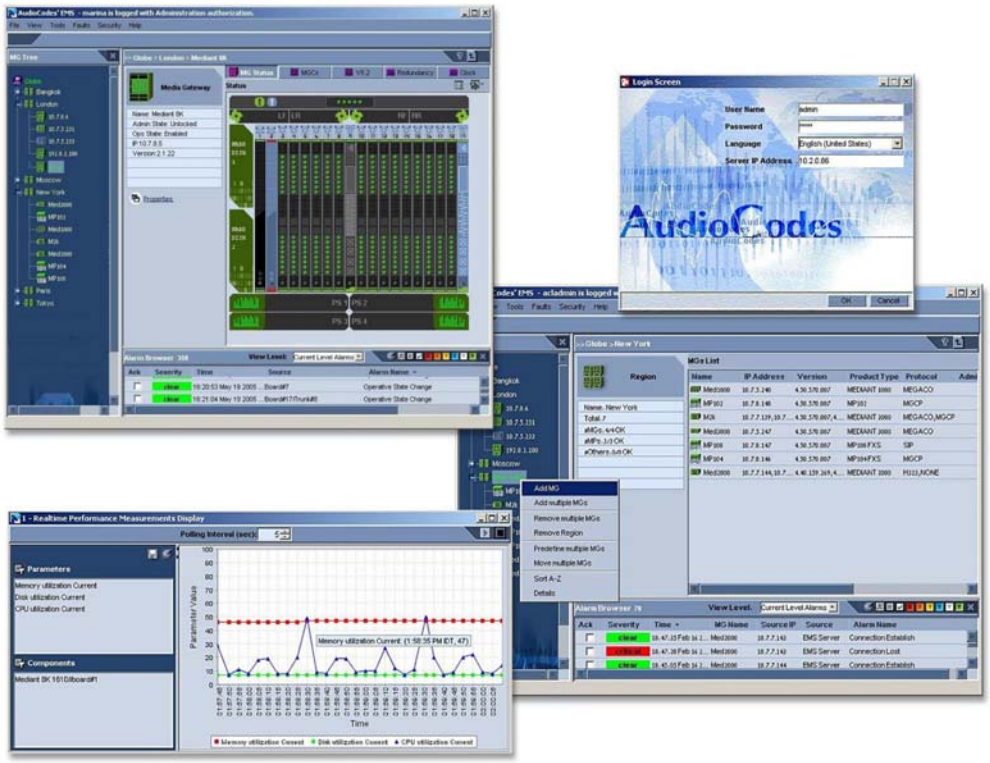
EMS for AudioCodes' Media Gateways and Servers

AudioCodes EMS Element Management System

OAMP (EMS) Integration Guide

Version 5.8

Document #: LTRT- 19207



Notice

In this document, the Avaya G860 Media Gateway corresponds to the Mediant 5000. Note that some features and capabilities contained in this document are not supported by Avaya. Consult your authorized Avaya Sales or Partner resource to confirm the Avaya support features.

AudioCodes

Table of Contents

1 About the AudioCodes Element Management System (EMS) 7

2 OAMP Integration Concepts 9

2.1 Overview 9
2.2 Client (GUI) Integration 12
2.2.1 JAWS URL Browsing 12
2.2.2 Command Line Interface – CLI Northbound Interface 14
2.2.2.1 Enabling Log-in from an NMS Client to a Single EMS Client 15
2.2.3 JAVA EMS API Northbound Interface 17
2.3 EMS Server Access 17
2.4 Topology File 19
2.5 Faults (Alarms & Events) 21
2.5.1 Alarms and Events Reception in the NMS 21
2.5.1.1 Option #1: MG and EMS alarms forwarding by the EMS application 22
2.5.1.2 Option #2: Each Network Element sends its alarms directly to NMS 24
2.5.2 Alarms Clearing Mechanism 29
2.5.3 Alarms Sequence Numbering 30
2.5.4 Alarms Synchronization via MG SNMP I/F 31
2.6 Status / State Management via MG SNMP I/F 33
2.7 Provisioning and Maintenance Actions 35
2.8 Performance Monitoring 36
2.8.1 Option #1: EMS Server CSV / XML File Format Interface 38
2.8.2 Option #2: Mediant 5000 / 8000 CSV File Format Interface 41
2.8.3 Option #3: Media Gateway SNMP Interface 41
2.9 Security Aspects 43
2.9.1 Centralized EMS Users Authentication and Authorization via Radius Server 44
2.9.1.1 Setting Up the Radius Server 44
2.9.1.2 Provisioning EMS to perform Radius Server Authentication and Authorization 45

3 EMS Private Labeling 47

3.1 Overview 47
3.2 Private Labeling Procedure 47
3.2.1 Creating a New Customer Specific EMS DVD 47
3.2.2 Custom Zip file 48
3.2.2.1 Overview 48
3.2.2.2 Images Folder 48
3.2.2.3 localeProperties Folder – currently not in use 49
3.2.2.4 ProductNames Folder 49
3.2.2.5 Online Help folder 50
3.2.3 EMS Server Full Branding Process 50

4 Appendix A – Private Labeling Icons 55

List of Figures

Figure 2-1: EMS - NMS Integration 11
Figure 2-2: 'Welcome to EMS CLI' Prompt 14
Figure 2-3: Log-in from NMS Client to a single EMS Client: 'Login Successful' in Prompt 15
Figure 2-4: Enabling Log-in from an NMS Client to a Single EMS Client (MGs Tree, Alarm Browser Not Viewed) 15
Figure 2-5: Switching to Another (Single) EMS Client 16
Figure 2-6: Switching to Another (Single) EMS Client 16
Figure 2-7: Choose a Digital Certificate 17
Figure 2-8: NBIF Parent Directory 18
Figure 2-9: NBIF Topology Directory 18
Figure 2-10: Topology File-Excel View 20
Figure 2-11:: Topology File: Notepad View 20
Figure 2-12: Faults (Alarms) 21
Figure 2-13: Traps Forwarding Configuration 22
Figure 2-14: SNMP Trap Forwarding 23
Figure 2-15: Destination Rule Configuration 26
Figure 2-16: Add New SNMPv3 User Dialog 28
Figure 2-17: Performance Monitoring - Intervals 36
Figure 2-18: Performance Monitoring 37
Figure 2-19: Background Monitoring *csv* File 39
Figure 2-20: xml File Header Example 40
Figure 2-21: xml File Data example 40
Figure 2-22: Authentication and Authorization Settings 46
Figure 2-23: Custom Zio File 48

Notice

This guide shows how OAMP (Operation, Administration and Maintenance) is integrated.

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

© 2009 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Sept-23-2009

Note: The EMS supports the following products:

- Mediant 600/1000/2000/3000/5000/8000 Media Gateways.
- IPmedia 2000/3000/5000 Media Servers.
- MediaPack Media Gateways MP-102 (FXS), MP-104 (FXS and FXO), MP-108 (FXS and FXO), MP-112 (FXS), MP-114 (FXS), MP-118 (FXS), MP-124 (FXS) and MP-500 (FXS and FXO) collectively referred to as *MediaPack*.

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

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

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com

Related Documentation

Manual Name
Mediant/IPmedia 5000 / 8000 Media Gateway IO&M Manual
Mediant/IPmedia 5000 / 8000 Media Gateway Release Notes
Mediant 3000 User's Manual
IPmedia 3000 Media Server User's Manual
Mediant 2000 User's Manual
IPmedia 2000 Media Server User's Manual
Mediant 1000 and Mediant 600 User's Manual
MediaPack User's Manual
MP-500 SIP User's Guide
EMS Server IO&M Manual
EMS Product Description
EMS Release Notes
EMS Online Help
Mediant 5000 / 8000 Media Gateway Programmer's User Manual
EMS Parameter Guide for the Mediant 5000 and Mediant 8000 Gateways
EMS Parameter Guide for Digital CPE
EMS Parameter Guide for MediaPack
EMS Alarm Guide

1 About the AudioCodes Element Management System (EMS)

The EMS is an advanced solution for standards-based management of Media Gateways within VoP networks, covering all areas that are vital for the efficient operation, administration, management and provisioning (OAMP&P) of the AudioCodes' family of Media Gateways/Servers, namely, the digital Mediant Series VoIP Media Gateways/Servers and the analog MediaPack Series VoIP Media Gateways.

Note: References in this document to Media Gateways also refers to Media Servers.

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

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

AudioCodes EMS provides a full control and management solution for all the AudioCodes analog and digital Media Gateways and Media Servers.

The current document describes two integral features of OEM Customization:

- How to integrate the product management into existing management architecture (NMS/OSS)
- How to perform product private labeling

Reader's Notes

2 OAMP Integration Concepts

2.1 Overview

The main purpose of the EMS is to provide an easy-to-use human interface to provision and maintain AudioCodes' Media Gateways. The EMS is implemented in a way that protects Media Gateways as much as possible from human errors. This is essential for the maintainance of a highly available solution. Development of the EMS is closely correlated with development of the Media Gateways. Every new Media Gateway software version requires that the EMS is correspondingly updated. Using the EMS allows customers to upgrade the software in the Media Gateways as soon it becomes available, without waiting for development on the management system.

In summary, the EMS is in AudioCodes' assessment the best tool to manage AudioCodes Media Gateways. It does not, however, replace NMS and OSS management systems which show operators a comprehensive view of the network (including other vendors' equipment). After defining and first-time provisioning a Media Gateway via the EMS, operators will usually work with an NMS / OSS for day-to-day maintenance. Only when problems occur with a Media Gateway or when provisioning or maintenance tasks must be performed, will operators open the EMS and work directly with it. Therefore, we developed and described in the document below, the proposed APIs for Single Login, Faults (alarms), Performance Monitoring and Security Intergation with a higher level management system.

Figure 2-1 on page 11 shows how the EMS Client (a Windows™ based Java™ 1.6 application running on the operator's PC) and EMS Server (running on a dedicated Sun™ based or Linux based server machine on a Solaris™ 10, or CentOS 5 operating system and utilizing an Oracle™ 11g Standard Edition Database) are integrated with a Network Management System (NMS)[1]. The EMS Client implements a EMS CLI API northbound interface which enables an NMS Client station to browse an EMS Client GUI in a Media Gateway/server context.

Single login: To enable a single login between the NMS and EMS applications, the EMS Client should be installed together with the NMS Client on the same machine. Thereafter, the NMS application can launch the EMS Client application when the operator runs file **cli.exe** that is located in the EMS Client installation directory; in the EMS CLI API (Command Line Interface), the EMS Client login definitions are set (refer to Command Line Interface – CLI Northbound Interface on page 14 more information).

The **EMS Topology** file includes a snapshot of all the GATEWAYs defined in EMS application. It can be found on the EMS server and is available for the higher level management system.**For more information, see** Topology File **on page 19.**

Faults are sent from Media Gateways / servers and EMS as SNMP notifications (traps). These traps can be either:

1. Forwarded by the EMS application to the NMS Server (for all the network elements and the EMS itself).
2. Sent by each one of the network elements directly to the NMS Server. In this case, there is the possibility to enable EMS Alarms .For example, ,when a connection between the EMS Server and a Media Gateway is established or lost, traps are forwarded to the NMS Server machine.

Status: The status of a Gateway can be attained based on the set of supported IETF Management Information Base (MIB-II) tables, described in Section 2.6, Status / State Management via MG SNMP I/F, on page 33.

[1] The same applies to a higher-level OSS (Operations Support System).

Performance Monitoring (PM) data and statistics can be made available to the NMS either:

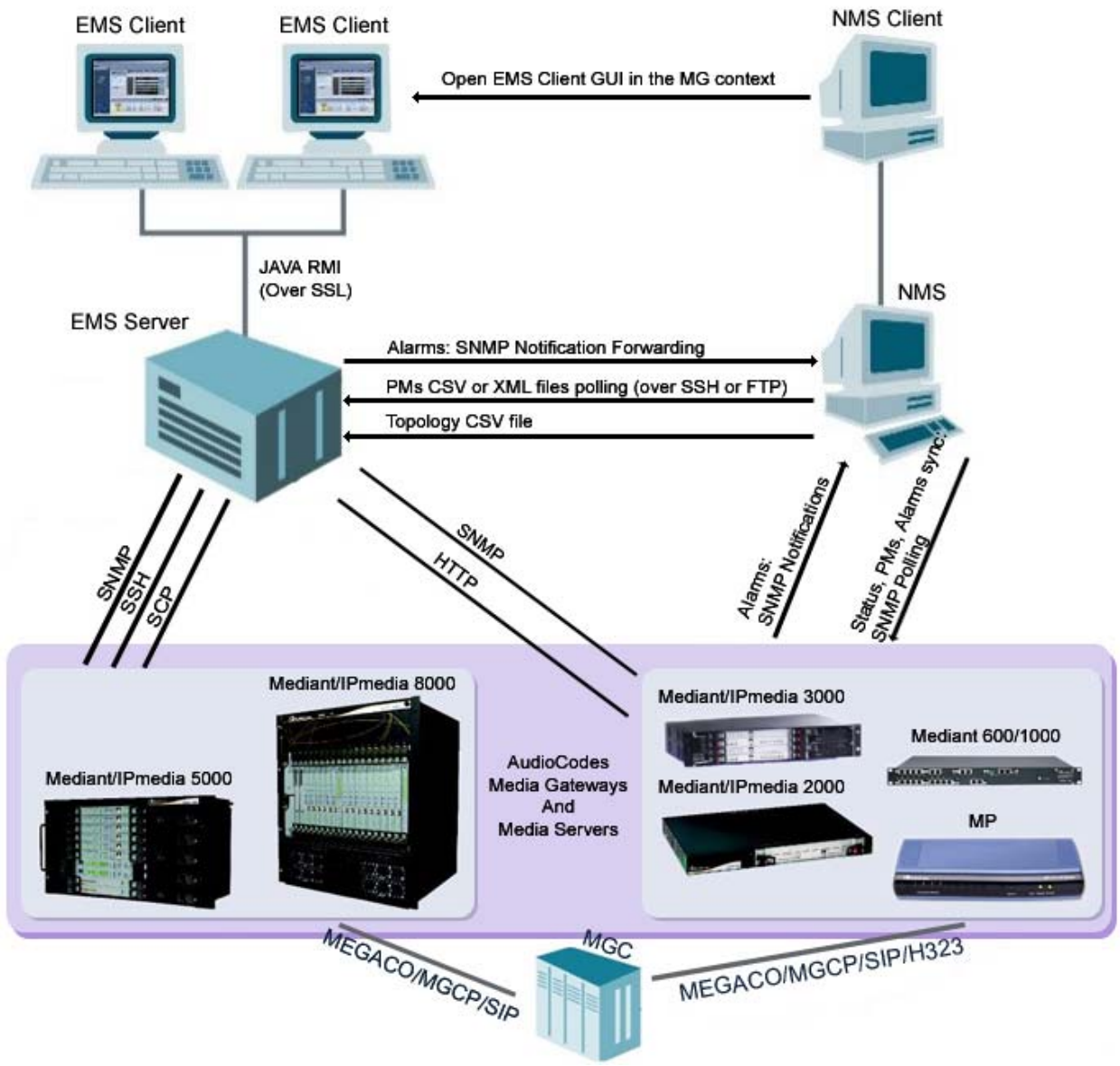
- Through collection of csv or xml files fom the EMS server machine via FTP or SFTP. EMS will perform SNMP polling of the network elements and create a summary file per element per collection interval.
- By collecting information directly from the network element via the SNMP interface.

