Element Management System User's Manual

Version 3.0

LTRT-91005 Rev 003

Notice

This User's Manual describes and explains the use of Nortel's Element Management System (EMS). Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, Nortel cannot guarantee the 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 and downloaded by registered Technical Support customers at www.nortel.com.

This document is subject to change without notice.

Refer to the current release notes that may be included with your documentation or hardware delivery.

Date Published: May-30-2005 Date Printed: May-31-2005

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press Alt + ← .

Note: The Element Management System supports the following products:

1. Media Gateway 3500

Trademarks

All products or trademarks are property of their respective owners.

Customer Support

Customer technical support and service are provided by Nortel. Contact support@nortel.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number.

When the term 'Trunking Gateway' is used in this manual, it refers to the Media Gateway 3500.

When 'MG' is used in this manual, it refers to 'media gateway'.

Related Documentation

Manual Name
Media Gateway 3500 Installation, Operation & Maintenance Manual
Media Gateway 3500 Product Description
Element Management System (EMS) Server Installation & Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) Online Help
EMS Parameter Guide for the Media Gateway 3500

Contents

Table of Figures

List of Tables

1 Introducing the Nortel Element Management System

The Nortel Element Management System (EMS) is an advanced solution for standards-based management of Media Gateways within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of the Nortel Media Gateway 3500.
The Nortel EMS enables Service Providers the capability of rapid time-to-market and inclusive, cost-effective management of next-generation networks.

The standards-compliant EMS for media gateways uses distributed SNMP-based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a feature-rich management framework. It supports fault management, configuration and security. The EMS simultaneously manages multiple Media Gateway 3500 systems and their modules.

1.1 Specifications

- Software Version Number: 3.0
- Release Date: Q2 2005
- Package and Upgrade Distribution: CD-ROM

Table 1-1: Element Management System (EMS) 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: at least a one-month history for up to 1100 media gateways (depending on disk size available). ▪ Graphical, context-sensitive Alarm History with filtering options. ▪ Application includes context-sensitive Alarm Browser with various filtering and search options, detailed alarm description, Acknowledge and Delete actions processing, audio indication on receipt of alarms. ▪ Automatic Alarm Clearing ▪ Traps Forwarding to Northbound Interface ▪ Save alarms in a *csv* file
Media Gateways Monitoring	Summary of all managed gateways' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.
Media Gateways Provisioning	▪ Adapts rapidly to changes in new media gateway software releases ▪ Based on hierarchy of managed objects concepts ▪ Online parameter provisioning support, with icons indicating provisioning type ▪ Profile-based provisioning, including Master Profile for all VoIP gateways and media servers, as well as for the TP-1610 board. 1. Search provisioning parameter ▪ Configuration database of gateways is kept inside the media gateways

Subject	Description
Security Management	Complies with T1M1.5/2003-007R4 and covers two aspects: Network communication security and EMS application security. **Network Communications Security** ▪ EMS server's network is configured and its ports opened during installation. ▪ EMS client-server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). ▪ Media Gateway 3500: SNMPv2c, Telnet and FTP over IPSec. **Application Security** ▪ User Management: Using an LDAP server for centralized user authentication, or in the EMS application. ▪ EMS application: Users List. Authentication-based operator access according to user name, password, security level, login machine IP. Modification of user details and access rights, user removal, forced logout, user suspension, releasing users from suspension, 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
Media Gateways Maintenance Actions	▪ Online software upgrade via a Wizard ▪ Gateway installation, startup and shutdown ▪ All maintenance actions (lock, unlock, add / remove board, etc.) for each media gateway entity, via a convenient Graphical User Interface.

Table 1-2: User Interface and External Interfaces Specifications

Subject	Description
User Access Control	Login + Password to EMS application
Northbound Interface	SNMPv2c traps
Southbound Interface	SNMPv2c, HTTP (MD5 encrypted)
Multi-Platform	Java-based, JDK version 1.4.2
Relational Database	Oracle 9i relational database is used for data storage
Internationalization	Multi-language support ready application

1.2 Supported VoIP Equipment

Table 1-3: Supported VoIP Equipment

Supported VoIP Equipment	Description
Media Gateway 3500	The Media Gateway 3500 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; SIGTRAN Interworking (PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant Applications: VoP Trunking Gateways, IP-Centrex Gateways, VoP Access Gateways Selected specifications: Up to 2,400 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, SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP (Refer to the product documentation for detailed information).

1.3 Supported Versions

1.3.1 Digital Gateways

- Media Gateway 3500
  - Versions **3.0**, 2.1

1.4 Characteristics

EMS System Characteristics

The EMS features a Client/Server architecture, enabling customers to access the EMS from multiple, remotely located work centers and workstations.

The entire system is designed in Java™, based on a consistent, vendor-neutral framework, and following recognized design patterns. Client - Server communication is implemented with Java™ RMI (Remote Method Invocation) protocol over TCP (Transmission Control Protocol).

The EMS enables multiple work centers and workstations to simultaneously access the EMS server (up to 10 concurrent clients connected to the server).

EMS Server, running on Sun™ Microsystems' Solaris™. All management data is stored in the server, using Oracle *9i* 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.

Versatile System

The EMS can simultaneously manage multiple MG 3500 gateways, even while having different software versions running on each.

FCAPS

The EMS supports **FCAPS** functionality:

- 'Fault management' on page 85
- 'Configuration management' on page 31
- Accounting (not applicable to media gateways)
- 'Performance Management' on page 101
- 'Security Management' on page 111

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.

Multi-Language Support

The EMS is a globally ready application. It can be adapted to various regions and languages without requiring engineering changes. Locale-dependent data such as dates and currencies appear in formats that conform to the customer's region and language. With the addition of localized (language) data, the same application can be used worldwide. A different locale can be selected per client application.

The default locale language is English (USA). The EMS is ready to include files to support left-to-right languages.

Customizable Features

The features listed in this subsection can be modified to fall in line with a Customer's request. Following customization, a new Client installation disc is provided the Customer who requested the customization.

- The EMS was developed as an internationalization-ready application; it can easily be customized and presented in an international language besides English by the addition of locally dependent data such as textual elements and system messages translation. The EMS supports left-to-right languages.
- All the texts in the application can be customizable (English to English)
- Menu Bar and Pop-up Menus Modifications
  - The order of items listed in the menu bar and pop-up menus can be changed
  - Items separator can be added where required
  - Items can be removed from the menus and Pop-up Menus modifications.
- Provisioning Frame modifications
  - Order of tabs can be changed
  - Tab can be removed from the frame
- Status pane navigation buttons can be removed or their order changed.

2 Installing the EMS Client on a PC

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

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

➢ To install the EMS from the supplied CD-ROM:

2. Insert the EMS installation disk.
3. Double-click the EMS Client (PC) Installation setupwin32.exe file and follow the installation instructions; as a result of installation process, the EMS Client icon is added to the desktop.

➢ 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.

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

   http://10.7.6.5/jaws/

2. Follow the online instructions.

2.1 Running the EMS Client

➢ To run the EMS client:

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

2.2 Management Procedure

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

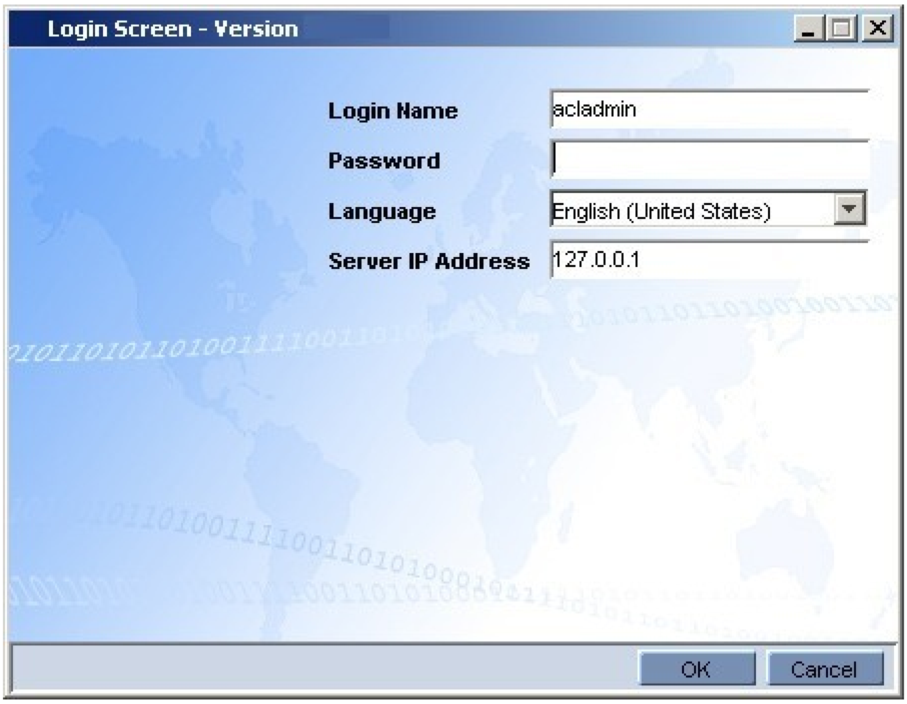
1. Define EMS users
2. Define and evoke your VoIP devices
3. Perform advanced provisioning
4. Monitor your VoIP devices
5. Maintain one of more VoIP devices with one action
6. Manage faults and performance
7. Manage security

3 Getting Started with the EMS

➢ To get started with the EMS:

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

Figure 3-1: Login Screen



Login Screen - Version

Login Name: acladmin

Password:

Language: English (United States)

Server IP Address: 127.0.0.1

3.1 Logging In

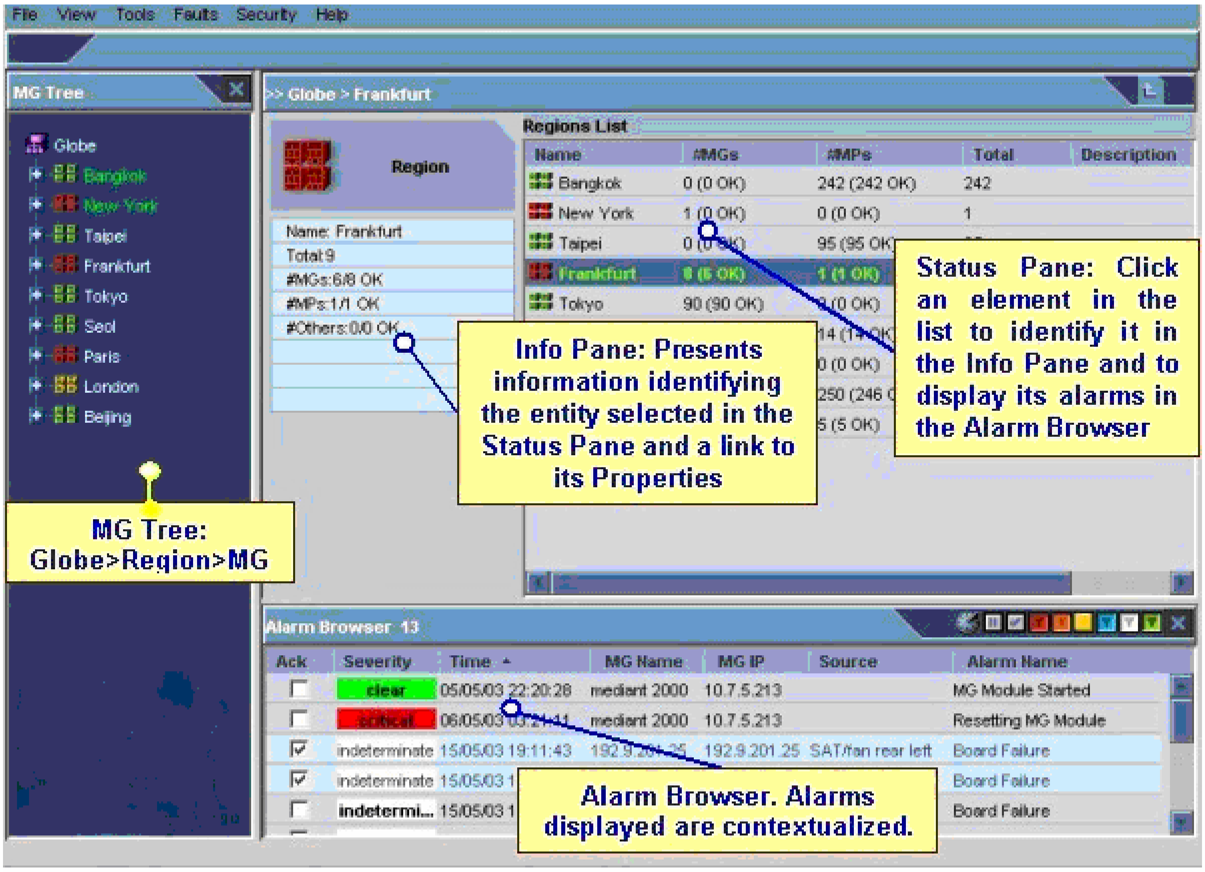
➢ To log in:

1. Define fields User Name, Password, Language and Server IP Address and press OK; the EMS's Main Screen opens. (Note that User Name and Password are case-sensitive). If incorrectly defined or if the Server IP Address field is incorrectly defined, a prompt is displayed indicating that the fields should be redefined correctly.

2. When logging in to the application for a second time, the User Name, Language and Server IP Address, defined when logging in previously, are displayed.

Note: When entering the EMS for the first time, the fields User Name and Password are by default set to 'admin' and 'admin'. The Administrator can modify these defaults after defining system Users.

Figure 3-2: Main Screen Indicating Navigation Concepts



Name: Frankfurt
Total:9
#MGs:6/8 OK
#MPs:1/1 OK
#Others:0/0 OK

Name	#MGs	#MPs	Total	Description
Bangkok	0 (0 OK)	242 (242 OK)	242	
New York	1 (0 OK)	0 (0 OK)	1	
Taipei	0 (0 OK)	95 (95 OK		
Frankfurt	8 (6 OK)	1 (1 OK)		
Tokyo	90 (90 OK)	0 (0 OK)		
		14 (14 OK		
		0 (0 OK)		
		250 (246 (		
		5 (5 OK)		

Ack	Severity	Time ▲	MG Name	MG IP	Source	Alarm Name
☐	clear	05/05/03 22:20:28	mediant 2000	10.7.5.213		MG Module Started
☐	critical	06/05/03 03:21:41	mediant 2000	10.7.5.213		Resetting MG Module
☑	indeterminate	15/05/03 19:11:43	192.9.201.25	192.9.201.25	SAT/fan rear left	Board Failure
☑	indeterminate	15/05/03 1				Board Failure
☐	indetermi...	15/05/03 1				Board Failure

MG Tree: Globe>Region>MG

Info Pane: Presents information identifying the entity selected in the Status Pane and a link to its Properties

Status Pane: Click an element in the list to identify it in the Info Pane and to display its alarms in the Alarm Browser

Alarm Browser. Alarms displayed are contextualized.

3.2 Getting Oriented in the EMS

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

1. 'Navigating Down and Up System Hierarchy' on page 22
2. 'Selecting an Interface in the Context of an Element' on page 23 (and the concept of context-oriented screens)
3. 'Using Color Coding to Assess Element Status' on page 24

3.2.1 Navigating Down and Up System Hierarchy

The EMS's main screen is divided into 5 sections:

1. Menu bar (File, View, Security)
2. MG Tree (Media Gateways Tree, in the left pane of the main screen)

3. Info pane
4. Status pane
5. Alarm Browser

Use the MG Tree and Status pane to navigate down/up the system's hierarchical layers (Globe>Region>MG>TP Board>Trunk) in the EMS. After expanding a region and selecting a media gateway in the MG Tree, the Status pane and Alarm Browser are immediately updated according to the media gateway selected. Use the "Up" button to navigate from an element of a low hierarchical level (e.g., Trunk) back up to an element of a high hierarchical level (e.g., media gateway).

3.2.2 Selecting an Interface in the Context of an Element

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

- After expanding a region and navigating to the level of a media gateway in the MG Tree, select a gateway in the MGs List; the Information Pane is immediately updated with basic information (if available) corresponding to the selected gateway.
- Double-click on the gateway listed under the MGs List; the gateway level Status pane graphically representing the gateway is displayed, including the navigation buttons.
- Click the "Properties" link in the gateway Info pane to access the gateway's provisioning parameters screens.
- Double-click a TP board to open that board's Status pane, including the navigation buttons (refer to 'Navigation Buttons to Provision the TP-1610 Board' on page 55). When working with the navigation buttons on the top of the Status pane at the TP board level, selecting a Trunk after clicking the Trunks navigation button (for example) changes the Info pane correspondingly. Double-clicking on these elements opens those elements' provisioning parameters screens. The same principle applies to working with the navigation buttons on the top of the Status pane at the gateway level.

3.2.3 Context-Sensitive Behavior

The Status pane as well as the navigation bar allow 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 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:

- Information pane shows details of the current location/level
- MG Tree shows the current region / media gateway, as selected
- Alarms displayed in the Alarm Browser are contextualized; only alarms associated with the entity selected in the MG Tree/Status pane/Board are displayed.
- Any action menu like "Properties" relates to the current location. E.g., the "Properties" link in the context of a media gateway will show that media gateway's properties, while the "Properties" link, enabled when a Trunk is selected in the Trunk List at the TP board level, shows the properties of that Trunk.

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 3-1: Assessing System Entity Status via Icon Color

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

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

4 Software Manager

The EMS can manage only media gateways whose software version is defined in the Software Manager.

Thus, before defining the MG Tree and the media gateways, introduce the software you'll be operating with to the EMS.

The EMS Software Manager (Tools > Software Manager) enables operators to view, add or remove configuration files and regional files. Each new version, fix or software update provided to customers should be added by them to the Software Manager.

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 (Show MG 3500 SW) facilitate easy access to device-specific files.

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

- Software Type

Three software types are supported:

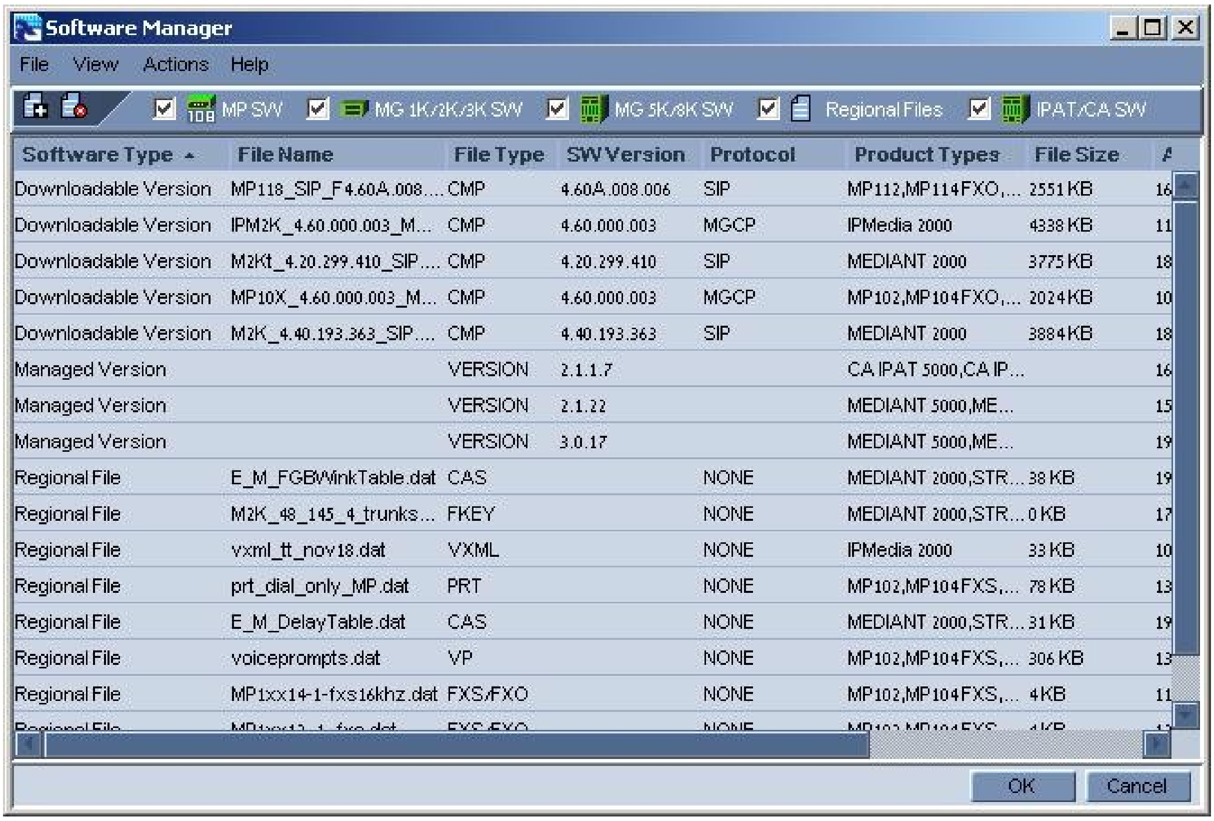
6. Loadable version: Media gateways of this version are recognized and managed by the EMS and users can load the version to the media gateway.

7. Managed version: Media gateways of this version are recognized and managed by the EMS. The version cannot be loaded to any media gateway.

- File Name
  - File Type: *cmp, tar* or *tar.gz*, *cpt, vp*, *cas* and *dat*. Refer below for detailed information.
  - SW Version: This column is relevant only to software files.
  - Protocol: Not applicable for MG 3500.
  - 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 was added.
  - Added By - the name of the operator who defined the software version.

- 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	A
Downloadable Version	MP118_SIP_F4.60A.008....	CMP	4.60A.008.006	SIP	MP112,MP114FXO,...	2551 KB	16
Downloadable Version	IPM2K_4.60.000.003_M...	CMP	4.60.000.003	MGCP	IPMedia 2000	4338 KB	11
Downloadable Version	M2Kt_4.20.299.410_SIP....	CMP	4.20.299.410	SIP	MEDIANT 2000	3775 KB	18
Downloadable Version	MP10X_4.60.000.003_M...	CMP	4.60.000.003	MGCP	MP102,MP104FXO,...	2024 KB	10
Downloadable Version	M2K_4.40.193.363_SIP....	CMP	4.40.193.363	SIP	MEDIANT 2000	3884 KB	18
Managed Version		VERSION	2.1.1.7		CA IPAT 5000,CA IP...		16
Managed Version		VERSION	2.1.22		MEDIANT 5000,ME...		15
Managed Version		VERSION	3.0.17		MEDIANT 5000,ME...		19
Regional File	E_M_FGBWinkTable.dat	CAS		NONE	MEDIANT 2000,STR...	38 KB	19
Regional File	M2K_48_145_4_trunks...	FKEY		NONE	MEDIANT 2000,STR...	0 KB	17
Regional File	vxml_tt_nov18.dat	VXML		NONE	IPMedia 2000	33 KB	10
Regional File	prt_dial_only_MP.dat	PRT		NONE	MP102,MP104FXS,...	78 KB	13
Regional File	E_M_DelayTable.dat	CAS		NONE	MEDIANT 2000,STR...	31 KB	19
Regional File	voiceprompts.dat	VP		NONE	MP102,MP104FXS,...	306 KB	13
Regional File	MP1xx14-1-fxs16khz.dat	FXS/FXO		NONE	MP102,MP104FXS,...	4 KB	11

Note: Software version files of all media gateways managed by the EMS must be defined in the Software Manager.

A media gateway whose software information is not registered in the Software Manager is displayed in the GUI as 'Unknown' ?.

File types managed by the Software Manager are:

- Configuration files for the Media Gateway 3500
  - *tar* or *tar.gz* file - This is the main software image file. Load the file to change the software version (for example).
  - *ems* file - Includes information relating to the software version. For EMS use only. The file is not loaded to the gateway.

- **Regional Files**

- Call Progress Tones - 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: North America.
- Prerecorded Tones – This dat file enhances the VoIP device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the Call Progress Tones file.
- Coefficient file - This file (different for FXS and FXO gateways) contains telephony interface configuration data for the VoIP device. This information includes telephony interface characteristics such as DC and AC impedance, feeding current and ringing voltage. The file is specific to the type of telephony interface that the VoIP device supports. In most cases, you must load this file.
- 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.

4.1 Adding a New File to the Software Manager

➢ To add new files to the Software Manager, take these steps:

1. Click the Add File icon (indicated with a plus sign in the upper left corner of the Software Manager screen) or open the Actions menu and choose the option Add File; the Add Files screen (shown in the figure below) opens.
2. Click the icon of a folder located adjacent to the File Type to be added, and in the dialog box that opens, navigate to the file (saved in your PC); click OK.

3. Define fields in the Add Files screen according to your requirements and press OK; the name of the file/s appear defined in the File Name field in the Software Manager screen. Click OK; the files that you defined will now appear listed in the Software Manager.

Figure 4-2: Add Files

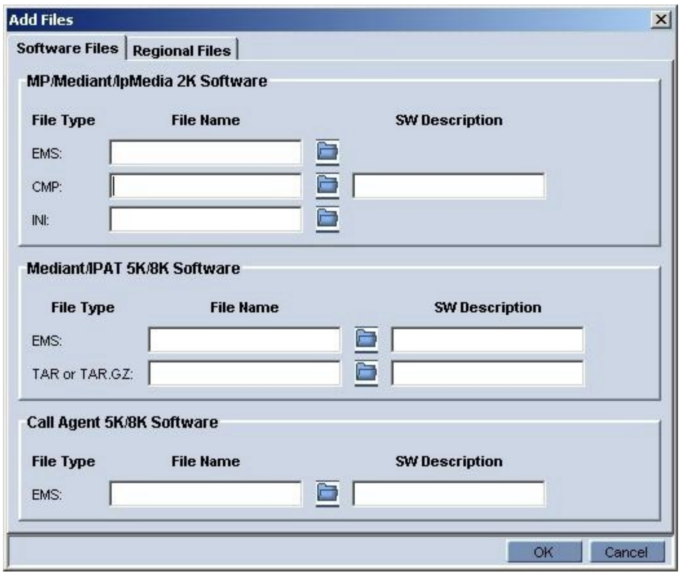
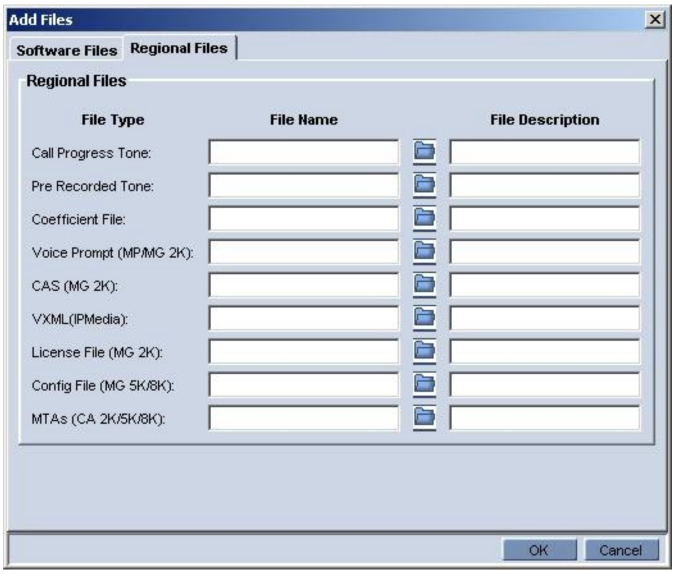


Figure 4-3: Add Files Screen in Software Manager - Regional Files



Add Files

Regional Files

File Type	File Name	File Description
Call Progress Tone:		
Pre Recorded Tone:		
Coefficient File:		
Voice Prompt (MP/MG 2K):		
CAS (MG 2K):		
VXML(IPMedia):		
License File (MG 2K):		
Config File (MG 5K/8K):		
MTAs (CA 2K/5K/8K):		

4.2 Removing Files from the Software Manager

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

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

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

5 Defining VoIP Devices, Managing the MG Tree

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

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

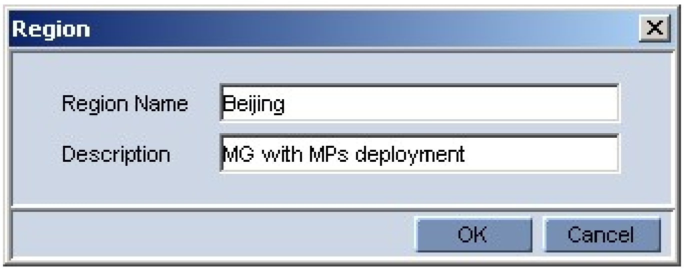
After defining the VoIP device, refer to section 'Basic Configuration' on page 41 to perform basic initialization of the device.

5.1 Configuring a Region

➢ To configure a region:

1. Right-click on Globe (the root) in the MG Tree and choose 'Add Region' from the submenu; the following screen appears:

Figure 5-1: Configuring a Region



Region Name: Beijing

Description: MG with MPs deployment

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

3. Press OK; the requested region is added.

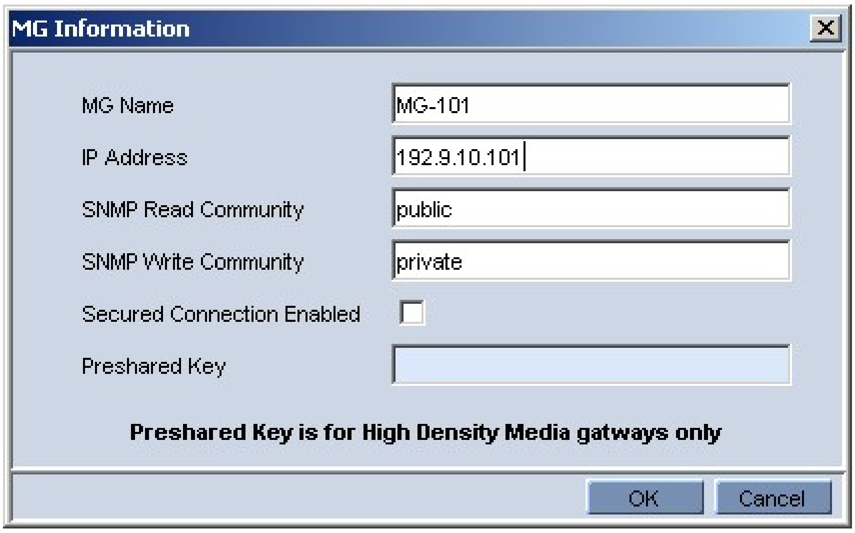
5.2 Defining a Media Gateway 3500

➢ To add a gateway, perform the following steps:

1. Add the gateway's software version file to the Software Manager. Use the file from the EMS or the gateway's CD, or contact Nortel for it. (Refer to 'Adding a New File to the Software Manager' on page 27).

2. Right-click the region in the Navigation tree to which to add a gateway and choose the option 'Add MG' from the submenu; the MG Information screen appears:

Figure 5-2: MG Information



MG Information

MG Name: MG-101

IP Address: 192.9.10.101

SNMP Read Community: public

SNMP Write Community: private

Secured Connection Enabled ☐

Preshared Key:

Preshared Key is for High Density Media gatways only

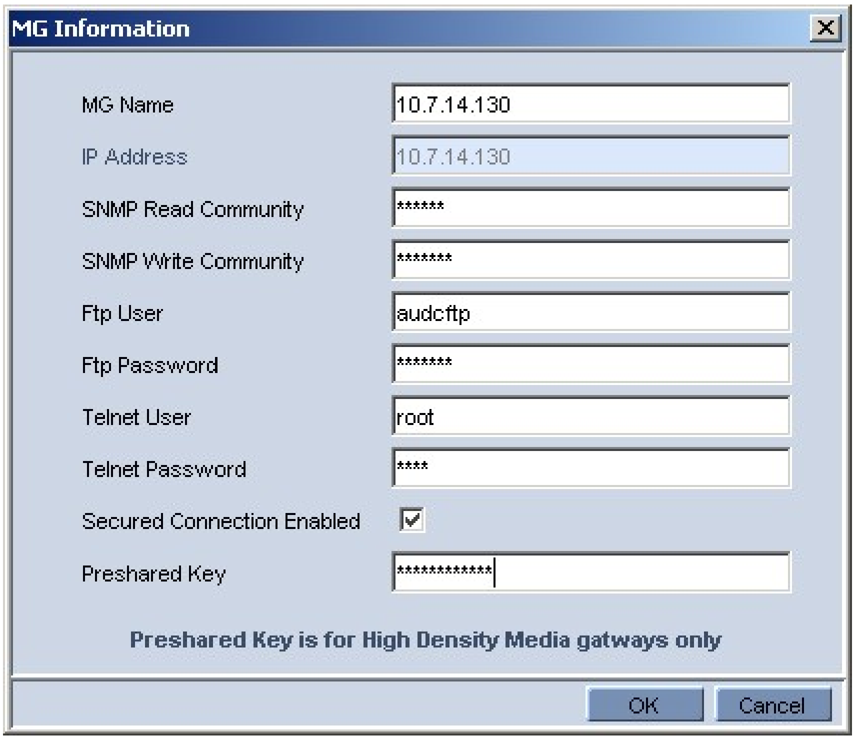
3. Define the gateway name, as you would like it to be referenced in the EMS; enter the gateway's IP Address, the gateway's SNMP Read and Write Community strings. If you're operating over a secured connection, check the option 'Secured Connection Enabled' and enter the Preshared Key provided by Nortel.

4. Press OK; the requested gateway is added to the required region.

5. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of it, including its LEDs, should be displayed in the EMS's Status screen (refer to the figures of the status panes). If you do not view a graphic representation of the gateway in the Status screen, refer to' Troubleshooting' on page 127 to resolve the issue.

6. To change the default FTP and Telnet user name and password, right-click in the MGs Tree on each gateway and choose ‘Details’; the MG Information screen opens (refer to the figure below).

Figure 5-3: MG Information - Secured Connection Enabled



MG Information

MG Name	10.7.14.130
IP Address	10.7.14.130
SNMP Read Community	******
SNMP Write Community	*******
Ftp User	audcftp
Ftp Password	*******
Telnet User	root
Telnet Password	****
Secured Connection Enabled	☑
Preshared Key	************

Preshared Key is for High Density Media gatways only

7. Define the FTP and Telnet user and password to be used during the Software Upgrade procedure. Note that the default username / passwords are:
   - a. SNMP Read Community: public
   - b. SNMP Write Community: private
   - c. FTP User: audcftp
   - d. FTP Password: audcftp
   - e. Telnet User: root
   - f. Telnet Password: root
8. To perform a basic configuration of the gateway, refer to 'Basic Configuration' on page 41.

