Alarms Guide

AudioCodes One Voice™ Operations Center

Managed Devices and Endpoints

Version 7.4

HD VoIP Sounds Better

AudioCodes

Contents

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 can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: September-26-2017

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 E-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
One Voice Operations Center IOM Manual
AudioCodes One Voice Operations Center Product Description
One Voice Operations Center User's Manual
IP Phone Management Server Administrator's Manual
IP Phone Manager Express Administrator's Manual
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
ARM User's Manual

Document Revision Record

LTRT	Description
41606	Initial document release for Version 7.4

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 Introduction

This document describes alarms that are raised on AudioCodes devices and endpoints. These alarms are displayed in the One Voice Operations Center Web interface.

Supported alarms / events can fall into one of these three categories:

- Standard traps: traps originated by the media gateway / server - all the standard traps are treated are events.
- Proprietary alarms / events: traps originated by the media gateway / server and defined in the gateway proprietary MIB.
- EMS alarms / events: traps originated by the EMS application and defined in the EMS proprietary MIB.

To find out which traps are defined as Events refer to 'Alarm Name' or 'Alarm Title' fields in the table. All the events are marked with [Event] prefix. This is how events are marked in the EMS Alarms Browser and Alarms History windows.

Each alarm / event described in this section includes the following information:

Information Included in Each Alarm

Alarm Name	The alarm name, as it appears in the EMS Alarm Browser.
Alarm Source	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource. For the complete list of Managed Objects, refer to the Mediant 5000 / 8000 Programmers' User Manual.
Severity	Possible values of severities. This value is displayed from the variable-binding tgTrapGlobalsSeverity.
Alarm Type	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsType.
Alarm Probable Cause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.
Description	Textual description of specific problem. This value is displayed from the variable-binding tgTrapGlobalsTextualDescription. The document includes a few examples of the possible values of this field.
Additional Info	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo1, tgTrapGlobalsAdditionalInfo2 and tgTrapGlobalsAdditionalInfo3. The document includes a few examples of the possible values of this field.
SNMP Trap Name	NOTIFICATION-TYPE Name as it appears in the MIB.
SNMP Trap OID	NOTIFICATION-TYPE OID as it appears in the MIB.
Corrective Action	Possible corrective action when applicable.

This page is intentionally left blank.

2 Standard Events

2.1 Cold Start

Cold Start

Description	SNMPv2-MIB: A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
SNMP Alarm	coldStart
SNMP OID	1.3.6.1.6.3.1.1.5.1
Alarm Title	[Event] Cold Start
Alarm Type	Communication Alarm
Alarm Source	-
Probable Cause	Other
Severity	Clear
Additional Info1,2,3	-
Corrective Action	-

2.2 Link Down

Link Down

Description	SNMPv2-MIB: A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
SNMP Alarm	[Event] linkDown
SNMP OID	1.3.6.1.6.3.1.1.5.3
Alarm Title	Link Down
Alarm Type	Communication Alarm
Alarm Source	-
Probable Cause	Other
Severity	Major
Additional Info1,2,3	-
Corrective Action	-

2.3 Link Up

Link Up

Description	SNMPv2-MIB: A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
SNMP Alarm	[Event] linkUp
SNMP OID	1.3.6.1.6.3.1.1.5.4
Alarm Title	Link Up
Alarm Type	Communication Alarm
Alarm Source	-
Probable Cause	Other
Severity	Clear
Additional Info1,2,3	-
Corrective Action	-

2.4 Entity Configuration Change

Entity Configuration Change

Description	Entity-MIB: An entConfigChange notification is generated when the value of entLastChangeTime changes.
SNMP Alarm	[Event] entConfigChange
SNMP OID	1.3.6.1.2.1.47.2.0.1
Alarm Title	Entity Configuration Change
Alarm Type	Equipment Alarm
Alarm Source	-
Probable Cause	Other
Severity	Info
Additional Info1,2,3	-
Corrective Action	-

2.5 Authentication Failure

Authentication Failure

Description	SNMPv2-MIB: An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is no properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
SNMP Alarm	[Event] authenticationFailure
SNMP OID	1.3.6.1.6.3.1.1.5.5
Alarm Title	Authentication Failure
Alarm Type	Communication Alarm
Alarm Source	-
Probable Cause	Other
Severity	Major
Additional Info1,2,3	-
Corrective Action	-

This page is intentionally left blank.

