

OVOC Integration with Northbound Interfaces

Version 7.2

Table of Contents

1	One Voice Operations Center - Overview	7
2	OVOC Integration	9
2.1	OVOC Integration Elements.....	10
2.1.1	EMS Topology File	10
2.1.2	Alarms.....	10
2.1.3	Gateway Status	10
2.1.4	Performance Monitoring Metrics	10
2.1.5	Security	11
2.1.6	Configuration and Maintenance	11
2.2	NBIF Folder	11
3	Topology File	15
4	Fault Management.....	17
4.1	Alarms and Events Reception in the NMS.....	17
4.1.1	Forwarding EMS Alarms and Events	18
4.1.2	Forwarding Other Alarms and Event Types from the EMS	20
4.1.3	Forwarding Alarms Directly from Devices	23
4.1.3.1	Configuring SNMPv3 User Settings	23
4.1.3.2	Modifying SNMPv2 Community Strings or SNMPv3 Passwords	25
4.1.3.3	Configuring Additional SNMPv3 Users.....	26
4.1.3.4	SNMPv3 User Cloning.....	26
4.1.4	Alarms Clearing Mechanism.....	28
4.1.5	Events Clearing Mechanism.....	28
4.1.6	Alarm Suppression Mechanism	28
4.1.7	Alarms Sequence Numbering.....	29
4.1.8	Alarms Synchronization via MG SNMP I/F	30
4.1.9	EMS Keep-alive.....	31
4.2	Status / State Management via MG SNMP I/F.....	34
5	Performance Monitoring.....	35
5.1	EMS Server CSV / XML File Format Interface.....	37
5.1.1	CSV File Format.....	38
5.1.2	XML File Format.....	39
5.2	Devices SNMP Interface.....	40
6	SEM Scheduled Reports.....	41
7	EMS Server Backup	43
8	Security.....	45
8.1	Network Communication Protocols.....	45
8.2	OVOC User Identity Management	46
8.2.1	Authentication and Authorization using a Radius Server	47
8.2.1.1	Configuring Radius Server Client	47
8.2.1.2	Configuring RADIUS Server	49
8.2.2	Authentication and Authorization using an LDAP Server	52
8.3	HTTPS Connection	54

List of Figures

Figure 2-1: OVOC Integration Overview	9
Figure 2-2: NBIF Parent Directory	12
Figure 2-3: NBIF Topology Directory	12
Figure 3-1: Topology File-Excel View	16
Figure 4-1: Alarm and Event Forwarding	18
Figure 4-2: Destination Rule Configuration	20
Figure 4-3: SNMP Trap Forwarding	21
Figure 4-4: Traps Forwarding Configuration	22
Figure 34-5: MG Information-New SNMPv3 User	24
Figure 34-6: Update SNMPv2 Settings for Multiple Devices	25
Figure 34-7: MG Information Screen-New SNMPv3 User	27
Figure 24-8: EMS Keep-alive	31
Figure 24-9: Alarm Forwarding Configuration	32
Figure 24-10: Destination Rule Configuration	33
Figure 5-1: Performance Monitoring - Intervals	35
Figure 5-2: Background Monitoring csv File	38
Figure 5-3: xml File Header Example	39
Figure 5-4: xml File Data Example	39
Figure 6-1: SEM Scheduled Report	41
Figure 8-1: OVOC User Management	46
Figure 35-2: RADIUS Authentication and Authorization	50
Figure 35-3: LDAP Authentication and Authorization	53

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 SW releases can be viewed by registered customers <http://www.audiocodes.com/downloads>.

This document is subject to change without notice.

Date Published: May-11-2017

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.

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 One Voice Operations Center - Overview

AudioCodes One Voice Operations Center (OVOC) delivers a comprehensive management tools suite comprising of base platform and add-on modular applications for the management, monitoring and operation of converged VoIP and data networks implemented in large-scale cloud or premise-based unified communications deployments using AudioCodes devices. The products that are managed by the OVOC include the Session Border Controllers (SBC), Media Gateways, Microsoft Survivable Branch Appliances (SBA), Multi Service Business Router (MSBR), residential gateways and endpoints (IP Phones). The OVOC also integrates with the Microsoft Lync environment platforms.

The Network Operations Center's core product, the Element Management System (EMS) manages these products in a centralized device inventory via a client-server console, enabling integrative network operations. The following describes the key products in the OVOC suite:

- **The Element Management System (EMS):** The EMS is an advanced solution for remote standards-based management of AudioCodes products within VoP networks, covering all areas vital for their efficient operation, administration, management and security. A single user interface provides real time information including network and device component status, activity logs and alarms. Complete End-to-End network control includes data on all devices, all locations, all sizes, all network functions and services and full control over the network, including services, updates, upgrades, and operations. The EMS is in AudioCodes' assessment, the best tool to manage AudioCodes devices. However, it does not replace the NMS and OSS management systems, which displays to operators a comprehensive view of the network, including other vendors' equipment. After defining and initially provisioning a device via the device's embedded Web server tool, operators will usually work with an NMS / OSS for day-to-day maintenance. Only in the event of problems with a device or when significant maintenance tasks must be performed, will operators open the EMS and work directly with it. Consequently, the EMS provides APIs for faults monitoring (alarms), performance monitoring and security integration with a higher level management system.
- **The Session Experience Manager (SEM):**
The SEM is used analyzing real-time Voice Quality statistics. The SEM enables the rapid identification of the metrics responsible for degradation in the quality of any VoIP call made over the network nodes including AudioCodes devices and links. It provides an accurate diagnostic and troubleshooting tool for analyzing quality problems in response to VoIP user criticism. It proactively prevents VoIP quality degradation and optimizes quality of experience for VoIP users. In addition, it integrates with Microsoft Lync Server monitoring server to provide end-to-end VoIP quality monitoring on Microsoft Lync deployments. In addition, the SEM integrates and monitors with endpoints reporting RFC 6035 SIP PUBLISH packets.

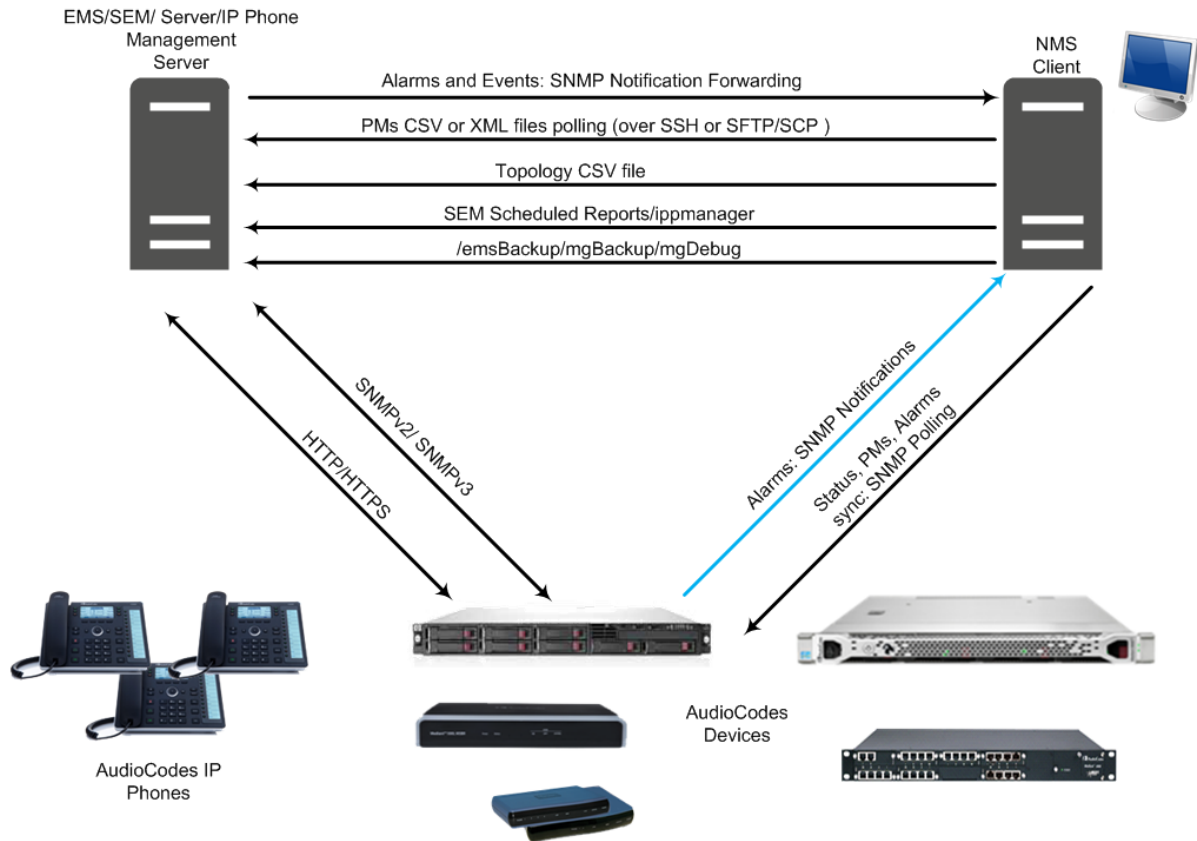
- **The IP Phone Management Server:**

AudioCodes' IP Phone Management Server enables enterprise network administrators to effortlessly and effectively set up, configure and update up to 10000 400HD Series IP phones in globally distributed corporations. These phones can upload configuration files from the EMS and send status updates over the REST protocol.

2 OVOC Integration

This document describes how to integrate the network elements of AudioCodes One Voice Operation Center (OVOC) with northbound interfaces. This includes the integration of alarms and events that are generated by the managed elements, the Performance Monitoring data, XML files polling and the Topology file. The figure below illustrates this integration.

Figure 2-1: OVOC Integration Overview



2.1 OVOC Integration Elements

This section describes the integration elements.

