

EMS, SEM and IP Phone Management

Table of Contents

1	Managed VoIP Equipment	11
2	New Features in Version 7.2.....	13
2.1	SEM.....	13
2.1.1	New Status for Voice Quality Data Port Connections	13
2.1.2	Determining SEM-Entity Connectivity Status	13
2.1.3	Secure Connection between Front-End Server and SEM Server.....	13
2.1.4	SEM Database Storage History Provisioning.....	13
2.1.5	Session Timeout.....	13
2.1.6	Report Scheduler Enhancements.....	14
2.1.7	Link Direction	14
2.1.8	Monitoring Endpoint Devices Reporting Voice Quality with SIP Publish (RFC 6035)	14
2.1.9	SEM For Microsoft Lync Server: Add Support for Conference Calls	14
2.1.10	Users View: Saving User Information in CSV File.....	15
2.2	EMS.....	15
2.2.1	New Web Server Connections.....	15
2.2.2	CloudBond 365 and CCE Appliance Support	15
2.2.3	Automatic SNMP Configuration for Device Auto Detection	16
2.2.4	License Enhancements	16
2.2.4.1	Time Base Licensing	16
2.2.4.2	Product key Display	16
2.2.5	SBC License Pool Manager Enhancements	17
2.2.6	Enhanced SBA Information	17
2.2.7	New MSBR Maintenance Action.....	17
2.2.8	Support for MP-1288 and MP-202 Devices	18
2.2.9	Windows 10 Support	18
2.2.10	Certificate Updates Using EMS Server Manager	18
2.2.11	EMS Client Launching Screen.....	18
2.2.12	New Managed Product Type - MTC (Media Transcoding Cluster)	18
2.2.13	SBC License Pool-Management of SBC Devices.....	19
2.2.14	Support for MEGACO Version 6.6 Devices	19
2.2.15	Summary Display of all EMS Licenses	19
2.2.16	LDAP Server SSL Connection.....	19
2.2.17	Automation of User-Defined SSL Certificate Installation	19
2.2.18	Certificate Store.....	20
2.2.19	Session Timeout.....	20
2.2.20	Support for New Call Statistics PMs	20
2.2.21	SBC License Pool	20
2.2.21.1	HA Devices	22
2.2.22	Devices Backup / Restore Improvements	22
2.2.23	Faults: Changes for Operator and Monitoring Security Levels	22
2.2.24	Client Software Signing by Trusted Certificate Provider.....	23
2.3	IP Phones Management	24
2.3.1	Full HTTPS Support for Endpoints Connections	24
2.3.2	Browser Redirect.....	24
2.3.3	Support for Management of the HD 450 Phone.....	24
2.3.4	Endpoint License Enforcement.....	24
2.3.5	Exporting Device Statuses to CSV File.....	24
2.3.6	Updating Firmware	24

2.3.7	Regions Support.....	25
2.3.8	Provisioning Phones with Regional Files (Zero Touch).....	25
2.3.9	Add Line URI to Device Status Page.....	25
2.3.10	Show only Updated Device Status on Dashboard.....	25
2.3.11	Enhanced Dashboard.....	25
2.3.12	Disconnect Timeout.....	26
2.3.14	Support for Managing Phones Inside the NAT Network Using SBC HTTP Proxy.....	26
2.3.15	Option to Provision EMS Server FQDN.....	26
2.3.16	Option to Edit the Initial DHCP Option 160 Cfg File.....	27
2.3.17	Show Registered Phones in the Users List.....	27
2.3.18	Open IPPhone Web interface with HTTPS.....	27
3	New Features in Version 7.0.....	28
3.1	SEM.....	28
3.1.1	Bandwidth and Concurrent Calls Alerts.....	28
3.1.2	Network page Map View per Operator (Multi-Tenancy).....	28
3.1.3	New Capability to Change Password.....	28
3.1.4	SEM Monitoring of Microsoft Lync Calls.....	28
3.1.5	New Microsoft Lync Devices and Network Map.....	28
3.1.6	Lync Calls in Network, Statistics & Report Views.....	29
3.1.7	Lync Calls Display in the Calls List and Call Details.....	29
3.1.8	Users View.....	29
3.1.9	SEM-Defined QoE Threshold Profiles.....	30
3.1.10	Server Storage.....	31
	3.1.10.1 Storage Level Configuration.....	31
	3.1.10.2 SEM Performance and Data Storage.....	32
3.1.11	Concurrent Calls Statistics.....	32
3.1.12	SEM Licensing Enhancements.....	33
3.1.13	SEM Actions Updated to the EMS Actions Journal.....	33
3.2	IP Phones Management.....	34
3.3	EMS Features.....	35
3.3.1	Single Sign-On.....	35
3.3.2	Auto-Provisioning.....	35
3.3.3	Trap Forwarding: Extended Filtering Criteria.....	35
3.3.4	Alarm Suppression Mechanism.....	36
3.3.5	Different Sounds per Alarms Severity.....	36
3.3.6	Alarm Details Screen Enhancements.....	36
3.3.7	Topology File Enhancements.....	37
4	New Features in Version 6.8.....	38
4.1	General.....	38
4.1.1	Improved/Enlarged Capacity of Managed Products.....	38
4.1.2	New Hardware Requirements.....	38
4.1.3	New Products Management.....	38
4.1.4	Virtualized EMS Server on HyperV.....	38
4.1.5	Supporting High Availability in Virtualized Solutions.....	38
4.1.6	EMS Client Support on Windows 8.....	39
4.1.7	EMS Server: Server Manager Improvements.....	39
4.2	EMS New Features.....	39
4.2.1	Security: Integration with LDAP Server for User Authentication and Authorization.....	39

4.2.2	Devices Configuration Backup and Data Synchronization	39
4.2.3	Performance Management Extensions.....	39
4.3	SEM New Features	40
4.3.1	Improvements in SEM Performance and Data Storage	40
4.3.2	New SEM Licensing Mechanism	40
4.3.3	Support New Link Types between Devices.....	41
4.3.4	New Links Table in Network View	41
4.3.5	SEM Application Multi - Tenancy.....	41
4.3.6	Scheduled Reports.....	42
4.3.7	Calls List: Add Calling Name Information.....	42
4.4	Changes from the Previous Version.....	42
5	Known Limitations and Workarounds.....	43

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: April-06-2017

WEEE EU Directive

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

Customer Support

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

Related Documentation

Manual Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Element Management System (EMS) Server Installation, Operation and Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) OAM Integration Guide
Element Management System (EMS) User's Manual
SEM User's Manual
IP Phone Management Server Administrator's Manual
IP Phone Manager Express Administrator's Manual
OVOC Security Guidelines
Element Management System (EMS) Online Help
Mediant 500 Gateway and E-SBC and MP-1288 Performance Monitors and Alarms Guide
Mediant 500 and Mediant 800 Gateway and E-SBC Series and MP-1288 Performance Monitors and Alarms Guide
Mediant 800 Gateway and E-SBC Mediant Software SBC CloudBond 365 and CCE Alarms Guide
Mediant 1000B Gateway and E-SBC Performance Monitors and Alarms Guide
Mediant 2600-4000-9000-SW SBC Series Performance Monitors and Alarms Guide
Mediant 3000 with TP-6310 Performance Monitors and Alarms Guide
Mediant 3000 with TP-8410 Performance Monitors and Alarms Guide
Mediant MSBR Series OAMP Guide

