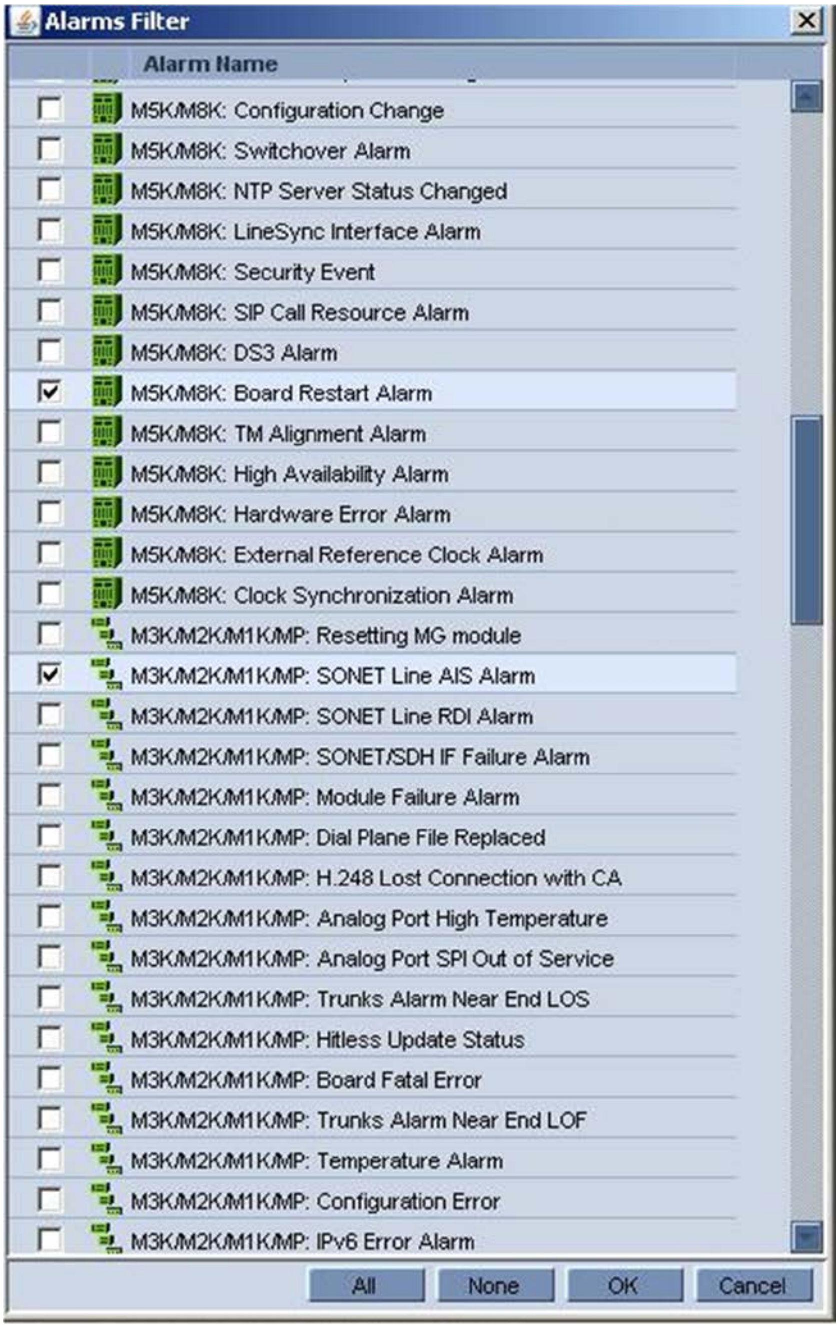
- **Journal Filters**

  To configure journal filters, click the Journal Filters icon in the Journal Filters pane. You can configure the following filters:

  - Actions Filter (all user actions are classified according to EMS functionality):
    - Fault Management Actions (acknowledge, delete, prioritize alarms, change trap configuration)
    - Configuration Management Actions (add, remove, update managed object, software upgrade, etc.)
    - Performance Management (start, stop polling, create, attach, detach PM profile)
    - Security Management Actions (add, remove, update operator info, login, logout)

The following screen displays an example of the Alarms Filter screen:

Figure 27-4: Alarms Filter



Alarms Filter

Alarm Name

- ☐ M5K/M8K: Configuration Change
- ☐ M5K/M8K: Switchover Alarm
- ☐ M5K/M8K: NTP Server Status Changed
- ☐ M5K/M8K: LineSync Interface Alarm
- ☐ M5K/M8K: Security Event
- ☐ M5K/M8K: SIP Call Resource Alarm
- ☐ M5K/M8K: DS3 Alarm
- ☑ M5K/M8K: Board Restart Alarm
- ☐ M5K/M8K: TM Alignment Alarm
- ☐ M5K/M8K: High Availability Alarm
- ☐ M5K/M8K: Hardware Error Alarm
- ☐ M5K/M8K: External Reference Clock Alarm
- ☐ M5K/M8K: Clock Synchronization Alarm
- ☐ M3K/M2K/M1K/MP: Resetting MG module
- ☑ M3K/M2K/M1K/MP: SONET Line AIS Alarm
- ☐ M3K/M2K/M1K/MP: SONET Line RDI Alarm
- ☐ M3K/M2K/M1K/MP: SONET/SDH IF Failure Alarm
- ☐ M3K/M2K/M1K/MP: Module Failure Alarm
- ☐ M3K/M2K/M1K/MP: Dial Plane File Replaced
- ☐ M3K/M2K/M1K/MP: H.248 Lost Connection with CA
- ☐ M3K/M2K/M1K/MP: Analog Port High Temperature
- ☐ M3K/M2K/M1K/MP: Analog Port SPI Out of Service
- ☐ M3K/M2K/M1K/MP: Trunks Alarm Near End LOS
- ☐ M3K/M2K/M1K/MP: Hitless Update Status
- ☐ M3K/M2K/M1K/MP: Board Fatal Error
- ☐ M3K/M2K/M1K/MP: Trunks Alarm Near End LOF
- ☐ M3K/M2K/M1K/MP: Temperature Alarm
- ☐ M3K/M2K/M1K/MP: Configuration Error
- ☐ M3K/M2K/M1K/MP: IPv6 Error Alarm

36 Defining Complex Queries using a Combination of Filters

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

36.1 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.

37 Viewing and Interpreting an Alarm's Details

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

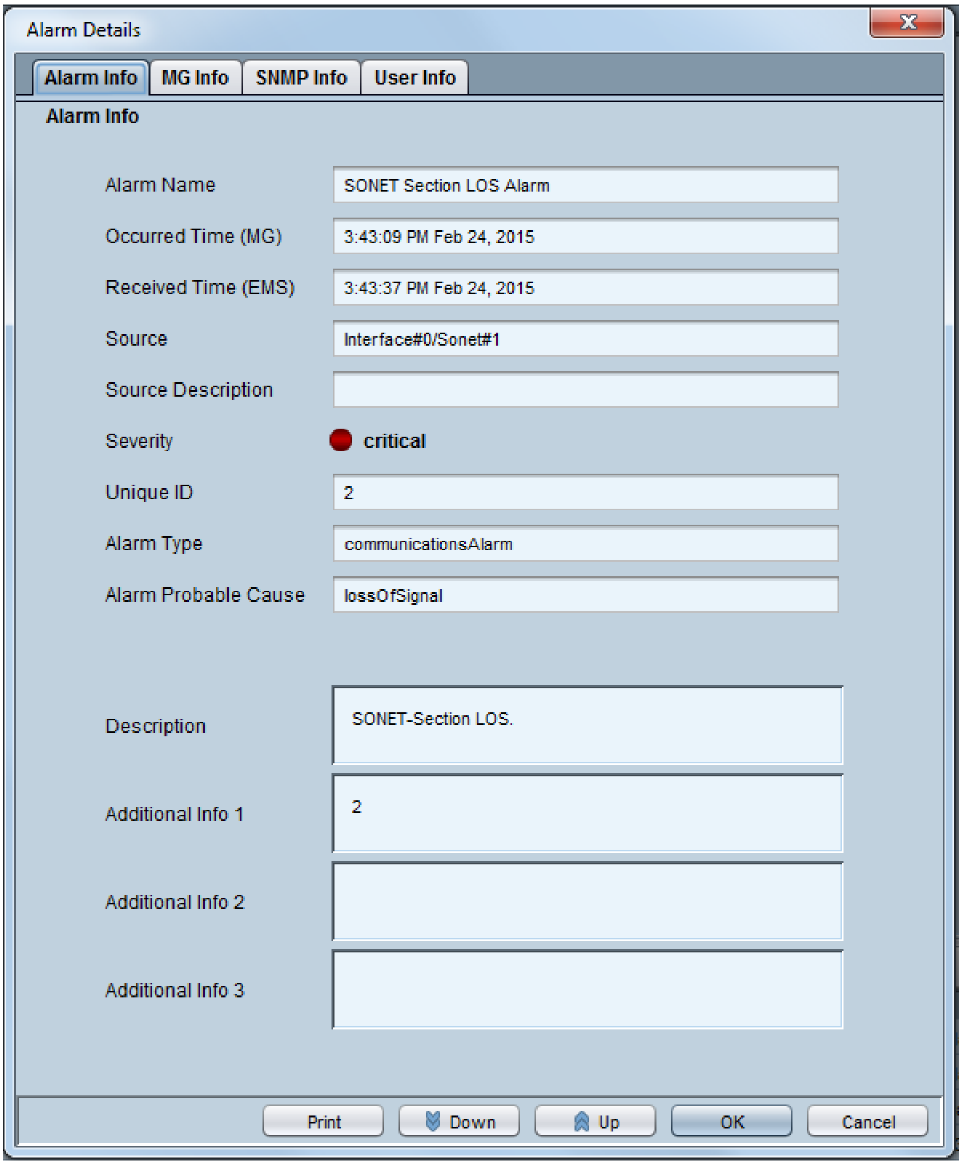
➢ **To view/interpret an alarm's details, do one of the following:**

- 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



Alarm Info

Alarm Name	SONET Section LOS Alarm
Occurred Time (MG)	3:43:09 PM Feb 24, 2015
Received Time (EMS)	3:43:37 PM Feb 24, 2015
Source	Interface#0/Sonet#1
Source Description	
Severity	● critical
Unique ID	2
Alarm Type	communicationsAlarm
Alarm Probable Cause	lossOfSignal
Description	SONET-Section LOS.
Additional Info 1	2
Additional Info 2	
Additional Info 3	

The Alarm Details screen features the following tabs:

- **Alarm Info** (includes all the information provided by the alarm; refer to its details below).
- **MG Info** (includes details regarding the location - region - of the 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).

37.1 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 259).
- **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

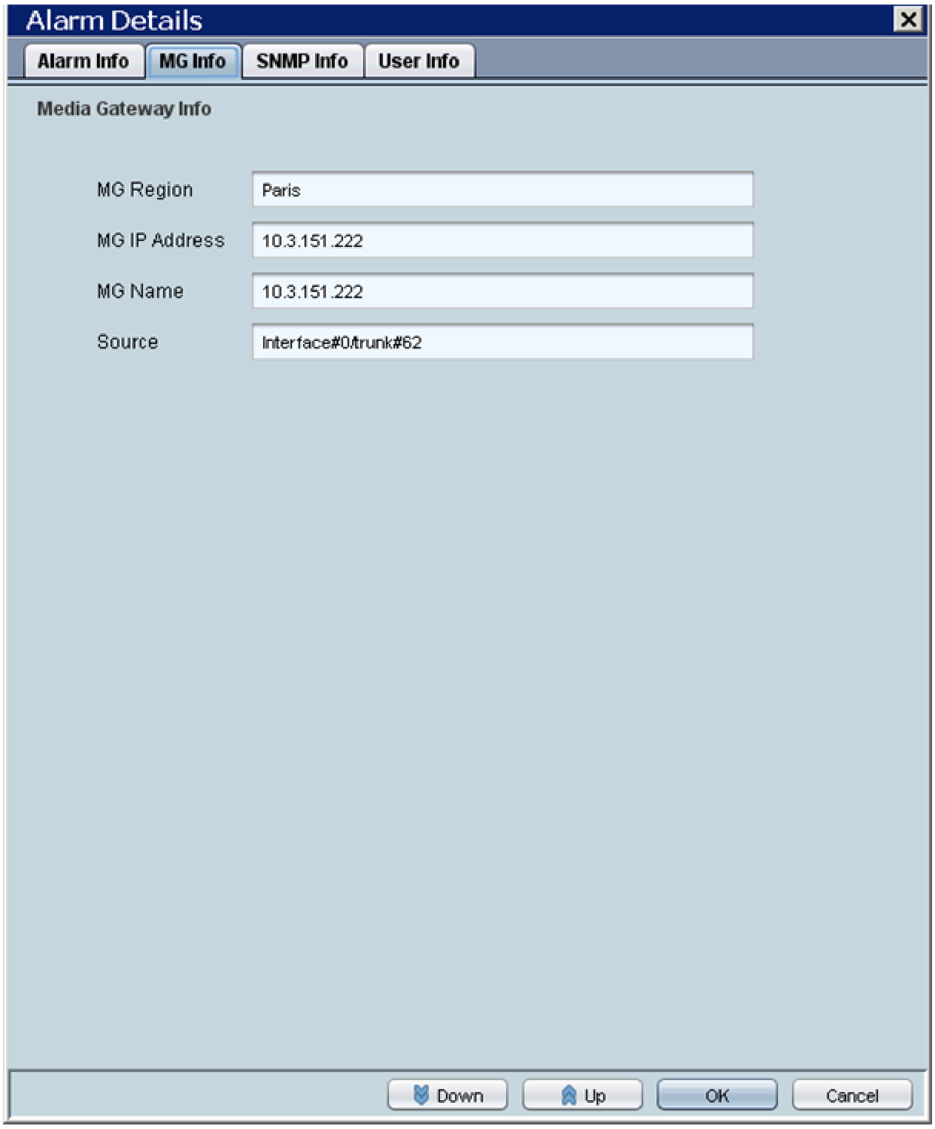
Notes: The parameter 'Alarm Type' is based on ITU X.733, X736 standards.

- **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.

37.2 Alarm Details - Tab MG Info

This section describes the MG Info tab.

Figure 29-2: Alarm Details-MG Info



Media Gateway Info

MG Region: Paris

MG IP Address: 10.3.151.222

MG Name: 10.3.151.222

Source: Interface#0/trunk#62

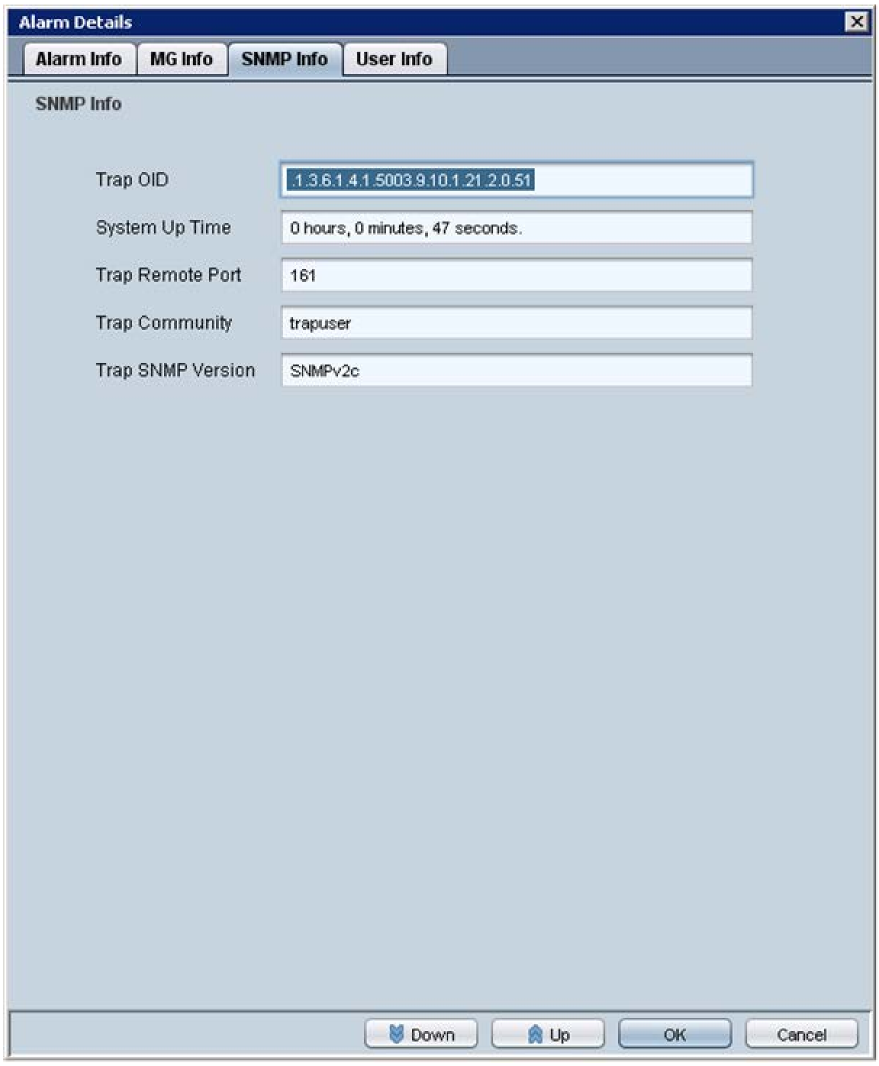
The **MG Info** tab features the following fields:

- **MG Region** – The name of the region in which the 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'.

37.3 Alarm Details > Tab SNMP Info

This section describes the SNMP Info tab.

Figure 29-3: Alarm Details-SNMP Info



SNMP Info

Trap OID: .1.3.6.1.4.1.5003.9.10.1.21.2.0.51

System Up Time: 0 hours, 0 minutes, 47 seconds.

Trap Remote Port: 161

Trap Community: trapuser

Trap SNMP Version: SNMPv2c

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

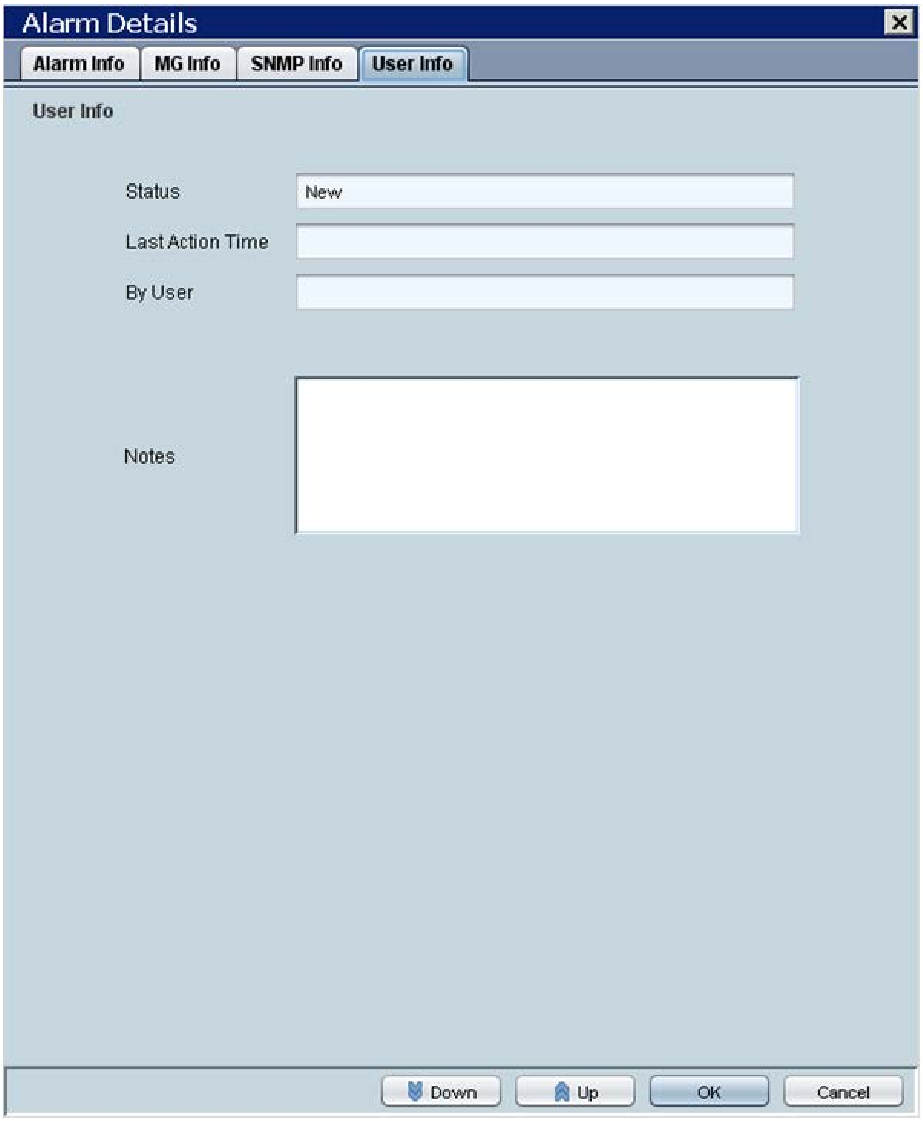
- **Trap OID** – Trap Object Identifier, as defined in the MIB.
- **System Up Time** – The time elapsed since the last system reset.
- **Trap Remote Port** – The EMS UDP remote port at which the trap was received.
- **Trap Community** – Trap Community String received as part of the Notification message

- **Trap SNMP Version** – The SNMP version of the Agent that sent the trap. The SNMP version can be one of the following:
    - SNMPv1
    - SNMPv2c
    - SNMPv3

37.4 Alarm Details > Tab User Info

This section describes the User Info tab.

Figure 29-4: Alarm Details-User Info



User Info

Status: New

Last Action Time:

By User:

Notes:

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.

38 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.

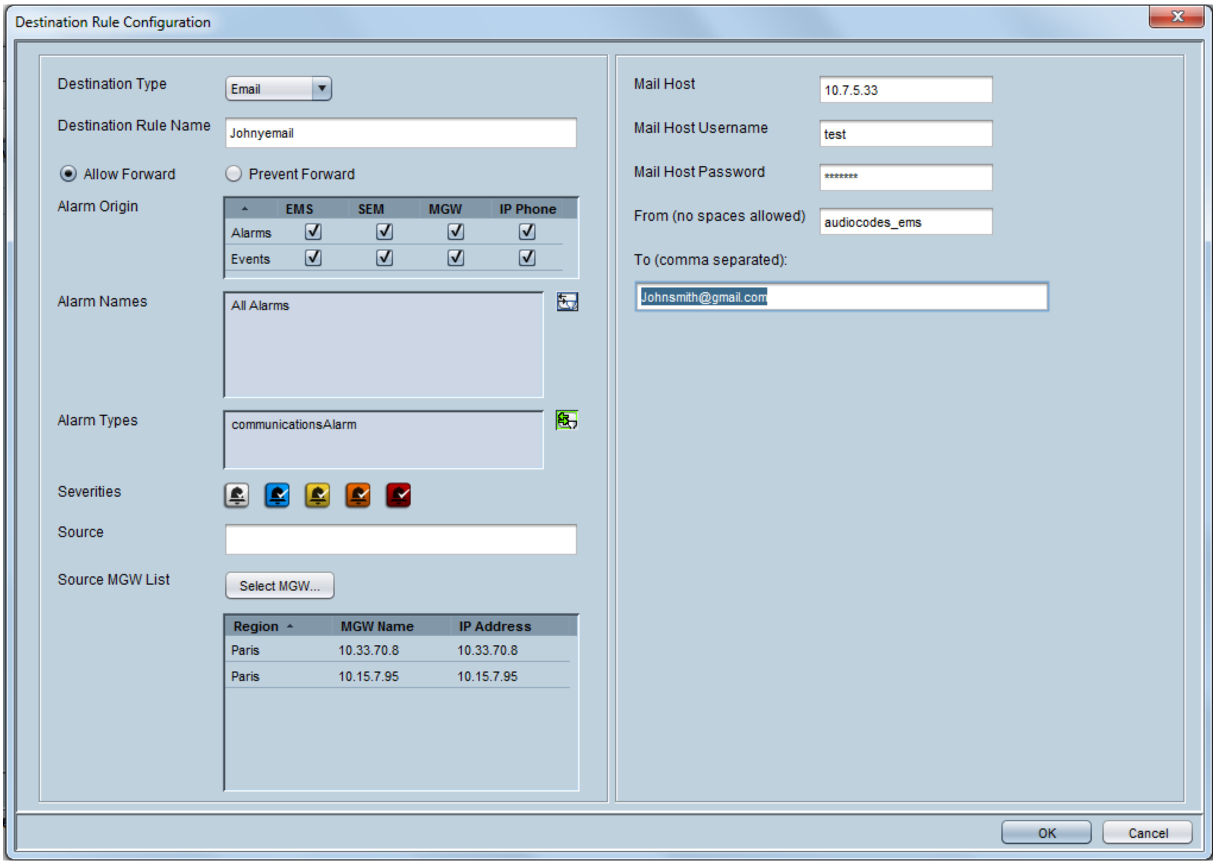
38.1 Trap Forwarding in Mail Format

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



Destination Rule Configuration

Destination Type: Email

Destination Rule Name: Johnyemail

● Allow Forward ○ Prevent Forward

Alarm Origin

	EMS	SEM	MGW	IP Phone
Alarms	☑	☑	☑	☑
Events	☑	☑	☑	☑

Alarm Names: All Alarms

Alarm Types: communicationsAlarm

Severities

Source:

Source MGW List: Select MGW...