3 Management Alarms

3.1 EMS Trap Receiver Binding Error

EMS Trap Receiver Binding Error

Description	This alarm is generated during server startup if an error occurs indicating that the SNMP trap receiver port is already taken.
SNMP OID	acEMSSnmpCannotBindError- 1.3.6.1.4.1.5003.9.20.3.2.0.1
AlarmTitle	[Event] EMS Trap Receiver Binding Error
ItuAlarmType	Environmental Alarm
AlarmSource	Management
Probable Cause	Application Subsystem Failure
Severity	Critical
Additional Info	-
Corrective Action	Run netstats command to verify which application uses the alarms reception port (by default UDP post 162). ▪ EMS application: If it's busy, check which application uses this port. If it's not freed by the EMS application, restart the EMS Server application according to the equipment installation manual. ▪ Other network management application: change the EMS application and all managed gateways' default alarm reception ports.
Media Gateways	All the gateways managed by the EMS

3.2 GW Connection Alarm

GW Connection Alarm

Description	Originated by the EMS when an SNMP Timeout occurs for the first time in the Media Gateway.
SNMP OID	acEMSNodeConnectionLostAlarm - 1.3.6.1.4.1.5003.9.20.3.2.0.3
AlarmTitle	GW Connection Alarm
ItuAlarmType	Communications Alarm
AlarmSource	Media Gateway
Probable Cause	Communications Subsystem Failure
Severity	Critical
Additional Info	When an SBA is configured, displays the 'SBA Description' field.
Corrective Action	Communication problem: Try to ping the gateway to check if there is network communication. ▪ Default gateway alive: Open the network screen. Check the default gateway IP address and ping it. ▪ SNMP Community Strings: Verify that the community string defined in the EMS for the gateway matchs the actual gateway community strings. To check the community string, right-click on the gateway, select the 'Details' menu. Default community strings: read = public, write = private. ▪ Hardware Problem: Check that the gateway is alive according to the LEDs. Verify that network and power cables are in place and plugged in.
Media Gateways	All the gateways managed by the EMS

3.3 GW Mismatch Alarm

GW Mismatch Alarm

Description	Activated when the EMS detects a hardware, software, predefine or configuration mismatch. • Software Mismatch: Activated when the EMS detects a software version mismatch between the actual and the previous definition of the Media Gateway (for example, Version 4.0.353 instead of the previously defined 4.0.278). This is also the case when the new version is not defined in the Software Manager. • Hardware Mismatch: Activated when the EMS detects a hardware mismatch between the actual and the previous definition of a Media Gateway. • Configuration Mismatch: Activated when the EMS detects a configuration mismatch between the actual parameter values provisioned and previous parameter values provisioned.
SNMP OID	acEMSNoMismatchNodeAlarm - 1.3.6.1.4.1.5003.9.20.3.2.0.9
AlarmTitle	GW Mismatch Alarm
ItuAlarmType	Equipment Alarm
AlarmSource	Media Gateway/Software Media Gateway/Hardware Media Gateway/Configuration
Probable Cause	Other
Severity	Clear
Additional Info	-

Corrective Action	• Software Mismatch: ✓ Define the detected version in the EMS Software Manager ✓ Perform a Software Upgrade on the gateway with one of the supported versions. • Hardware Mismatch: ✓ Perform remove / add a gateway from the EMS tree in order to resync EMS and the gateway status ✓ Verify in the Software Manager that an appropriate version exists for the hardware type displayed in the error message • Configuration Mismatch: ✓ Run Configuration Verification command in order to compare EMS configuration and actual MG configuration: **-MG configuration is incorrect**: use configuration download to update MG with correct configuration saved in the EMS database. **-MG is correct, EMS is not updated**: use configuration upload to save a correct MG configuration in the EMS database. • Check the Actions Journal for recent updates of the gateway.
Media Gateways	All the gateways managed by the EMS.

