AudioCodes EMS  Element Management System

Element Management System (EMS)

Release Notes

Version 5.8

Document #: LTRT-90522
# Table of Contents

1 Managed VoIP Equipment .................................................................................................. 7  
   1.1 Managed 5.8 Version Gateways and Control Protocols ............................................. 7  

2 New Features in EMS Version 5.8 ..................................................................................... 9  
   2.1 General ..................................................................................................................... 9  
      2.1.1 EMS Server on Linux ....................................................................................... 9  
      2.1.2 Oracle Database Version Update ...................................................................... 9  
      2.1.3 EMS Server Manager ..................................................................................... 9  
      2.1.4 Automatic Gateway Software Version Detection ............................................. 9  
   2.2 Security Management ............................................................................................... 9  
      2.2.1 EMS Server FIPS Compliance ......................................................................... 9  
      2.2.2 EMS User Management .................................................................................. 9  
   2.3 Configuration, Management and Maintenance ......................................................... 12  
      2.3.1 Digital Gateway Related Features Mediant  
           600/1000/2000/3000/5000/8000 (for VoP Boards) ............................................. 12  
      2.3.2 Mediant, IPmedia 5000/8000 Related Features ................................................. 13  
      2.3.3 New Features of the Mediant 1000/2000/3000, IPmedia 2000/3000 and  
           MediaPack ..................................................................................................... 14  

3 New Features in EMS Version 5.6 ..................................................................................... 15  
   3.1 General ..................................................................................................................... 15  
      3.1.1 Java Version Update .......................................................................................... 15  
      3.1.2 Oracle Database Version Update ...................................................................... 15  
      3.1.3 Apache Version Upgrade ............................................................................... 15  
      3.1.4 EMS Server Configuration display in the EMS Client GUI ................................. 15  
      3.1.5 EMS Server Maintenance Improvements ........................................................ 15  
      3.1.6 EMS Server North Bound Interface Changes ................................................... 16  
      3.1.7 Software Manager – Save file ......................................................................... 16  
      3.1.8 Online Help ..................................................................................................... 16  
      3.1.9 OpenCA OCSP Daemon (OCSPD) ................................................................... 16  
   3.2 Fault Management ................................................................................................ ..... 16  
      3.2.1 Carrier-Grade Alarms System between EMS & Media Gateway’s ................... 16  
      3.2.2 Events View in Alarm Browser ........................................................................ 16  
      3.2.3 Trap Forwarding ............................................................................................... 17  
      3.2.4 Alarms and Journal Unified View and Filters .................................................... 17  
      3.2.5 Alarm Browser and History Columns Enhancements ....................................... 17  
      3.2.6 New Alarms / Events Support ......................................................................... 17  
   3.3 Security Management (EMS Server) ............................................................................. 17  
      3.3.1 EMS Server File Integrity Checking .................................................................. 17  
      3.3.2 Intrusion Detection System .............................................................................. 17  
      3.3.3 EMS Server Security Patches Loading During Version Installation & Upgrade .... 18  
   3.4 Configuration Management and Maintenance ............................................................ 18  
      3.4.1 Mediant, IPmedia 5000 / 8000 Related Features ............. ................................. 18  
      3.4.2 New Features of the Mediant 1000/2000/3000, IPM-260/IPmedia  
           2000/3000 and MediaPack ............................................................................... 19
4 New Features in EMS Version 5.4 ................................................................................................. 21
  4.1 General ..................................................................................................................................... 21
      4.1.1 EMS Server Maintenance Improvements ........................................................................... 21
      4.1.2 Multiple Ethernet Interfaces on the EMS Server ............................................................. 21
      4.1.3 Ethernet Interfaces Redundancy ...................................................................................... 21
      4.1.4 NTPv4 on the EMS Server ............................................................................................... 21
      4.1.5 Apache Version Upgrade ................................................................................................. 21
  4.2 Fault Management .................................................................................................................... 21
      4.2.1 Events Presentation and Filtering .................................................................................... 21
      4.2.2 SNMPv3 Traps Forwarding ............................................................................................... 21
      4.2.3 Trap Forwarding Enhancements ...................................................................................... 22
      4.2.4 New Alarms Support ........................................................................................................ 22
  4.3 Security Management ................................................................................................................. 22
      4.3.1 Radius Server Authentication and Authorization .............................................................. 22
      4.3.2 Welcome (Advisory) Message .......................................................................................... 22
      4.3.3 Last Successful Login Time Display .................................................................................. 22
      4.3.4 EMS Authentication - Password Aging Provisioning ...................................................... 22
  4.4 Configuration Management and Maintenance ........................................................................... 23
      4.4.1 Mediant, IPmedia 5000 / 8000 Related Features .............................................................. 23
  5 Known Limitations and Workarounds ......................................................................................... 25
Notice

This document describes the new features released in Version 5.8 for AudioCodes’ 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, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers http://www.audiocodes.com/downloads.