2.1.1 EMS Topology File

The EMS Topology file includes a snapshot of all the devices that are defined in the EMS application. This file is located on the EMS server and is available for the higher level management system (see Chapter 3).

2.1.2 Alarms

Alarms are sent from devices, IP Phones, SEM and EMS as SNMP notifications (traps). These traps can be forwarded using one of the following methods:

- Forwarded by the EMS application to the NMS server (for all the network elements and the EMS itself).
- Sent by each one of the network elements directly to the NMS server. In this case, there is the possibility to enable EMS alarms. For example, when a connection between the EMS server and device is established or lost, traps are forwarded to the NMS server.

For detailed information, see Chapter 4.

2.1.3 Gateway Status

The status of a device can be determined based on the set of supported IETF Management Information Base (MIB-II) tables(described in the *SNMP Reference Guide*).

2.1.4 Performance Monitoring Metrics

Performance Monitoring (PM) data and statistics are made available to the NMS using either of the following methods:

- Collection of csv or xml files from the EMS server via FTP or SFTP. EMS performs SNMP polling of the network elements and creates a summary file per element or per collection interval.
- Collection of information directly from the network element via the SNMP interface.

For detailed information, see Chapter 5.

2.1.5 Security

Security integration covers two main areas: Users Management and Network Communication protocols.

- EMS Users Management (Authentication and Authorization) locally in the EMS database or via a centralized RADIUS server or LDAP server.
- Network Communication Protocols:
 - **HTTP/HTTPS:**
 - ◆ NBIF Client- EMS Server connection is secured over HTTPS port 443 using AudioCodes default certificates or custom certificates.
 - ◆ File transfer.
 - **SNMPv3** and **SNMPv3**: For Maintenance Action, Faults and Performance Monitoring.
 - **SSH/SFTP/SCP**: used for File transfer.

For detailed information, see Chapter 7.

2.1.6 Configuration and Maintenance

A **REST API** will be available in a future release for performing configuration and maintenance actions from the NMS and running automation scripts using REST API URLs. For more information, contact your AudioCodes representative.

2.2 NBIF Folder

All EMS and device information available for the NMS and other Northbound interfaces including Topology, Performance and Backup data is located in the EMS server machine under the folder **/NBIF**. This folder can be accessed using HTTPS browsing by entering the URL `https://<EMS Server IP>/NBIF` in your Web browser.














Note:

- The customer's Web browser must have installed the appropriate X.509 certificates signed by the same Certificate Authority (CA) as the EMS server web browser certificates. Choose the appropriate certificate, and then click OK.
- For more information on the implementation of X.509 certificates, refer to the *OVOC Security Guidelines*.

The 'NBIF' folder content opens; double-click each one of the folders to list it's contents. Double-click each file to open its contents.

Figure 2-2: NBIF Parent Directory



Index of /NBIF

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 SEM/	21-Dec-2015 17:00	-	
 alarms/	17-Nov-2015 11:47	-	
 emsBackup/	18-Mar-2017 02:03	-	
 ippmanager/	14-Feb-2017 09:19	-	
 mgBackup/	22-Mar-2017 04:00	-	
 mgDebug/	13-Apr-2016 13:27	-	
 mgmt ca/	07-Jan-2016 17:18	-	
 pmFiles/	19-Apr-2016 09:25	-	
 tmp/	21-Mar-2017 14:03	-	
 topology/	21-Mar-2017 14:03	-	

Apache/2.2.3 (CentOS) Server at 10.3.180.2 Port 80

Figure 2-3: NBIF Topology Directory

Index of /NBIF/topology

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 MGsTopologyList.csv	21-Mar-2017 14:03	13K	

Apache/2.2.3 (CentOS) Server at 10.3.180.2 Port 80

The 'NBIF' folder contains the following sub-folders:

- **SEM:** this folder contains Scheduled Reports that were generated in the SEM. For more information, see Chapter 6,
- **alarms:** this folder contains a file saved by the EMS user (Faults > Save Alarms As') where the action result displays no less than 1500 records. This file is created for local user requests and must not be collected by higher level Management or Backup systems.

- **emsBackup:** this folder contains the daily and weekly backup of the EMS server. For more information, see Chapter 7.
- **ippmanager:** this folder contains the following folders:
 - **generate:** contains the IP Phones firmware files.
 - **regioncache:** contains the IP Phones global cfg files
 - **sess:** contains system folder for sessions management
 - **templates:** contains the IP Phones cfg template files
 - **tmp:** contains system folder for temporary files
- **mgBackup:** this folder contains the backed up device INI and CLI configuration files.
- **mgDebug:** this folder contains Syslog and Packets debug information.
- **Mgmt_ca:** this folder contains the default certificate files for the AudioCodes devices and the EMS Root CA file.
- **pmFiles:** this folder contains Performance Monitoring files collected by EMS for all the defined and provisioned devices. These files are stored under the 'pmFiles' folder. For more information regarding the file naming convention, file structure and file management policy for this folder, see Chapter 5.
- **topology:** A Summary file of all the devices and their basic properties defined in the EMS application. The summary file is located under the 'topology' folder and is always named **MGsTopologyList.csv**. For more information, see Chapter 3.

This page is intentionally left blank.

3 Topology File

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

The Topology file is automatically updated upon the addition /removal of a device or upon updates to the device's properties, such as name, IP address or region modification. It is also updated upon Performance Monitoring polling status changes. The EMS sends 'acEMSTopologyUpdateEvent' (Topology Update) for changes in the definition or update of a device and sends 'acEMSTopologyFileEvent' (Topology File Generated) for a topology file update. These events are displayed in the EMS Alarm Browser and in the NMS Alarm Browser when the 'EMS Events Forwarding' check box is selected in the Trap Configuration 'Destination Rule Configuration' dialog.

When multiple devices are added, the Topology file is updated approximately once per minute as the entire operation may take more than a few minutes. For detailed information on the exact event fields, refer to the relevant *Device's Performance Monitoring and Alarm Guide*.

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

- Serial Number
- IP Address
- Node Name
- Region Name
- Description
- Product Type
- Software Version
- Connection Status – Connected / Not Connected – represent the ability of EMS application to communicate with MG
- Administrative State – Locked / Unlocked / Shutting Down
- Operational State – Enabled / Disabled
- Mismatch State – No Mismatch / SW Version Unsupported / SW Mismatch / HW Mismatch.
- Last Change Time
- Performance Polling Status – Polling / Not Polling
- Performance Profile

- Protocol Type – MGCP / MEGACO / SIP
- Master Profile
- Reset Needed
- SBA FQDN Name
- SBA IP Address
- SNMP Version – options are SNMPv2/SNMPv3
- SNMP Read – encrypted SNMP read community
- SNMP Write – encrypted SNMP write community
- SNMP User Profile - SNMP v3 user credentials in format:
(EnginID;SecurityName;SecurityLevel;AuthProtocol;PrivacyKey)
- Gateway User – user name for MG web access
- Gateway Password– user password for MG web access
- HTTPS Enabled – 0-disabled/1-enabled HTTPS access to the MG

See an example Excel file view in the figure below.

Figure 3-1: Topology File-Excel View

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1	Serial Nu	IP Address	Node Name	Region	Product T	Software	Connectiv	Administr	Operative	Mismatch	Last Chan	Preformat	Performa	Protocol T	Master Pr	Reset	Nea	Descriptio	SBA FQDN	SBA IP	/SNMP Vv	SNMP Re	SNMP Write	SNMP User	Gateway i	Gateway	HTTPS Enabled
2	3583846	192.168.1.1	550-Proxy	Eran	UNKNOWN	unknown	Not Connected				No Mismatch	2014-12-31	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
3	3846546	10.3.101.1	1444	Eran	MEDIAN	7.00A.003	Connectiv	Unlocked			No Mismatch	2015-02-01	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
4	1242278	10.3.151.2	558C	Eran	SW SBC	7.00A.005	Connectiv	Unlocked			No Mismatch	2015-02-01	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	0	
5	123456	1.1.1.1		Eran	UNKNOWN	unknown	Not Connected				No Mismatch	2014-12-31	Not Polling				1.1.1					SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
6	273196	10.4.100.3	10.4.100.3	Vladi	MEDIAN	6.80A.255	Connectiv	Unlocked			No Mismatch	2015-02-01	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
7	4773083	10.3.181.9	10.4.100.1	AutoDete	MEDIAN	7.00A.004	Not Connv	Unlocked			No Mismatch	2015-02-0	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
8	760978	10.3.80.16	10.3.80.16	AutoDete	MP124	6.60A.290	Not Connv	Unlocked			No Mismatch	2015-02-0	Not Polling					SIP		Reset Not Needed		SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
9	9480922	10.15.4.6	10.15.4.6	AutoDete	Mediant	8.6.80A.261	Connectiv	Unlocked			No Mismatch	2015-02-01	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
10	520544	10.3.181.7	10.3.181.7	AutoDete	Mediant	5.6.90A.048	Not Connv	Unlocked	Enabled		No Mismatch	2014-12-1	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	0	
11	893335	10.3.181.2	10.3.181.2	AutoDete	MEDIAN	6.80A.219	Not Connv	Unlocked	Enabled		No Mismatch	2015-01-0	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
12	3037728	10.3.181.6	10.3.181.6	AutoDete	Mediant	5.6.80.244.0	Connectiv	Unlocked			Hardware	2015-02-01	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
13	5264110	10.3.181.1	10.3.181.1	AutoDete	UNKNOWN	unknown	Not Connected				No Mismatch	2014-12-1	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	
14	4979399	10.3.3.214	10.3.3.214	AutoDete	Mediant	8.7.00A.001	Not Connv	Unlocked			No Mismatch	2015-01-0	Not Polling									SNMPv2	8k0tnrBul	f/0BAMNtinsMVeryk4thf Admin	fseUajP5a	1	



Note: EMS Device report files can also be exported from the EMS application using the 'File > MGs Report' option. This file contains more information than the Topology report on the EMS server machine. Both the MG Report and the Topology file reports, received from the EMS client or the EMS server can be imported using the 'Add multiple MGs' option from the EMS Tree Region (right-click option).