3.4 EMS Server Started

EMS Server Started

Description	Originated each time the server is started or restarted (warm boot/reboot) by the EMS Watchdog Process
SNMP OID	acEMSServerStartup- 1.3.6.1.4.1.5003.9.20.3.2.0.11
AlarmTitle	[Event] EMS Server Started
ItuAlarmType	Communications Alarm
AlarmSource	Management
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	All the gateways managed by the EMS.

3.5 Software Replaced

Software Replaced

Description	Originates when the EMS discovers a software version replace between board versions, for example, from V4.6.009.004 to V4.6.152.003 (when both versions are managed by the EMS). Software Replace old version : <old version> new version <new version>
SNMP OID	acEMSSoftwareReplaceAlarm- 1.3.6.1.4.1.5003.9.20.3.2.0.14
AlarmTitle	[Event] Software Replaced
ItuAlarmType	Communications Alarm
AlarmSource	Management
Probable Cause	Other
Severity	Info
Additional Info	If you initiated a performance measurements polling process before you initiated the software replacement process, the polling process is stopped.
Corrective Action	No action should be taken; this is an information alarm.
Media Gateways	All the gateways managed by the EMS.

3.6 Hardware Replaced

Hardware Replaced

Description	Originated when the EMS discovers a different gateway (according to the MAC address) to what was initially defined, while the Hardware Type remains the same. Hardware Replace is discovered by the MAC address and performed during Board Started trap.
SNMP OID	acEMSHardwareReplaceAlarm - 1.3.6.1.4.1.5003.9.20.3.2.0.15
AlarmTitle	[Event] Hardware Replaced
ItuAlarmType	Equipment Alarm
AlarmSource	Media Gateway
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000

3.7 HTTP/HTTPS Access Disabled

HTTP/HTTPS Access Disabled

Description	Originated when HTTP access is disabled by EMS hardening but the EMS manages media gateways that require HTTP access for software upgrade. Originated on server startup.
SNMP OID	acEMSHTTPDisabled - 1.3.6.1.4.1.5003.9.20.3.2.0.16
AlarmTitle	[Event] HTTP/HTTPS Access Disabled
ItuAlarmType	Environmental Alarm
AlarmSource	Management
Probable Cause	Application Subsystem Failure
Severity	Major
Additional Info	-
Corrective Action	Separate the gateways between two EMS servers (secured & unsecured)
Media Gateways	Gateways using the HTTP server for the software upgrade procedure: MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000

3.8 PM File Generated

PM File Generated

Description	Originated when a PM file is generated in the EMS server, and it can be retrieved by a higher level management system.
SNMP OID	acEMSPmFileGenerate - 1.3.6.1.4.1.5003.9.20.3.2.0.18
AlarmTitle	[Event] PM File Generated
ItuAlarmType	Other
AlarmSource	Management
Probable Cause	Other
Severity	Info
Additional Info	The performance summary data from<start polling interval time> to<timeStempFileTo> of media gateway<nodeIPAdd> was saved in PM file <fileName>.
Corrective Action	-
Media Gateways	All Gateways

3.9 PM Polling Error

PM Polling Error

Description	Originated when a PM History stops collecting performance summary data from MG. Possible reasons are: NTP synchronization lost, Connection Loss, SW Mismatch, etc..
SNMP OID	acEMSPmHistoryAlarm - 1.3.6.1.4.1.5003.9.20.3.2.0.19
AlarmTitle	[Event] PM Polling Error
ItuAlarmType	Other
AlarmSource	Management
Probable Cause	Other
Severity	Minor
Additional Info	-
Corrective Action	Verify in the 'Description' (see above) the reason why the PM history stopped. ▪ When the reason is 'NTP synchronization lost', verify that the gateway and the EMS Server machine are synchronized to the same NTP server and have accurate time definitions. ▪ When the reason is 'Software Mismatch', you can stop the PM history collection until the new version is added to the Software Manager. ▪ When the reason is 'Connection Loss' between the EMS Server and the gateway, polling continues automatically when the connection is re-established; the purpose of the alarm in this case is to inform users of missing samples. Note: The alarm continues to activate every 15 minutes unless you fix the problem or manually stop PM polling of the Gateway.
Media Gateways	All Gateways