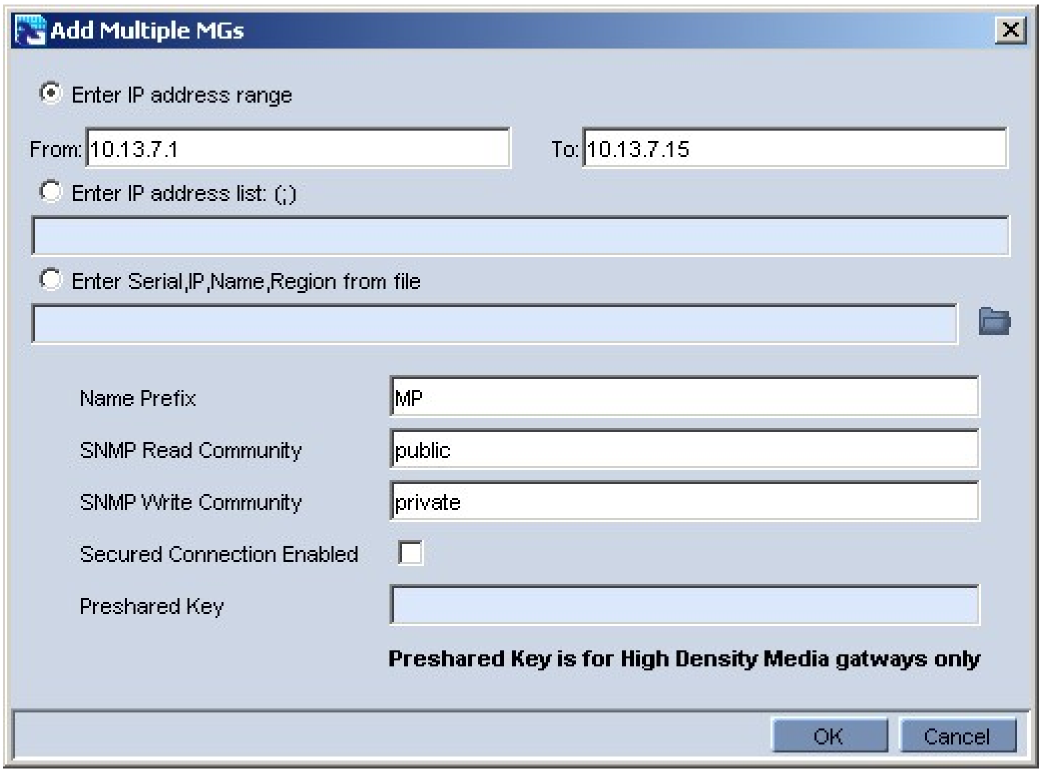
5.2.1 Defining Multiple Media Gateway 3500 Gateways

➢ To add a set of gateways simultaneously:

1. Add the gateways’ software version file to the Software Manager. Use the file from the EMS or the gateway’s CD, or contact Nortel for it. (Refer to 'Adding a New File to the Software Manager' on page 27).

2. Right-click the region in the MG Tree tree to which to add the multiple gateways and choose the option 'Add MG' from the submenu; the 'Add Multiple MGs' screen screen appears:

Figure 5-4: Add Multiple MGs



Add Multiple MGs

● Enter IP address range

From: 10.13.7.1 To: 10.13.7.15

○ Enter IP address list: (;)

○ Enter Serial,IP,Name,Region from file

Name Prefix: MP

SNMP Read Community: public

SNMP Write Community: private

Secured Connection Enabled: □

Preshared Key:

Preshared Key is for High Density Media gatways only

3. Check the 'Enter IP address range' check box, define the 'From' and 'To' fields and click OK. All devices in the defined range are added to the MG Tree with name combined as 'Name Prefix' + 'IP Address'.

4. Alternately, define multiple devices by checking check box 'Enter IP address list; in the field, define the IP addresses of the multiple gateways to be added, separating the IP address from each other with a semi colon.

5. Define the gateway name prefix as you would like it to be referenced in the EMS (a gateway's name comprises the prefix and IP address) and the gateway's SNMP Read and Write Community strings. If you're operating over a secured connection, check option 'Secured Connection Enabled' and enter the Preshared Key supplied by Nortel. The default Preshared Key is same for all gateways.

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

7. Verify that all the gateways are successfully defined in the EMS: Firstly, check the MGs List information; secondly, enter each gateway's status screen. Verify if the gateway is up and running (you can verify by performing a ping to its IP address). If it is up and running, a graphic representation of the gateway, including its LEDs, should be displayed in the Status screen (refer to the figures displaying gateway status under 'MediaPack' on page 61). If you do not view a graphic representation of the gateway in the Status screen, refer to 'Troubleshooting' on page 127 to resolve the issue.

8. To change the default FTP and Telnet user name and password, right-click in the MGs Tree on each gateway and choose ‘Details’. Define the FTP and Telnet user and password to be used during the Software Upgrade procedure.

9. To perform a basic configuration, refer to 'Media Gateway 3500' on page 41.

> Note: The last option of defining a Serial Number, IP and Name from the file is not supported for the Media Gateway 3500.

5.3 First-Time Connection Problems

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

1. Unknown Hardware: The Product Type, returned by the MIBII sysDescr value, is not recognized by the EMS. The gateway cannot be managed by the EMS.

2. Unknown Software: The Software Version, returned by the MIBII sysDescr value, is not recognized by the EMS. Either add the specified version to the EMS Software Manager or download one of the existing software versions.

5.4 Moving a Gateway from Region to Region

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

1. Drag the device from its current Region and drop it into the destination region

2. Alternatively, right-click on the gateway in the MG Tree and choose option ‘Move MG’ from the pop-up menu; a list of regions pops up.

3. Select a region from the list and press OK; the gateway is moved.

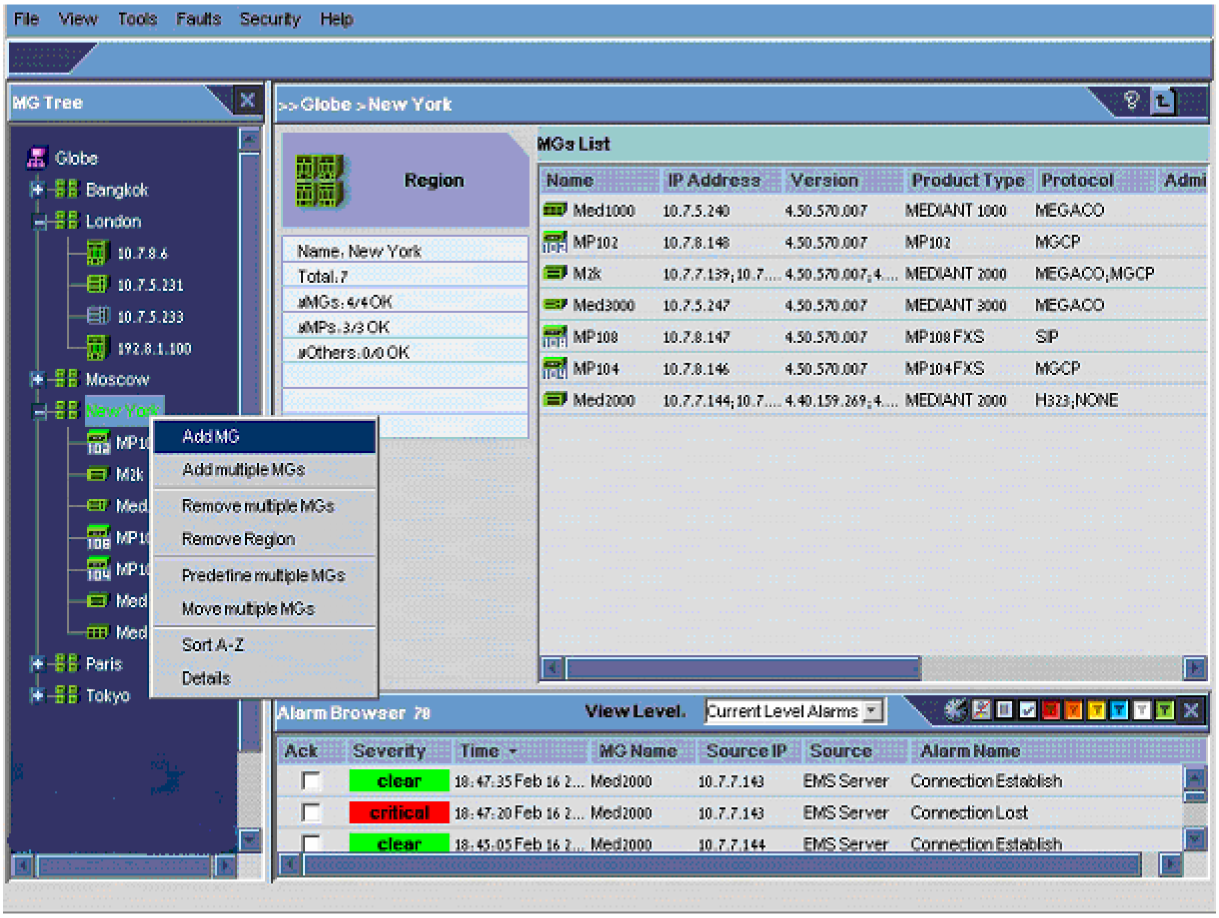
5.5 Moving Multiple Gateways from Region to Region

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

➢ To move multiple gateways from one region to another:

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

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



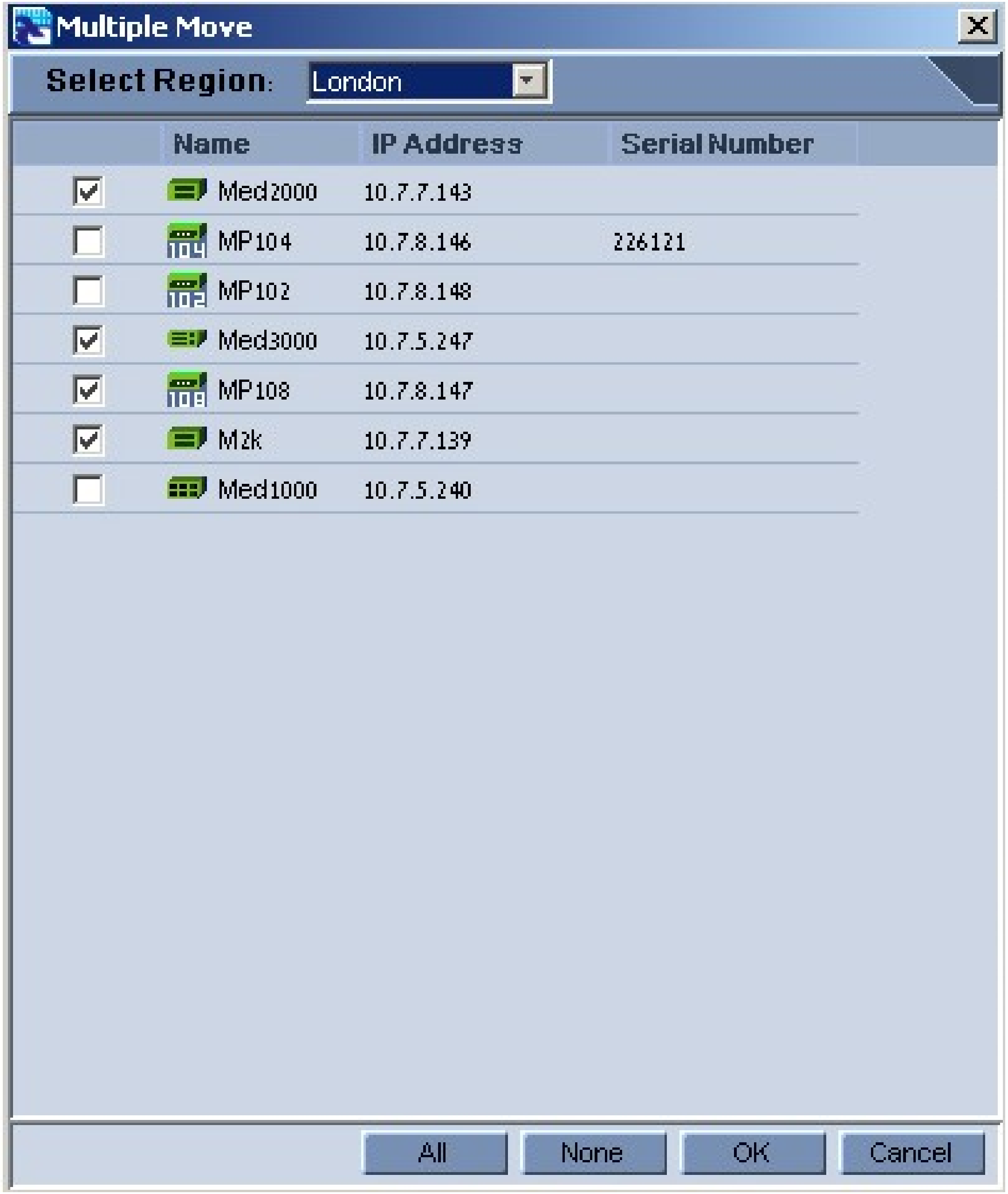
Name. New York
Total. 7
#MGs. 4/4 OK
#MPs. 3/3 OK
#Others. 0/0 OK

MGs List

Name	IP Address	Version	Product Type	Protocol	Admi
Med1000	10.7.5.240	4.50.570.007	MEDIANT 1000	MEGACO	
MP102	10.7.8.148	4.50.570.007	MP102	MGCP	
M2k	10.7.7.139; 10.7....	4.50.570.007; 4....	MEDIANT 2000	MEGACO;MGCP	
Med3000	10.7.5.247	4.50.570.007	MEDIANT 3000	MEGACO	
MP108	10.7.8.147	4.50.570.007	MP108 FXS	SIP	
MP104	10.7.8.146	4.50.570.007	MP104 FXS	MGCP	
Med2000	10.7.7.144; 10.7....	4.40.159.269; 4....	MEDIANT 2000	H323;NONE	

Ack	Severity	Time	MG Name	Source IP	Source	Alarm Name
☐	clear	18:47:35 Feb 16 2...	Med2000	10.7.7.143	EMS Server	Connection Establish
☐	critical	18:47:20 Feb 16 2...	Med2000	10.7.7.143	EMS Server	Connection Lost
☐	clear	18:45:05 Feb 16 2...	Med2000	10.7.7.144	EMS Server	Connection Establish

Figure 5-6: Multiple Move from Region to Region



Select Region: London

	Name	IP Address	Serial Number
☑	Med2000	10.7.7.143	
□	MP104	10.7.8.146	226121
□	MP102	10.7.8.148	
☑	Med3000	10.7.5.247	
☑	MP108	10.7.8.147	
☑	M2k	10.7.7.139	
□	Med1000	10.7.5.240	

2. In the ‘Multiple Move’ screen, select the gateways to move. To make your selection process quick and efficient, the screen provides you indicatations as to MG name, hardware type (icon), IP address and serial number.

3. From the ‘Select Region’ drop-down list, choose the name of the destination region to which to move the gateways.

4. Press OK; a Multiple Response screen opens, showing the results of the operation.

5.6 Removing a Gateway

➢ To remove a gateway:

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

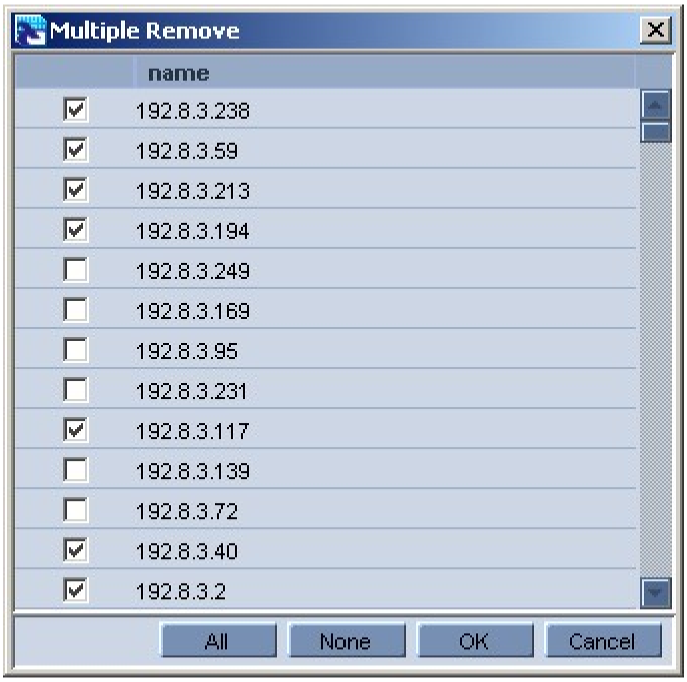
5.7 Removing Multiple Gateways

The EMS supports removing multiple gateways in a single screen (refer to the figure below), on condition that all devices are located in the same Region. Note that the Media Gateway 3500 should be locked prior to removal.

➢ To remove multiple gateways:

1. Right-click the region in the MG Tree and choose option 'Remove Multiple MGs' from the submenu; the ‘Multiple Remove’ screen is displayed:

Figure 5-7: Removing Multiple Media Gateways



	name
☑	192.8.3.238
☑	192.8.3.59
☑	192.8.3.213
☑	192.8.3.194
□	192.8.3.249
□	192.8.3.169
□	192.8.3.95
□	192.8.3.231
☑	192.8.3.117
□	192.8.3.139
□	192.8.3.72
☑	192.8.3.40
☑	192.8.3.2

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

5.8 Searching for a Gateway

➢ To search for a media gateway:

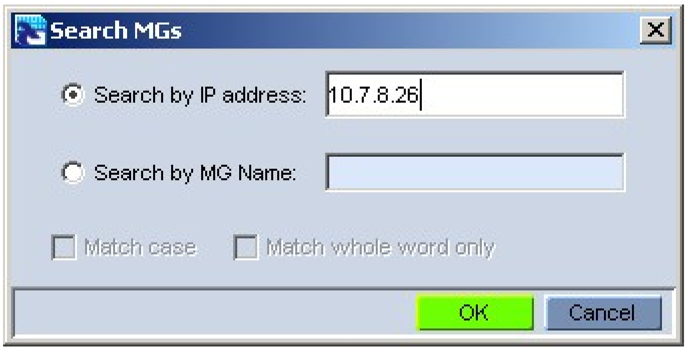
Either:

1. In the MG Tree, right-click on ‘Globe’ and select 'Search MG'.

   -OR-

2. In the Tools menu, choose option ‘Search MG’); the ‘Search MGs’ screen is displayed (refer to the figure below).

Figure 5-8: Search MGs (by IP Address)



Search MGs

● Search by IP address: 10.7.8.26

○ Search by MG Name:

□ Match case □ Match whole word only

3. Search by IP Address: Enter the media gateway’s IP address and press OK; if the media gateway is located, it is selected in the MG Tree and its Status screen is opened.

4. Search by MG Name: Enter the name of the media gateway you’re trying to locate and press OK; if more than one appropriate media gateway is located, the Search Result screen is displayed.

5. In the Search Result screen, locate the media gateway in the list and double-click it; the media gateway is selected in the MG Tree and its Status screen is opened.

Note that you can expedite your search for a media gateway (especially when searching by name) by checking the ‘Match case’ and/or ‘Match whole word only’ check boxes.

When only the ‘Match Case’ check box is checked, 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 checked, 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 checked, the EMS performs a search based on the text that the operator entered in the field ‘Search by MG Name’ as well as on the letter case.

6 Basic Configuration

6.1 Media Gateway 3500

The section explains how to connect the EMS to an existing, pre-installed gateway and configure the mandatory parameters required to activate all modules in the chassis.

Later, following this basic configuration, you'll need to provision the gateway more comprehensively in order to prepare it for service inside a given, specific network.

After performing a basic configuration, the EMS will manage the gateway and will show if the gateway hardware is operating correctly.

> Note: If you encounter a problem when defining the gateway in the EMS, refer to 'Troubleshooting' on page 127.

6.1.1 Configuring the Gateway IP Address, Booting the Boards

➢ **To run the gateway with all boards identified and operating:**

1. After defining each board, return up to the 'MG Status' screen (using the button ↰) and in the Info pane, click the link 'Properties'; the 'Media Gateway Parameters Provisioning' screen opens. Click the tab 'Boards Table' and in the 'Boards Table' screen, enter the IP and MAC address for each TP board (click twice on the relevant cell to enable address definition).

> Note: The Media Gateway 3500 gateways are delivered to customers with software pre-installed and with all boards factory pre-configured. However, due to the changed network environment following delivery, the default IP addresses of the boards are incorrect and must be reconfigured. MAC addresses remain correct and unchanged. Customers are recommended to copy the table of MAC IP addresses to an offline file and retained for reference.

- In the 'MGs Tree', unlock the gateway (right-click on it and choose option 'Unlock' from the pop-up).
- Lock and then Unlock each board (right-click on each in the Status screen's graphic representation and from the pop-up choose option 'Unlock').
- Verify that the gateway and all boards are Unlocked and Enabled (color-coded green).

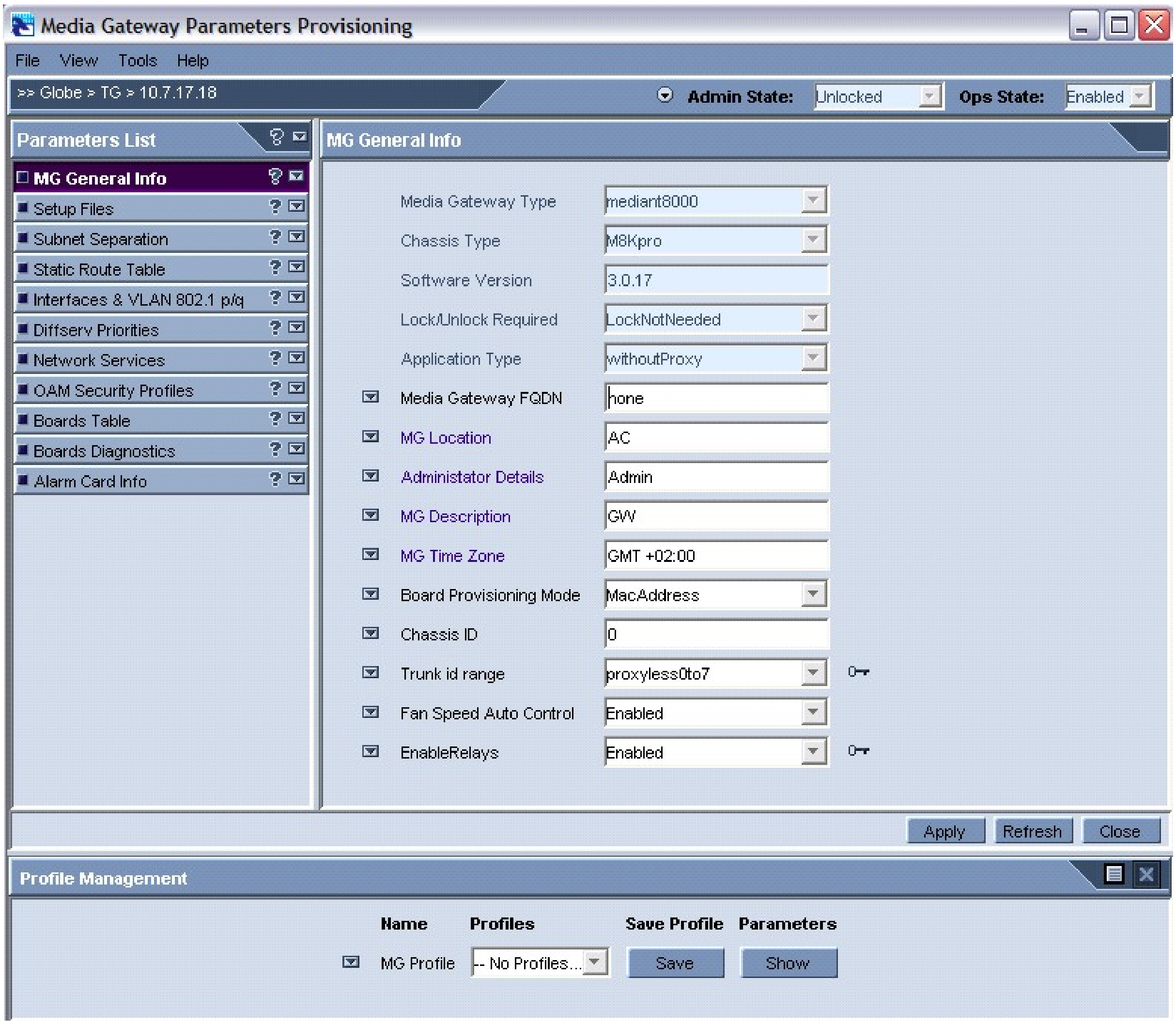
6.1.2 Getting Started with Provisioning a Gateway

➢ **To get started with provisioning a gateway:**

1. Select the gateway in the 'MG Tree'; its details are graphically represented in the MG Status pane.

2. In the Info pane, click the ‘Properties’ link; the ‘Media Gateway Parameters Provisioning’ screen opens (shown in the figure below).

Figure 6-1: Media Gateway 3500 Parameters Provisioning Screen



Admin State: Unlocked Ops State: Enabled

Media Gateway Type	mediant8000
Chassis Type	M8Kpro
Software Version	3.0.17
Lock/Unlock Required	LockNotNeeded
Application Type	withoutProxy
Media Gateway FQDN	none
MG Location	AC
Administator Details	Admin
MG Description	GW
MG Time Zone	GMT +02:00
Board Provisioning Mode	MacAddress
Chassis ID	0
Trunk id range	proxyless0to7
Fan Speed Auto Control	Enabled
EnableRelays	Enabled

Name	Profiles	Save Profile	Parameters
MG Profile	-- No Profiles...	Save	Show

➢ **To provision the gateway, define the fields in the Parameters Provisioning screen (refer to the figure above) according to the parameter explanations under:**

- 'Locking a Media Gateway' on page 43 and 'Unlocking a Media Gateway' on page 43
- 'Searching for a Provisioned Parameter' on page 77
- EMS Parameter Guide for the Media Gateway 3500

6.1.3 Locking a Gateway

➢ **To lock a gateway:**

1. In the MG Tree, expand the region in which the gateway is located and right-click on the gateway you want to lock. Alternatively, in the MG Tree, click on the region under which the gateway is located; the MGs List is displayed.
2. In the MGs List, select the gateway you need to lock; ensure from the identifying details that appear in the Status pane that this is indeed the gateway you need to lock.
3. Right-click on it in the MGs List and select the “Lock” option in the pop-up menu. Click “Yes” in the confirmation prompt.
4. Wait until the “lock” is finished.

6.1.4 Provisioning a Gateway

To bring a gateway to a state in which all boards are recognized and operating, select it in the MGs List so that its details are displayed in the Status pane, and in the Info pane click the “Properties” link; the Media Gateway Provisioning screen opens.

➢ **To provision the gateway, define the fields in the Parameters Provisioning screen (shown above) according to provisioning parameter explanations under:**

- EMS Parameter Guide for the Media Gateway 3500

6.1.5 Unlocking a Gateway

➢ **To unlock a gateway:**

1. In the MG Tree, expand the region under which the gateway you need to unlock is located, and right-click on the gateway. In the resulting pop-up, choose option “Unlocked”.
2. Alternatively, click on the region under which the gateway you need to lock is located; the MGs List is displayed. In the MGs List, right-click on the gateway to unlock and in the resulting pop-up menu, select the “Unlock” option.
3. Wait until the “unlock” process is completed.

7 Monitoring Multiple Media Gateways

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

Following are the EMS status components:

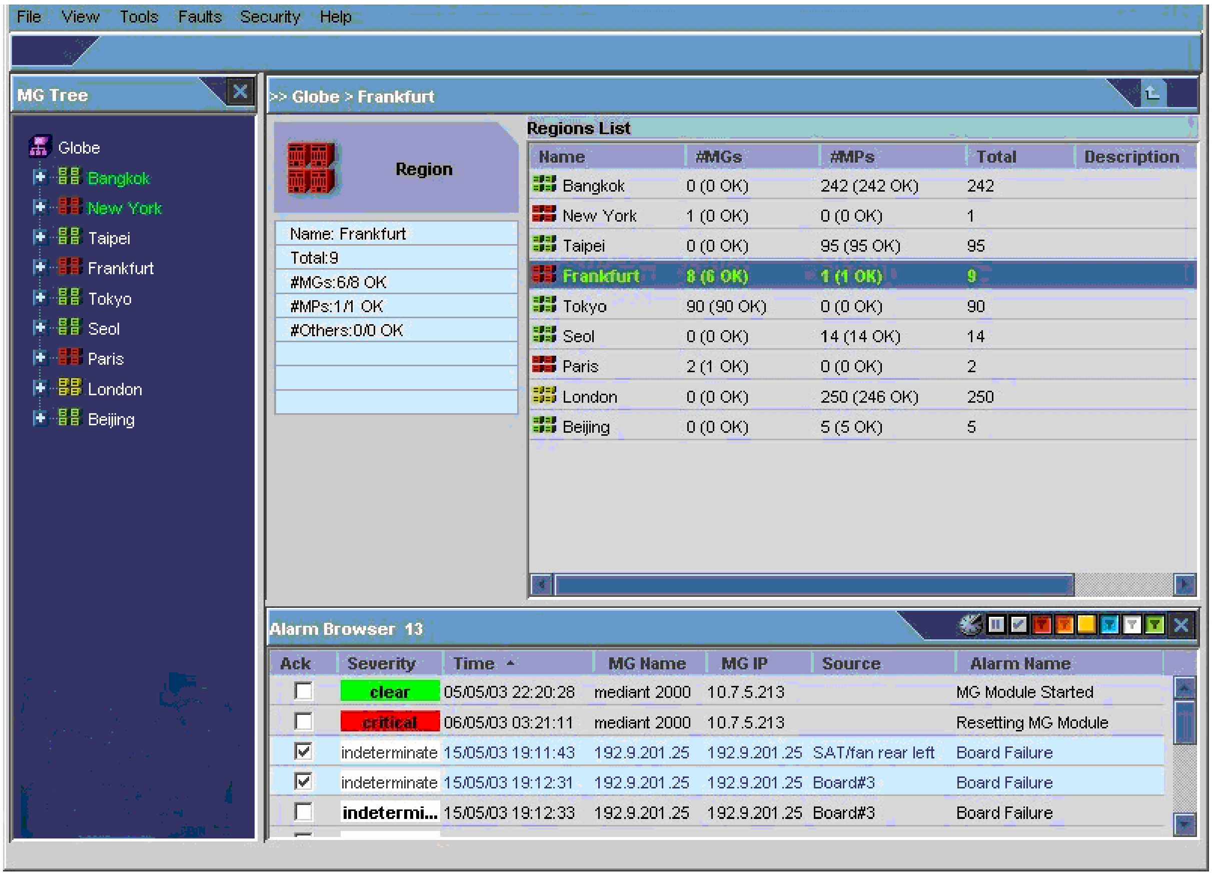
- 'Regions List' on page 45
- 'MGs List' on page 46

7.1 Regions List

➢ To access the Regions List:

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

Figure 7-1: Regions List



Name: Frankfurt
Total:9
#MGs:6/8 OK
#MPs:1/1 OK
#Others:0/0 OK

Regions List

Name	#MGs	#MPs	Total	Description
Bangkok	0 (0 OK)	242 (242 OK)	242	
New York	1 (0 OK)	0 (0 OK)	1	
Taipei	0 (0 OK)	95 (95 OK)	95	
Frankfurt	8 (6 OK)	1 (1 OK)	9	
Tokyo	90 (90 OK)	0 (0 OK)	90	
Seol	0 (0 OK)	14 (14 OK)	14	
Paris	2 (1 OK)	0 (0 OK)	2	
London	0 (0 OK)	250 (246 OK)	250	
Beijing	0 (0 OK)	5 (5 OK)	5	

Ack	Severity	Time ▲	MG Name	MG IP	Source	Alarm Name
□	clear	05/05/03 22:20:28	mediant 2000	10.7.5.213		MG Module Started
□	critical	06/05/03 03:21:11	mediant 2000	10.7.5.213		Resetting MG Module
☑	indeterminate	15/05/03 19:11:43	192.9.201.25	192.9.201.25	SAT/fan rear left	Board Failure
☑	indeterminate	15/05/03 19:12:31	192.9.201.25	192.9.201.25	Board#3	Board Failure
□	indetermi...	15/05/03 19:12:33	192.9.201.25	192.9.201.25	Board#3	Board Failure

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

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

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

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

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

Threshold: Each gateway group (digital gateways, analog MediaPacks and Unknown) has a threshold value: digital gateways = 1%, analog MediaPacks = 50%, Unknown = 50%.

The table below indicates how to quickly determine the status of a region and the status of the gateways defined under it.

Note: The Administrator can change the threshold numbers in the EMS server properties file.