© 2009 AudioCodes Inc. All rights reserved

This document is subject to change without notice.

Date Published: November-15-2009

Note: The EMS supports the following products:

- Mediant 600/1000/2000/3000/5000/8000 Media Gateways.
- IPmedia 2000/3000/5000/8000 Media Servers.
- MediaPack Media Gateways MP-500, MP-102 (FXS), MP-104 (FXS and FXO), MP-108 (FXS and FXO), MP-112 (FXS), MP-114 (FXS), MP-118 (FXS) and MP-124 (FXS), 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, VolPerfect, VolPerfectHD, 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.
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. The $ symbol indicates hexadecimal notation.

Related Documentation

<table>
<thead>
<tr>
<th>Manual Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediant 5000 / 8000/IPmedia 8000 Media Gateway Installation, Operation and Maintenance Manual</td>
</tr>
<tr>
<td>Mediant 5000 / 8000/IPmedia 8000 Media Gateway Release Notes</td>
</tr>
<tr>
<td>Mediant 3000 User’s Manual</td>
</tr>
<tr>
<td>IPmedia 3000 Media Server User’s Manual</td>
</tr>
<tr>
<td>Mediant 2000 User’s Manual</td>
</tr>
<tr>
<td>MP-500 User’s Manual</td>
</tr>
<tr>
<td>Mediant 600 User’s Manual</td>
</tr>
<tr>
<td>MediaPack User’s Manual</td>
</tr>
<tr>
<td>Element Management System (EMS) Product Description</td>
</tr>
<tr>
<td>Element Management System (EMS) User’s Manual</td>
</tr>
<tr>
<td>Element Management System (EMS) Online Help</td>
</tr>
<tr>
<td>Mediant 5000 / 8000/IPmedia 8000 Media Gateway Programmer’s User Manual</td>
</tr>
<tr>
<td>EMS Parameter Guide for the Mediant 5000 and Mediant 8000 Gateways</td>
</tr>
<tr>
<td>EMS Parameter Guide for Mediant 1000, Mediant 2000, Mediant 3000, IPmedia 3000 and IPmedia 2000</td>
</tr>
<tr>
<td>EMS Parameter Guide for MediaPack</td>
</tr>
</tbody>
</table>
1 **Managed VoIP Equipment**

The list of media gateways, media servers and boards (below) is accurate for version 5.8. **Bold** font indicates new products / versions.

- Mediant 5000/8000 Media Gateway and the IPmedia 5000/8000 Media Server: versions **5.8**, **5.6**, **5.4**, **5.2**
- Mediant 3000 Media Gateways and IPmedia 3000 Media Server: versions **5.8**, **5.6**, **5.4**
- Mediant 2000 Media Gateways and IPmedia 2000 Media Server: versions **5.8**, **5.6**, **5.4**
- Mediant 1000: versions **5.8**, **5.6**, **5.4**
- Mediant 600: versions **5.8**, **5.6**
- MediaPack Media Gateways: versions **5.8**, **5.6**, **5.4**

1.1 **Managed 5.8 Version Gateways and Control Protocols**

<table>
<thead>
<tr>
<th>Product / Control Protocol</th>
<th>MGCP</th>
<th>MEGACO</th>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediant 8000, IPmedia 8000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mediant 5000, IPmedia 5000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mediant 3000, TP-8410</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPMedia 3000, IPM-8410</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Mediant 3000, TP-6310</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPMedia 3000, IPM-6310</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mediant 2000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mediant 1000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mediant 600</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>MP-500 and MediaPack</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
2 New Features in EMS Version 5.8

2.1 General

2.1.1 EMS Server on Linux
EMS server Software is now supported on the CentOS 5 Linux Operating System. The Solaris Operating System is supported as well.

2.1.2 Oracle Database Version Update
The Oracle Database version has been updated from version Oracle 9.2i to Oracle 11g. During the EMS server installation, the Oracle 11g software and corresponding security patches are installed.

2.1.3 EMS Server Manager
The EMS Solaris Manager has been renamed the EMS Server Manager. It runs on both the Solaris and Linux platforms.

2.1.4 Automatic Gateway Software Version Detection
From this version, there is no need to add the Media Gateway Software to the Software Manager in order to manage the Media Gateway via the EMS. During the Gateway definition in the EMS (Add Gateway action or Auto Detection), the EMS connects to the Gateway and automatically determines its version. When performing a Gateway Software Version upgrade, you are still required to add the Media Gateway installation file to the EMS Software Manager.