Document Revision Record

LTRT	Description
90535	Initial document release for Version 7.2.
90536	<p>SEM: Determining SEM-Entity connectivity status; securing connection between Front-End Server and SEM Server; SEM Database storage history provisioning; new session timeout mechanism; Report Scheduler enhancements; link direction configuration.</p> <p>EMS: EMS Client launching screen; New Managed Product Type - MTC (Media Transcoding Cluster); SBC License Pool-Management of SBC devices; support for MEGACO Version 6.6 devices; summary display of all EMS licenses; LDAP server SSL connection enhancements; automation of User-Defined SSL certificate installation; Certificate Store updates using EMS Software Manager; new session timeout mechanism and support for New Call Statistics PMs.</p> <p>IP Phone Manager: Regions support; Provisioning Phones with Regional Files (Zero Touch); adding line URI to Device Status Page; showing only updated device Status on dashboard; enhanced dashboard and disconnect timeout.</p>
90537	<p>SEM: New Status for Voice Quality Data Port Connections</p> <p>EMS: Time License; SBC License Pool Manager Enhancements; Enhanced SBA Information; Support for MP-1288 and MP-202 devices; support for Windows 10; Certificate Updates using EMS Server Manager</p> <p>IP Phone Manager: Endpoint License Enforcement; Telnet Debugging; Exporting Device Statuses to CSV File; Updating Firmware when managing multiple devices.</p>
90538	<p>EMS: CloudBond 365 and CCE Appliance support; support for MediaPack MP-124 Rev. D and E.</p> <p>IP Phone Manager: HTTPS Support for Endpoints REST connection.</p>
90541	<p>EMS: Single Sign-on to device's Web interfaces is not supported if the devices are located behind a NAT.</p>
90542	<p>EMS: Further update for the issue described above; Single Sign-on to device's Web interfaces is not supported if the devices are located behind a NAT.</p>

Documentation Feedback

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

This page is intentionally left blank.

1 Managed VoIP Equipment

The following products (and product versions) can be managed by this EMS / SEM release:

- Mediant 9000 SBC – versions 7.2 (including support for MTC), 7.0, 6.8
- Mediant 4000 SBC – versions 7.2, 7.0, 6.8
- Mediant 4000B SBC – version 7.2, 7.0
- Mediant 2600 E-SBC – versions 7.2, 7.0, 6.8
- Mediant 2600B E-SBC – version 7.2, 7.0
- Mediant Server Addition (SE) SBC – versions 7.2, 7.0 and 6.8
- Mediant Virtual Addition (VE) SBC – versions 7.2 (**including support for MTC**), 7.0 and 6.8
- Mediant 3000 Media Gateways (TP-8410 and TP-6310) – versions 7.0 (SIP), 6.8 (SIP) and 6.6 (SIP and MEGACO)
- Mediant 2000 Media Gateways – version 6.6
- *Mediant 1000 Gateway – version 6.6 (SIP and MEGACO)
- Mediant 1000B Gateway and E-SBC – versions **7.2** 7.0, 6.8 and 6.6
- Mediant 1000B MSBR – versions 6.8
- Mediant 800B Gateway and E-SBC – versions **7.2** 7.0, 6.8 and 6.6
- **Mediant 500 E-SBC** – version **7.2**
- **Mediant 500L E-SBC** – version **7.2**
- Mediant 800B MSBR – versions **7.2**, 6.8 and 6.6
- *Mediant 600 – version 6.6
- Mediant 500L MSBR, Mediant 500 MSBR – version **7.2**, 6.8
- MediaPack MP-11x series – version 6.6 (SIP and MEGACO)
- MediaPack MP-124 Rev. **D** and **E** – version 6.6 (SIP and MEGACO)
- **MP-20x B** – version **7.2**
- **MP-1288** – version **7.2**
- *Mediant 800B SBA, *Mediant 1000B SBA, and *Mediant 2600B SBA devices with SBA version 1.1.12.x and above and gateway versions **7.2**, **7.0**, 6.8
- 400 HD Series: from version 2.0.13 (Skype for Business) and from version 2.2.2 (Non-Lync): 420HD, 430HD and 440HD and 405.
- 400 HD Series from version 3.0 (Skype for Business): **450 HD**
- **CloudBond 365 Series**: version **7.4**: Standard Edition (Mediant 800B platform); Standard Plus Edition (Mediant 800B platform); Pro Edition (Mediant Server platform); Enterprise Edition (Mediant Server platform); Virtualized Edition (Mediant Server platform).
- **Mediant 800 CCE Appliance** and **Mediant Server CCE Appliance** ¹

¹ Contact AudioCodes regarding version support for these products.

**Note:**

- * Refers to products that are not supported by the SEM.
- All versions VoIP equipment work with the SIP control protocol.
- **Bold** refers to new product support and version support.

2 New Features in Version 7.2

2.1 SEM

2.1.1 New Status for Voice Quality Data Port Connections

A new icon for the SEM entity connectivity status indicates when an AudioCodes device entity (e.g., SBC) hasn't sent voice quality data to the SEM because connectivity with the entity couldn't be established. A new tooltip also summarizes the status.

2.1.2 Determining SEM-Entity Connectivity Status

The SEM's Network page's Map view view provides new color icons and tooltip descriptions to represent different connectivity statuses. The Network page's Table view also shows these connectivity statuses for a managed device. The following connectivity statuses are shown:

- A successful initial connection has been established with an AudioCodes entity (e.g., SBC).
- A successful initial connection has been established with a Microsoft Lync entity.
- A connection cannot be successfully established with an AudioCodes entity.
- A connection cannot be successfully established with a Microsoft Lync entity.
- A device is not configured to send voice data to the SEM.
- The connection with the SEM server cannot be established.

2.1.3 Secure Connection between Front-End Server and SEM Server

The connection between the Front End server and the SEM can now be secured using SSL. When adding a Microsoft Lync device, you can choose to secure the connection with an SSL handshake with or without certificate authentication.

2.1.4 SEM Database Storage History Provisioning

You can now purge the call statistics data according to the configurable number of storage days that are allowed per network dimension. When exceeded, the oldest call statistics data are purged from the database to free space.

2.1.5 Session Timeout

'Session Timeout Period' is configured in the EMS (see above). If the period configured lapses, the SEM session with the EMS server is dropped and users are prompted again for username and password. After logging in again, the session is restarted.

Every time a user interacts with the SEM application (e.g., by clicking a menu), the session timeout is reset. When interaction with the application does not occur for the period configured for this parameter, the session is dropped and the user is prompted to log in again.

2.1.6 Report Scheduler Enhancements

When you use the **Scheduled Reports** feature to schedule a report all columns that feature in the report type's page are included by default in the report.

2.1.7 Link Direction

You can now configure the direction of the port link between the source and the destination device. For example, when the link is configured as 'Bi Directional', this indicates that a bi-directional port is used for this connection.

2.1.8 Monitoring Endpoint Devices Reporting Voice Quality with SIP Publish (RFC 6035)

The SEM application now supports endpoint devices reporting call quality using SIP Publish message according to compliance with RFC 6035. This integration was made with AudioCodes IP Phone models 420, 430 and 440 starting version 2.2.0.

Endpoints are added to the SEM application automatically after the first time that SIP Publish messages are sent to the SEM server.

The Endpoint devices status is displayed in the Network Table view under new navigation button 'Endpoints'.

The Statistics screen has been extended with an Endpoints statistics view and summary. The Calls List screen retrieves all the calls reported by the Endpoint devices. These calls are indicated with a new icon, and include a link to view Call Details.

2.1.9 SEM For Microsoft Lync Server: Add Support for Conference Calls

The SEM has been enhanced to display and analyze Microsoft Lync Conference calls. Each conference call participant is counted and displayed as a separate call in the Calls list, including voice quality information and other call related details. The Monitoring Endpoint type for these calls is indicated as 'MS Lync Conference', and each call can be of one of the following Media Types: Voice & Video, Chat or Screen sharing.