4 Fault Management

AudioCodes devices and IP Phones reports their faults (alarms and events) and state changes (Administrative/Operative state) via SNMP notification traps. Both standard and proprietary traps are supported. AudioCodes proprietary traps have the same variable bindings set. Each alarm includes information required by the ITU-T X.733 standard. Operative and Administrative states are managed according to the ITU-T X.731 standard. See the relevant product *Alarm and Performance Monitoring Guides* for the exact list of standard, MG proprietary and EMS proprietary traps that are supported for each device. For each trap description, it's indicated whether the trap is defined as an alarm or an event.

4.1 Alarms and Events Reception in the NMS

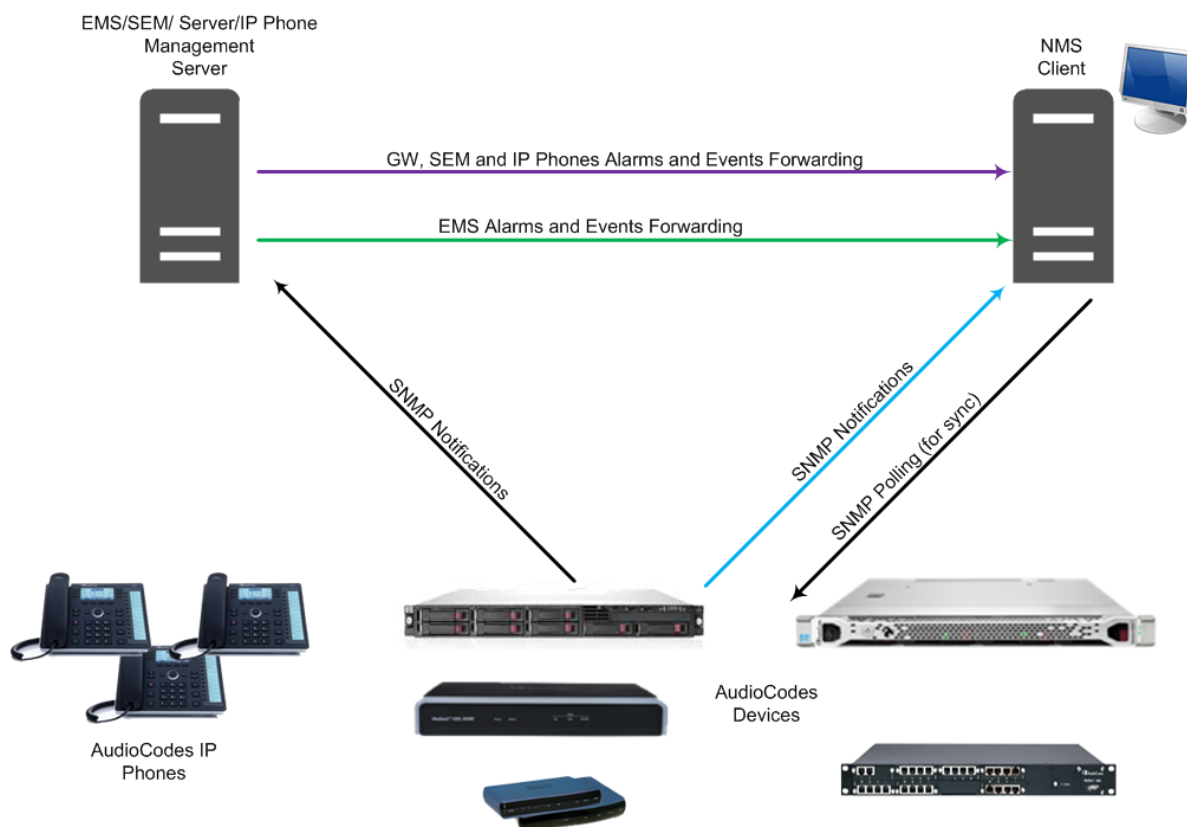
Alarms can be forwarded to the NMS using one of the following methods:

- Alarms and events are forwarded by the EMS application to the NMS for all network elements (SEM, devices and IP Phones) (**purple**-colored path in the figure below) or only EMS alarms and events are forwarded (**green**-colored path in the figure below). See Section 4.1.1.
- Each one of the network elements (EMS, SEM, devices and IP Phones) sends it's own alarms directly to the NMS (**blue**-colored path in the figure below). The device can send alarms to several destinations (the exact number of destinations depends on the device type). For example, the device can send alarms to the EMS and NMS. You can configure each destination with a different trap port.



Note: Although the EMS can forward alarms and events in several formats (SNMP Notifications, SMS, Mail and Syslog), alarms and events are always sent to an NMS as SNMP notifications for purposes of NMS integration (see Section 4.1).

Figure 4-1: Alarm and Event Forwarding



4.1.1 Forwarding EMS Alarms and Events

This section describes how to forward EMS alarms and events to the NMS.

➤ To forward alarms and events from the EMS application:

1. In the EMS menu, choose **Faults > Traps Configuration**; the Destination Rule Configuration dialog is displayed.
2. In the sub-menu, choose **Actions > Add Destination** or in the Actions bar, click **+**.
3. From the Select Destination Type drop-down list, choose **SNMP**.
4. In the left-hand pane, provision the following parameters for defining the destination rule:
 - 'Destination Rule Name' as you wish it to appear in the summary screen.
 - Select the following subset of alarms and events that must be forwarded to the NMS (by default, all the alarms and events are selected):
 - ◆ EMS Alarms
 - ◆ EMS Events
 - Alarm Names (for EMS alarms): allows the user to forward alarms according to specific alarm names.
 - Alarm Types (for EMS alarms): allows the user to forward alarms according to specific alarm types.

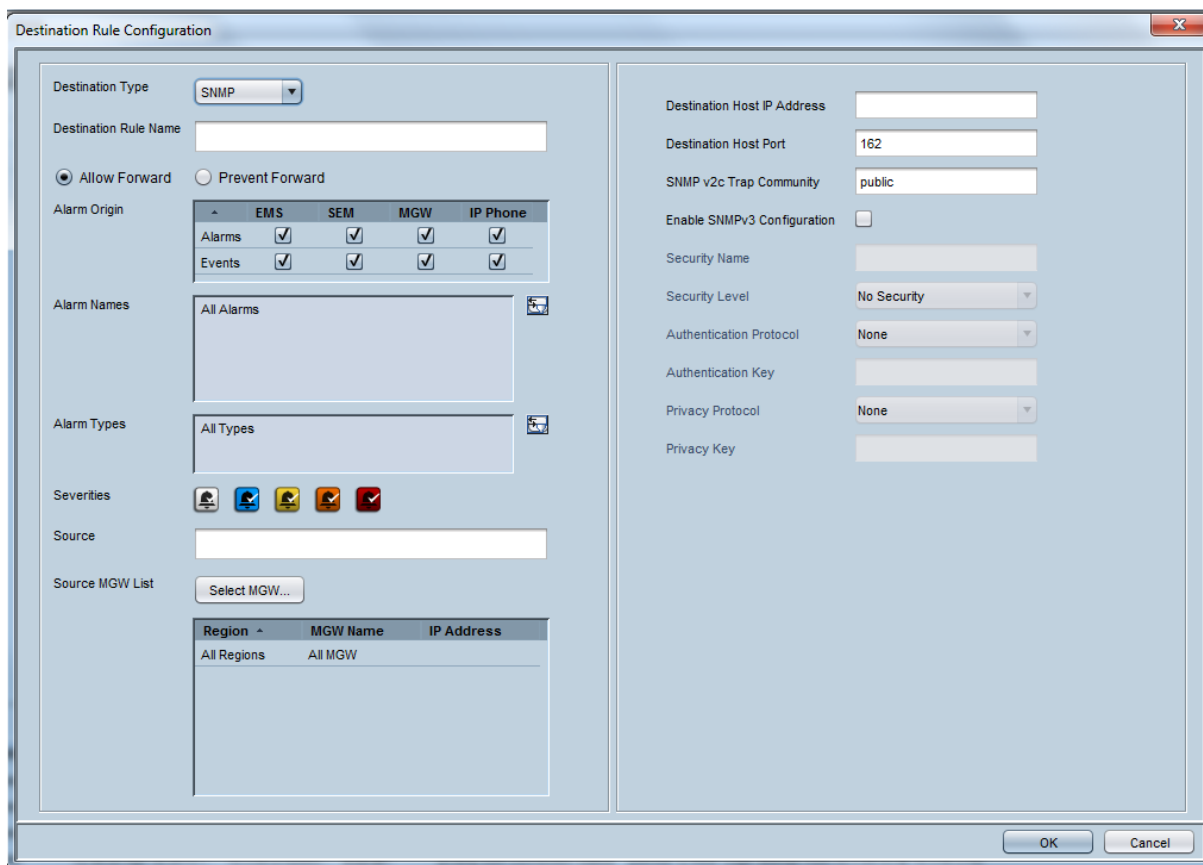
- Select the subset of 'Severities To Forward': severities that you wish to receive in the NMS application (by default, all the severities are selected). Note: CLEAR alarms for selected subset of the alarms are always forwarded.
 - Source: allows the user to forward alarms according to the alarm source as displayed in the Alarm Browser 'Source' field. For example, 'EMS server'.
5. In the right-hand pane, provision the following parameters:
- In the 'Destination Host IP Address' field, enter the NMS IP address.
 - In the 'Destination Host port' field, enter the port number of the destination host (the default SNMP port for trap reception is **162**).