Security:

1. EMS Users Management (Authentication and Authorization): locally in the EMS database, or via a centralized Radius Server.
2. Network Communication Protocols
   - EMS Client-Server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). EMS also enables Client installation and launching via JAWS running over HTTPS.
   - The connection between the EMS Server and the Gateway can be secured as follows:
     - Mediant 5000 / 8000:
       - SNMPv3 for Provisioning, Maintenance Action, Faults and Performance Monitoring
       - SSH and SCP for File transfer and Online Sotwware Upgrade
       - IPsec IKE pre-shared key for other communication (such as NTP)
     - Mediant 1000 /2000 /3000 and MPs:
       - SNMPv3 for Provisioning, Maintenance Action, Faults and Performance Monitoring
       - HTTPS for File transfer and Online Sotware Upgrade
       - IPsec IKE pre-shared key for other communication (like NTP)

The connection between the EMS Server and the NMS server can optionally be secured over IPsec with an IKE pre-shared key. In addition, SSH and SFTP are suggested to be used.

Figure 2-1: EMS - NMS Integration



2.2 Client (GUI) Integration

The EMS Client is a Java™ application running on a Windows™ operating system. It can be installed on the Desktop either from DVD, or via Web interface by running Java Web Start (JAWS) from the EMS servr machine.

Use one of the following options to perform integration for the purpose of a single login:

1. JAWS URL browsing with appropriate parameters
2. Command Line Interface – CLI (applicable for Desktop Clients integration)
3. JAVA EMS API Northbound Interface

All the above options can be run together with other management systems clients such as an NMS / OSS. In this way, the NMS /OSS can pop up the EMS Client when the AudioCodes Media Gateway icon is pressed. This allows operators to browse through the various management systems without moving from their desks.

The drill-down feature is possible through popping up the EMS Client. All the above three options provide the following additional features:

- **Single login**: When opening the EMS Client, the login screen is skipped if the user name and password are provided through the CLI.
- **Select the Media Gateway/media server**: If switch **–I** is defined in the CLI, the status screen of that specific Media Gateway / media server (whose IP address was defined) will display in the EMS Client GUI on opening.
- **Enable / disable navigation tree**: If a specific operator is not allowed to view any other Media Gateways, the navigation tree can be hidden so that they'll not be able to move to other Media Gateways.
- **Enable / disable active alarms browser view**: The active alarms pane can be hidden from the EMS screen, which forces operators to choose the NMS / OSS alarm browser.

2.2.1 JAWS URL Browsing

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

- https://<server_ip>/jaws - it will open a regular 'EMS Login Screen'.

  For example:
  `http://10.7.6.18/jaws/`

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

  For example:
  `http://10.7.6.18/jaws/?username=acladmin&password=pass_12345`

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

Supported arguments are as follows:

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

For example:

```
http://10.7.6.18/jaws/?username=acladmin&password=pass 12345&challe
nge=nomatter&showtree=false&showalarmbrowser=false&nodeip=10.7.5.20
1
```

2.2.2 Command Line Interface – CLI Northbound Interface

The EMS features a EMS CLI API Northbound Interface (Command Line Interface) that enable 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).

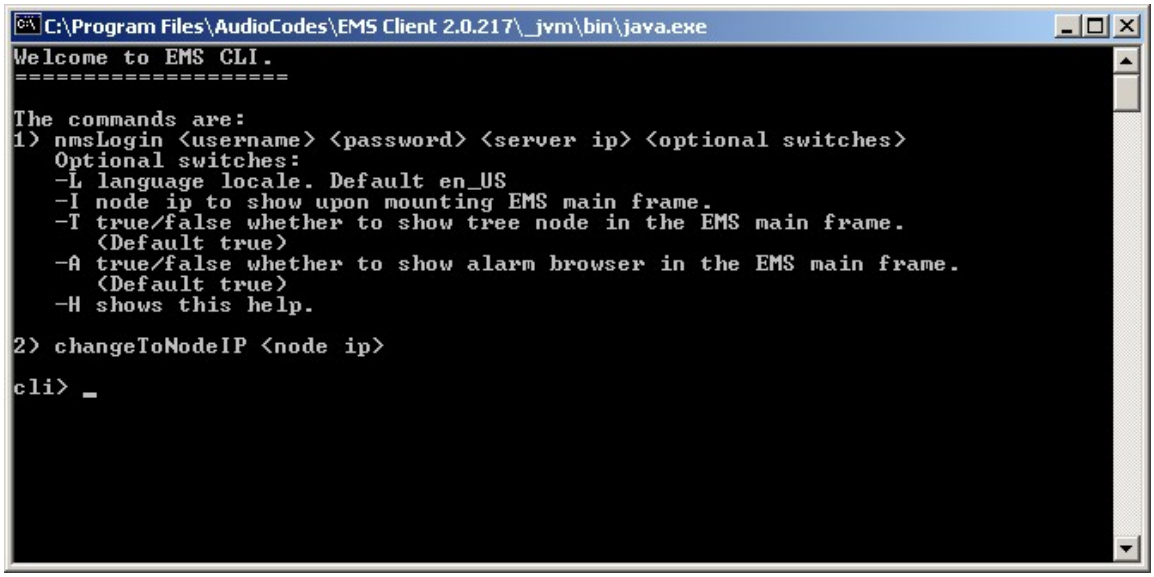
The folder 'Nbif' includes two important files:

- nbif.jar (this file is the EMS CLI Northbound Interface; refer to 'EMS CLI Northbound Interface' on page 17)
- NbIf.html (this file includes API information that programmers should know in order to connect to the CLI).

➢ **To run the CLI:**

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

Figure 2-2: 'Welcome to EMS CLI' Prompt



The following commands can be added in the EMS CLI:

EMS CLI Switch	Description
-L	Language locale. Default en_US
-I	Node IP to display 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
-H	Shows this help

2.2.2.1 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 displayed in the 'Welcome to EMS CLI' prompt (refer to' Command Line Interface (CLI)' on page 17, 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 refers to the Media Gateway with IP address 10.7.8.150. Its MGs Tree and Alarm Browser cannot be displayed:

Figure 2-3: Log-in from NMS Client to a single EMS Client: 'Login Successful' in Prompt

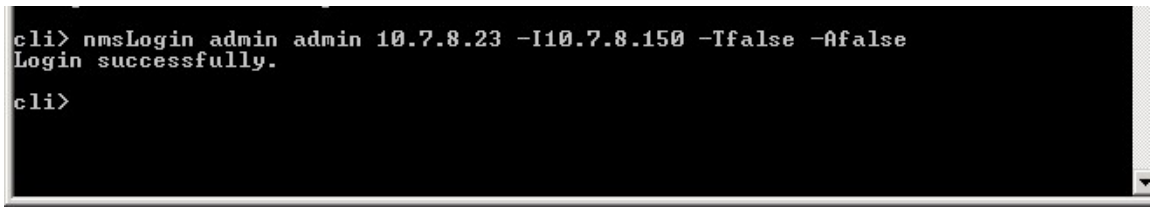
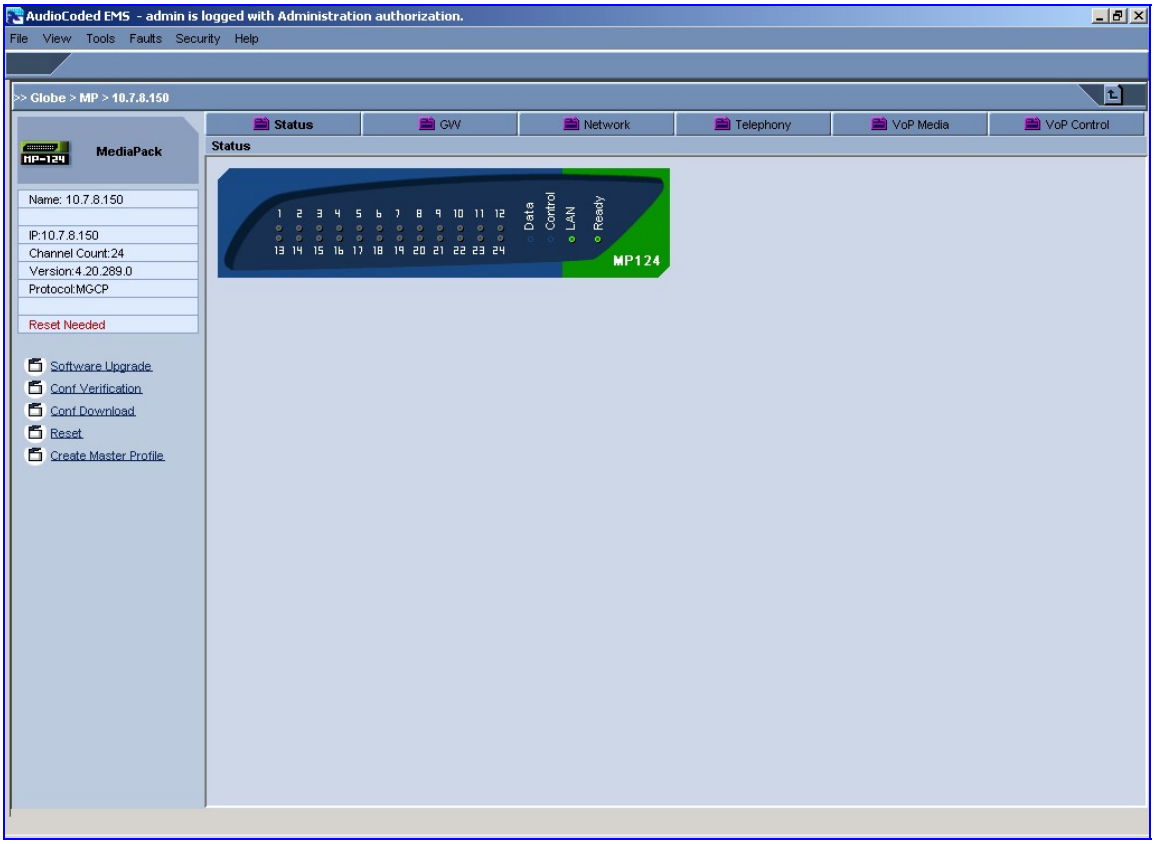


Figure 2-4: Enabling Log-in from an NMS Client to a Single EMS Client (MGs Tree, Alarm Browser Not Viewed)



➢ To switch to another (single) EMS Client:

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

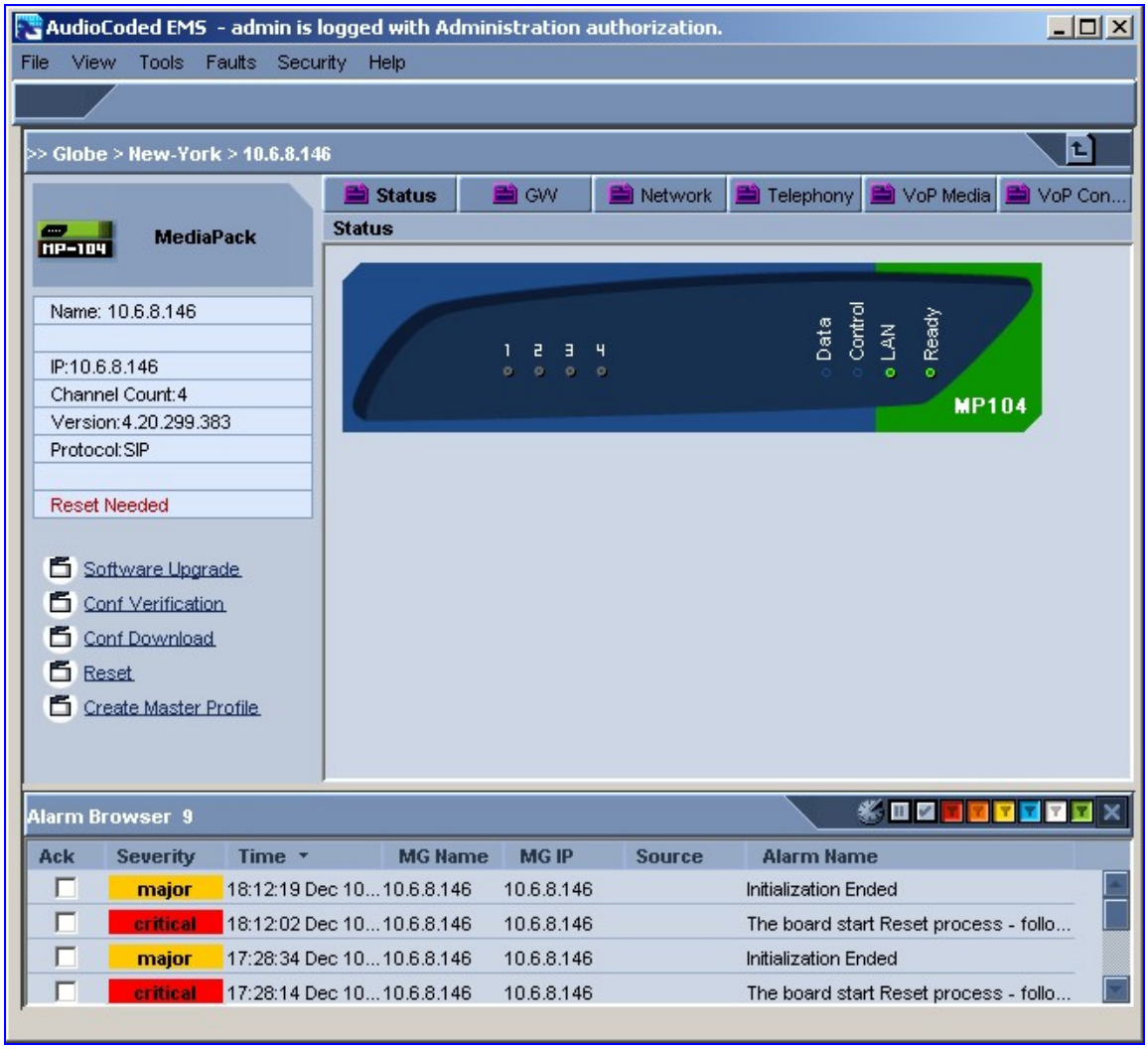
   `(Example: cli> changeToNodeIP 10.6.8.146)`

Figure 2-5: Switching to Another (Single) EMS Client

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

2. Press **Enter;** the command is executed and the EMS switches to the Media Gateway with the IP address 10.6.8.146 (refer to the figure below).