Region	MGW Name	IP Address
Paris	10.33.70.8	10.33.70.8
Paris	10.15.7.95	10.15.7.95

Mail Host: 10.7.5.33

Mail Host Username: test

Mail Host Password: *******

From (no spaces allowed): audiocodes_ems

To (comma separated): Johnsmith@gmail.com

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

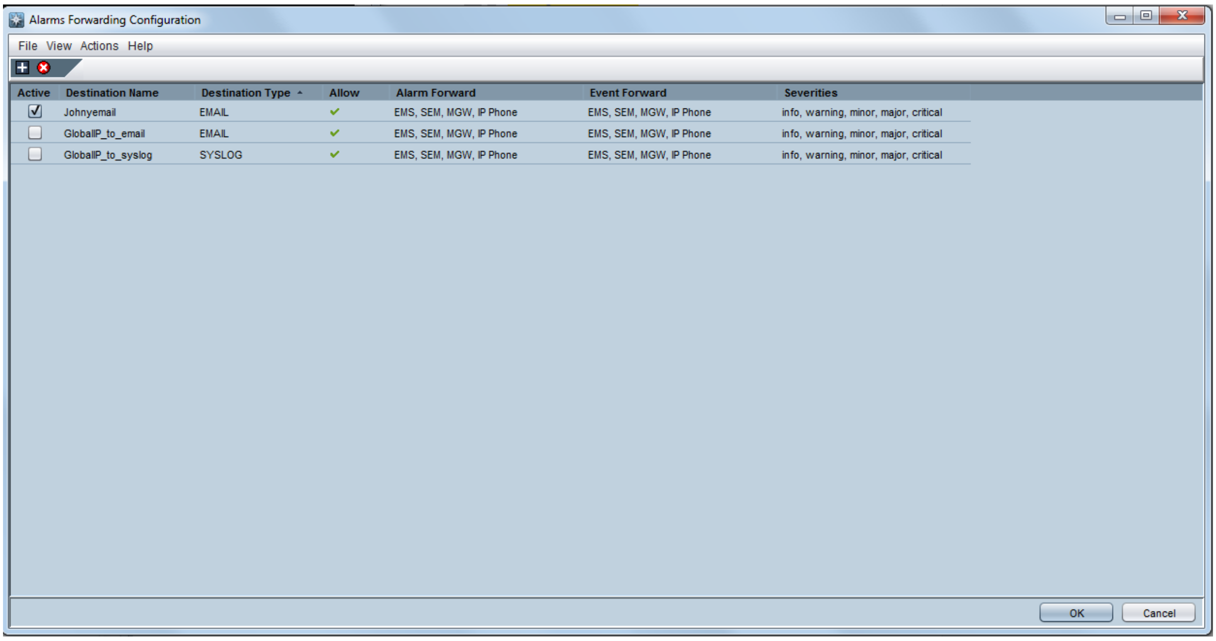
'Prevent Forward', and then in the 'Source' field, you specify 'Board#1/EthernetLink#2', then whenever LAN port #2 is down, an Ethernet link alarm is not forwarded.

- 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.
- 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.

5. In the right-hand pane, provision the following parameters:
   - In the 'Mail Host IP Address' field, enter the **Mail Host IP address or FQDN** (e.g. "smtp.office365.com").
   - 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



Active	Destination Name	Destination Type	Allow	Alarm Forward	Event Forward	Severities
☑	Johnyemail	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_email	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_syslog	SYSLOG	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical

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
```

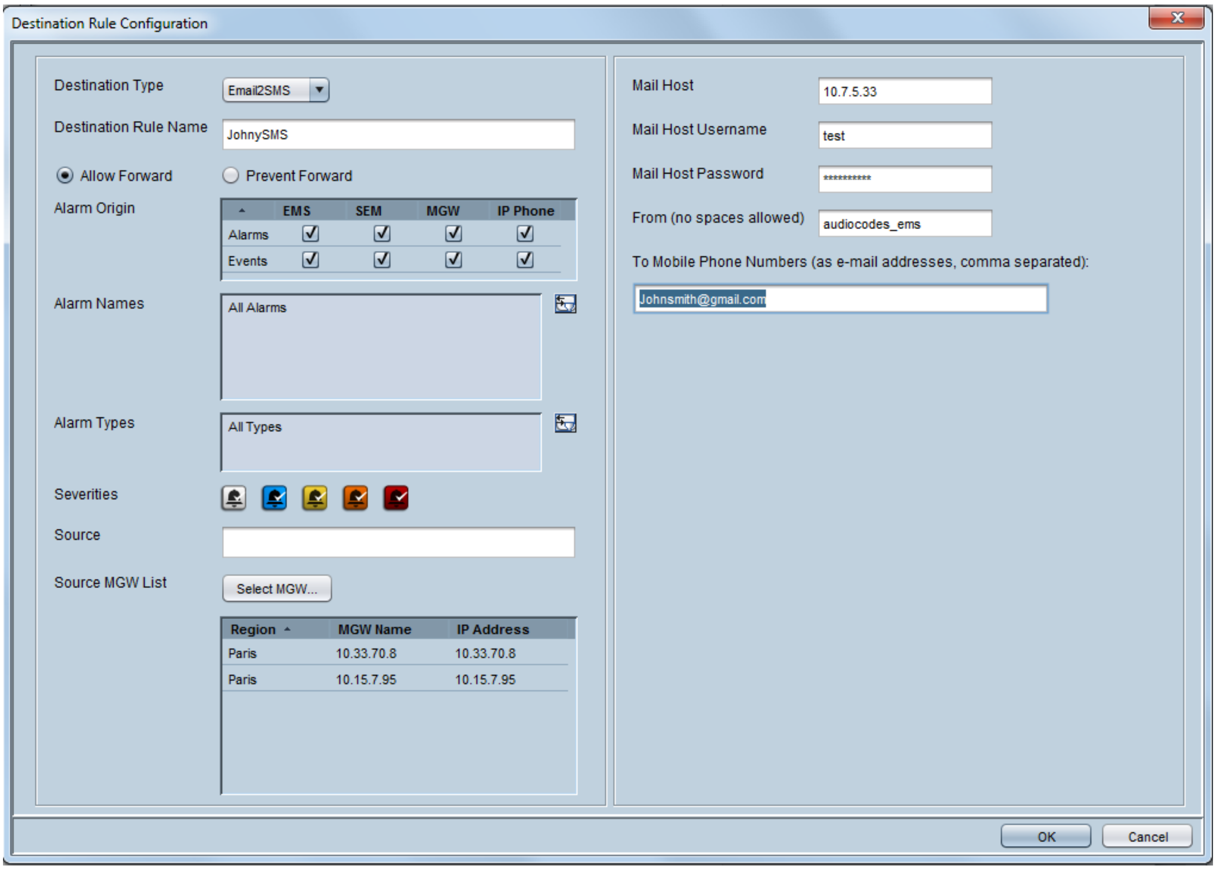
38.2 Trap Forwarding in Mail2SMS Format

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 292.
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



Destination Rule Configuration

Destination Type: Email2SMS

Destination Rule Name: JohnySMS

● Allow Forward ○ Prevent Forward

Alarm Origin

	EMS	SEM	MGW	IP Phone
Alarms	☑	☑	☑	☑
Events	☑	☑	☑	☑

Alarm Names: All Alarms

Alarm Types: All Types

Severities

Source:

Source MGW List: Select MGW...

Region	MGW Name	IP Address
Paris	10.33.70.8	10.33.70.8
Paris	10.15.7.95	10.15.7.95

Mail Host: 10.7.5.33

Mail Host Username: test

Mail Host Password: **********

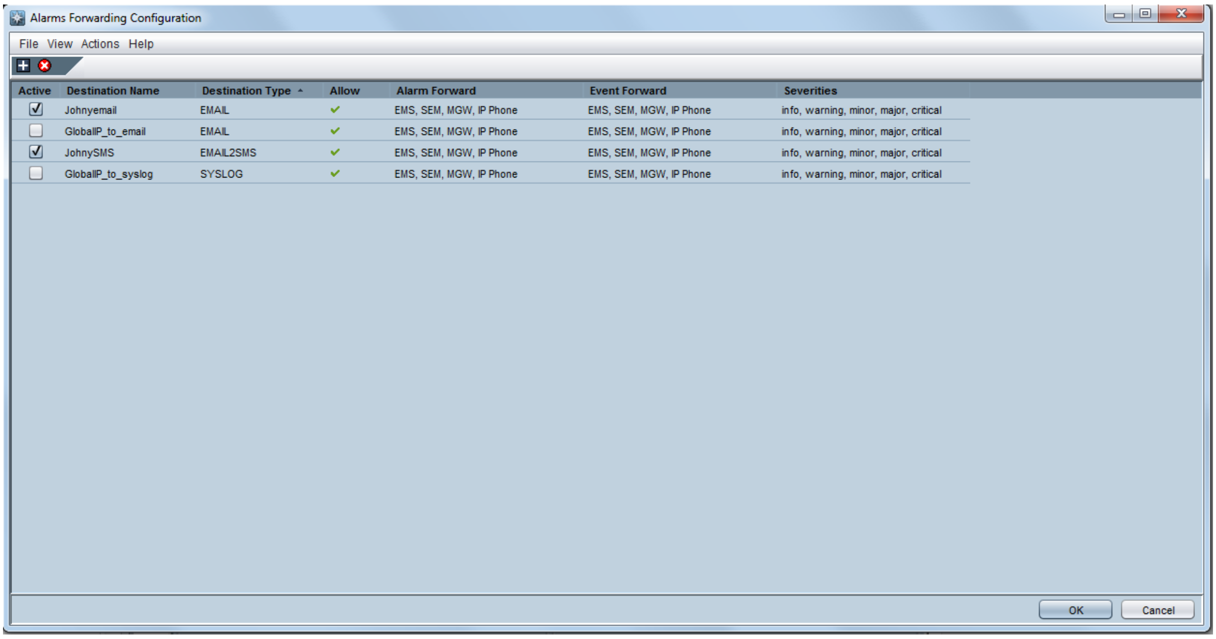
From (no spaces allowed): audiocodes_ems

To Mobile Phone Numbers (as e-mail addresses, comma separated): Johnsmith@gmail.com

6. Click **OK.**

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

Figure 30-4: Trap Forwarding Summary-Mail2SMS



Active	Destination Name	Destination Type	Allow	Alarm Forward	Event Forward	Severities
☑	Johnyemail	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_email	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
☑	JohnySMS	EMAIL2SMS	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_syslog	SYSLOG	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical

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

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

38.3 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:**

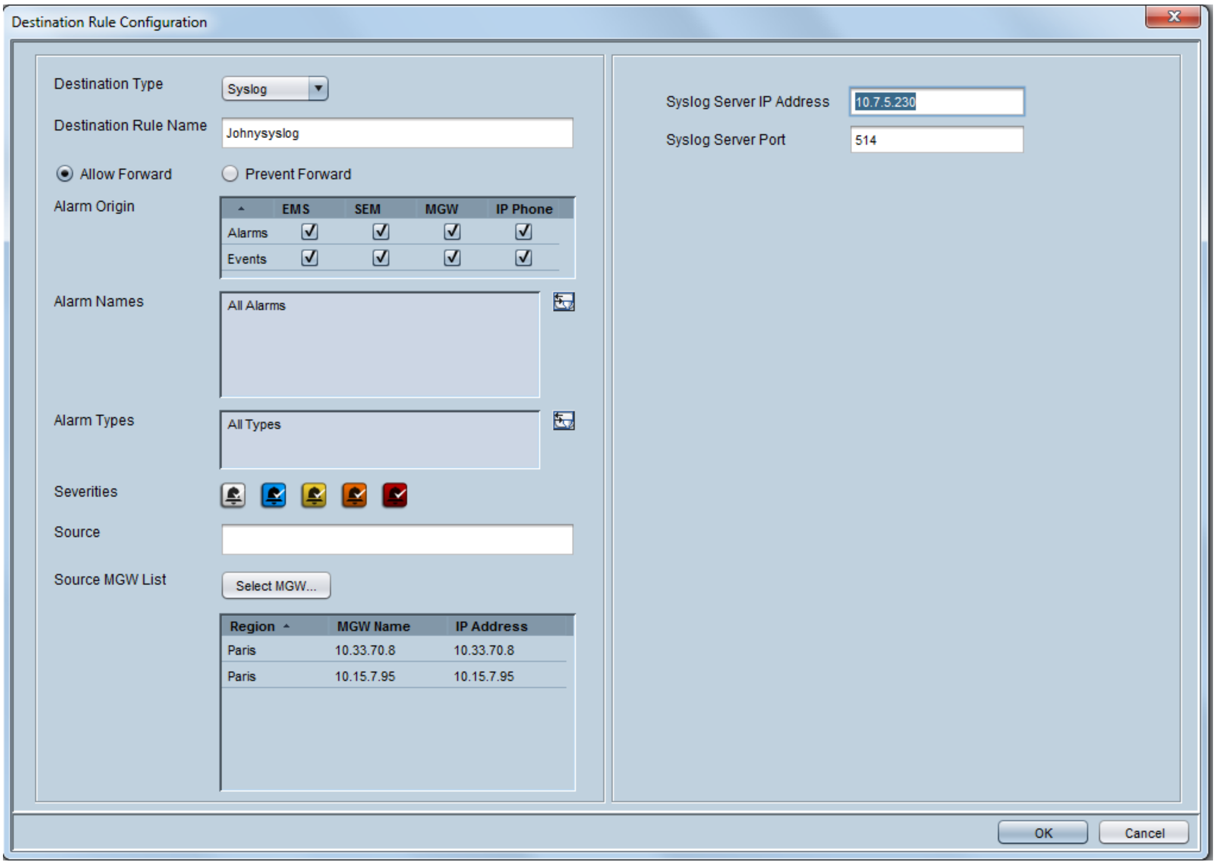
1. Open the **Faults** > **Trap configuration** menu. The Destination Rule Configuration dialog is displayed.
2. In the Actions menu, select **Add Destination** or click **+** in the menu bar.
3. Set the Destination Type to **Syslog**.
4. In the left-hand pane, configure the destination rule as described above in Section 30.2 on page 292.

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



Destination Rule Configuration

Destination Type: Syslog

Destination Rule Name: Johnysyslog

● Allow Forward ○ Prevent Forward

Alarm Origin

	EMS	SEM	MGW	IP Phone
Alarms	☑	☑	☑	☑
Events	☑	☑	☑	☑

Alarm Names: All Alarms

Alarm Types: All Types

Severities

Source:

Source MGW List: Select MGW...

Region	MGW Name	IP Address
Paris	10.33.70.8	10.33.70.8
Paris	10.15.7.95	10.15.7.95

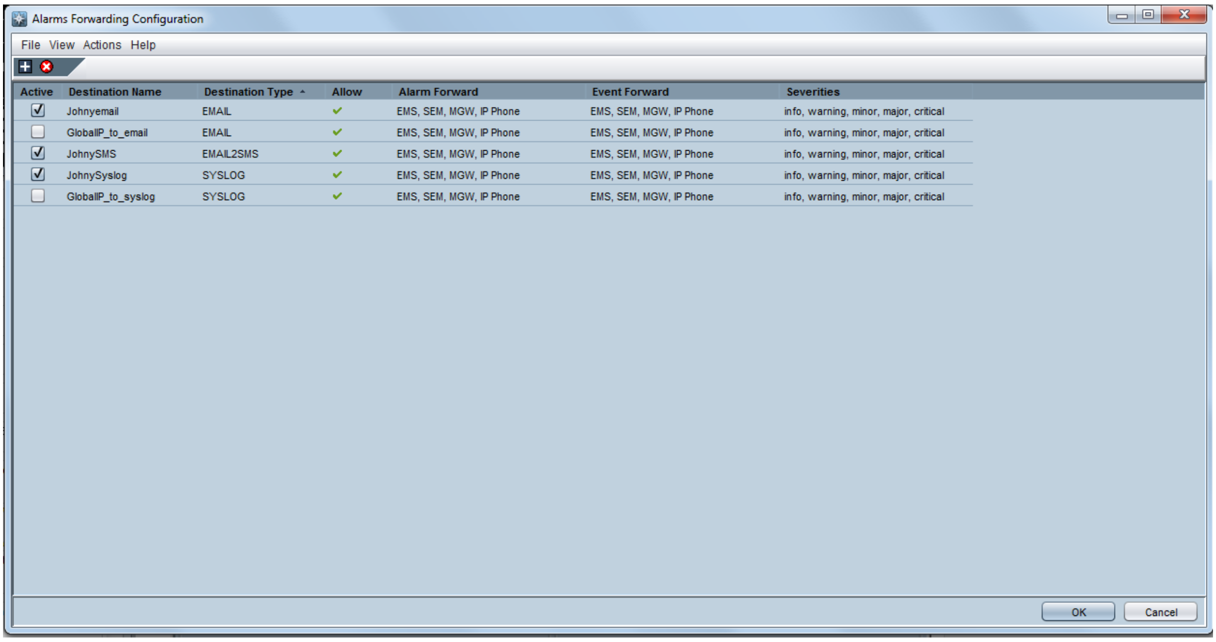
Syslog Server IP Address: 10.7.5.230

Syslog Server Port: 514

6. Click **OK.**

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

Figure 30-6: Trap Forwarding Configuration Summary-Syslog



Alarms Forwarding Configuration

Active	Destination Name	Destination Type	Allow	Alarm Forward	Event Forward	Severities
☑	Johnyemail	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_email	EMAIL	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
☑	JohnySMS	EMAIL2SMS	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
☑	JohnySyslog	SYSLOG	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical
□	GlobalIP_to_syslog	SYSLOG	✓	EMS, SEM, MGW, IP Phone	EMS, SEM, MGW, IP Phone	info, warning, minor, major, critical

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 265) then the Node IP is the global IP address.

This page is intentionally left blank.

39 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 for the relevant context are saved. For example, if the region is selected then all region alarms are saved or if MP devices are selected, then all alarms are saved for the selected MP devices.

  Note that the "View Level" indicator has no affect on the saved 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.

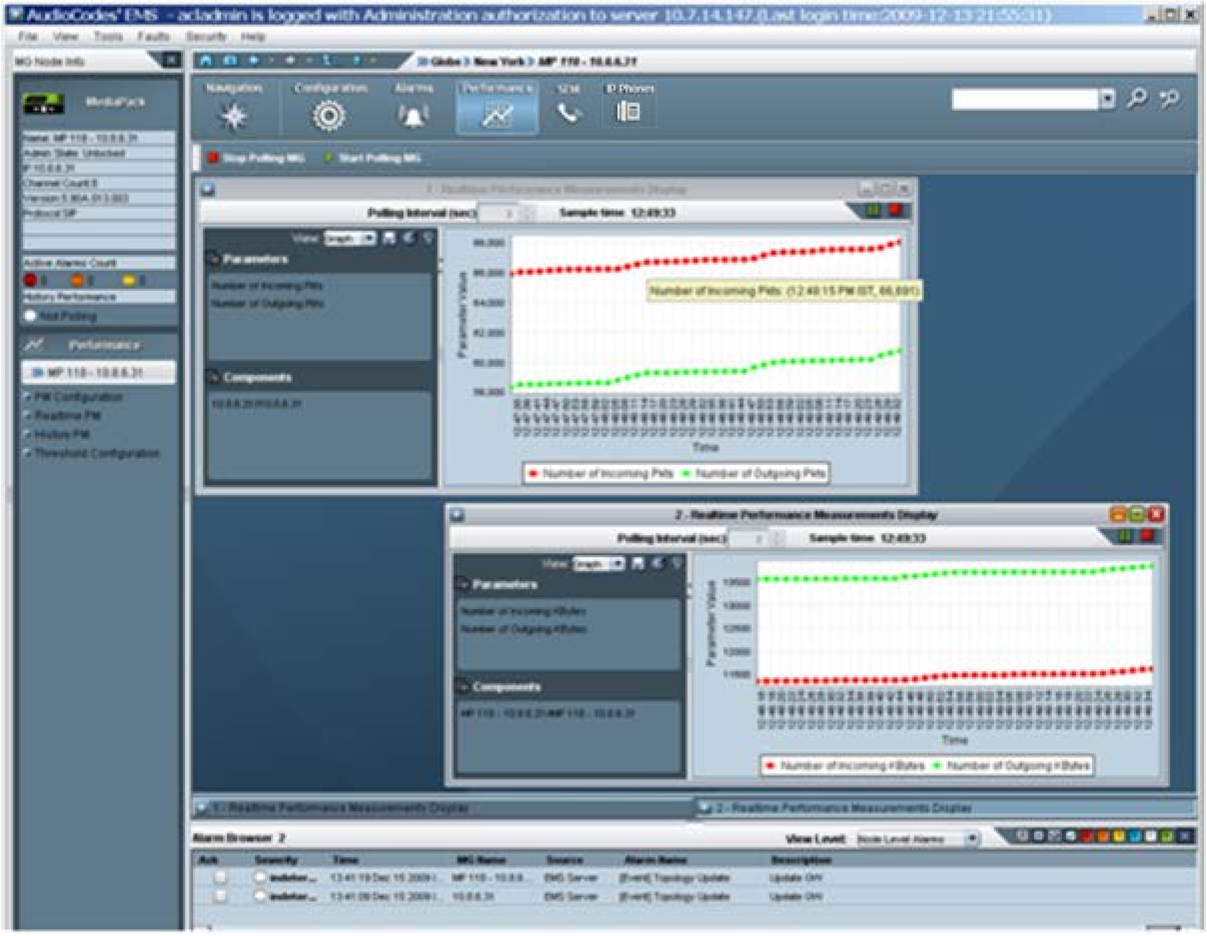
This page is intentionally left blank.

40 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 GuideAlarm and Performance Monitoring Guide*..

Figure 32-1: Performance Desktop

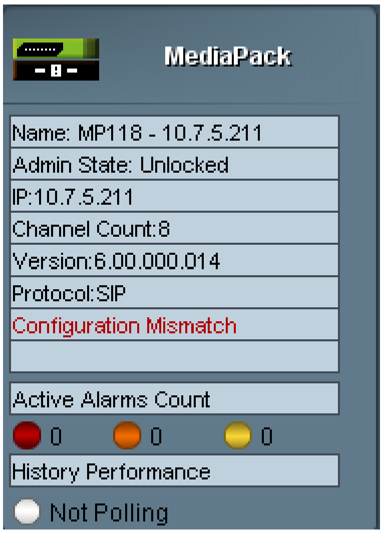


AudioCodes' EMS - acladmin is logged with Administration authorization to server 10.7.14.147.(Last login time:2009-12-13 21:55:31)

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	○ Indeter...	13:41:19 Dec 15 2009 I...	MP 118 - 10.8.6...	EMS Server	[Event] Topology Update	Update GW
□	○ Indeter...	13:41:09 Dec 15 2009 I...	10.8.6.21	EMS Server	[Event] Topology Update	Update GW

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



MediaPack

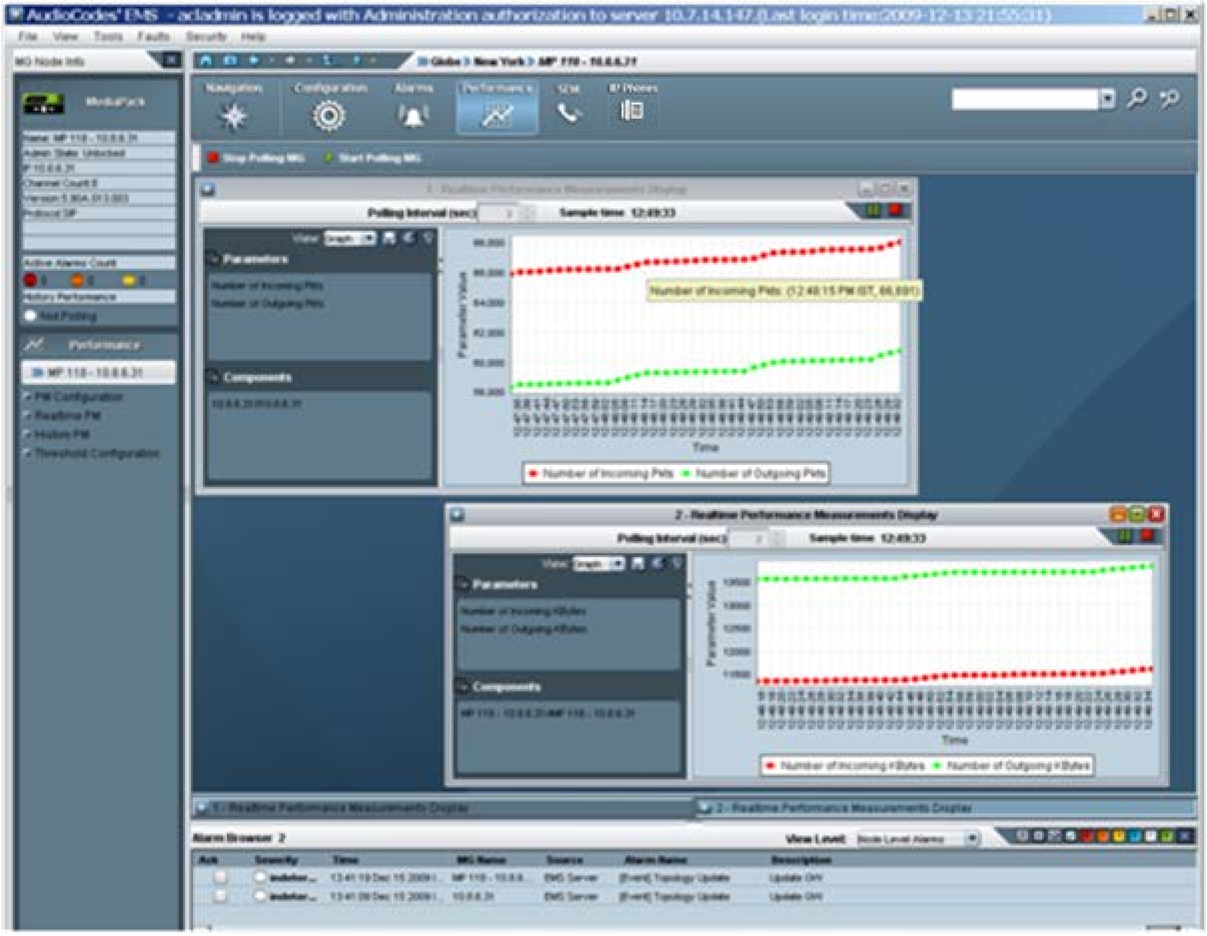
Name: MP118 - 10.7.5.211
Admin State: Unlocked
IP:10.7.5.211
Channel Count:8
Version:6.00.000.014
Protocol:SIP
Configuration Mismatch

Active Alarms Count
● 0 ● 0 ● 0
History Performance
○ Not Polling

40.1 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



AudioCodes' EMS - acladmin is logged with Administration authorization to server 10.7.14.147 (Last login time:2009-12-13 21:55:31)

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	indeter...	13:41:19 Dec 15 2009 I...	MP 110 - 10.8.6...	EMS Server	[Event] Topology Update	Update GW
□	indeter...	13:41:09 Dec 15 2009 I...	10.8.6.31	EMS Server	[Event] Topology Update	Update GW

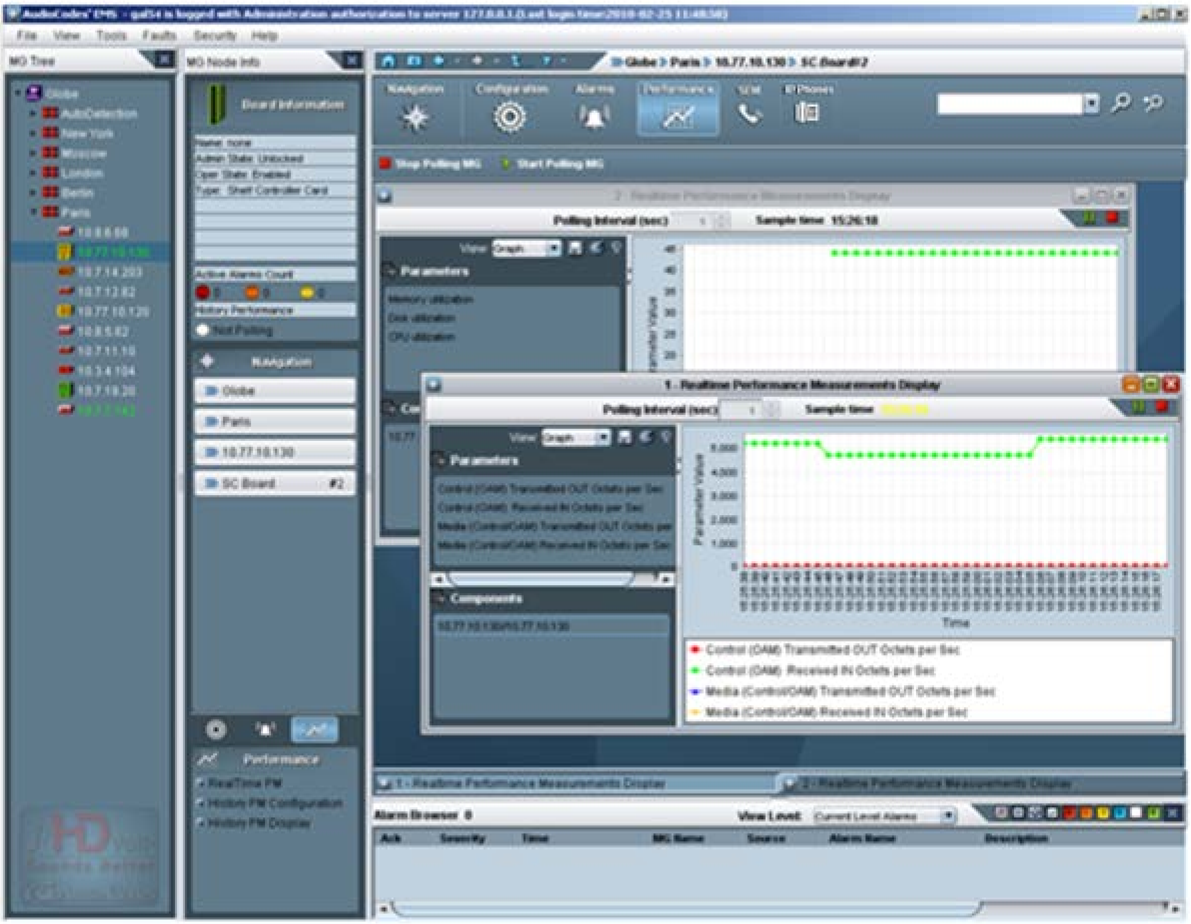
➢ To select an entity to poll:

1. Select the relevant device entity for which you wish to display Real Time PMs.. For example, in the Navigation pane, navigate to the IP Group entity (**VoIP** > **VoIP Network** > **IP Groups**). In the IP Group table, select an IP Group and then select **RealTime PM**.
2. In the Realtime Performance Measurements Display window, select the **Parameters** icon; the IP Group Monitoring (Real-Time) window is displayed.
3. Select the parameters that you wish to poll and then click **OK**.
4. Click the Polling button (green arrow) to start polling.

   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.

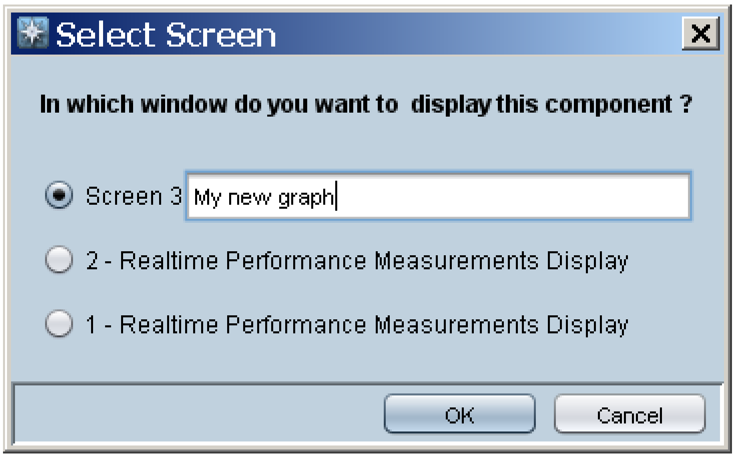
5. To define additional real-time performance monitoring windows, in the Performance pane, select **RealTime PM**.

Figure 32-4: Select Real-time Polling Entity



6. 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


Select Screen

In which window do you want to display this component ?

● Screen 3 My new graph

○ 2 - Realtime Performance Measurements Display

○ 1 - Realtime Performance Measurements Display

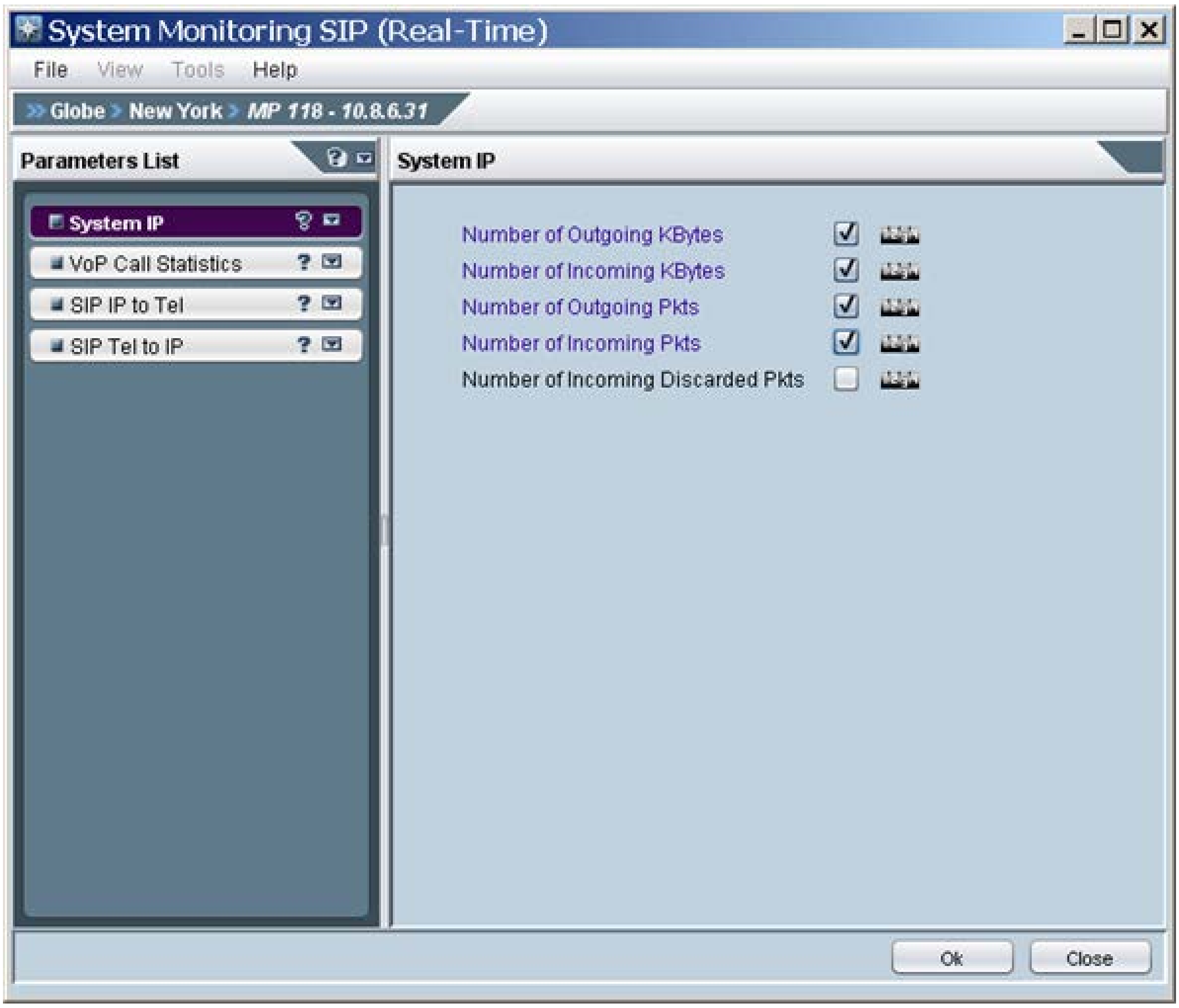
Users can open up to five separate real-time graphs in the same client application. There are two graph types that operators can use: Line Graph and Table View. In most cases, Line Graph is recommended when only a few parameters are compared. Table View is recommended when extensive data is displayed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

In each Line Graph, you can simultaneously view up to 10 parameters of the same entity (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

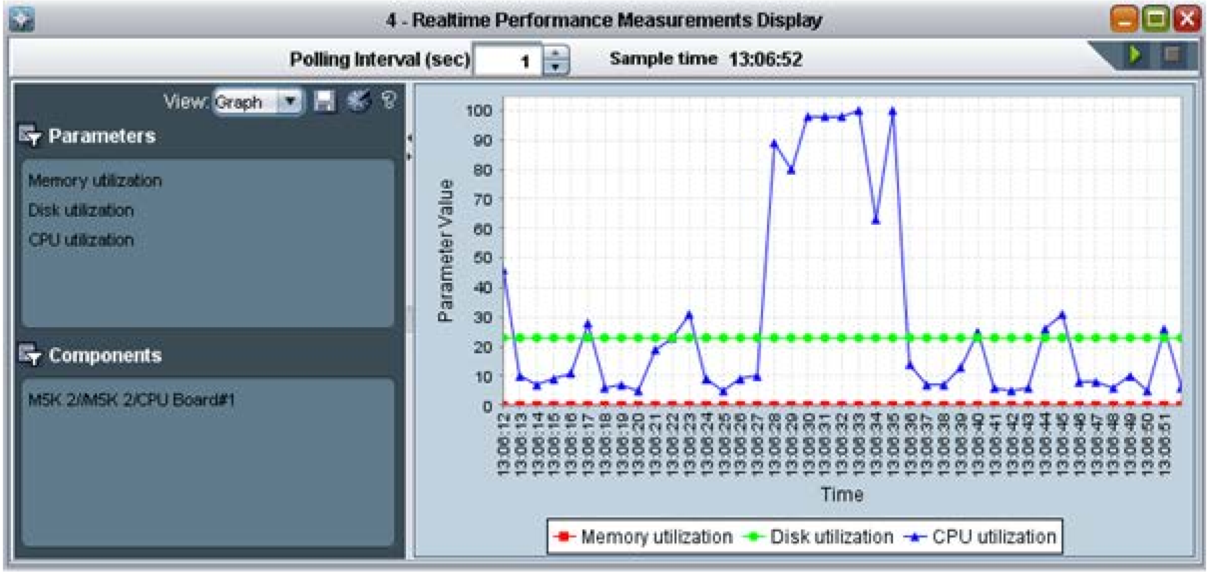


Number of Outgoing KBytes ☑
Number of Incoming KBytes ☑
Number of Outgoing Pkts ☑
Number of Incoming Pkts ☑
Number of Incoming Discarded Pkts □

In the screen 'Real-Time Performance Measurements Display' (refer to the figures below), choose the type of view (Graph or Table). Choose the Polling Interval you require from the drop-down under the title bar and click the Start button ▶ to start polling; a real-time graph or table is displayed. You can pause the polling by clicking the pause button ⏸ and restart it again by clicking the Start button. To stop polling, click the Stop button ■. You can view a color legend (below the graph) for entities / parameters. You can choose to save the graph as an image by clicking the Save button in the left pane. Historical data of the selected components and parameters can be viewed by clicking the 'History' button and then defining the History View. To view the Online Help, click the Help button.

In addition, you can apply Parameters or Components filters by clicking the filter button.

Figure 32-7: Graph Comparing CPU, Disk and Memory Utilization



4 - Realtime Performance Measurements Display

Polling Interval (sec) 1

Sample time 13:06:52

View: Graph

Parameters

- Memory utilization
- Disk utilization
- CPU utilization

Components

- M5K 2/M5K 2/CPU Board#1

In the screen 'Real-Time Performance Measurements Display' (refer to the figures below), choose the 'Polling Interval you require from the drop-down under the title bar and click the Start button ▶ to start polling; a real-time graph is displayed. At the bottom of the graph you can view a color legend for entities / parameters.

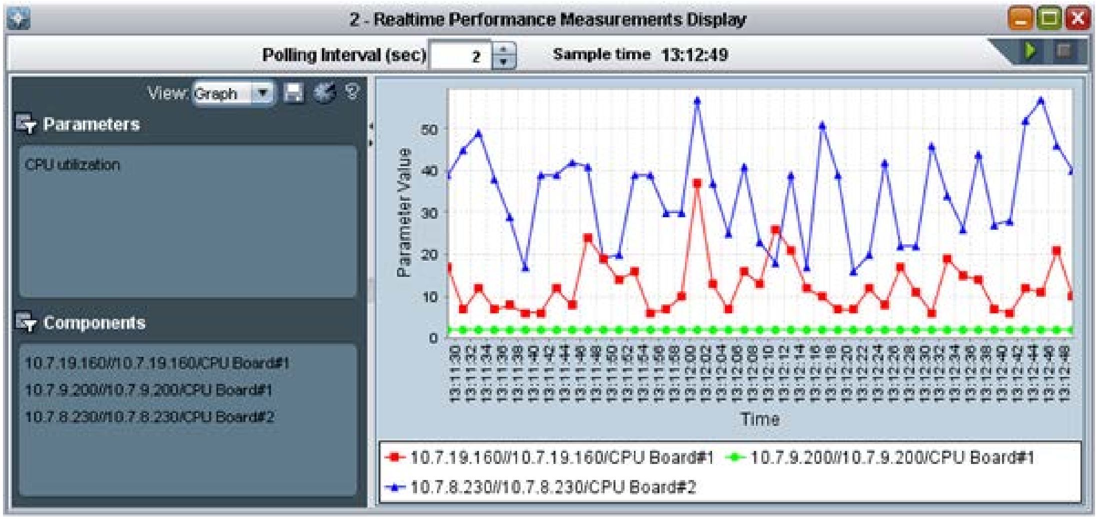
➢ To add / remove parameters / entities from the real-time graph or to change the polling interval:

- Stop the current graph, perform the required configuration changes and then restart the polling.

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

  The figures below show graphs depicting the following examples:

Figure 32-8: Realtime Performance Measurements Display-CPU Utilization



2 - Realtime Performance Measurements Display

Polling Interval (sec) 2 Sample time 13:12:49

View: Graph

Parameters

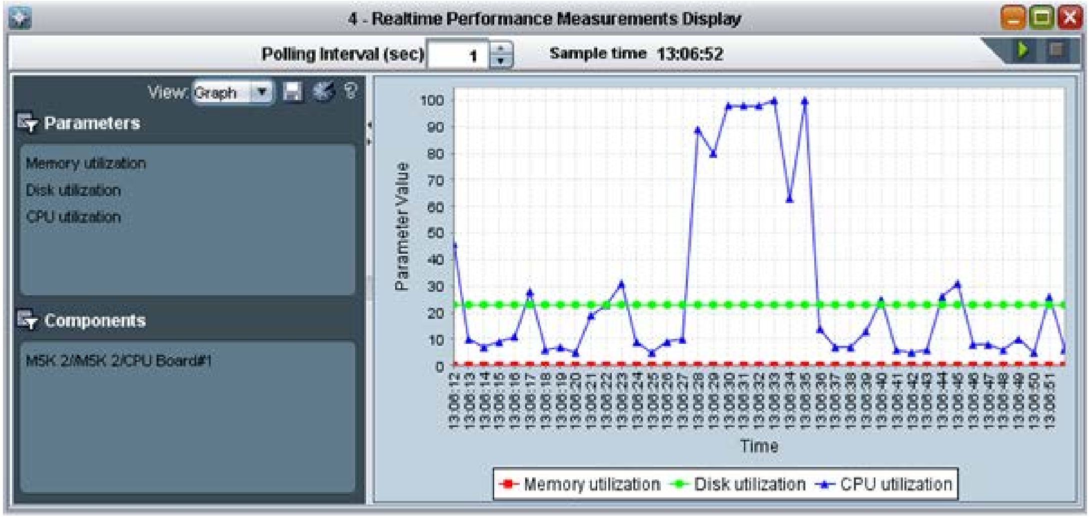
CPU utilization

Components

10.7.19.160//10.7.19.160/CPU Board#1
10.7.9.200//10.7.9.200/CPU Board#1
10.7.8.230//10.7.8.230/CPU Board#2

Parameter Value
0
10
20
30
40
50
13:11:30 … 13:12:48
Time
10.7.19.160//10.7.19.160/CPU Board#1
10.7.9.200//10.7.9.200/CPU Board#1
10.7.8.230//10.7.8.230/CPU Board#2

Figure 32-9: Realtime Performance Measurements Display-Memory, Disk and CPU Utilization



4 - Realtime Performance Measurements Display

Polling Interval (sec) 1 Sample time 13:06:52

View: Graph

Parameters

Memory utilization
Disk utilization
CPU utilization

Components

MSK 2//MSK 2/CPU Board#1

40.2 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 311 below.

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

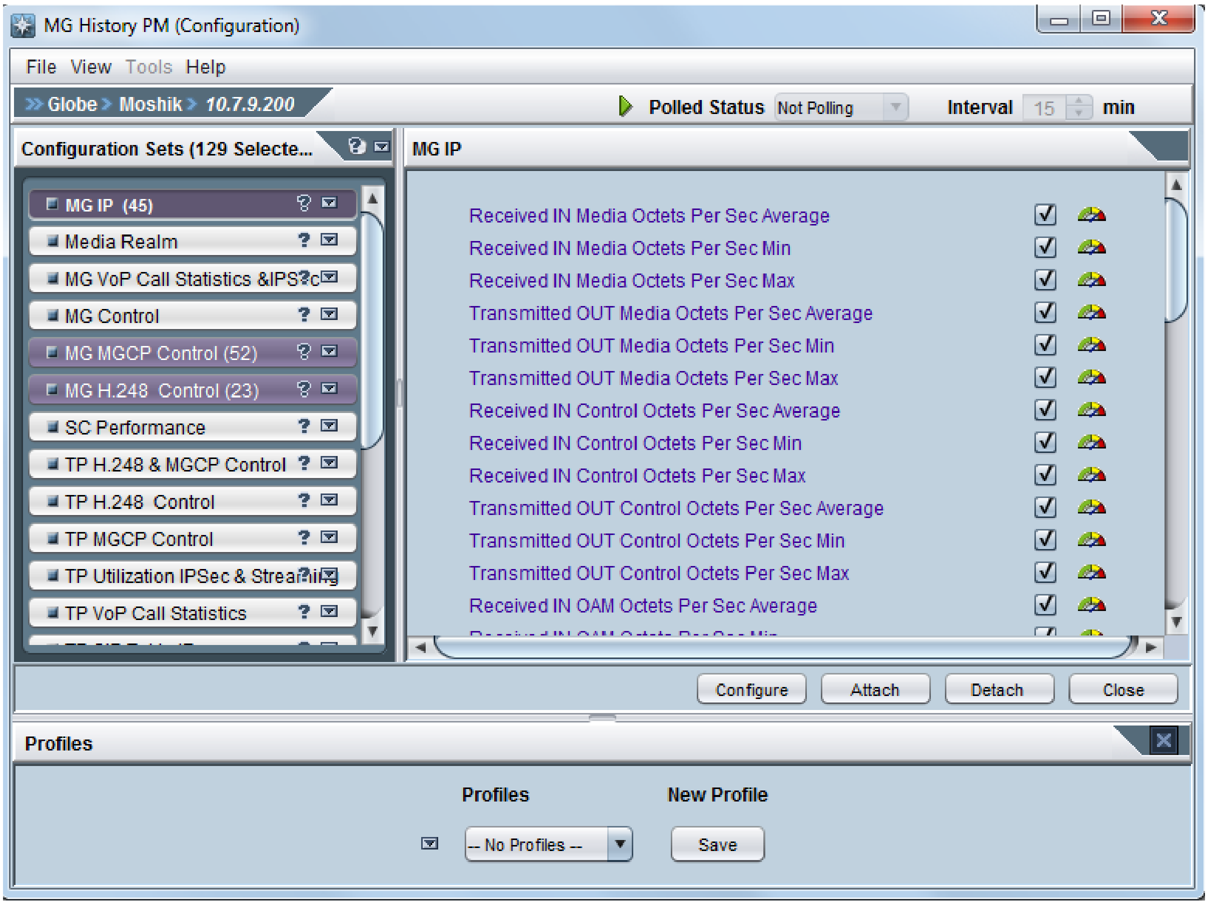
40.2.1 Configuring Background Monitoring

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.



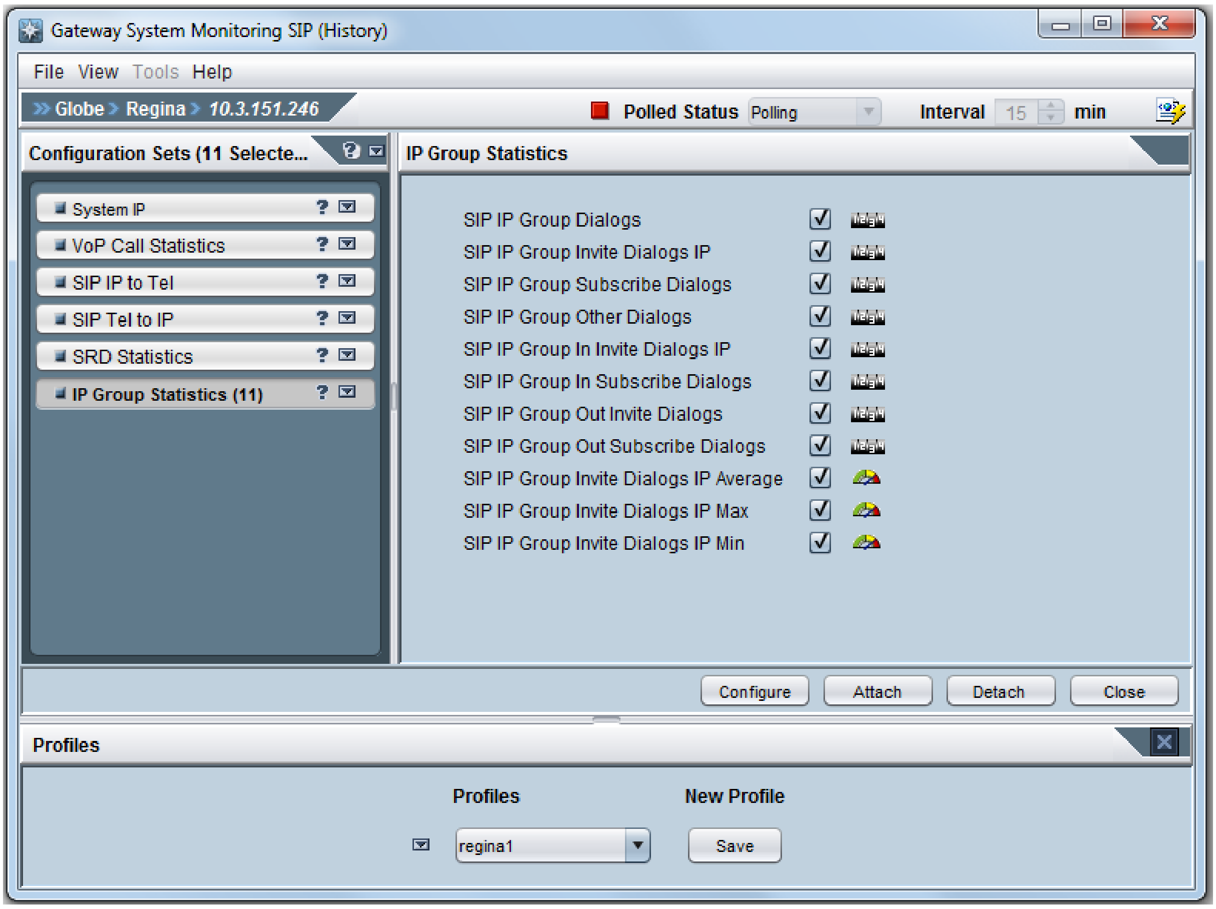
Polled Status: Not Polling

Interval: 15 min

Received IN Media Octets Per Sec Average ☑
Received IN Media Octets Per Sec Min ☑
Received IN Media Octets Per Sec Max ☑
Transmitted OUT Media Octets Per Sec Average ☑
Transmitted OUT Media Octets Per Sec Min ☑
Transmitted OUT Media Octets Per Sec Max ☑
Received IN Control Octets Per Sec Average ☑