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

6. You can optionally select the 'Enable SNMPv3 Configuration' box to enable forwarding traps to the NMS using SNMPv3. In this case, set the following additional fields:
- In the 'Security Name' field, enter the Security name of the SNMPv3 user.
 - From the 'Authentication Protocol' drop-down list, select an authentication protocol; the corresponding security level is displayed in the 'Security Level' field.
 - In the 'New Authentication Password' field, enter a new Authentication Password.
 - From the 'Privacy Protocol' drop-down list, select a Privacy Protocol.
 - In the 'New Privacy Password' field, enter a new Privacy Password.
7. Click **OK**.

Figure 4-2: Destination Rule Configuration



The dialog box is titled "Destination Rule Configuration". It is divided into two main panels. The left panel contains configuration options for the destination rule, and the right panel contains security and host information.

Left Panel:

- Destination Type:** A dropdown menu set to "SNMP".
- Destination Rule Name:** A text input field.
- Forwarding:** Two radio buttons: "Allow Forward" (selected) and "Prevent Forward".
- Alarm Origin:** A table with columns: EMS, SEM, MGW, IP Phone. Rows: Alarms, Events. All cells are checked.
- Alarm Names:** A text input field containing "All Alarms".
- Alarm Types:** A text input field containing "All Types".
- Severities:** A row of five icons representing different severity levels.
- Source:** A text input field.
- Source MGW List:** A button labeled "Select MGW..." and a table below it.

Region	MGW Name	IP Address
All Regions	All MGW	

Right Panel:

- Destination Host IP Address:** A text input field.
- Destination Host Port:** A text input field containing "162".
- SNMP v2c Trap Community:** A text input field containing "public".
- Enable SNMPv3 Configuration:** An unchecked checkbox.
- Security Name:** A text input field.
- Security Level:** A dropdown menu set to "No Security".
- Authentication Protocol:** A dropdown menu set to "None".
- Authentication Key:** A text input field.
- Privacy Protocol:** A dropdown menu set to "None".
- Privacy Key:** A text input field.

At the bottom right are "OK" and "Cancel" buttons.

4.1.2 Forwarding Other Alarms and Event Types from the EMS

This section describes how to forward all other alarm types from the EMS to the NMS including SEM alarms and events; MGW alarms and events and IP Phone alarms and events.

➤ • To forward alarms from the EMS to the NMS:

1. In the EMS menu, choose **Faults >Traps Configuration**; the Destination Rule Configuration dialog is displayed.
2. In the sub-menu, choose **Actions > Add Destination** or in the Actions bar, click **+**.
3. From the 'Destination Type' drop-down list, select **SNMP**.

Figure 4-3: SNMP Trap Forwarding

Destination Rule Configuration

Destination Type: **SNMP**

Destination Rule Name:

☒ Allow Forward ☐ Prevent Forward

Alarm Origin:

	EMS	SEM	MGW	IP Phone
Alarms	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Alarm Names:

Alarm Types:

Severities:

Source:

Source MGW List:

Region	MGW Name	IP Address
All Regions	All MGW	

Destination Host IP Address:

Destination Host Port:

SNMP v2c Trap Community:

Enable SNMPv3 Configuration: ☐

Security Name:

Security Level: **No Security**

Authentication Protocol: **None**

Authentication Key:

Privacy Protocol: **None**

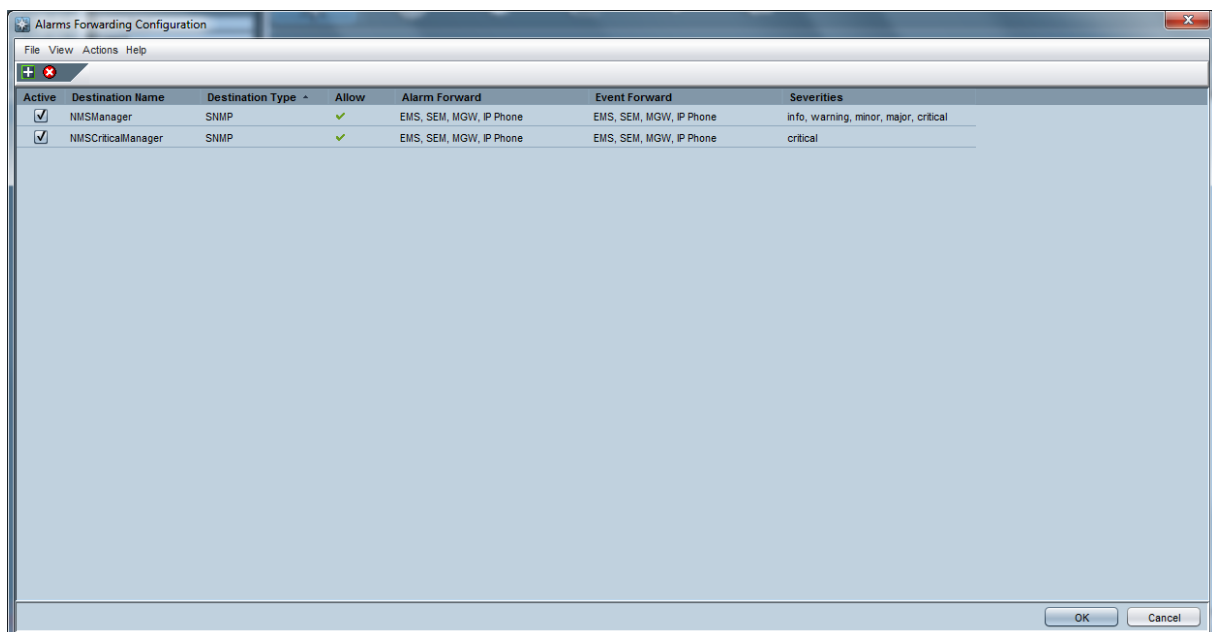
Privacy Key:

OK Cancel

4. In the left-hand pane, provision the following parameters for defining the destination rule:
 - 'Destination Rule Name' as you wish it to appear in the summary screen.
 - 'Allow Forward' or 'Prevent Forward': allow or prevent the forwarding of specific alarms according to the filtering criteria specified in the 'Destination Rule' Configuration window. When you select the 'Prevent Forward' or 'Allow Forward' buttons, and then specify additional filter criteria (as described in this step), then alarms are forwarded according to the specified filter criteria. For example, when you select 'Prevent Forward', and then select the 'Minor Alarms' severity icon, then minor alarms are not forwarded (according to the entities selected in the 'Alarm Origin' table). Alternatively, when you select 'Prevent Forward', and then in the 'Source' field, you specify 'Board#1/EthernetLink#2', then whenever LAN port #2 is down, an Ethernet link alarm is not forwarded.
 - Select the following subset of alarms and events to forward to the NMS (by default, all the alarms and events are selected):
 - ◆ SEM Alarms
 - ◆ SEM Events
 - ◆ MGW Alarms
 - ◆ MGW Events
 - ◆ IP Phone Events
 - ◆ IP Phone Alarms

- Alarm Names: allows the user to forward alarms according to specific alarm names. For example, setting this filter to forward the 'Power Supply' alarm.
 - Alarm Types: allows the user to forward alarms according to specific alarm types. For example, forwarding only 'communications-related' alarms.
 - Select the subset of 'Severities To Forward': severities that you wish to receive in the NMS application (by default, all the severities are selected).
Note: CLEAR alarms for selected subset of the alarms are always forwarded.
 - Source: allows the user to forward alarms according to the alarm source as displayed in the Alarm Browser 'Source' field. For example, 'EMS server' or a specific device board number.
 - Source MGW List: Select the devices from which you wish to forward alarms and events. The selected devices are displayed in the dialog box below. In the right-hand pane, provision the following parameters:
5. In the right-hand pane:
- In the 'Destination Host IP Address' field, enter the NMS IP address.
 - In the 'Destination Host port' field, enter the port number of the destination host (the default SNMP port for trap reception is **162**).

Figure 4-4: Traps Forwarding Configuration



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

6. (Optional) Select the 'Enable SNMPv3 Configuration' box to enable forwarding traps to the NMS using SNMPv3. In this case, set the following additional fields:
 - In the 'Security Name' field, enter the Security name of the SNMPv3 user.
 - From the 'Authentication Protocol' drop-down list, select an authentication protocol. The corresponding security level is displayed in the 'Security Level' field.
 - In the 'New Authentication Password' field, enter a new Authentication Password.
 - From the 'Privacy Protocol' drop-down list box, select a Privacy Protocol.
 - In the 'New Privacy Password' field, enter a new Privacy Password.
7. Click **OK**.



Note: During the EMS synchronization process with the managed devices, the EMS may recover missed alarms. As part of the alarms definition in the EMS, missed alarms are also forwarded to the NMS. By default, this synchronization process is performed with the Gateway Alarms History tables. When only partial Alarms History table is retrieved, the EMS notifies the user with one of the following events: 'Synchronizing Alarms Event' and 'Synchronizing Active Alarms Event'. For more details regarding Events fields and suggested corrective actions, see the relevant product *Performance Monitoring and Alarm Guide*.

4.1.3 Forwarding Alarms Directly from Devices

Alarms are forwarded directly from the network element to the NMS over SNMPv2 or SNMPv3. The SNMPv3 protocol provides more sophisticated security mechanisms than SNMPv2c. It implements a user-based security model (USM), allowing both authentication and encryption of the requests sent between the EMS Manager and their agents, as well as user-based access control. This section describes the SNMP settings on the EMS server side. You must configure identical SNMP settings on the managed devices (refer to Chapter "Configuring SNMP" in the *EMS User's Manual*).

4.1.3.1 Configuring SNMPv3 User Settings

This section describes how to configure the SNMPv3 user settings.