3.10 Cold Start Missed

Cold Start Missed

Description	Originated when Carrier Grade Alarm System recognizes coldStart trap has been missed.
SNMP OID	acEMSNodeColdStartMissedEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.20
AlarmTitle	[Event] Cold Start Missed
ItuAlarmType	Other
AlarmSource	-
Probable Cause	Receive failure

Description	Originated when Carrier Grade Alarm System recognizes coldStart trap has been missed.
Severity	Clear
Additional Info	-
Corrective Action	-
Media Gateways	All the managed Gateways

3.11 Security Alarm

Security Alarm

Description	Activated when one of more Radius servers are not reachable. When none of the radius servers can be reached, a Critical Severity alarm is generated.
SNMP OID	acEMSSecurityAlarm - 1.3.6.1.4.1.5003.9.20.3.2.0.23
AlarmTitle	Security Alarm
ItuAlarmType	Processing Error Alarm
AlarmSource	Management / Radius <#>
Probable Cause	Other
Severity	Minor, Major, Critical
Additional Info	-
Corrective Action	-
Media Gateways	-

3.12 Security Event

Security Event

Description	This event is generated when a specific user is blocked after reaching the maximum number of login attempts, or when the EMS failed to sync EMS and Mediant 5000 / 8000 users.
SNMP OID	acEMSSecurityEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.24
AlarmTitle	[Event] Security Event
ItuAlarmType	Other
AlarmSource	Management / User Name, Management / User Sync
Probable Cause	Other
Severity	Indeterminate
Additional Info	-
Corrective Action	-
Media Gateways	-

3.13 Topology Update Event

Topology Update Event

Description	This event is issued by the EMS when a Gateway or Region is added/removed/updated in the EMS application and includes the following information: • Action: Add / Remove / Update GW or Region • Region Name • GW Name • GW IP Note: For opening an EMS client in the MG context, the gateway IP address should be provided.
SNMP OID	acEMSTopologyUpdateEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.25
Alarm Title	[Event] Topology Update
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other

Additional Info	Additional Info 1 field will include following details: Region: X1 'X2' [GW: Y1 'Y2' 'Y3' 'Y4'] X1 = Region ID (unique identifier in the EMS data base used for region identification) X2 = Region name as it defined by EMS operator Y1 = GW ID (unique identifier in the EMS data base used for GW identification) Y2 = GW Name as it defined by EMS operator Y3 = GW IP as it defined by EMS operator Y4 = GW Type as it identified by EMS during the first connection to the GW. If first connection was not successful during the add operation, it will trigger an 'Add GW' event with Unknown GW type, and 'Update GW' event once the initial connection to the GW has been successfull. The following GWs will be supported: MP,M1K, M2K, M3K, M5K, M8K Region details will always be part of the alarm, while GW info will be displayed when event is GW related. All the fields related to the GW will always be displayed to allow easy parsing. Examples: (Description=Add Region) Region: 7 'Test Lab' (Description=Update Region) Region: 7 'My Updated Region' (Description=Add GW) Region: 7 'My Updated Region', GW: 22 'MG14' '1.2.3.4' 'Unknown', PM Polling: disabled (Description=Update GW) Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7' 'M3K' (Description=Update GW) Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7', PM Polling: enabled (Description=Remove GW) Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7' 'M3K', Polling: enabled (Description=Remove Region) Region: 7 'My Updated Region'
Corrective Action	-
Media Gateways	-

3.14 Topology File Event

Topology File Event

Description	This event is issued by the EMS when the Topology File is updated on the EMS Server machine.The Topology file is automatically updated upon the addition /removal of a Media Gateway or upon updates to the Media Gateway properties. For more information, refer to the *OAMP Integration Guide*.
SNMP OID	acEMSTopologyFileEvent- 1.3.6.1.4.1.5003.9.20.3.2.0.26
Alarm Title	[Event] Topology File
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Additional Info	File Name: MGsTopologyList.csv
Corrective Action	-
Media Gateways	-

3.15 Synchronizing Alarms Event

Synchronizing Alarms Event

Description	This event is issued when the OC is not able to retrieve the entire missing alarms list from the History table. Information regarding the number of retrieved alarms, and number of alarms OC failed to retrieve is provided in the Additional Info field.
SNMP OID	acEMSSyncAlarmEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.27
Alarm Title	[Event] Synchronizing Alarms
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Additional Info	Retrieved x missed alarms, failed to retrieve y alarms.
Corrective Action	-
Media Gateways	-