Table 7-1: Region Status and Statuses of Gateways Defined Under It

Region Severity	Digital Gateways	Analog MediaPacks	Unknown	Comment
🟩 Clear (OK)	100% OK	100% OK	100% OK	The statuses of all gateways in the region are OK
🟨 Minor	Up to 1% failed	Up to 50% failed	Up to 50% failed	At least one of the groups has at least one gateway that has failed, but the number of failed gateways is less than the group threshold
🟥 Critical	1% or more failed	50% or more failed	50% or more failed	At least one of the groups has a number of failed gateways that exceeds the group threshold

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

7.2 MGs List

➢ To access the MGs List:

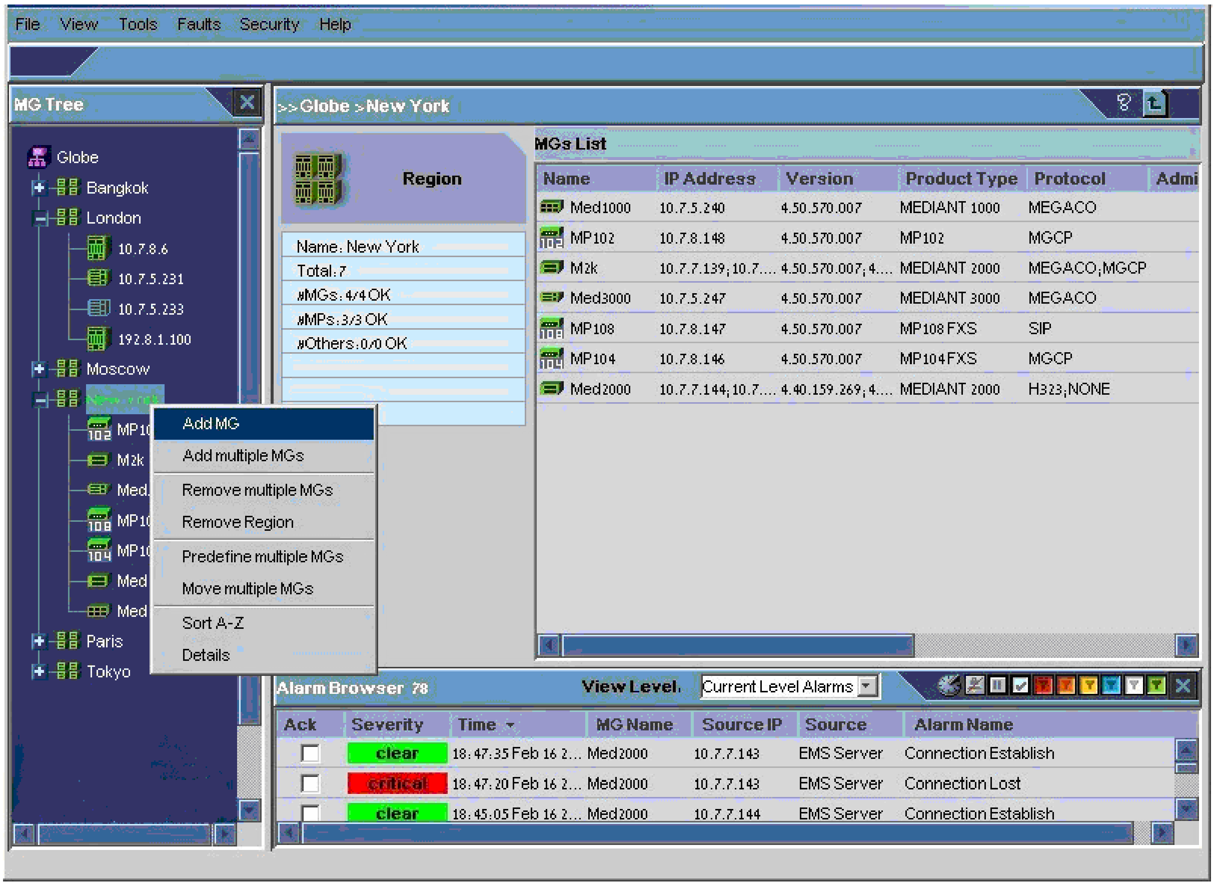
1. Click a region in the MG Tree; the MGs List pane is displayed in the Status pane of the main screen, listing all the gateways located under that region.

2. Right-click on a gateway to lock or unlock it, or to access its properties (access to a gateway's properties, i.e., to the Gateway Parameter Provisioning screen, can additionally be done by clicking the 'Properties' link in the Info pane after selecting the gateway in the MGs List).

3. Double-click a device in the MGs List; the Main Screen displays the Status pane.

4. Press the 'Up' button on the gateway level screens to return to the MGs List in the Main Screen.

Figure 7-2: MGs List



Name: New York
Total: 7
#MGs: 4/4 OK
#MPs: 3/3 OK
#Others: 0/0 OK

MGs List

Name	IP Address	Version	Product Type	Protocol	Admi
Med1000	10.7.5.240	4.50.570.007	MEDIANT 1000	MEGACO	
MP102	10.7.8.148	4.50.570.007	MP102	MGCP	
M2k	10.7.7.139;10.7....	4.50.570.007;4....	MEDIANT 2000	MEGACO;MGCP	
Med3000	10.7.5.247	4.50.570.007	MEDIANT 3000	MEGACO	
MP108	10.7.8.147	4.50.570.007	MP108 FXS	SIP	
MP104	10.7.8.146	4.50.570.007	MP104FXS	MGCP	
Med2000	10.7.7.144;10.7....	4.40.159.269;4....	MEDIANT 2000	H323;NONE	

Alarm Browser 78 View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source IP	Source	Alarm Name
□	clear	18:47:35 Feb 16 2...	Med2000	10.7.7.143	EMS Server	Connection Establish
□	critical	18:47:20 Feb 16 2...	Med2000	10.7.7.143	EMS Server	Connection Lost
□	clear	18:45:05 Feb 16 2...	Med2000	10.7.7.144	EMS Server	Connection Establish

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

- Gateway name & status (status is indicated by the color coding)
- Gateway IP address
- SW Version
- Product Type (Media Gateway 3500)
- Protocol (MEGACO or None)
- Administrative State (Shut Down/Locked/Unlocked)
- Operational State (Enabled/Disabled)

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

7.3 Media Gateway Level Status Pane

➢ To access a media gateway:

Either:

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

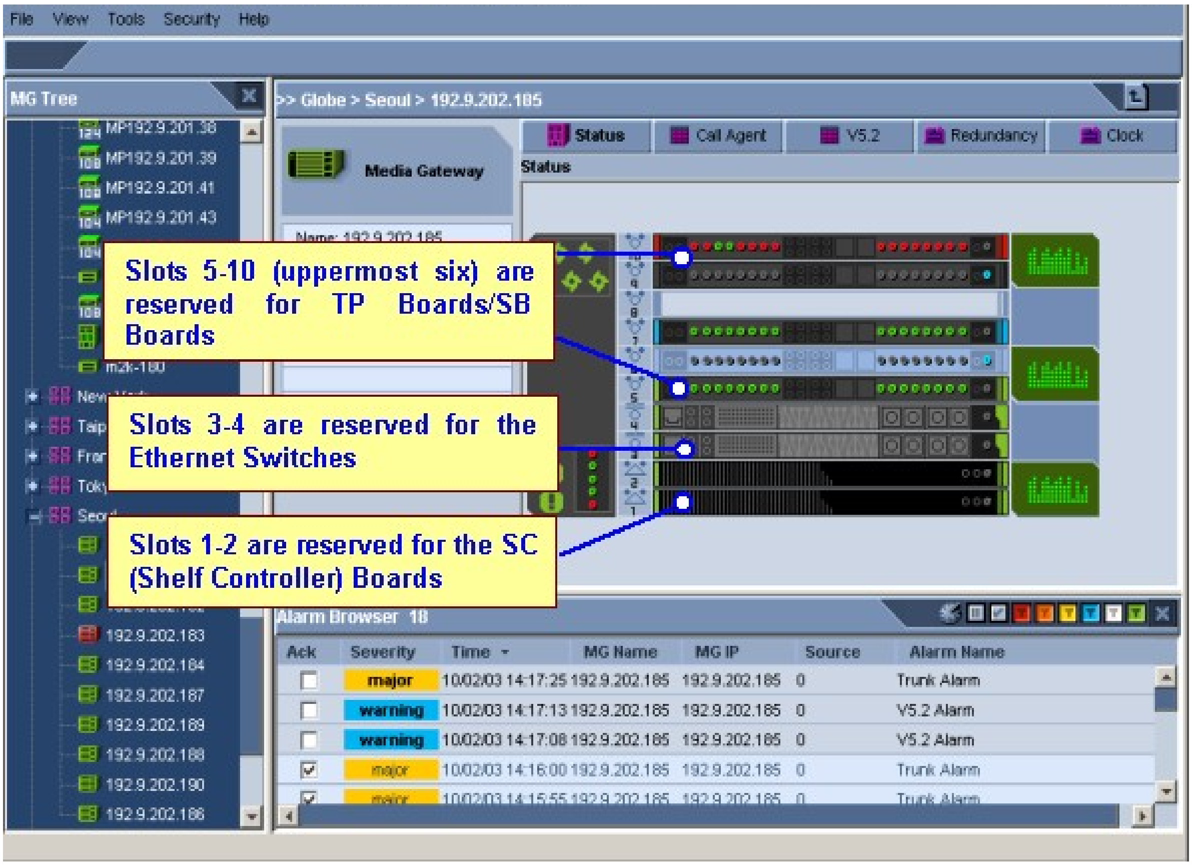
  -OR-

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

8 Media Gateway 3500 Media Gateways

8.1 Media Gateway 3500 Status Pane

Figure 8-1: Media Gateway 3500 Status Pane



Slots 5-10 (uppermost six) are reserved for TP Boards/SB Boards

Slots 3-4 are reserved for the Ethernet Switches

Slots 1-2 are reserved for the SC (Shelf Controller) Boards

Ack	Severity	Time	MG Name	MG IP	Source	Alarm Name
□	major	10/02/03 14:17:25	192.9.202.185	192.9.202.185	0	Trunk Alarm
□	warning	10/02/03 14:17:13	192.9.202.185	192.9.202.185	0	V5.2 Alarm
□	warning	10/02/03 14:17:08	192.9.202.185	192.9.202.185	0	V5.2 Alarm
☑	major	10/02/03 14:16:00	192.9.202.185	192.9.202.185	0	Trunk Alarm
☑	major	10/02/03 14:15:55	192.9.202.185	192.9.202.185	0	Trunk Alarm

Status for the Media Gateway 3500 includes:

1. Alarm Cards Status - each alarm card is represented as "!" near the corresponding SC board.
   Color convention: Red = Failed, Green = OK

   Shelf LEDs

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

   1. System: Red = System Error occurred; Green = OK
   2. Critical: Red = Critical Error occurred; Green = OK
   3. Major: Orange = Major Error occurred; Green = OK
   4. Minor: Yellow = Minor Error occurred; Green = OK
   5. Shelf: Red = Critical Error occurred; Orange = Major Error occurred; Green = OK; Gray = Off

2. Fan status - Fans' two rows are read as follows:

- Top Row: Top Front, Top Rear
- Bottom Row: Bottom Front, Bottom Middle, Bottom Rear

Color convention: Red = Failed; Green = OK

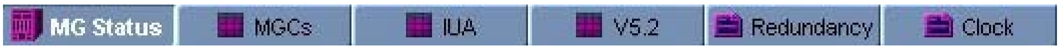
3. Boards status
   - Background color: Dark Gray = Active board; Blue = Redundant board
   - Upper & lower color: Gray = Lock, Red = Disabled, Green = Enabled, Orange = Major Severity
4. Trunks status
   - Trunk LEDs color convention: Red=Disabled, Green=Enabled, Gray=Locked
5. Power Suppliers Status

   Color convention: Red = Failed; Green = OK

8.1.1 Navigation Buttons to Provision the Media Gateway 3500

The figure below shows the navigation buttons used to provision the gateway.

Figure 8-2: Navigation Buttons to Provision the Media Gateway 3500



- **Button 1: Media Gateway Status**
- **Button 2**: **MGCs (Media Gateway Controllers)**

  The media gateway supports numerous MGCs (Media Gateway Controllers) so that the media gateway's resources can be distributed over up to 15 simultaneous active MGCs. Click the button to evoke the MGCs List. Each listed entry represents a single MGC. To add/remove a Group, lock/unlock a Group or access a Group's properties, right-click (or double-click) a row.

  The MGCs Group is a group of MGCs; one is active, all others are alternate managers in case the first fails. The group must always contain at least one MGC. One of the MGCs is assigned to be *primary*, while the others are the *back-up* MGCs. All MGCs in the same group have the same parameters in terms of managed PSTN circuits (like protocol or channels characteristics). There is always only one active MGC in an MGCs Group.
- **Button 3: IUA** (ISDN Q.921-User Adaptation Layer)

Note: The IUA button is only relevant to media gateway version 2.2 when working with an IUA proxy.

Click this button to define all Application Server Processes (ASPs). To add/remove an ASP group, lock/unlock it, or access its properties, right-click a row (or double-click) and choose the action you require from the popup.

- **Button 4: V5.2 Interfaces**

  Not applicable to the MG 3500.
- **Button 5: Redundancy Group Properties**

Use this button to access the properties of the Redundancy Group. Two redundancy types can be defined: Enhanced Redundancy and Redundancy.
If the redundant TP board (for example) is defined in its properties as an *Enhanced Redundancy* redundancy-type board, the calls in a failed TP are *immediately* transferred to the redundant board and are resumed *in milliseconds*. The failed TP board is automatically reset and if normal functioning is restored, the calls revert back to it.

If the redundant TP board is defined in its properties as a *Redundancy* redundancy-type board, the failed TP board is automatically reset and when normal functioning is restored, calls that were previously active in it are restored.

- **Button 6: Clock Properties**

  Use this button to access the parameters that define the clock references for the entire media gateway (for all TP boards residing within the media gateway). The slot number for the primary and secondary clock reference is defined here as well. Note that the trunk for clock reference is chosen according to the clock reference priority, defined per trunk in the Trunk List.

8.2 Media Gateway 3500 Maintenance Actions

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

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

Version 3.0 Board Actions:

- Right-click on the board; a popup menu listing available Board Actions is displayed. In media gateways version 3.0, board actions are dependent on board type and state.

Table 8-1: Board Actions (for Gateways version 3.0)

Board Icon	Board Type	Action	Supported Maintenance Actions	Action Description
▨	SC Board	Switch Over	When a redundant SC board is present	
▨	TP-1610 Board	Switch Over	Board is **unlocked** and **active**	
		Switch Back	**Board is switched-over**	
		Lock	Always	Caution: This action resets the board and drops all active calls on it.
		Unlock	Always	
		Remove	Board is Locked	
		Make Board Redundant	Board is Locked	
		Make Board Active	Board is Locked & redundant	
▨	Empty Board	Add TP-1610 Board		

Version 2.1 Board Actions:

- Right-click on the board; a pop-up menu listing available Board Actions is displayed. In media gateways version 2.1, board actions are dependent on board type and state.

Table 8-2: Board Actions (for Gateways version 2.1)

Board Icon	Board Type	Action	Supported Maintenance Actions	Action Description
	SC Board	Switch Over	When a redundant SC board is present	
	Ethernet Switch Board	Lock	Always	
		Unlock	Always	
		Reset	Always	
	TP-1610 Board	Switch Over	Board is **unlocked** and **active**	
		Switch Back	**Board is switched-over**	
		Lock	Always	Caution: This action resets the board and drops all active calls on it.
		Unlock	Always	
		Remove	Board is Locked	
		Make Board Redundant	Board is Locked	
		Make Board Active	Board is Locked & redundant	
	Empty Board	Add TP 1610 Board		
				Call Agent IP address should be provided

Note: In the Media Gateway 3500, slots 5-10 inclusively are reserved for TP boards, slots 1-2 are reserved for the SC (System Controller) Boards, and slots 3-4 are reserved for the Ethernet Switch boards.

9 Accessing a TP-1610 in a Media Gateway 3500 (v3.0)

➢ To access the 'Board Provisioning Parameters' screen:

1. In the 'MG Status' pane, select the board (depicted in the graphic representation of the gateway) to which you require access; the Board Information pane is updated with the board's identifying information.
2. In the Board Information pane, click the "Properties" link; the 'Board Provisioning Parameters' screen is displayed.

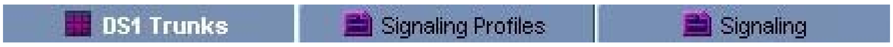
➢ To access the board's 'Trunks List' screen:

1. Double-click on the board (whose Trunk List you need to access) in the graphic representation of the gateway (alternatively, right-click on it and select the option Trunk List from the pop-up menu); the Trunk List is displayed, including the board-level navigation buttons.
   Refer to 'Navigation Buttons to Provision the TP-1610 Board' on page 55.
2. Right-click on an occupied row to lock, unlock, or access that trunk's properties.

9.1 Navigation Buttons to Provision the TP-1610 Board

The figure below shows the navigation buttons used to provision the TP-1610 board.

Figure 9-1: Navigation Buttons to Provision the TP-1610 Board



For detailed information, refer to the documentation on the TP-1610 signaling profiles and signaling submenus below.

- **Button 1: DS1 Trunks**

  Use this button to access the definitions for the 16 E1/T1 trunks (0-15) in the TP board in the gateway system. Each row in the Trunk List of the board-level screen refers to a single E1 or T1 trunk. Select an E1/T1 trunk (0-15) in the Trunk List and click the 'Properties' link to access that trunk's Parameters Provisioning screen.

10 Accessing a TP-1610 in a Media Gateway 3500 (v2.1)

➢ To access the 'Board Provisioning Parameters' screen:

1. In the 'MG Status' pane, select the board (depicted in the graphic representation of the gateway) to which you require access; the Board Information pane is updated with the board's identifying information.
2. In the Board Information pane, click the "Properties" link; the 'Board Provisioning Parameters' screen is displayed.

➢ To access the board's 'Trunks List' screen:

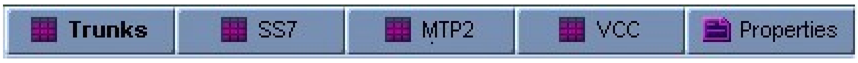
1. Double-click on the board (whose Trunk List you need to access) in the graphic representation of the gateway (alternatively, right-click on it and select the option Trunk List from the pop-up menu); the Trunk List is displayed, including the board-level navigation buttons.
   Refer to 'Navigation Buttons to Provision the TP-1610 Board' on page 55.

2. Right-click on an occupied row to lock, unlock, or access that trunk's properties.

10.1 Navigation Buttons to Provision a TP-1610

The figure below shows the navigation buttons used to provision the TP-1610 board.

Figure 10-1: Navigation Buttons to Provision the TP-1610 Board



- **Button 1: E1/T1 Trunks**

  Use this button to access the definitions for the 16 E1/T1 trunks (0-15) in the TP board in the gateway system. Each row in the Trunk List of the board-level screen refers to a single E1 or T1 trunk. Select an E1/T1 trunk (0-15) in the Trunk List and click the 'Properties' link to access that trunk's Parameters Provisioning screen.

- **Buttons 2 through 4: SS7, MTP2, and VCC**

  Not applicable to the Media Gateway 3500.

- **Button 5: Properties**

  Use this button to access the definitions of the overall board properties.

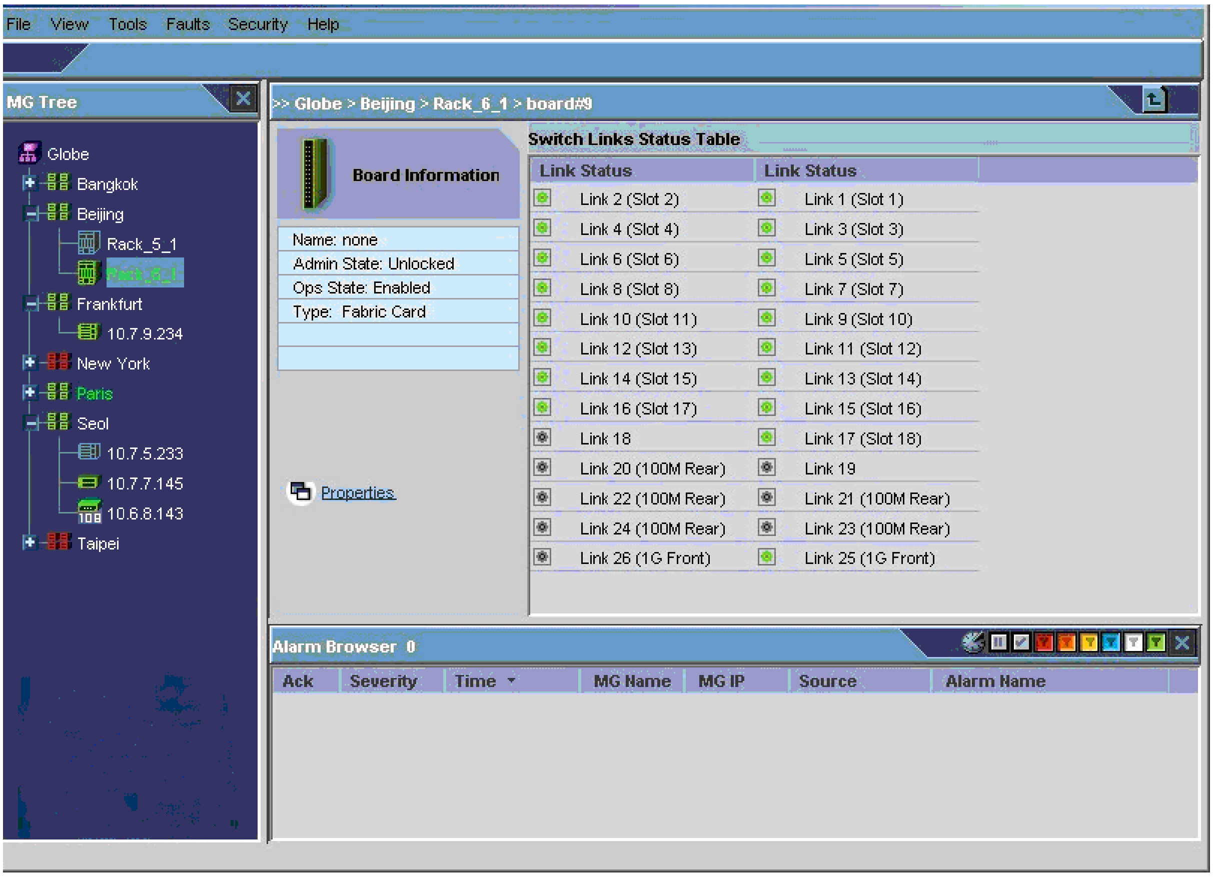
11 Ethernet Switch Board's Links' Status

Ethernet Switch boards populate slots 3 and 4 in the Media Gateway 3500. Each contains a maximum of 26 links, of which 19 are used internally, two externally from/to the Gigabit Ethernet link, and five can be made available if a dedicated RTM is inserted behind the ES board.

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

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

Figure 11-1: Switch Links Status Screen



Name: none
Admin State: Unlocked
Ops State: Enabled
Type: Fabric Card

Switch Links Status Table

Link Status		Link Status	
🟢	Link 2 (Slot 2)	🟢	Link 1 (Slot 1)
🟢	Link 4 (Slot 4)	🟢	Link 3 (Slot 3)
🟢	Link 6 (Slot 6)	🟢	Link 5 (Slot 5)
🟢	Link 8 (Slot 8)	🟢	Link 7 (Slot 7)
🟢	Link 10 (Slot 11)	🟢	Link 9 (Slot 10)
🟢	Link 12 (Slot 13)	🟢	Link 11 (Slot 12)
🟢	Link 14 (Slot 15)	🟢	Link 13 (Slot 14)
🟢	Link 16 (Slot 17)	🟢	Link 15 (Slot 16)
⚫	Link 18	🟢	Link 17 (Slot 18)
⚫	Link 20 (100M Rear)	⚫	Link 19
⚫	Link 22 (100M Rear)	⚫	Link 21 (100M Rear)
⚫	Link 24 (100M Rear)	⚫	Link 23 (100M Rear)
⚫	Link 26 (1G Front)	🟢	Link 25 (1G Front)

Ack	Severity	Time	MG Name	MG IP	Source	Alarm Name

The figure above shows the status of each link in the Switch Links Status screen of the Media Gateway 3500, mapping which link is connected to each board. Link status can be either:

Green - OK

or

Gray - not connected

12 Provisioning Concepts

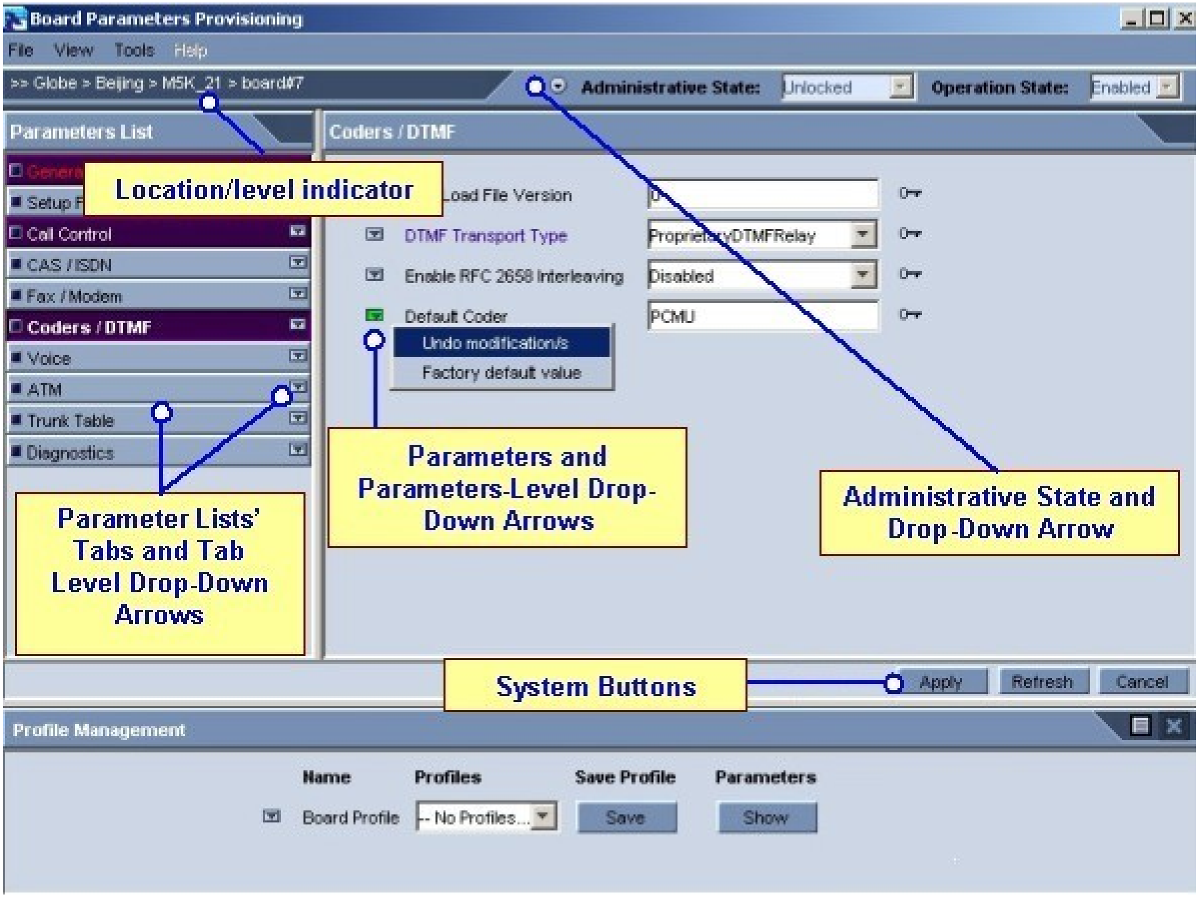
12.1 Working with the EMS's Provisioning Screens

All screens in the EMS that enable operators to provision the media gateway, 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 system hierarchy to select the entity to be provisioned. In that entity's Info pane, press the 'Properties' link, or press the parameters provisioning screen's buttons on the top of the Status pane; the provisioning screen for that specific entity is displayed.

A single provisioning screen, that of a TP board, is presented in the figure below by way of example. All entities are provisioned in exactly the same way as the board whose provisioning screen shown here is provisioned.

Figure 12-1: Media Gateway 3500 Board Parameters Provisioning Screen



Administrative State: Unlocked
Operation State: Enabled

Load File Version: 0
DTMF Transport Type: ProprietaryDTMFRelay
Enable RFC 2658 Interleaving: Disabled
Default Coder: PCMU

Name: Board Profile
Profiles: -- No Profiles...

The Board Provisioning screen displayed in the figure contains:

- Toolbar

  Includes the path of the EMS-managed entity (in the case of the illustrative example shown in the figure above, Board #7 in the media gateway named M5K_21 located under the region of Beijing), as well as its Administrative State (Locked/Unlocked) and its Operational State (Enabled/Disabled). The Administrative State of the board can be changed using the Administrative State drop-down arrow.

- 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 12-1: Provisioning Parameters in the Board Provisioning Screen – Color Codes

Color	Meaning
Red on violet	Error in data as a result of operator’s modification
White on violet	The button was modified and all data in it is valid.
Black on blue	Button is not modified and all data in it is valid
Green on dark blue	Currently viewed button
Green on violet	Currently viewed and already modified button
Red on blue	Error in data produced by the media gateway

- 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.

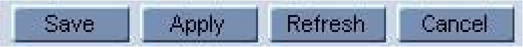
  Each drop-down combo lists two actions that operators can optionally perform (for each individual parameter and for each provisioning parameters category:

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

- 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 12-2: System Buttons in Board Parameters Provisioning Screen



Save - Save your changes.

Apply - Load your changes to the gateway.

Refresh - Read the current gateway setting (replace your changes with the current data).

Cancel - Cancel your changes and close the screen.

12.1.1 Provisioning Procedure for Media Gateway 3500 Gateways

➢ **To provision a Media Gateway 3500, follow these procedures:**

1. In the Main Screen, navigate to the element/entity to provision, select it (for a gateway, select it in the MGs List under the region; for a board, select it in the graphic representation of the gateway; and for a trunk, select it in the Trunk List), and in the Info pane click the 'Properties' link; the provisioning screen for that element is displayed.
2. Modify the required parameters using the interface-context buttons.
3. Change the managed element/entity to the 'Locked' Administrative State (refer to the bullet 'Toolbar', above).
4. Press the 'Apply' system button; your changes are loaded to the gateway.
5. Change the managed element/entity to the 'Unlocked' Administrative State (refer to the bullet 'Toolbar', above) to return it to service.
6. Press 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).

Note: If you make a mistake in the provisioning process, the system notifies you and prompts you for the corrective action.

12.2 Parameters Provisioning Types

The EMS features three provisioning parameter types:

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

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

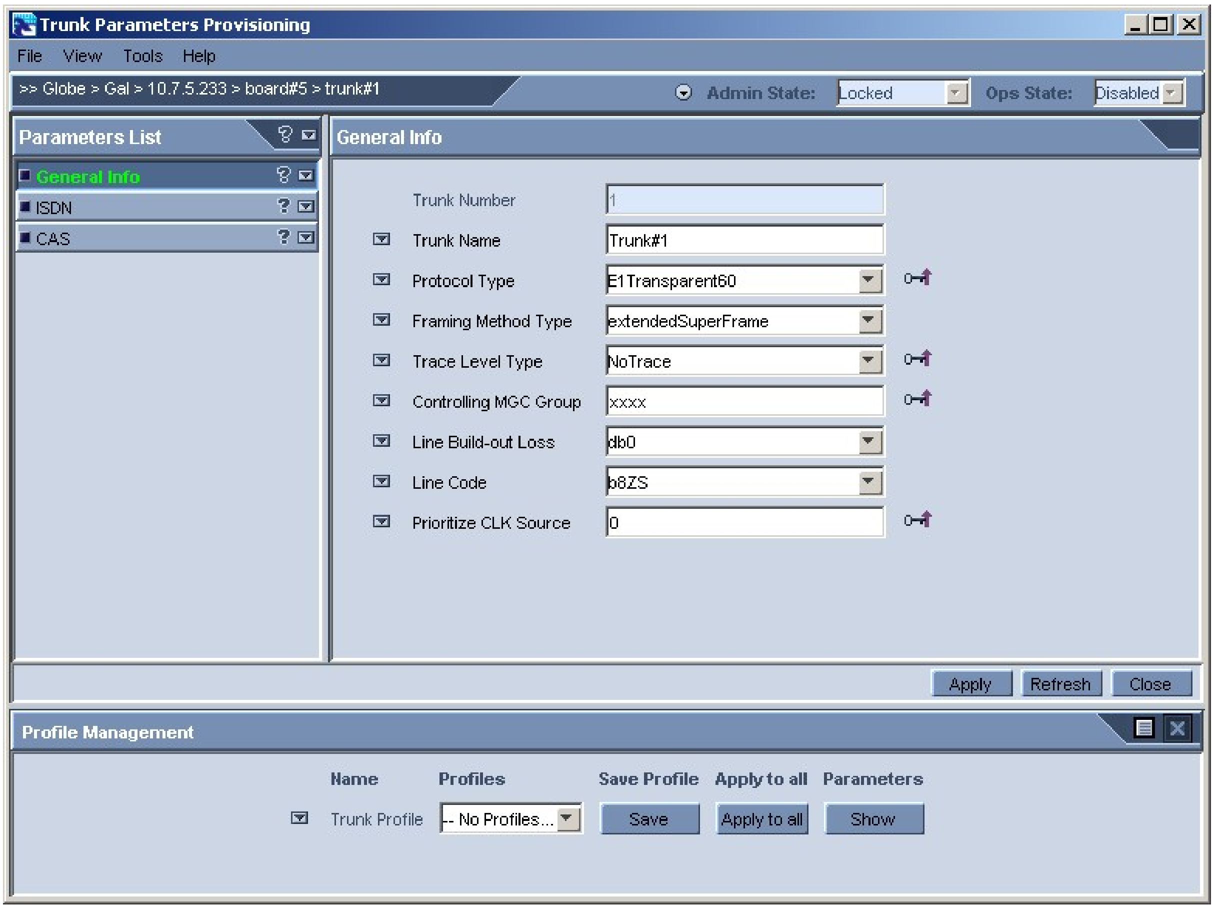
Table 12-2: Indication Mapping Summary

Parameter Provisioning Type	Indication / Gateway Type	Description
Instant	No indication	Press ‘Apply’, ‘OK’ button to load changes to the media gateway.
Online	🔑	Lock / Unlock modified entity (trunk, for example)
Offline	🔑⬆ Media Gateway 3500	Lock/Unlock the physical entity within/under which the managed entity is located, and the managed entity itself

- ‘**Online**’ - To configure an ‘Online’ mode parameter (indicated in the EMS by the icon 🔑 adjacent to the parameter), you need to lock *only the entity containing the parameter*. *You do not need to lock the board/media gateway* containing the entity. The mode is called ‘Online’ because the parameter can be configured without resetting any board in the media gateway.
- **‘Offline’ -** To configure an ‘Offline’ mode parameter (indicated in the EMS by the icon 🔑⬆ adjacent to the parameter), you need to lock the board/media gateway containing the entity as well as the entity in order to configure the entity’s parameter. The mode is called ‘Offline’ because all calls active on the board/media gateway containing the entity’s parameter are dropped when you lock the board/media gateway and entity in order to configure the parameter.

- **'Instant' -** An 'Instant' mode parameter can be configured on the fly; the configuration takes effect immediately. No icon is displayed adjacent to the parameter in the EMS GUI. No locking or unlocking of the entity or of the board/media gateway is required to perform the configuration.