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

1. Right-click the device you wish to provision in the MG Tree and choose **Details**; the MG Information screen opens (see the figure below).
2. In the 'Security Name' field, enter the Security name of the SNMPv3 user.
3. In the 'Authentication Protocol' field, select an authentication protocol from the drop-down list box. The corresponding security level is displayed in the Security Level field.
4. In the 'New Authentication Password' field, enter a new Authentication Password; In the Privacy Protocol field, select a Privacy Protocol from the drop-down list box;

5. In the 'New Privacy Password' field, enter a new Privacy Password.

➤ **To switch MG & EMS communication from one SNMP version to another via EMS:**

1. In the Region Status screen, select one or more devices (multiple selections are relevant when all the devices are updated to the same community strings / passwords).
2. Right-click **Configuration** ➤ **SNMP Configuration** option. The MG Information screen is displayed.

Figure 34-5: MG Information-New SNMPv3 User



The image shows a 'SNMP Configuration' dialog box. At the top, there are two radio buttons: 'SNMPv2' and 'SNMPv3'. The 'SNMPv3' radio button is selected. Below the radio buttons, the 'SNMP' section is expanded, showing several fields: 'Engine ID' (text box), 'Security Name' (text box), 'Security Level' (dropdown menu with 'No Security' selected), 'Authentication Protocol' (dropdown menu with 'None' selected), 'Authentication Key' (text box), 'Privacy Protocol' (dropdown menu with 'None' selected), and 'Privacy Key' (text box). At the bottom of the dialog, there is a checkbox labeled 'Update Media Gateway SNMP Settings' which is checked. Below the checkbox are 'OK' and 'Cancel' buttons.

3. To switch from a SNMPv2 user to a SNMP v3 user, click the SNMPv3 button and enter the required SNMPv3 fields as described above.
4. To switch from an SNMP v3 user to a SNMP v2 user, click the SNMPv2 button and fill in the SNMP community strings.
5. Select the **Update Media Gateway SNMP Settings** checkbox.

EMS updates the EMS database and the device. If you do not check this option, any changes performed in the MG Information screen are only updated to the EMS database.



Note: When you switch from a SNMPv2 to a SNMPv3 user and select the **Update Media Gateway SNMP Settings** checkbox, the EMS logs into the device using the SNMPv2 user privileges. SNMPv3 user privileges are used the next time you connect to the device. Sometimes this operation might take up to three minutes.

4.1.3.2 Modifying SNMPv2 Community Strings or SNMPv3 Passwords

This section describes how to modify SNMPv2 Community Strings or SNMPv3 passwords.

➤ **To Modify SNMPv2 community strings or SNMP v3 User Passwords in MG & EMS via EMS:**

1. From the Region Status screen, select CPE/s (multiple selections are relevant when all the devices are updated to the same community strings / passwords) and right-click **Configuration** ➤ **SNMP Configuration** option.

Figure 34-6: Update SNMPv2 Settings for Multiple Devices

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

4.1.3.3 Configuring Additional SNMPv3 Users

You can configure additional SNMPv3 users with different security permissions or for sending traps to another SNMP Trap Manager such as an NMS.

For managing devices running firmware versions 7.0 or later, you must use the device's Web server to configure additional SNMP users. In the device's Web server, configure the following:

- In the SNMPv3 Users table, add the new SNMPv3 user (ensure that "SNMPUsers_Group" is set to **Trap**).
- In the SNMP Trap Destinations table, assign the new trap user to the EMS server entry or add a new entry for an additional SNMP trap manager and assign the new user to this trap manager.

For more information, refer to the relevant device's *SIP User's Manual*.

4.1.3.4 SNMPv3 User Cloning

According to the SNMPv3 standard, SNMPv3 users on the SNMP agent (on the device) cannot be directly added via the SNMP protocol e.g. SNMP Manager (EMS). Instead new users must be added via User Cloning. The SNMP Manager then creates a new user based on the original SNMPv3 user permission levels.

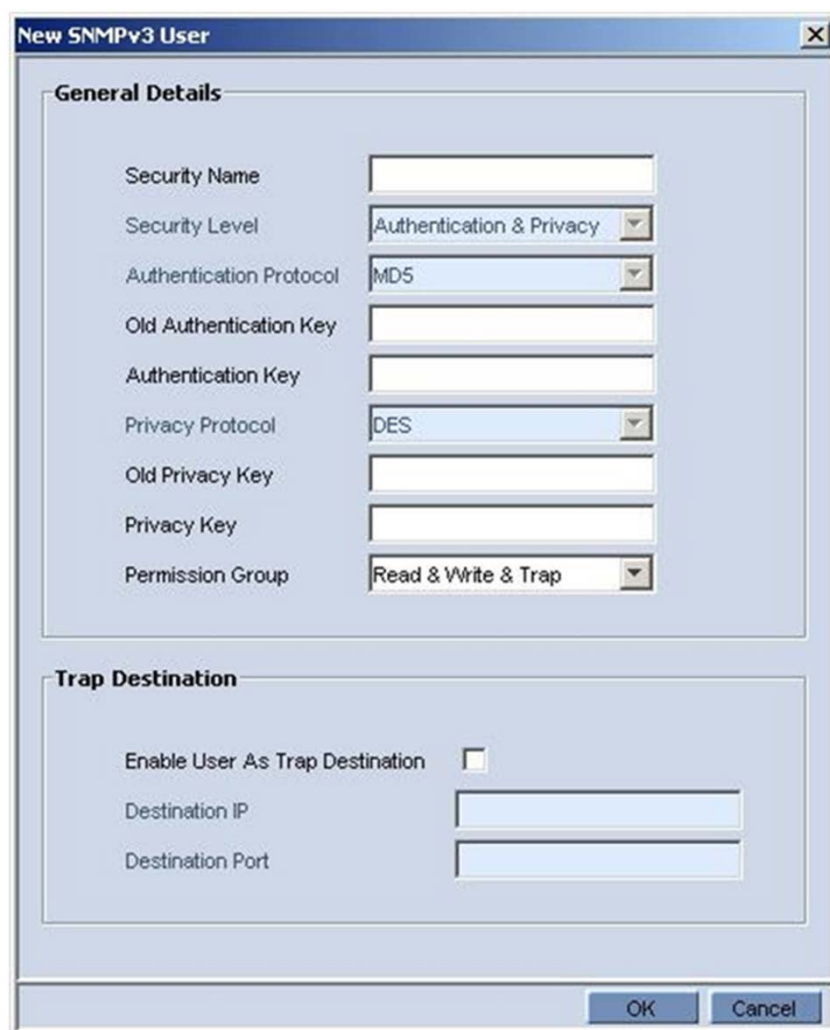


Note: The procedure below is only relevant for managed devices running firmware prior to version 7.0.

➤ To clone SNMPv3 users:

1. In the Desktop toolbar, click **Configuration** and in the Configuration pane, click **Network Frame**; The Network Parameters Provisioning screen is displayed.
 2. Select the **SNMPv3 Users** tab and select the user you wish to clone permission levels.
 3. Click **+** button; the New SNMPv3 User window is opened.
 4. Provide a new user name, old passwords of the user you clone permissions from and new user passwords.
 5. Select a User permission group.
 6. If the new user wishes to receive traps to the defined destination, check the **Enable User as Trap Destination** option to provision Trap a destination IP and Port. The EMS adds this new user to the SNMP Trap Managers Table. It is also possible to define an additional trap destination after a new user is defined.
- The new user is added to the SNMPv3 Users table.

Figure 34-7: MG Information Screen-New SNMPv3 User



The image shows a 'New SNMPv3 User' dialog box with two main sections: 'General Details' and 'Trap Destination'. The 'General Details' section contains fields for Security Name, Security Level (set to 'Authentication & Privacy'), Authentication Protocol (set to 'MD5'), Old Authentication Key, Authentication Key, Privacy Protocol (set to 'DES'), Old Privacy Key, Privacy Key, and Permission Group (set to 'Read & Write & Trap'). The 'Trap Destination' section contains a checkbox for 'Enable User As Trap Destination' (unchecked), and fields for 'Destination IP' and 'Destination Port'. At the bottom right are 'OK' and 'Cancel' buttons.

General Details	
Security Name	<input type="text"/>
Security Level	Authentication & Privacy
Authentication Protocol	MD5
Old Authentication Key	<input type="text"/>
Authentication Key	<input type="text"/>
Privacy Protocol	DES
Old Privacy Key	<input type="text"/>
Privacy Key	<input type="text"/>
Permission Group	Read & Write & Trap

Trap Destination	
Enable User As Trap Destination	<input type="checkbox"/>
Destination IP	<input type="text"/>
Destination Port	<input type="text"/>

OK Cancel

4.1.4 Alarms Clearing Mechanism

The Alarm Browser for each device is cleared of all the current alarms upon system GW startup (cold start event). Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) when a Clear alarm is generated by the same entity (source) and the same device. This feature prevents irrelevant alarms from congesting the Alarms Browser. Operators only view the list of the currently active alarms.