2.2 Security Management

2.2.1 EMS Server FIPS Compliance
EMS Application USA Department of Defense Certification (for low- and medium-density Gateway products).
The EMS application has been certified for the extensive Security requirements of the USA Department of Defense. Encryption and authentication related software are now implemented using FIPS compliant, third-party software. Therefore, the entire encryption modules of the EMS application are FIPS 140-2 certified (FIPS-Federal Information Processing Standards-US Government Security Standards for Cryptography modules).

2.2.2 EMS User Management

2.2.2.1 Force Password Changes
This feature forces the user to change the user’s password on the next login attempt, before the previously defined password expiration time has expired. Active users are not required to logout the application until their session has ended.
2.2.2.2 **Session Inactivity Timer**

The Session Inactivity Timer ensures that a malicious intruder cannot use the EMS application’s active session if no action is performed by the user during a administrator-defined period. The user should close the EMS application when the user has completed a work session, using the newly defined ‘Session Lock’ option, otherwise, this session is considered as inactive and is subsequently automatically locked. The user must enter a password to unlock the session. The Administrator can define a different Session Inactivity Timer per user.

2.2.2.3 **User Accounts Inactivity Timer**

Users cannot login to the EMS application when their account has been inactive for an administrator-defined time. The blocking of inactive user accounts is intended to prevent usage of these accounts by potential intruders.

2.2.2.4 **Password Expiration and Warning Period per User**

In the previous version, password expiration and warning periods were defined globally for the EMS application and were the same for all users. In this version, these parameters can be defined per user.

2.2.2.5 **Password Complexity and Maintenance Extensions**

In this version, user password complexity rules have been extended with the following additional requirements. Rules provisioning is performed globally for the EMS application and not for a single user:

- Password Length configuration. Default password length remains unchanged – 8 characters. Password length can vary from between 4 to 30 characters.
- The Number of Previous Not Reused Passwords can be configured between 5 (default) and 10 characters.
- The Number of Not Repetitive Digits from Previous Password can be configured between 0 (default) and 10.
Passwords can be defined with one of the following complexity rules:

- Must contain a mix of upper case letters, lower case letters, numbers, and special characters
- Must contain three out of four of the above requirements

Password verification includes text for weak passwords (including names or well-known dictionary words) and enforces the user not to use weak passwords.

### 2.2.2.6 Login Information Display

After a successful login to the EMS application, the user is now notified with the following information:

- Latest successful login date, time and EMS Client machine IP address.
- Number of unsuccessful logins since the latest successful login.
- Latest unsuccessful login date, time and EMS Client machine IP address.
2.3 Configuration, Management and Maintenance

2.3.1 Digital Gateway Related Features Mediant 600/1000/2000/3000/5000/8000 (for VoP Boards)

2.3.1.1 TP-6310 OC-3 Board (in Mediant 3000/5000/8000) – Channelized DS3 Support

Channelized DS3-to-OC3 mapping is now supported. The OC3 interface on the TP-6310 board is mapped to three DS3 Trunks. Therefore, the following three options for SONET/SDH mapping are now supported:

- DS1 $\Rightarrow$ VT1.5 $\Rightarrow$ OC3 mapping for North America market.
- DS3 $\Rightarrow$ STS1 $\Rightarrow$ OC3 mapping for North America market.
- E1 $\Rightarrow$ VC12 $\Rightarrow$ STM1 for European market.

2.3.1.2 E1/T1 Trunks New Actions and Statuses

- Trunk Activity. New Activate/Deactivate maintenance actions on E1/T1 trunks have been added to the Trunk Status Screen maintenance menu options. This option allows the temporary stopping/starting of services on a specific trunk by raising/clearing an AIS alarm. These actions should be used when a trunk cannot be locked and additional configuration on this trunk is required (e.g. when an SS7 link is defined on this trunk). These actions can be performed for single selected or multiple trunks. The Trunk Activity status is displayed in a new column named ‘Activity’ in the Trunk status screen.

- D-Channel status. New Column ‘D-Channel Status’ has been added to the Trunks Status screen. D-Channel status can be one of the following: ‘Established’, ‘Not Established’ or ‘Not Applicable’.

- The Channel Status screen has been added. This screen enables the user to view the status of all the individual channels of all the Trunks of the TP board.

2.3.1.3 SS7 Alias Point Code Functionality

The definition of SS7 Point Code aliases is now supported. An “alias” point code is shared by more than one system supporting the same Global Title Translation (GTT). Each of the Signaling Points with the same “alias” point code is capable of providing predefined functionality in the network.