3.16 Synchronizing Active Alarms Event

Synchronizing Active Alarms Event

Description	This event is issued when the OC is not able to perform synchronization with the History alarms table, and instead performs synchronization with the Active Alarms Table.
SNMP OID	acEMSSyncActiveAlarmEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.28
Alarm Title	[Event] Synchronizing Active Alarms
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Additional Info	-
Corrective Action	-
Media Gateways	-

3.17 Alarm Supression Alarm

Description	This alarm is sent when the EMS suppresses alarms (of the same alarm type and alarm source), once the number of such alarms reaches a configured threshold level in a configured interval (configured in the EMS in the Alarms Settings screen). When this alarm is sent, such alarms are not added to the EMS database and are not forwarded to configured destinations.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.42
Alarm Title	AlarmSuppressionAlarm
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Threshold crossed.
Alarm Text	Alarm Suppression activated
Status Changes	The alarm is cleared when in the subsequent interval, the number of such alarms falls below the configured threshold. Once the alarm is cleared, then these alarms are once more added to the EMS database and forwarded to configured destinations.
Additional Info	-
Corrective Action	Investigate the recurrence of such alarms.

3.18 EMS Keep Alive Alarm

Description	This alarm indicates that an SNMP Keep-alive trap has been sent from EMS to a third-party destination such as a Syslog server to indicate EMS liveness (configured in the EMS Alarms Settings window).
SNMP Alarm	EMSKeepAliveAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.45
Alarm Title	EMS Keep Alive Alarm
Alarm Source	Management
Default Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Alarm Text	Management Keep-Alive
Status Changes	-
Additional Info	-
Corrective Action	-

3.19 Pre-provisioning Alarm

Description	This alarm is generated when the operation for pre-provisioning the device upon initial connection to the EMS fails.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.46
AlarmTitle	Pre-Provisioning
AlarmType	operational/Violation
AlarmSource	Management
Probable Cause	The template file could not be applied to the device because there was a mismatch between the template file and the device's existing ini file or there was a mismatch between the device type and the firmware file applied to the device.
Severity	Critical
Additional Info	-

Corrective Action	• When this alarm is raised, you cannot reload configuration or firmware files to the device as it has already been connected to the EMS. Instead download these files to the device using the Software Manager and then use the 'Software Upgrade' action. OR • Remove the device from the EMS and then reconnect it i.e. repeat the pre-provisioning process.
Media Gateways	All gateways managed by EMS.

3.20 Disk Space Alarm

Disk Space Alarm

Description	This alarm is issued in one of the following cases: • The Archive Logs directory capacity has reached {0}%. • The Oracle partition capacity has reached {0}%.
SNMP Alarm	acEMSDiskSpaceAlarmCheck
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.51
AlarmTitle	Disk Space Alarm
AlarmType	Equipment Alarm
AlarmSource	Management
Probable Cause	Storage Capacity Problem
Severity	• 70% < Minor • 80% < Major • 90% < Critical
Additional Info	-
Corrective Action	▪ The Archive Logs directory: Free space in /ACEMS/NBIF/emsBackup/DBEMS/archivelog/ to avoid system failure. ▪ The Oracle partition: Free space using the command rm -f /oracle/DIAG/diag/rdbms/dbems/dbems/trace/*.tr* to avoid system failure.
Media Gateways	-

3.21 Oracle Disk Space Alarm

Oracle Disk Space Alarm

Description	This alarm is issued when the Oracle partition capacity has reached {0}%.
SNMP Alarm	acEMSNotEnoughOracleSpaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.52
AlarmTitle	Oracle Disk Space Alarm
AlarmType	Equipment Alarm
AlarmSource	Management
Probable Cause	Storage Capacity Problem
Severity	• 70% < Minor • 80% < Major • 90% < Critical
Additional Info	-
Corrective Action	Free space using the command rm -f /oracle/DIAG/diag/rdbms/dbems/dbems/trace/*.tr* to avoid system failure.
Media Gateways	-