The conference participant name is shown in the 'Caller' column of the Calls List table. In order to find and aggregate all the participants and stream types, it is suggested to filter the table according to the 'Conf ID' reported in the 'Callee' column. The 'Conf ID' for all the participants of the same conference call is the same.

The SEM application uses the Microsoft Lync ConferenceSessionDetailsView Monitoring Server report to retrieve the Lync conference calls.

2.1.10 Users View: Saving User Information in CSV File

The Users View now includes a new option to export the Users information and statistics into the CSV file.

2.2 EMS

2.2.1 New Web Server Connections

You can now open and close the following port connections from the EMS Server Manager Web Server menu item:

- IPPs FILES (Port 8080): this HTTP port is used for downloading firmware and configuration files from the EMS server to the endpoints.
- IPPs HTTP (Port 8081): this HTTP port is used for sending REST updates from the endpoints to the EMS server, such as alarms, alerts and statuses.
- IPPs HTTP (Port 8082): this HTTPS port is used for sending secure REST updates from the endpoints to the EMS server, such as alarmss and statuses (HTTPS without certificate). For more information, see Section 2.3.1.

2.2.2 CloudBond 365 and CCE Appliance Support

The EMS now supports the status monitoring and license pool management for the CloudBond and CCE Appliance product series. You can monitor the components of the CloudBond and CCE Appliance platforms including the Domain Controller, Front End and Edge Server. In addition, new alarms have been added to support this feature (refer to the *Mediant 800 Gateway and E-SBC Mediant Software SBC CloudBond and CCE Alarms Guide*).

When both the CloudBond 365/CCE Appliance and SBC applications are installed on the same device, you can also monitor the SBC components including Reverse Proxy, Host and SBC. Executable actions such as uploading files to the device are not supported for these products.

In the License Pool, you can configure the following license parameters for the CloudBond 365 or CCE Appliance products:

- CB users- the maximum number of CB user sessions that can be managed.
- CB PBX users – the maximum number of PBX users that can be managed.
- CB Analog devices (for future use)
- CB Voicemail accounts – the maximum number of voicemail accounts that can be managed.

2.2.3 Automatic SNMP Configuration for Device Auto Detection

Devices can now be automatically connected to EMS using Auto Detection for both SNMPv2 and SNMPv3 configurations using the following default credentials:

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

If different credentials to the default values described above are configured on the device, then the device is added to the EMS as "Unknown" until these credentials are updated in the MG Information screen.

2.2.4 License Enhancements

2.2.4.1 Time Base Licensing

The EMS and SEM license may control the time period for which the product can be used. When the time license is enabled and the configured license time expires, The connection to the EMS/SEM server is denied. The time based license affects all the features in the EMS and SEM including the SBC License Pool, EMS for IP Phones and SEM. The License menu in the EMS Server Manager has been updated as follows:

- The License Status and the Expiration Date are displayed in the License menu in the EMS Server Manager; for example, the 'License Status' field displays "Enabled" and the 'Expiration Date' field displays "09:05:57 May 15 2016".
- In the absence of a configured expiration date, the 'Expiration Date' field displays "Unlimited".

When the EMS server time license approaches its expiration date, an appropriate warning alarms are issued.

The timezone is determined by the configured date and time in the Date & Time menu in the EMS Server Manager.

The time-based license is used for POCs and SORs.

2.2.4.2 Product key Display

The Product Key string is displayed in the license menu information. This string represents the customer order for the EMS and SEM products. For more information, contact your AudioCodes partner.

2.2.5 SBC License Pool Manager Enhancements

The following enhancements have been made to the SBC License Pool Manager:

- Hitless license upgrades can now be performed in the SBC License Pool Manager using the 'Apply Hitless License' right-click option. This option is only supported for SBC HA devices. The Hitless mechanism enables the license update to be performed using the HA switchover mechanism without the need to perform a device reset and therefore not affecting the device's current traffic (maintaining active calls) New statuses have also been added for this feature.
- A new column 'Require Action' has been added. This column displays icons that represent the recommended actions that should be performed by the user. For example, the 'Configuration' icon indicates that the device license needs to be updated.
- The Status column now includes new status icons. Each icon either represents the required action corresponding to the action that is described in the 'Require Action' column or represents a status update. Yellow icons are displayed for the most critical statuses (Reset Needed, Apply Needed, License Fail) and red icons are displayed when the user configured pool value exceeds the available license pool allocation and for indicating the Last Request Time.
- A new information dialog displays a legend which describes the main fields in the License Pool Manager (accessed from the Toolbar).

2.2.6 Enhanced SBA Information

The 'SBA Description' field has been added to the SBA Module information in the MG Information screen. This field identifies the SBA that is configured on the device's OSN server. This information is also displayed in the Additional info field in the 'SBA Services Status' and the 'GW Connection Alarm' alarm. The following new alarms have been added:

- CPU Status alarm-indicates the status of the SBA server's CPU. When a pre-defined threshold approaches or is reached, the appropriate alarm is raised.
- Memory threshold alarm-indicates the status of the SBA server's memory. When a pre-defined threshold approaches or is reached, the appropriate alarm is raised.
- SBA diskspace alarm-indicates the status of the SBA servers diskspace. When a pre-defined threshold approaches or is reached, the appropriate alarm is raised. This alarm also includes the disk drive source e.g. drive C in the varbind text.

2.2.7 New MSBR Maintenance Action

For MSBR devices, a new maintenance action allows you to upload the results of the of the latest CLI script file to your PC. The operator can use this file to investigate the results of the CLI script download especially when this operation was not successful. The file includes the results for each CLI action performed using the last downloaded CLI script.

2.2.8 Support for MP-1288 and MP-202 Devices

The EMS now supports the management of the MP-1288 and MP-20x devices. New alarms have been added as part of the support for the MP-1288 device (refer to the *Mediant 500 E-SBC and Mediant 800 Gateway and E-SBC Performance Monitors and Alarms Guide*).

2.2.9 Windows 10 Support

The EMS PC client can now be run on the Windows 10 platform.

2.2.10 Certificate Updates Using EMS Server Manager

The EMS Server Manager option for updating SSL certificates has been changed as follows:

- The option for generating client certificates has been removed (option has been renamed 'Server Certificates Update').
- A new option has been added for updating the Client Java Web Start certificates. This option is relevant in the following circumstances:
 - You are running the JAWS client.
 - You are using non-default certificates.
 - You have upgraded the EMS server
- If you are running the EMS PC client, you still need to copy the new Keystore file to the EMS client installation directory after you have generated the new server certificate (as was previously required).

2.2.11 EMS Client Launching Screen

The EMS client can now be launched directly from a web browser by simply entering the EMS server IP address. A new launching page is then displayed with a link to open the EMS login screen in a single click. .

2.2.12 New Managed Product Type - MTC (Media Transcoding Cluster)

A new product type "MTC" has been added for supporting a transcoding cluster. This product type is relevant for the Mediant 9000 and Mediant Software SBC products. The status screen for the above mentioned products when configured for this feature displays the MTC Current Utilization and the HA Usage and HA Status: for the Media Transcoders that are configured in the cluster.

2.2.13 SBC License Pool-Management of SBC Devices

The License Pool manager has been extended with the capability to configure the number of SBC devices that can be managed by the license pool.



Note: The license keys that are required to support this feature and the other license parameters should be purchased from AudioCodes. For more information, contact your AudioCodes representative.