Figure 12-3: Trunk Parameters Provisioning Screen



>> Globe > Gal > 10.7.5.233 > board#5 > trunk#1

Admin State: Locked

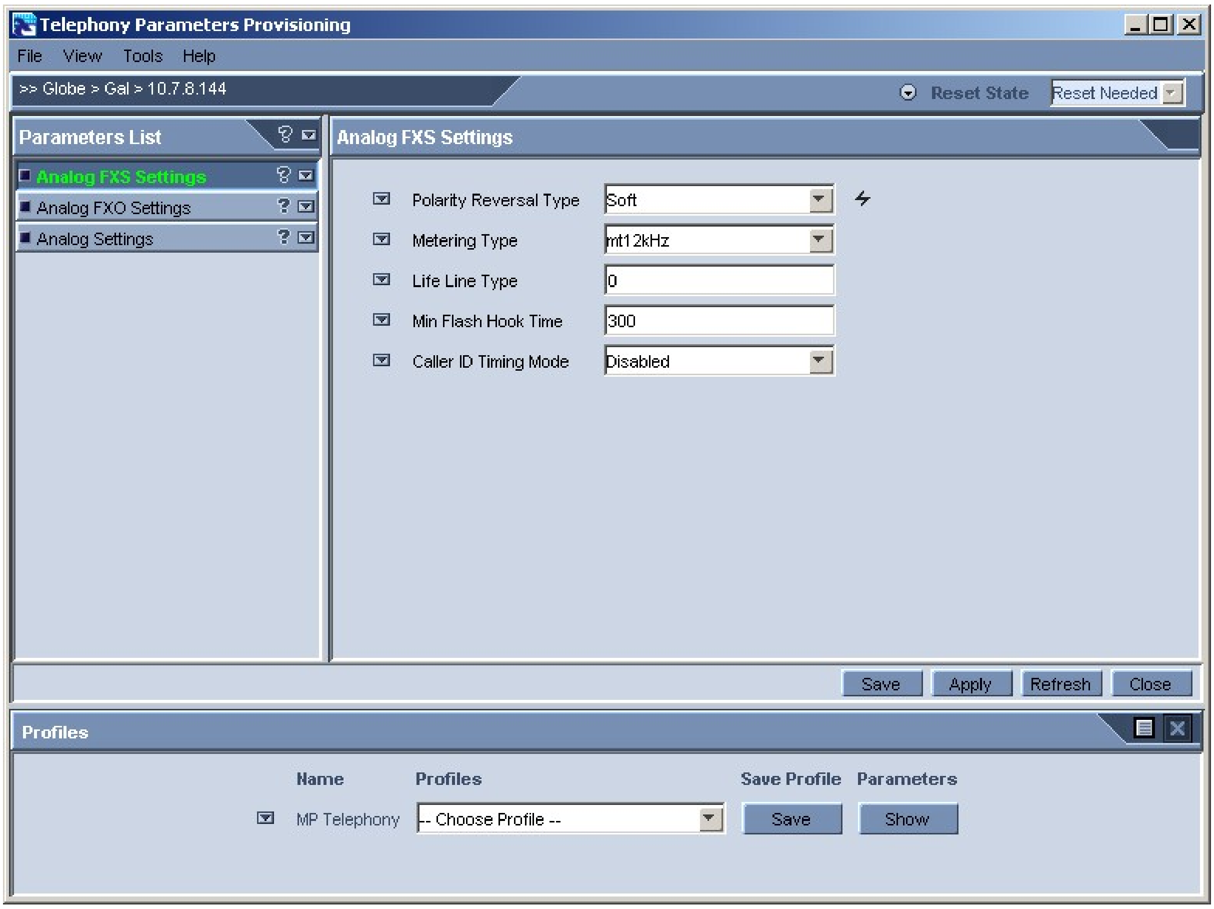
Ops State: Disabled

General Info

Trunk Number	1
Trunk Name	Trunk#1
Protocol Type	E1Transparent60
Framing Method Type	extendedSuperFrame
Trace Level Type	NoTrace
Controlling MGC Group	xxxx
Line Build-out Loss	db0
Line Code	b8ZS
Prioritize CLK Source	0

Name	Profiles	Save Profile	Apply to all	Parameters
Trunk Profile	-- No Profiles...	Save	Apply to all	Show

Figure 12-4: Telephony Parameters Provisioning Screen



Analog FXS Settings

Polarity Reversal Type: Soft

Metering Type: mt12kHz

Life Line Type: 0

Min Flash Hook Time: 300

Caller ID Timing Mode: Disabled

12.3 Exporting, Importing an Entity Configuration as a File

The EMS enables operators to export an entity's entire parameters provisioning screen as a file.

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.

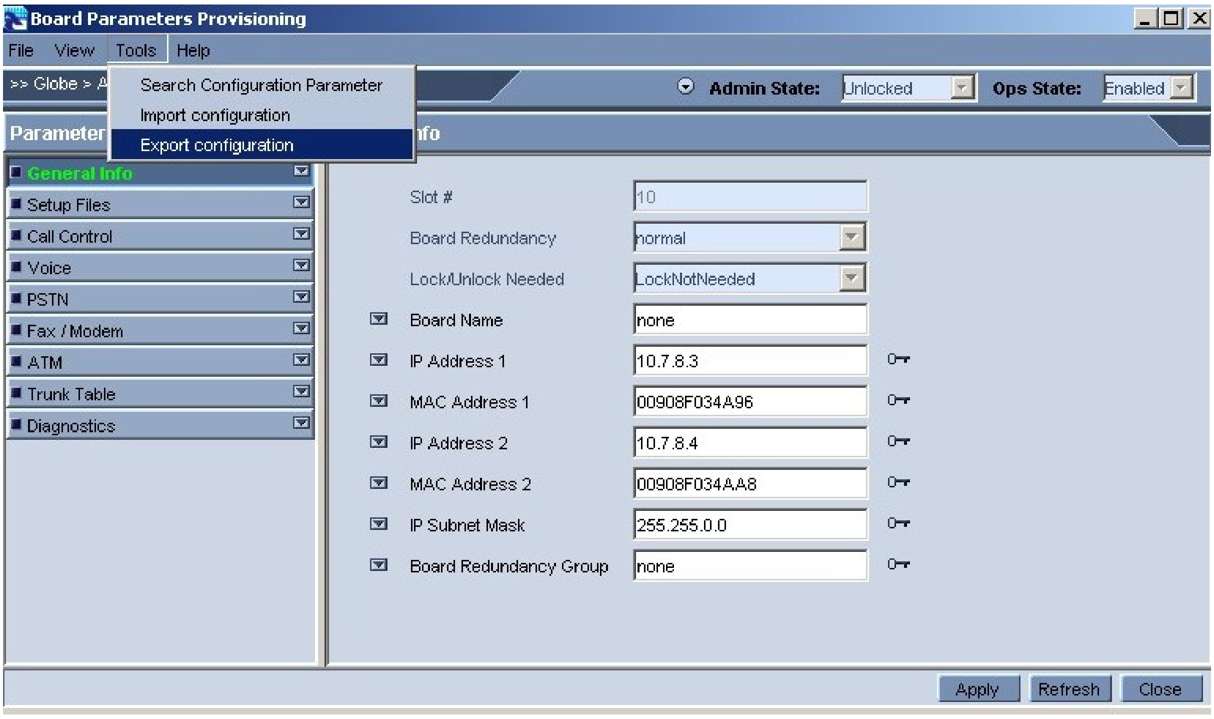
After the file is imported, operators can view the imported parameter configurations in the provisioning screen and decide whether or not to apply the configurations to the entity (by clicking the 'Apply' button).

After the 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 the same EMS.

➢ To export an entity's parameters provisioning screen as a file, take these steps:

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 .prv is created.

Figure 12-5: Export Configuration Screen



Admin State: Unlocked
Ops State: Enabled

Slot #	10
Board Redundancy	normal
Lock/Unlock Needed	LockNotNeeded
Board Name	none
IP Address 1	10.7.8.3
MAC Address 1	00908F034A96
IP Address 2	10.7.8.4
MAC Address 2	00908F034AA8
IP Subnet Mask	255.255.0.0
Board Redundancy Group	none

➢ To import the .prv file into an entity, take these steps:

1. Open the parameters provisioning screen of the entity into which you want to import the *prv* 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 *prv* configuration file and double-click on it; the entity's provisioning screen now displays the parameter configurations retrieved from the *prv* file; parameter configurations that differ from the previous configuration are colored in purple.

12.4 Provisioning Entity Profiles

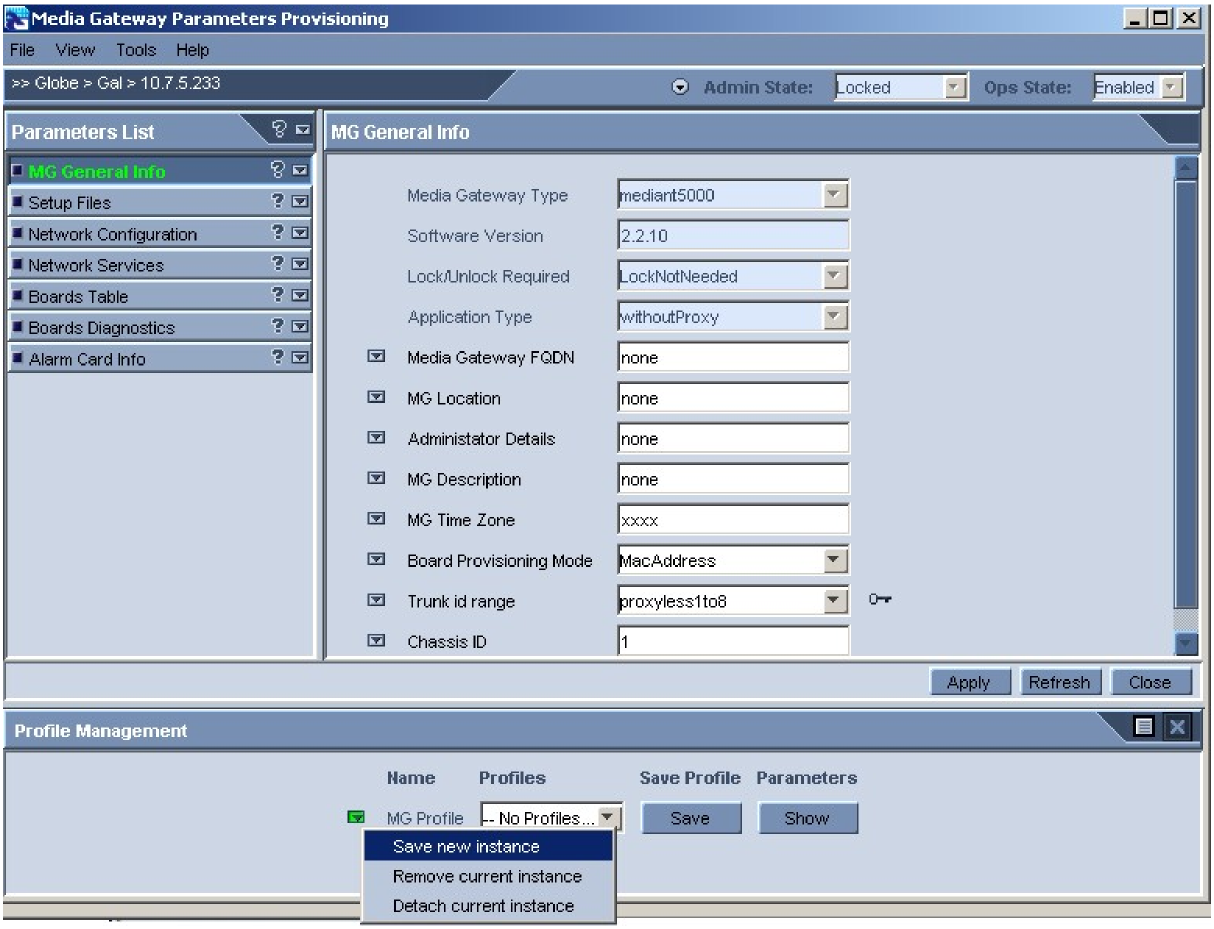
The EMS's Profile Management enables Customers to rapidly provision values to entity parameters by loading a profile. The Profile Manager feature is located in the lowermost pane of the Parameters Provisioning screen.

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

Customers can also delete profiles from the pool of profiles.

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

Figure 12-6: Profile Management



Media Gateway Type	mediant5000
Software Version	2.2.10
Lock/Unlock Required	LockNotNeeded
Application Type	withoutProxy
Media Gateway FQDN	none
MG Location	none
Administator Details	none
MG Description	none
MG Time Zone	xxxx
Board Provisioning Mode	MacAddress
Trunk id range	proxyless1to8
Chassis ID	1

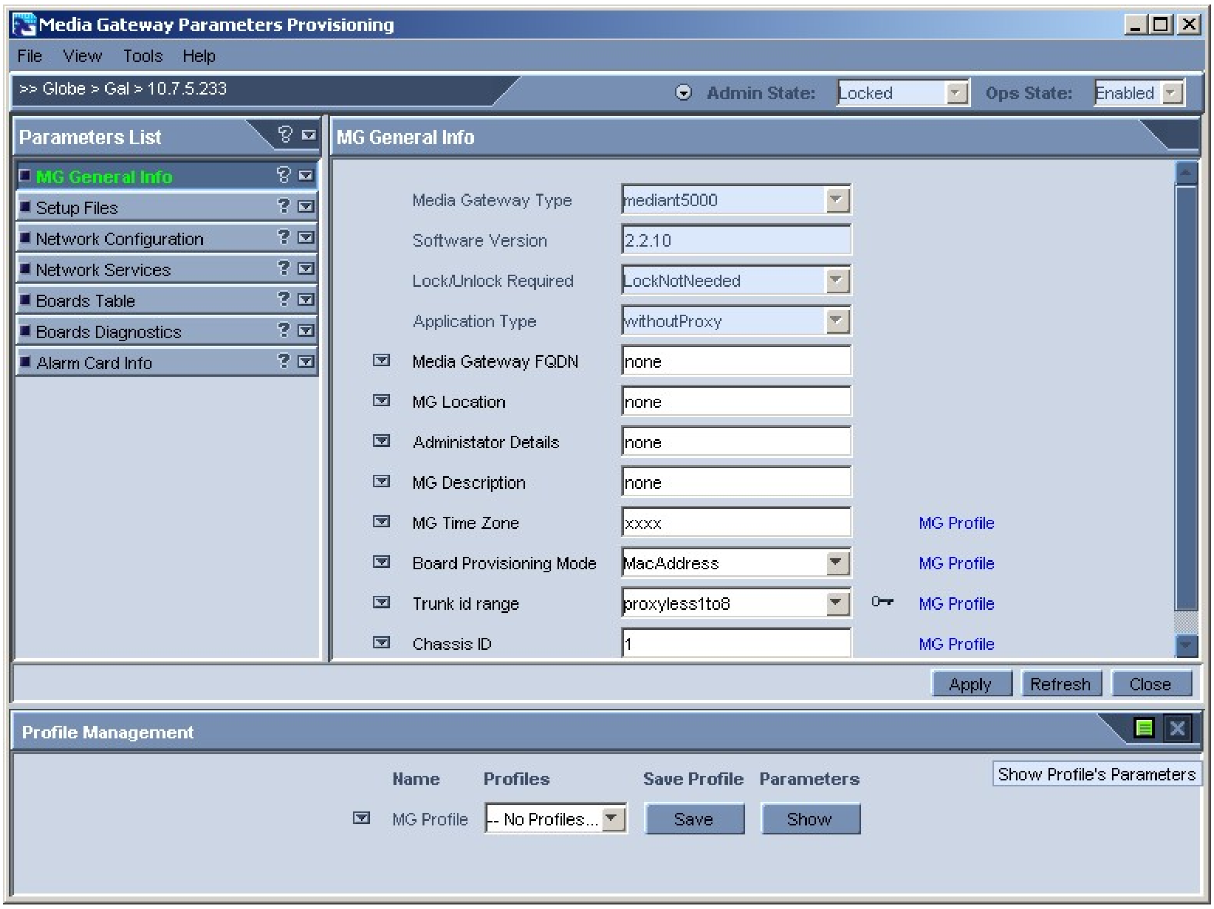
12.4.1 Creating Entity Profiles

Note: Entity profiles cannot be modified.

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

1. Click the 'Show' button located in the same row as that of the profile; the 'Show Parameters' screen is displayed on top of the parameters provisioning screen, listing all parameters that are under the requested profile and their tab location. Alternatively, you can check 'Show' icon on the 'Profile Management' pane, and Name of the profiles will be added to the profiled parameters.

Figure 12-7: Profile Management: Show Profile's Parameters



Media Gateway Parameters Provisioning

>> Globe > Gal > 10.7.5.233

Admin State: Locked
Ops State: Enabled

Parameters List: MG General Info, Setup Files, Network Configuration, Network Services, Boards Table, Boards Diagnostics, Alarm Card Info

MG General Info

Media Gateway Type	mediant5000	
Software Version	2.2.10	
Lock/Unlock Required	LockNotNeeded	
Application Type	withoutProxy	
Media Gateway FQDN	none	
MG Location	none	
Administator Details	none	
MG Description	none	
MG Time Zone	xxxx	MG Profile
Board Provisioning Mode	MacAddress	MG Profile
Trunk id range	proxyless1to8	MG Profile
Chassis ID	1	MG Profile

Profile Management

Name	Profiles	Save Profile	Parameters
MG Profile	-- No Profiles...	Save	Show

2. Edit/modify the parameter/s field/s and click the 'Save' button in the Profiles Management pane; you're prompted in the 'New Profile' prompt (field 'Provide a New Profile Name') for a new name for the profile whose parameter/s / field/s you've modified.

3. Press OK; the modified values of the parameter/s field/s are saved in the new profile and the new profile is added to the 'Profiles' drop-down list; the current media gateway's entity is now attached to the new profile.

12.4.2 Loading - Attaching - an Entity Profile

➢ To load an entity profile:

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

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

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

12.4.3 Detaching a Profile from an Entity

A profile is detached from an entity in the event that:

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

12.4.4 Removing a Profile

➢ To remove a profile from the profiles pool:

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

Note: The current profile is removed if and only if no other entity is attached to this profile beside the current entity (for whom the screen is opened). If there is another entity attached to the profile, the 'Remove Profile' function fails and a list of the currently attached entities is displayed.

Therefore, before removing a profile from the profiles pool, first detach it from any entity it may be attached to (refer to 'Detaching a Profile from an Entity' on page 70).

12.5 TP-1610 Master Profile (Media Gateway 3500)

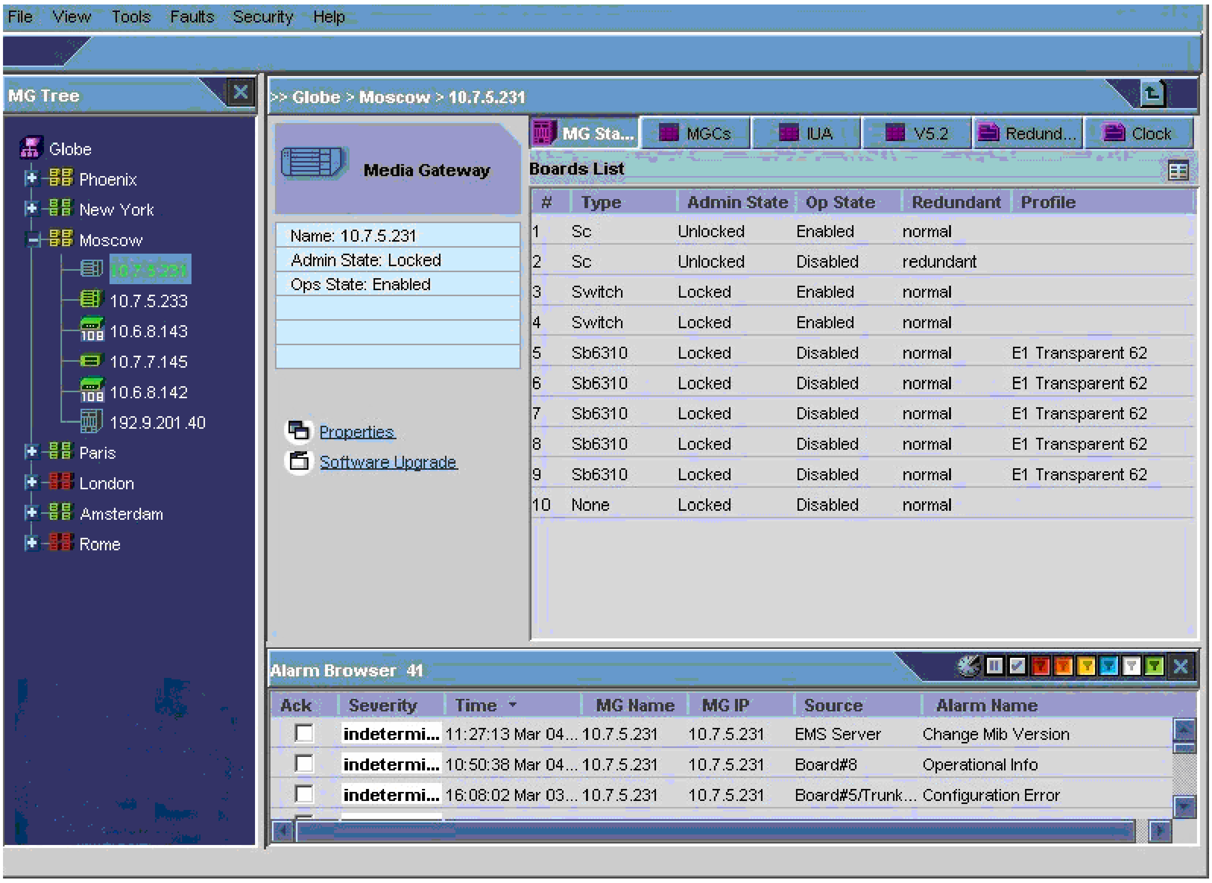
12.5.1 Ascertaining a TP-1610 Board Master Profile

A TP-1610 master profile is composed of:

- The board-level configuration
- The trunks configuration

To ascertain whether a master profile is attached to a TP-1610 board and (in the event that a master profile is attached) the name of the master profile (refer to the figure below), press the icon ‘Table View’ in the gateway Status screen and check the ‘Profile’ column.

Figure 12-8: Profile Column in the Boards List Screen



Name: 10.7.5.231
Admin State: Locked
Ops State: Enabled

Boards List

#	Type	Admin State	Op State	Redundant	Profile
1	Sc	Unlocked	Enabled	normal	
2	Sc	Unlocked	Disabled	redundant	
3	Switch	Locked	Enabled	normal	
4	Switch	Locked	Enabled	normal	
5	Sb6310	Locked	Disabled	normal	E1 Transparent 62
6	Sb6310	Locked	Disabled	normal	E1 Transparent 62
7	Sb6310	Locked	Disabled	normal	E1 Transparent 62
8	Sb6310	Locked	Disabled	normal	E1 Transparent 62
9	Sb6310	Locked	Disabled	normal	E1 Transparent 62
10	None	Locked	Disabled	normal	

Alarm Browser 41

Ack	Severity	Time	MG Name	MG IP	Source	Alarm Name
□	indetermi...	11:27:13 Mar 04...	10.7.5.231	10.7.5.231	EMS Server	Change Mib Version
□	indetermi...	10:50:38 Mar 04...	10.7.5.231	10.7.5.231	Board#8	Operational Info
□	indetermi...	16:08:02 Mar 03...	10.7.5.231	10.7.5.231	Board#5/Trunk...	Configuration Error

12.5.2 Creating a Master Profile

Note: A master profile cannot be modified after it is created. Operators must instead modify the configuration of a TP-1610 and then save the new configuration as a new master profile (to be applied to the boards).

To apply a master profile to the TP-1610 board, all its trunks should be profiled. If all trunks have the same configuration, operators can use the button 'Apply to All' in the 'Trunk Properties Profile Manager' pane.

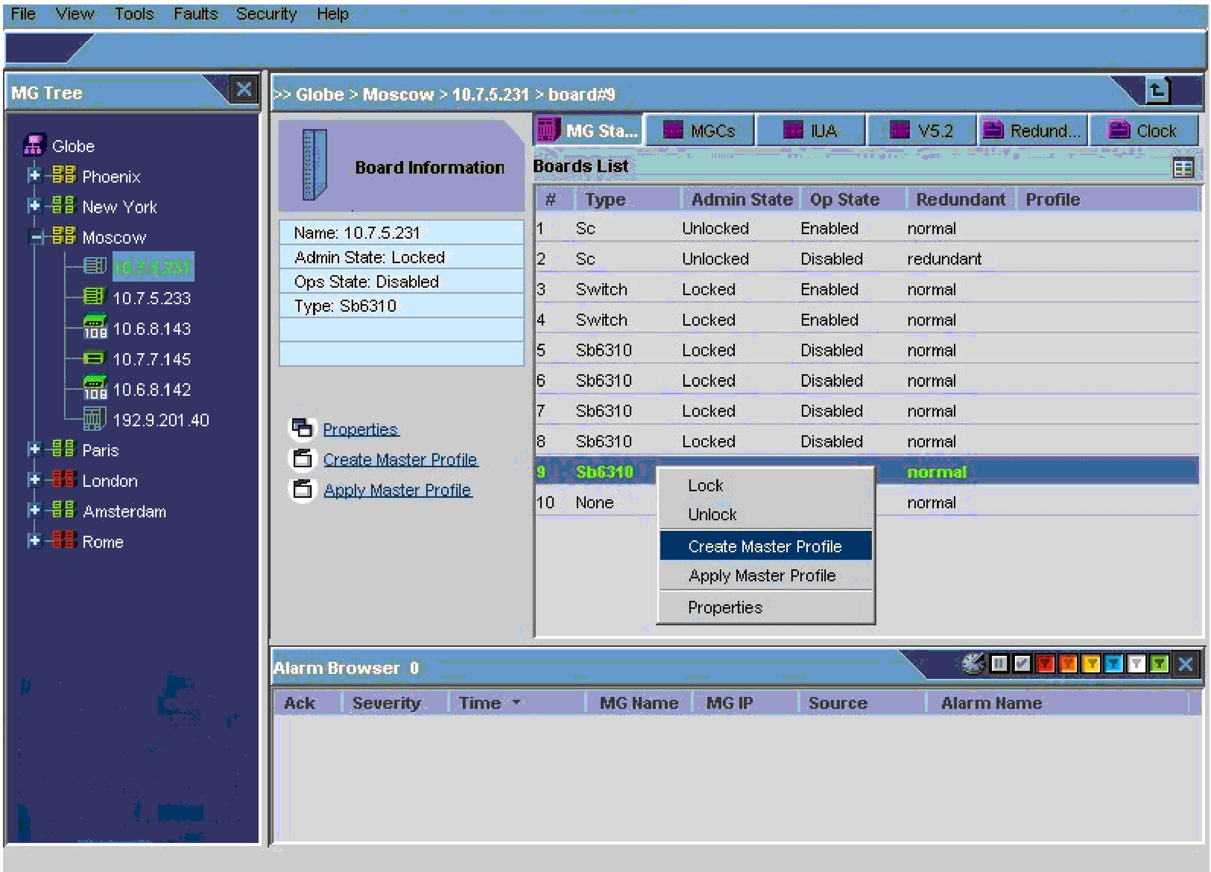
After finishing configuring the profiles parameters of a TP-1610 board, operators can save the configuration as a master profile. The master profile comprises following entity profiles

- Board Provisioning Frame
- Trunks Provisioning Frame (for all the trunks)

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

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

Figure 12-9: Creating a Master Profile - TP-1610



Name: 10.7.5.231
Admin State: Locked
Ops State: Disabled
Type: Sb6310

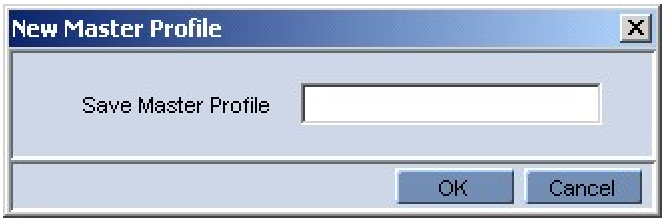
Boards List

#	Type	Admin State	Op State	Redundant	Profile
1	Sc	Unlocked	Enabled	normal	
2	Sc	Unlocked	Disabled	redundant	
3	Switch	Locked	Enabled	normal	
4	Switch	Locked	Enabled	normal	
5	Sb6310	Locked	Disabled	normal	
6	Sb6310	Locked	Disabled	normal	
7	Sb6310	Locked	Disabled	normal	
8	Sb6310	Locked	Disabled	normal	
9	Sb6310			normal	
10	None			normal	

➢ To create a master profile:

1. In the Information pane, click the link 'Create Master Profile'; the New Master Profile prompt appears (shown in the figure below).

Figure 12-10: New Master Profile Prompt



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

➢ To create a master profile using an alternative procedure:

1. In the Boards List, select the TP-1610 boards to which to attach a master profile.
2. Right-click on the selected boards and from the popup menu, choose option 'Create Master Profile'; the New Master Profile prompt appears (shown in the figure above).
3. Enter a name for the master profile in the field 'Save Master Profile' and press OK.

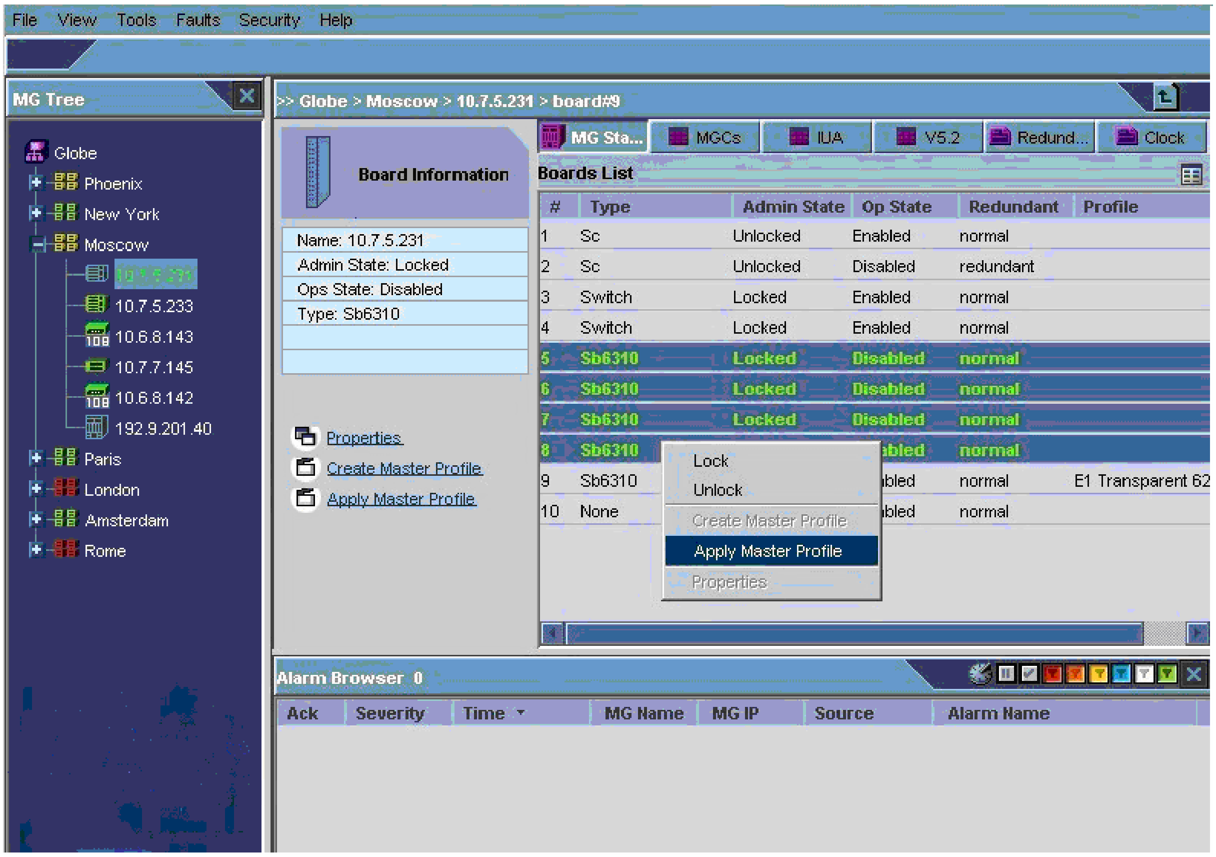
12.5.3 Attaching a Master Profile to TP-1610 Boards

➢ To attach a master profile to TP-1610 board/s:

1. Change the 'MG Status' screen to Table View (click the 'Table View' icon).

2. In the Boards List, select a TP-1610 board (or select multiple boards).

Figure 12-11: Selecting TP-1610 Boards



Name: 10.7.5.231
Admin State: Locked
Ops State: Disabled
Type: Sb6310

Boards List

#	Type	Admin State	Op State	Redundant	Profile
1	Sc	Unlocked	Enabled	normal	
2	Sc	Unlocked	Disabled	redundant	
3	Switch	Locked	Enabled	normal	
4	Switch	Locked	Enabled	normal	
5	Sb6310	Locked	Disabled	normal	
6	Sb6310	Locked	Disabled	normal	
7	Sb6310	Locked	Disabled	normal	
8	Sb6310		abled	normal	
9	Sb6310		bled	normal	E1 Transparent 62
10	None		bled	normal	

3. Right-click on the selected board (or on multiple selected boards) and from the popup menu, choose option 'Apply Master Profile'; the 'Select Master Profile' prompt appears on the screen.

4. Select the Master Profile you require and press OK; the master profile you selected is attached to all selected boards.