2.3.1.4 Realm – IP Domain Connectivity (IPDC) Mode for Multiple VLANs

The new H.248.41 IPDC package provisioning and management at the TP-6310/8410 board level is now supported. This package enables the interconnection between two media packet network subnets (IP-to-IP calls), using an IP Realm identifier property to indicate which packet network the media represented by the termination.
2.3.2 Mediant, IPmedia 5000/8000 Related Features

2.3.2.1 Supported VoP Board Types

VoP board types (and application types) supported in this version include the following:
- TP-6310 OC-3/STM-1/T3
- IPM-6310
- TP-8410

2.3.2.2 Installation Package Changes

The EMS Software Manager and Online Software Upgrade tools have been enhanced to support a new Mediant 5000/8000 installation package and to use new commands to install the Gateway software. In this version, the Software Manager supports both old and new formats, since the EMS also manages the Gateway with the previously installed version software.

2.3.2.3 Networking Provisioning Changes

The Board level MGW Networking Provisioning Frame has extended networking options. For more information, refer to the Mediant 5000 / 8000 Media Gateway Installation, Operation & Maintenance Manual document.

2.3.2.4 VoP Boards SIP IP-to-IP Features Definition

In this version, EMS supports SIP VoP Boards Provisioning of IP-to-IP call routing (or SIP trunking). This feature enables Enterprises to seamlessly connect their IP-PBX to a SIP trunk provided by an Internet Telephony Service Provider (ITSP).

2.3.2.5 TP-8410 (in Mediant 3000/5000/8000) – V5.2 Protocol Support (MGCP/MEGACO)

The AudioCodes V5.2 Access application aggregates legacy circuit-switched voice from the subscriber side, converts V5.2 protocol messages to the H.248 IP protocol and then sends them to a softswitch and vice versa (the softswitch replaces the traditional Class 5 switch).

The ability to provision and monitor V5.2 Protocol Interfaces and Links has been added to the EMS application. In addition, a new download file type is supported. The V5.2 users file includes definitions for Port/Line numbers and L3 addresses for all the V5.2 interfaces in the Gateway.
2.3.3 New Features of the Mediant 1000/2000/3000, IPmedia 2000/3000 and MediaPack

2.3.3.1 Configuration Verification and Download – Extended with Auxiliary Files Functionality

In this version, the EMS Configuration Verification action now compares both provisioning parameters values and Auxiliary files stored in the EMS and loaded to the Gateway. User display information includes a separation between Provisioning parameters and Auxiliary files. The Configuration Download has been enhanced with an option to perform Auxiliary files download. The default Configuration Download is unchanged for all configuration parameters.

2.3.3.2 Remove Auxiliary Files from Gateway

The EMS supports the removal of Auxiliary files from the Gateway. Upon selecting this option, the user is prompted with a list of all the files used by a specific Gateway. The user can then select file/s to remove.

2.3.3.3 Upload INI file from Gateway

A new option to perform an INI file upload from the Gateway to the EMS client has been added. The INI file is defined as a Debug interface and is used to assist the AudioCodes FAEs to perform problem debugging.

2.3.3.4 Mediant 3000 8410 V5.2 – Support Incremental Ports File Download

In addition to capabilities introduced in the previous version, this version supports the incremental V5.2 users file download. For example, the user can define a separate V5.2 users file per V5.2 interface, and download each one of these files whenever a new V5.2 Interface is added. In the previous version, only one V5.2 users file per Gateway was supported.
3 New Features in EMS Version 5.6

3.1 General

3.1.1 Java Version Update
The Java version has been updated to Java 6 JDK from Java 5. EMS uses build 1.6.0_06.

3.1.2 Oracle Database Version Update
The Oracle Database version has been updated to version 9.2.0.8 from 9.2.0.7. During the current EMS version installation, Oracle security patches are by default installed with Oracle database security hardening.

3.1.3 Apache Version Upgrade
The Apache Web server running on the EMS server machine and used for JAWS and Gateway Software and Auxiliary files upgrade has been upgraded from version 2.2.4 to version 2.2.6 (openssl version is version 0.9.8h).

3.1.4 EMS Server Configuration display in the EMS Client GUI
The EMS Client now includes an option to display EMS server related settings such as Network Interfaces and their redundancy definitions, Server Java version, Server security status, Web Server and NTP server information and statuses.

3.1.5 EMS Server Maintenance Improvements
The EMS Server Manager has been enhanced with the following features:

- Apache Web Server Management (status / start / stop), ability to disable HTTP (port 80), HTTPS (port 443) and JAWS applications. The Apache Web Server is used for JAWS and software and auxiliary files upgrade for low density gateways.