2.2.14 Support for MEGACO Version 6.6 Devices

This version supports the following MEGACO products for backward compatibility:

- MediaPack
- Mediant 1000
- Mediant 3000 with TP-6310
- Mediant 3000 with TP-8410

2.2.15 Summary Display of all EMS Licenses

The EMS Server Manager License menu option displays separate summaries for the purchased licenses managed by the License pool, including the following:

- **Licenses managed by the EMS** - the number of SBC devices, the number of SBC sessions, the number of SBC user registrations, the number of SBC transcoding sessions and the number of SBC signaling sessions .
- **Licenses managed by the IP Phone Manager** – the number of IP phones that can be managed.
- **Licenses managed by the SEM** - the number of devices, the number of IP Phones, the number of simultaneous call sessions and the number of users.

2.2.16 LDAP Server SSL Connection

The connection between the EMS and an LDAP server (for user authentication and authorization) can now be secured using SSL certificates.

2.2.17 Automation of User-Defined SSL Certificate Installation

The procedure for installing user-defined SSL certificates has now been automated using the EMS Server Manager.

2.2.18 Certificate Store

A new option enables the loading of SSL certificate files using the EMS Software Manager "Certificate File". When such files are loaded using this option, they are added to the EMS server keystore. Previously, when loading certificate files using the X509 Private Key File, X509 Server Certificate File and X509 Trusted Root Certificate File options, the keystore was not updated. When certificate files are loaded using this option, they can be used to authenticate an LDAP server and AudioCodes device (for Single-Sign On to the device's embedded Web server).

2.2.19 Session Timeout

A new session timeout mechanism has been implemented for measuring user inactivity period. This timeout is a mechanism is used for releasing unutilized server resources. It applies to the EMS, SEM and IP Phone Manager applications.

2.2.20 Support for New Call Statistics PMs

The following new PMs for calculating various call statistics are supported in this release:

- ASR (per device / IP Group / SRD)
- ACD (per device / IP Group / SRD)
- NER (per device / IP Group / SRD)
- Number of LAD legs (per device)
- Inbound CAPS (per device / IP Group / SRD)
- Outbound CAPS (per device / IP Group / SRD)

2.2.21 SBC License Pool

A new feature called "License Pool Manager" is available in the EMS. This feature enables operators to centrally manage and distribute SBC sessions licenses for multiple devices using a flexible license pool. This feature is relevant for devices running version 7.0 and above. The operator can allocate and de-allocate the licenses for the devices in the pool according to their capacity requirements. This feature delivers the following benefits:

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

The License Pool feature does not require a new License key file per device from AudioCodes each time the user wishes to apply different settings to each device.

- Enables service providers to manage licenses for multiple customers by using the license pool to globally allocate licenses between them.



Note: License pool configuration changes are offline and therefore require a device reset to take effect.

The operator can manage the following SBC license parameters using the 'License Pool':

- SBC Sessions (media and signaling)
- SBC Transcoding
- SBC Registrations (number of SIP endpoints that can register with the SBC)
- SBC Signaling

In order to generate the initial SBC License Pool, you must load the appropriate license to the EMS using the EMS Server Manager. This license should include the total pool numbers.

The License Pool Manager Interface displays the total number of pool licenses available for each SBC license category and for each device displays the number of pre-loaded "local" licenses and the incremental licenses "pool" licenses that are added in the License Pool Manager.

A summary pane with bar charts illustrates the percentage of utilized and free licenses for each of the above SBC categories.

All the user actions performed in the License Pool Manager are shown as EMS journal entries and the relevant alarms that are sent from the device are displayed in the Alarms Browser.

Communication between the device and the EMS License Manager is over SNMP and REST with an HTTPS connection. A designated user is configured on the EMS for securing this connection.

If the device cannot connect to the EMS port used for REST communication for seven days then the device license expires and the device is automatically reset with its initial SBC license. This mechanism prevents the misuse of the issued licenses. Consequently, it is recommended to use EMS HA schemes as described in the *EMS IOM* manual.

2.2.21.1 HA Devices

For devices configured with HA systems, the License Pool Manager divides an equal number of SBC pool licenses between the active and redundant devices. For example, if the License Pool Manager Server allocates 200 sessions to the active device, it also allocates 200 sessions to the redundant device. Consequently, customers must take this into consideration when ordering licenses. For more information, contact your AudioCodes representative.

2.2.22 Devices Backup / Restore Improvements

The MG Backup Manager screen has been enhanced with a new MG Backup Summary tab, which displays a summary line for each device including the following information:

- The number of files that have been backed up from the device to the EMS.
- The date of the last backup file.
- Device display according to Region and Product Type.
- Last backup status e.g. Successful.

The following actions are available for each device:

- A link to detailed information of the latest file that was backed up from the device.
- An option to upload the latest configuration files from the device.
- An option to restore or download the latest backup file to the device.
- A filter for displaying backup file information for specific devices.

The Backup Settings are now available via the Settings icon in the Tool bar.

The Backup Files tab displays all backup files that have been saved to the MG Backup Manager. This screen includes the same functionality as the previous version.

2.2.23 Faults: Changes for Operator and Monitoring Security Levels

The EMS Alarms browser now displays alarms according to the security level of the administrator as follows:

- Operators with "Operator and Monitoring" security levels can view those alarms for devices in their managed Region. For example, 'Topology event', 'Proxy Connection Lost' and 'GW Connection Alarm'.
- Only Operators with "Admin" or "SuperAdmin" security levels can view system alarms. For example, 'Disk Space' alarm, 'EMS Server Started' or 'Security Event' alarms.

2.2.24 Client Software Signing by Trusted Certificate Provider

The EMS client software (jars) are signed using the komodo Trusted Certificate Authority.

The EMS client now conforms with Java's security limitations, which allows the user to launch the EMS client via Java Web Start without adding the EMS server to Java's "Exception Site List". See the following link:

http://docs.oracle.com/javase/8/docs/technotes/guides/deploy/exception_site_list.html

2.3 IP Phones Management

2.3.1 Full HTTPS Support for Endpoints Connections

The REST connection that is used for sending REST updates such as alarms and statuses from the endpoints to the EMS server can now be secured over HTTPS (via port 8082). This connection implements SSL encryption (encrypting data using AudioCodes default certificates) without certificate authentication.

If you replace the default AudioCodes certificates on the EMS server with custom certificates, this does not affect the HTTPS connection between the endpoints and the EMS server i.e. data is still encrypted using the default certificates.

To enable this connection, you need to enable the option in the IP Phone Management server (in the System Settings screen). The 8082 port connection is open by default and can be closed using the EMS Server Manager (in the Web Servers menu).

The downloading of firmware and configuration files from the EMS server to the endpoints is also supported over HTTPS (port 443).

2.3.2 Browser Redirect

The IP Phone Management Server URL is now automatically redirected from HTTP to HTTPS when accessed from the EMS or directly from a Web browser.

2.3.3 Support for Management of the HD 450 Phone

This release supports the 450HD phone model.

2.3.4 Endpoint License Enforcement

- The number of endpoints that can be managed by the IP Phone Manager and the SEM management is controlled by the license that is loaded to the EMS server. When the number of endpoints currently running on the SEM server (Management of endpoints in the SEM) or the number of endpoints running on the EMS server (Management of Endpoints in the IP Phone Manager) approach license capacity, the appropriate warning alarms are raised according to the percentage utilization of the license; the alarm source (SEM or EMS server) is also indicated in the alarm.
- The use of the endpoint licenses is globally overridden according to the Time License as described above in Section 2.2.4.