3.22 License Alarm

License Alarm

Description	This alarm is issued when the EMS License approaches or reaches it's expiration date or the EMS server machine ID is no longer valid.
SNMP Alarm	acLicenseAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.53
AlarmTitle	License Alarm
AlarmType	Other
AlarmSource	Management
Probable Cause	Other
Additional Info	Info1: • Machine ID In The License Is {0} • Expiration Date In The License Is {0}
Corrective Action	Contact your AudioCodes partner ASAP. Note that when notification that this license has expired is received, the server remains connected for a few minutes in order to allow the forwarding traps to northbound destinations.
Media Gateways	-

Alarm Severity	Condition	Alarm Text
Critical	The license expiration date is less than equal to 7 days.	• EMS License is about to expire in {0} days. • EMS License is about to expire in 1 day. • EMS License Will Expire Today
Major	The license expiration date is more than 7 days and less than equal to 30 days.	EMS License is about to expire in {0} days.
Clear	The license expiration date is greater than 30 days.	-

3.23 Synchronizing Alarms

Description	This event is sent out to an SMMP NBI using user defined alarms forwarding rules once the NMS has activated the ReSync Alarms feature.
SNMP OID	ac OCReSyncEvent - 1.3.6.1.4.1.5003.9.20.3.2.0.58
Alarm Title	[Event] Synchronizing Alarms
Alarm Source	Management
Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Additional Info	-
Corrective Action	-
Media Gateways	-

This page is intentionally left blank.

4 Voice Quality Alarms

4.1 Failed Calls Alarm

Failed Calls Alarm

Description	This alarm is raised when the failed calls threshold is crossed and is cleared when the failed calls ratio returns below the threshold value. The description field includes the info: Failed X1% of calls, X2 of X3 calls.
SNMP Alarm	acVoice QualityRuleFailedCallsAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.30
Alarm Title	Voice Quality - Failed Calls Alarm
Alarm Source	Voice Quality/<Device Name> or Voice Quality/<Link Name> (According to provisioned scope)
alarm type	Quality of service alarm.
Probable Cause	The minimum or maximum threshold is crossed.
Severity	According to provisioned thresholds: critical, major or clear
Additional Info	Critical or Major severity threshold is Y%: • Critical Threshold: **5**% of calls (default) • Major Threshold: **3**% of calls (default
Corrective Action	Investigate the source (device or link) of the failed calls.

4.2 Voice Quality Alarm

Voice Quality Alarm

Description	This alarm is raised when the poor quality calls threshold is crossed and is cleared when the poor quality calls ratio returns below the threshold value. The description field includes the info: Poor Quality X1% of calls, X2 of X3 calls.
SNMP Alarm	acVoice QualityRulePoorQualityCallsAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.31
Alarm Title	Voice Quality – Voice Quality Alarm
Alarm Source	Voice Quality/<Device Name> or Voice Quality/<Link Name> (According to provisioned scope)
Alarm Type	Quality of service alarm.
Probable Cause	The minimum or maximum threshold is crossed.
Severity	According to provisioned thresholds: critical, major or clear

Additional Info	Critical or Major severity threshold is Y%: • Critical Threshold: **10**% of calls (default). • Major Threshold: **8**% of calls (default);
Corrective Action	Investigate the source (device or link) of the poor quality calls.

4.3 Average Call Duration Alarm

Average Call Duration Alarm

Description	This alarm is raised when the average call duration time threshold is crossed and is cleared when the average call duration time ratio returns below the threshold value. The description field includes the info: Average Call Duration is X sec.
SNMP Alarm	acVoice QualityRuleAvrgCallDurationAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.32
Alarm Title	Voice Quality – Average Call Duration Alarm
Alarm Source	Voice Quality/<Device Name> or Voice Quality/<Link Name> (According to provisioned scope)
Alarm Type	Quality of service alarm.
Probable Cause	The minimum or maximum threshold is crossed.
Severity	According to provisioned thresholds: critical, major or clear
Additional Info	Critical or Major severity threshold is Y sec.
Corrective Action	Investigate the source (device or link) reporting the excessive average call duration.