Received IN Control Octets Per Sec Min ☑
Received IN Control Octets Per Sec Max ☑
Transmitted OUT Control Octets Per Sec Average ☑
Transmitted OUT Control Octets Per Sec Min ☑
Transmitted OUT Control Octets Per Sec Max ☑
Received IN OAM Octets Per Sec Average ☑
Received IN OAM Octets Per Sec Min

Profiles: -- No Profiles --

Figure 32-10: Gateway System Monitoring SIP (History)



SIP IP Group Dialogs	☑
SIP IP Group Invite Dialogs IP	☑
SIP IP Group Subscribe Dialogs	☑
SIP IP Group Other Dialogs	☑
SIP IP Group In Invite Dialogs IP	☑
SIP IP Group In Subscribe Dialogs	☑
SIP IP Group Out Invite Dialogs	☑
SIP IP Group Out Subscribe Dialogs	☑
SIP IP Group Invite Dialogs IP Average	☑
SIP IP Group Invite Dialogs IP Max	☑
SIP IP Group Invite Dialogs IP Min	☑

Profiles: regina1

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 start or to stop polling, click the **Polled Status** button.

Note: The Polling interval is 15 minutes and cannot be changed.

40.2.2 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. 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:

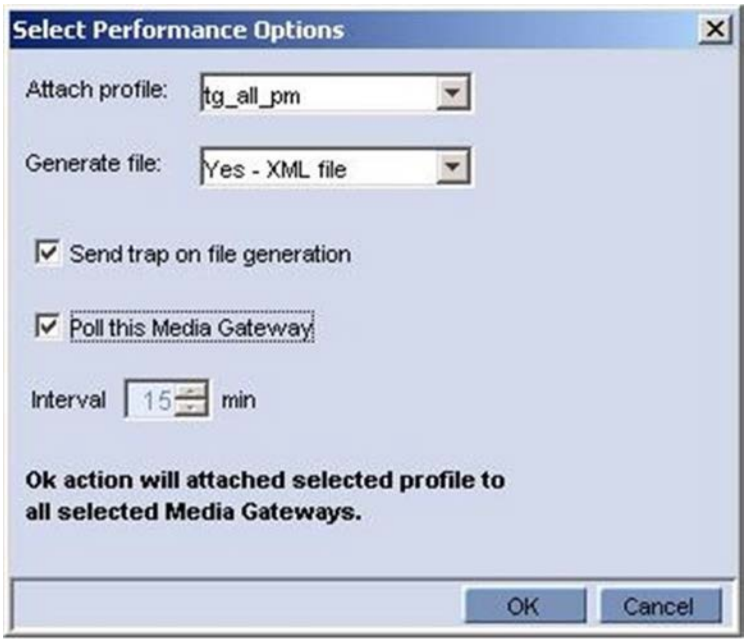
```
ACEMS/NBIF/pmFiles
```

Users should forward the trap to the NMS (Network Management System) (see Section 'Trap Forwarding to NB IF' on page 290).

➢ 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 32-11: Background Monitoring - Generate File Options



Attach profile: tg_all_pm

Generate file: Yes - XML file

☑ Send trap on file generation

☑ Poll this Media Gateway

Interval 15 min

Ok action will attached selected profile to all selected Media Gateways.

Notes: A performance data file cannot be created unless the device is polled (see Section 'Configuring Background Monitoring' on page 311.

- 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*.

40.2.3 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 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.

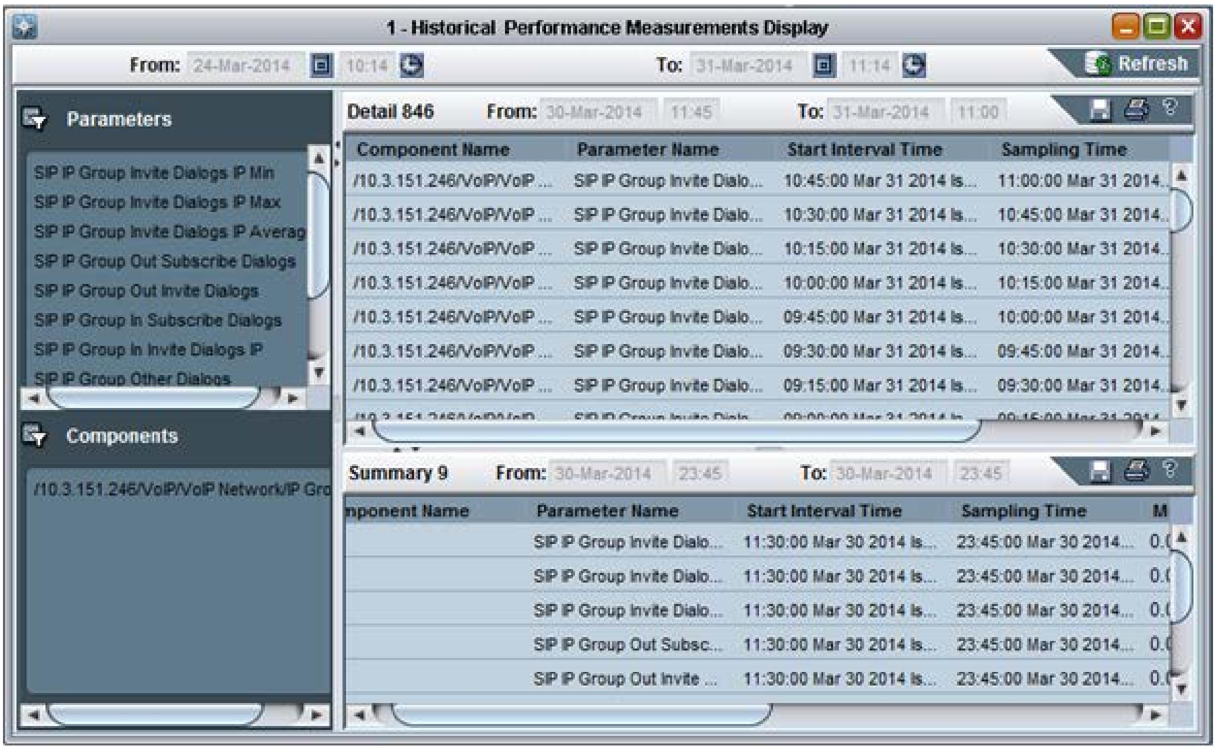
   Each time a sample is taken from the device, it is stored in the detailed table, where the entity name and index, parameter name, start, stop polling time and parameter value are specified.

   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.
   - **Sampling 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 32-12: Performance Monitoring - Historical Data



1 - Historical Performance Measurements Display

From: 24-Mar-2014 10:14 To: 31-Mar-2014 11:14 Refresh

Parameters

- SIP IP Group Invite Dialogs IP Min
- SIP IP Group Invite Dialogs IP Max
- SIP IP Group Invite Dialogs IP Averag
- SIP IP Group Out Subscribe Dialogs
- SIP IP Group Out Invite Dialogs
- SIP IP Group In Subscribe Dialogs
- SIP IP Group In Invite Dialogs IP
- SIP IP Group Other Dialogs

Components

- /10.3.151.246/VoIP/VoIP Network/IP Gro

Detail 846 From: 30-Mar-2014 11:45 To: 31-Mar-2014 11:00

Component Name	Parameter Name	Start Interval Time	Sampling Time
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:45:00 Mar 31 2014 Is...	11:00:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:30:00 Mar 31 2014 Is...	10:45:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:15:00 Mar 31 2014 Is...	10:30:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	10:00:00 Mar 31 2014 Is...	10:15:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:45:00 Mar 31 2014 Is...	10:00:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:30:00 Mar 31 2014 Is...	09:45:00 Mar 31 2014...
/10.3.151.246/VoIP/VoIP ...	SIP IP Group Invite Dialo...	09:15:00 Mar 31 2014 Is...	09:30:00 Mar 31 2014...

Summary 9 From: 30-Mar-2014 23:45 To: 30-Mar-2014 23:45

nponent Name	Parameter Name	Start Interval Time	Sampling Time	M
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Invite Dialo...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Out Subsc...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(
	SIP IP Group Out Invite ...	11:30:00 Mar 30 2014 Is...	23:45:00 Mar 30 2014...	0.(

It's possible to save selected data by clicking **Save** button 💾 on the right size of the History Data display. Data is saved in .csv file format.

40.2.4 Printing Historical Data PM Reports

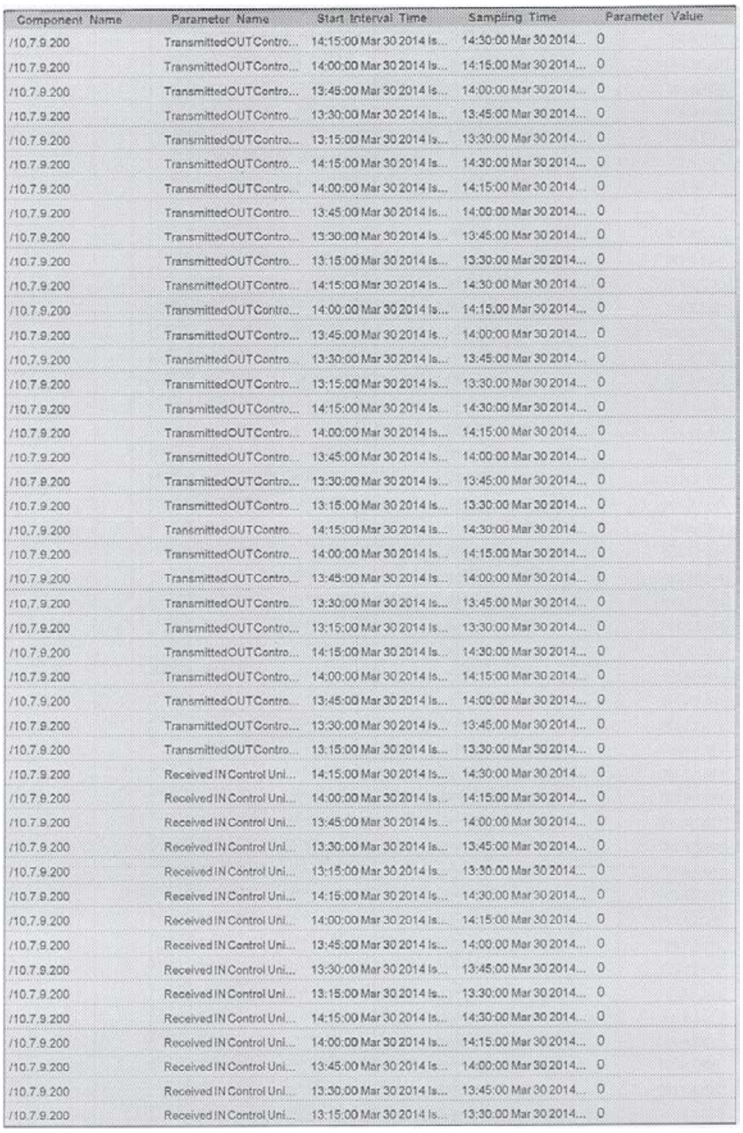
Once you view the sample polled data, you can also print the displayed data by clicking the **Print** icon.

➢ 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 32-13: 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	ReceivedINControl Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	14:15:00 Mar 30 2014 Is...	14:30:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	14:00:00 Mar 30 2014 Is...	14:15:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:45:00 Mar 30 2014 Is...	14:00:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:30:00 Mar 30 2014 Is...	13:45:00 Mar 30 2014...	0
/10.7.9.200	ReceivedINControl Uni...	13:15:00 Mar 30 2014 Is...	13:30:00 Mar 30 2014...	0

40.3 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.

40.3.1 Configuring Performance Monitoring Threshold Values for CPE Products

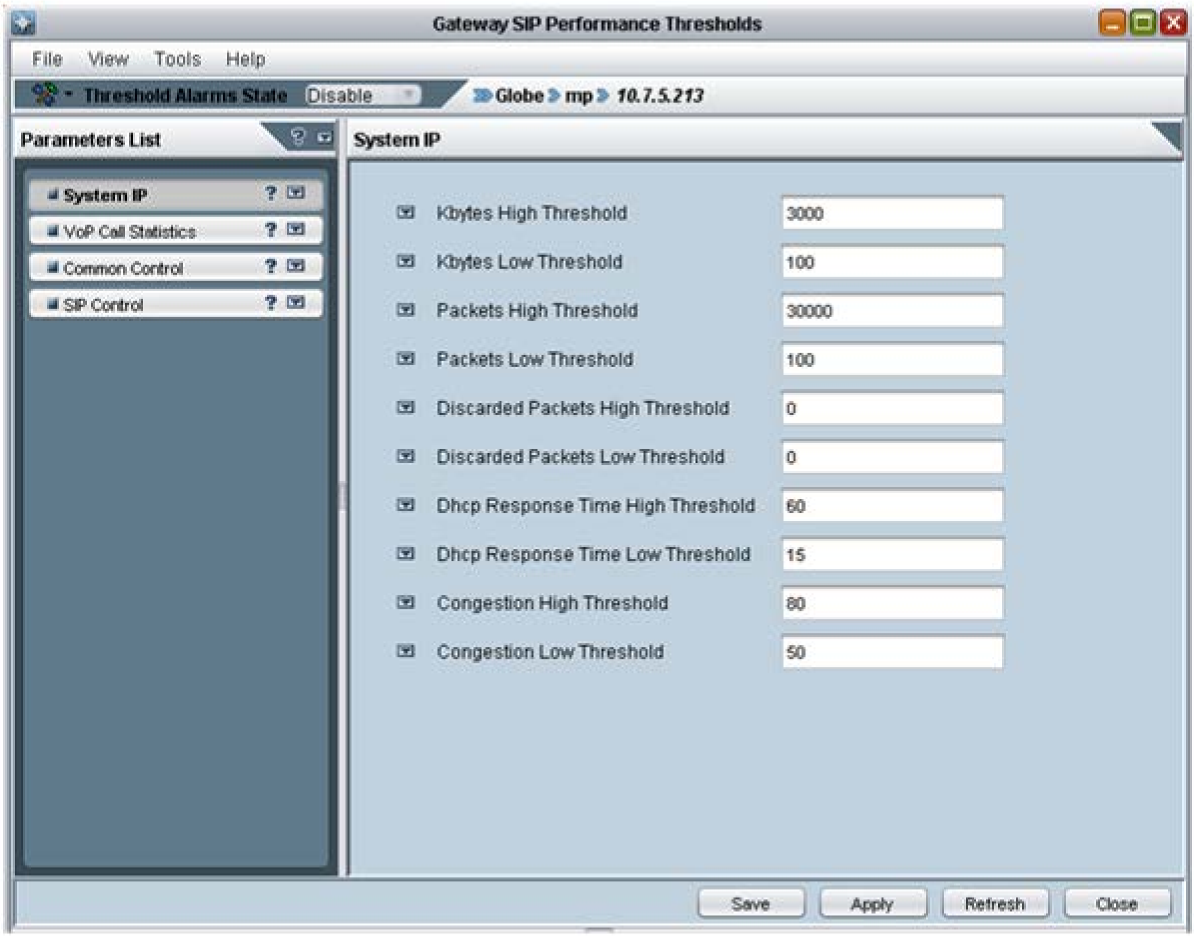
This section describes how to configure performance monitoring thresholds for CPE Products.

➢ **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 32-14: MediaPack Performance Thresholds



Kbytes High Threshold	3000
Kbytes Low Threshold	100
Packets High Threshold	30000
Packets Low Threshold	100
Discarded Packets High Threshold	0
Discarded Packets Low Threshold	0
Dhcp Response Time High Threshold	60
Dhcp Response Time Low Threshold	15
Congestion High Threshold	80
Congestion Low Threshold	50

3. To provision the required threshold parameters, click **Apply**.

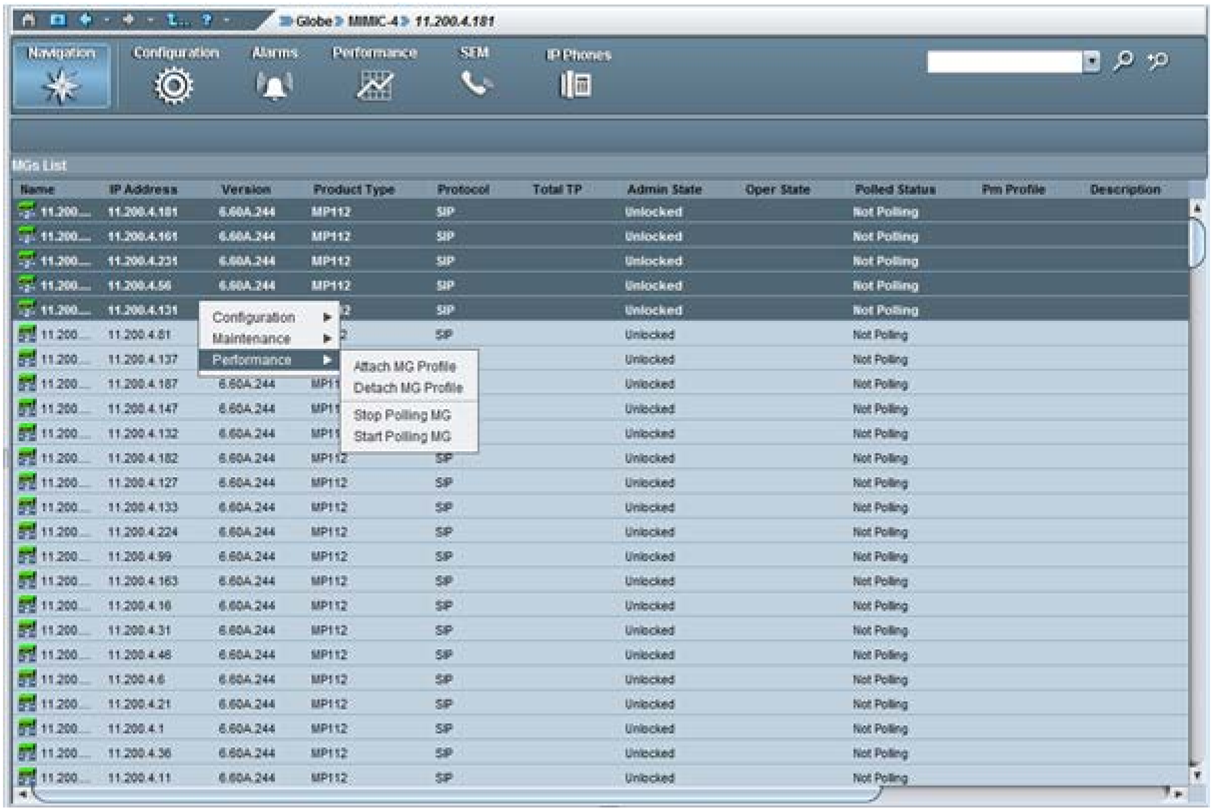
   If the 'Threshold Alarms State' parameter is Disabled, select the **Enable** option from the drop-down menu adjacent to the Maintenance icon.

   The 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.

40.4 Performance Monitoring Actions

This section describes performance monitoring actions on devices.

Figure 32-15: Performance Monitoring Actions on Devices



Name	IP Address	Version	Product Type	Protocol	Total TP	Admin State	Oper State	Polled Status	Pm Profile	Description
11.200....	11.200.4.181	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.161	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.231	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.56	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.131		2	SIP		Unlocked		Not Polling		
11.200....	11.200.4.81		2	SIP		Unlocked		Not Polling		
11.200....	11.200.4.137					Unlocked		Not Polling		
11.200....	11.200.4.187	6.60A.244	MP11			Unlocked		Not Polling		
11.200....	11.200.4.147	6.60A.244	MP11			Unlocked		Not Polling		
11.200....	11.200.4.132	6.60A.244	MP11			Unlocked		Not Polling		
11.200....	11.200.4.182	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.127	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.133	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.224	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.99	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.163	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.16	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.31	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.46	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.6	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.21	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.1	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.36	6.60A.244	MP112	SIP		Unlocked		Not Polling		
11.200....	11.200.4.11	6.60A.244	MP112	SIP		Unlocked		Not Polling		

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.

Part V

Security Management

This section describes the security features implemented on the EMS.

41 Overview

This section describes the following EMS Security Management features:

- HTTPS Network Communication Security (see Chapter 42)
- Enterprise Firewall (see Chapter 43)
- EMS Application Security (see Chapter 44).
- EMS User Activities Journal (see Chapter 45).
- EMS server machine (refer to the *EMS Server IO&M Manual*).
- Recent security patches installations.
- 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.

For more details, refer to the *OVOC Security Guidelines* document.

This page is intentionally left blank.

42 HTTPS Network Security

HTTPS Network communication between the EMS and its managed components is implemented for the following purposes:

- Installing and upgrading software
- Downloading auxiliary files
- Connecting to the device's embedded Web interface, the endpoints, the SEM interface, the IP Phone Manager interface and to the JAWS and NBIF clients.
- For REST communication between the EMS and devices and endpoints.

An HTTPS connection can be secured with the EMS server for the following OVOC client connections:

- The AudioCodes device (see Section 42.1)
- The EMS PC client (see Section 42.3)
- The JAWS client (see Section 42.3)
- The IP Phone Manager client (see Section 42.5)
- The SEM client (see Section 42.6)
- Active Directory (LDAP) and the EMS server (see Section 42.7)

Note: The above described connections can be secured using AudioCodes default self-signed certificates or using custom certificates. For detailed information on SSL certificate implementation, refer to the *OVOC Security Guidelines* document.

42.1 AudioCodes Device Connection

Securing the OVOC server and AudioCodes device connection over HTTPS is used for files upload/download and for Web Client Single-Sign On. To secure the connection between the EMS server and the device over HTTPS:

- Enable HTTPS ("Enable HTTPS Connection") when adding the device to the EMS (see Section 6.2.1 on page 81).
- Configure HTTPS on the AudioCodes device (refer to the *EMS Server IOM manual*).
- Secure the connection using the default AudioCodes self-signed certificate or load custom certificates to the EMS server (refer to the *EMS Server IOM* manual).

In addition, if you wish to work in Mutual Authentication mode:

- Set the HTTPS Authentication option “Set Mutual Authentication” using the EMS Server Manager (refer to the *EMS Server IOM*).
- Load certificates to the device (you must use the same root CA for signing the device certificate as is used for signing the certificate installed on the EMS server) (refer to 'Custom X.509 Certificates- Supplementary Procedures' in the *EMS Server IOM).*