2.3.5 Exporting Device Statuses to CSV File

A new option has been added to the Device Status page to export the current device status entries to a CSV file for the management; for obtaining a list of phone MAC address or Serial Numbers,

2.3.6 Updating Firmware

A new action is now available from the Manage Multiple Devices page to update device firmware.

2.3.7 Regions Support

IP Phones can now be managed in regions (as exists for AudioCodes devices managed in EMS and SEM). The IPP Management administrator can be assigned the appropriate security level in the EMS User's list (Monitoring, Operator and Not Visible). Users that are not assigned to a Region will be managed with the "Super Admin" security level. This feature is significantly useful for SP's and large enterprises that typically use EMS to manage phones that are located in different regions.

2.3.8 Provisioning Phones with Regional Files (Zero Touch)

Administrators can now automatically provision phones in different regions using regional template files. Upon the initial connection to the EMS, the phones download their respective firmware models and regional definitions, and then later when the user signs-in, the system automatically adds the user and phone and loads its private CFG file. This feature is enabled using the Region URL in the DHCP option 160 rather than the System URL. This method of provisioning phones using the Region URL is called Zero Touch provisioning.

This feature enhances the implementation of Region Support (as described above). The Zero Touch feature significantly accelerates uptime by enabling multiple users and phones to automatically be added to the server.

You can also optionally configure the Regional URL to retrieve files using an SBC HTTP proxy server. This feature is especially useful for customers whose EMS is installed in the cloud, or when the phones are located behind a NAT.



Note: This feature is supported for all phones with sign-in capabilities i.e. Microsoft Lync.

2.3.9 Add Line URI to Device Status Page

The line URI has been added to the Device status page for each user record.

2.3.10 Show only Updated Device Status on Dashboard

The dashboard short status list now shows only the latest updated status and not the latest reported statuses.

2.3.11 Enhanced Dashboard

The dashboard has been enhanced to display the following information in pie-charts:

- Number of users per Region
- Number of devices per model
- Number of devices per firmware

2.3.12 Disconnect Timeout

The IP phone reports its status to the EMS server every hour. If it does not report its status before the 'Disconnect Timeout' lapses, the status changes from Registered to Disconnected and the phone's 'Status' column in the Devices Status screen is red-coded.

2.3.14 Support for Managing Phones Inside the NAT Network Using SBC HTTP Proxy

Phones residing behind a NAT with internal IP addresses can now be managed by the EMS via AudioCodes SBC HTTP proxy server. In this scenario, requests are sent to and from the Proxy server from the EMS and the phones using REST over HTTPS.

2.3.15 Option to Provision EMS Server FQDN

When a REST connection request is sent from the phones to the EMS, an FQDN can be used to connect to the EMS server instead of an IP address. The FQDN may be useful, for example, when the EMS server is moved due to organizational changes within the enterprise, and consequently all phones are disconnected from it.

2.3.16 Option to Edit the Initial DHCP Option 160 Cfg File

The DHCP Option 160 string can be configured in a unique format for the following scenarios:

- Connecting directly from the phones to the EMS.

For example: `http://<EMS IP address>/firmwarefiles;ipp/dhcpcoption160.cfg`

- Connecting from the phones to the EMS via an HTTP proxy server.

For example:

`http://<Proxy SBC IP address><Proxy SBC Port>/firmwarefiles;ipp/httpproxy.cfg`

2.3.17 Show Registered Phones in the Users List

The Manage Users screen now displays an icon indicating whether a user is registered. When this icon is clicked, comprehensive device information, such as the device's MAC address and ID is displayed.

2.3.18 Open IPPhone Web interface with HTTPS

The IP Phone Manager interface can now be opened in a Web browser with an HTTPS connection (HTTPS port 443). This feature must be enabled using the EMS Server Manager.

3 New Features in Version 7.0

3.1 SEM

3.1.1 Bandwidth and Concurrent Calls Alerts

The SEM now supports the following alarms/rules:

- Bandwidth Alarm – this alarm is sent when the media bandwidth falls below, or exceeds, minimum or maximum threshold values (kbps), which users can configure in a rule. Minimum: 0. Maximum: 1000000 (1Gbps).
- Maximum Concurrent Calls Alarm – this alarm is sent when the number of concurrent calls falls below, or exceeds, minimum or maximum threshold values, which users can configure in a rule. Minimum: 0. Maximum: 100000.

3.1.2 Network page Map View per Operator (Multi-Tenancy)

The SEM's Network page Map view (in which users can drag and drop and reposition entities) now supports topology view per operator. Now, users whose security level is non-admin/superadmin can change entity locations and save the modified topology in their local browser for later viewing. By contrast, the user whose security level is admin/superadmin can modify entity locations; however, when the changed topology is saved, it's saved in the database, and the last save determines the topology view for all users.

3.1.3 New Capability to Change Password

Users can now change their password using the SEM interface.

3.1.4 SEM Monitoring of Microsoft Lync Calls

In this version, the SEM application has been extended to display VoIP calls from the Microsoft Lync Server. Now, in the Network map, users can define all the major Microsoft Lync-related components (Front End, Edge, SBA and Mediation servers) and their connecting links.

3.1.5 New Microsoft Lync Devices and Network Map

Once the Lync components have been added to the Network map, the SEM server connects to the Microsoft Lync QoE server, retrieves the call quality-related data, and then represents this information in the Microsoft Lync and AudioCodes device icons in the Network map. The user can then view the calls success / failure rate, and the call quality statistics distribution over all the Lync components. In addition, new types of links are supported for Lync devices. The Device Actions and Link Actions are identical to the actions used for AudioCodes devices.

3.1.6 Lync Calls in Network, Statistics & Report Views

Lync devices in the Network, Statistics and Reports views are displayed identically for AudioCodes and Microsoft Lync entities. All functionalities, views and filters are identical.

3.1.7 Lync Calls Display in the Calls List and Call Details

A new field 'Call Source ' indicates whether the source of the call is from Lync or from an AudioCodes device. In each case, the respective icon is displayed. The call details provide different sets of information which is relevant for each respective component i.e. calls from Lync and calls from AudioCodes devices.

3.1.8 Users View

A new SEM view 'Users' enables the management of Active Directories organization users. Once the Active Directory is defined in the SEM, it is synchronized with the SEM database and then all the registered users are retrieved. You can then manage the telephony experience from this retrieved list of the enterprise's Active Directory listed employees.

This view comprises the following tabs:

- User Experience – this tab shows the quality of experience for each AD user. For example, the number of calls the employee made during the time period and the total amount of time the employee spoke on their phone during the time period.
- User Details – this tab lists personal contact details of the user including phone numbers and email.
- Active Directories – lists the Active Directories where the organization users are defined. For example, host and server details. In addition, the AD database Sync times are also displayed.

SEM automatically synchronizes with Active Directories according to a user-configured Sync time scheduling interval. In addition, the user may also randomly perform the Sync operation.

The 'User's Experience' and 'User's Details' tabs include a powerful feature which enables the following:

- Viewing call statistics for the user including charts and data tables (similar to the display in the Statistics view). For example, the ratio of successful calls to failed calls and the ratio of calls whose voice quality was Good, to those calls whose voice quality was Fair, Poor and Unknown.
- Making Lync calls and as a result, view the statistics for these calls in real-time.
- Sending Lync messages and sending emails.
- Managing other user details, such as User's details and Lync User details.