Figure 2-6: Switching to Another (Single) EMS Client



2.2.3 JAVA EMS API Northbound Interface

The following .jar files should be added to your Java™ application:

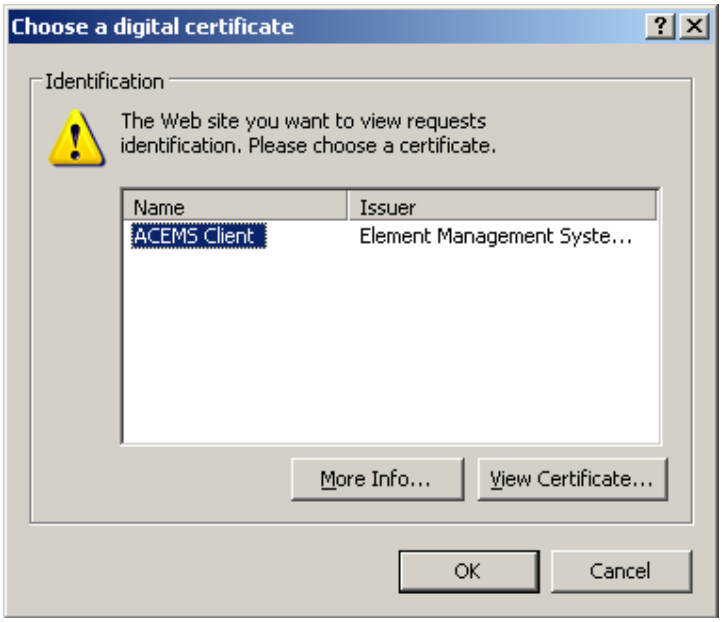
- nbif.jar (Nbif folder)
- client.jar
- jbcl.jar
- Externals (client installation folder)

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

2.3 EMS Server Access

All EMS and Gateway information available for the NMS and other North Bound interfaces including Topology, Performance and Backup data is located in the EMS server machine under the folder **/ACEMS/NBIF**. This folder can be accessed using HTTPS browsing by entering the URL https://<EMS Server IP>/NBIF in your Web Browser. Note, that the customer's Web Browser should have the appropriate X.509 certificates signed by the same Certificate Authority (CA) as the EMS Server Web browser certificates. Choose the appropriate certificate, and press OK.

Figure 2-7: Choose a Digital Certificate



The NBIF folder content opens. Double click each one of the folders to list it's contents. Double click each one of the files to open it.

Figure 2-8: NBIF Parent Directory

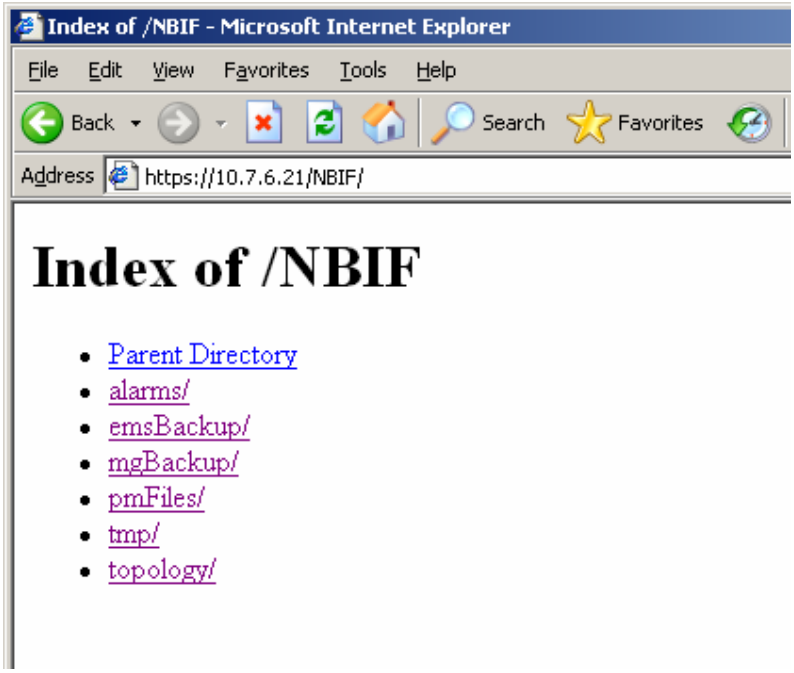
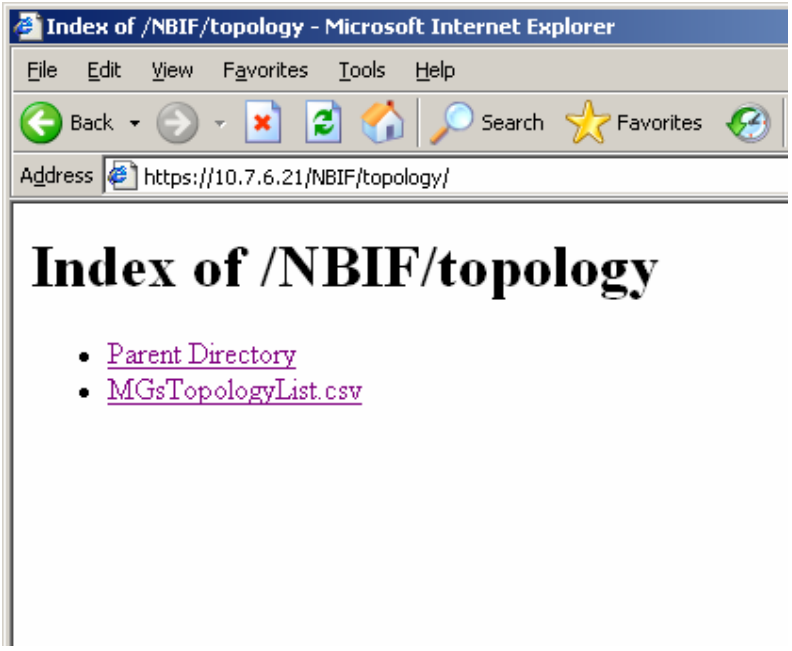


Figure 2-9: NBIF Topology Directory



For the procedure for creating and updating Web server certificates, refer to the EMS server IOM Guide.

EMS provides the following information in the NBIF folder:

- A Summary file of all the Gateways and their basic properties defined in the EMS application. The summary file is located under the 'topology' folder and is always named **MGsTopologyList**. For more information on this file, refer to section Topology File on page 19.

- Performance Monitoring files collected by EMS for all the defined and provisioned Gateways. Files are stored under the 'pmFiles' folder. For more information regarding the file naming convention, file structure and file management policy in this folder, refer to section Performance Monitoring on page 36.

- EMS Server, Mediant / IPmedia 5000 & 8000 backup files could be collected from the 'emsBackup' and 'mgBackup' folders. These files are usually collected via a cenral backup tool.

- Alarms query result is located under the 'alarms' folder when the EMS user performed the 'Faults->Save Alarms As alarms action in the client and the action result displayed more than 1500 records. This file is created for local user requests and should not be collected by higher level management or backup systems.

2.4 Topology File

A Topology file is created and maintained by the EMS application. This file includes updated information regarding managed Gateways and their availability on the EMS server machine. It is used by the NMS system to synchronize the list of MGs that are currently managed by the EMS for the purposes of Alarms Forwarding and Performance Management integration. For example, if a specific Media Gateway has not been receiving alarms, then you can verify in the topology file whether the relevant Gateway is displayed in the list of connected Gateways. In addition, if you are monitoring performance of a specific Gateway, you can verify in the topology file whether the Gateway is currently being polled.

The Topology file is automatically updated upon the addition /removal of a Media Gateway or upon updates to the Media Gateway properties such as name, IP address or region modification. It is also updated upon Performance Monitoring pollings status changes. The EMS informs about the definition or update of a Media Gateway by sending a **acEMSTopologyUpdateEvent** (Topology Update), and about a topology file update by sending a **acEMSTopologyFileEvent** (Topology File Generated). These events are displayed in the EMS Alarm Browser and in the NMS Alarm Browser when the "EMS Events Forwarding" checkbox is selected in the Trap Configuration "Destination Rule Configuration" dialog.

When multiple Gateways are added, the Topology file is updated approximately once per minute as the entire operation may take more than a few minutes. For more information regarding the exact event fields, refer to the relevant Media Gateway OAMP Guide – Alarms Chapter.

The Topology file **MGsTopologyList.csv** is saved in the CSV format and is located under the **ACEMS/NBIF/topology** folder on the EMS server machine. The file can be retrieved via the FTP or SFTP protocol, or read via Telnet or SSH using **nbif** user. The file header is composed of two lines commencing with ";" : file format version, and column names. Each row in the file represents a Media Gateway in the EMS tree and includes the following information:

- **Serial Number** (optional) for Mediant 5000 / 8000 Gateways will always be empty

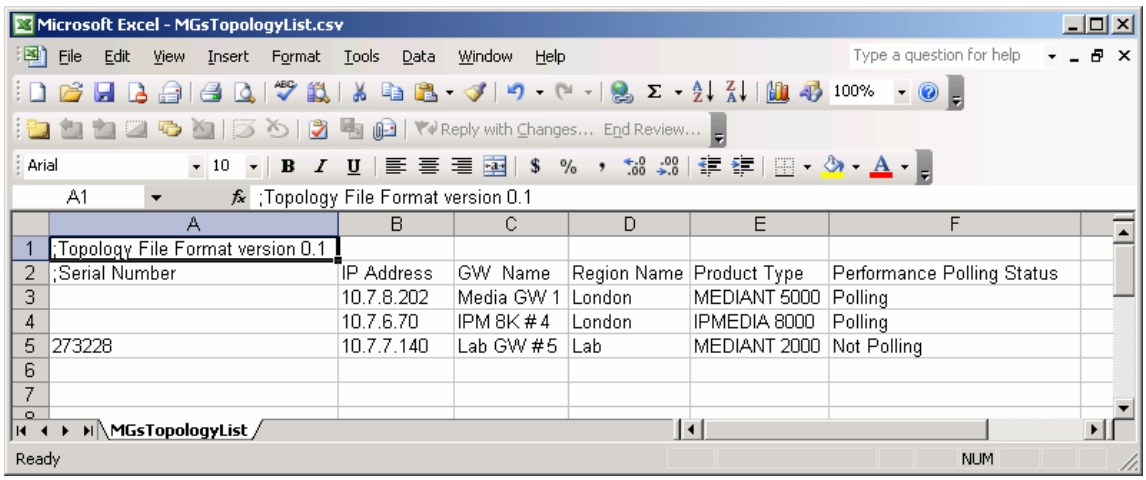
- **IP Address** – as provisioned by User or auto detected

- **GATEWAY Name** – as it appears in the EMS Tree

- **Region Name** - as it appears in the EMS Tree
- **Product Type** – Mediant 600 / 1000 / 2000 / 3000 / 5000 / 8000 or MP
- **Performance Polling Status** – is EMS currently collecting (Polling) or not GATEWAY history performance monitoring data.

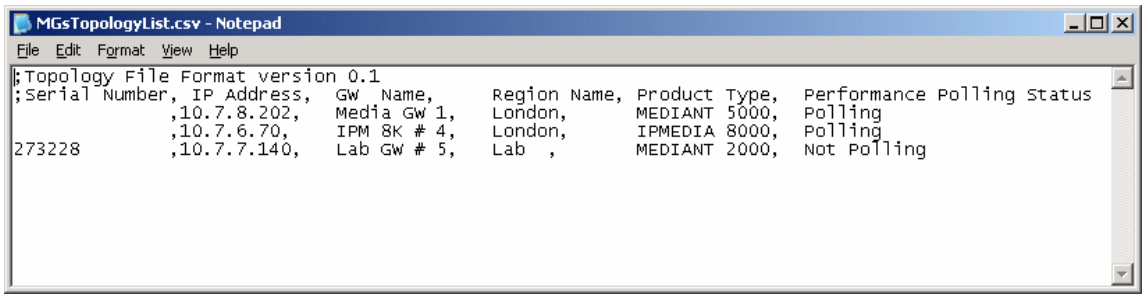
Below are examples of Excel and Notepad file views:

Figure 2-10: Topology File-Excel View



	A	B	C	D	E	F
1	;Topology File Format version 0.1					
2	;Serial Number	IP Address	GW Name	Region Name	Product Type	Performance Polling Status
3		10.7.8.202	Media GW 1	London	MEDIANT 5000	Polling
4		10.7.6.70	IPM 8K # 4	London	IPMEDIA 8000	Polling
5	273228	10.7.7.140	Lab GW # 5	Lab	MEDIANT 2000	Not Polling
6						
7						

Figure 2-11:: Topology File: Notepad View



Note: EMS Media Gateway report files can also be exported from the EMS application using the 'File -> MGs Report' command. This file contains more information than the Topology report on the EMS server machine. The detailed file description can be found in the EMS User Manual document.