- Configure HTTPS on the device (refer to 'Custom X.509 Certificates-Supplementary Procedures' in the *EMS Server IOM).*

42.1.1 Single Sign-On

The Single-Sign On is used to enable automatic login to the devices embedded Web server tool from the device's status screen in the EMS over HTTP/HTTPS. When you enable this connection (see Section 6.2.1), it is by default secured using the AudioCodes Self-Signed certificate.

If you wish to secure this connection using custom certificate files, then you can load these files using the “Certificate File” option in the Software Manager (see Chapter 4). When the certificate file is loaded using this method, the EMS server keystore file is updated. The custom certificate must be signed by the same root CA used by the AudioCodes device. In this scenario, the EMS authenticates the device before establishing the connection.

Note: Single Sign-on is supported for device versions 7.0 and later.

42.1.1.1 Single Sign-On for NAT Devices

When devices are located behind a NAT, you cannot automatically connect to these devices using the Single Sign-on feature and therefore must do the following to enable this feature:

1. In the device’s IP Interface table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**), configure the ‘OAMP interface’ with a static route.
2. In the NAT, configure a static route to the OAMP interface (configured above in Step 1) with port 443.

Note: If your network uses a DHCP server to obtain IP addresses for the devices automatically, then you can use the **Software Upgrade** action with the **Incremental INI** file option to perform configuration updates to the device. In this case, you cannot enable the Single Sign-on feature.

42.2 Upload and Download Actions

File upload and download actions are by default secured using the AudioCodes Self-Signed certificate. If you wish to secure these actions using custom certificate files, you need to install these files on the EMS server using the EMS Server Manager (refer to the *EMS Server IOM* manual).

Note: If you are using custom certificates, you must load theses certificate files using the "Server Certificates Update" procedure in the EMS Server Manager because this certificate installation updates a different file on the EMS server to the certificate installation method described in Section 42.1.1. Consequently, to secure both the Single-Sign On mechanism and upload/ download actions, you must perform both the actions described in this Section and in Section 42.1.1.

42.3 EMS Desktop PC Client

Connection between the EMS PC client and the EMS server is by default implemented over HTTPS using AudioCodes default self-signed certificate.

42.4 EMS JAWS Client

When you want to secure the JAWS Web page over HTTPS (secures Web page through port 443), you need to enable the option 'Enable IP Phone Manager Client JAWS and NBIF Secured Communication' in the EMS Server Manager (refer to Section 'Enable IP Phone Manager Client JAWS and NBIF Secured Communication' in the *EMS Server IOM*). This connection is then secured using the AudioCodes self-signed certificate.

You also need to update the Java Security level on your PC in order for the JAWS page to be accessible (relevant for both HTTP and HTTPS connections). Refer to Section 'Update the Java Security Level on PC' in the *EMS Server IOM*.

42.5 EMS for IP Phones Web Client

When you want to secure the IP Phone Manager Web page over HTTPS (secures Web page through port 443), you need to enable the option 'Enable IP Phone Manager Client JAWS and NBIF Secured Communication' in the EMS Server Manager (refer to Section 'Enable IP Phone Manager Client JAWS and NBIF Secured Communication' in the *EMS Server IOM)*. This connection is then secured using the AudioCodes self-signed certificate.This connection also serves for secure download of firmware and configuration files to the endpoints from the EMS server.

42.6 SEM Web Client

When you want to secure the SEM Web page over HTTPS (secures Web page through port 9400), you need to enable the option 'Enable SEM Client Secured Connection' in the EMS Server Manager (refer to Section 'Enable SEM Client Secured

Connection' in the *EMS Server IOM*). This connection is then secured using the AudioCodes self-signed certificate.

42.7 Securing EMS and Active Directory (LDAP) Connection

When you secure the connection with an Active Directory LDAP server over HTTPS using certificate authentication (see Section 44.3), then the certificate file can be installed on the EMS server using the “Certificate File” option in the Software Manager (see Chapter 4). When the certificate file is loaded using this method, the EMS server keystore is updated. In this scenario, the EMS authenticates the LDAP server before establishing the connection.

42.8 Securing EMS and Endpoints Connection

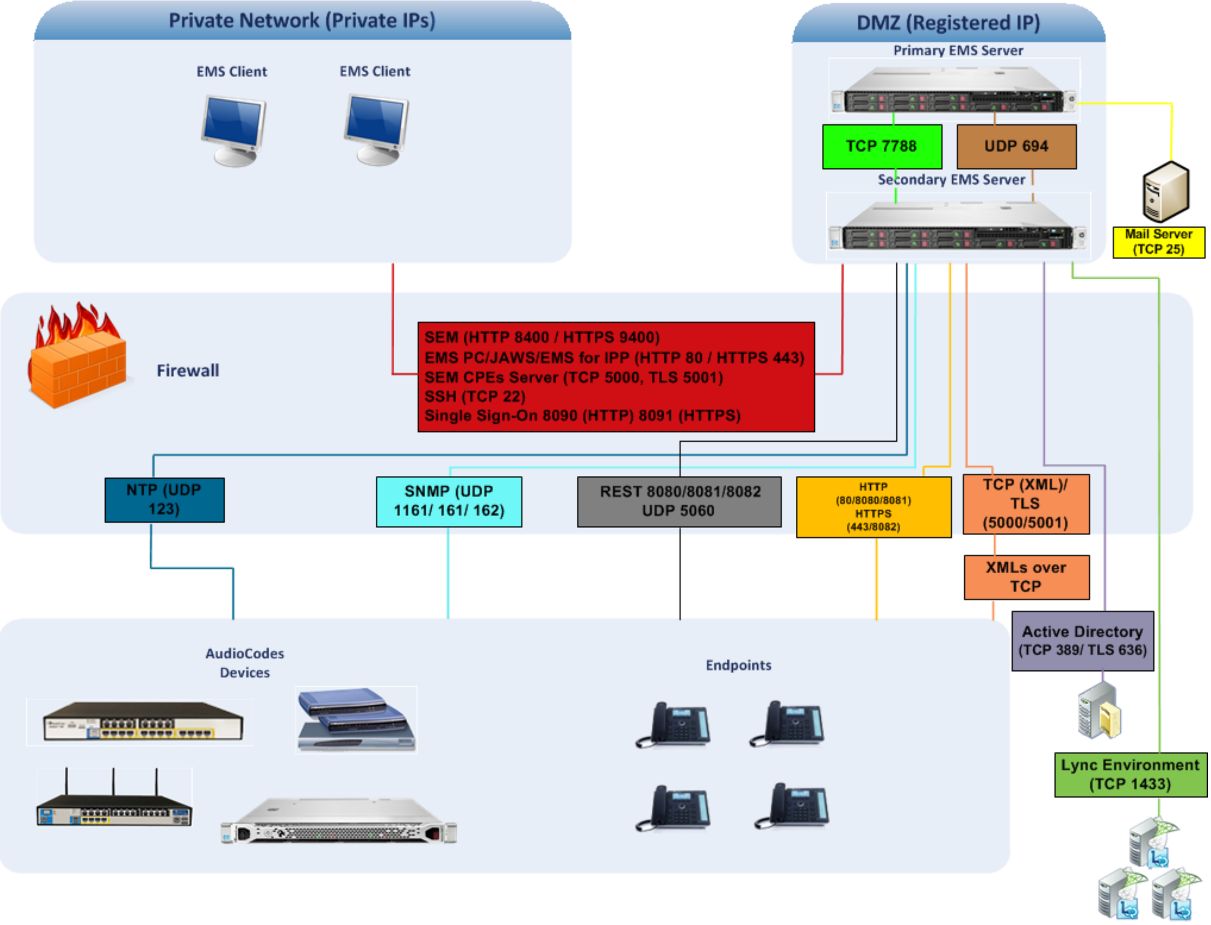
The HTTPS REST connection (for sending alarms, alerts and statuses) from the endpoints to the EMS server) is secured through port 8082 (open by default, refer to Section ‘Endpoint Connection Processes' in the EMS Server IOM). However, to fully enable this connection, you need to enable the option “Send Secure HTTPS to the IPP” in the System Settings page in the IP Phone Management Server. This connection is then secured (encryption only without SSL authentication) using the AudioCodes self-signed certificate.

43 Enterprise Firewall

The EMS interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. You need to define rules in your Enterprise firewall to manage the secure communications for all OVOC client processes that connect to the OVOC server. Each of these processes use different communication ports which should be secured appropriately.

By default, all ports are open on the OVOC server side. When installing the OVOC server, you need to configure its network and open the ports in your Enterprise LAN according to your site requirements; based on the firewall configuration rules (representing these port connections) that are described in the table below. For more information, refer to the *EMS Server IOM* manual.

Figure 34-1: EMS Firewall Configuration Schema


Private Network (Private IPs)
EMS Client
EMS Client
DMZ (Registered IP)
Primary EMS Server
TCP 7788
UDP 694
Secondary EMS Server
Mail Server (TCP 25)
Firewall
SEM (HTTP 8400 / HTTPS 9400)
EMS PC/JAWS/EMS for IPP (HTTP 80 / HTTPS 443)
SEM CPEs Server (TCP 5000, TLS 5001)
SSH (TCP 22)
Single Sign-On 8090 (HTTP) 8091 (HTTPS)
NTP (UDP 123)
SNMP (UDP 1161/ 161/ 162)
REST 8080/8081/8082 UDP 5060
HTTP (80/8080/8081) HTTPS (443/8082)
TCP (XML)/ TLS (5000/5001)
XMLs over TCP
Active Directory (TCP 389/ TLS 636)
Lync Environment (TCP 1433)
AudioCodes Devices
Endpoints

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

This page is intentionally left blank.

44 EMS Application Security

EMS Operator's can either be managed locally in the EMS database (default), or by using a centralized database on either a RADIUS or LDAP Active Directory platform.

Note:

- By default, the EMS application manages its users in the local EMS server, However, it is *recommended* to implement a third-party LDAP server or RADIUS server in your network for authenticating and authorizing the EMS/SEM management users (Web and CLI). Consequently, you should only implement local user management when you do not have a LDAP or RADIUS authentication server in your network.
- You must initially connect to the EMS using the default user 'acems'. Once you have successfully connected with the 'acems' user, you can then change the authentication and authorization settings to RADIUS or LDAP.
- Multi-tenancy with regions is not supported for RADIUS and LDAP users.

These options are described as follows:

- Centralized User Management using either an RADIUS or LDAP Active Directory authentication server:

  Users are managed in an LDAP-compliant server such as Microsoft Active Directory (AD) or a RADIUS server. When a user attempts to log in to the EMS, the EMS server verifies the login username and password with the AD server or RADIUS sever.

  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 for these users (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:

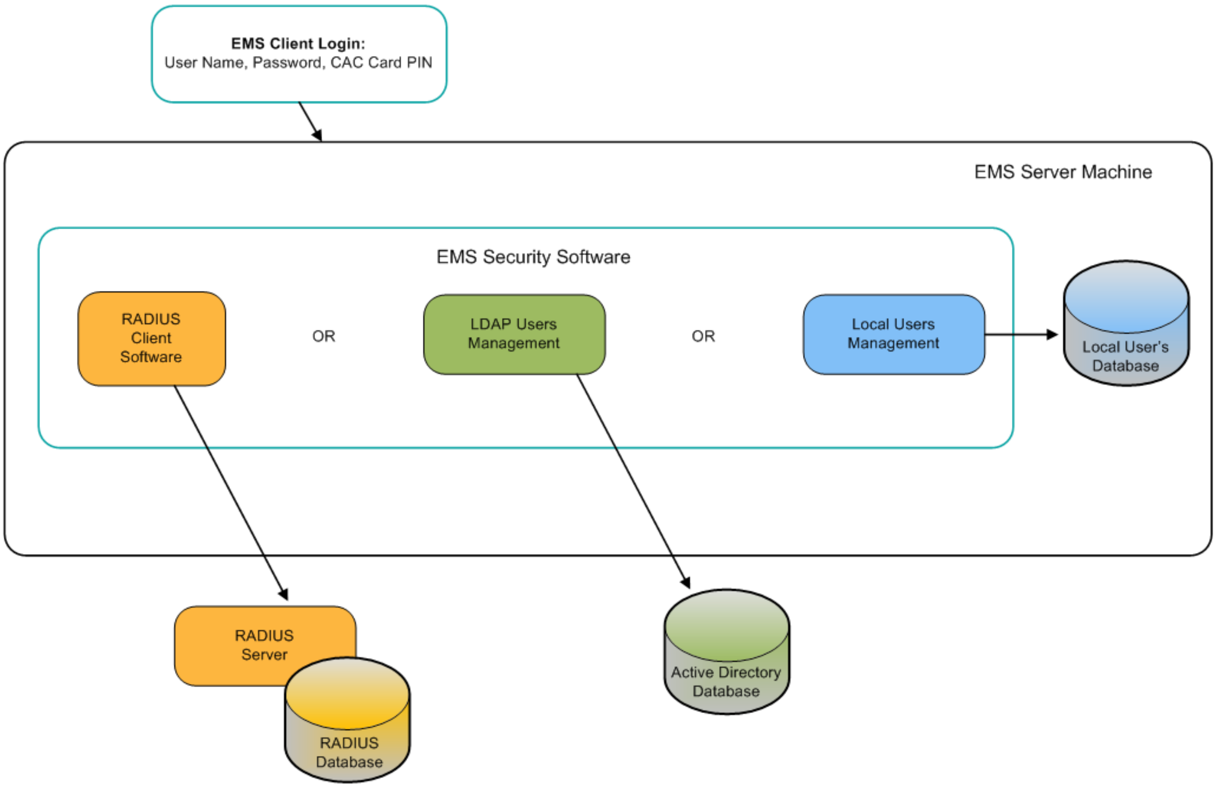
  - Remote Authentication Dial-In User Service (RADIUS) (see Section 35.2.1 on page 350).
  - Lightweight Directory Access Protocol (LDAP) server (see Section 35.2.3 on page 353).

- Local User Management:

  Users are managed in a local EMS database (where the users and passwords are saved in the EMS database) and can be managed from the Users List. See Section 44.1.

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).

44.1 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 in the EMS can be performed by the user with the Administrator security level.

The local EMS user's management feature enables the operator with the Administrator security level to exert control over other operators' access to system resources. This ensures that sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators. In addition, the Administrator can set different user permissions for different regions. This feature has been implemented for Enterprise and Service provider environments that 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.

44.1.1 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.

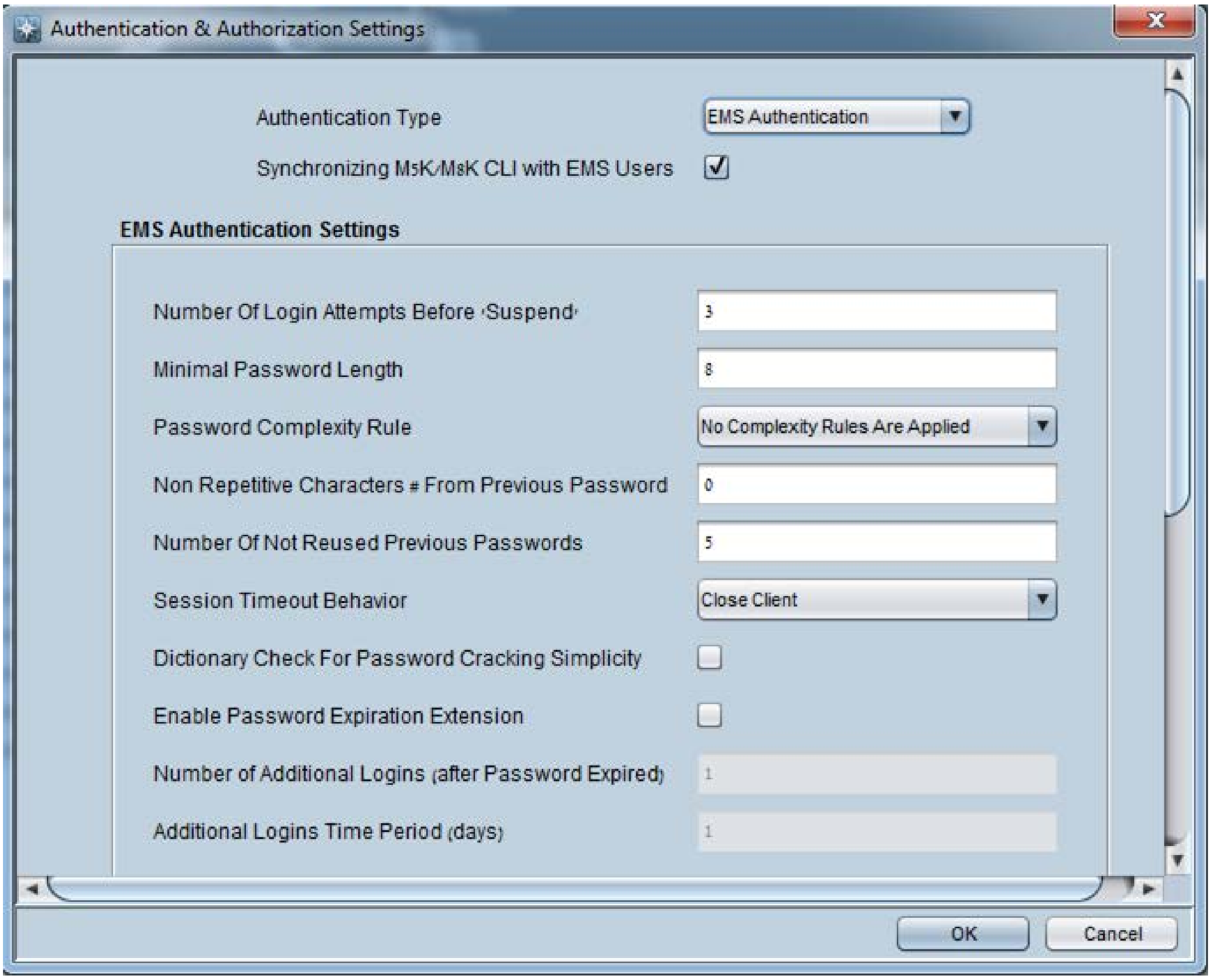
44.1.2 EMS User Global Authentication Settings

This section describes how to set the global authentication settings for all EMS users.

➢ **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 35-2: EMS Authentication Settings



Authentication Type: EMS Authentication ▼

Synchronizing M5K/M8K CLI with EMS Users ☑

EMS Authentication Settings

Number Of Login Attempts Before 'Suspend'	3
Minimal Password Length	8
Password Complexity Rule	No Complexity Rules Are Applied ▼
Non Repetitive Characters # From Previous Password	0
Number Of Not Reused Previous Passwords	5
Session Timeout Behavior	Close Client ▼
Dictionary Check For Password Cracking Simplicity	□
Enable Password Expiration Extension	□
Number of Additional Logins (after Password Expired)	1
Additional Logins Time Period (days)	1