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

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

4.1.5 Events Clearing Mechanism

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

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

4.1.6 Alarm Suppression Mechanism

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

4.1.7 Alarms Sequence Numbering

1. When receiving alarms directly from the device, SEM or IP Phone:
 - These alarms and events have a different scale of sequence numbers. These sequence numbers are placed at 'TrapGlobalsUniqID' varbindings (respectively 'tgTrapGlobalsUniqID', 'acBoardTrapGlobalsUniqID').
 - EMS alarms have a sequence number scale. Events are always sent with 'acEMSTrapGlobalsUniqID -1'.
2. When the EMS forwards device and EMS alarms:
 - Cold Start Trap is the only standard event that is forwarded by the EMS application. The remainder of the standard Notifications are not forwarded.
 - Each one of the alarms and events are forwarded with the original Notification OID and variable bindings OIDs.
 - The original content of 'TrapGlobalsUniqID' varbinding (respectively 'tgTrapGlobalsUniqID', 'acBoardTrapGlobalsUniqID' and 'acEMSTrapGlobalsUniqID') is updated as follows:
 - ◆ For all the forwarded events, the 'TrapGlobalsUniqID' is set to -1.
 - ◆ For all the forwarded alarms, the original 'TrapGlobalsUniqID' is replaced with the EMS sequence number, allowing the NMS to follow the forwarded alarms sequencing. The original device 'TrapGlobalsUniqID' is transferred to 'TrapGlobalsAdditionalInfo3' varbinding.
 - ◆ For all the forwarded alarms and events, 'TrapGlobalsAdditionalInfo3' varbinding (respectively 'tgTrapGlobals AdditionalInfo3', 'acBoardTrapGlobals AdditionalInfo3' and 'acEMSTrapGlobals' 'AdditionalInfo3') is updated as follows: original device IP address and device 'TrapGlobalsUniqID' in the following format:

```
GATEWAY_IP:x , GATEWAY_TRAP_ID:y
```

4.1.8 Alarms Synchronization via MG SNMP I/F

Alarm Synchronization is supported for alarms and not for events. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account Element Management system outages, network outages, and transport mechanism, such as SNMP over UDP. This mechanism is implemented in the level SNMP agent, and serves EMS, NMS, or higher level management system synchronization purposes.



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

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

■ Active Alarms

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

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

- CPE's – 200 alarms
- MP 11x, MP 124 - 40 alarms

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

- The device sends a cold start trap to indicate that it is starting up. This allows the management system to synchronize its view of the device's active alarms.
- Two views of active alarms table are supported by devices:
 - ◆ **Standard MIB:** alarmActiveTable and alarmActiveVariableTable in the IETF ALARM MIB for all the devices.
 - ◆ **Enterprise MIB:**
 - ✓ acActiveAlarmTable in the AC-ALARM-MIB mib for devices products.

■ History Alarms

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

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

- CPE's – 1.000 alarms
- MP 11x, MP 124 - 100 alarms

When the history alarm list exceeds its maximum size, it starts overriding the oldest alarms in the list in cyclic order.

- The following views of log history alarms table are supported by the devices:
 - ♦ **Standard MIB:** 'nlmLogTable' and 'nlmLogVariableTable' in the NOTIFICATION-LOG-MIB for all the devices.
 - ♦ **Enterprise MIB:**
 - ✓ acAlarmHistoryTable in the 'AC-ALARM-MIB mib' for CPE and MP products.

4.1.9 EMS Keep-alive

You can configure the EMS to generate SNMP Keep-alive traps toward the SNMP destination. When the “EMS Keep-Alive” check box is checked, this trap is sent from the EMS to a configured destination according to a configured interval (default 60 seconds). You can send the Keep-alive trap to the desired SNMP destination (according to an existing configured forwarding destination rule).

➤ **To configure EMS Keep-alive:**

1. In the EMS menu, choose **Faults > Alarm Settings**.

Figure 24-8: EMS Keep-alive

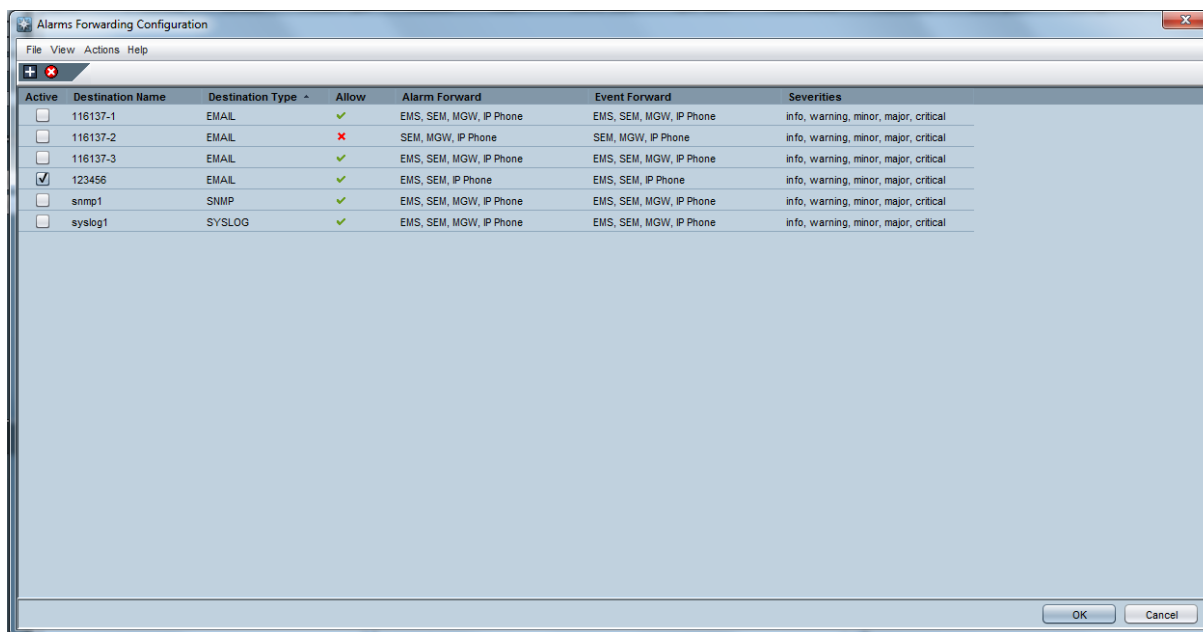
The screenshot shows the 'Alarms Settings' dialog box with the following sections:

- Events Automatic Clearing:**
 - Events Automatic Clearing: ☒
 - Events Automatic Clearing Period (days): 3
- Alarms Automatic Clearing:**
 - Alarms Automatic Clearing: ☐
 - Alarms Automatic Clearing Period (days): 30
- Alarms Suppression:**
 - Alarms Suppression: ☒
 - Alarms Suppression Counter Threshold: 5
 - Alarms Suppression Interval (seconds): 60
 - Note that this configuration applies to the same alarm type from the same source
- EMS Keep-Alive (highlighted with a red rectangle):**
 - EMS Keep-Alive: ☐
 - EMS Keep-Alive (seconds): 60

At the bottom of the dialog, there is a 'Destination Provisioning' button and 'OK' and 'Cancel' buttons.

2. Select the EMS Keep-Alive check box.
3. Click the **Destination Provisioning** button; the Alarm Forwarding Configuration window is displayed

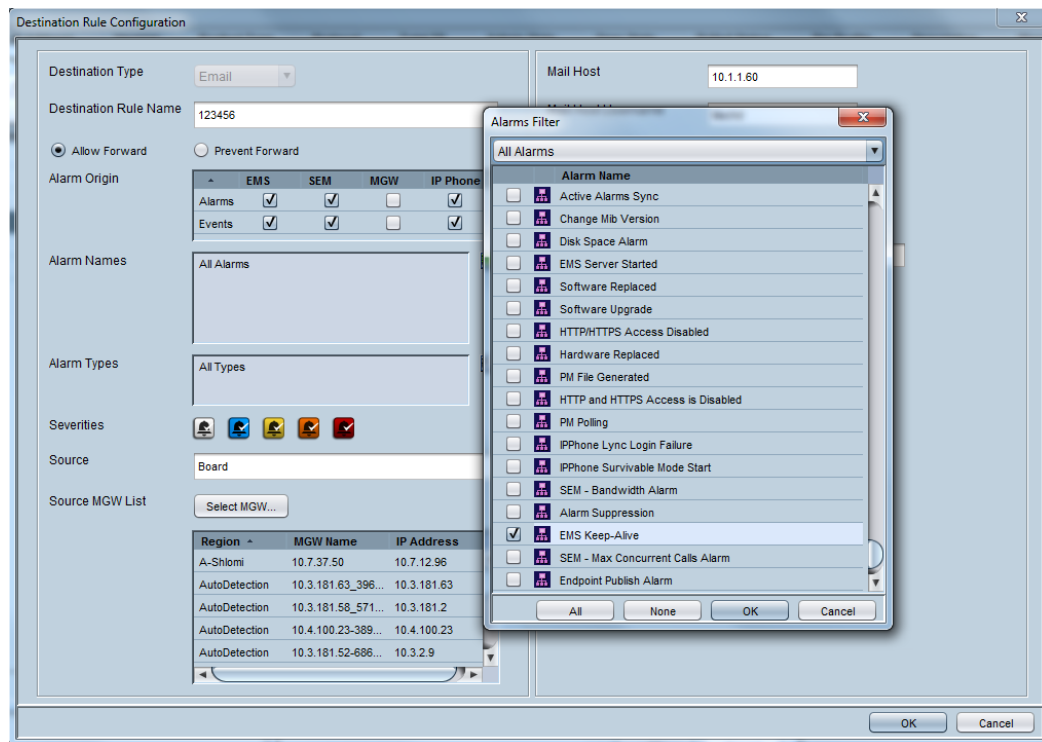
Figure 24-9: Alarm Forwarding Configuration



4. Select the Active check box for the destination that you wish to forward the EMS Keep-alive trap.

5. Double-click the destination rule to open the Destination Rule Configuration window.

Figure 24-10: Destination Rule Configuration



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

4.2 Status / State Management via MG SNMP I/F

For details regarding supported SNMP MIBs, refer to the *SNMP Reference Guide*.

5 Performance Monitoring

Customers often face a complex VoIP network with minimal information on the status and capacities of each component in the network. PMs help the system architect design a better network. In addition, PMs help operators discover malfunctioning devices before they start causing a problem on the production network.