Both reports, received from the EMS Client or the EMS server can be imported using the 'Add multiple MGs' command from the EMS Tree Region right click option.

2.5 Faults (Alarms & Events)

The Media Gateway reports its faults (alarms and events) and state changes (Administrative / Operative state) via SNMP Notification traps. Both standard and proprietary traps are supported. Audiocodes proprietary traps have the same variable bindings set. Each alarm includes information required by the ITU-T X.733 standard. Operative and Administrative states are managed according to the ITU-T X.731 standard. The Alarms section in each one of the product OAMP Guides define the exact list of standard, MG proprietary and EMS proprietary traps supported for each one of the Gateways. Each one of the traps includes information whether its defined as an alarm or an event.

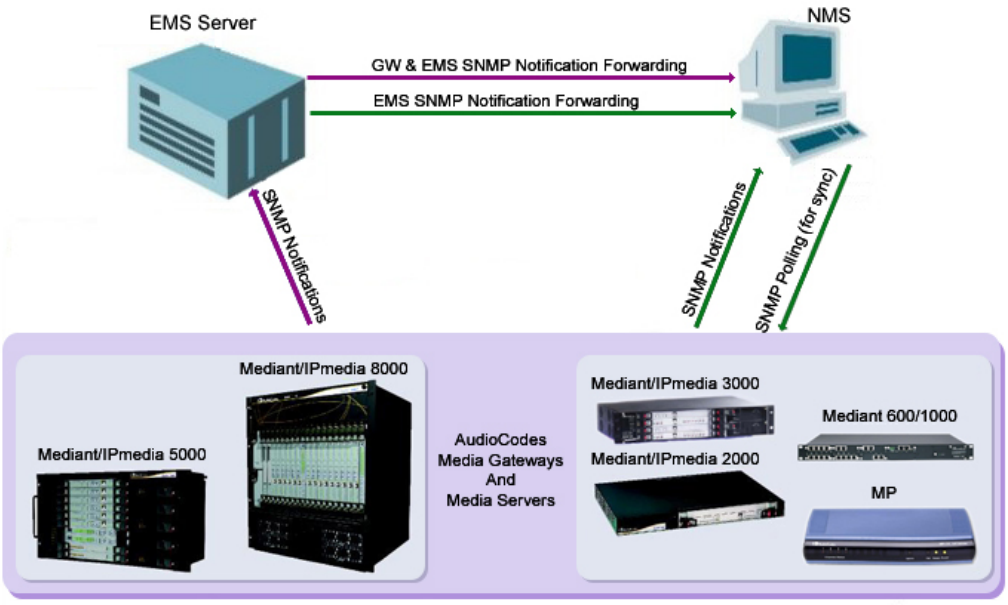
2.5.1 Alarms and Events Reception in the NMS

Media Gateway alarms can be forwarded to the NMS using one of the following methods:

- MGs and EMS Alarms forwarding is performed by the EMS application to the NMS (purple-colored path in the figure below).
- Each one of the Network Elements (MGs and EMS) sends it's own alarms directly to the NMS. The MG is capable of sending alarms to two destinations: EMS and NMS. Each destination can be configured with a different trap port. The Gateway supports issuing alarms to up to three destinations. EMS can be configured to perform alarms forwarding only for EMS alarms (green–colored path in the figure below) and not for MG alarms.

Note: All the alarms and events issues by MGs are send as SNMP Notifications. EMS can forward alarms and events in the following formats: SNMP Notifications, SMS, Mail, Syslog. In the section below, the SNMP Notifications forwarding is described as suggested for EMS – NMS integration.

Figure 2-12: Faults (Alarms)



To receive alarms in the NMS, perform appropriate provisioning of the EMS and MGs as follows:

2.5.1.1 Option #1: MG and EMS alarms forwarding by the EMS application

➢ **To forward alarms from the EMS application:**

1. Open the Faults->Trap configuration menu. The **Destination Rule Configuration** dialog is displayed.

2. In the Actions menu, select **Add Destination** or click "+" in the menu bar.

3. Set the Destination Type to **SNMP**.

4. In the left-hand pane, provision the following parameters:

   - **Destination Rule Name** as you wish it to appear in the summary screen.

   - Select the subset of alarms and events that should be forwarded to the NMS from the following subset (by default, all the alarms and events are selected):

     - EMS Alarms Forwarding

     - EMS Events Forwarding

     - MGW Alarms Forwarding

     - MGW Events Forwarding

   - **Severities To Forward** – select the subset of severeties that you wish to receive in the NMS application (by default, all the severeties are selected). Note: CLEAR alarms for selected subset of the alarms are always forwarded.

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

5. In the right-hand pane, provision the following parameters:

   - In the **Destination Host IP Address** field, enter the NMS IP address.

   - In the **Destination Host port** field, enter the port number of the destination host (the default SNMP port for trap reception is 162).

Figure 2-13: Traps Forwarding Configuration

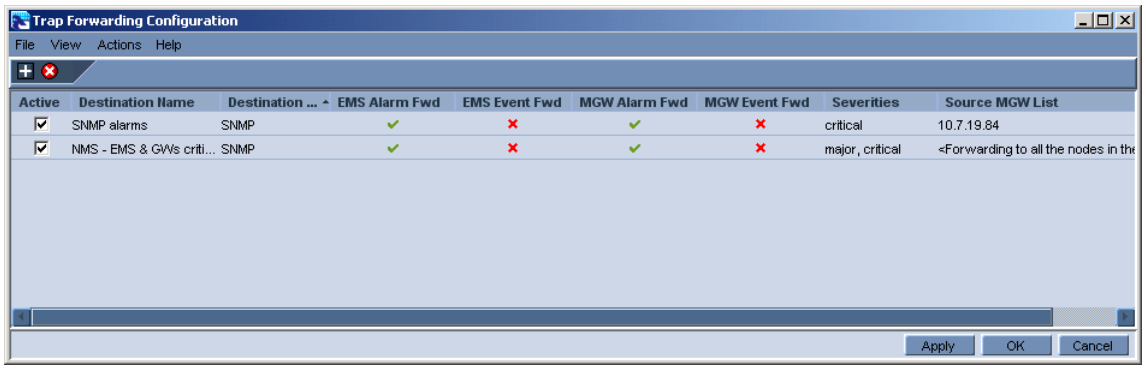
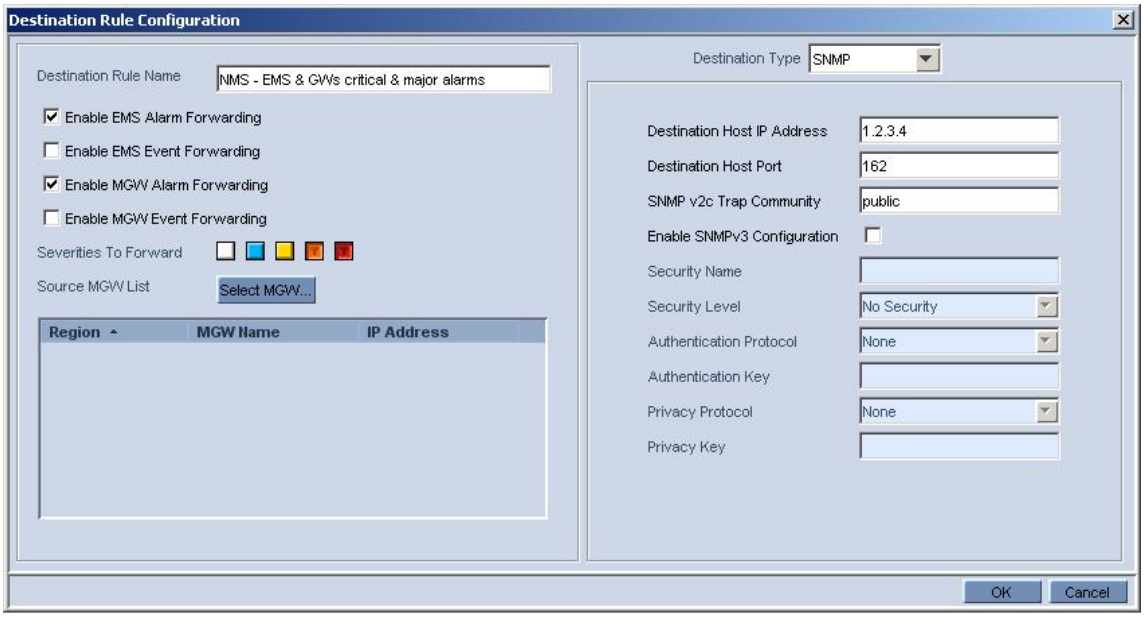


Figure 2-14: SNMP Trap Forwarding



Note: EMS issues SNMPv2c traps with the field SNMPv2c Trap Community set to “public”.

6. **(Optional)** check the **Enable SNMPv3 Configuration** box to enable forwarding traps to the NMS using SNMPv3. In this case, set the following additional fields:

   - In the **Security Name** field, enter the Security name of the SNMPv3 user.
   - In the **Authentication Protocol** field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the **Security Level** field.
   - In the **New Authentication Password** field, enter a new Authentication Password.
   - In the **Privacy Protocol** field, select a Privacy Protocol from the drop-down list box.
   - In the **New Privacy Password** field, enter a new Privacy Password.

7. Click **OK**.

Note: During the EMS synchronization with the managed Gateways, it might recover missed alarms and retrieve them. As part of the defining alarms in the EMS, missed alarms will be forwarded to the NMS as well. By default, the synchronization process is performed with Gateway alarms history tables. In the event of a failure to retrieve part of whole alarms history, EMS notifies the user with one of the following events: 'Synchronizing Alarms Event' and 'Synchronizing Active Alarms Event'. For more details regarding Events fields and suggested corrective actions, refer to the relevant product OAMP Guide.

2.5.1.2 Option #2: Each Network Element sends its alarms directly to NMS

2.5.1.2.1 EMS Alarms and Events

➢ **To forward alarms and events from the EMS application:**

1. Open the Faults->Trap configuration menu. The **Destination Rule Configuration** dialog is displayed.
2. Select **Add Destination Action** in the Actions Menu or '**+**' in the Menu Bar.
3. Select Destination Type as **SNMP**.
4. On the left hand pane, provision the following parameters:
   - **Destination Rule Name** as you wish it to appear in the summary screen.
   - Select the subset of alarms and events that should be forwarded to the NMS from the following subset (by default, all the alarms and events are selected):
     - Enable EMS Alarm Forwarding
     - Enable EMS Event Forwarding
   - Ensure that MGATEWAY alarms and events checkboxes are not selected:
     - De-select Enable MGATEWAY Alarms Forwarding
     - De-select Enable MGATEWAY Events Forwarding
   - **Severities To Forward** – select the subset of severeties that you wish to receive in the NMS application (by default, all the severeties are selected). Note: CLEAR alarms for selected subset of the alarms are always forwarded.
   - Select the Media Gateways from which you wish to forward alarms and events.
5. In the right-hand pane, provision the following parameters:
   - In the **Destination Host IP Address** field, enter the NMS IP address.
   - In the **Destination Host port** field, enter the port number of the destination host (the default SNMP port for trap reception is 162).

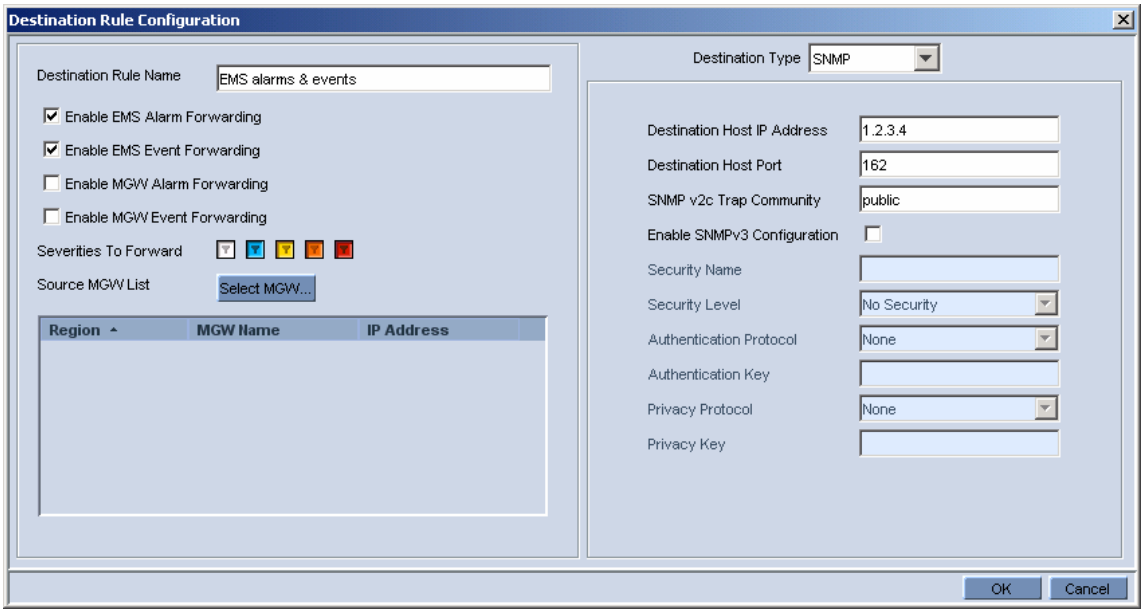
Note: EMS issues SNMPv2c traps with the field SNMPv2c Trap Community set to "public".

6. You can optionally check the **Enable SNMPv3 Configuration** box to enable forwarding traps to the NMS using SNMPv3. In this case, set the following additional fields:

   - In the **Security Name** field, enter the Security name of the SNMPv3 user.
   - In the **Authentication Protocol** field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the **Security Level** field.
   - In the **New Authentication Password** field, enter a new Authentication Password.
   - In the **Privacy Protocol** field, select a Privacy Protocol from the drop-down list box.
   - In the **New Privacy Password** field, enter a new Privacy Password.