3.1.9 SEM-Defined QoE Threshold Profiles

The Utilities view now includes a new tab 'QoE Thresholds'. In this tab, the user can apply QoE Threshold profiles for voice quality metrics (MOS, Delay, Packet Loss, Echo and Jitter). The QoE Threshold profile consists of threshold values set for each of these metrics for the following different call quality categories: 'Poor', 'Fair' and 'Good'. This feature includes the following three pre-defined profiles:

- Low Sensitivity Threshold – pre-defined threshold values representing recommended data for the 'Low' sensitivity level.
- Medium Sensitivity Threshold – pre-defined threshold values representing recommended data for the 'Medium' sensitivity level.
- High Sensitivity Threshold – pre-defined threshold values representing recommended data for the 'High' sensitivity level.

In addition, the user can optionally define their own custom profile in which they can manually define threshold values and include or exclude specific metrics. For example, the user can define values for excluding the definition of threshold values for MOS, Delay and Echo; however, exclude 'Packet Loss' and 'Jitter' metrics from the profile. Once you define the profile, you can do the following:

- Save and attach it to specific devices and/or links.
- Save and attach it to all devices and links.

The saved profile can then be optionally set as the default profile for specific or all devices and/or specific or all links.

3.1.10 Server Storage

The Utilities view now includes a new tab 'Server Storage'. In this tab, the user can view SEM server storage capacity and configure specific parameters for optimizing database storage. The following information is displayed in this tab:

- **Calls Details Storage** – Represents detailed information per call (stored according to the number of days). This information represents actual call records (as displayed in the 'SEM Calls' view). The call details storage capacity is shown in the table below. Once this storage level reaches its full capacity, the oldest call details data is purged from the database to free space.
- **Calls Statistics Storage** – Represents statistic information storage (stored according to the number of days with intervals). This information represents statistics calculations that are associated with each call (as displayed in the 'Network', 'Statistics' and 'Reports' tabs). The Calls statistics storage capacity is shown in the table below. Once this storage level reaches its full capacity, the oldest call statistics data is purged from the database to free space.

3.1.10.1 Storage Level Configuration

A new configuration pane for setting the Storage Level Configuration is now provided. In this pane, you can determine the composition and level of the data that is stored in the SEM database for the following components:

- **Calls** – representing the actual call records ('Calls Details Storage').
- **Trends** – representing the total call trends i.e. the changes in the call quality over the duration of the call.

Based on the above components, you can set the following compositions:

- **All Calls, All Trends** – All calls and all trends are saved to the SEM server.
- **All Calls, Partial Trends** – All calls; however, no trends for good quality calls are saved to the SEM server (default).
- **All Calls, No Trends** – All calls; however, no trends are saved to the SEM server. This option is recommended if you are operating with more than 50 CAPs.
- **Partial Calls, No Trends** – Only failed, poor and fair quality calls, and no trends are saved to the SEM server.

This option is recommended if you are operating with more than 100 CAPs.

In summary, the larger the number of CAPs that you are managing, the more critical it is efficiently manage the SEM database size. Consequently, the best practice is to save mission - critical data, such as poor quality call statistics and to relinquish less critical data, such as good quality calls statistics.

If you are managing only Lync calls, then the option 'All Calls, No Trends' should be used because call trends are not generated for Lync calls.

3.1.10.2 SEM Performance and Data Storage

The following table shows the SEM performance and data storage capacities for this version.

SEM Performance and Data Storage

Parameter	Capacity
Maximum number of CAPS per device.	160
Maximum number of CAPS per server.	300
Maximum concurrent sessions	30,000
Maximum number of devices per region	500
Maximum number of managed devices.	5000 devices
Maximum number of links between devices.	6000
Call Details Storage - Detailed information per Call	Up to one month or 80 million calls.
Calls Statistics Storage - Statistic information storage.	Up to six months or 150 million intervals.

3.1.11 Concurrent Calls Statistics

A new calculation displaying the concurrent call statistics has been added to the SEM Summary pane in the Statistics view. The maximum number of concurrent calls calculates the cumulative total number of calls from all devices at a specific point in time (the maximum concurrent sessions is specified in the table above).

3.1.12 SEM Licensing Enhancements

The SEM licensing mechanism has been enhanced. The SEM license is determined by the following parameters:

- The maximum number of monitored devices
- The maximum number of concurrent sessions

When the SEM application reaches 80% of the maximum number of monitored devices or 80% of the maximum number of concurrent sessions, the 'License Key' alarm is raised on the device with the 'Major' severity. When the maximum number of monitored devices reaches full capacity, each new device trying to establish connection with the SEM is refused, and an additional 'License Key' alarm per device is raised with the severity 'Critical'. When the maximum number of concurrent sessions reaches full capacity, each subsequent new session will not be monitored by the SEM (all the relevant information is dropped) and an additional 'License Key' alarm per device is raised with the severity 'Critical'.



Notes:

- The SEM license is enforced on AudioCodes devices only. Lync calls are not covered by this mechanism.
- When full capacity is reached, customers should contact their AudioCodes representative to purchase a new license according to their capacity requirements.

3.1.13 SEM Actions Updated to the EMS Actions Journal

All the user actions that are performed in the SEM application, such as devices / links updates, alert rules and reports scheduler changes are updated to the EMS Actions Journal. All SEM actions are identified in the EMS Actions Journal in the 'Source' field by the entry "SEM Server".

3.2 IP Phones Management

AudioCodes' IP Phone Management server enables enterprise network administrators to easily set up, configure, and maintain up to 10000 AudioCodes 400HD Series IP phones in globally distributed corporations. The IP Phone Management Server client can be run on any standard web browser, such as Internet Explorer, Firefox or Chrome. REST (Representational State Transfer) based architecture, an extension of HTTP, enables statuses, commands and alarms to be communicated between the IP phones and the server and also with the EMS. The IP phones send their status to the server periodically for display in the user interface. Accessed from AudioCodes' Element Manager Server (EMS), the IP Phone Management Server user interface enables network administrators to effortlessly load configuration files and firmware files on up to 10000 IP phones. A configuration file template feature lets network administrators customize configuration files per phone model, region, and device. Integrated into the EMS, the IP Phone Management Server provides added value to AudioCodes 400HD Series IP phones.

3.3 EMS Features

3.3.1 Single Sign-On

Device provisioning is no longer performed in the EMS. Instead, the device's Status screen now includes a link to the device's embedded Web server. When this link is clicked, the EMS logs in to the device's Web server with a Single Sign-On implementation (the Web server home page is opened directly and the user is not prompted to enter their login credentials). The Web server user and password is configured when adding the device to the EMS (in the MG Information screen).

Device status screens, alarms, performance monitoring metrics and actions (for single devices and for multiple devices) functionality remains unchanged. In addition, the configuration of digital PSTN trunks, such as those for the Mediant 3000, can still be performed using the EMS.

3.3.2 Auto-Provisioning

When a device is added to the EMS, the user now has the option in the MG Information scene to pre-provision the device with an existing configuration or firmware file (ini or .cmp), which has been pre-loaded to the EMS Software Manager. The user firstly adds those devices that they wish to provision to the EMS, and then when the non-configured device is powered up, it sends a keep alive trap to the EMS, which recognizes the device, connects it and uploads the pre[provisioned] configuration or firmware file. A journal action is displayed in EMS to confirm the successful file load.

3.3.3 Trap Forwarding: Extended Filtering Criteria

The Destination Rule Configuration window has been improved with the following new filtering criteria for all destination types:

- **Alarm Names** – allows the user to forward alarms according to specific alarm names. For example, setting this filter to forward the 'Power Supply' alarm.
- **Alarm Types** – allows the user to forward alarms according to specific alarm types. For example, setting this filter to forward only 'communications-related' alarms.
- **Source** – allows the user to forward alarms according to the alarm source as displayed in the Alarm Browser 'Source' field. For example, 'EMS server' or a specific device board number.
- **Alarm Origin table** – This table has been extended to allow you to forward alarms/events from the SEM and the IP Phone Manager, in addition to the EMS and Gateways.