12.5.4 Detaching a Master Profile from TP-1610 Boards

A profile is detached from the TP-1610 board in the event that:

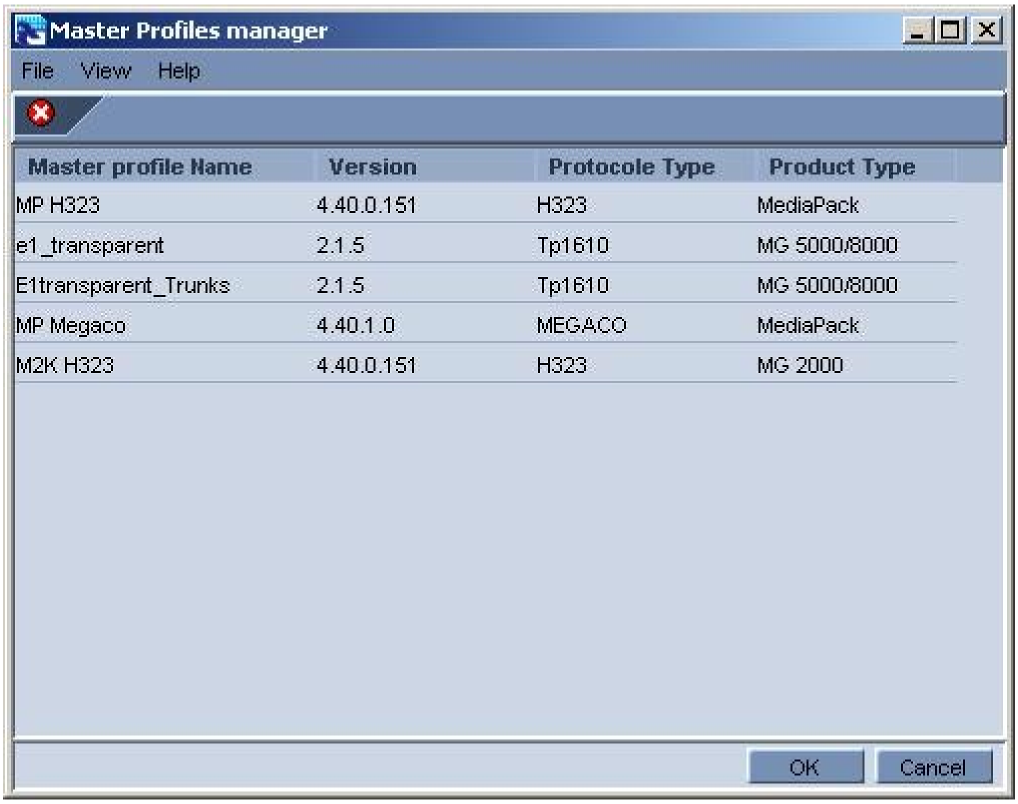
- You change the configuration of one of the profiled parameters. After pressing 'Apply', the master profile is detached from the TP-1610 board.
- You apply a master profile to an TP-1610 board that is already attached to a master profile and the two master profiles are different. When clicking Apply, the TP-1610 is detached from the previously applied master profile and the new profile is applied.

12.5.5 Master Profiles Manager

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

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

Figure 12-12: Master Profiles Manager



Master profile Name	Version	Protocole Type	Product Type
MP H323	4.40.0.151	H323	MediaPack
e1_transparent	2.1.5	Tp1610	MG 5000/8000
E1transparent_Trunks	2.1.5	Tp1610	MG 5000/8000
MP Megaco	4.40.1.0	MEGACO	MediaPack
M2K H323	4.40.0.151	H323	MG 2000

2. Select the master profile/s that you require to be removed from the master profiles pool and press the button ☒ to remove the master profile/s you selected.

3. If a master profile is used by one or more devices, it cannot be removed.

12.6 Provisioning Tones and Prompts

Tone and prompt files are *dat* files each containing the raw data used for a certain task such as Call Progress Tones, Voice Prompts, etc. Some sample tone files are available in the MG 3500 software package CD. These *dat* files are downloaded to the MG 3500 using EMS.

12.6.1 Call Progress Tones

The Call Progress Tones and User-Defined Tones file used by the MG 3500 is a binary file with the extension "*.dat*". Only this binary *tone.dat* file can be loaded to a MG 3500. Users can generate their own *tone.dat* file by opening the modifiable *tone.ini* file (supplied with the *tone.dat* file as part of the software package on the CD accompanying the MG 3500) in any text editor, modify it, and convert the modified *tone.ini* back into a binary *tones.dat* file using the DConvert Utility supplied with the MG 3500 software package.

12.6.2 Prerecorded Tones (PRT)

The Call Progress Tones and the User-Defined Tones mechanisms have several limitations such as limited number of predefined tones, or limited number of frequency integrations in one tone. To solve these problems and provide a more flexible tone generation capability, prerecorded tones can be downloaded to the MG 3500 and be played using regular tone generation commands.

Note 1: The maximum PRT buffer size is 1 MB. Therefore, the pre-recorded-tones.dat file must be smaller than this value.

Note 2: If the same tone type was defined as PRT and as Call Progress Tone or User-Defined Tone, the MG 3500 plays it using the PRT module.

12.6.3 Voice Prompts

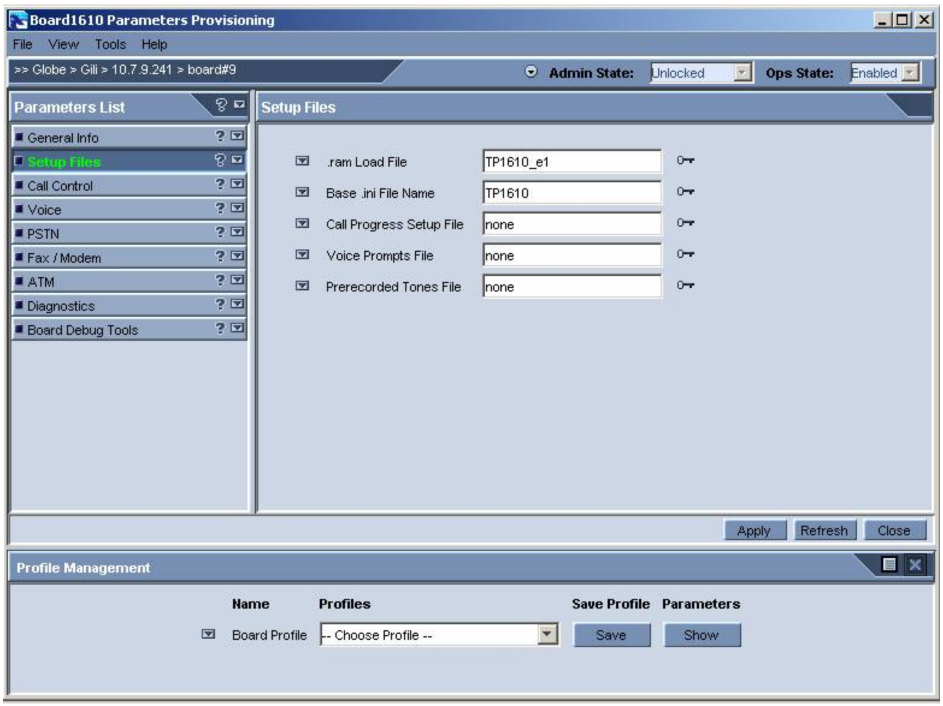
Voice prompt files are used to download voice prompts or announcements which can be played by the gateway. Refer to the Media Gateway 3500 Installation, Operation, and Maintenance manual for more information.

12.6.4 Provisioning the Files

To load the call progress tones, pre-recorded tones, and/or prompt files to the MG 3500, take the following steps:

1. Copy tones files to /tftpboot directory on both SCs
2. Select the board to receive the tones files.
3. Select "Setup Files" from the left menu. See Figure 12-13
4. Enter the name of the tones file in the Call Progress Setup File field.
5. Enter the name of the pre-recorded tones file in the Pre-recorded Tones File field.
6. Enter the name of the prompt file in the Voice Prompts File field.
7. Click Apply. This will require locking the board.
8. Unlock the board.

Figure 12-13: Tones Provisioning Screen



Board1610 Parameters Provisioning

>> Globe > Gili > 10.7.9.241 > board#9

Admin State: Unlocked

Ops State: Enabled

Setup Files

.ram Load File	TP1610_e1
Base .ini File Name	TP1610
Call Progress Setup File	none
Voice Prompts File	none
Prerecorded Tones File	none

Profile Management

Name	Profiles	Save Profile	Parameters
Board Profile	-- Choose Profile --	Save	Show

13 Gateway Installation, Software Upgrade and Regional Files Distribution

Software can be loaded to a gateway / media server in order to update the current software version and to provide the appropriate regional files.

During the software upgrade process, the gateway / media server configuration is saved.

For the Media Gateway 3500, online software upgrade is supported (the gateway continues its operation uninterruptedly during the software upgrade).

Software loading involves two procedures:

1. Introduce new files to the EMS by adding files to the Software Manager.

2. Load the required file/s to the gateway / media server.

13.1 Software Manager

Refer to 'Software Manager' on page 25.

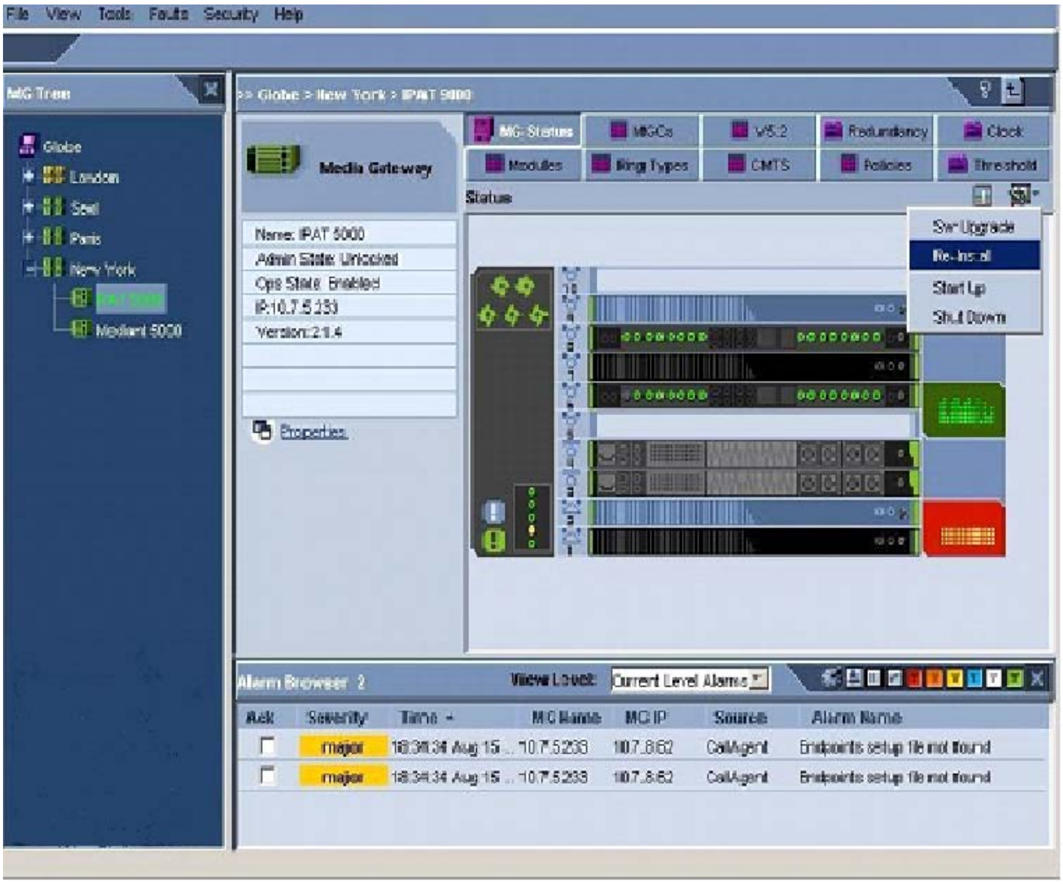
13.2 Media Gateway 3500 Maintenance Actions

➢ To perform maintenance actions, take these steps:

1. In the MG Tree, select the gateway on which maintenance action is required.

2. Click the 'Maintenance Actions' icon located at the top right of the Status screen; the popup menu opens (refer to the figure below). Select the maintenance action you require.

Figure 13-1: Maintenance Actions Icon and Popup Menu



Name: IPAT 5000
Admin State: Unlocked
Ops State: Enabled
IP:10.7.5.233
Version:2.1.4

Ack	Severity	Time	MG Name	MG IP	Source	Alarm Name
□	major	18:34:34 Aug 15 ..	10.7.5.233	10.7.8.62	CallAgent	Endpoints setup file not found
□	major	18:34:34 Aug 15 ..	10.7.5.233	10.7.8.62	CallAgent	Endpoints setup file not found

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

The software distribution process is performed via FTP and Telnet. The EMS server implements the FTP client. The Media Gateway 3500 has an FTP server.

13.2.1 Online Software Upgrade Wizard

An online software upgrade is performed when both System Controllers are up and running. The software upgrade process upgrades both System Controller and TP boards' software.

The gateway continues its operation uninterruptedly during a software upgrade of the System Controller. However, calls are dropped during an upgrade of TP boards. To minimize impact on media gateway service, TP boards are upgraded one at a time, after a predefined graceful shutdown period. The media gateway's capacity is thus never reduced by more than a single TP board’s capacity.

Because of the above, an online software upgrade should best be performed at night when traffic volume is low. It's also recommended to perform a configuration backup prior to starting an online software upgrade.

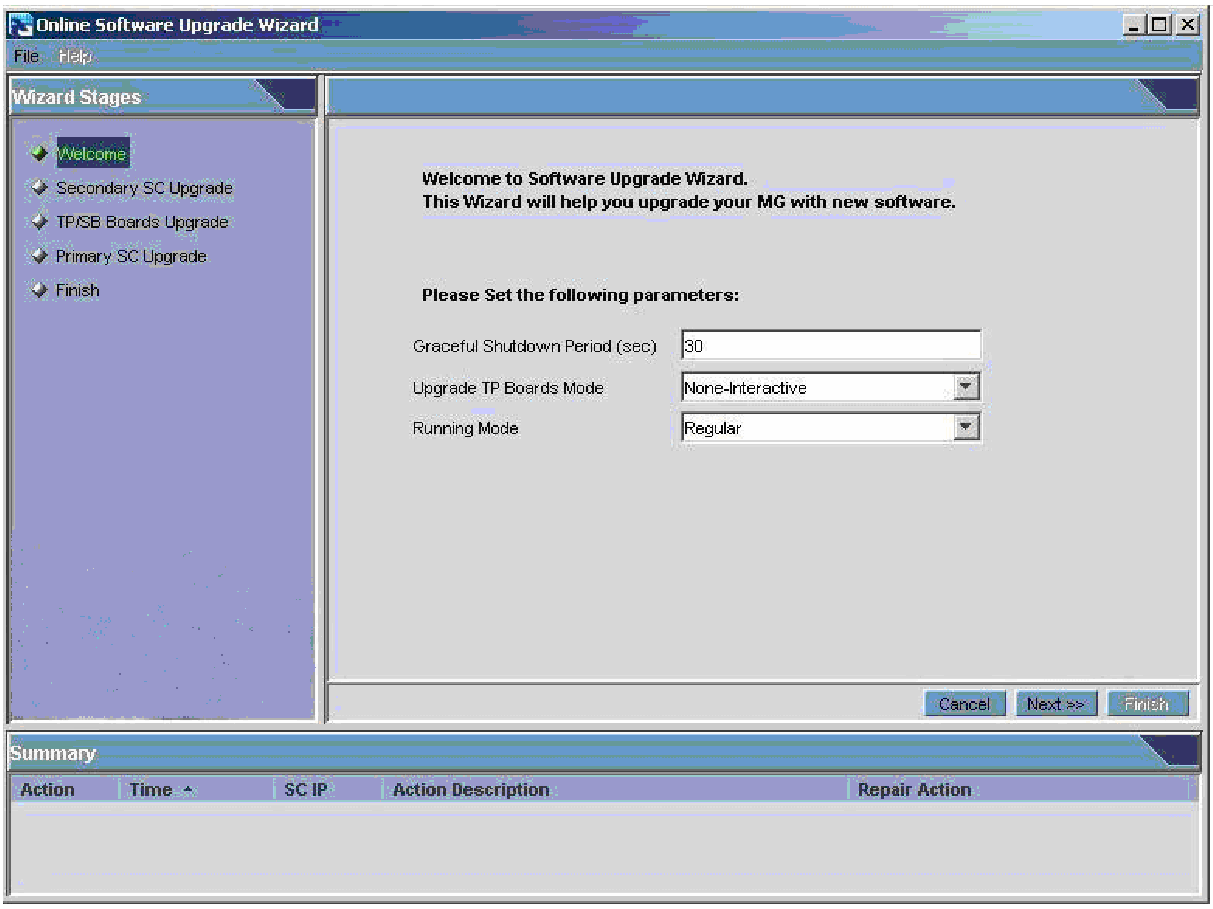
The Online Software Upgrade Wizard GUI includes 'Wizard Stages' screen section and a 'Summary Table' screen section. The Summary Table includes a summary of the Request / Response messages exchanged between the EMS server and each of the System Controller boards during the upgrade process. This screen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

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

1. Welcome screen

Includes basic questions regarding the software upgrade process. In this screen (refer to the figure below), select the 'Running Mode' in which to run the Wizard: choose 'Regular' or ‘Debug’. ‘Regular’ mode performs an automatic skip to the next Wizard stage after each stage is successfully completed. ‘Debug’ mode enables the ‘Next’ button at the end of each stage, providing users with the possibility to perform a test at any stage and to either proceed to ‘Next’ or to 'Cancel' (rollback) the process in case of problems.

Figure 13-2: Welcome to the Online Software Upgrade Wizard



Welcome to Software Upgrade Wizard.
This Wizard will help you upgrade your MG with new software.

Please Set the following parameters:

Graceful Shutdown Period (sec): 30

Upgrade TP Boards Mode: None-Interactive

Running Mode: Regular

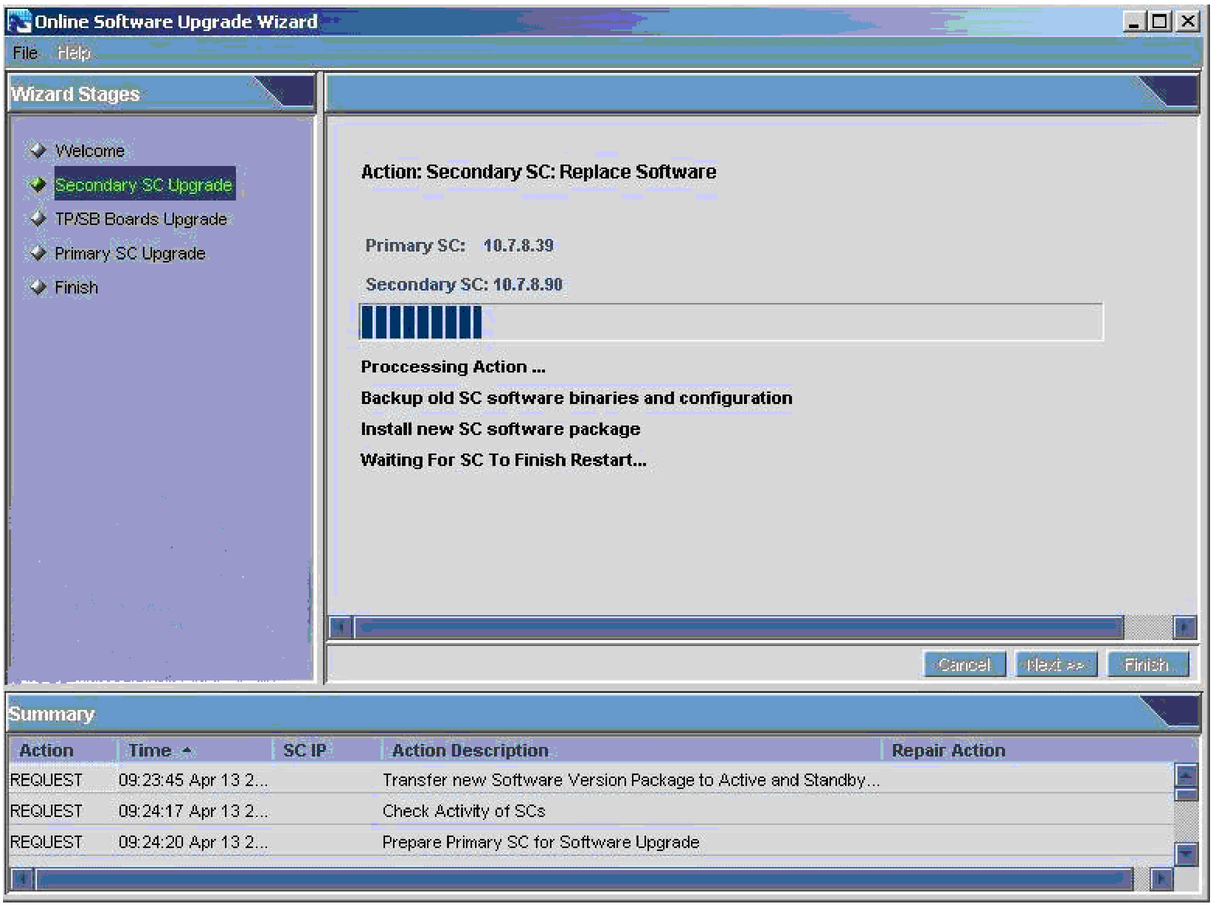
Action	Time	SC IP	Action Description	Repair Action

2. Secondary SC Update

In the first stage, the secondary System Controller’s software is upgraded. Thereafter, the secondary SC actually manages the upgrade process of the TP boards (refer to the figure below).

After the secondary System Controller's software is updated, the primary System Controller is taken down and an activity switchover to the secondary System Controller is performed.

Figure 13-3: Software Upgrade in Process, Managed by the System Controller



Action: Secondary SC: Replace Software

Primary SC: 10.7.8.39

Secondary SC: 10.7.8.90

Proccessing Action ...

Backup old SC software binaries and configuration

Install new SC software package

Waiting For SC To Finish Restart...

Action	Time	SC IP	Action Description	Repair Action
REQUEST	09:23:45 Apr 13 2...		Transfer new Software Version Package to Active and Standby...	
REQUEST	09:24:17 Apr 13 2...		Check Activity of SCs	
REQUEST	09:24:20 Apr 13 2...		Prepare Primary SC for Software Upgrade	

3. TP Boards Update

Note that at this stage of the software upgrade, active calls are dropped. The secondary SC upgrades all TP boards in the system, shutting down one at a time after a predefined graceful shutdown period.

4. Primary SC Upgrade

After the secondary SC and all TP boards are updated, the primary SC is upgraded to the new version.

5. Finish

13.2.1.1 Rollback

At any time during an upgrade process, users can perform a rollback to the previous software configuration by pressing the 'Cancel' button in the Online Software Upgrade Wizard. A rollback may or may not affect media gateway service. It depends on how far the upgrade has progressed by the time the rollback is performed. A rollback is not service-affecting (i.e., it can be performed without impacting the calls serviced by the media gateway) until the final phase of the 'Secondary SC Upgrade' stage - up to the point that the primary Shelf Controller is shut down and an activity switchover to the secondary Shelf Controller is performed. After this point, rollback will be service-affecting and will cause a reset of all TP boards.

If an upgrade fails, the EMS informs users of the failure and automatically performs a rollback.

13.2.1.2 Troubleshooting

If you experience an unexpected network or software problem during online software upgrade (e.g., if the PC, on which the EMS client runs, crashes or the network connection to the media gateway is lost) and because of the failure you can neither complete nor cancel the online software upgrade, you must perform a manual rollback to the previous software configuration.

➢ To perform a manual rollback to the previous software configuration:

- Connect to both Shelf Controllers through Telnet or RS-232 port and perform the commands shown in the table below:

Table 13-1: Commands to Perform a Manual Rollback to the Previous Software Configuration

	On Primary SC	On Secondary SC
1.	/tg_upgrade continue	
2.		/tg_upgrade continue
3.	REQUEST ABORT_PREPARE	
4.	Wait for RESPONSE_OK	
5.		REQUEST ABORT_PREPARE
6.		Wait for RESPONSE_OK
7.	REQUEST ABORT	
8.	Wait for RESPONSE_OK	
9.		REQUEST ABORT
10.		Wait for RESPONSE_OK
11.	QUIT	
12.		QUIT

13.2.2 Offline Software Upgrade Wizard

An offline software upgrade is performed when one System Controller is up and running. During the offline software upgrade process, the gateway configuration is saved.

The Offline Software Upgrade Wizard is almost identical to the Online Software Upgrade Wizard. Refer to 'Online Software Upgrade Wizard' on page 80.

13.3 Media Gateway 3500 Startup and Shutdown

➢ **To reset the gateway software, take this step:**

- From the ‘Maintenance Actions’ popup menu, select ‘Start Up’ (if you haven’t started up yet) or ‘Shut Down’ (if you previously started up but now want to shut down).

  Note that you cannot start up an already started gateway.

14 Fault 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 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. EMSs provide 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 in order to alert operations personnel to a problem before it affects customers.

The EMS's Fault Management features:

1. Active Alarms - Alarm Browser
2. History Alarms - Alarm History
3. Interpreting Alarm Fields
4. Alarms Clearing Concepts
5. Trap Forwarding to North Bound Interface
6. Save Alarms in File
7. List of Alarms

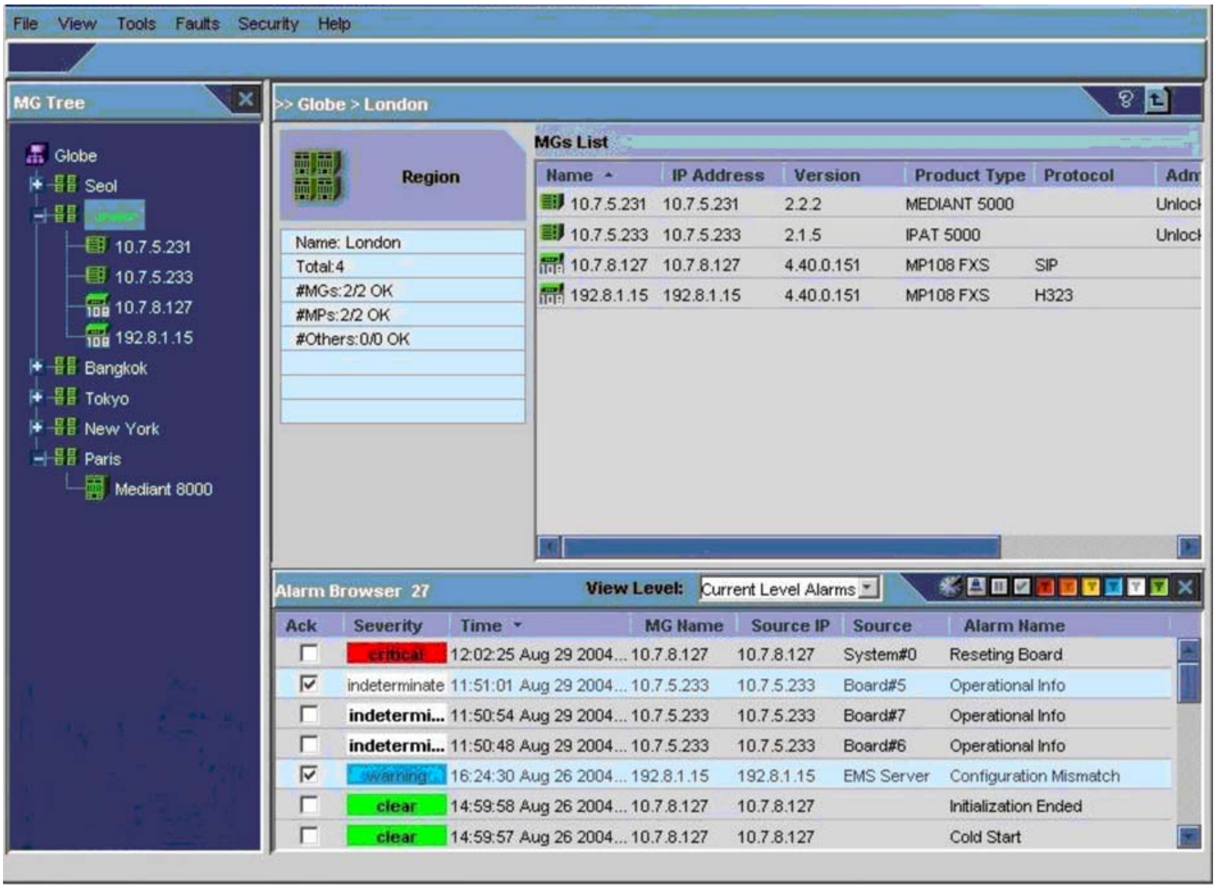
14.1 Alarm Browser

The EMS’s fault management functionality manages and presents all alarms 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 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* system faults at the top of the alarms list, allowing Operators to identify equipment and facilities most recently affected.

The Alarm Browser is context-based so that (for example) only alarms of the media gateway selected in the MGs List will be displayed in the Alarm Browser or (as another example) only alarms of the TP board selected in the graphic representation of the media gateway will be displayed in the Alarm Browser. The figure below shows the Alarm Browser, the Globe-context alarms displayed in the Alarm Browser.

Figure 14-1: Alarm Browser in Main Screen



Name: London
Total:4
#MGs:2/2 OK
#MPs:2/2 OK
#Others:0/0 OK

Name	IP Address	Version	Product Type	Protocol	Adn
10.7.5.231	10.7.5.231	2.2.2	MEDIANT 5000		Unlocl
10.7.5.233	10.7.5.233	2.1.5	IPAT 5000		Unlocl
10.7.8.127	10.7.8.127	4.40.0.151	MP108 FXS	SIP	
192.8.1.15	192.8.1.15	4.40.0.151	MP108 FXS	H323	

Ack	Severity	Time	MG Name	Source IP	Source	Alarm Name
□	critical	12:02:25 Aug 29 2004...	10.7.8.127	10.7.8.127	System#0	Reseting Board
☑	indeterminate	11:51:01 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#5	Operational Info
□	indetermi...	11:50:54 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#7	Operational Info
□	indetermi...	11:50:48 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#6	Operational Info
☑	warning	16:24:30 Aug 26 2004...	192.8.1.15	192.8.1.15	EMS Server	Configuration Mismatch
□	clear	14:59:58 Aug 26 2004...	10.7.8.127	10.7.8.127		Initialization Ended
□	clear	14:59:57 Aug 26 2004...	10.7.8.127	10.7.8.127		Cold Start

The number of alarms currently displayed in the Alarms Browser is indicated adjacent to the pane title bar. For each alarm, the following alarm details are displayed in the Alarm Browser pane:

- Ack - a check box in the left column of the Alarm Browser indicates if an alarm has been Acknowledged (checked) or Unacknowledged (unchecked). After an alarm is acknowledged, the entire row displaying the alarm and its details becomes gray (disabled).
- Severity - indicates the alarm's severity level. green=Clear; white=Indeterminate; blue=Warning; yellow=Minor; orange=Major; red=Critical.
- Time (Day of the Week, Month, Date in the Month, Hours:Minutes:Seconds, Time Zone, Year)
- MG Name
- Media Gateway IP address
- Source - the source of the alarm; the failed entity that generated the alarm (in format Board#1/Trunk#2, etc.)
- Alarm Name (short description of the alarm)

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

14.1.1 Filtering Alarms

The Alarm Browser lists all currently active alarms in the EMS for a context selected in the Main Screen. When selecting the root (Globe) of the managed media gateways in the MG Tree, the Alarm Browser displays all alarms for all EMS -managed elements (as shown in the figure below).

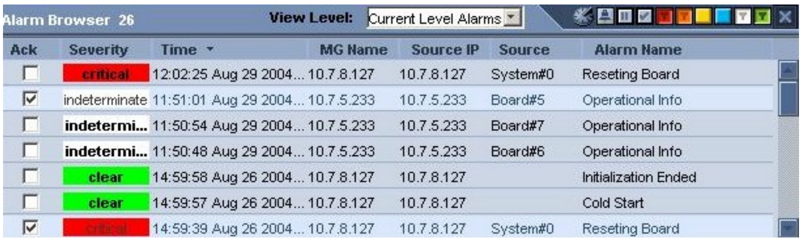
When selecting a region in the MG Tree, for example, the Alarm Browser displays all alarms for all media gateways under that region.

Available contexts are:

- Globe - all alarms in the entire system.
- Region - alarms of all nodes located under the region.
- Media Gateway - all the alarms of the media gateway
- TP Board and its subcomponents (Trunks), SAT, Ethernet Switch and System Controller boards - all the alarms of the selected entity.

Additionally, operators can filter alarms according to Ack status and/or severity (using the Alarm Browser’s toolbar buttons).

Figure 14-2: Alarm Browser - Alarm Severity Filtration Buttons



Alarm Browser 26 View Level: Current Level Alarms

Ack	Severity	Time	MG Name	Source IP	Source	Alarm Name
☐	critical	12:02:25 Aug 29 2004...	10.7.8.127	10.7.8.127	System#0	Reseting Board
☑	indeterminate	11:51:01 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#5	Operational Info
☐	indetermi...	11:50:54 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#7	Operational Info
☐	indetermi...	11:50:48 Aug 29 2004...	10.7.5.233	10.7.5.233	Board#6	Operational Info
☐	clear	14:59:58 Aug 26 2004...	10.7.8.127	10.7.8.127		Initialization Ended
☐	clear	14:59:57 Aug 26 2004...	10.7.8.127	10.7.8.127		Cold Start
☑	critical	14:59:39 Aug 26 2004...	10.7.8.127	10.7.8.127	System#0	Reseting Board

Table 14-1: Alarm Severity Filtration Buttons

Alarm Severity Filtration Toolbar	Purpose (When Pressing a Button on the Toolbar)
☑	Filter Unacknowledged Alarms; acknowledged alarms will not be displayed
🟥	Filter Critical Alarms, i.e., critical alarms will be displayed
🟧	Filter Major Alarms, i.e., major alarms will be displayed
🟨	Filter Minor Alarms, i.e., minor alarms will be displayed
🟦	Filter Warning Alarms, i.e., warning alarms will be displayed
⬜	Filter Info Alarms, i.e., info alarms will be displayed
🟩	Filter Clear Alarms, i.e., clear alarms will be displayed

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

14.1.2 Changing the 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.

14.1.3 Open Alarms History

Refer to 'Alarms History' on page 89.

14.1.4 Audio Indication on Receipt of Alarms

Each time a new alarm answering context selection criteria is received and displayed in the Alarm Browser, a bell sound is played by EMS application.

➢ To disable the bell sound:

- Click the button ‘Alarm Sound Enabled’ on the Alarm Browser toolbar.

14.1.5 Pause Alarms 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 pressed (selected), the alarm browser presentation is paused as well.

14.1.6 Closing the Alarm Browser Pane

➢ To close the Alarm Browser pane:

- Press 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'.