7. Click **OK**.

Figure 2-15: Destination Rule Configuration



2.5.1.2.2 Issuing Mediant 5000 / 8000 Alarms/Events to an NMS

- **SNMPv2 Traps**

  In case you wish the NMS to receive SNMPv2 notifications, open the **MG Provisioning Frame / Network Services tab** and define a new NMS or OSS Trap Destination IP address, port and OAMP security Profile (if you wish to receive traps in SNMPv2c over IPSec protocol-if the Gateway is configured for SNMPv2 traps with IPSec secured.

Note: The Mediant 5000 / 8000 issues SNMPv2c traps with the field **SNMPv2c Trap Community** set to 'public'.

- **SNMPv3 Traps**

  For SNMPv3 Gateways, there is a possibility that the NMS / OSS user will select an SNMPv3 profile that is different to the EMS application defined profile. In this case, the user should perform the procedure below in order to configure as the SNMPv3 user for the Gateway.

➢ **To configure as an SNMPv3 user for the Gateway:**

1. Open the Media Gateway Provisioning Frame / SNMPv3 Users Tab.
2. Select a User Profile you would like to create a user from, by selecting one of the rows in the SNMPV3 Users table. Since new users can only be created from existing users, upon Gateway definition as an SNMPv3 Gateway, the initial templates are created.
3. Press the **+** button, a window asking you to provide old and new passwords opens. The Default password for all the template users are '123456'.

4. Select Manager permission group: **Trap Only, Read & Trap or Read & Write & Trap**
5. Check the 'Enable User as Trap destination and define the NMS / OSS IP and Port for receiving traps. EMS will define this manager to the 'Trap Destinations' tab as an SNMPv3 Trap destination.

2.5.1.2.3 Issuing Mediant 1000 / 2000 / 3000 and MPs Alarms / Events to an NMS

- **SNMPv2 Traps**

  In case the NMS wishes to receive SNMPv2 notifications, open **Network Settings Provisioning Frame / SNMP Managers Table tab**, and define a new NMS or OSS Trap Destination IP address and port. If the Gateway is configured as IPSec secured, SNMPv2 traps will be sent over IPSec protocol.

Note: The Mediant 1000 / 2000 / 3000 and MP issues SNMPv2c traps with the field SNMPv2c Trap Community set to 'trapuser'.

- **SNMPv3 Traps**

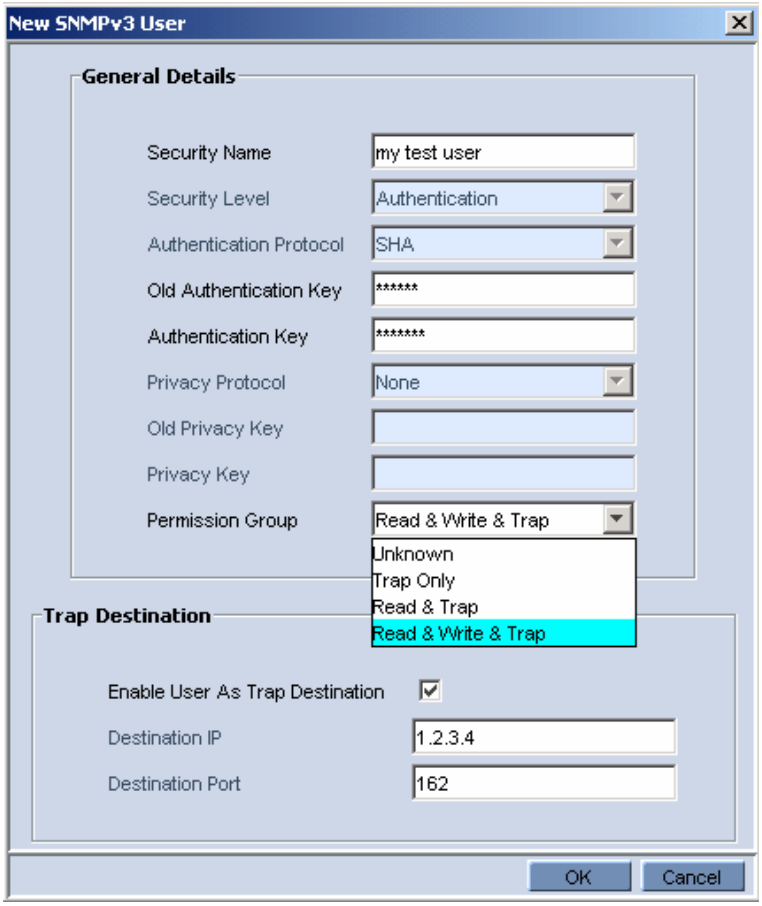
  For SNMPv3 Gateways, there is a possibility that the NMS / OSS user will choose an SNMPv3 profile that is different to the EMS application SNMPv3 profile. In this case, the user should perform the procedure below to configure as an SNMPv3 user for the Gateway.

➢ **To configure as an SNMPv3 user for the Gateway:**

1. Open the Network Settings Provisioning Frame / SNMPv3 Users Tab.
2. Select a User Profile you would like to create a user from by selecting one of the rows in SNMPV3 Users table.
3. Press the **+** button, a window asking to provide old and new passwords opens.
4. Select the Manager permission group: **Trap Only, Read & Trap or Read & Write & Trap**
5. Check the 'Enable User as Trap destination button and define NMS / OSS IP and Port for trap reception. EMS will define this manager in the 'SNMP Managers Table' tab as an SNMPv3 Trap destination.

The figure below is relevant for both Mediant 5000 / 8000 and for Mediant 1000 / 2000 / 3000 and MPs Gateways.

Figure 2-16: Add New SNMPv3 User Dialog



2.5.2 Alarms Clearing Mechanism

All active Alarms and Events for each Media Gateway are cleared upon GATEWAY startup (cold start trap). The active and history alarms tables are emptied.

Critical, Major, Minor, Warning or Info alarms are automatically cleared when a Notification (OID) Clear alarm is generated by the same entity (source) and the same Media Gateway that originally generated the Critical, Major, Minor, Warning or Info alarms.

Media Gateway events are not automatically cleared. When an event becomes redundant, the operator should manually delete it.

Note: There is no aging rule for alarms and events clearing.

2.5.3 Alarms Sequence Numbering

1. When receiving alarms directly from the Media Gateway:

   - Gateway Alarms and Events have a different scala of sequence numbers. These sequence numbers are placed at **TrapGlobalsUniqID** varbindings (respectively **tgTrapGlobalsUniqID**, **acBoardTrapGlobalsUniqID**).

   - EMS Alarms have a sequence number scala. Events are always sent with **acEMSTrapGlobalsUniqID -1**.

2. When EMS is forwarding GATEWAY and EMS alarms:

   - Cold Start Trap is the only standard event that forwarded by EMS application. Rest of the standard Notifications are not forwarded.

   - Each one of the alarms and events are forwarded with the original Notification OID and variable bindings OIDs.

   - The original content of **TrapGlobalsUniqID** varbinding (respectively **tgTrapGlobalsUniqID**, **acBoardTrapGlobalsUniqID** and **acEMSTrapGlobalsUniqID**) is updated as following:

     - For all the forwarded events the **TrapGlobalsUniqID** is set to -1.

     - For all the forwarded GATEWAY alarms and EMS alarms the original **TrapGlobalsUniqID** is replaced with the EMS sequence number, allowing NMS to follow the forwarded alarms sequencing. The original GATEWAY **TrapGlobalsUniqID** is transferred to **TrapGlobalsAdditionalInfo3** varbinding.

     - For all the forwarded alarms and events, **TrapGlobalsAdditionalInfo3** varbinding (respectively **tgTrapGlobals AdditionalInfo3**, **acBoardTrapGlobals AdditionalInfo3** and **acEMSTrapGlobals AdditionalInfo3**) is updated as follows: original GATEWAY IP address and GATEWAY **TrapGlobalsUniqID** in the following format:

       `GATEWAY_IP:x  ,GATEWAY_TRAP_ID:y`

2.5.4 Alarms Synchronization via MG SNMP I/F

Synchronization is supported for alarms and not for events.

A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element management system outages, network outages, and transport mechanism such as SNMP over UDP. This mechanism is implemented in the Media Gateway level SNMP agent, and serves EMS, NMS, or higher level management system synchronization purposes.

Note: The EMS Application does not support carrier-grade alarms synchronization towards NMS in this version.

A carrier-grade alarm system is characterized by the following:

1. Active Alarms

   The device can determine which alarms are currently active in the device by maintaining active alarms table. When an alarm is raised, it is added to the active alarms list. Upon alarm clearing, it will be removed from the active alarms list.

   The maximal size of active alarms table is defined as follows:

   - Mediant 5000 / 8000 and IPMedia 5000 / 8000 Gateways – 1.000 alarms
   - Mediant / IPMedia 3000 – 140 alarms
   - Mediant / IPMedia 2000,– 200 alarms
   - Mediant 1000 – 200 alarms
   - MediaPack - 40 alarms

   When the active alarms list exceeds its maximum size, an enterprise Active Alarms Overflow alarm is sent to the management system.

   The device sends a cold start trap to indicate that it is starting. This allows the management system to synchronize its view of the device's active alarms.

   Two views of active alarms table are supported by the Media Gateways:

   - **Standard MIB**: alarmActiveTable and alarmActiveVariableTable in the IETF ALARM MIB for all the Media Gateways.
   - **Enterprise MIB**:
     - tgActiveAlarmTable in the enterprise TG-ALARM-MIB mib for Mediant 5000 / 8000 and IPMedia 5000 / 8000 Gateways.
     - acActiveAlarmTable in the AC-ALARM-MIB mib for Mediant 1000 / 2000 / 3000, IPMedia 2000 / 3000 and Media Pack products.

2. **History Alarms**

   The device allows recovery of lost alarm raise and clear notifications by maintaining a log history alarms table. Each time an alarm-type trap (raise or clear) is sent, the Carrier-Grade Alarm System will add it to the alarms history list. The trap will contain a unique Sequence Number. Each time a trap is sent, this number is incremented.

The device allows detection of lost alarms and clear notifications by managing alarm sequence number and displaying current number.

The maximal size of history alarms table is defined as follows:

- Mediant 5000 / 8000 and IPMedia 5000 / 8000 Gateways – 10.000 alarms
- Mediant / IPMedia 3000 – 1.000 alarms
- Mediant / IPMedia 2000– 1.000 alarms
- Mediant 1000 – 1.000 alarms
- MediaPack - 100 alarms

When the history alarm list exceeds its maximum size, it will start overiding the oldest alarms in the list in cyclic order.

Two views of log history alarms table are supported by the Media Gateways:

- **Standard MIB**: nlmLogTable and nlmLogVariableTable in the NOTIFICATION-LOG-MIB for all the Media Gateways.
- **Enterprise MIB**:
  - tgAlarmHistoryTable in the enterprise TG-ALARM-MIB mib for Mediant 5000 / 8000 and IPMedia 5000 / 8000 Gateways.
  - acAlarmHistoryTable in the AC-ALARM-MIB mib for Mediant 1000 / 2000 / 3000, IPMedia 2000 / 3000 and Media Pack products.

2.6 Status / State Management via MG SNMP I/F

This subsection applies to Mediant 5000/8000 Media Gateways. For details on the other Media Gateways, refer to the relevant User's Manual ('SNMP' section).

The current status of a Media Gateway and its components (such as VoP boards or PSTN interfaces) can be acquired directly through SNMP. Operative and Administrative states are managed according to the ITU-T X.731 standard for each Managed Object in the Gateway / server.

Both standard and proprietary MIBs are supported. AudioCodes recommends fetching information from the standard MIBs. The following standard MIBs are supported:

- RFC 1450: mib2.system (sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, sysServices)
- RFC 2233: mib-2.interfaces.ifTable is supported for IP external interfaces (following columns are supported: ifDescr, ifType, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus) and mib-2.ifMib.ifMIBObjects.ifXtable – for interfaces mapping (following columns are supported: ifName, ifAlias, ifHighSpeed)
- RFC 1213: mib-2.ip – ipForwarding and ipAddrTable are supported.
- RFC 4133: mib-2.entityMIB – entPhysicalTable (entPhysicalDescr, entPhysicalVendorType, entPhysicalContainedIn, entPhysicalClass, entPhysicalParentRelPos, entPhysicalName, entPhysicalHardwareRev, entPhysicalFirmwareRev, entPhysicalSoftwareRev, entPhysicalSerialNum) and entAliasMappingTable are supported.

When the Media Gateway is defined as an SNMPv2c Gateway, no additional definitions are required. For SNMPv3 Gateways, there is a possibility that the NMS / OSS user will choose an SNMPv3 profile that is different to the EMS application profile. In this case, the user should perform the procedure described in the

Faults (Alarms & Events) chapter on page 21.

2.7 Provisioning and Maintenance Actions

The EMS application is fully responsible for Media Gateway provisioning and maintenance actions, and advanced components status display, including but not limited to the following:

- Overall MG status screen displaying all components
- Managed Objects definition and provisioning
- Administrative actions on the MOs (like lock / unlock, manual switchover / switchback, etc.)
- Regional (auxiliary) files downloading
- Software upgrade / Online Software Upgrade

The EMS features multiple tools to easily and quickly configure a set of Gateways. For example, after one Gateway is configured and operational, its configuration can be saved as a Master Profile and applied with one click to a set of selected Media Gateways of the same type. In the same way, all Gateway maintenance actions such as reset, software upgrade or downloading regional files can be performed with a one-click action to a large set of the selected Gateways.

For detailed information on EMS features, refer to the EMS User's Manual.

2.8 Performance Monitoring

Customers often face a complex VoIP network with little or no information on the status and capacities of each component in the network. PMs help the system architect design a better network. In addition, PMs help operators discover malfunctioning devices before they start causing a problem on the production network.