- **Additional Filters** – In addition, there are new filters for preventing or allowing the forwarding of specific alarms according to the filtering criteria specified in the 'Destination Rule' Configuration window. When you select the 'Prevent Forward' or 'Allow Forward' buttons, and then specify additional filter criteria, then alarms are forwarded according to the specified filter criteria. For example, when you select 'Prevent Forward' and then select the 'Minor Alarms' severity icon, then minor alarms are not forwarded (according to the entities selected in the 'Alarm Origin' table). Alternatively, when you select 'Prevent Forward', and then in the 'Source' field, you specify 'Board#1/EthernetLink#2', then whenever LAN port #2 is down, an Ethernet link alarm is not forwarded.

3.3.4 Alarm Suppression Mechanism

A new feature for suppressing “flickering” alarms has been added. When the EMS server recognizes that there are greater than a threshold-defined number of alarms of the same type and from the same source that are generated in a threshold-defined time, a new 'Alarm Suppression' alarm is generated. At this point, these alarms are not added to the database and are not forwarded to configured destinations.

This feature is configured in the 'Alarm Settings' window. In this window, the user enables the option, and then configures a counter threshold (default - 10 alarms) and interval (default - 10 seconds). This feature applies for alarms of the same type and from the same source. For example, if there are 10 alarms generated from 'Board#1/EthernetLink#2' in 10 seconds, then alarms from this source are suppressed and the 'Suppression' alarm is generated. This alarm is cleared when in the subsequent 10 second interval, less than 10 alarms are sent from this source. At this point, updating to the EMS database is resumed (the last received alarm is updated).

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

3.3.5 Different Sounds per Alarms Severity

When the Alarm sound feature is enabled (by selecting the 'Alarm Sound Enabled' icon in the Alarm Browser), a different sound is heard for each severity type.

3.3.6 Alarm Details Screen Enhancements

The Alarm Details screen now displays both the time the alarm was raised on the gateway device and when it was raised on the EMS (previously only the time that the alarm was raised on the EMS was displayed). You can also now print the information that is displayed in this screen (the information displayed in each tab is printed).

3.3.7 Topology File Enhancements

The following new parameters are now supported by the EMS Topology file:

- SNMP Version
- SNMP Read
- SNMP Write
- SNMP User Profile
- Gateway User
- Gateway Password
- HTTPS Enabled

4 New Features in Version 6.8

4.1 General

4.1.1 Improved/Enlarged Capacity of Managed Products

- EMS
 - Up to 5000 devices per installation.
 - Up to 500 devices per region.
- SEM – see Section 4.3 on page 40.

4.1.2 New Hardware Requirements

The new hardware platform for the EMS / SEM 6.8 version is defined as follows:

- HP DL360 G8 server with the following minimum requirements:
 - CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each)
 - Memory: 32 GB
 - Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0

4.1.3 New Products Management

In this version, the following new products are supported by EMS and SEM:

- Mediant 4000 E-SBC: versions 6.6, **6.8**
- Mediant 2600 E-SBC: versions 6.6, **6.8**
- Mediant SE SBC and Mediant VE SBC: **6.8**
- Mediant 500 MSBR: version **6.8**
- Mediant 500 E-SBC and Mediant 500 MSBR: version **6.8**
- *Mediant 800 SBA, *Mediant 1000 SBA and *Mediant 2000 SBA devices with SBA version **1.1.13.0** and above and gateway versions 6.6 and **6.8**

* Refers to products that are not supported by the SEM

4.1.4 Virtualized EMS Server on HyperV

In this version the EMS server, is delivered as a virtual appliance on the HyperV Virtual Servers (in addition to previously released setups).

The virtual environment allows the IT manager, carriers and all EMS customers to minimize dedicated hardware per application usage, which leads to IT maintenance cost savings.

4.1.5 Supporting High Availability in Virtualized Solutions

On both the VMWare and HyperV servers, EMS can run as Standalone application or as part of a High Availability solution supported by a virtualization vendor.

For a list of all supported configurations, refer to the *EMS Server IOM Guide*.

4.1.6 EMS Client Support on Windows 8

In this version, the EMS client application is supported on the Windows 8 Operating System.

4.1.7 EMS Server: Server Manager Improvements

The EMS Server Manager user experience has been enhanced with new features such as color-coded statuses, improved menu design and navigation, as well as improved responses. These changes are described in the *EMS Server IOM* document.

4.2 EMS New Features

4.2.1 Security: Integration with LDAP Server for User Authentication and Authorization

EMS application users can now be authenticated and authorized using an LDAP server, in addition to the existing methods (local users on the EMS server) storage, RADIUS or TACACS+ server).

4.2.2 Devices Configuration Backup and Data Synchronization

Starting this version, device configuration is backed up in the EMS server as an *ini* file. EMS server updates the device *ini* file each time the device configuration is updated via EMS. In addition, periodic checks are performed to detect configuration changes on the device. As a consequence of these checks, a backup file is generated on the EMS server several times each day, based upon these most recent updates. Up to 10 backup files can be stored per device.

4.2.3 Performance Management Extensions

- A new option to print detailed summary reports has been added in the History PM Display.
- In the History PM Display, new parameters 'Min Value Time' and 'Max Value Time' have been added. These parameters display the time interval at which the minimum and maximal values occurred during the polling interval period.
- New History PM Configuration performance management metrics 'IP Group Statistics' can be defined per IP Group. For example, you can poll 'SIP IP Group Dialogs' and 'SIP IP Group Invite Dialogs IP Max'.

4.3 SEM New Features

4.3.1 Improvements in SEM Performance and Data Storage

The table below describes enhancements in SEM performance and data storage.

SEM Performance and Data Storage

Parameter	Capacity
Maximal number of CAPS per device.	160
Total maximal number of CAPS per server.	300
Maximal number of managed devices.	3000 devices
Maximal number of links between devices.	6000
Detailed information per Call (*)	Up to 1 month or 80 million calls.
Statistic information storage.	Up to 6 months or 150 million intervals.
Network, Statistics and Reports Views.	Improved Capacity Volumes.

Note the following:

- (*) Our recommendation for high capacity setups (100 CAPS and Higher) is to set the SEM parameter 'SEM Server Storage Level' to 'Failed, Poor or Fair Quality Calls, No Trends'.
- In this version, the Network, Statistics and Report Views enable the user to view up to six months of archived information (instead of the 10 million calls limitation in the previous version).

4.3.2 New SEM Licensing Mechanism

In this version, a new SEM Licensing mechanism has been implemented.

The Licensing mechanism applied by the customer is based on EMS/SEM server machine identifier, which can be extracted from the machine after it's installed.

After applying the new SEM license to the EMS/SEM server machine, SEM will work according to the license key definition. You no longer need to apply the QoE feature licenses at the device level.

4.3.3 Support New Link Types between Devices

The following links between devices are supported in this version:

- IP Group
- Media Realm
- Remote Media Subnet
- Trunk Group
- Phone/URI Prefix
- Control IP Address
- Media IP Address



Notes:

- In this release, support has been added for the Media Realm, Remote Media Subnet and the Media IP Address links. This extension is relevant for devices from version 6.8 and later.
- For the IP Group, Media Realm and Sub-Media Realm link types, different QoE calls threshold per each link may be configured (e.g. calls are colored red on MOS < 3.0).
- This configuration should be performed on the VoIP device using any of the supported management interfaces.