14.2 Alarms History

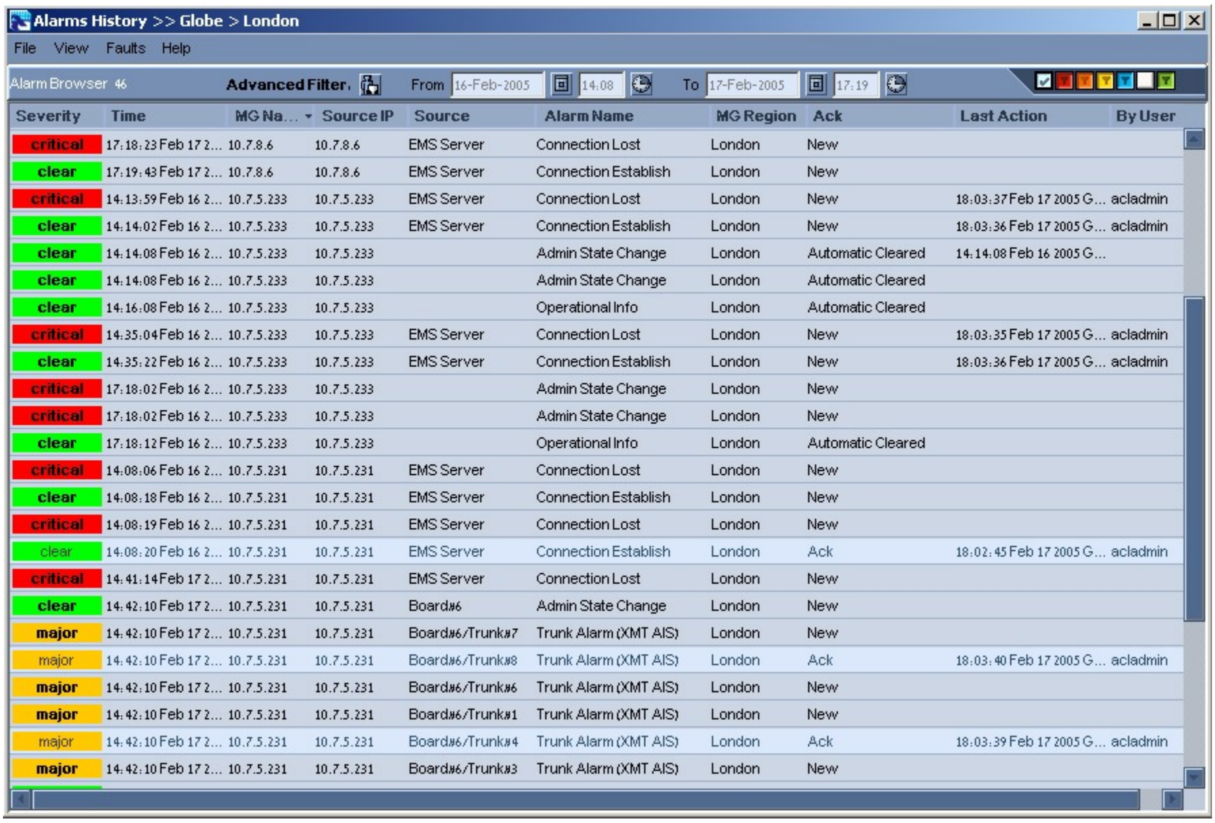
All alarms received by the EMS are archived in a database. Extensive information related to the alarm is saved, together with the alarm itself: Region and media gateway location, physical attributes of failed entity.

Open the Alarms History screen from Faults > Alarms History, or press the ‘View Alarms History’ icon (graphically representing a clock) located with the Alarm Browser’s filter icons. 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 (a history of at least one month, depending on disk space available - 1000 alarms per day for up to 100 digital media gateways. EMS operators can time-filter alarms according to a time definition so that they are operator-organized and viewed according to operator requirements.

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 14-3: Alarms History



Severity	Time	MG Na...	Source IP	Source	Alarm Name	MG Region	Ack	Last Action	By User
critical	17:18:23 Feb 17 2...	10.7.8.6	10.7.8.6	EMS Server	Connection Lost	London	New		
clear	17:19:43 Feb 17 2...	10.7.8.6	10.7.8.6	EMS Server	Connection Establish	London	New		
critical	14:13:59 Feb 16 2...	10.7.5.233	10.7.5.233	EMS Server	Connection Lost	London	New	18:03:37 Feb 17 2005 G...	acladmin
clear	14:14:02 Feb 16 2...	10.7.5.233	10.7.5.233	EMS Server	Connection Establish	London	New	18:03:36 Feb 17 2005 G...	acladmin
clear	14:14:08 Feb 16 2...	10.7.5.233	10.7.5.233		Admin State Change	London	Automatic Cleared	14:14:08 Feb 16 2005 G...	
clear	14:14:08 Feb 16 2...	10.7.5.233	10.7.5.233		Admin State Change	London	Automatic Cleared		
clear	14:16:08 Feb 16 2...	10.7.5.233	10.7.5.233		Operational Info	London	Automatic Cleared		
critical	14:35:04 Feb 16 2...	10.7.5.233	10.7.5.233	EMS Server	Connection Lost	London	New	18:03:35 Feb 17 2005 G...	acladmin
clear	14:35:22 Feb 16 2...	10.7.5.233	10.7.5.233	EMS Server	Connection Establish	London	New	18:03:36 Feb 17 2005 G...	acladmin
critical	17:18:02 Feb 16 2...	10.7.5.233	10.7.5.233		Admin State Change	London	New		
critical	17:18:02 Feb 16 2...	10.7.5.233	10.7.5.233		Admin State Change	London	New		
clear	17:18:12 Feb 16 2...	10.7.5.233	10.7.5.233		Operational Info	London	Automatic Cleared		
critical	14:08:06 Feb 16 2...	10.7.5.231	10.7.5.231	EMS Server	Connection Lost	London	New		
clear	14:08:18 Feb 16 2...	10.7.5.231	10.7.5.231	EMS Server	Connection Establish	London	New		
critical	14:08:19 Feb 16 2...	10.7.5.231	10.7.5.231	EMS Server	Connection Lost	London	New		
clear	14:08:20 Feb 16 2...	10.7.5.231	10.7.5.231	EMS Server	Connection Establish	London	Ack	18:02:45 Feb 17 2005 G...	acladmin
critical	14:41:14 Feb 17 2...	10.7.5.231	10.7.5.231	EMS Server	Connection Lost	London	New		
clear	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6	Admin State Change	London	New		
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#7	Trunk Alarm (XMT AIS)	London	New		
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#8	Trunk Alarm (XMT AIS)	London	Ack	18:03:40 Feb 17 2005 G...	acladmin
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#6	Trunk Alarm (XMT AIS)	London	New		
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#1	Trunk Alarm (XMT AIS)	London	New		
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#4	Trunk Alarm (XMT AIS)	London	Ack	18:03:39 Feb 17 2005 G...	acladmin
major	14:42:10 Feb 17 2...	10.7.5.231	10.7.5.231	Board#6/Trunk#3	Trunk Alarm (XMT AIS)	London	New		

The Time Filtering fields enable filtering alarms along the parameters of date and time. They’re located adjacent to the filter buttons on the Alarms History screen’s top bar, to their left. The date and time parameters both have a ‘From’ and ‘To’ (). This filter feature functions similarly to the other Alarms Browser filters. Refer to 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.

14.3 Using the Advanced Filter

Users can use the ‘Advanced Filter’ screen to seach for words defined in the fields ‘Description’ and ‘Additional Info’ of the ‘Alarm Details’ screen.

➢ To use the Advanced Filter, take these steps:

1. Define your query by defining fields ‘IP’ (gateway IP address), (alarm) ‘Source’ and ‘Free Text’. When defining a source string, a partial definition is valid. For example, when source = Trunk , all instances of the Trunk are searched (Trunk#1, Trunk#2, etc.) If you define both ‘Free Text’ fields, the EMS searches for at least one of the strings in the query and displays all alarms having at least one of the strings (OR search). Note that if you are navigating under a specific gateway, you must define ‘IP’ else the search result will be empty.

2. After defining all required fields, press OK; the ‘Alarms History’ screen displays alarms answering the search criteria. When the result is displayed, the ‘Alarm Filter’ button is colored in green.

Refer to the ‘Alarms History’ screen displaying results resulting from the following query:

Find all minor alarms (use the filter button; refer to section ‘Filtering Alarms’) in the entire EMS server (indicated by path ‘Globe’ in the title bar; refer to section ‘Filtering Alarms’) where the (alarm) Source is SAT and (alarm) Free Text includes strings ‘fan’ or ‘tray’. The result displays the number of alarms (3) and the ‘From’ and ‘To’ actual time range.

14.4 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. Refer to 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 14-4: Alarms History Screen: Defining Time Filtration using Calendar

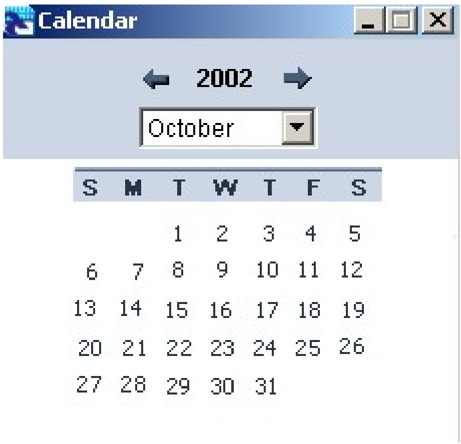
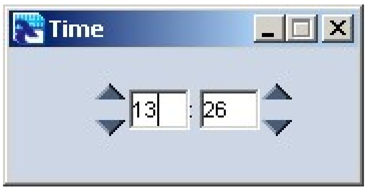


Figure 14-5: Alarms History Screen: Defining Time Filtration using Hour & Minutes



14.5 Defining Complex Queries using a Combination of Filters

Using a combination of filtering options, users can easily create complex queries. Following are few examples:

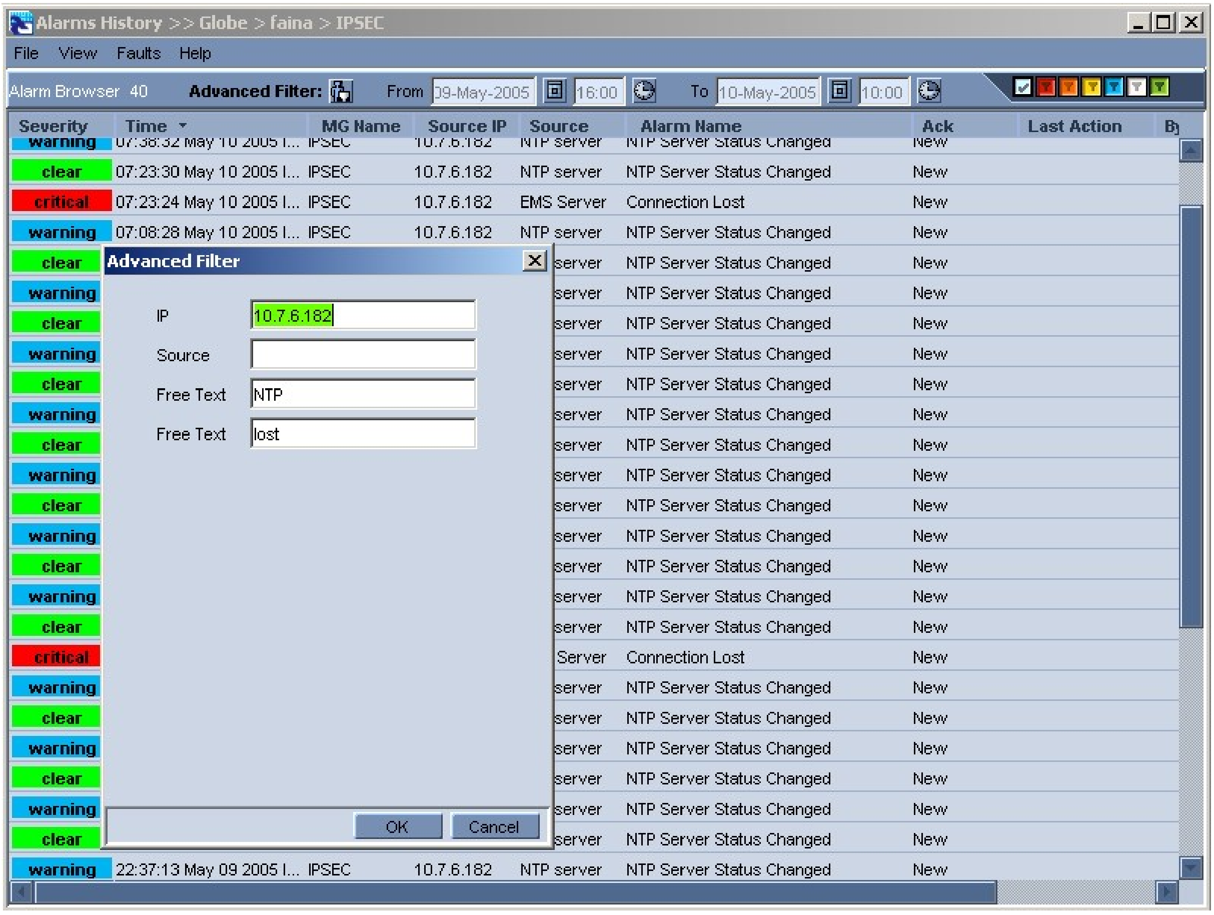
a. Find all major alarms including the word ‘state’ for trunk # 4 of board #7 in a media gateway named ‘Trunking GW 5’.

1. Go to relevant media gateway named ‘Trunking GW 5’.
2. Double-click board #7 and select trunk # 4 in the Status screen.
3. In the Alarms Browser, leave only the ‘Major’ severity filter checked (uncheck the other severity level buttons).
4. Click the button ‘View Alarm History’ on the Alarms Browser pane.
5. Click the ‘Advanced’ filter button and define the IP address and the required string ‘state’. Click ‘OK’.

b. Find all alarms from a media gateway named ‘IPSEC’, which included string ‘NTP’ or ‘lost’, and which occured between May 9 at 16:00 and May 10 at 10:00.

1. Go to the media gateway named ‘IPSEC’.
2. Click the button ‘View Alarms History’ on the Alarm Browser’s upper bar
3. Click the ‘Advanced’ filter button and define the IP address and strings ‘NTP’ and ‘lost’ (refer to the figure below). Click ‘OK’.
4. Go to the ‘From’ and ‘To’ filters and define the time range: From May 9 at 16:00 to May 10 at 10:00. Click ‘OK’; the required result is displayed in the Alarms History screen.

Figure 14-6: Defining Complex Queries using a Combination of Filters - Advanced Filter



Alarm Browser 40 Advanced Filter: From 09-May-2005 16:00 To 10-May-2005 10:00

Severity	Time	MG Name	Source IP	Source	Alarm Name	Ack	Last Action	By
warning	07:38:32 May 10 2005 I...	IPSEC	10.7.6.182	NTP server	NTP Server Status Changed	New		
clear	07:23:30 May 10 2005 I...	IPSEC	10.7.6.182	NTP server	NTP Server Status Changed	New		
critical	07:23:24 May 10 2005 I...	IPSEC	10.7.6.182	EMS Server	Connection Lost	New		
warning	07:08:28 May 10 2005 I...	IPSEC	10.7.6.182	NTP server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
critical				Server	Connection Lost	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning				server	NTP Server Status Changed	New		
clear				server	NTP Server Status Changed	New		
warning	22:37:13 May 09 2005 I...	IPSEC	10.7.6.182	NTP server	NTP Server Status Changed	New		

Advanced Filter

IP: 10.7.6.182

Source:

Free Text: NTP

Free Text: lost

14.6 Viewing, Interpreting an Alarm's Details

➢ To view/interpret an alarm’s details:

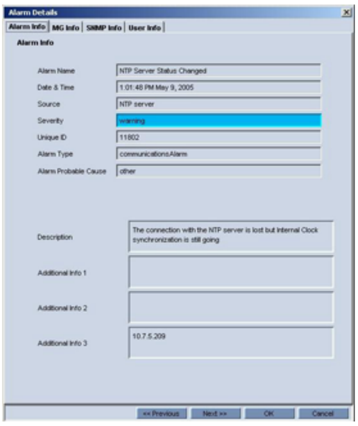
Either:

- 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 14-7: Alarm Details



Alarm Info

Alarm Name: NTP Server Status Changed
Date & Time: 1:01:48 PM May 9, 2005
Source: NTP server
Severity: warning
Unique ID: 11802
Alarm Type: communicationsAlarm
Alarm Probable Cause: other
Description: The connection with the NTP server is lost but Internal Clock synchronization is still going
Additional Info 1:
Additional Info 2:
Additional Info 3: 10.7.5.209

The Alarm Details screen features four tabs:

1. Alarm Info (includes all the information provided by the alarm; refer to its details below)
2. MG Info (includes details regarding the location - region - of the media gateway, and the precise source of the alarm; refer to its details below)
3. SNMP Info (includes SNMP-related information such as Trap OID, etc.; refer to its details below)
4. User Info (includes user-specific information such as alarm status and identifying data fields that users can define in order to use as future reference when searching; refer to its details below).

Alarm Info Tab

- Title

  The name of the alarm, provided in the Alarm Browser.

- Date & Time

  Date and Time when the alarm was received by the EMS.

- Source

The exact alarm source, in format: “board#3/trunk#7”.

- Severity

  Alarm Severity as displayed in Alarm Browser pane, according to- ITU X.733 standard

- Unique ID

  Alarm Unique ID provided by the media gateway for alarm clearing and correlation purposes.

- Alarm Type

  The alarm type can be one of the following:

  1. Communication (inter-process communication alarm)
  2. Quality of Service (indicates degradation in service performance)
  3. Processing Error (used for internal software errors)
  4. Equipment Alarm (indicates a hardware failure)
  5. Environmental alarm (used to indicate environmental errors such as temperature, power, etc.)

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

- Probable Cause

  The probable cause of the alarm. The probable cause can be one of the following:

  1. Degraded Signal for Trunk Alarm
  2. Underlying Resource Unavailable for a Change in a Managed Entity’s Administrative State or Operational State
  3. Configuration Or Customization Error for Configuration Error Alarm
  4. Heating Vent Cooling System Problem for Fan or Temperature Alarm
  5. Temperature Unacceptable for Temperature Alarm
  6. Power Problem for Voltage Alarm

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

- Description

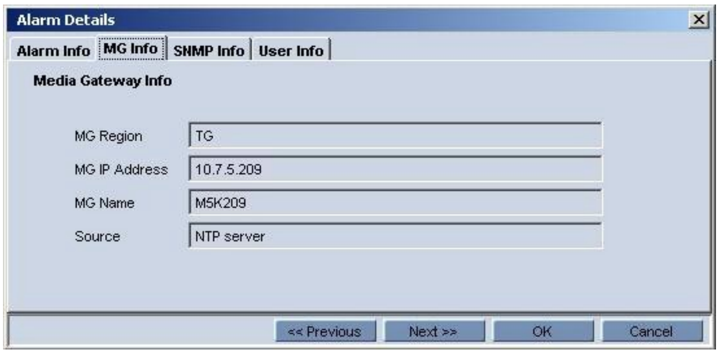
  Textual description of the alarm, received as part of the alarm information

- Additional Info 1-3

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

Alarm Details - tab MG Info

Figure 14-8: Alarm Details



Media Gateway Info

MG Region: TG
MG IP Address: 10.7.5.209
MG Name: M5K209
Source: NTP server

- MG Region

  The name of the region in which the media gateway is located.

- MG IP Address

  The IP address of the media gateway that originated the alarm.

- MG Name

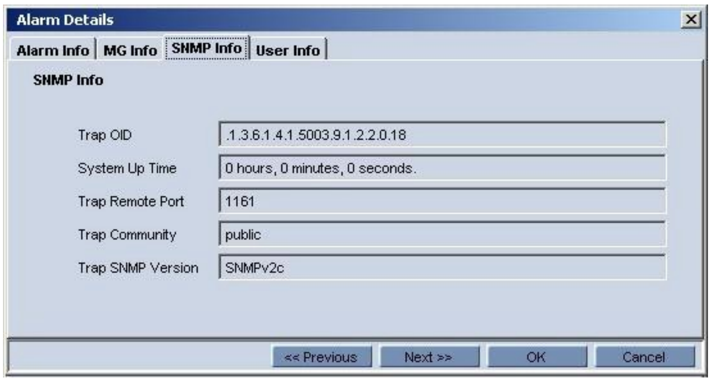
  Name of the media gateway that originated the alarm.

- Source

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

Alarm Details > tab SNMP Info

Figure 14-9: Alarm Details



SNMP Info

Trap OID: .1.3.6.1.4.1.5003.9.1.2.2.0.18
System Up Time: 0 hours, 0 minutes, 0 seconds.
Trap Remote Port: 1161
Trap Community: public
Trap SNMP Version: SNMPv2c

- Trap OID

  Trap Object Identifier, as defined in the MIB.

- System Up Time

  The time lapsed since the last system reset.

- Trap Remote Port

  The EMS UDP remote port at which the trap was received.

- Trap CommDescription
- Textual description of the alarm, received as part of the alarm information
- unity

  SNMP Community string, provided as part of the SNMP trap.

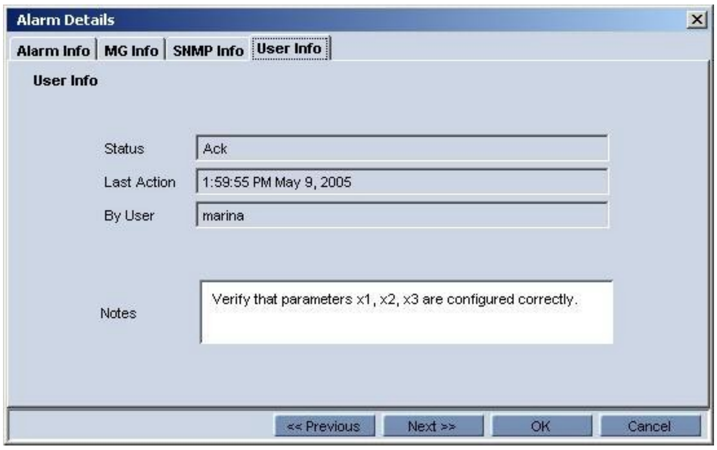
- Trap SNMP Version

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

  - v1 for SNMPv1
  - v2c for SNMPv2
  - v3 for SNMPv3

Alarm Details > tab User Info

Figure 14-10: Alarm Details - User Info



Status: Ack

Last Action: 1:59:55 PM May 9, 2005

By User: marina

Notes: Verify that parameters x1, x2, x3 are configured correctly.

- Status

  Either:

  - New (the alarm has recently been received by the EMS).
  - Ack (the alarm was manually acknowledged by a user. Refer to the other User Info fields.)
  - Manually Cleared (the alarm was manually cleared (deleted) by a user. Refer to the other User Info fields.)
  - Automatically Cleared (a clear alarm was received by the EMS from the media gateway; the alarm condition no longer exists.)

- 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.

14.7 Acknowledging an Alarm

Operators should acknowledge an alarm in order 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:

Either:

- Right-click on 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.

14.8 Alarms Clearing

Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) when a Clear alarm is generated by **the same entity (source) and same media gateway** that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature prevents irrelevant alarms from congesting the Alarms Browser. Operators view the list of **only the currently active alarms.**

14.8.1 After an Alarm is Cleared

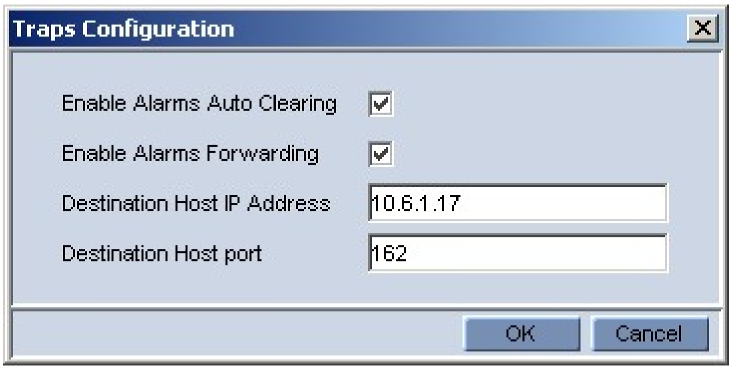
After an alarm is cleared, the cleared alarm is saved in the Alarms History where its status is indicated as 'Automatically Cleared' and notification of the time when the clearing was performed is displayed.

By default, the EMS performs automatic alarms clearing. This feature is available for system debug purposes.

Administrators can disable automatic alarms clearing and switch to manual clearing mode by opening the Faults menu > Trap Configuration, and unchecking the 'Automatic Clearing' check box.

Clicking the OK button applies the configuration to all managed media gateways and to all EMS clients.

Figure 14-11: Traps Configuration Screen



Traps Configuration

Enable Alarms Auto Clearing ☑

Enable Alarms Forwarding ☑

Destination Host IP Address 10.6.1.17

Destination Host port 162

14.9 Trap Forwarding to Northbound IF

All traps received by the EMS from managed media gateways can be forwarded to the NMS (Network Management System) as SNMPv2 traps.

Administrators can configure the EMS to forward traps to the NMS by opening the Faults menu > Trap Configuration (refer to 'After an Alarm is Cleared' on page 97, specifically, the figure) and checking the check box ‘Enable Alarms Forwarding’. Clicking the OK button applies the configuration to all managed media gateway alarms and to all EMS clients.

14.10 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, take these steps:

- Open the 'Faults' menu and choose option 'Save Alarms' in the EMS main screen; Alarms viewed in the Alarm Browser screens are saved (apply appropriate filters before saving alarms).

➢ To save ‘Alarms History’ alarms in a *.csv file, take these steps:

- Open the 'Faults' menu and choose option 'Save Alarms' in the Alarms History screen.

  Result:

  a. 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)

  b. 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 ‘emsFiles/Logs’. 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.

15 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.

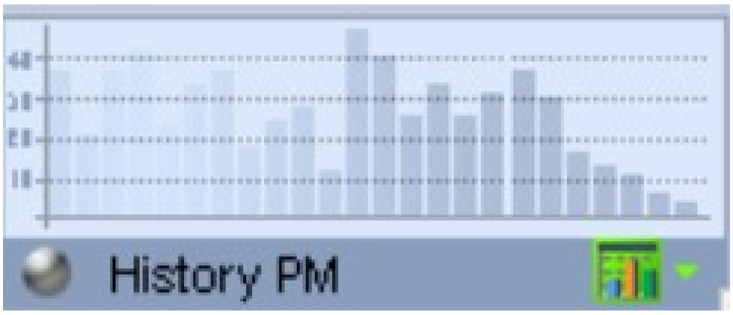
Historical data can be used for long-term network analysis and planning.

In this version, the following equipment supports performance supports performance-monitoring data:

- Media Gateway 3500, version 3.0 (System Controller board, TP modules and DS1 trunk level)

Note: The performance monitoring icon in the Info pane (refer to the figure below) is only displayed for relevant media gateways / managed entities. The color of the globe icon (adjacent to 'History PM') indicates whether background monitoring is running for a certain device. Green indicates that it is running; gray indicates that it is not.

Figure 15-1: Performance Monitoring Icon in the Info Pane



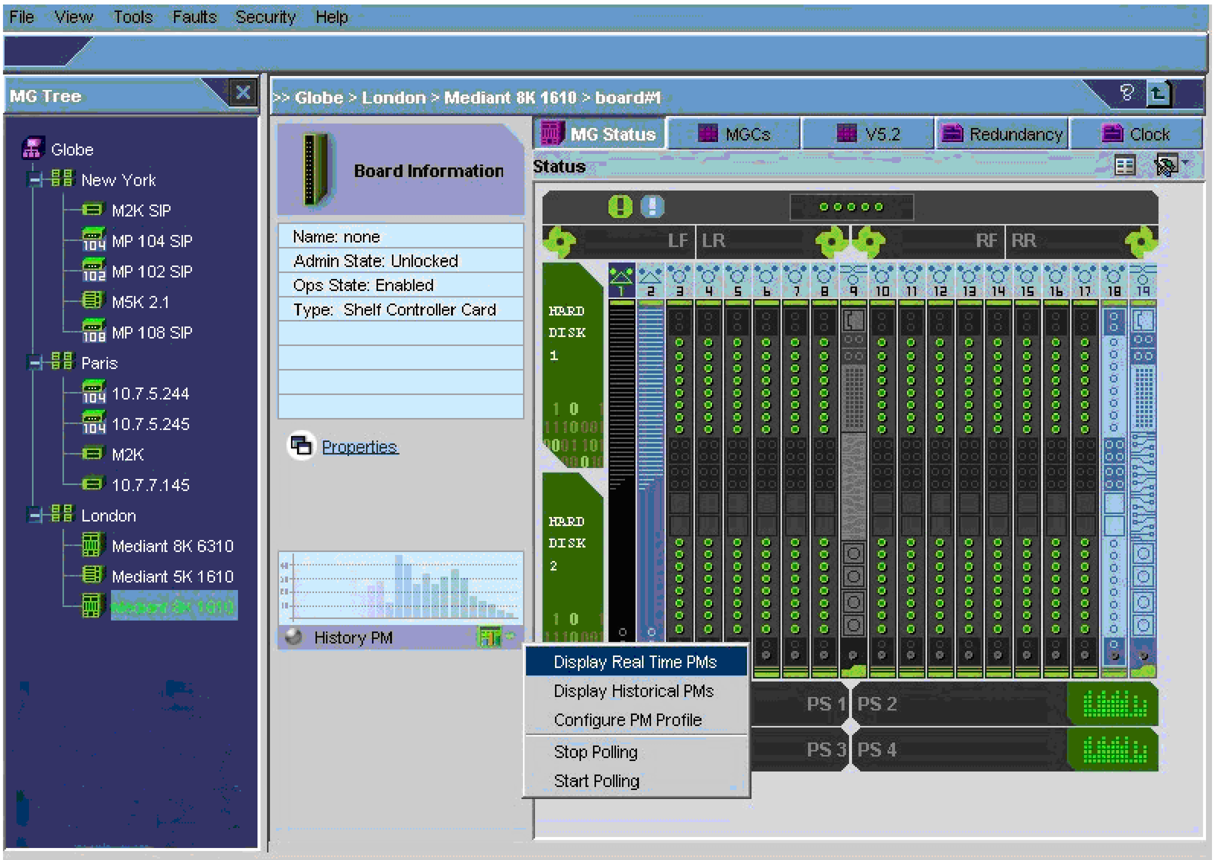
15.1 Real-Time Performance Monitoring

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

➢ To select an entity to poll, take these steps:

1. Navigate to the entity according to regular EMS navigation concepts and from the ‘Performance Monitoring’ menu in the Info pane, select the option 'Display Real Time PMs' (refer to the figure below).

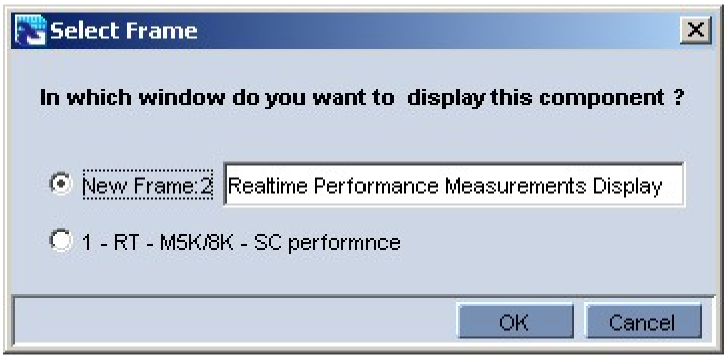
Figure 15-2: Display Real-Time PMs



Name: none
Admin State: Unlocked
Ops State: Enabled
Type: Shelf Controller Card

2. 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 15-3: Selecting the Frame to Display the Graph of the Entity's Performance



In which window do you want to display this component ?

● New Frame:2 Realtime Performance Measurements Display

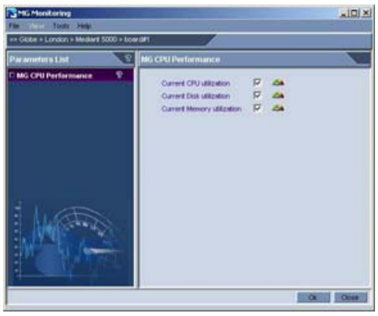
○ 1 - RT - M5K/8K - SC performnce

Users can open up to five separate real-time graphs in the same client application. In each graph, you can simultaneously view up to 5 parameters of the same entity (media gateway, board, trunk) or compare the same parameters over different entities (different boards / trunks of the same or different gateways).

After the real-time frame is opened, users can continue to select entities to be added to the same frame. After all entities are selected, select the parameter to poll by clicking the 'Parameters Filter' button. Only parameters available for that entity type are displayed for selection. Note that you can either select a few entities or a few parameters.

The performance-monitoring feature supports two parameter types: Gauges and Counters. Gauges are indicated by and Counters are indicated by .

Figure 15-4: Parameter Type: Gauges



MG Monitoring

>> Globe > London > Mediant 5000 > board#1

Parameters List

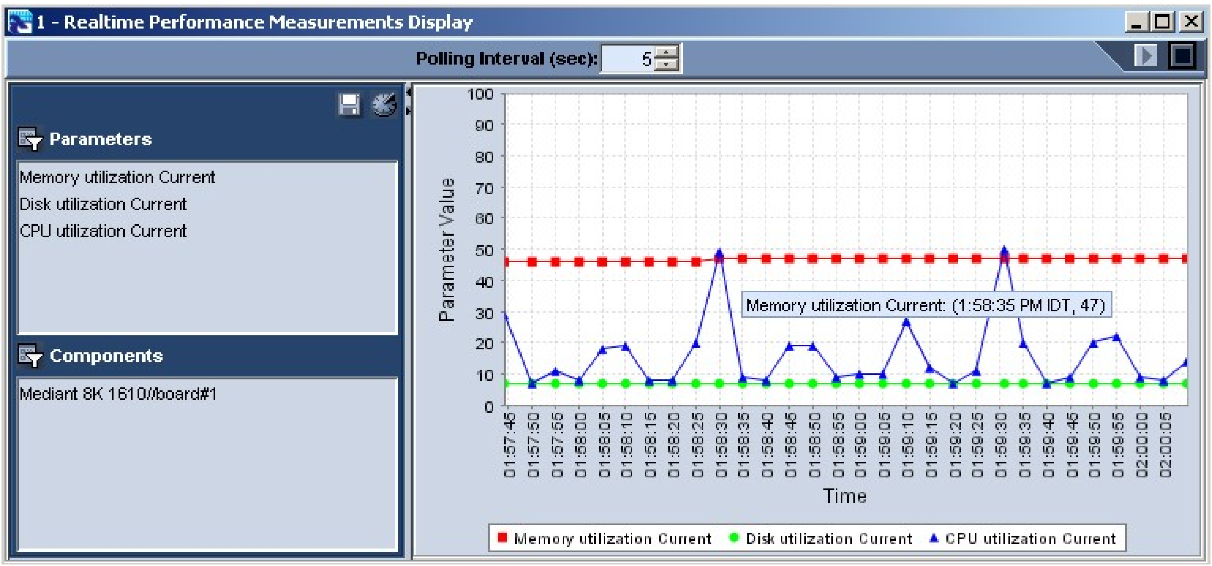
□ MG CPU Performance

MG CPU Performance

Current CPU utilization ☑
Current Disk utilization ☑
Current Memory utilization ☑

In the 'Real-Time Performance Measurements Display' screen (refer to the figures below), choose the Polling Interval you require from the drop-down under the title bar and press 'Start' to start polling; a real-time graph is displayed. You can pause the polling by pressing the pause button and restart it again by pressing the start 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. In addition, you can apply Parameters or Components filters by clicking the filter button.