The system provides two types of performance measurements:

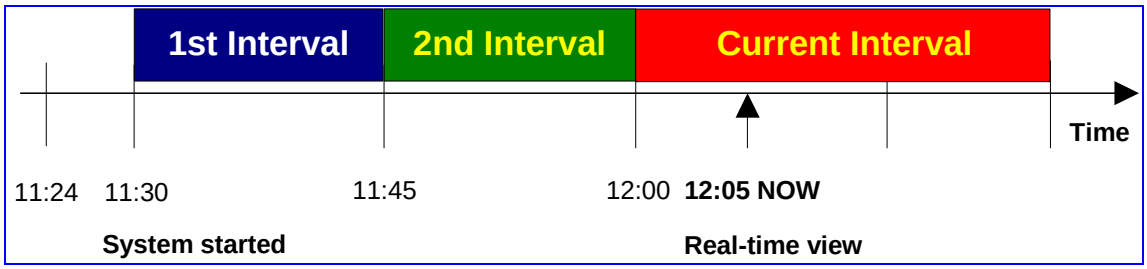
1. **Gauges**: Gauges represent the current state of a PM parameter in the system. Gauges, unlike counters, can decrease in value, and like counters, can increase. For Gauges, the interval data is referred as *minimum*, *maximum* and *average* values.
2. **Counters**: Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the system is reset. The counters are then zeroed. For Counters, the interval data is referred as *last interval value.*

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. The EMS application supports graphical representation of the real-time data and provides the user with graphical tools to perform high-frequency polling of various system parameters. For more information in reference to graph types and application User Interface, refer to the EMS User Manual.

Historical data can be used for long-term network analysis and planning. The rest of the chapter, and all the interfaces mentioned, refer to the historical data collection which is usually the subject of interest for NMS and OSS systems.

Figure 2-17: Performance Monitoring - Intervals



Performance is usually measured in a constant time interval to which all elements are synchronized. Intervals commence on the hour - expiring at 12:00:00, 12:15:00, 12:30:00, 12:45:00, etc. This allows synchronization of several elements in the system to the same interval time frame. Note that the first interval after start-up is always shorter (in the above example, the first interval only lasts 6 minutes - so that a new interval can start at 11:30:00).

Audiocodes equipments support 15-minute intervals for historical performance monitoring data collection.

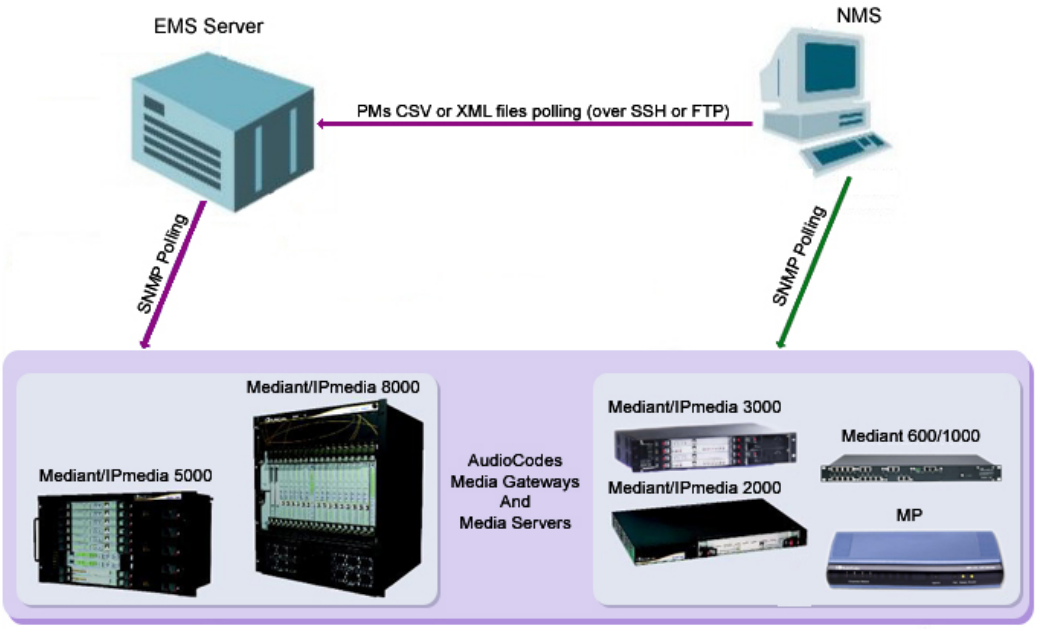
Note: In order to perform accurate history PM polling, all the network elements (MG, EMS, NMS.) must be synchronized on the same NTP server. The EMS Server machine can be defined as an NTP server machine.

There are two ways that the NMS can receive performance monitoring data:

1. By collecting csv or sml files fom the EMS server machine via FTP or SFTP. EMS will perform SNMP polling of the network elements and create a summary file per element per collection interval (purple-colored path in the figure below).

2. By collecting information directly from the network element via SNMP interface (green-colored path in the figure below).

Figure 2-18: Performance Monitoring



2.8.1 Option #1: EMS Server CSV / XML File Format Interface

The EMS stores historical data in the EMS Server database. Additionally, an *xml* or *csv* file can be created per time interval.

The file is created at the end of the PM polling interval in accordance with a user-defined PM profile, and stored in the EMS server under directory 'ACEMS/NBIF/pmFiles'. The EMS keeps PM files for 24 hours (up to 96 files per Gateway). NMS can retrieve the PM file via FTP or SFTP (in the event of EMS server machine hardening). Login as *acems* user to access EMS server machine. Users can choose whether or not to receive a trap when each file is created. The trap name is **acEMSPmFileGenerate (PM File Generated)** . The trap information includes the file name and the time it was created.

Refer to the EMS User Manual, Performance Monitoring section for PM profile configuration (a list of collected parameters), file type, and trap presence. Refer to the specific product OAMP Guide for the exact list of supported performance measurement parameters. The OAMP Guide includes both EMS and SNMP parameter names.

The file name is composed of the Gateway's IP address , interval ending time stamp, and performance data collection period size. For example:

```
'10.7.6.161_Sun_Nov_18_13_00_00_IST_2007_PT15M.xml',
```

where '10.7.6.161' is Gateway IP address, 'Sun_Nov_18_13_00_00_IST_2007' - interval ending time stamp, and 'PT15M' is interval time.

Note: In this version only 15 minutes intervals are supported.

Users can choose whether or not to receive a trap when each file is created. The trap name is **acEMSPmFileGenerate**. The trap contains information as to the file name and the time it was created.

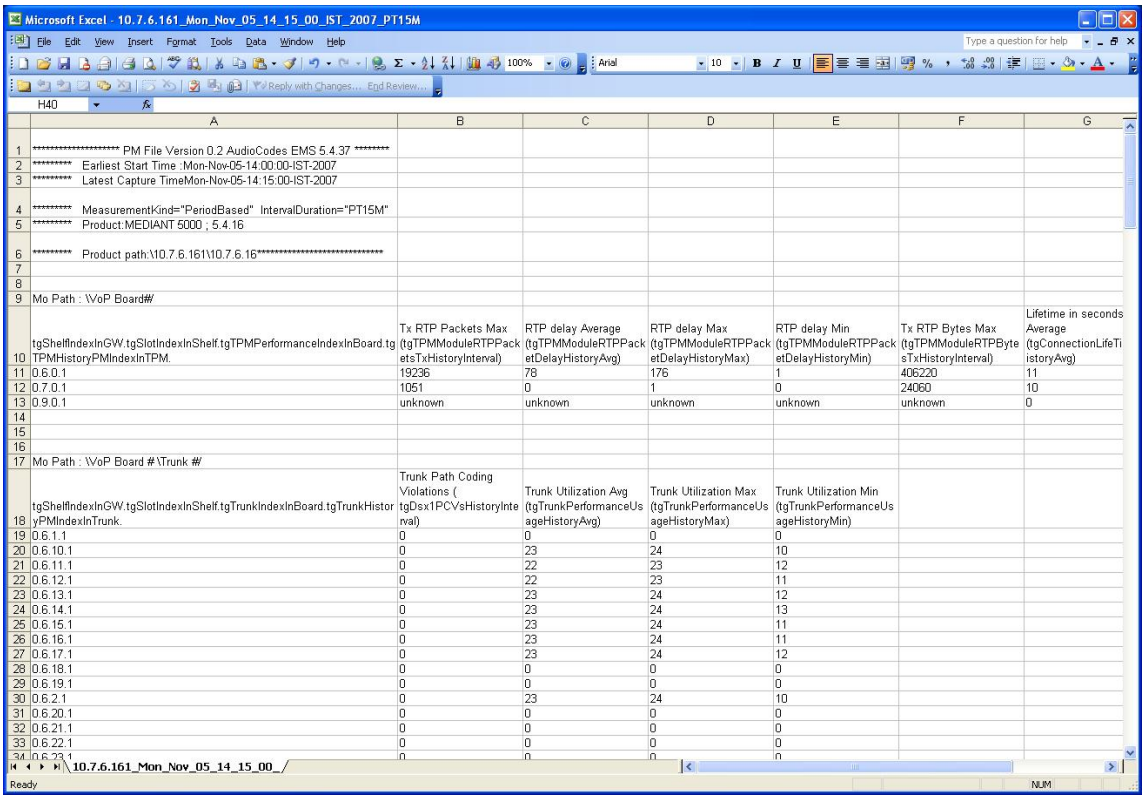
- Retrieve the PM file from the FTP server with the NMS / OSS system. In the event of EMS server machine hardening, use a secure FTP.
- The EMS keeps PM files for 24 hours (up to 96 files per Gateway).
- File format. Each file is composed of the following:
  - Header which includes a summary of the relevant information, such as EMS Version, File format version; product type, version, and path; measurement type, and interval start and end time.
  - Data contained in the tables according to the managed object type. For example: VoP Board, SC Board, VoP Board Trunks, etc. Each table has a title specifying managed object name. Each table is composed of the measured parameters name (defined as column name as combination of EMS Name and MIB name), and data which starts with the index (as it polled from the MIB), and is followed by the actual value. An *'unknown'* value can be received from the Gateway if the TP board is locked or for some other reason information is not received from the TP board.

csv File Format

The file header contains the device information.

PM File Version 0.2 AudioCodes EMS Version 5.4.27		
Earliest Start Time: Example: Thu-Dec-29-10:00:00-IST-2005		
Latest Capture: Example - TimeThu-Dec-29-10:15:00-IST-2005		
MeasurementKind ="PeriodBased" IntervalDuration="PT15M"		
Product: Hardware Type; software version		
Product Path:\xxxx\xxx		

Figure 2-19: Background Monitoring *csv* File



	A	B	C	D	E	F	G
1	********** PM File Version 0.2 AudioCodes EMS 5.4.37 ********						
2	********* Earliest Start Time :Mon-Nov-05-14:00:00-IST-2007						
3	********* Latest Capture TimeMon-Nov-05-14:15:00-IST-2007						
4	********* MeasurementKind="PeriodBased" IntervalDuration="PT15M"						
5	********* Product:MEDIANT 5000 ; 5.4.16						
6	********* Product path:\10.7.6.161\10.7.6.16**********						
7							
8							
9	Mo Path : \VoP Board#/						
10	tgShelfIndexInGW.tgSlotIndexInShelf.tgTPMPerformanceIndexInBoard.tgTPMHistoryPMIndexInTPM.	Tx RTP Packets Max (tgTPMModuleRTPPacketsTxHistoryInterval)	RTP delay Average (tgTPMModuleRTPPacketDelayHistoryAvg)	RTP delay Max (tgTPMModuleRTPPacketDelayHistoryMax)	RTP delay Min (tgTPMModuleRTPPacketDelayHistoryMin)	Tx RTP Bytes Max (tgTPMModuleRTPBytesTxHistoryInterval)	Lifetime in seconds Average (tgConnectionLifeTiistoryAvg)
11	0.6.0.1	19236	78	176	1	406220	11
12	0.7.0.1	1051	0	1	0	24060	10
13	0.9.0.1	unknown	unknown	unknown	unknown	unknown	0
14							
15							
16							
17	Mo Path : \VoP Board # \Trunk #/						
18	tgShelfIndexInGW.tgSlotIndexInShelf.tgTrunkIndexInBoard.tgTrunkHistoryPMIndexInTrunk.	Trunk Path Coding Violations (tgDsx1PCVsHistoryInterval)	Trunk Utilization Avg (tgTrunkPerformanceUsageHistoryAvg)	Trunk Utilization Max (tgTrunkPerformanceUsageHistoryMax)	Trunk Utilization Min (tgTrunkPerformanceUsageHistoryMin)		
19	0.6.1.1	0	0	0	0		
20	0.6.10.1	0	23	24	10		
21	0.6.11.1	0	22	23	12		
22	0.6.12.1	0	22	23	11		
23	0.6.13.1	0	23	24	12		
24	0.6.14.1	0	23	24	13		
25	0.6.15.1	0	23	24	11		
26	0.6.16.1	0	23	24	11		
27	0.6.17.1	0	23	24	12		
28	0.6.18.1	0	0	0	0		
29	0.6.19.1	0	0	0	0		
30	0.6.2.1	0	23	24	10		
31	0.6.20.1	0	0	0	0		
32	0.6.21.1	0	0	0	0		
33	0.6.22.1	0	0	0	0		
34	0.6.23.1	0	0	0	0		

xml File Format

The concept is the same as the *csv* file's format. Below are examples of the file header and content.