44.1.2.1 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 Suspend:** 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.

44.1.2.2 Session Timeout Behavior

The Session Timeout behavior determines whether to close the client session or force the user to reenter their password whenever the "Session Timeout Period (Minutes)" or "Session Leasing Timeout (Hours)" settings expire (see Section 44.1.7.3).

➢ **To set session timeout behavior:**

- From the "Session Timeout Behavior" drop-down list, select one of the following actions:
  - **Close Client:** closes the current EMS client session.
  - **Lock Client:** forces the user to reenter their password to access the application.

44.1.2.3 Provisioning Password Expiration Extension Period

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

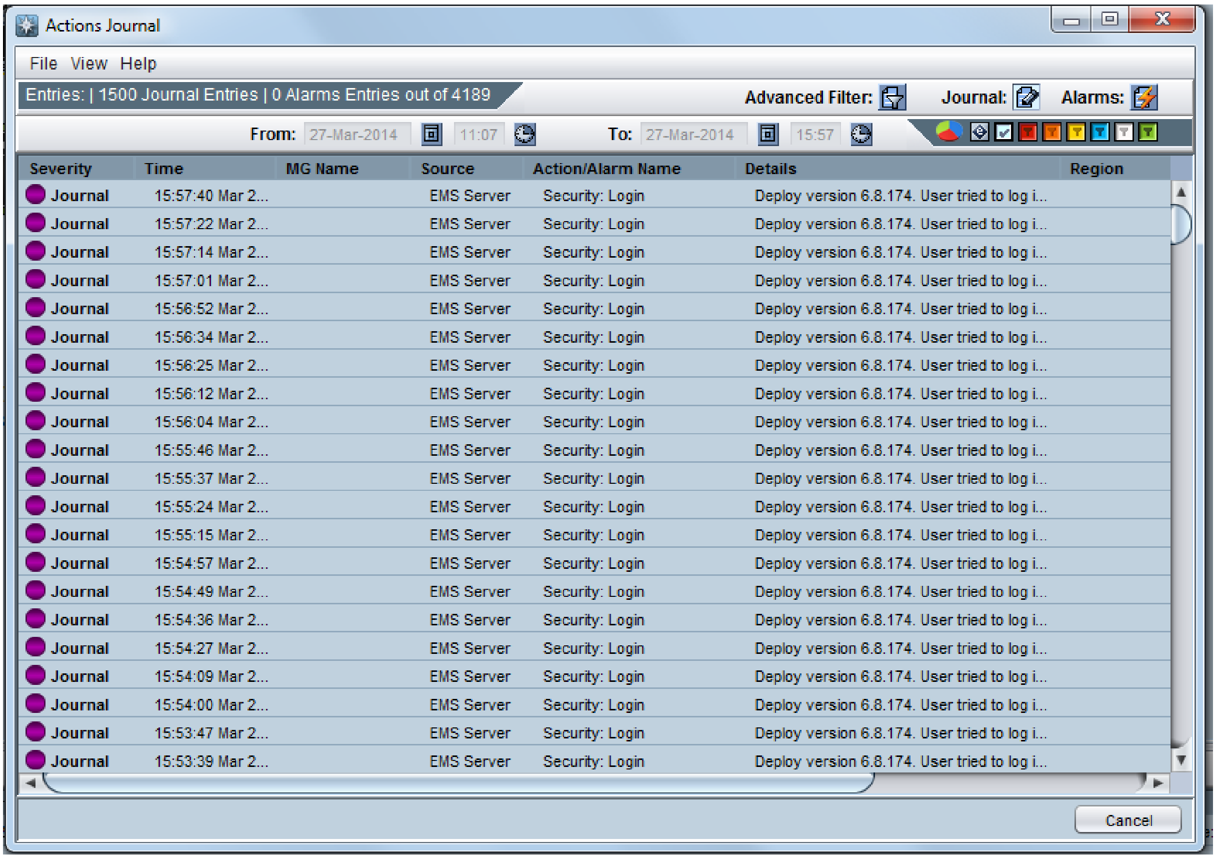
➢ **To provision password expiration extension period:**

1. In the Authorization and Authentication Settings window, select the "Enable Password Expiration Extension" checkbox, and set the following parameters:
   - **Number of Additional Logins:** defines the number of logins user can perform after his password already expired. Valid range: 1-10. Default: disabled.
   - 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.

44.1.3 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 357.

Figure 35-3: Actions Journal-Security Items



Entries: | 1500 Journal Entries | 0 Alarms Entries out of 4189

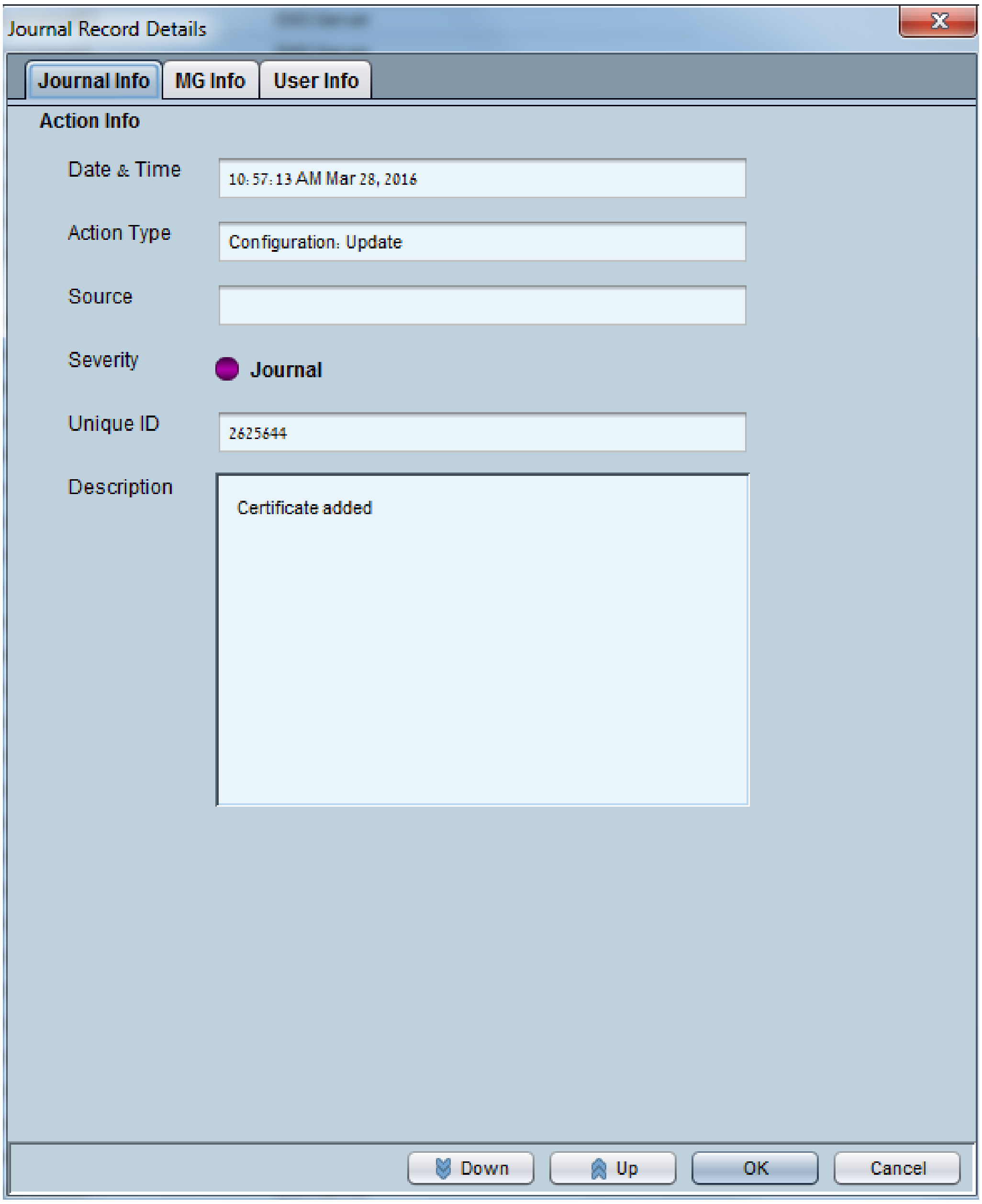
Advanced Filter: Journal: Alarms:

From: 27-Mar-2014 11:07 To: 27-Mar-2014 15:57

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region
Journal	15:57:40 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:22 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:14 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:57:01 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:52 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:34 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:25 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:12 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:56:04 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:46 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:37 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:24 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:55:15 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:57 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:49 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:36 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:27 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:09 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:54:00 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:53:47 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	
Journal	15:53:39 Mar 2...		EMS Server	Security: Login	Deploy version 6.8.174. User tried to log i...	

When a certificate file is loaded to the EMS server using the "Certificate File" option in the EMS Software Manager, the following journal entry is displayed:

Figure 35-4: Certificate File Added



Action Info

Date & Time: 10:57:13 AM Mar 28, 2016

Action Type: Configuration: Update

Source:

Severity: ● Journal

Unique ID: 2625644

Description: Certificate added

44.1.4 Managing the Users List

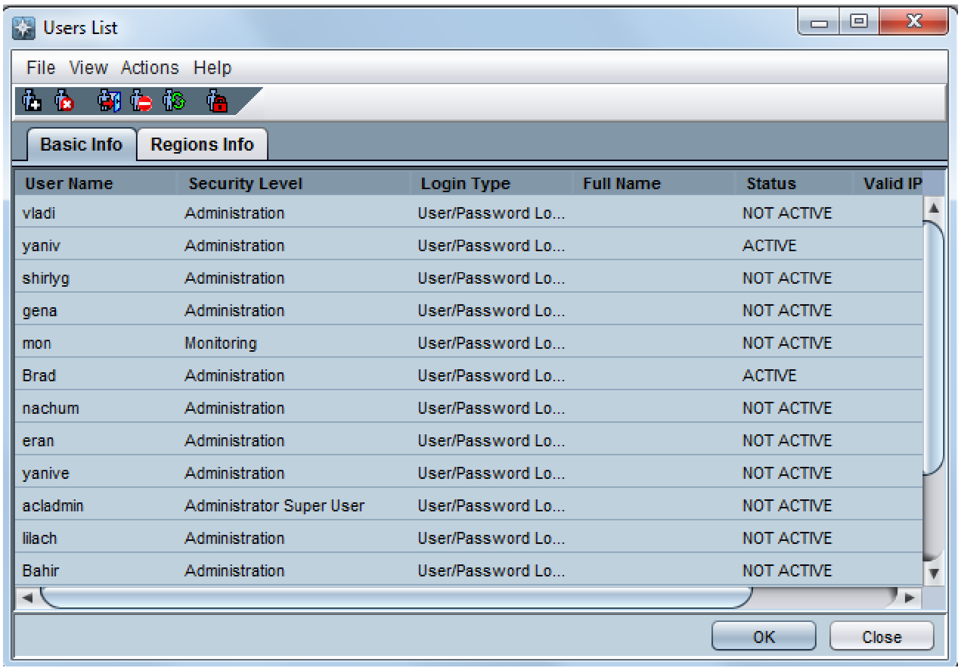
This section describes how to access the EMS Users list. User security level can be defined either per entire application or per Region.

Note: The User's list is used for managing user's in the local EMS database. Therefore, this section is not relevant for users that are managed on the RADIUS or LDAP servers.

➢ **To open the Users List:**

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

Figure 35-5: Users List



User Name	Security Level	Login Type	Full Name	Status	Valid IP
vladi	Administration	User/Password Lo...		NOT ACTIVE	
yaniv	Administration	User/Password Lo...		ACTIVE	
shirlyg	Administration	User/Password Lo...		NOT ACTIVE	
gena	Administration	User/Password Lo...		NOT ACTIVE	
mon	Monitoring	User/Password Lo...		NOT ACTIVE	
Brad	Administration	User/Password Lo...		ACTIVE	
nachum	Administration	User/Password Lo...		NOT ACTIVE	
eran	Administration	User/Password Lo...		NOT ACTIVE	
yanive	Administration	User/Password Lo...		NOT ACTIVE	
acladmin	Administrator Super User	User/Password Lo...		NOT ACTIVE	
lilach	Administration	User/Password Lo...		NOT ACTIVE	
Bahir	Administration	User/Password Lo...		NOT ACTIVE	

The EMS application supports 25 concurrent (active) EMS users. In the Users List screen (displayed in the above figure) you can do the following:

- View the list of operators defined in the EMS system
- View each user's status:
  - **Active** (the user is currently connected to the EMS application)
  - **Not Active** (the user is not connected to the EMS application)
  - **Suspended** (the user was suspended by the Administrator; double-click the row of the user for more details).
  - **Automatically Suspended** (the user was automatically suspended by the EMS system. This occurs when a user exceeds the maximum number of allowed login attempts (3). An operator with Administration security level is automatically released from suspension after 1 hour. An operator with Monitoring or Operation security level will require manual release by the Administrator).
- View Login type:
  - **User / Password User** – the user should identify themselves by typing user / password in the Login Frame.
  - **CAC User** – the user is identified using the CAC card and by 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.

44.1.5 User Details

When you select and double-click a user, the User Details screen is displayed. This screen is divided into the following tabs:

- **Basic Info:** includes configuration of basic user information and security settings. See Section 44.1.7.1.
- **Advanced Info:** includes configuration of advanced account and password settings. See Section 44.1.7.3.
- **Region Info:** includes configuration of the security permissions for each region. See Section 44.1.7.4.

44.1.6 User 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.

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 devices between regions.
- Provision Trap Forwarding Rules
- View system alarms in the Alarms Browser. For example, 'Disk Space' alarm, 'EMS Server Started' or 'Security Event' alarm.

Note:

- The above actions are not supported at the Regions level.
- Only users with "Admin" or "SuperAdmin" security levels can view system alarms in the Alarms Browser.
- Users with" Operator and Monitoring" security levels can view alarms for devices in their managed Region. For example, 'Topology event', 'Proxy Connection Lost' and 'GW Connection Alarm'.

44.1.7 Adding an Operator

This section describes how to add an EMS Operator.

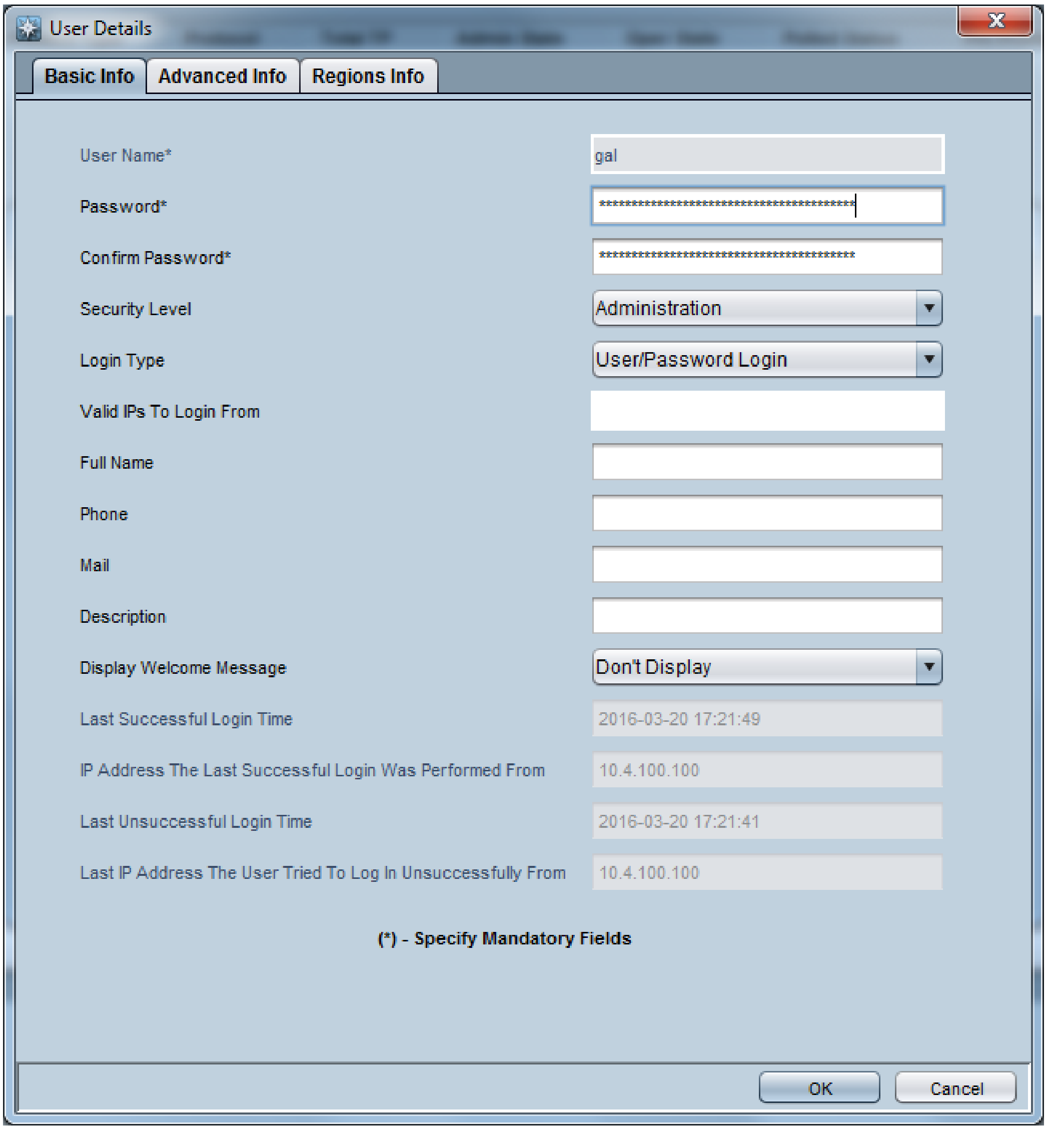
➢ **To add an operator, do one of the following:**

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

  -OR-

- Click the button **Add User** on the Users List toolbar; the User Details screen (**Basic Info** tab) opens.

Figure 35-6: User Details screen - Basic Info



User Name* gal

Password* **

Confirm Password* **

Security Level Administration

Login Type User/Password Login

Valid IPs To Login From

Full Name

Phone

Mail

Description

Display Welcome Message Don't Display

Last Successful Login Time 2016-03-20 17:21:49

IP Address The Last Successful Login Was Performed From 10.4.100.100

Last Unsuccessful Login Time 2016-03-20 17:21:41

Last IP Address The User Tried To Log In Unsuccessfully From 10.4.100.100

(*) - Specify Mandatory Fields

- 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 323, 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.

44.1.7.1 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:** See Section 44.1.6.
- **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.

44.1.7.2 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

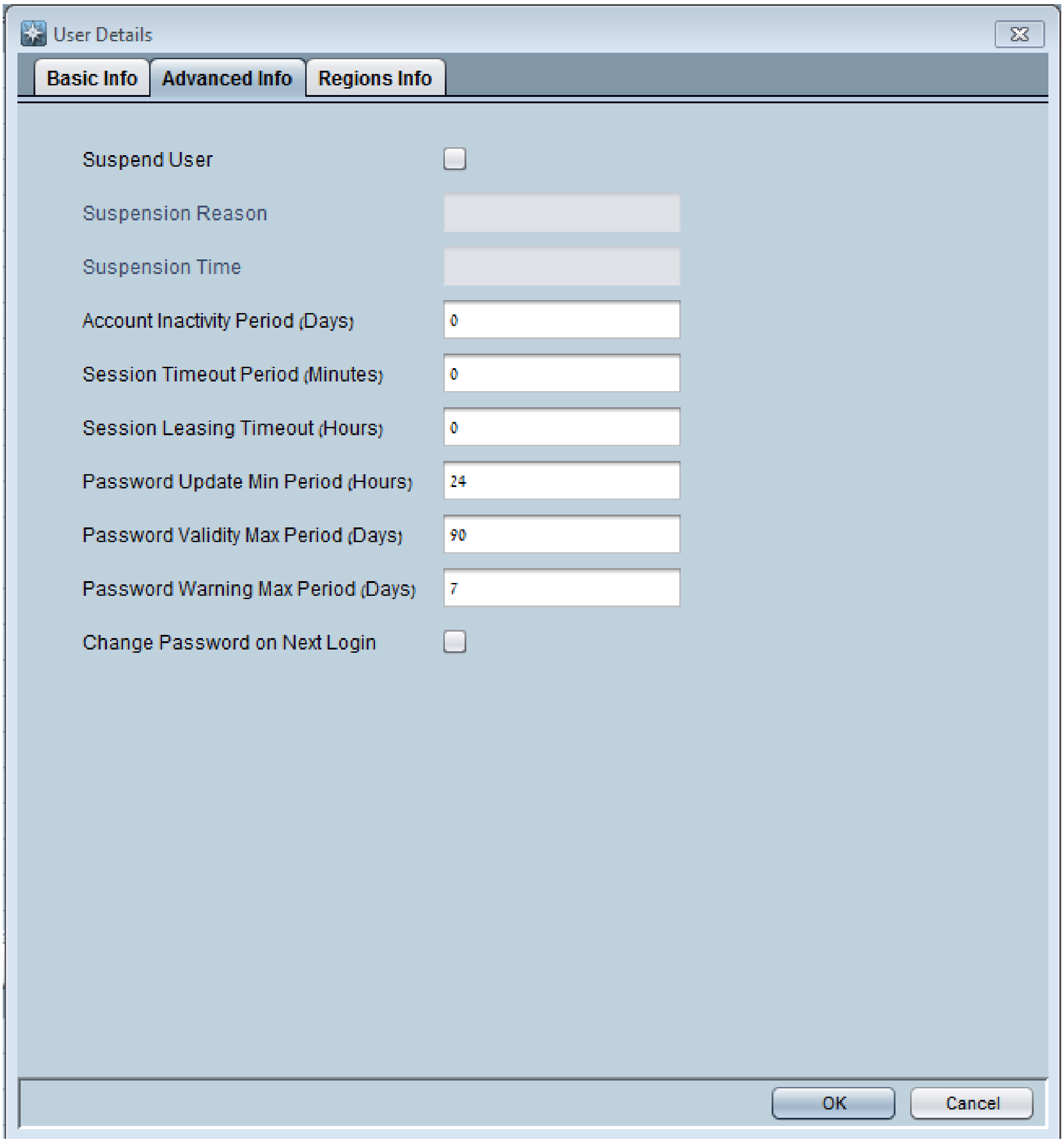
Welcome Message Options	Don't Display	Display	Display without Login Information
Mandatory	Welcome Message	Welcome Message + Login Information	Welcome Message

Welcome Message Options	Don't Display	Display	Display without Login Information
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.

44.1.7.3 Advanced Info

Figure 35-7: User Details screen - Advanced Info



Suspend User □

Suspension Reason

Suspension Time

Account Inactivity Period (Days) 0

Session Timeout Period (Minutes) 0

Session Leasing Timeout (Hours) 0

Password Update Min Period (Hours) 24

Password Validity Max Period (Days) 90

Password Warning Max Period (Days) 7

Change Password on Next Login □

- **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 has not logged into the EMS application for 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 days.
  - **Session Timeout Period (Minutes):** After the defined period of inactivity time if the user has not used the application (didn't execute any mouse or keyboard actions), the application will either be “Locked” or be “Closed” according to “Session Timeout Behavior” (see Section 44.1.2.2). This parameter applies to EMS and SEM users. Default value= 0
  - **Session Leasing Timeout (Hours):** After a defined period of time from the time of the Login, the application will either be “Locked” or be “Closed” according to "Session Timeout Behavior” (see Section 44.1.2.2). Default value= 0
- **Password Settings:**
  - **Password Update Min Period (Hours):** A user password cannot be changed more than once within the time specified by this parameter. Default-24 hours.
  - **Password Validity Max 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.
  - **Change Password on 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.

44.1.7.4 Regions Info

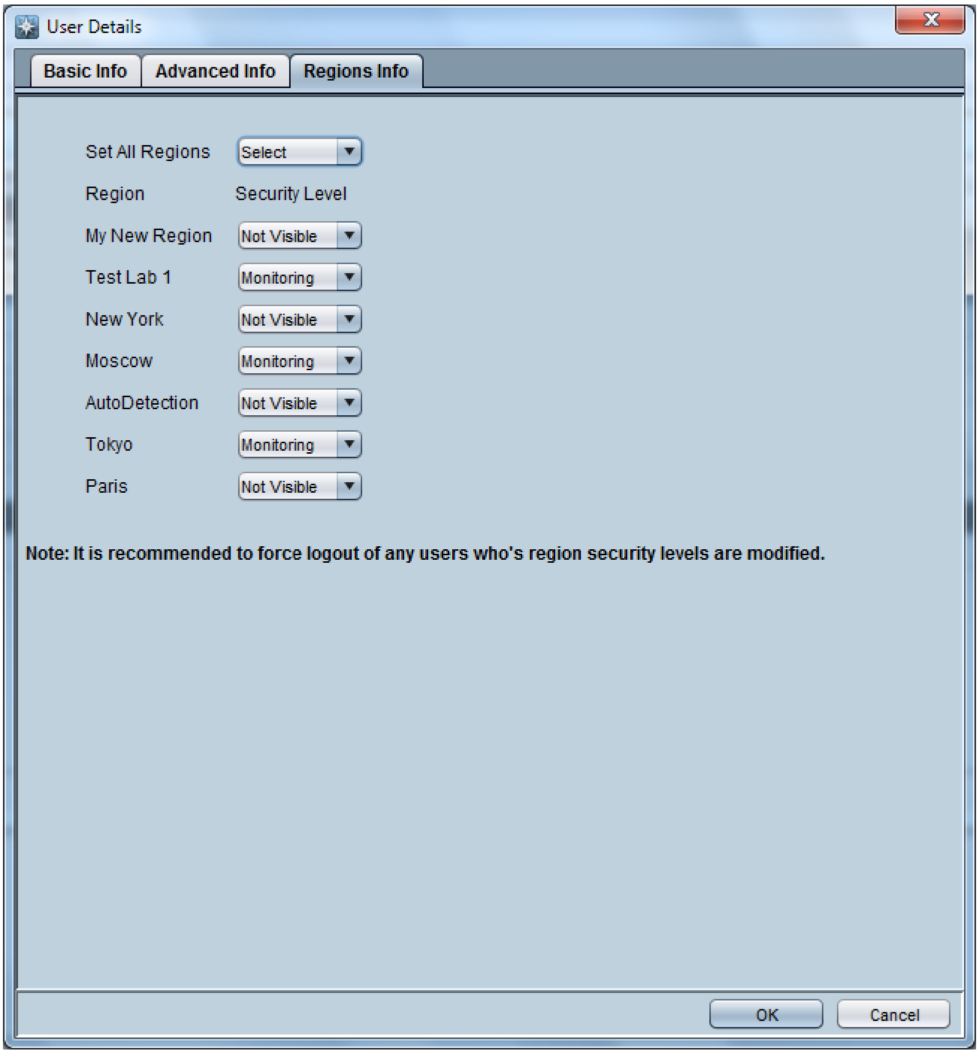
- The **Regions Info** tab includes the currently defined regions in the EMS and the security level for each region. The security level can be defined per region only for users with the following security permissions:
  - **Operator (read-write):** Perform any actions and/or provisioning changes on all 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.

Note:

- You cannot define the 'Super-Admin' & 'Admin' levels security level per region, since these users are system level users.