- You can now define additional SNMP managers in the EMS for low density gateways. During the Mediant 600/1000/2000/3000 & MP Gateway definition process in the EMS GUI (ADD GW), EMS will search for additional IP addresses and automatically add them as a manager to the SNMP managers table.

- The Show Info command has been enhanced with EMS Application and Oracle database processes statuses. The Show Info option provides the general EMS server information from the Solaris operating system. In this version, this command includes the following: EMS Version; EMS server Process Status; Oracle Server Status; Apache Server Status; Java Version; Memory size and Time Zone information.

- A File Integrity Tool (Yafic) Management (start / stop commands) is now used. The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported via EMS Security Events.

- Oracle Hardening is now performed as part of the installation process. This option is no longer available in the EMS Server Manager.
The EMS server could be defined as both NTP Client and NTP Server (for managed Gateways). In this version, the EMS NTP Client definition can support provisioning of up to 4 NTP servers.

The NBIF user is used by a Network Management system to access the ACEMS/NBIF folder, for poll backup, topology and performance monitoring data. NBIF user password management is now supported in the EMS Server Manager.

3.1.6 EMS Server North Bound Interface Changes

The EMS server has defined a new /ACEMS/NBIF folder for all the files provided for the NMS system. It includes an EMS topology definition (a list of Regions and GWs defined in the EMS application), Performance Monitoring Files and Mediant 5000 / 8000 and EMS server backup files. Detailed descriptions can be found in the document LTRT-19206 OAM Integration Guide. During the EMS server installation process, a new UNIX user ‘nbif’ is defined. This user has permission to access /ACEMS/NBIF and should be the user for this purpose.

3.1.7 Software Manager – Save file

You can now externally save files that have already been loaded to the EMS Software Manager has been added.

3.1.8 Online Help

The Online help includes links to Mediant 5000, IPmedia 5000, Mediant 8000 and IPMedia 8000 IOM Guides documents.

3.1.9 OpenCA OCSP Daemon (OCSPD)

OpenCA OCSP Daemon (OCSPD) is an RFC2560 compliant OCSP responder. It can be used to verify the statuses of MEGACO/SIP device certificates via the OCSP online protocol.

The following functionality is provided by OpenCA OCSPD:

- CRL retrieval via HTTP, HTTPS and LDAP protocols
- Support for multiple CAs (one CRL per CA)
- Periodic reload of the CRL file

3.2 Fault Management

3.2.1 Carrier-Grade Alarms System between EMS & Media Gateway’s

EMS now has the ability to synchronize with the Media Gateways on missed alarms which could occur due to Network Connectivity or other problems. EMS will retrieve these missed alarms and add them to the Alarm Browser / History windows. Upon alarms retrieval, depending on the trap forwarding rules, alarms will also be forwarded.

3.2.2 Events View in Alarm Browser

Alarms and Events are now displayed as separate graphic entities in the Alarm Browser and History screens. You can easily sort between alarms and events, or filter out events from the Alarm Browser and History windows.
3.2.3 Trap Forwarding

SNMP trap forwarding from the EMS application has been enhanced with the following features:

- Multiple Trap forwarding destinations are supported
- Media Gateway and EMS alarms and events can be forwarded in the following different types: SNMPv2 or v3 traps, Mail notifications, SMS, or Syslog messages.
- Each one of the trap destination users can filter trap forwarding according to the following trap types: (Event or Alarm);the source (EMS or Media Gateway);Alarm Severity or Media Gateway IP addresses.

3.2.4 Alarms and Journal Unified View and Filters

The user can view a combined table with all the alarms, events and journal records in order to correlate user activities with system behavior and responses. The combined view is opened from the Alarms Browser, Alarm History and Journal Frames. A unified Advanced Filter allows you to view the filter according to Time interval, GW IP address, User name or Action Type, Alarm Name, Source or Free text in Description Fields.

3.2.5 Alarm Browser and History Columns Enhancements

A new option to select viewed columns in the Alarm Browser and Alarms History window has been added. Default columns are not changed; however, in this version the user can add a new column to view the Source Description field (implemented for Mediant 5000 / 8000 Gateways and for IPmedia 5000 / 8000 Media Server products). The Source description field includes the object name as it defined by the user in the Name field in each one of the Provisioning Screens. Users can also decide to reduce the number of viewed columns. You can view the Source Description column by right-clicking on the Alarms Browser and Alarms History table’s title bars.

3.2.6 New Alarms / Events Support

A list of new alarms has been added in this version. For an updated list of alarms per GW type, refer to the relevant OAM Guide Alarms Chapter.

3.3 Security Management (EMS Server)

3.3.1 EMS Server File Integrity Checking

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported via EMS Security Events. The File Integrity checker tool runs on the EMS server machine.