Figure 2-20: xml File Header Example


```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile MeasurementCategory="PM">
    <EarliestStartTime>Sun-Nov-18-12:45:00-IST-2007</EarliestStartTime>
    <LatestCaptureTime>Sun-Nov-18-13:00:00-IST-2007</LatestCaptureTime>
  - <System>
      <SystemId>PM File Version 0.2 AudioCodes EMS 5.4.45</SystemId>
    - <Entity>
        <EntityId>Product:MEDIANT 5000 ; 5.4.18</EntityId>
        <EntityAddress>\10.7.6.161\10.7.6.161</EntityAddress>
    + <Table MeasurementKind="PeriodBased" IntervalDuration="PT15M">
    + <Table MeasurementKind="PeriodBased" IntervalDuration="PT15M">
      </Entity>
    </System>
  </PMFile>
```


Figure 2-21: xml File Data example


```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile MeasurementCategory="PM">
    <EarliestStartTime>Sun-Nov-18-12:45:00-IST-2007</EarliestStartTime>
    <LatestCaptureTime>Sun-Nov-18-13:00:00-IST-2007</LatestCaptureTime>
  - <System>
      <SystemId>PM File Version 0.2 AudioCodes EMS 5.4.45</SystemId>
    - <Entity>
        <EntityId>Product:MEDIANT 5000 ; 5.4.18</EntityId>
        <EntityAddress>\10.7.6.161\10.7.6.161</EntityAddress>
    - <Table MeasurementKind="PeriodBased" IntervalDuration="PT15M">
        <TableId>\VoP Board#</TableId>
      - <Labels>
          <Label KeyOfRow="true"
            ValueType="string">tgShelfIndexInGW.tgSlotIndexInShelf.tgTPMPerformanceIndexInBoard.tgTPMHistoryPM
          <Label>Tx RTP Packet loss Max (tgTPMModuleRTPPacketLossTxHistoryInterval)</Label>
          <Label>RTP delay Average (tgTPMModuleRTPPacketDelayHistoryAvg)</Label>
          <Label>RTP delay Max (tgTPMModuleRTPPacketDelayHistoryMax)</Label>
          <Label>RTP delay Min (tgTPMModuleRTPPacketDelayHistoryMin)</Label>
          <Label>Rx RTP Packet loss Max (tgTPMModuleRTPPacketLossRxHistoryInterval)</Label>
        </Labels>
      - <RowOfValues>
        - <RowValue>
            <Value>0.6.0.1</Value>
          </RowValue>
        - <RowValue>
            <Value>0</Value>
          </RowValue>
        + <RowValue>
        + <RowValue>
        + <RowValue>
        + <RowValue>
        </RowOfValues>
      + <RowOfValues>
      + <RowOfValues>
      </Table>
    + <Table MeasurementKind="PeriodBased" IntervalDuration="PT15M">
      </Entity>
    </System>
  </PMFile>
```

2.8.2 Option #2: Mediant 5000 / 8000 CSV File Format Interface

Refer to the Mediant 5000 / 8000 OAMP Guide for the exact list of supported performance measurement parameters. The OAMP Guide includes both EMS and SNMP parameter names.

The file is created at the end of the PM polling interval and includes all the PM parameters supported by the GATEWAY. Files are stored and can be retrieved from the GATEWAY Global IP address under directory '/Project/bin/log/pm'. The GATEWAY keeps PM files for 24 hours (up to 96 files per Gateway). NMS can retrieve the PM file via FTP or SFTP (in case of GATEWAY hardening).

File name and file structure are same as for EMS CSV file.

2.8.3 Option #3: Media Gateway SNMP Interface

Refer to the specific product OAMP Guide for the exact list of supported performance measurement parameters. The OAMP Guide includes both EMS and SNMP parameter names.

The following information refers to Mediant 5000 / 8000 Gateways:

- The only valid SNMP agent for PMs Polling is MG Global IP address on the SC, and PM MIBS provided as part of the Mediant 5000/8000 SW package (SC board).
- In order to perform accurate polling of the parameters defined as 'Hist' in the OAMP Guide, the following read-only parameters are available at the MG level:
  - **PM Operative State** – read-only - (**tgMGInfoPMOperativeState**) – history data can be collected only when PM Operative State is enabled.
  - **Sample Time** - read-only - (**tgMGInfoSampleTime**) – Statistics sample period (seconds). How often the System Controller samples SC related parameters.
  - **Report Period** - read-only - (**tgMGInfoReportPeriod**) – Statistics report period (seconds), in the current version only 15 minute sample periods are supported (900 seconds).
  - **Current Interval Collection status** – read-only - (**tgMGInfoHistoryIntervalStatus**) – indicates whether the MG history collection is in progress or completed. When MG status is reported as completed, the management system can start polling the latest history parameters (refer to RT / Hist mark in the parameters tables).

- **MG Last Interval End Time** – read-only - (**tgMGInfoLastIntervalEndingTime**) – When the last polling interval became available at the MG level. This information is inserted together with the following:

  - Board Last Interval Time – read-only - (tgMGInfoBoardLastIntervalTime) – TP Board report last interval time. For example, when returned value is 2006-2-2 16:15:00, last polling interval include information for 2006-2-2, 16:00:00 – 16:15:00. The information will be available in the MG level when Current Interval Collection Status will receive 'complete' value.

See the Mediant 8000 response example below:

```
1. tgMGInfoPMOperativeState.0 (INTEGER) enabled(1)
2. tgMGInfoSampleTime.0 (INTEGER) 60
3. tgMGInfoReportPeriod.0 (INTEGER) 900
3. tgMGInfoHistoryIntervalStatus.0 (INTEGER) complete(0)
4. tgMGInfoBoardLastIntervalTime.0 (OCTET STRING) 2006-2-2 16:15:00
5. tgMGInfoLastIntervalEndingTime.0 (OCTET STRING) 2006-2-2
   16:18:12
```

2.9 Security Aspects

To understand application and network security between the EMS and the Media Gateway, refer to the Security Management section in the EMS User's Manual.

The following aspects are related to the NMS application when integrating the EMS and the Media Gateway:

1. **EMS Users Management (Authentication & Authorization)**: EMS Users can be managed either locally in the EMS Server database, or via a centralized Radius Server. The details below describe how to provision the Radius Server and the EMS application in order to enable centralized users authentication and authorization via a Radius server.
2. **Network Communication Protocols**:
   - **EMS Client - Server** communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). EMS also enables Client installation and launching via JAWS running over HTTPS.
   - **EMS Server – managed Gateways** communication can be secured as following:
     - Mediant 5000 / 8000:
       - SNMPv3 for Provisioning, Maintenance Action, Faults and Performance Monitoring
       - SSH and SCP for File transfer and Online Software Upgrade
       - IPec with an IKE pre-shared key for other communication (like NTP)
     - Mediant 1000 /2000 /3000 and MPs:
       - SNMPv3 for Provisioning, Maintenance Action, Faults and Performance Monitoring
       - HTTPS for File transfer and Online Sotwware Upgrade
       - IPec with an IKE pre-shared key for other communication (like NTP)
3. **EMS server secure access.** The secure access to the EMS Server machine is possible via SSH and SFTP protocols in order to perform maintenance actions and access files. SNMPv3 traps can be forwarded from the EMS server machine. In addition, overall EMS server connectivity can be secured using IPSec protocol (with the IKE pre-shared key).

In each one of the options below, User Authentication and Authorization is performed either via the EMS Application local database, or via centralized Radius server in accordance with the Security profile configured by the Administrator User of the EMS application. For more information, refer to the Security Management chapter in the EMS User Guide.

2.9.1 Centralized EMS Users Authentication and Authorization via Radius Server

Customers may enhance the security and capabilities of logging into the EMS application by using a Remote Authentication Dial-In User Service (RADIUS) to store numerous usernames, passwords and access level attributes. This feature allows multiple user management on a centralized platform. RADIUS (RFC 2865) is a standard authentication protocol that defines a method for contacting a predefined server and verifying a given name and password pair against a remote database, in a secure manner.

When accessing the EMS application, users must provide a valid username and password of up to 128 Unicode characters. EMS doesn't store the username and password; however, forwards them to the pre-configured RADIUS server for authentication (acceptance or rejection). The local EMS users and passwords defined in Users' List can be used as a fallback mechanism in case the RADIUS servers does not respond.

EMS supports provisioning of up to three Radius Servers for redundancy purposes. When the first server does not respond, EMS proceeds to the second server, and then to the third server. EMS will always start working with the previously responded server that is indicated as 'Current Active Radius Server'.

2.9.1.1 Setting Up the Radius Server

This section describes an example of a RADIUS Server configuration. You must configure the EMS Server as a RADIUS client in order to perform authentication and authorization of EMS Users using the RADIUS server from the EMS application.

The example configuration is based on FreeRADIUS, which can be downloaded from the following location: www.freeradius.org. Follow the directions on this site for information on installing and configuring the server.

Note: If you use a RADIUS server from a different vendor, refer to its appropriate documentation.

➢ **To set up a RADIUS server using FreeRADIUS, take these steps:**

1. Define the EMS Server as an authorized client of the RADIUS server, with a predefined 'shared secret' (a password used to secure communication) and a vendor ID. The figure below displays an example of the file **clients.conf** (FreeRADIUS client configuration).

Example of the File clients.conf (FreeRADIUS Client Configuration)

```
#
# clients.conf - client configuration directives
#
client 10.31.4.47 {
        secret          = FutureRADIUS
        shortname       = ems
}
```

2. If access levels are required, set up a VSA dictionary for the RADIUS server and select an attribute ID that represents each user's access level. The following example shows a dictionary file for FreeRADIUS that defines the attribute 'ACL-Auth-Level' with ID=35.

Example of a Dictionary File for FreeRADIUS (FreeRADIUS Client Configuration)

```
#
# AudioCodes VSA dictionary
#
VENDOR AudioCodes 5003
ATTRIBUTE ACL-Auth-Level 35 integer AudioCodes
VALUE ACL-Auth-Level ACL-Auth-Monitor 50
VALUE ACL-Auth-Level ACL-Auth-Operator 100
VALUE ACL-Auth-Level ACL-Auth-Admin 200
```

3. In the RADIUS server, define the list of users authorized to use the Gateway, using one of the password authentication methods supported by the server implementation. The following example shows a user configuration file for FreeRADIUS using a plain-text password.

Example of a User Configuration File for FreeRADIUS Using a Plain-Text Password

```
# users - local user configuration database

john    Auth-Type := Local, User-Password == "qwerty"
        Service-Type = Login-User,
        ACL-Auth-Level = ACL-Auth-Monitor

larry   Auth-Type := Local, User-Password == "123456"
        Service-Type = Login-User,
        ACL-Auth-Level = ACL-Auth-Admin
```

4. Record and retain the IP address, port number, 'shared secret', vendor ID and VSA access level identifier (if access levels are used) used by the RADIUS server.

5. Provision the relevant EMS parameters according to the section below.

2.9.1.2 Provisioning EMS to perform Radius Server Authentication and Authorization

This section describes how to provision EMS users stored on a Radius Server using the EMS application.

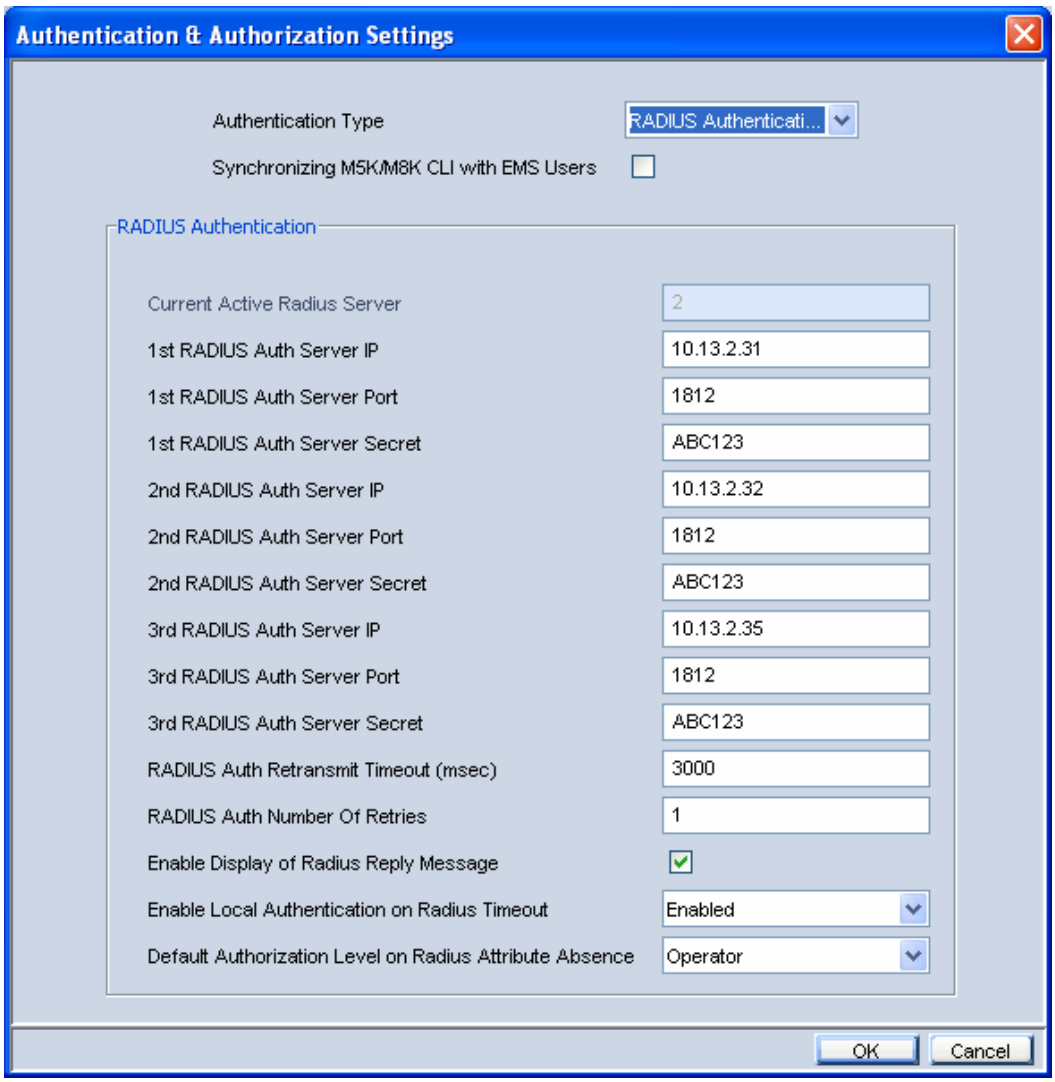
➢ **To provision EMS to connect Radius Server, perform the following steps:**

1. In the Security menu, choose the **Authentication and Authorization** option.
2. Select Authentication Type to **Radius Authentication**.
3. For each one of the three Radius Servers, define Radius Server IP, Port and Secret. Note, that at least one Radius Server should be provisioned.
4. Define Radius Server Retransmit Timeout and Number of Retries. Default values are Retransmit Timeout = 3000 msec, and Number of Retries = 1. Note that these parameters will be used for each one of the Radius Servers.
5. Define if you wish to display the Radius Reply message. By default this parameter is enabled.