Figure 15-5: Real-Time Performance Measurements Display



1 - Realtime Performance Measurements Display

Polling Interval (sec): 5

Parameters

Memory utilization Current
Disk utilization Current
CPU utilization Current

Components

Mediant 8K 1610//board#1

Memory utilization Current: (1:58:35 PM IDT, 47)

In the ‘Real-Time Performance Measurements Display’ screen (refer to the figures below), choose the 'Polling Interval you require from the drop-down under the title bar and press ‘Start’ 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, take this step:

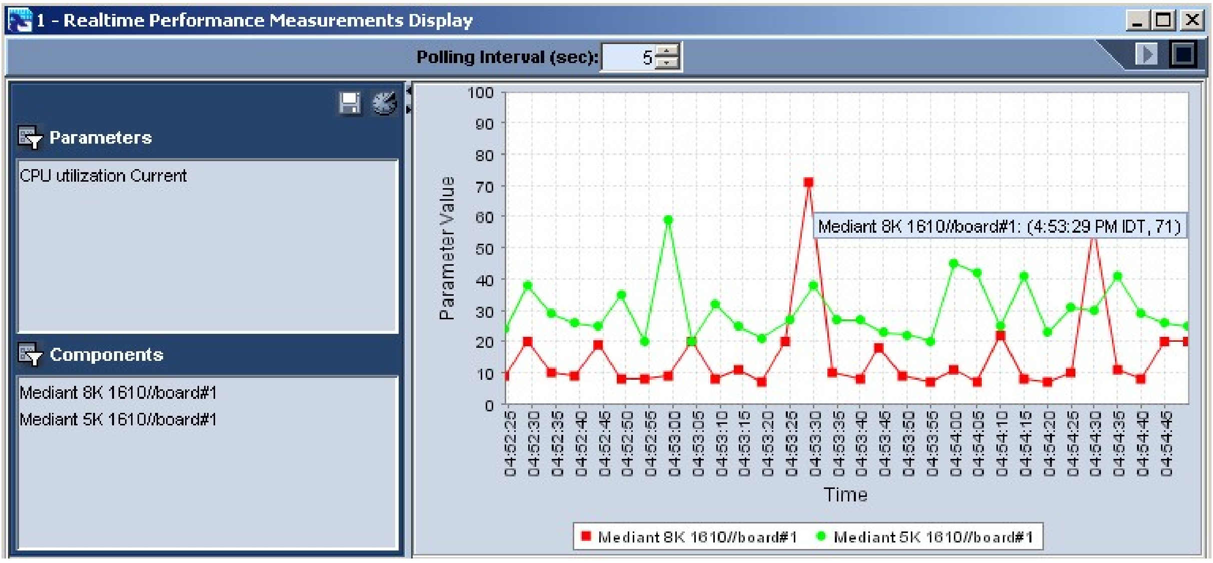
- Stop the current graph, perform the required configuration changes and then restart the polling.

  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:

  1. Compare CPU utilization of System Controller boards in the Media Gateway 3500 (refer to the figure below):

Figure 15-6: Graph Comparing CPU Utilization of SC Boards in Media Gateways



1 - Realtime Performance Measurements Display

Polling Interval (sec): 5

Parameters

CPU utilization Current

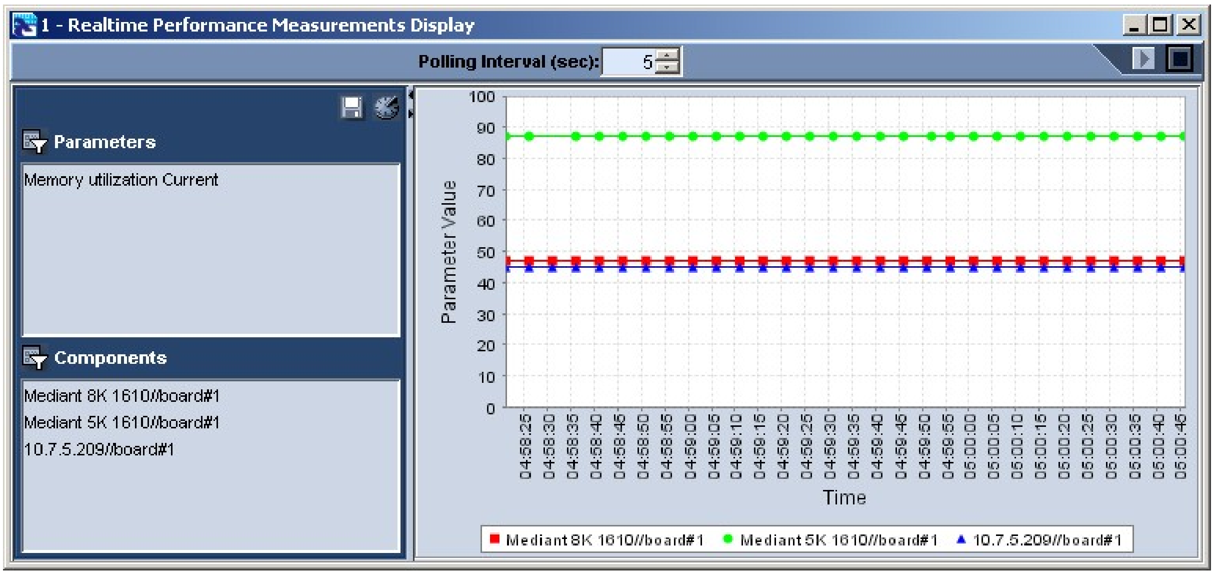
Components

Mediant 8K 1610//board#1
Mediant 5K 1610//board#1

Mediant 8K 1610//board#1: (4:53:29 PM IDT, 71)

2. Compare memory utilization of System Controller boards in the gateways.

Figure 15-7: Graph Comparing Memory Utilization of SC Boards in Media Gateways



1 - Realtime Performance Measurements Display

Polling Interval (sec): 5

Parameters

Memory utilization Current

Components

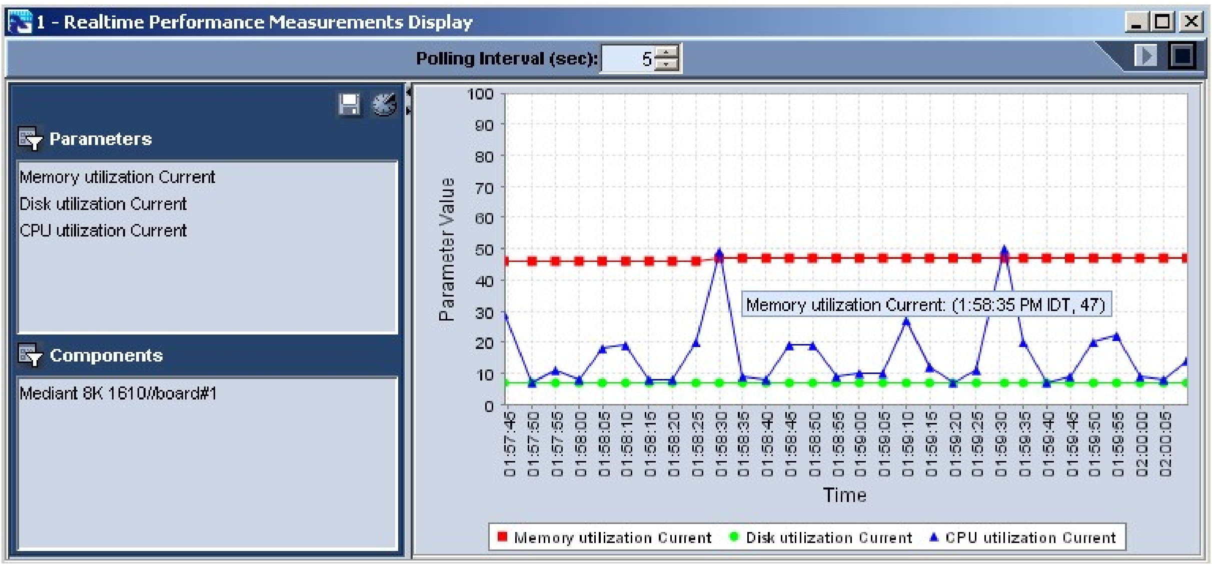
Mediant 8K 1610//board#1

Mediant 5K 1610//board#1

10.7.5.209//board#1

3. View CPU, Memory and Disk utilization of the System Controller board #1 in the Media Gateway 3500.

Figure 15-8: View CPU, Memory and Disk Utilization of Media Gateway 3500 SC Board 1



1 - Realtime Performance Measurements Display

Polling Interval (sec): 5

Parameters

Memory utilization Current

Disk utilization Current

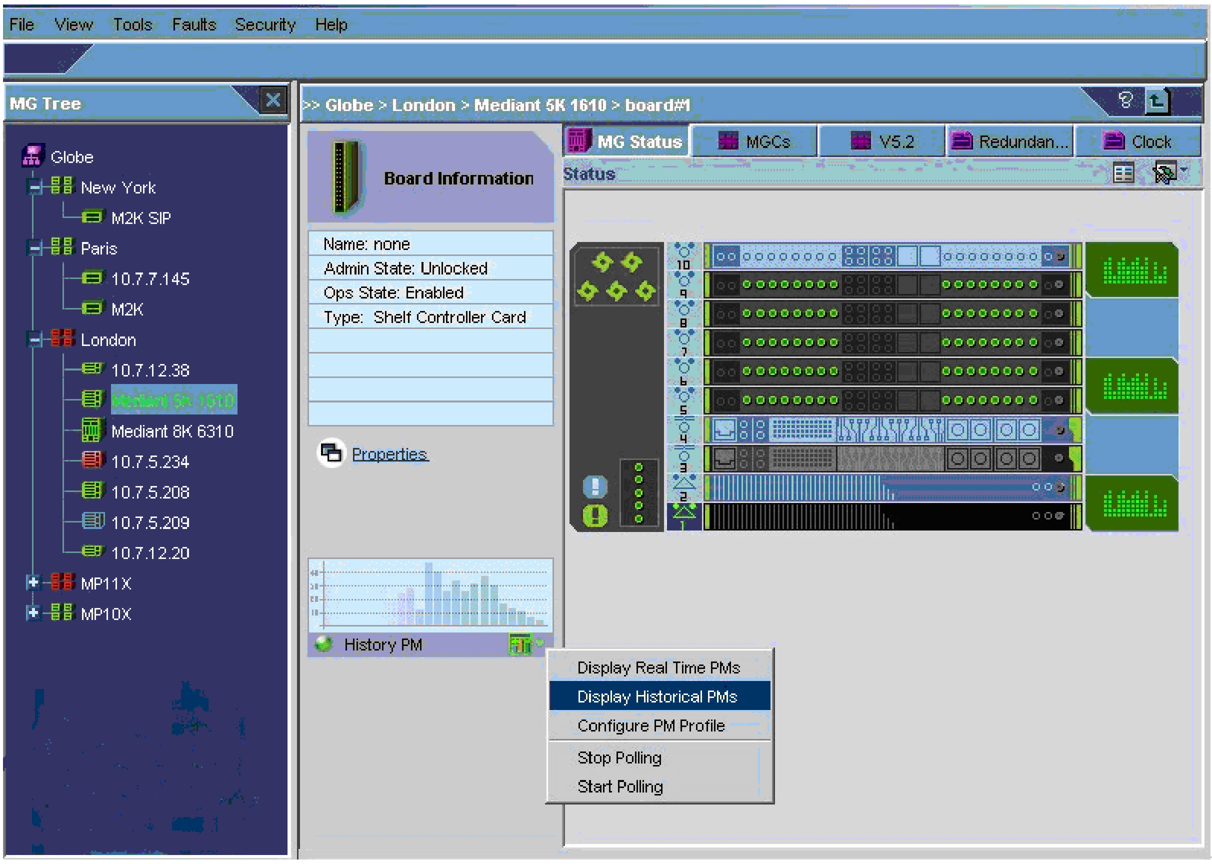
CPU utilization Current

Components

Mediant 8K 1610//board#1

15.2 Background (History) Performance Monitoring

Figure 15-9: Performance Monitoring Menu - Display Historical PMs



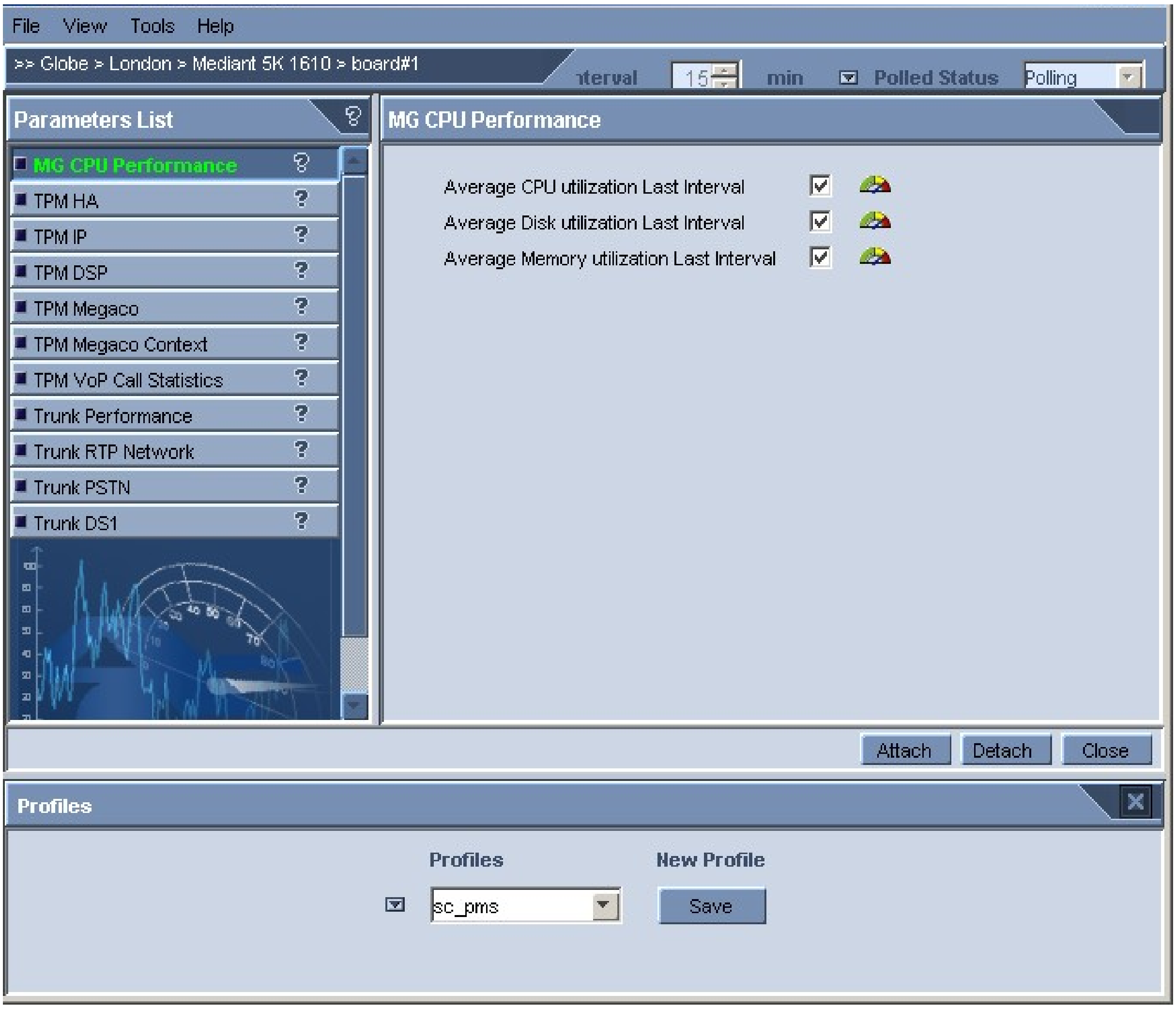
Name: none
Admin State: Unlocked
Ops State: Enabled
Type: Shelf Controller Card

15.3 Configuring Background Monitoring

➢ To collect historical performance data, take these steps:

1. Select the option ‘Configure PM Profile’ in the ‘Performance Monitoring’ menu; the background configuration screen opens (refer to the figure below). Note that each gateway and control protocol features a different set of available parameters. The figure below shows the gateway background monitoring provisioning parameters.

Figure 15-10: Background Monitoring Provisioning Parameters



>> Globe > London > Mediant 5K 1610 > board#1

nterval 15 min

Polled Status Polling

MG CPU Performance

Average CPU utilization Last Interval ☑

Average Disk utilization Last Interval ☑

Average Memory utilization Last Interval ☑

Profiles

Profiles: sc_pms

New Profile: Save

2. 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.

3. Click the ‘Attach’ button. Note that the parameters of all media gateway entities are polled. For example, trunk performance parameters are polled for all trunks of the selected media gateway. Note too that the same background configuration screen opens from every media gateway entity.

4. Select the Time Interval according to which to perform the polling (the default interval is 15 minutes) and press the polling state menu item 'Start' option. Verify that the polling status has changed to 'Polled'.

5. To change the polling interval or the PM profile, or to stop polling, press polling state menu item 'Stop' option.

15.4 Viewing Historical Data

➢ To view collected (historical) data, take these steps:

1. Select the option 'Display Historical PMs' in the 'Performance Monitoring' menu; the 'History PM' screen opens.

2. Continue (if needs be) to select entities to be added to the same screen. All entities must be of the same type (trunks, or System Controller boards, or gateways of the same control protocol type). After all entities are selected, select the parameter to view by pressing 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.

3. Select the Time Interval according to which you need to review data and click 'Refresh'; after data is displayed, you can save it as a *csv* file by clicking the 'Save' icon.

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

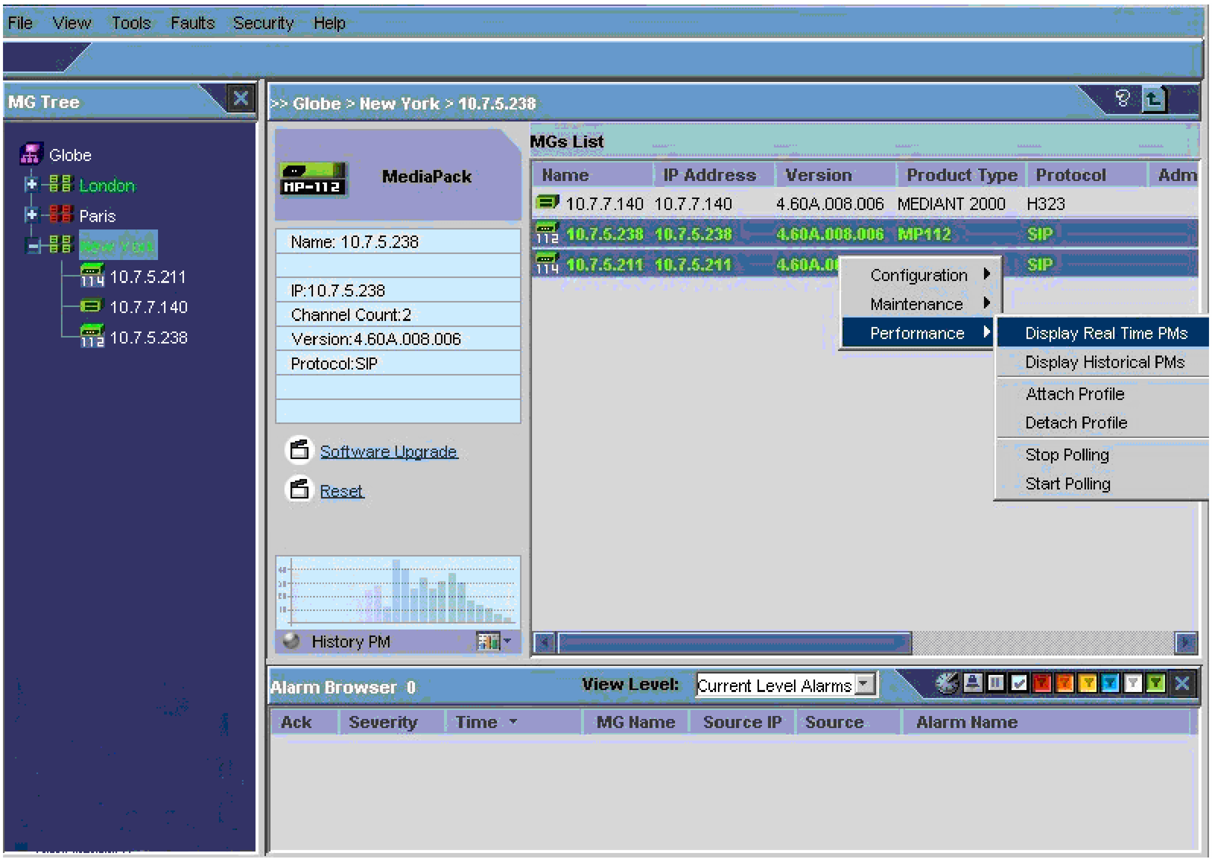
   Each time a sample is taken from the gateway, it is stored in the detailed table, where the entity name and index, parameter name, start, stop polling time and parameter value are specified.

   After every 24 hours of sampled data, the detailed table is summarized. For each entity and parameter, the start and stop summary time is stored and the average, minimal and maximal value is displayed.

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

15.5 Performance Monitoring Actions on Multiple Media Gateways

Figure 15-11: Performance Monitoring Actions on Multiple Media Gateways



Name: 10.7.5.238

IP:10.7.5.238

Channel Count:2

Version:4.60A.008.006

Protocol:SIP

Name	IP Address	Version	Product Type	Protocol	Adm
10.7.7.140	10.7.7.140	4.60A.008.006	MEDIANT 2000	H323	
10.7.5.238	10.7.5.238	4.60A.008.006	MP112	SIP	
10.7.5.211	10.7.5.211	4.60A.0		SIP	

Ack	Severity	Time	MG Name	Source IP	Source	Alarm Name

Users can perform following actions on multiple gateways:

a. Display Real Time / Historical PMs (refer to 'Real-Time Performance Monitoring' on page 106)

b. Attach / Detach Profile

c. Start / Stop Polling

16 Security Management

EMS Security Management features two aspects:

Network Communication Security (refer to 'Network Communication Security' on page 111).

EMS Application Security (refer to 'EMS Application Security' on page 112).

16.1 Network Communication Security

When installing the EMS server, configure its network and open the ports required for EMS client-server and EMS server-media gateway communication (refer to the EMS Server Installation and Maintenance Manual).

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

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

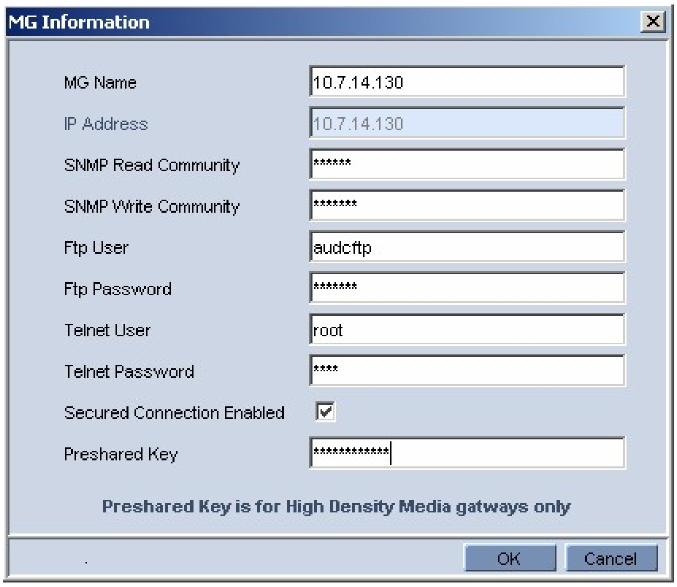
EMS server communications with media gateways is performed over the following protocols:

- SNMPv2c for provisioning, maintenance actions and fault management. SNMPv2c security is achieved by running SNMP communication over IPSec protocol.

- Telnet and FTP for installation and upgrading software. Telnet and FTP communications are secured by running them over IPSec protocol.

- To configure EMS-gateway communication over IPSec, open the ‘MG Information’ screen (right-click device in MGs List > option ‘Details’), check the ‘Secure Connection Enabled’ checkbox and enter the ‘Preshared Key’ string (refer to the figure below). This configuration can be performed either during the gateway definition stage or later. The Preshared Key string defined in the EMS and in the gateway should be identical.

Figure 16-1: MG Information - Secured Connection Enabled



MG Information

MG Name	10.7.14.130
IP Address	10.7.14.130
SNMP Read Community	******
SNMP Write Community	*******
Ftp User	audcftp
Ftp Password	*******
Telnet User	root
Telnet Password	****
Secured Connection Enabled	☑
Preshared Key	************

Preshared Key is for High Density Media gatways only

16.2 EMS Application Security

The EMS's security management feature enables the operator who holds the Administrator security level to exert control over other operators' access to system resources. Thus, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators.

Security management is carried out in the Users List screen (accessed from the Main Screen in the Security menu, option Users List) and in the Actions Journal screen (accessed from the Main Screen in the Security menu, option Actions Journal). 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.

16.3 Users Management in the EMS Application

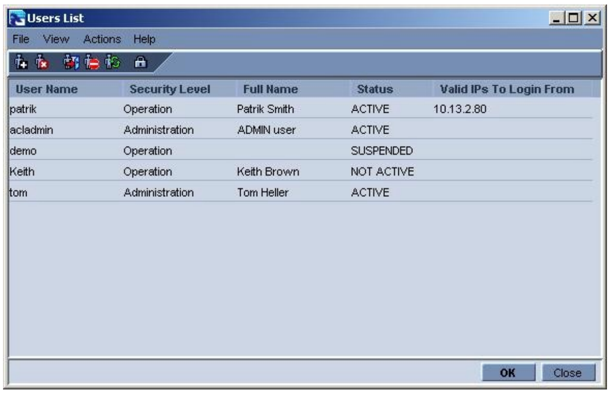
Management of users can be performed using one of two applications:

1. Centralized LDAP server. (Refer to the Installation, Operation & Maintenance Manual for instructions on how to integrate the EMS server with the LDAP server. Skip this section if you're working with a centralized LDAP server).
2. The EMS application. (If your security management is performed via the EMS application, refer to the remainder of this section for descriptions of relevant features).

➢ To open the Users List:

- In the Main Screen, open the Security menu and select the option 'Users List'; the Users List screen opens:

Figure 16-2: Users List



User Name	Security Level	Full Name	Status	Valid IPs To Login From
patrik	Operation	Patrik Smith	ACTIVE	10.13.2.80
acladmin	Administration	ADMIN user	ACTIVE	
demo	Operation		SUSPENDED	
Keith	Operation	Keith Brown	NOT ACTIVE	
tom	Administration	Tom Heller	ACTIVE	

In the Users List screen (displayed in the above figure) you can:

- 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 on 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).

Note: A user can hold only one active session at a time. If a user is in Active state, that user cannot enter the application a second time.

- Perform the following user management actions:
  - Add an operator (refer to 'Adding an Operator' on page 113)
  - Modify an operator's details and access rights (refer to 'Modifying Operator Details' on page 115)
  - Remove an operator (refer to 'Removing an Operator' on page 115)
  - Perform the forced logout of an active user (refer to 'Forcing the Logout of a Currently Active Operator' on page 115)
  - Suspend a user (refer to 'Suspending an Operator' on page 116)
  - Release an operator from suspension (refer to 'Releasing an Operator from Suspension' on page 116)
  - Cancel changes made to the Users List (refer to 'Canceling Changes Made to the Users List' on page 116)
  - Change an operator's password (refer to 'Changing an Operator's Password' on page 116)
  - View/assess an operator's actions in an Actions Journal (refer to 'Viewing Operator Actions in the Actions Journal' on page 118)

16.3.1 Adding an Operator

➢ To add an operator:

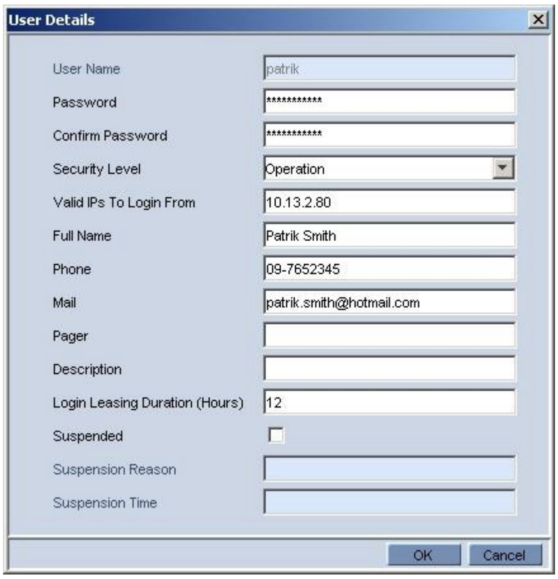
Either:

- Open the menu Actions and choose option Add User.

  -OR-

- Click the button “Add User” on the toolbar; the User Details screen opens.

Figure 16-3: User Details Screen



User Details

User Name	patrik
Password	***********
Confirm Password	***********
Security Level	Operation
Valid IPs To Login From	10.13.2.80
Full Name	Patrik Smith
Phone	09-7652345
Mail	patrik.smith@hotmail.com
Pager	
Description	
Login Leasing Duration (Hours)	12
Suspended	□
Suspension Reason	
Suspension Time	

- 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 (refer to 'Security Management' on page 111, specifically, to the figure 'Users List').
- Mandatory fields in the User Details screen are Login Name and Password. The other fields in the screen are optional.
- Click 'OK' at the bottom of the screen to send your changes to the server.

Parameters that can be defined during an ‘Add User’ operation or modified thereafter:

- 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. Operators are not allowed to reuse their five previously used passwords. The Password should include between 8-15 characters. The Password should answer at least 3 out of 4 requirements: It should be combined of small and capital letters, digits and signs. It should not be a repetition of the User Name.
  - Security Level: EMS operators can be allocated one of 3 security levels:
  - Monitoring (viewing only)
  - Operation (viewing and all system provisioning operations)
- Administration (viewing, all system provisioning operations, and operator security management described in this section).
- Valid IPs to Log In From: An IP address or list of IP addresses (separated by ;) from which the operator is allowed to log into the EMS application.
- 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.

- Login Leasing Duration (Hours): After the defined period of time, the user is notified that the session is finished and is prompted to enter his/her password in order to work with the EMS. When defined as 0 (default configuration), no leasing time is applied. Leasing time is a security mechanism to permit the operator to log in to a time duration that is equal to one shift (i.e., 8 hours).
- User suspension information: Suspension Status, Suspension Reason and Suspension Time.

16.3.2 Modifying Operator Details

➢ To modify operator details:

1. Double-click on 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' (refer to 'Adding an Operator' on page 113) 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 Administrator to set access rights for each operator: 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.

16.3.3 Removing an Operator

➢ To remove a operator:

1. In the Users List screen, select the row of the operator to be removed. 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 will be 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 should always be defined in the EMS system. Attempted removal of the last user with the security level of Administrator will fail.

16.3.4 Forcing the Logout of a Currently Active Operator

➢ To force the logout of a currently active operator, take these steps:

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.

16.3.5 Suspending an Operator

➢ To suspend an operator, take these steps:

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 check the check box ‘Suspended’; all selected rows now indicate ‘SUSPENDED’.

3. Open the ‘User Details’ screen (double-click on 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 cannot be suspended.

16.3.6 Releasing an 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 uncheck the checkbox ‘Suspended’; all selected rows now indicate ‘NOT ACTIVE’.

3. Click OK to send your changes to the server.

16.3.7 Canceling 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.

16.4 Changing an Operator's Password

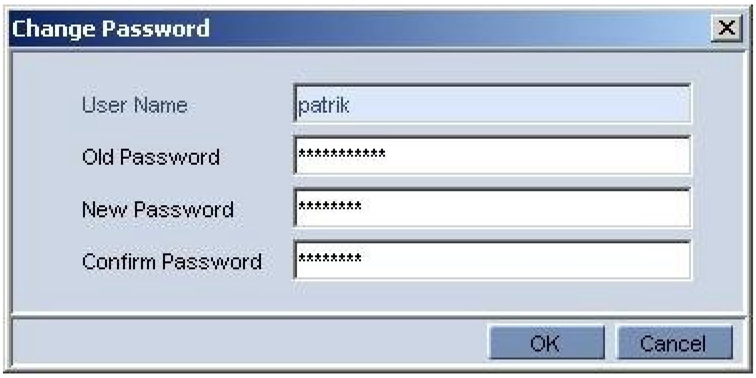
- Every operator should change password once at the end of every predefined period of time (by default, every 90 days). The operator receives a password expiry warning 7 days before the date on which the password expires.

- Operators are not allowed to reuse their five previously used passwords.
- The password should include between 8-15 characters. The password should answer at least 3 out of 4 requirements: It should be combined of small and capital letters, digits and signs.
- The password should not be a repetition of the User Name.

➢ 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 (refer to the figure below).

Figure 16-4: Change Password



Change Password

User Name: patrik

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

New Password: ********

Confirm Password: ********

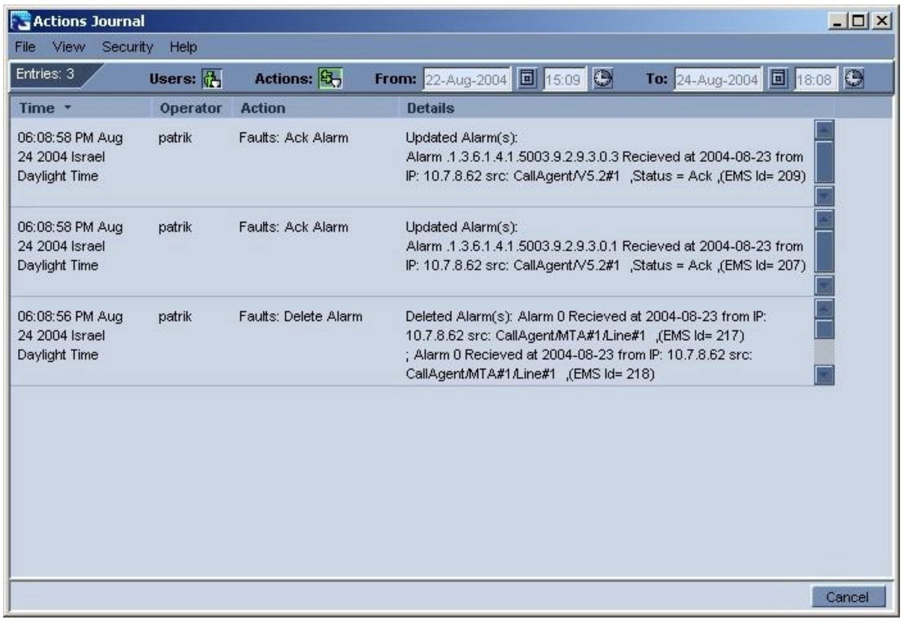
2. Change the password previously defined in the Password field.