The system provides two types of performance measurements:

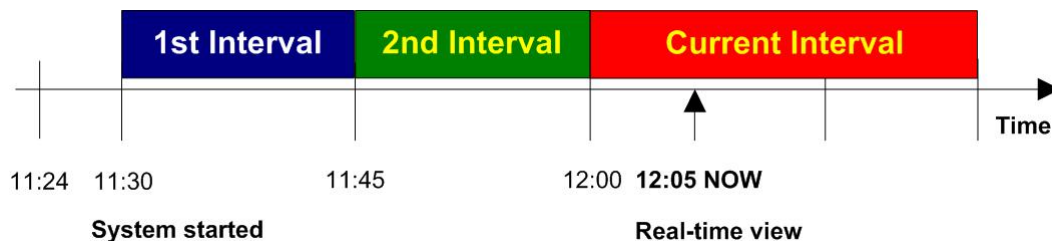
- **Gauges:** Gauges represent the current state of a PM parameter in the system. Gauges, unlike counters, can decrease in value, and like counters, can increase in value. For Gauges, the interval data is referred as *minimum*, *maximum* and *average* values.
- **Counters:** Counters always increase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

Performance Management is composed of real-time and historical data monitoring.

Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. The EMS application supports graphical representation of the real-time data and provides the user with graphical tools to perform high-frequency polling of various system parameters. For more information on graph types and the User Interface, refer to the *EMS User's Manual*.

Historical data can be used by NMS and OSS systems for long-term network analysis and planning.

Figure 5-1: Performance Monitoring - Intervals



History Performance is measured in a constant time interval of 15 minutes to which all elements in the network are synchronized. Intervals commence precisely every 15 minutes, for example, 12:00:00, 12:15:00, 12:30:00, 12:45:00, etc. This allows synchronization of several management systems to the same interval time frame. Note that the first interval after start-up is always shorter (in the example above, the first interval only lasts 6 minutes - so that a new interval can start exactly on the 15 minute interval, in this case 11:30:00). During the initial start-up interval i.e. 6 minutes in the example above, polling is not performed.

**Note:**

- AudioCodes equipment support 15-minute intervals for historical performance monitoring data collection.
- To perform accurate history PM polling, all the network elements (gateway, SEM, IP Phones , EMS and NMS) must be synchronized on the same NTP server. The EMS server machine can also be defined as an NTP server machine.

The NMS can receive performance monitoring data using one of the following methods:

- Collecting .csv or .sml files from the EMS server machine via FTP or SFTP. EMS performs SNMP polling of the network elements and creates a summary file per element per collection interval. See [Section 5.1](#).
- Collecting information directly from the network element via the SNMP interface. For more information, see [Section 5.2](#).

5.1 EMS Server CSV / XML File Format Interface

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

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

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

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

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

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



Note: Currently only 15 minutes intervals are supported.

Users can choose to receive a trap when each file is created. The trap name is 'acEMSPmFileGenerate' and contains information on the file name and the time it was created. Note the following:

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

5.1.2 XML File Format

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

Figure 5-3: xml File Header Example

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

Figure 5-4: xml File Data Example

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

5.2 Devices SNMP Interface

Refer to the specific device's *Performance Monitoring and Alarm Guide* for the exact list of supported performance measurement parameters. Note that these Guides include both EMS and SNMP parameter names.

6 SEM Scheduled Reports

Scheduled reports can be generated in the SEM for selected managed devices. This report contains the tabulated call statistics and summary data that have been retrieved from these managed devices by the SEM. See an example of scheduled report in the figure below. For more information, refer to the *SEM User's Manual*.

Figure 6-1: SEM Scheduled Report

```
Scheduler Name: Try
Scheduler Description: null
Scheduler Period: Hourly

Report Generation Number: 1
Report Generated at: Tue Aug 23 15:10:00 +0300 2016

Report Name: Call Statistics By Device (40)
Report Topic Name: Network Status Reports (0)
Report Group Name: SEM Report (0)

From: Tue Aug 23 14:10:00 +0300 2016
To: Tue Aug 23 15:10:00 +0300 2016

Top Users Number:

Report Devices: hkgiksdfvns;adasda;assaa;FE1;Med1;ACL FE;ac1lync01.corp.audiocodes.com;tytyt;11.200.1
Report Links:

Table:
Report ID,Device Name,Calls#,Calls$,Total Duration,AVG Duration,Established Calls,Max Concurrent Call
40,172.17.116.72-5713853,100,12.06,00:08:20,00:00:05,100,0,100.0,0.0,100,0,0.0,0.0,0.0,100.0,0,0,0,10
40,172.17.116.72-5223883,300,36.19,00:10:00,00:00:05,120,35,40.0,60.0,120,180,0.0,0.0,0.0,100.0,0,0,0,0
40,172.17.116.219-9397067,100,12.06,00:06:40,00:00:05,80,35,80.0,20.0,80,20,0.0,0.0,0.0,100.0,0,0,0,1
40,167.17.116.219-9397067,100,12.06,00:06:40,00:00:05,80,35,80.0,20.0,80,20,0.0,0.0,0.0,100.0,0,0,0,1
```

This page is intentionally left blank.

7 EMS Server Backup

There are two main backup processes that run on the EMS server:

- **Weekly backup:** runs once a week at a pre-configured date & time (default is Saturday 02:00). In this process, the whole database is backed up into several “RMAN” files that are located in /NBIF/emsBackup/RmanBackup directory. In addition, many other configuration and software files are backed up to a TAR file in the /data/NBIF/emsBackup directory. In general, this TAR file contains the entire /data/NBIF directory's content (except 'emsBackup' directory), EMS Software Manager content and server_XXX directory's content.

To change the weekly backup's time and date, refer to the *EMS SEM and IP Phone Manager IOM Manual*.

- **Daily backup:** runs daily except on the scheduled week day (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.



Warning: The Backup process does not backup configurations performed using EMS Server Manager, such as networking and security.

It is highly recommended to maintain all backup files on an external machine.

These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user. These backup files are as follows:

- /data/NBIF/emsBackup/emsServerBackup_<time&date>.tar file.

All files in /data/NBIF/emsBackup/RmanBackup directory (including control.ctl and init.ora files).

This page is intentionally left blank.

8 Security

The following aspects are relevant for the NMS application when integrating the EMS and the Media Gateway:

- Network Communication Protocols (see below).
- OVOC Users Management (Authentication and Authorization) (see Section 8.2).
- HTTPS Connection (see Section 8.3)



Note: For detailed information, refer to the *OVOC Security Guidelines* document.

8.1 Network Communication Protocols

The following describes the different EMS network communication protocols:

- EMS client - server communication is secured using an HTTPS tunnel with a single HTTPS port. EMS also enables client installation and launching via JAWS running over HTTPS.
- EMS server – managed devices communication can be secured as follows:
 - Devices:
 - ◆ SNMPv3 for Maintenance Action, Faults and Performance Monitoring
 - ◆ HTTPS for file transfer and for Single-Sign On to the device's Web server
- EMS server secure access:
 - Secure access to the EMS server machine is possible via SSH and SFTP protocols for performing maintenance actions and accessing files.
 - SNMPv3 traps can be forwarded from the EMS server machine to another SNMP Trap Manager.
 - EMS User Authentication and Authorization is performed either via the EMS Application local database, or via a centralized RADIUS or LDAP server database (see Section 8.2) according to the Security profile configured by the EMS Administrator. For more information, refer to the 'Security Management' chapter in the *EMS User's Manual*.



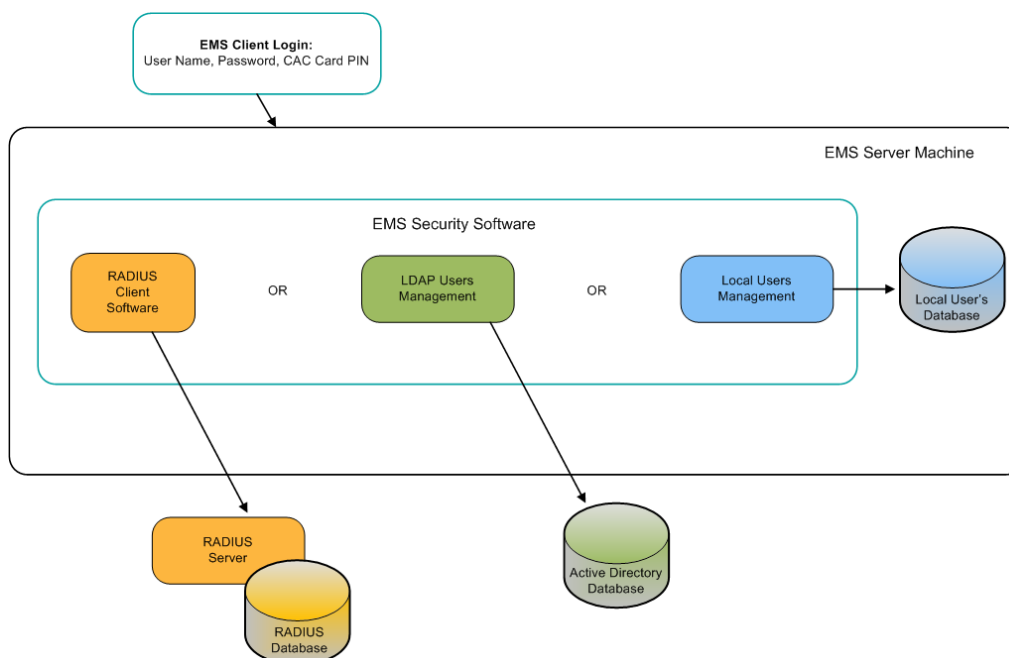
Note:

- Syslog messages and emails sent from the EMS to a northbound interface are not secured.
- Single sign-on is not supported for devices located behind a NAT.

8.2 OVOC User Identity Management

By default, OVOC users (EMS, SEM and IP Phone Manager) are managed in the local EMS server where the usernames and passwords are saved in the local EMS database. Alternatively, users can be managed via a centralized RADIUS or LDAP server. The figure below illustrates these options.