3.3.2 Intrusion Detection System

The Intrusion Detection tool scans predefined Solaris system files for specific danger patterns which might indicate whether the EMS server machine was accessed and / or modified by an external intruder. Intrusion Detection problems are reported via EMS Security Events. The Intrusion Detection tool runs on the EMS server machine.
3.3.3 EMS Server Security Patches Loading During Version Installation & Upgrade

The EMS server installation now performs an installation of security patches set as part of the application install or upgrade. It will also remove unnecessary and unused Solaris packages.

3.4 Configuration Management and Maintenance

Support of new features and parameters, including new configuration and performance monitoring parameters.

3.4.1 Mediant, IPmedia 5000 / 8000 Related Features

3.4.1.1 Supported VoP Board Types

VoP board types (and application types) supported in the version are as follows:
- TP-6310 OC-3/STM-1/T3
- IPM-6310
- TP-8410

3.4.1.2 Timing Module New Features

Line timing mode is now supported for the TP8410 board.
In addition, the new ‘Advanced None’ mode has been introduced; where each TP board synchronizes its clock using one of the E1/T1 trunks. Users can provision priority for each one of the E1/T1 Trunks.

3.4.1.3 MGW and Boards Level Provisioning changes

The MGW & VoP Board Provisioning screens have been divided into the Properties and the Advanced Properties screen to allow more user friendly navigation options. For example, when you select the Advanced Properties button, you can provision the Diagnostics, Debugging and Security Settings.

3.4.1.4 Multiple Redundancy Groups

The Media Gateway now supports multiple redundancy groups definition and assignment of the VoP boards to multiple groups. Multiple Redundancy groups may be used when:
- Media Gateway boards have different hardware or application types installed in the chassis
- Media Gateway boards have different configurations, which makes it impossible to provide ‘Hot’ redundancy for all boards by a single redundancy group.

Each redundancy group has its own redundant board, accompanied by a redundant RTM module, which is capable of protecting service on a failed active board within the group.

3.4.1.5 Lock / Unlock of SC Board

New actions that enable you to reset a redundant SC board are supported: Lock / Unlock.
3.4.1.6 **Backup / Restore of the Media Gateway Configuration**

The EMS now performs automatic backup of the Gateway configuration file according to user provisioned frequency. In addition, the user now has the option to perform a random backup of the Gateway configuration.

3.4.1.7 **GW Log Files Collection**

A new option to collect Gateway log files has been added to the main status screen maintenance drop down icon. The user can select from which SC boards they wish to collect the log files (primary or secondary) and which files to collect (SC Log, Core file, VoP Boards log file and / or GW configuration file). Log files should serve customers and FAEs for troubleshooting purposes.

3.4.1.8 **TP INI file Collection**

A new option to save a TP/IPM board INI file has been added. This option is available from the main status screen by right clicking on a specific TP board. The INI file is used by customers and FAEs for troubleshooting purposes.

3.4.1.9 **SS7 Static Route Contexts support**

New provisioning and status screens have been added to support SS7 Static Route Context definition, status and maintenance.

3.4.1.10 **Performance Monitoring – Aggregated PMs support**

New Performance Monitoring parameters, aggregating all the VoP boards statistics are supported. These parameters are defined at the MGW level. For a detailed specification of the parameters list, refer to the Mediant IPMedia 5000 8000 OAM Guide Version 5.6.

3.4.2 **New Features of the Mediant 1000/2000/3000, IPM-260/IPmedia 2000/3000 and MediaPack**

3.4.2.1 **Mediant 600 Support**

A new status screen and the appropriate navigation buttons have been added for the Mediant 600. This product has the same navigation concepts and provisioning screens as the Mediant 1000.

3.4.2.2 **Mediant 3000 – Timing Module & BITs status and Provisioning**

A new status indication on the main Mediant 3000 status screen SA module representing BITs A/B and Active Source of A and B has been added. Double clicking on the BITs status represents both SAT cards, Timing Unit statuses, BITs A and B detailed statuses and PLL Lock Indications.

New provisioning parameters defining the Timing Module configuration have also been added to the Telephony Provisioning screen.

3.4.2.3 **SS7 MTP 3 Point Code Sharing**

A new set parameters enabling SS7 MTP 3 Point code sharing is supported in the Signaling Provisioning screens.
3.4.2.4 SS7 Static Route Contexts Support
New provisioning and status screens have been added to support SS7 Static Route Context definition and maintenance.

3.4.2.5 IPv6 Provisioning Support
Provisioning of IPv6 IP addresses has been added to the relevant provisioning screens.

3.4.2.6 X.509 PKI Certificates Enhancements
Support for X.509 Public Key Infrastructure. The EMS enables you to generate self-signed certificates, private files and CSR requests.