4.3.4 New Links Table in Network View

- Improved links table design allows the management of a larger number of links.
- Fast and Easy link search according to name, source or destination devices is supported.

A summary of the most important link statistics, such as Calls Number and Calls Success Rate, Quality, and the most important metrics with sorting options are supported.

4.3.5 SEM Application Multi - Tenancy

The EMS user permissions per region feature, introduced in the previous version to the EMS application, have now been extended to the SEM. Each operator will now be able to view/change only those devices and links defined in the region upon which they have access privileges. This includes the entire set of SEM pages: Network, Statistics, Calls, Alarms and Reports.

4.3.6 Scheduled Reports

You can now automate report generation using scheduling criteria. The following summarizes the scheduling criteria that you can define in the scheduled reports:

- Setting the type of report. For example, 'Call Statistics by Device' or 'Call Statistics by Link'.
- Setting further report type criteria; for example in the event of a Links report, you can define link filter settings. For example, generate a report for a specific IP Group or Media Realm.
- Set the scheduler to generate hourly, daily, weekly or monthly reports.
- Set the time of the day to run the report.
- Set the number of times to run the report.
- Send the reports to an email addresses or view a separate list of the generated reports for each specific report type. For example, view a list of generated reports for "Call Utilization by Device". You can generate reports for all existing SEM report types.

4.3.7 Calls List: Add Calling Name Information

When the device is integrated with the Active Directory server (when LDAP is enabled on the device) and manages the users list, the SEM will be able to display the user with their Calling Name as it appears in Active Directory definitions. This Calling Name will be displayed in the Calls List in the 'Caller' field, and in the 'Top Users' reports in the "User Name" field. In addition, users can sort, or search according to this Calling Name in the Calls List.

4.4 Changes from the Previous Version

- Installation Process: this version does not support an upgrade from any previous version for working with Oracle Enterprise Edition. Import of the managed devices should be performed using the latest version of the Topology file. Server machine format and clean install using three DVDs (DVD1, DVD2 and DVD3) is required. A minor version 6.8 upgrade is supported.
- EMS: The Master Profile is not supported in EMS version 6.8. The suggested method for replicating a configuration to multiple devices is by using an incremental INI file.
- SEM: The Calls List, Voice and Fax Calls buttons have been removed.
- SEM: The Calls List screen is not auto-refreshable. To initially retrieve the Calls List, set filter parameters, and then click the Refresh button each time to update the list.
- SEM: Statistics view: The Failed Calls Termination Reasons distribution has been removed.
- SEM: Links. When adding or modifying link it will affect only to the next calls.

5 Known Limitations and Workarounds

The table below lists the Known Limitations and Workarounds in this release.

Known Limitations and Workarounds

Issue	Problem/Limitation	Comments and Workaround
First-time login	<p>Important note for first-time users (this is not a problem; however first-time users may encounter the following):</p> <p>When logging in for the first time:</p> <ol style="list-style-type: none"> 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	For optimal system performance, do not define more than 500 Media Gateways in any one region.	-
Online Help	The Online Help is not available in this version.	The Online Help will be available in one of the future fixes.
EMS Server – Virtual Platform	The Multiple Ethernet redundancy with EMS server HA is not supported in this version for the Virtualized server.	This feature will be supported in one of the future fixes.
SEM-Monitoring Endpoint Devices Reporting	A single report per call at the call end stage using VQSessionReport message of CallTerm type is supported. Aggregation of the interval reports during the call is not supported. The transport layer supported in this version is UDP.	This issue will be resolved in one of the future fixes.
SEM for Lync Conference Calls	Sometimes when conference participants dropped the conference earlier than 10 minutes before the conference had finished, reported information may be incomplete or missing.	This issue will be resolved in one of the future fixes.
License Pool Manager with Multi-Tenant support	This License Pool Manager does not currently support the multi-tenant configuration, where each tenant is represented by an EMS region and managed by an EMS administrator with "Operation" permissions. In this release, when a service provider or integrator manages multiple customers, licenses must be allocated globally per EMS server installation by an EMS administrator with either "Administrator" or "Super Administrator" permissions. In a future release, support will be provided per region; including the ability for an EMS administrator with "Operation" permissions to	This feature will be supported in one of the future fixes.

Issue	Problem/Limitation	Comments and Workaround
	configure license sub-pools for each region.	
Single-Sign On	When logging onto the device using the Single-sign on mechanism (using the link to the device's Web server in the device's status page in the EMS) and entering the "Message Log" page under the Troubleshooting tab: <ul style="list-style-type: none"> • It might take time to display this page. • When moving from this page to other pages, the Navigation tree might not be displayed properly. 	Select a higher-level menu option in the Navigation tree.
Adding Multiple Devices	When adding multiple devices to the EMS, do not use underscores in device names (MG Name).	
SEM communication	SEM: when changing the SEM <-> Device communication to be TLS, need to restart EMS Server.	
HA Devices support behind the NAT	EMS & SEM do not support HA devices behind the NAT.	
Number of Login Attempts	The number of login attempts before a user is suspended cannot be defined per user.	
EMS HA Support for EMS Version 7.2.1000 (or higher)	When upgrading to EMS Version 7.2.1000 (or higher) in an HA setup, you must do the following: <ul style="list-style-type: none"> • Upgrade the EMS servers to Version 7.2.1000 (or higher) • Backup all data • Upgrade the Linux Operating System to Cent OS 5.9 Rev8 • Restore data to new installation. The full procedure is described in the EMS Server IOM manual.	
SBC License Pool Product support	The SBC license pool does not support the Mediant 3000 and MP-1288 (Lag) products.	
SEM and Microsoft Lync Server	When working with Lync server pools (FE, Edge and Mediation), the FE server defined in the SEM functions as the monitoring SQL database. After connecting, the SEM displays all Call Details from the Lync network in the SEM's Calls List and Call Details views. When functioning with Lync pools, FE, Edge and Mediation servers cannot be defined in the SEM, so the entire Lync network is displayed in the SEM only as a single object, namely, the monitoring SQL database.	

Issue	Problem/Limitation	Comments and Workaround
	The SEM connection with the Microsoft Lync Server supports one Front End server and one SQL server.	
	The SEM connection with the Microsoft Lync server supports up to two Microsoft Lync solutions in one SEM application.	
Trunk Group Based Links in SEM	In cases when upgrading to this version and SEM trunk groups based links are used prior to the upgrade, and in case you encounter a problem similar to the problem raised in "Trunk Group Mismatch between SEM and the Mediant 800", remove the SEM Trunk Groups links and redefine them to resolve the problem.	
Endpoints Management	When Endpoints are managed by both EMS for IP Phones and SEM, and the operator wishes to remove the endpoints and the region, first remove the endpoints in the EMS for IP Phones application. Only then you can remove the corresponding Region in the EMS GUI.	
Maximum Number of Managed Endpoints for IP Phone Management Server over HTTPS	When managing endpoints connections with the EMS server over HTTPS, the maximum number of endpoints that can be managed are as follows: <ul style="list-style-type: none"> • HP DL360p G8-10,000 • VMware/Microsoft Hyper-V - Low Profile-1000 ▪ VMware/Microsoft Hyper-V – High Profile-5000 	
Single Sign-on to devices located behind a NAT	Single Sign-on to AudioCodes devices' Web interfaces from the devices' status screens in the EMS is not supported if these devices are located behind a NAT. In this case, it is recommended for these connections to work over HTTPS using port 443. This port must be opened on the firewall with a static forwarding rule configured in the NAT.	

International Headquarters

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

AudioCodes Inc.

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

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com

©2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-90542