- A user cannot be assigned a higher security level in the Region Info settings than is set for this user's "Security Level"in the Basic Info settings.
- A user that is configured with Security Level "Monitoring" in the Basic Info settings cannot be assigned with "Operator" permissions for any region.

Figure 35-8: User Details - Regions Info



Set All Regions	Select
Region	Security Level
My New Region	Not Visible
Test Lab 1	Monitoring
New York	Not Visible
Moscow	Monitoring
AutoDetection	Not Visible
Tokyo	Monitoring
Paris	Not Visible

Note: It is recommended to force logout of any users who's region security levels are modified.

44.1.8 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 357) 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.

44.1.9 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.

44.1.10 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.

44.1.11 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.

44.1.12 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.

44.1.13 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.

44.1.14 Changing an Operator's Password

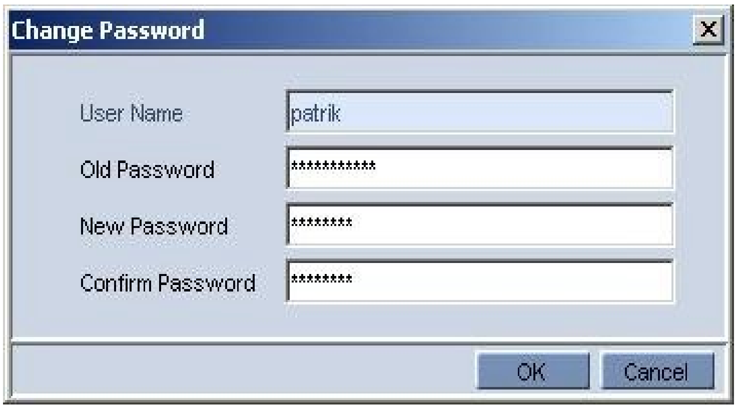
The following describes the conditions for changing an EMS operator's password:

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 35-9: Change Password



Change Password

User Name: patrik

Old Password: ***********

New Password: ********

Confirm Password: ********

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

44.2 RADIUS Server

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

If the connection to the RADIUS servers fails, the local users database can be automatically used as a backup after a defined timeout ie. when the RADIUS connection fails, the user and password are replicated to the local users database and therefore the user can login to the EMS as a local user and this user is displayed in the User's List. This feature is configured by parameter 'Enable Local Authentication on Radius Timeout' and depends on the timeout value defined in 'RADIUS Auth Retransmit Timeout (msec)'.

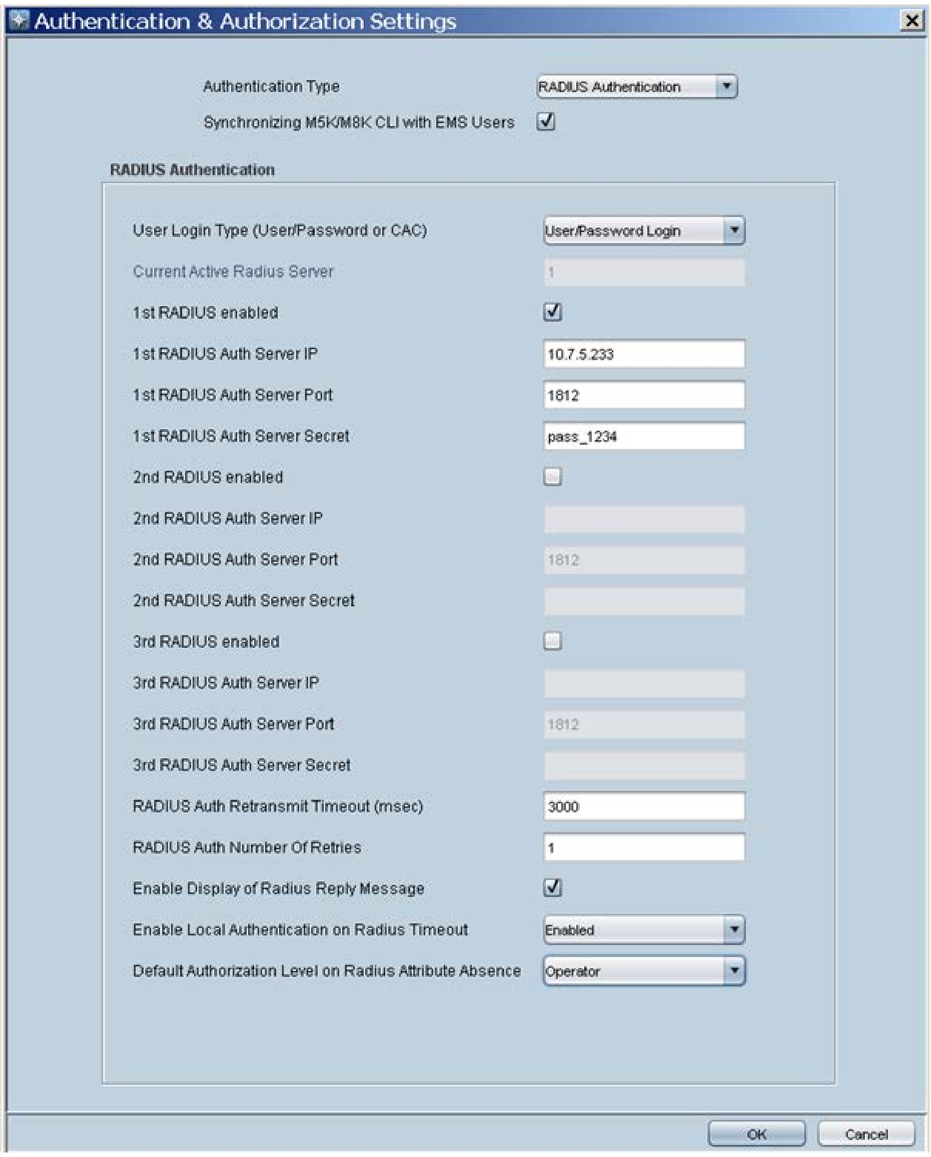
When the RADIUS user logs into the EMS it is assigned one of the EMS security levels, for example 'Operator' (see Section 44.1.6). When one of these security levels is not defined on the RADIUS server, the EMS by default allows access for the RADIUS user with the 'Operator' permissions (see description for parameter 'Default Authorization Level on Radius Attribute Absence' below).

Note: This method is not supported for the SEM and IP Phone Manager applications.

➢ **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 35-10: RADIUS Authentication and Authorization



Authentication & Authorization Settings

Authentication Type	RADIUS Authentication
Synchronizing M5K/M8K CLI with EMS Users	☑

RADIUS Authentication

User Login Type (User/Password or CAC)	User/Password Login
Current Active Radius Server	1
1st RADIUS enabled	☑
1st RADIUS Auth Server IP	10.7.5.233
1st RADIUS Auth Server Port	1812
1st RADIUS Auth Server Secret	pass_1234
2nd RADIUS enabled	□
2nd RADIUS Auth Server IP	
2nd RADIUS Auth Server Port	1812
2nd RADIUS Auth Server Secret	
3rd RADIUS enabled	□
3rd RADIUS Auth Server IP	
3rd RADIUS Auth Server Port	1812
3rd RADIUS Auth Server Secret	
RADIUS Auth Retransmit Timeout (msec)	3000
RADIUS Auth Number Of Retries	1
Enable Display of Radius Reply Message	☑
Enable Local Authentication on Radius Timeout	Enabled
Default Authorization Level on Radius Attribute Absence	Operator

3. For each one of the three RADIUS servers, define the IP address, port and Secret. Note, that at least one RADIUS server must be provisioned.

4. Define the following parameters:
   - RADIUS Auth Retransmit Timeout' (default-3000 msec)
   - RADIUS Auth Number of Retries (default-1)

   Note that these parameters will be used for each one of the Radius Servers.
5. Determine if you wish to display the Radius Reply message. By default, the parameter 'Enable Display of Radius Reply Message' is enabled.
6. Set parameter 'Enable Local Authentication on Radius Timeout' to determine whether local authentication is performed whenever the connection to the RADIUS server fails. By default, the parameter 'Enable Local Authentication on Radius Timeout' i.e. EMS local authentication is enabled (see note above). This parameter's behavior depends on the parameter 'RADIUS Auth Retransmit Timeout', whenever this timeout expires, local authentication is performed.
7. Set the parameter 'Default Authorization Level on Radius Attribute Absence' .

   'Default Authorization Level on Radius Attribute Absence'. This parameter defines the EMS behavior in cases where the user has been successfully authenticated by the RADIUS server; however, the RADIUS server response does not include an EMS security level (Authorization Vendor Specific Element). This implies that the user properties custom attribute “Security Level” (this attribute is specifically defined for the EMS) has not been defined on the RADIUS server and configured with one of the EMS Security levels (Not visible; Monitoring (viewing only); Operation (viewing and all system provisioning operations on devices); Administration or Administrator Super User). In this case, the Administrator can either deny user access or set a default security level to grant to the user. By default, the EMS provides access to the application with the “Operator” security level.
8. Configure other parameters as required according to your RADIUS server configuration.

44.3 LDAP Server

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

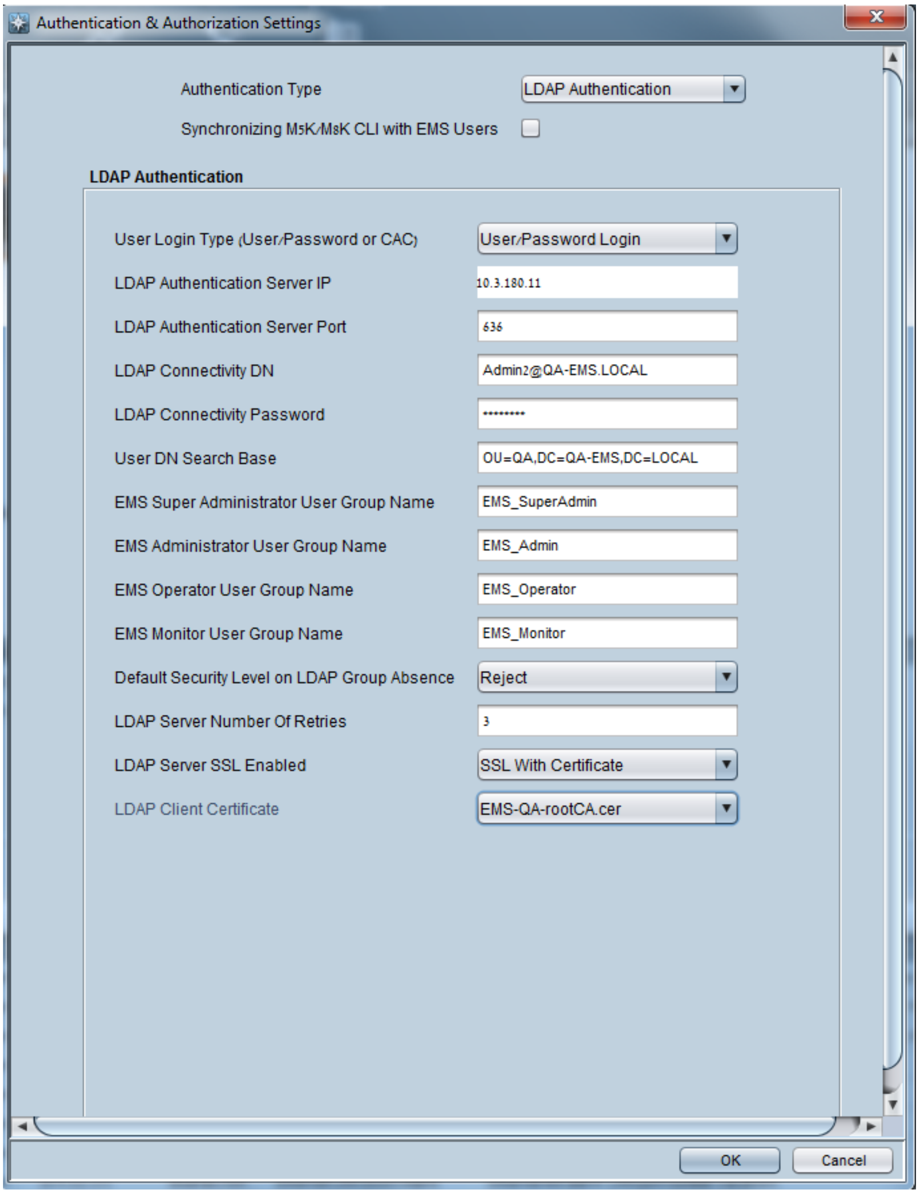
When the LDAP user logs into the EMS it is assigned one of the EMS security levels, for example 'Operator' (see Section 44.1.6). The equivalent names for these security levels on the LDAP server are shown in the figure below. For example, the EMS Operator on the LDAP server is equivalent to 'EMS Operator User Group Name' on the LDAP server. When one of these security levels is not defined on the LDAP server, the EMS by default allows access for the LDAP user with the 'Operator' permissions (see description for parameter 'Default Authorization Level on LDAP Group Absence' below).

⚠ **Note:** When the connection to the LDAP server fails, this user is not replicated to the EMS local database.

➢ 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 35-11: LDAP Authentication and Authorization



Authentication & Authorization Settings

Authentication Type	LDAP Authentication
Synchronizing M5K/M8K CLI with EMS Users	□

LDAP Authentication

User Login Type (User/Password or CAC)	User/Password Login
LDAP Authentication Server IP	10.3.180.11
LDAP Authentication Server Port	636
LDAP Connectivity DN	Admin2@QA-EMS.LOCAL
LDAP Connectivity Password	********
User DN Search Base	OU=QA,DC=QA-EMS,DC=LOCAL
EMS Super Administrator User Group Name	EMS_SuperAdmin
EMS Administrator User Group Name	EMS_Admin
EMS Operator User Group Name	EMS_Operator
EMS Monitor User Group Name	EMS_Monitor
Default Security Level on LDAP Group Absence	Reject
LDAP Server Number Of Retries	3
LDAP Server SSL Enabled	SSL With Certificate
LDAP Client Certificate	EMS-QA-rootCA.cer

3. Configure the LDAP Authentication Server IP and Server Port.
4. Configure the LDAP Connectivity DN parameter as required.
5. Configure LDAP Connectivity Password as required.
6. Configure the User DN Search Base as required.

7. 'Default Authorization Level on LDAP Group Absence'. This parameter defines the EMS behavior in cases where the user has been successfully authenticated by the LDAP server; however, the LDAP server response does not include an EMS security level (Authorization Vendor Specific Element). This implies that the user properties custom attribute “Security Level” (this attribute is specifically defined for the EMS) has not been defined on the LDAP server and configured with one of the EMS Security levels (Not visible; Monitoring (viewing only); Operation (viewing and all system provisioning operations on devices); Administration or Administrator Super User). In this case, the Administrator can either deny user access or set a default security level to grant to the user. By default, the EMS provides access to the application with the “Operator” security level.

8. If you wish to secure the connection with the LDAP server over SSL:

   a. From the "LDAP Server Number of Retries" drop-down list, select one of the following options:

      - **Plain Connection (default):** non-secured connection with the LDAP server.
      - **SSL With Certificate**: an HTTPS connection between the EMS server and the LDAP server is opened. The EMS authenticates the SSL connection using a certificate.
      - **SSL Without Certificate:** an HTTPS connection between the EMS server and the LDAP server is opened; however is not authenticated using a certificate.

   b. From the "LDAP Client Certificate" drop-down list, select the certificate file that you wish to use to secure the connection with the LDAP server.

Note:

- If you chose the option “SSL With Certificate”, ensure that you have loaded the required SSL certificate file (certificate required by the LDAP Active Directory platform) to the EMS Software Manager using the "Certificate File" option (see Section 4.1).
- If the login credentials to the LDAP server are incorrect, you will not be able to connect to the LDAP server and an appropriate message is displayed.

This page is intentionally left blank.

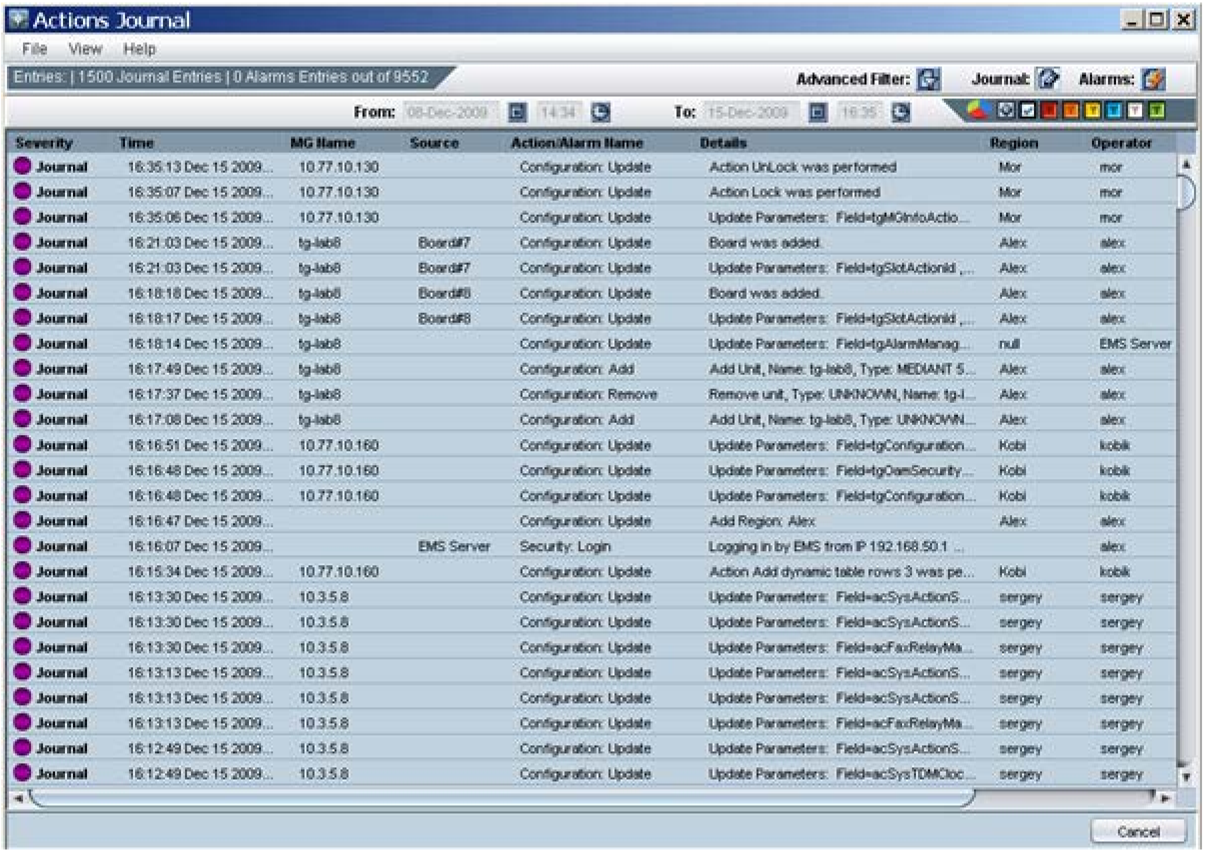
45 Viewing Operator Actions in the Actions Journal

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



Entries: | 1500 Journal Entries | 0 Alarms Entries out of 9552

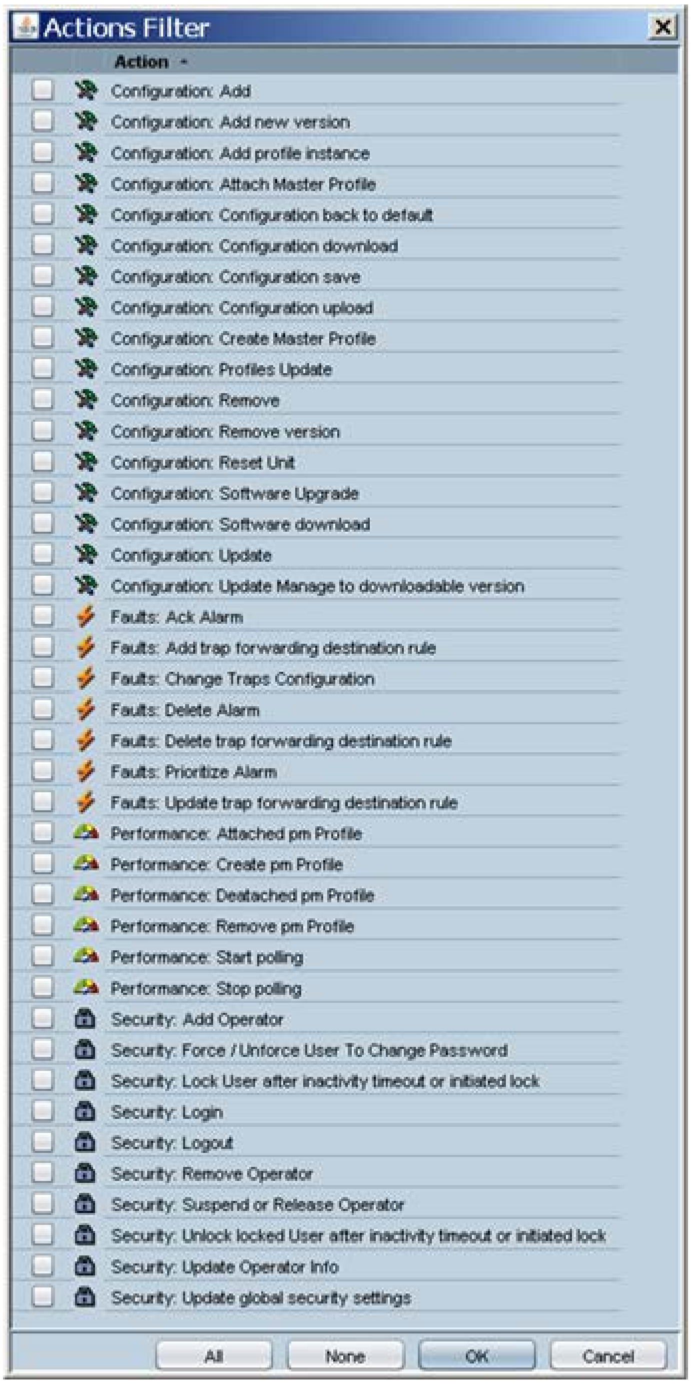
From: 08-Dec-2009 14:34 To: 15-Dec-2009 16:35

Severity	Time	MG Name	Source	Action/Alarm Name	Details	Region	Operator
Journal	16:35:13 Dec 15 2009...	10.77.10.130		Configuration: Update	Action UnLock was performed	Mor	mor
Journal	16:35:07 Dec 15 2009...	10.77.10.130		Configuration: Update	Action Lock was performed	Mor	mor
Journal	16:35:06 Dec 15 2009...	10.77.10.130		Configuration: Update	Update Parameters: Field=tgMGInfoActio...	Mor	mor