3.4.2.7 IPMedia 2000 / 3000 – Voice Prompt Repository Update
When adding a voice prompt file to the Software Manager, the EMS verifies whether there is enough available memory on the Media Gateway. If there is not enough memory, the EMS advises the user to reset the Media Gateway.

3.4.2.8 Performance Monitoring – Threshold Definitions
Performance Threshold definition is supported. When predefined thresholds are exceeded, an appropriate Alarm is issued by the Gateway and is displayed in the EMS. For example: once 'Lifetime in Seconds (Max)' has exceeded the user defined 'Lifetime High Threshold', a Threshold exceed alarm is generated.

3.4.2.9 Mediant 3000 – V5.2 Protocol Support
The ability to provision and monitor V5.2 Protocol Interfaces and Links has been added to the EMS application. In addition, a new download file type is supported. The V5.2 users file includes definitions for Port/Line numbers and L3 addresses for all the V5.2 interfaces in the Media Gateway.
4 New Features in EMS Version 5.4

4.1 General

4.1.1 EMS Server Maintenance Improvements

A new centralized tool to perform EMS server machine monitoring and management is now provided. This tool includes: automatic logs collection; networking configuration; security enabling (various types of hardening; passwords modifications and maintenance of the Solaris services (such as NTP, date and time, etc.).

4.1.2 Multiple Ethernet Interfaces on the EMS Server

The EMS server now supports up to 4 Ethernet Interfaces. It is recommended to define the Ethernet interfaces as in the following example:

- North Bound (EMS clients)
- South Bound (Media Gateways / Media Servers)
- Utility: for backup / Terminal Servers

4.1.3 Ethernet Interfaces Redundancy

The EMS server supports up to 4 Ethernet interfaces. When defining redundancy, the following is recommended:

- North Bound 1+1 – Active stand by (EMS clients)
- South Bound 1+1 – Active stand by (Media Gateways / Media Servers)

4.1.4 NTPv4 on the EMS Server

The EMS server NTP server package was upgraded to version 4. This is the latest version of the NTP package that is currently available.

4.1.5 Apache Version Upgrade

The Apache Web server running on the EMS server machine and used for JAWS and GWs Software and Auxiliary files upgrade has been upgraded to version 2.2.4.

4.2 Fault Management

4.2.1 Events Presentation and Filtering

Alarms and Events are now displayed as separate graphic entities in the Alarm Browser and History screens. You can easily sort between alarms and events, or filter out events from the Alarm Browser and History windows.

4.2.2 SNMPv3 Traps Forwarding

When defining SNMP Trap Forwarding, the user can optionally receive traps via the SNMPv3 protocol. The Default is SNMPv2c traps.
4.2.3 Trap Forwarding Enhancements

All traps received by the EMS from managed Media Gateways can be forwarded to the NMS (Network Management System) as SNMP traps. In addition, you can forward EMS alarms to the NMS.

This option enables you to determine whether to send EMS alarms and/or Media Gateway alarms to the NMS. If you have already provisioned the Gateway to send traps directly to the NMS, then in the EMS it is recommended to only send EMS alarms to the NMS (to avoid receiving the same Gateway alarms from the Gateway itself and from the EMS).

4.2.4 New Alarms Support

The entire list of new alarms added in the current version by all the Gateways is supported in the EMS. For an updated list of alarms per Gateway type, refer to the appropriate OAM Guide, Alarms Chapter.

4.3 Security Management

4.3.1 Radius Server Authentication and Authorization

The operator can perform EMS Users authentication and authorization using the Radius Server. When provisioning centralized Users Authentication, it is recommended to use the same Radius server for all the AudioCodes Gateways.

4.3.2 Welcome (Advisory) Message

A predefined Welcome message can now be defined to display in the EMS after a successful login.

4.3.3 Last Successful Login Time Display

The Last successful User login date and time are now displayed in the Title Bar of the EMS Main Screen.

4.3.4 EMS Authentication - Password Aging Provisioning

Non-radius provisioning for EMS password parameters is now available. Provisioning includes Password aging related parameters, such as password update minimal period, password validity maximal period. These parameters can now be provisioned globally per EMS application. In addition, EMS and Mediant 5000 / 8000 CLI users can now be synchronized. For more information, see EMS and CLI Users Synchronization.
4.4 Configuration Management and Maintenance

Support of new features and parameters, including new configuration and performance monitoring parameters.