16.5 Viewing Operator Actions in the Actions Journal

➢ To view the Actions Journal:

- In the Main Screen, open the 'Security' menu and choose option 'Actions Journal'; the Actions Journal screen is displayed.

Figure 16-5: Actions Journal



Entries: 3

From: 22-Aug-2004 15:09 To: 24-Aug-2004 18:08

Time	Operator	Action	Details
06:08:58 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Ack Alarm	Updated Alarm(s): Alarm .1.3.6.1.4.1.5003.9.2.9.3.0.3 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/V5.2#1 ,Status = Ack ,(EMS Id= 209)
06:08:58 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Ack Alarm	Updated Alarm(s): Alarm .1.3.6.1.4.1.5003.9.2.9.3.0.1 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/V5.2#1 ,Status = Ack ,(EMS Id= 207)
06:08:56 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Delete Alarm	Deleted Alarm(s): Alarm 0 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/MTA#1/Line#1 ,(EMS Id= 217) ; Alarm 0 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/MTA#1/Line#1 ,(EMS Id= 218)

- The Actions Journal screen enables the operator to track all EMS actions.
- Operators can filter according to Users, Date and Time.
- The Actions Journal screen is read-only and non-configurable.
- Data displayed in the Actions Journal can be saved in a *csv* file.

16.5.1 Filters Supported in the Actions Journal

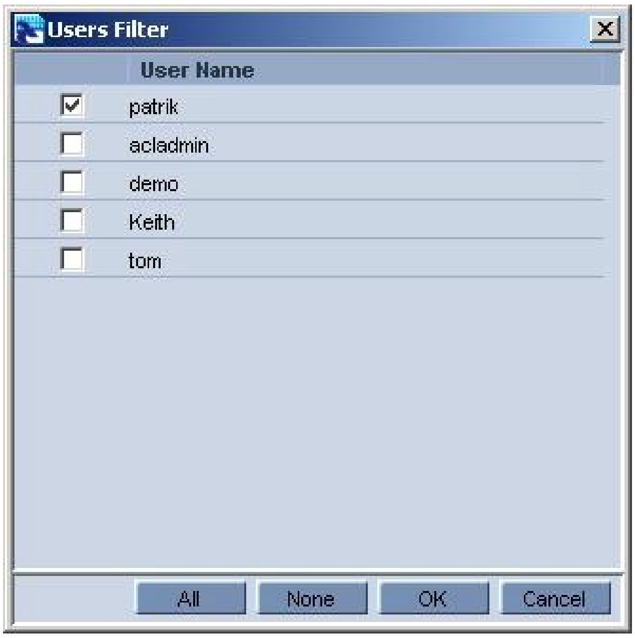
The Actions Journal supports the following filters:

- User's Filter
  - An operator can select a user or a set of users whose actions the operator needs to view.
- Action Type 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.)
  - Security Management Actions (add, remove, update operator info, login, logout)
- Date and Time Filter

All filters can be applied simultaneously. For example, to determine which actions relating to Fault management were performed by the operator ‘patrik’ between August 22 and August 24, you’d perform following actions:

1. Open the Users Filter (refer to the figure below) and check the checkbox adjacent to user name ‘patrik’.

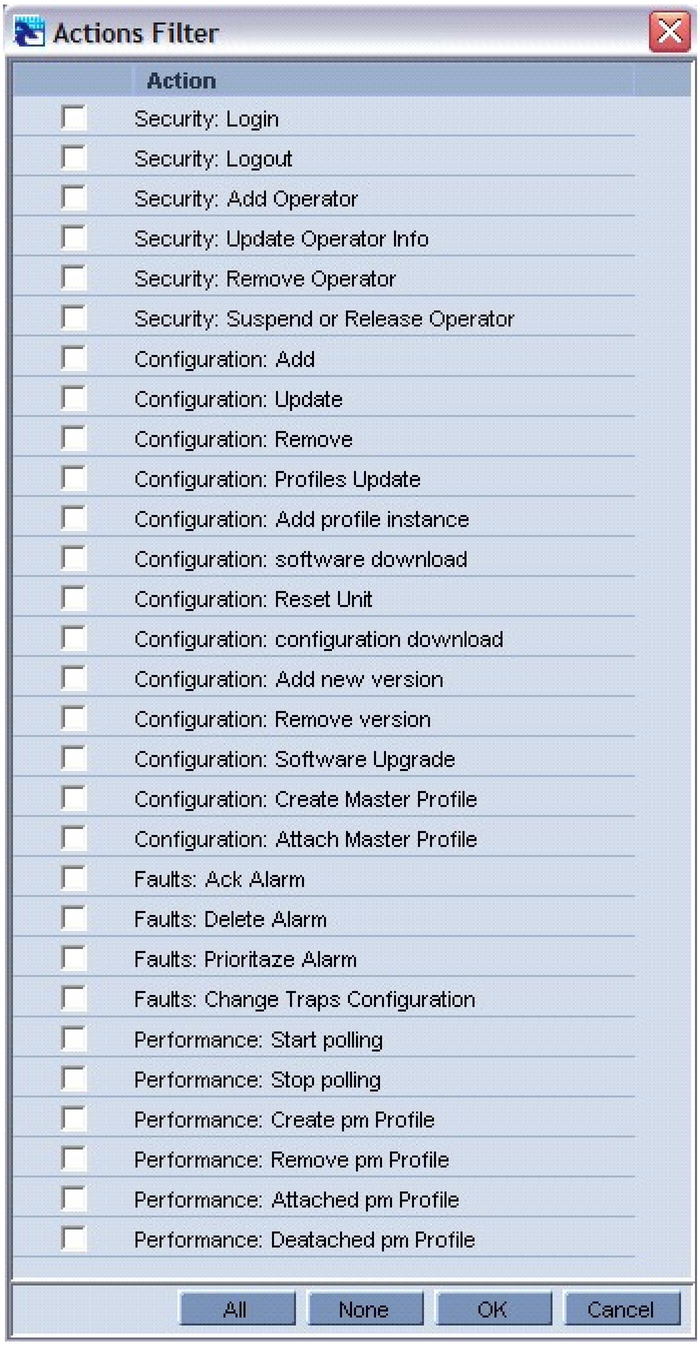
Figure 16-6: Users Filter



	User Name
☑	patrik
□	acladmin
□	demo
□	Keith
□	tom

2. Open the Actions Filter and check each checkbox adjacent to actions related to Faults (refer to the figure below).

Figure 16-7: Actions Filter

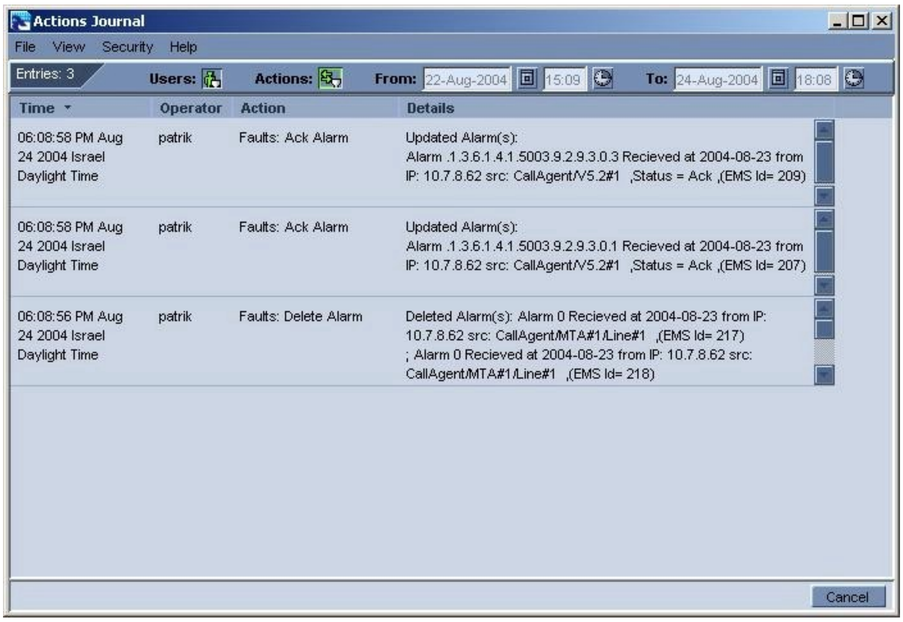


Actions Filter

	Action
□	Security: Login
□	Security: Logout
□	Security: Add Operator
□	Security: Update Operator Info
□	Security: Remove Operator
□	Security: Suspend or Release Operator
□	Configuration: Add
□	Configuration: Update
□	Configuration: Remove
□	Configuration: Profiles Update
□	Configuration: Add profile instance
□	Configuration: software download
□	Configuration: Reset Unit
□	Configuration: configuration download
□	Configuration: Add new version
□	Configuration: Remove version
□	Configuration: Software Upgrade
□	Configuration: Create Master Profile
□	Configuration: Attach Master Profile
□	Faults: Ack Alarm
□	Faults: Delete Alarm
□	Faults: Prioritaze Alarm
□	Faults: Change Traps Configuration
□	Performance: Start polling
□	Performance: Stop polling
□	Performance: Create pm Profile
□	Performance: Remove pm Profile
□	Performance: Attached pm Profile
□	Performance: Deatached pm Profile

3. Open the ‘Date From’ filter and select August 22 (refer to the figure below). Define the ‘Time From’ filter. Open the ‘Date To’ filter and select August 24. Define the ‘Time To’ filter; all filters are applied simultaneously to provide the view displayed in the figure below.

Figure 16-8: Actions Journal



Entries: 3 Users: Actions: From: 22-Aug-2004 15:09 To: 24-Aug-2004 18:08

Time	Operator	Action	Details
06:08:58 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Ack Alarm	Updated Alarm(s): Alarm .1.3.6.1.4.1.5003.9.2.9.3.0.3 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/V5.2#1 ,Status = Ack ,(EMS Id= 209)
06:08:58 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Ack Alarm	Updated Alarm(s): Alarm .1.3.6.1.4.1.5003.9.2.9.3.0.1 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/V5.2#1 ,Status = Ack ,(EMS Id= 207)
06:08:56 PM Aug 24 2004 Israel Daylight Time	patrik	Faults: Delete Alarm	Deleted Alarm(s): Alarm 0 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/MTA#1/Line#1 ,(EMS Id= 217) ; Alarm 0 Recieved at 2004-08-23 from IP: 10.7.8.62 src: CallAgent/MTA#1/Line#1 ,(EMS Id= 218)

16.5.2 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, take these steps:**

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).

17 Single Log-In Northbound Interface

The EMS features a Java™ API Northbound Interface and a CLI (Command Line Interface), enabling operators to log in from an NMS client to a single EMS client.

After the EMS client is installed, operators can access a folder named “Nbif” located under the client directory (Program Files>EMS Client).

The folder “Nbif” includes two important files:

- nbif.jar (this file is the Java™ API Northbound Interface; refer to 'Java API Northbound Interface' on page 123)
- NbIf.html (this file includes API information that programmers should know when programming with Java™ code, in order to connect to code via a CLI).

17.1 Java API Northbound Interface

Introduce the following .jar files to your Java™ application:

- nbif.jar (Nbif folder)
- client.jar
- jbcl.jar
- Externals (client installation folder)

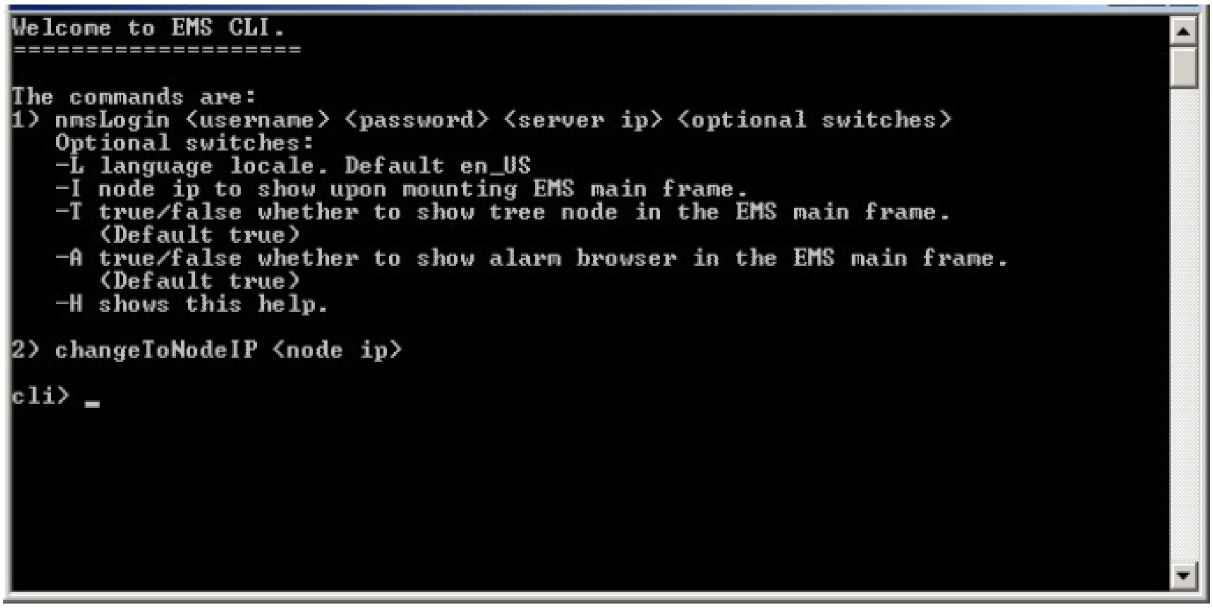
For a detailed description of the Java™ API, open the file Nbif.html located in the folder “Nbif” located in the client directory (Program Files>EMS Client).

17.2 CLI - Command Line Interface

➢ To run the CLI:

1. In the EMS client installation directory on your C: drive, double-click file cli.exe; the ‘Welcome to EMS CLI’ DOS prompt opens.

Figure 17-1: ‘Welcome to EMS CLI’ DOS Prompt



```
Welcome to EMS CLI.
====================

The commands are:
1> nmsLogin <username> <password> <server ip> <optional switches>
   Optional switches:
   -L language locale. Default en_US
   -I node ip to show upon mounting EMS main frame.
   -T true/false whether to show tree node in the EMS main frame.
      (Default true)
   -A true/false whether to show alarm browser in the EMS main frame.
      (Default true)
   -H shows this help.

2> changeToNodeIP <node ip>

cli> _
```

17.2.1 Enabling Log-in from an NMS Client to a Single EMS Client

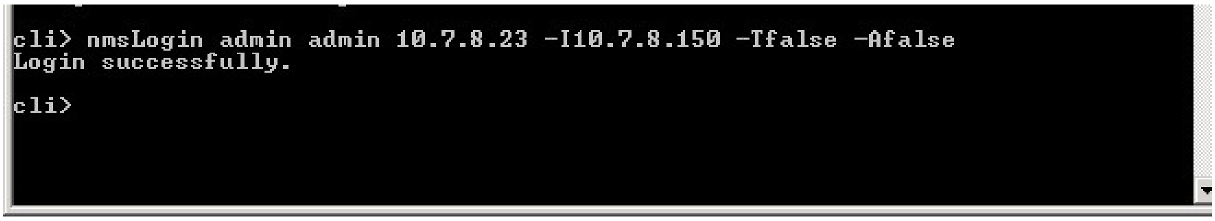
➢ To enable a log-in from an NMS client to a single EMS client:

1. Follow the format presented in the ‘Welcome to EMS CLI’ DOS prompt (refer to' Command Line Interface (CLI)' on page 124, to the figure) and type (for example) the following:

   cli> nmsLogin admin admin 10.7.8.23 -I10.7.8.150 -Tfalse -Afalse

2. Press Enter to execute this command; ‘Login successfully’ is displayed (shown below) and the EMS client connection to server 10.7.8.23 with username ‘admin’, password ‘admin’ is opened (shown below). The EMS client is focused on the media gateway whose IP address is 10.7.8.150. Its MGs Tree and Alarm Browser are not viewable:

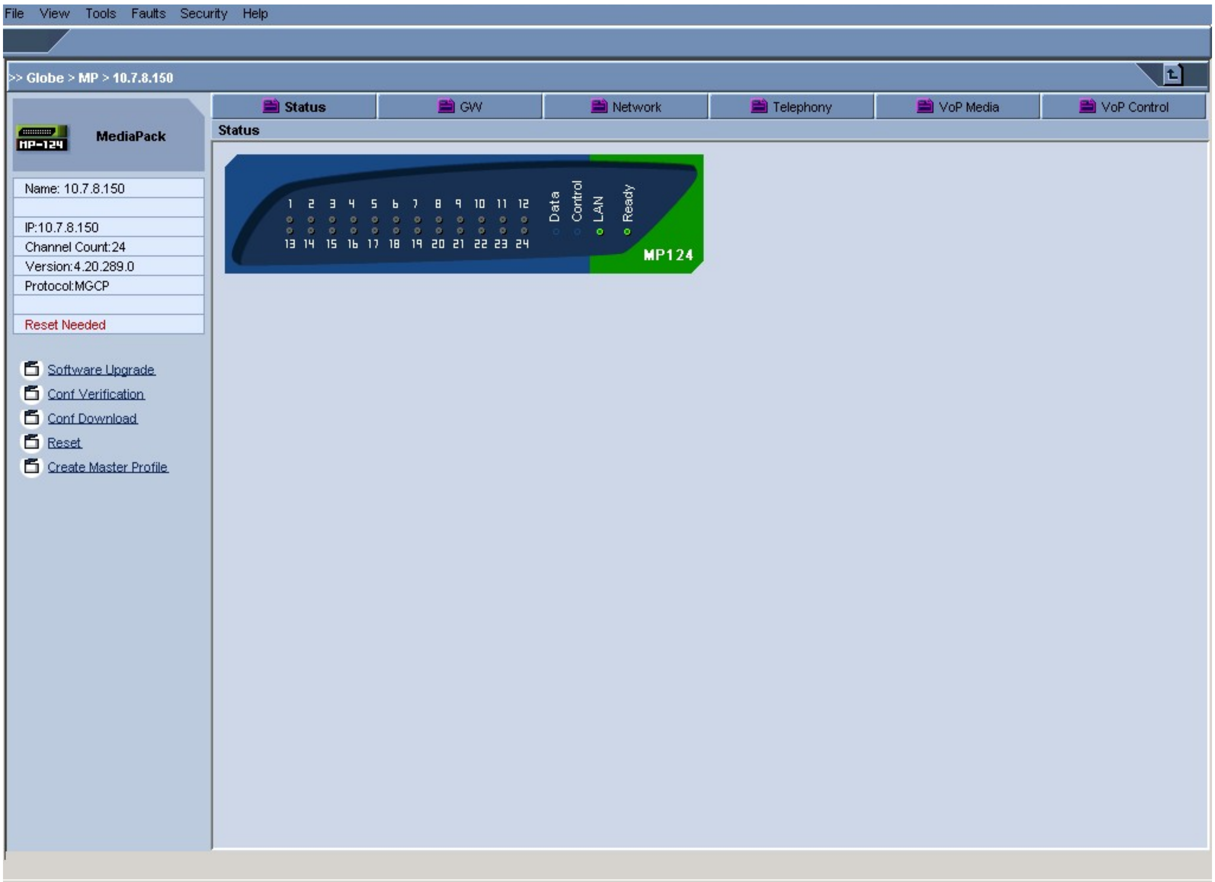
Figure 17-2: Log-in from NMS Client to a single EMS Client: 'Login Successful' in DOS Prompt



```
cli> nmsLogin admin admin 10.7.8.23 -I10.7.8.150 -Tfalse -Afalse
Login successfully.

cli>
```

Figure 17-3: Enabling Log-in from an NMS Client to a Single EMS Client (MGs Tree, Alarm Browser Not Viewed)



Name: 10.7.8.150

IP:10.7.8.150

Channel Count:24

Version:4.20.289.0

Protocol:MGCP

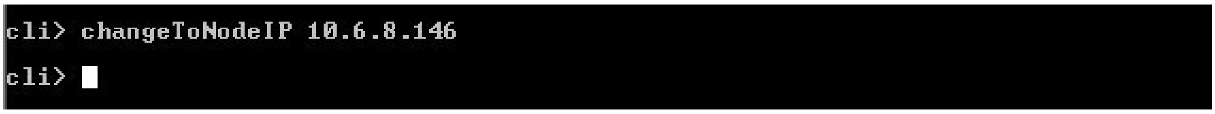
Reset Needed

➢ To switch to another (single) EMS client:

1. In the cli> command line in the DOS prompt adjacent to **changeToNode**, type the IP address of the EMS client that you need to switch to (refer to the figure below).

- (Example: cli> changeToNodeIP 10.6.8.146)

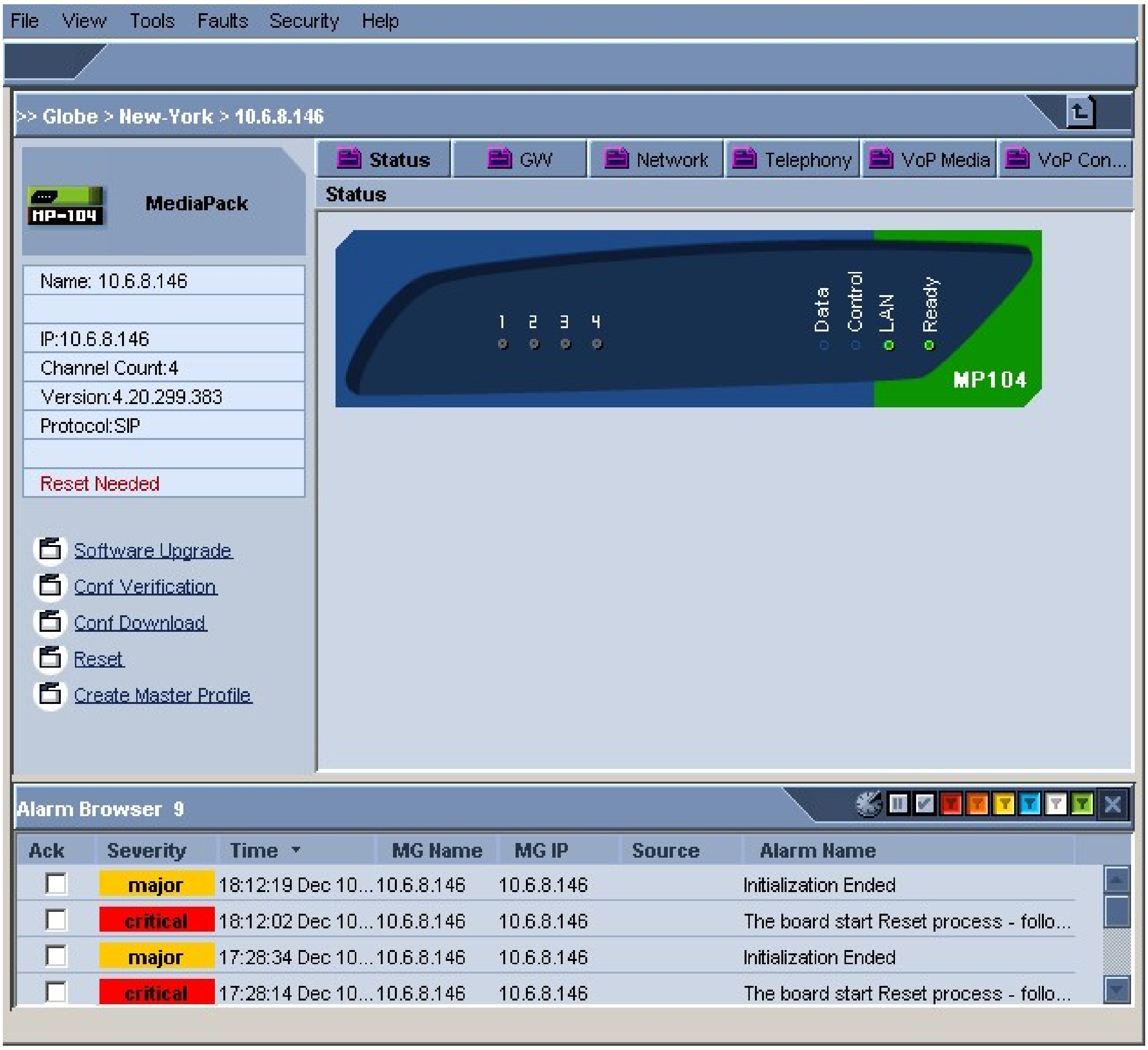
Figure 17-4: Switching to Another (Single) EMS Client



```
cli> changeToNodeIP 10.6.8.146
cli> █
```

2. Press Enter**;** the command is executed and the EMS changes focus to the media gateway with IP address 10.6.8.146 (refer to the figure below).

Figure 17-5: Switching to Another (Single) EMS Client



Name: 10.6.8.146

IP:10.6.8.146

Channel Count:4

Version:4.20.299.383

Protocol:SIP

Reset Needed

Ack	Severity	Time ▾	MG Name	MG IP	Source	Alarm Name
□	major	18:12:19 Dec 10...	10.6.8.146	10.6.8.146		Initialization Ended
□	critical	18:12:02 Dec 10...	10.6.8.146	10.6.8.146		The board start Reset process - follo...
□	major	17:28:34 Dec 10...	10.6.8.146	10.6.8.146		Initialization Ended
□	critical	17:28:14 Dec 10...	10.6.8.146	10.6.8.146		The board start Reset process - follo...

18 Troubleshooting

18.1 Failure to Connect to a Media Gateway - all MGs

Failure to connect to a gateway can occur:

- When attempting to connect to a gateway for the first time
- When attempting to connect to a gateway after already having established a connection but in the interim the gateway’s operation was interrupted due to an electricity surge (for example).

There are three EMS GUI indications as to a first-time connection failure:

1. Notification of the failure to connect appears in the EMS’s Status pane: “*Cannot establish connection*”.
2. One of the following two question marks ? ? is displayed under the Region instead of the gateway icon, shown in the figure 'Failure to Connect to a Media Gateway IP Address', below.
3. When selecting the Region (London, in this example), then in the Status pane under MGs List a question mark appears and **UNKNOWN** appears under the column Product Type.

Five possible reasons for a first-time connection failure are:

1. You’ve incorrectly defined the IP address of the media gateway you’re attempting to connect to (in the MG Information screen; refer to the figure 'Incorrectly Defined MG Information Screen', below)
2. An operational problem exists in the system (lack of communication with the server, for example).
3. A network problem prevents the EMS server from connecting to the media gateway. Ping the Media Gateway’s IP address to verify that it exists.
4. The community string is incorrect.
5. Unrecognized software version.

The table below summarizes possible first-time connection problem scenarios, the verification test that operators should perform in each scenario, and how to fix the problem.

Table 18-1: Possible First-Time Connection Problems: How to Verify Them, How to Fix Them

Possible Problem	How to Verify It	How to Fix It
Wrong Media Gateway IP Address defined in EMS	In the MG Tree, right-click on the gateway and choose option 'Details'; verify that the gateway IP address is correct.	▪ Delete the gateway (right-click the question-mark icon and choose the option 'Remove MG'). ▪ Add a new gateway (refer to Adding a Single Media Gateway). Define the MG Information fields ensuring that the IP address for the gateway you're attempting to add (connect to for the first time) is the correct one, and that all other fields are correctly defined.
Wrong MG SNMP Read Community String defined in the EMS	In the MG Tree, right-click on the gateway and choose option 'Details'; verify that the SNMP Read and Write Community Strings are defined correctly.	Note that the factory default values for SNMP community strings are: read=public, write=private. Contact your system integrator to verify correct values.
The Media Gateway is not connected to the Network	In the cmd window (Start > Run), ping the gateway to verify that it is responding.	If the gateway isn't responding to the ping, check if there is a network problem or if the gateway is not operating.
The Media Gateway version is not defined in the EMS Software Manager	A message notifying you that the current gateway version is not supported by the EMS will be displayed in the status screen.	Operators can either add the missing software version to the Software Manager or load the software to the gateway of one of the EMS- supported versions.
The Media Gateway type is not supported by the EMS	In the 'MGs List' pane, an entry under the Product Type column is identified as UNKNOWN_XXX (where XXX is the product description returned by the gateway).	Contact Customer Support.

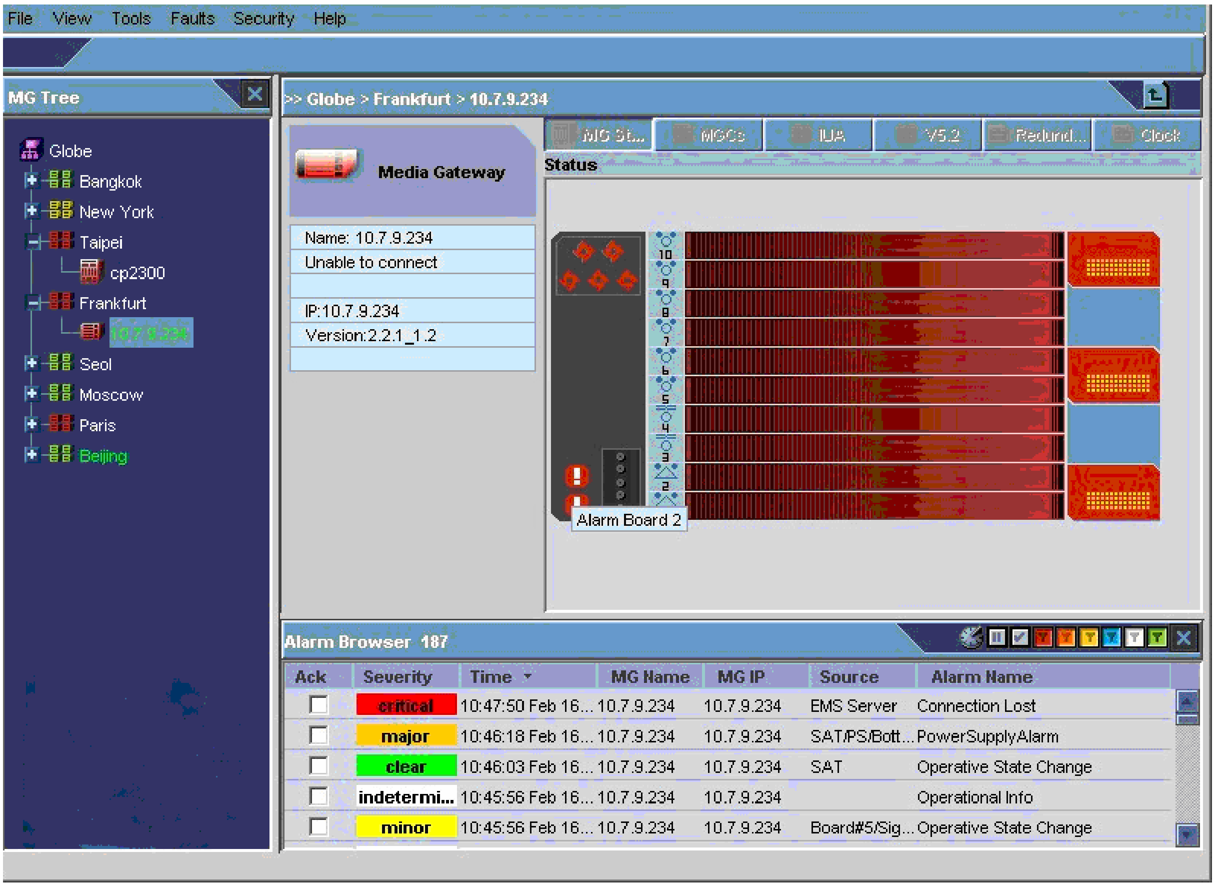
18.1.1 Failure to Reconnect to a Previously-Connected MG Whose Operation Was Interrupted

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

1. A red icon of a gateway is displayed under the Region and in the Status pane (when the Region is selected).
2. A media gateway color-coded red is displayed in the Status pane (after double-clicking the icon color-coded red in the MGs List).

3. The Status pane’s navigation buttons are disabled, shown in the figure below.

Figure 18-1: Failure to Reconnect to a Media Gateway Whose Operation was Interrupted



Name: 10.7.9.234
Unable to connect

IP:10.7.9.234
Version:2.2.1_1.2

Ack	Severity	Time	MG Name	MG IP	Source	Alarm Name
□	critical	10:47:50 Feb 16...	10.7.9.234	10.7.9.234	EMS Server	Connection Lost
□	major	10:46:18 Feb 16...	10.7.9.234	10.7.9.234	SAT/PS/Bott...	PowerSupplyAlarm
□	clear	10:46:03 Feb 16...	10.7.9.234	10.7.9.234	SAT	Operative State Change
□	indetermi...	10:45:56 Feb 16...	10.7.9.234	10.7.9.234		Operational Info
□	minor	10:45:56 Feb 16...	10.7.9.234	10.7.9.234	Board#5/Sig...	Operative State Change

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 18-2: Possible Reconnection Problems: How to Verify Them, How to Fix Them

Possible Problem	How to Verify It	How to Fix It
Network Problems	Network problems can occasionally interrupt valid and quick EMS Client / EMS Server / Media Gateway communication.	Refresh by pressing F5 or View > Refresh. If the EMS cannot reestablish connection with the media gateway, ping the media gateway from the EMS client or EMS server.
Invalid modification of Community Strings	If you changed the Read Community String to an invalid value, the EMS will not be able to connect to the media gateway again. (SNMP error 22 – Timeout) will be constantly received.	Verify in the EMS's Users Journal that the media gateway Community Strings were changed. Verify that MG is up and running and you're able to connect it via PING and MIB Browser. Fix the community string problem
MG has failed and is not responding	The media gateway is not responding to ping requests.	Refer to the sections on troubleshooting the media gateway.

Note: A media gateway (that was previously connected but whose operation has been interrupted) is **automatically reconnected** by the system when its operation resumes.

There is no need to attempt to *manually* add a new media gateway, as was the case with a first-time connection failure.

19 Index

Reader's Notes

Originally printed on recycled paper and available on CD or Web site

CERTIFIED QMS
SI
ISO 9001:
2000
THE STANDARDS INSTITUTION OF ISRAEL