Journal	16:21:03 Dec 15 2009...	tg-lab8	Board#7	Configuration: Update	Board was added.	Alex	alex
Journal	16:21:03 Dec 15 2009...	tg-lab8	Board#7	Configuration: Update	Update Parameters: Field=tgSlotActionId ,...	Alex	alex
Journal	16:18:18 Dec 15 2009...	tg-lab8	Board#8	Configuration: Update	Board was added.	Alex	alex
Journal	16:18:17 Dec 15 2009...	tg-lab8	Board#8	Configuration: Update	Update Parameters: Field=tgSlotActionId ,...	Alex	alex
Journal	16:18:14 Dec 15 2009...	tg-lab8		Configuration: Update	Update Parameters: Field=tgAlarmManag...	null	EMS Server
Journal	16:17:49 Dec 15 2009...	tg-lab8		Configuration: Add	Add Unit, Name: tg-lab8, Type: MEDIANT 5...	Alex	alex
Journal	16:17:37 Dec 15 2009...	tg-lab8		Configuration: Remove	Remove unit, Type: UNKNOWN, Name: tg-l...	Alex	alex
Journal	16:17:08 Dec 15 2009...	tg-lab8		Configuration: Add	Add Unit, Name: tg-lab8, Type: UNKNOWN...	Alex	alex
Journal	16:16:51 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=tgConfiguration...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=tgOamSecurity...	Kobi	kobik
Journal	16:16:48 Dec 15 2009...	10.77.10.160		Configuration: Update	Update Parameters: Field=tgConfiguration...	Kobi	kobik
Journal	16:16:47 Dec 15 2009...			Configuration: Update	Add Region: Alex	Alex	alex
Journal	16:16:07 Dec 15 2009...		EMS Server	Security: Login	Logging in by EMS from IP 192.168.50.1 ...		alex
Journal	16:15:34 Dec 15 2009...	10.77.10.160		Configuration: Update	Action Add dynamic table rows 3 was pe...	Kobi	kobik
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:30 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acFaxRelayMa...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:13:13 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acFaxRelayMa...	sergey	sergey
Journal	16:12:49 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysActionS...	sergey	sergey
Journal	16:12:49 Dec 15 2009...	10.3.5.8		Configuration: Update	Update Parameters: Field=acSysTDMCloc...	sergey	sergey

- The Actions Journal screen enables the operator to track all actions performed by all users on all MGs in all Regions.
- The Actions Journal can be opened either by opening menu **Security** > **Actions Journal**, or by clicking the icon **Journal** on the Alarm Browser tool bar. When opening the Journal from the Alarm Browser, it's opened in the context of the Alarm Browser (Status screen).
- In addition to a context filter, available from the Alarm Browser tool bar, operators filter according to Users, Date and Time, and Action Type.
- The Actions Journal screen is read-only and non-configurable.
- Data displayed in the Actions Journal can be saved in a *csv* file.

- Following are columns displayed in the Actions Journal:
  - **Time** - date & time of the action
  - **MG Name** - the name of the MG on which the action was performed.
  - **Source** - managed object on which the action was performed, for example, 'Board#8'
  - **Action** - Action type, one of the values from the list displayed in the figure below.

Figure 36-2: Journal Actions



□ Configuration: Add
□ Configuration: Add new version
□ Configuration: Add profile instance
□ Configuration: Attach Master Profile
□ Configuration: Configuration back to default
□ Configuration: Configuration download
□ Configuration: Configuration save
□ Configuration: Configuration upload
□ Configuration: Create Master Profile
□ Configuration: Profiles Update
□ Configuration: Remove
□ Configuration: Remove version
□ Configuration: Reset Unit
□ Configuration: Software Upgrade
□ Configuration: Software download
□ Configuration: Update
□ Configuration: Update Manage to downloadable version
□ Faults: Ack Alarm
□ Faults: Add trap forwarding destination rule
□ Faults: Change Traps Configuration
□ Faults: Delete Alarm
□ Faults: Delete trap forwarding destination rule
□ Faults: Prioritize Alarm
□ Faults: Update trap forwarding destination rule
□ Performance: Attached pm Profile
□ Performance: Create pm Profile
□ Performance: Deatached pm Profile
□ Performance: Remove pm Profile
□ Performance: Start polling
□ Performance: Stop polling
□ Security: Add Operator
□ Security: Force / Unforce User To Change Password
□ Security: Lock User after inactivity timeout or initiated lock
□ Security: Login
□ Security: Logout
□ Security: Remove Operator
□ Security: Suspend or Release Operator
□ Security: Unlock locked User after inactivity timeout or initiated lock
□ Security: Update Operator Info
□ Security: Update global security settings

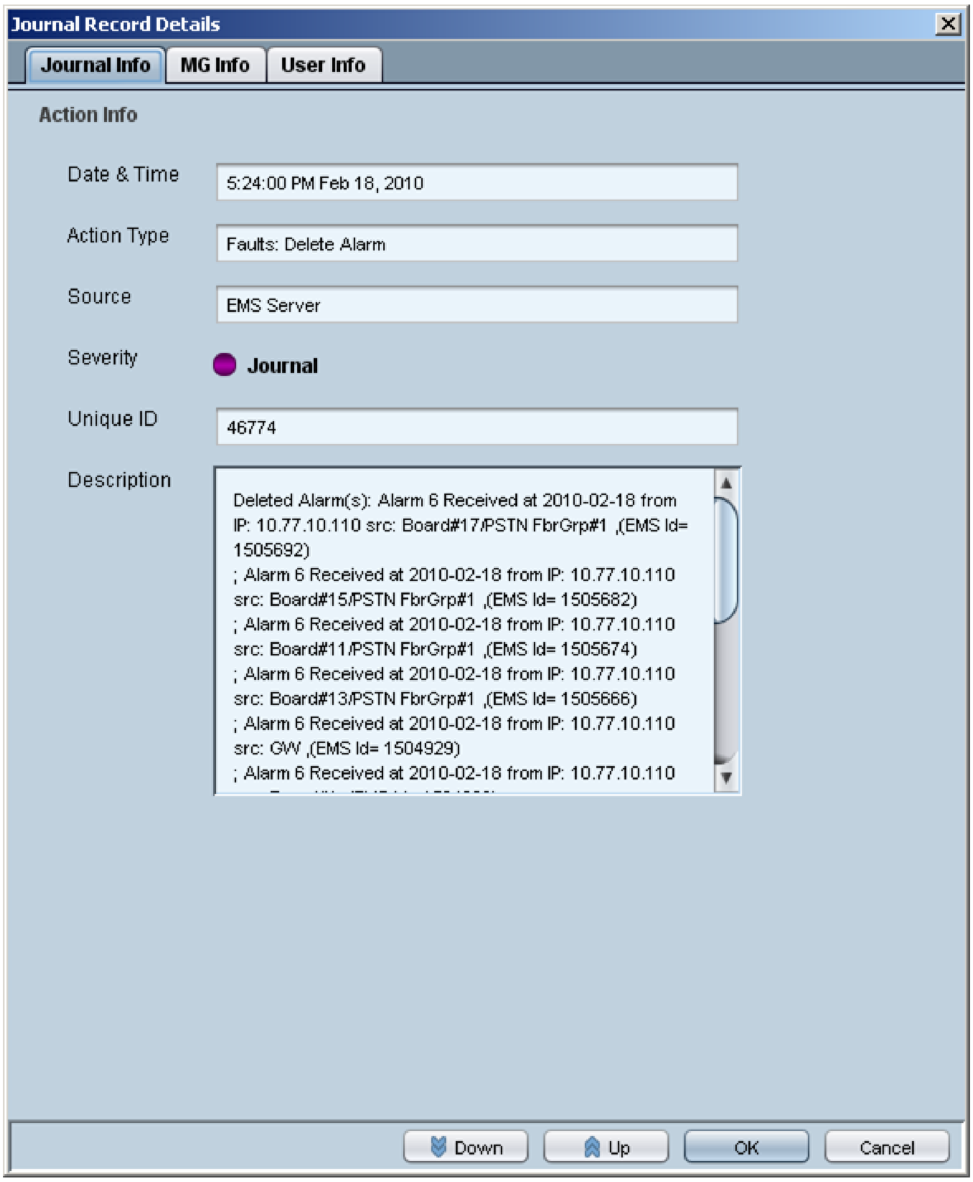
- **Details** - a precisely detailed description of the action, for example, parameter names and values for a Configuration Update action.
- **Operator** - the name of the operator who performed the action.
- **Region** - the region in which the device resides.

45.1 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



Action Info

Date & Time: 5:24:00 PM Feb 18, 2010

Action Type: Faults: Delete Alarm

Source: EMS Server

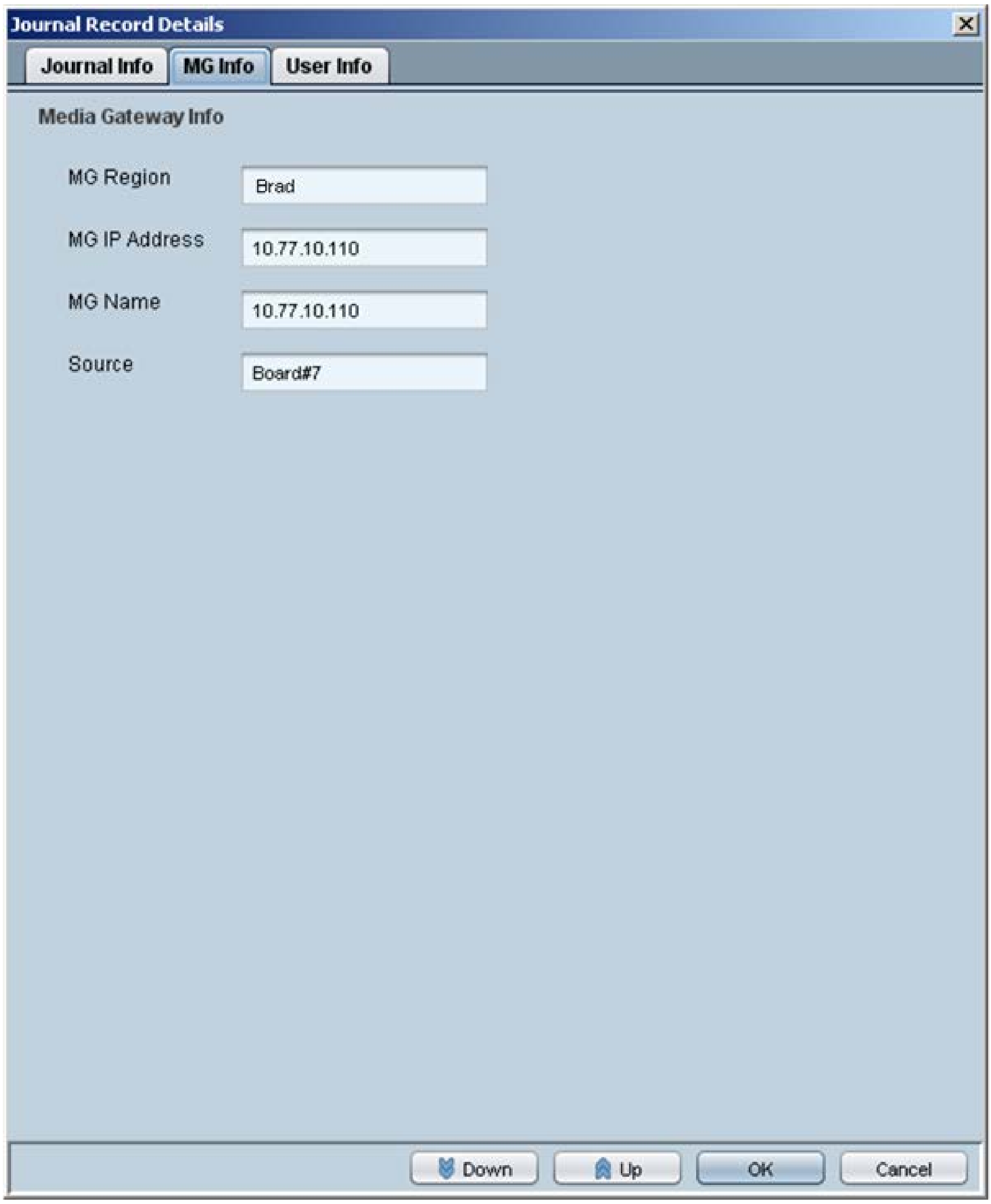
Severity: ● Journal

Unique ID: 46774

Description: Deleted Alarm(s): Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#17/PSTN FbrGrp#1 ,(EMS Id= 1505692)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#15/PSTN FbrGrp#1 ,(EMS Id= 1505682)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#11/PSTN FbrGrp#1 ,(EMS Id= 1505674)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: Board#13/PSTN FbrGrp#1 ,(EMS Id= 1505666)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110 src: GW ,(EMS Id= 1504929)
; Alarm 6 Received at 2010-02-18 from IP: 10.77.10.110

- MG Info

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



Media Gateway Info

MG Region: Brad

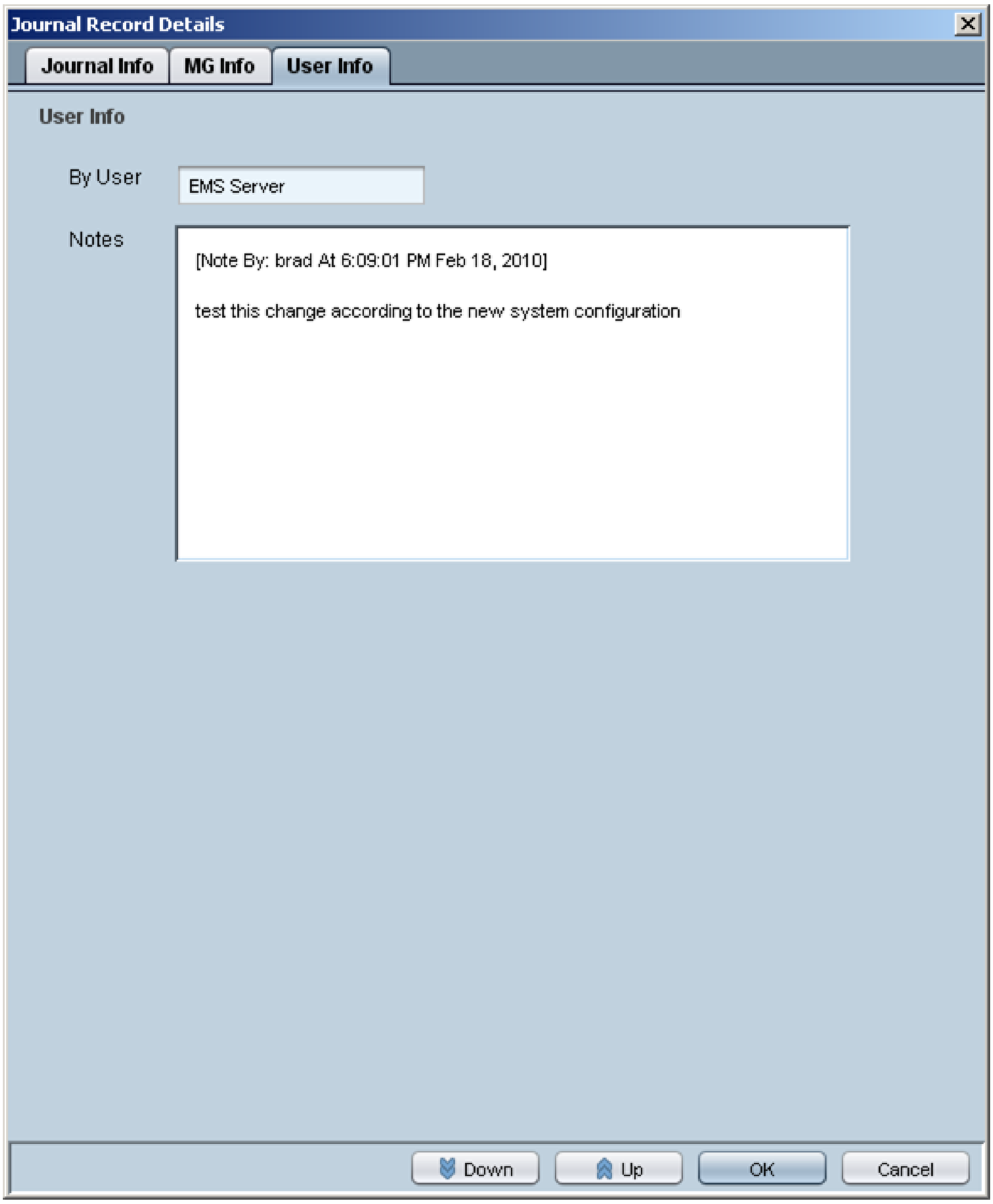
MG IP Address: 10.77.10.110

MG Name: 10.77.10.110

Source: Board#7

- User Info

Figure 36-5: Journal Record Details - User Info



By User: EMS Server

Notes:

[Note By: brad At 6:09:01 PM Feb 18, 2010]

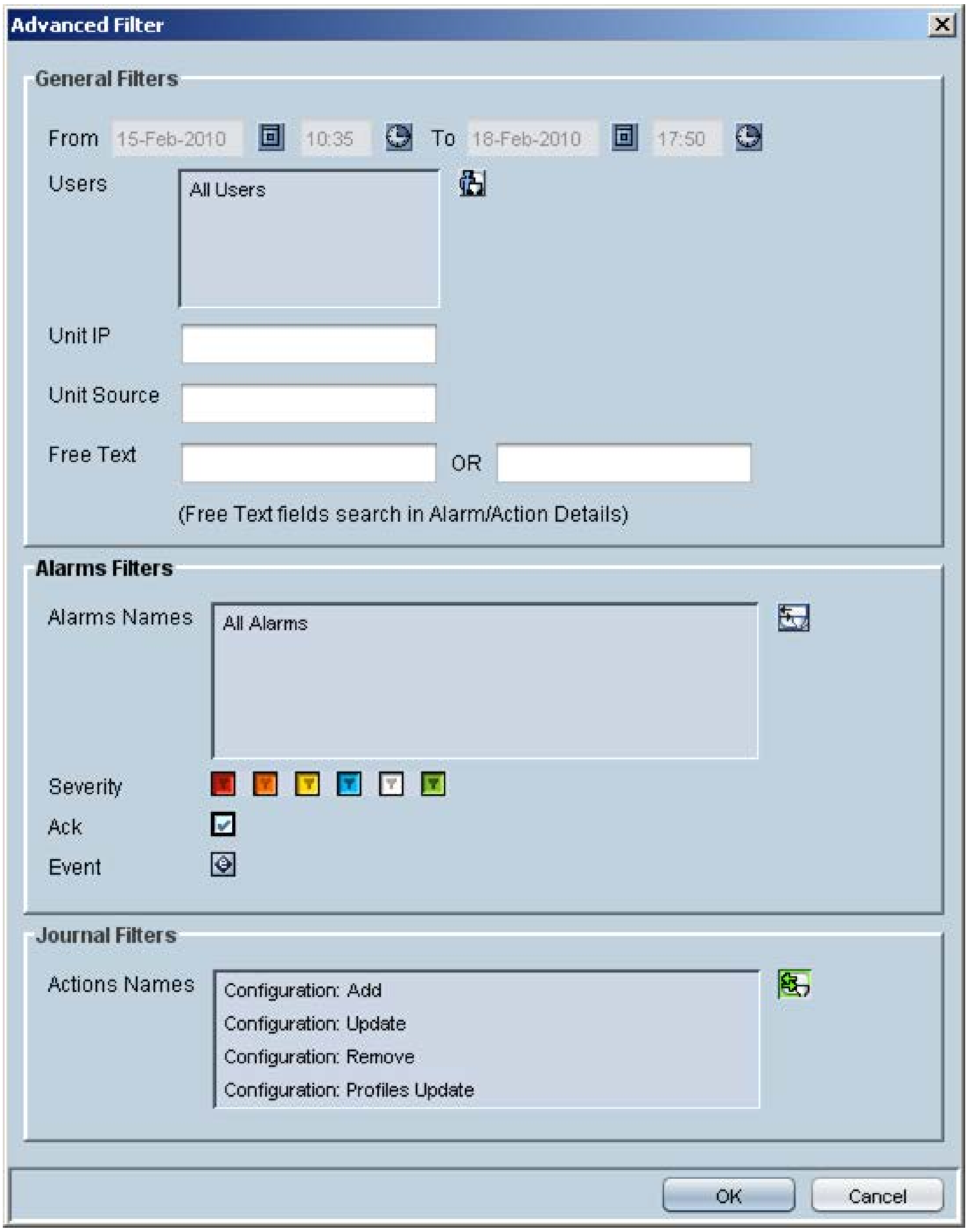
test this change according to the new system configuration

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

45.2 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



Advanced Filter

General Filters

From 15-Feb-2010 10:35 To 18-Feb-2010 17:50

Users: All Users

Unit IP

Unit Source

Free Text OR

(Free Text fields search in Alarm/Action Details)

Alarms Filters

Alarms Names: All Alarms

Severity

Ack

Event

Journal Filters

Actions Names:
Configuration: Add
Configuration: Update
Configuration: Remove
Configuration: Profiles Update

- **General Filters**
  - Date and Time Filter
  - Users Filter. An operator can select a user or a set of users whose actions the operator needs to view.
  - Unit IP
  - Unit Source
  - Free Text 1 (searched in the Details filed)
  - Free Text 2 (searched in the Details filed)
- **Alarms Filters** (See Section 'Fault Management' on page 257)
- **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)

45.2.1 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.

45.3 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.

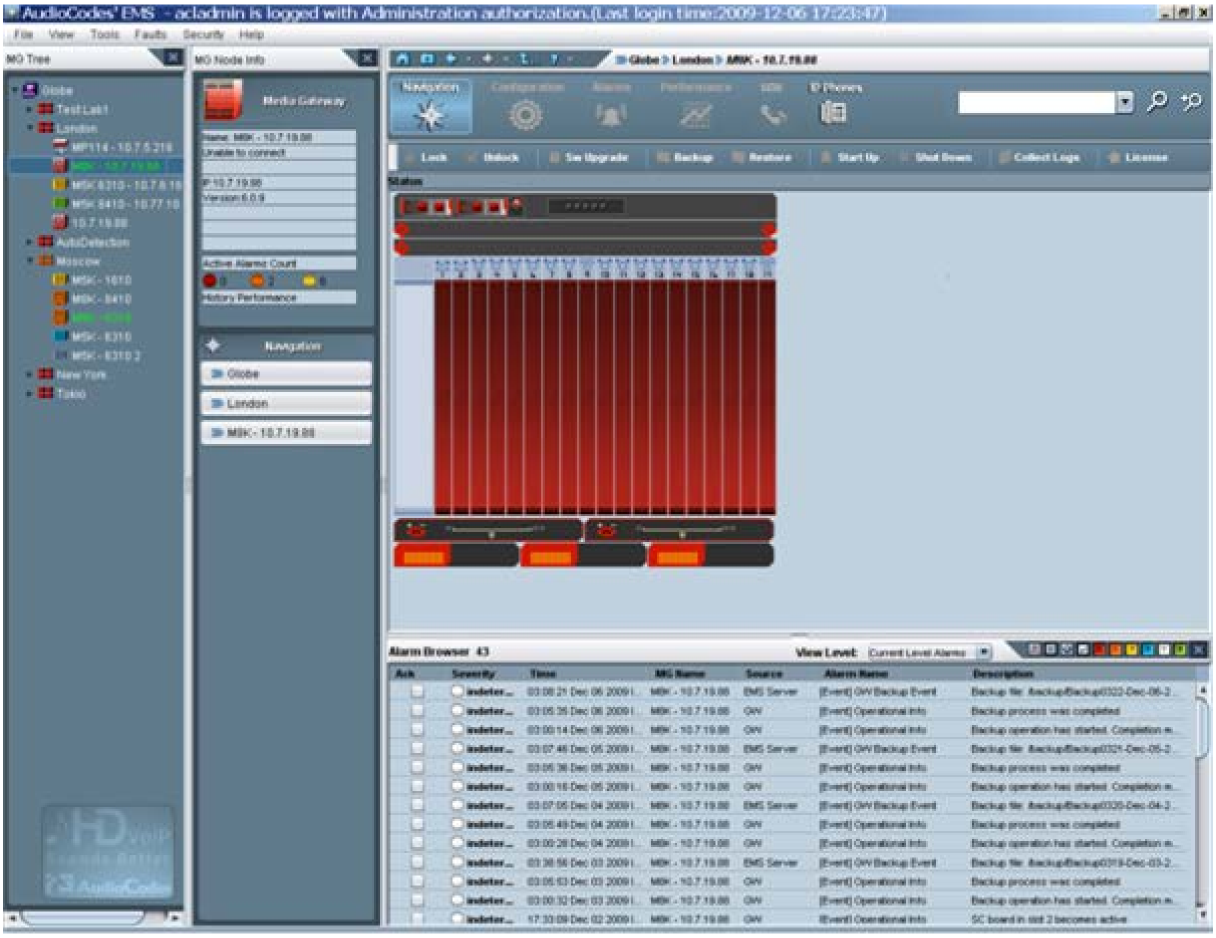
46 Failure to Reconnect to a Previously-Connected Device whose Operation was Interrupted

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 37-1: Failure to Reconnect to a Device Whose Operation was Interrupted



AudioCodes' EMS - acladmin is logged with Administration authorization.(Last login time:2009-12-06 17:23:47)

Name: MSK - 10.7.19.88
Unable to connect
IP 10.7.19.88
Version 6.0.9
Active Alarms Count
History Performance

Alarm Browser 43 — View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
□	indeter...	03:08:21 Dec 06 2009 I...	MSK - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0322-Dec-06-2...
□	indeter...	03:05:35 Dec 06 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	indeter...	03:00:14 Dec 06 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	indeter...	03:07:46 Dec 05 2009 I...	MSK - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0321-Dec-05-2...
□	indeter...	03:05:36 Dec 05 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	indeter...	03:00:16 Dec 05 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	indeter...	03:07:05 Dec 04 2009 I...	MSK - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0320-Dec-04-2...
□	indeter...	03:05:49 Dec 04 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	indeter...	03:00:28 Dec 04 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	indeter...	03:38:56 Dec 03 2009 I...	MSK - 10.7.19.88	EMS Server	[Event] GW Backup Event	Backup file: /backup/Backup0319-Dec-03-2...
□	indeter...	03:05:53 Dec 03 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup process was completed
□	indeter...	03:00:32 Dec 03 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	Backup operation has started. Completion m...
□	indeter...	17:33:09 Dec 02 2009 I...	MSK - 10.7.19.88	GW	[Event] Operational Info	SC board in slot 2 becomes active

The table below summarizes possible reconnection (following disconnection) problem scenarios, the verification test that operators should perform in each scenario, and how to fix the problem.

Table 37-1: 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.

47 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

This page is intentionally left blank.

Part VII

Appendix

This section describes various miscellaneous procedures.

A Preparing Network Connectivity for Interoperability Automatic Provisioning

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 same 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 376).

Note:

- 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 11.6.2).
- 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 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 373. In addition, see page 376 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 (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
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

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

A.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.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 the 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 Pre-provisioning process.

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.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/contact
Website: www.audiocodes.com