4.4.1 Mediant, IPmedia 5000 / 8000 Related Features

4.4.1.1 Supported VoP Board Types

VoP board types (and application types) supported in the version are:
- TP-1610
- TP-6310 OC-3/STM-1/T3
- IPM-6310 OC-3/STM-1/T3
- TP-8410 (new board)
- IPM-8410 Video (new board)

4.4.1.2 Centralized Backup Files Collection

The EMS can now collect backup files (.bk files) that were created and locally stored on the Media Gateway and store them on the EMS server machine, thereby enabling centralize backup files location for all managed Gateways.

4.4.1.3 EMS and CLI Users Synchronization

The EMS and the Gateway CLI users can now be automatically synchronized by the EMS application. When a new user is added, removed or its password is changed in the EMS, it will be synchronized to all the managed Gateways. The user will be able to enter both the EMS and Gateway CLI with the same user and password defined in the EMS application.

4.4.1.4 Configuration Freeze Mode

A new provisioning mode called ‘Configuration Freeze’ has been defined. When this mode is enabled, configuration changes cannot be performed; however maintenance actions such as existing lock/ unlock of existing entities can be supported. This mode is recommended when Gateway provisioning is complete and the user wishes to avoid errors as a result of configuration changes. The Main Gateway status screen includes an indication when the Configuration Freeze is activated. In addition, an error message is displayed in the EMS when the user performs a configuration change when this mode is enabled.

4.4.1.5 Provisioning Frame Apply Action

Provisioning Frame Apply Action now displays a detailed description of parameters inconsistencies and errors.

4.4.1.6 NTP Servers Provisioning

Online configuration of multiple NTP servers is supported. The status of the currently selected NTP server and information regarding all the provisioned NTP servers are now displayed. In addition, you can now unlock/lock the NTP server to determine whether to use this NTP server as the synchronize clock source and enable/disable communication with a specific NTP server.
4.4.1.7 Multiple VLANs Support
The Gateway now supports separate VLANs for OAM, Control and Media. For the Media interface, up to two separate VLANS are supported.

4.4.1.8 X.509 PKI Certificates Enhancements
Support for 1X.509 Public Key Infrastructure. The EMS enables you to generate Self-signed certificates, Private files and CSR requests. In addition, files upload from the Gateway Files Status to the User workstation is now supported.

4.4.1.9 Timing Module Enhancements
Overall PSTN System Clock status is now displayed on the main Gateway status screen. Line Sync Timing Module status for the TP-6310 board and provisioning support has also been added.

4.4.1.10 ES Port Mirroring
A new debug recording tool has been added. This tool enables you to intercept traffic from the ES boards and output the traffic to a debug file.


4.4.2.1 Mediant 3000 - 8410 board including Video
A new status screen and appropriate navigation buttons have been added.

4.4.2.2 Mediant 1000 – support New Modules BRI and IPMedia
The status screen has been enhanced to display new modules and their respective statuses as well as additional provisioning options for BRI trunks.

4.4.2.3 SS7 Provisioning for Digital GWs
MTP3 levels including Redundancy mode status, maintenance actions and provisioning have been added.

4.4.2.4 Multiple VLANs (Network Separation) Provisioning Support
Multiple VLANs can now be configured for all the gateways and IP network separation.

4.4.2.5 Performance Monitoring
Real-Time and History PMs are now supported. For a detailed list of PM parameters, refer to the OAM Guide for the relevant Media Gateway product.
## Known Limitations and Workarounds

<table>
<thead>
<tr>
<th>Issue</th>
<th>Problem/Limitation</th>
<th>Comments and Workaround</th>
</tr>
</thead>
</table>
| First-time login             | Important note for first-time users (this is not a problem; however first-time users may encounter the following):  
**When logging in for the first time:**  
1. Login as user ‘acladmin’ with password ‘pass_1234’ or with ‘pass_12345’.  
2. From the main screen, open the 'Users List' (menu 'Security' > option 'Users List') and add new users according to your requirements. | -                                                                                      |
| Number of MGs in one region  | It’s recommended to define no more than 500 Media Gateways in any one region in order to derive optimal system performance.                                                                                       | -                                                                                      |
| Working with MediaPack, Mediant 1000/2000/3000 via satellite | A round trip IP network delay of up to 0.5 seconds is supported.                                                                                                                                                | -                                                                                      |
| Software Version number update after Software Upgrade | Occasionally after a Software Upgrade, or an Online Software Upgrade, the EMS status screen is not updated with the new version number.                                                                        | Select Region status on the EMS Tree panel and then select the MG again. The new version number will be updated.                                      |
| EMS Server on Linux - Limitations | 1. High Availability is not supported.  
2. SSL Tunneling is not supported.                                                                                                               |                                                                                        |
Element Management System (EMS)

Release Notes

Version 5.8

Document #: LTRT-90522