6. Define EMS behavior in case the Radius server does not respond. By default EMS local authentication is enabled. To provision the list of local users and their properties, refer to section "User's List" . When the **Enable Local Authentication on Radius Timeout** parameter is enabled, it's possible to select the **Synchronize M5K / M8K with EMS Users** option. In this case, EMS will update each one of the managed nodes upon any of the User's List changes (add, remove, and update users). For more information, see Local Users Management in the EMS Application.

7. Define EMS behavior in case the Radius server response does not include Authorization Vendor Specific Element (described above). In this case, the Administrator can either deny user access or set a default security level to be granted to the User. By default, EMS provides access to the application and provisions an Operator security level to the User.

Figure 2-22: Authentication and Authorization Settings



3 EMS Private Labeling

3.1 Overview

Private labeling is designed to enable the customer to customize EMS and MG labeling according to their specific requirements. This allows the customer to use the EMS under their own company name, Gateways names, logos and images.

The customization process involves preparing files and images as described in this document, and then packaging these files and images in a custom. zip file. At the end of the customization process, customer should create a new DVD that includes the custom.zip file.

This zip file is then placed on the customer prepared DVD.

The following items can be customized by the private labeling process:

- License agreement document replacement
- Company Logos & Icons
- Company name, MG and TP boards naming
- Online Help

Note: The customer should verify that the EMS Server installation is working properly after the server branding procedure. Client / Server communication and Media Gateway configuration are also required as minimal sanity testing of the branding DVDs.

3.2 Private Labeling Procedure

This section describes the Private Labeling procedure. The Audiocodes EMS DVD includes a folder named **PrivateLabeling**. This folder contains all of the files required for performing Private Labeling. Once the files in this folder are updated, they should be compressed and placed on a new DVD.

3.2.1 Creating a New Customer Specific EMS DVD

The new EMS DVD should include the following folders:

- **Documentation/Patches**: Note that default documentation set provided in the EMS DVD is AudioCodes branded and customers should replace all the documentation according to their branding requirements. The Patches folder should remain unchanged. Documentation/PrivateLabeling: this folder is an intermediate folder that should not be located on the customized DVDs.
- **EmsClientInstall**: In order to create new, private labeled DVDs, the customer should perform all the required updates in a default custom.zip file, and then replace the existing **EmsClientInstall** file in the PrivateLabeling/EmsClientInstall folder.

  For more information, refer to section EMS Server Full Branding Process on page 50 below.
- **EmsServerInstall**: The new server software file created as a result of the procedure described on page 50 below should replace the existing **EMSServerInstall** file in the EmsServerInstall folder.

- **MG_sw**: The .ems file should be updated according to customer product names specified in the custom.zip file **product_names**.properties file. For more information, see page 49.

3.2.2 Custom Zip file

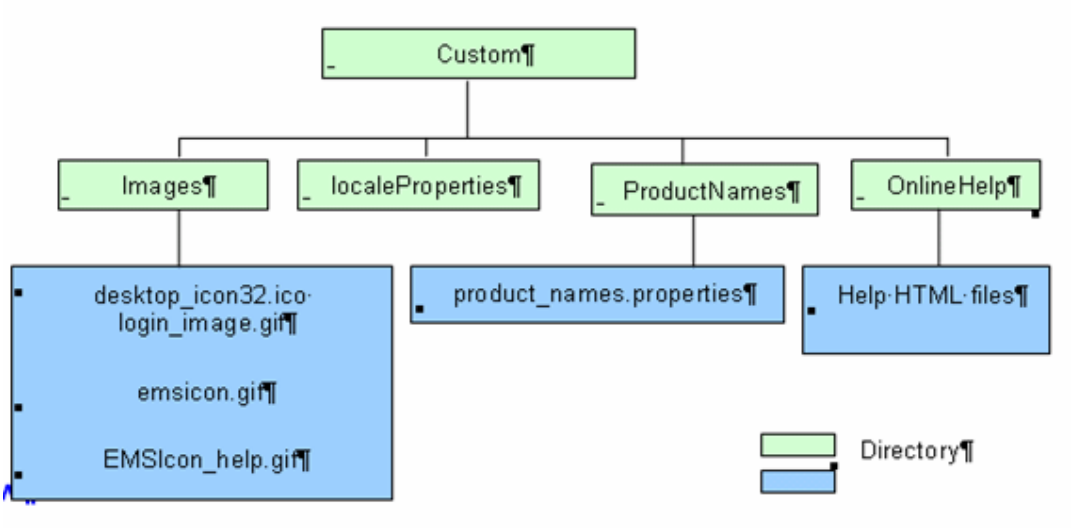
This section describes the custom zip file.

In order to open the encrypted zip file, password 'pass_1234' should be used. The file should be closed with the same password.

3.2.2.1 Overview

The following diagram illustrates the components of the Custom.zip file.

Figure 2-23: Custom Zio File



3.2.2.2 Images Folder

This folder includes all the default replacements for all the icons and images (in the original application is the Audiocodes logo). Customers can replace these images, while the file name and image size are not changed.

Note: **It is recommended** to use the same color convention as in the original EMS application.

The Table below summarizes the details of each image:

Image Name	Image Size	Format	Description
desktop_icon32.ico	32X32	ICO	Desktop icon located at the operator Desktop at the end of client installation
login_image.gif	445X311	Gif	Background picture in the Login Screen
emsicon.gif	16X16	Gif	Icon located in the left corner of application title bar
EMSIcon_help.gif	16X16	Gif	Icon located in the left corner of the Online Help title bar
bottom_left_image.gif	150X137	Gif	Image located in the bottom of the EMS Tree Panel
wizard_background.gif	193X119	Gif	Image located in the left bottom corner of the Mediant 5000 / 8000 and IPMedia 5000 / 8000 Online Software Upgrade Wizard
performance_background.gif	182X138	Gif	Image located in the left bottom corner of the Mediant 5000 / 8000 and IPMedia 5000 / 8000 Performance Monitoring screens

For more information, refer to Appendix A – Private Labeling Icons on page 55.

3.2.2.3 localeProperties Folder – currently not in use.

3.2.2.4 ProductNames Folder

This folder includes ASCII file named **product_names** properties file. This file includes Company Name and names of all the Audiocodes products supported by EMS. For some of the products, VoP board names can also be also customized. Most of the products have full and short names. When the full name is changed or removed, the short name should be updated accordingly.

This file includes:

- Company Name – to change the company name, the 'AudioCodes' string should be replaced with the new company name

- Product Full Names - Customer should change product names in the right side of the equals mark. The Left side name is used internally by the EMS application and should not be changed. For example, when the user wishes to change 'Mediant 5000' product name to MyGATEWAY 5K', the default line #1 should be replaced with line #2. When the user wishes to remove the product name from the EMS application, the default definition (line#1) should be replaced with line#3 below:

```
Line#1: Mediant_5000=Mediant 5000
Line#2: Mediant_5000=MyGATEWAY 5K
Line#3: Mediant_5000=
```

- Product Short Names. Following is a list of the currently used short names: M5K, M8K, MP, M3K, M1K, M2K, IPM2K, IPM3K.

- VoP Board Names. Following is list of currently supported VoP boards: TP-1610, TP-6310, SB-1610, IPM-6310.

When changing the name of one of the following products: Mediant_5000, Mediant_8000, Ipmedia_5000 or Ipmedia_8000, the .ems file located in the original CD under **MG_sw** folder should be updated with the list of new names. In reference to the Mediant_5000 example above, Line#1 in the original file should be replaced with Line#2, and all the unused products should be removed.

```
Line #1: product_type1=MEDIANT 5000
Line #2: product_type1= MyGATEWAY 5K
```

3.2.2.5 Online Help folder

By default, the Online Help folder is empty. This implies that when customers don't perform Online Help branding, the Online Help feature will be disabled by the EMS application, and when 'Online Help' is clicked,,the information message: 'Online Help is not supported' is displayed The reason for this is that Online Help is created based on the EMS documentation, which includes multiple references to AudioCodes, original product names, company logos, etc.

In order to perform branding of the Online Help, the customer should copy all the files from the **PrivateLabeling/OnlineHelp** folder, and update all the .html files (about 1050 HTML files).

Note the following:

1. Only the content of these files can be updated.

   Note : the names (an index number) **MUST** remain unchanged.
2. The content of the file **index.xml** can be updated for the help index view.

   Note : the links numbers **MUST** remain unchanged.
3. The content of the file **toc.xml** can be updated for the help content view

   Note : the links numbers **MUST** remain unchanged.

3.2.3 EMS Server Full Branding Process

This section describes the procedure to customize EMS server software. During the customization procedure, the EMS server software tar file is opened, modified, signed, and closed again. The modified file should be placed on the new customer CD/DVD.

Note: In order to perform server branding, the EMS server should meet the minimum requirements as specified in the EMS System Requirements in the EMS Users Manual.

➢ **To customize EMS Server Software, do the following:**

1. Copy the entire folder **PrivateLabeling/EmsServerInstall** content to the EMS server machine **ACEMS** folder. The folder content includes:

   - emsServerDeploy_5.x.y.tar – EMS server original software file
   - custom.zip file prepared as part of EMS client branding (for more information, refer to Custom Zip file on page 48.
   - unzip – unzip software required by EMS application

- branding.sh – the script that the customer should run in order to create a new emsServerDeploy_5.x.y.tar file

2. Change permission of branding.sh to be executable, by running command:

```
[ACEMS] chmod 755 branding.sh
```

In order to perform jars signing, customer can use it's own jar signing file **jarsKeyStore**, which should be placed in the ACEMS folder. If there is no customer specific file, EMS will use its own default file.

Run server_branding_script. This script requires the original EMS server software file **emsServerDeploy_5.x.y.tar** as input parameter.

```
[ACEMS] ./branding.sh 5.x.y
```

This script performs server software opening, modifications, and jars signing.

a. When user specific jarsKeyStore file is found, user will be asked to provide **Keystore alias** and **storepass** for keystore for each one of the jars (see Example 1 below)
b. If the specific jarsKeyStore file was created also with key password then the user will be asked to also provide **keyPass** for each one of the jars.
c. When user specific jarsKeyStore file is not found, user will not need to provide any key and pass (see Example 2 below)

Note: In the event of errors, the script details the errors, and the initial emsServerDeploy_5.x.y.tar file is restored.

At the end of the server_branding_script, a new emsServerDeploy_5.x.y.tar EMS server file is created. This file should replace the default (ACL branded) server file in the customer DVD.

Note: The customer should verify that the EMS Server installation is working properly after the server branding procedure. Client / Server communication and Media Gateway configuration are also required as minimal sanity testing of the branding DVDs.

Example 1:

```
****************************************
    ***** START  CUSTOMIZATION PROCESS *****
    ****************************************

   SYSTEM CHECKS
===================
     Server tar: OK
     custom.zip: OK
     unzip: OK
     Jar keystyore: OK

   Extracting tar files...
```

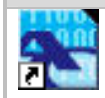
```
============================
x EmsServerInstall, 0 bytes, 0 tape blocks
x EmsServerInstall/ac_ems_deploy, 0 bytes, 0 tape blocks
x EmsServerInstall/values.install, 2542 bytes, 5 tape blocks
x EmsServerInstall/versionUpgradeMap.txt, 1268 bytes, 3 tape blocks

   Extracting custom.zip files...
===================================
    custom.zip extraction: OK
==================================================
Start updating files. This may take 5-10 minutes.[Thu Apr 12
06:48:16 EDT 2007]
==================================================
 Replacing images .....
 Replacing files .....

   Checking help files...
=========================
Help files:Not Exist--> Disabling online help

   Update license agreement
===========================
    Agreement updated: OK

   Creating jar for re-signing
==============================
     ---> configurationProperties
     ---> emsSwVersionFiles
     ---> help
     ---> images
     ---> localeProperties
     ---> mibs
     ---> sounds
     ---> security

   Jars re-signing
=====================
    Signing jars with given key
Please provide parameters for jar signing.
Enter Keystore alias:
Enter storepass for keystore:
Error: Keystore alias or password incorrect!!
Enter Keystore alias:
Enter storepass for keystore:

Warning: The signer certificate will expire within six months.
*******************************************************
***** Customization Process Finished Successfully *****
```

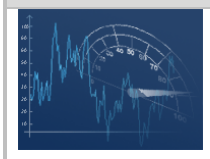
Example 2:

```
****************************************
    ***** START  CUSTOMIZATION PROCESS *****
    ****************************************
   SYSTEM CHECKS
===================
     Server tar: OK
     custom.zip: OK
     unzip: OK
     Jar keystore: Not Exists

   Extracting tar files...
============================
x EmsServerInstall, 0 bytes, 0 tape blocks
x EmsServerInstall/ac_ems_deploy, 0 bytes, 0 tape blocks
...
x EmsServerInstall/values.install, 2542 bytes, 5 tape blocks
x EmsServerInstall/versionUpgradeMap.txt, 1268 bytes, 3 tape blocks

   Extracting custom.zip files...
===================================
    custom.zip extraction: OK
==================================================
Start updating files. This may take 5-10 minutes.[Thu Apr 12
03:52:10 EDT 2007]
==================================================
 Replacing images .....
 Replacing files .....
   Checking help files...
=========================
Help files:Not Exists --> Disabling online help
   Update license agreement
============================
    Agreement updated: OK

   Creating jar for re-signing
==============================
     ---> configurationProperties
     ---> emsSwVersionFiles
     ---> help
     ---> images
     ---> localeProperties
     ---> mibs
     ---> sounds
     ---> security

   Jars re-signing
=====================
    Signing jars with self created key

Warning: The signer certificate will expire within six months.
*******************************************************
***** Customization Process Finished Successfully *****
```

Reader's Notes

4 Appendix A – Private Labeling Icons

Icon	Description
	ACL Desktop Icon
	Default Desktop Icon
	ACL Login Image
	Default Login Image
	ACL Window Icon
	Default Window Icon
	ACL Help Icon
	Default Help Icon
	ACL Tree Image
	Default Tree Image
	ACL Wizard Image
	Default Wizard Image
	ACL Performance Image

Icon	Description
	Default Performance Image

Reader's Notes

EMS for AudioCodes' Media Gateways and Servers

AudioCodes EMS Element Management System

OAMP (EMS) Integration Guide

Version 5.8

Document #: LTRT- 19207

AudioCodes

www.audiocodes.com