Figure 8-1: OVOC User Management



- For information on the local EMS users database, refer to the EMS User's Manual.
- For RADIUS server management, see Section 8.2.1
- For LDAP server management, see Section 8.2.2



Note: The RADIUS server is not supported for the IP Phone Manager and SEM applications.

8.2.1 Authentication and Authorization using a Radius Server

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

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

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

8.2.1.1 Configuring Radius Server Client

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

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



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

➤ **To set up EMS RADIUS client using FreeRADIUS:**

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

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

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

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

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

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

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

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

```
# users - local user configuration database

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

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

4. Record and retain the IP address, port number, 'shared secret', vendor ID and VSA access level identifier (if access levels are used) used by the RADIUS server.
5. Provision the relevant EMS parameters according to the section below.

8.2.1.2 Configuring RADIUS Server

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

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

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

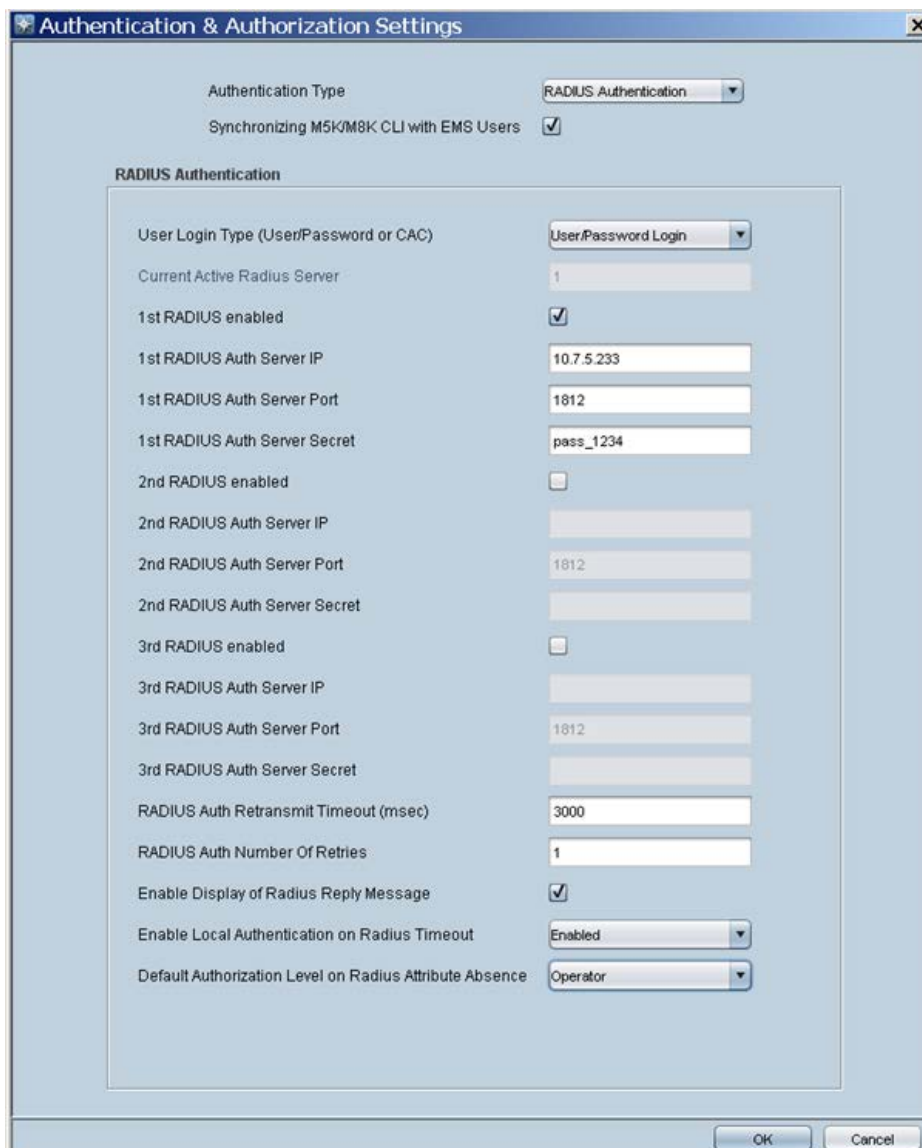


Note: This method is not supported for the SEM and IP Phone Manager applications.

➤ **To configure using a RADIUS server.**

1. In the EMS menu, choose **Security > Authentication & Authorization**; the RADIUS Authentication & Authorization Settings screen is displayed.
2. From the Authentication Type drop-down list, select **RADIUS Authentication**.

Figure 35-2: RADIUS Authentication and Authorization



Authentication & Authorization Settings

Authentication Type: RADIUS Authentication

Synchronizing M5K/M8K CLI with EMS Users: ☒

RADIUS Authentication

User Login Type (User/Password or CAC): User/Password Login

Current Active Radius Server: 1

1st RADIUS enabled: ☒

1st RADIUS Auth Server IP: 10.7.5.233

1st RADIUS Auth Server Port: 1812

1st RADIUS Auth Server Secret: pass_1234

2nd RADIUS enabled: ☐

2nd RADIUS Auth Server IP:

2nd RADIUS Auth Server Port: 1812

2nd RADIUS Auth Server Secret:

3rd RADIUS enabled: ☐

3rd RADIUS Auth Server IP:

3rd RADIUS Auth Server Port: 1812

3rd RADIUS Auth Server Secret:

RADIUS Auth Retransmit Timeout (msec): 3000

RADIUS Auth Number Of Retries: 1

Enable Display of Radius Reply Message: ☒

Enable Local Authentication on Radius Timeout: Enabled

Default Authorization Level on Radius Attribute Absence: Operator

OK Cancel

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

4. Define the following parameters:

- RADIUS Auth Retransmit Timeout' (default-3000 msec)
- RADIUS Auth Number of Retries (default-1)

Note that these parameters will be used for each one of the Radius Servers.

5. Determine if you wish to display the Radius Reply message. By default, the parameter 'Enable Display of Radius Reply Message' is enabled.
6. Set parameter 'Enable Local Authentication on Radius Timeout' to determine whether local authentication is performed whenever the connection to the RADIUS server fails. By default, the parameter 'Enable Local Authentication on Radius Timeout' i.e. EMS local authentication is enabled (see note above). This parameter's behavior depends on the parameter 'RADIUS Auth Retransmit Timeout', whenever this timeout expires, local authentication is performed.
7. Set the parameter 'Default Authorization Level on Radius Attribute Absence' . 'Default Authorization Level on Radius Attribute Absence'. This parameter defines the EMS behavior in cases where the user has been successfully authenticated by the RADIUS server; however, the RADIUS server response does not include an EMS security level (Authorization Vendor Specific Element). This implies that the user properties custom attribute "Security Level" (this attribute is specifically defined for the EMS) has not been defined on the RADIUS server and configured with one of the EMS Security levels (Not visible; Monitoring (viewing only); Operation (viewing and all system provisioning operations on devices); Administration or Administrator Super User). In this case, the Administrator can either deny user access or set a default security level to grant to the user. By default, the EMS provides access to the application with the "Operator" security level.
8. Configure other parameters as required according to your RADIUS server configuration.

8.2.2 Authentication and Authorization using an LDAP Server

This section describes how to setup EMS users (in the EMS application) for authentication and authorization using an LDAP server.

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



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

➤ To configure using an LDAP server.

1. In the EMS menu, choose **Security > Authentication & Authorization**; the LDAP Authentication & Authorization Settings screen is displayed.

2. From the Authentication Type drop-down list, select **LDAP Authentication**.

Figure 35-3: LDAP Authentication and Authorization

The screenshot shows the 'Authentication & Authorization Settings' dialog box. At the top, 'Authentication Type' is set to 'LDAP Authentication'. Below it, 'Synchronizing Msk/Msk CLI with EMS Users' is unchecked. The 'LDAP Authentication' section contains the following fields:

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

At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Configure the LDAP Authentication Server IP and Server Port.
4. Configure the LDAP Connectivity DN parameter as required.
5. Configure LDAP Connectivity Password as required.
6. Configure the User DN Search Base as required.
7. 'Default Authorization Level on LDAP Group Absence'. This parameter defines the EMS behavior in cases where the user has been successfully authenticated by the LDAP server; however, the LDAP server response does not include an EMS security level (Authorization Vendor Specific Element). This implies that the user properties custom attribute "Security Level" (this attribute is specifically defined for the EMS) has not been defined on the LDAP server and configured with one of the EMS Security levels (Not visible; Monitoring (viewing only);

Operation (viewing and all system provisioning operations on devices); Administration or Administrator Super User). In this case, the Administrator can either deny user access or set a default security level to grant to the user. By default, the EMS provides access to the application with the "Operator" security level.

8. If you wish to secure the connection with the LDAP server over SSL:
 - a. From the "LDAP Server Number of Retries" drop-down list, select one of the following options:
 - ◆ **Plain Connection (default):** non-secured connection with the LDAP server.
 - ◆ **SSL With Certificate:** an HTTPS connection between the EMS server and the LDAP server is opened. The EMS authenticates the SSL connection using a certificate.
 - ◆ **SSL Without Certificate:** an HTTPS connection between the EMS server and the LDAP server is opened; however is not authenticated using a certificate.
 - b. From the "LDAP Client Certificate" drop-down list, select the certificate file that you wish to use to secure the connection with the LDAP server.



Note:

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

8.3 HTTPS Connection

You can secure the connection between the NBIF client and the EMS server over HTTPS (port 443). You can secure this connection either using AudioCodes default self-signed certificates or by applying custom certificates signed by an external CA. For more information, refer to the *OVOC Security Guidelines* document.

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

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

Contact us: www.audiocodes.com/contact

Website: www.audiocodes.com

©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-19213