4.4 License Key Alarm

License Key Alarm

Description	This alarm is sent in the following circumstances: ▪ When the number of devices connected to the OC approaches or reaches license capacity (shown as 'Devices Number' in the EMS Server Manager License screen). • When the number of sessions running on the OC approaches or reaches license capacity (shown as 'Voice Quality Sessions' in the EMS Server Manager License screen).
SNMP Alarm	acVoice QualityLicenseKeyAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.33
Alarm Title	Voice Quality License key alarm.
Alarm Source	Voice Quality
Alarm Type	Other
Probable Cause	Key Expired
Corrective Action	Contact your AudioCodes representitve to obtain the requiredt license key.

Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	The number of currently running sessions/devices has reached 100% of the Voice Quality servers license capacity.	Current server load reached 100% of VOICE QUALITY License capacity.	-
Major	The number of currently running sessions/devices has reached 80% of Voice Quality servers license capacity.	Current server load reached 80% of Voice Quality License capacity.	-
Clear	The number of currently running sessions/devices has dropped below 80% of Voice Quality servers license capacity.	Clearing currently active device alarm.	-

4.5 System Load Alarm

System Load Alarm

Description	This alarm is sent when the Voice Quality system capacity is high and the system consequently becomes loaded. Three levels are supported: • Minor - > Events are not stored for green calls. Trend Info will not be displayed. • Major -> Events are not stored. Trend Info will not be displayed. • Critical -> Green calls are not stored.
SNMP Alarm	acVoice QualityCallDroppedAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.34
Alarm Title	Voice Quality – System Load Alarm
Alarm Source	Voice Quality
Alarm Type	Quality of service alarm.
Probable Cause	AlarmProbableCauseType.THRESHOLDCROSSED
Severity	MINOR/ MAJOR/ CRITICAL
Additional Info	• Medium load level is reached - {0}%, {1} calls of {2}. / • High load level is reached - {0}%, {1} calls of {2}. / • Approaching maximal system capacity - {0}%, {1} calls of {2}.
Corrective Action	Reduce the system load.

4.5.1 Call Details Storage Level has Changed

Call Details Storage Level has Changed

Description	This alarm is sent when the operator changes the Call Details Storage Level from one level to another.
SNMP Alarm	acVoice QualityClientLoadFlagAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.35
Alarm Title	Voice Quality – Call Details Storage Level has been changed.
Alarm Source	Voice Quality
Alarm Type	Quality of service alarm
Probable Cause	Threshold crossed.
Severity	Indeterminate
Additional Info	-
Corrective Action	-

4.6 Time Synchronization Alarm

Time Synchronization Alarm

Description	This alarm is sent when Device and Server are not synchronized: Server Time: {0}, Device Time: {1}.
SNMP Alarm	acVoice QualityTimeSynchronizationAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.36
Alarm Title	Voice Quality – Time Synchronization Alarm
Alarm Source	Voice Quality/<Device Name> or Voice Quality/<Link Name> (According to provisioned scope)
Alarm Type	Timedomainviolational
Probable Cause	Timing Problem
Severity	Critical
Additional Info	One of the following reasons will appear: • Check your NTP configuration on the device. • NTP servers are not configured on the device. • Ensure that the Voice Quality server and device time is properly synchronized. • Verify that the NTP configuration is correct; verify your network conditions (Firewalls, Ports, etc ..) and make sure that the NTP sync of the Voice Quality server and/or the devices is performed correctly. • Refer to the EMS client / Help menu / EMS Server Configuration frame to verify the network configuration.
Corrective Action	See above.

4.7 MS Lync Connection Lost

Description	This alarm is sent when there is no connectivity with the Lync SQL Server database.
SNMP Alarm	acMSLyncConnectionAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.37
Alarm Title	Voice Quality AD Lync Connection Alarm
Alarm Source	Skype for Business/Lync SQL Server
Alarm Type	Communications alarm
Probable Cause	Communications sub-system failure
Severity	Critical
Additional Info	-
Corrective Action	Check the Lync SQL server for problems.

4.8 Active Directory Server Synchronization Alarm

Description	This alarm is sent when there is no connectivity with the Active Directory LDAP server.
SNMP Alarm	acVoice QualityMSLyncADServerAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.38
Alarm Title	Voice Quality MS Lync AD Server Alarm
Alarm Source	Active Directory LDAP server
Alarm Type	Communications alarm
Probable Cause	Communications sub-system failure
Severity	Critical
Additional Info	Voice Quality - AD Lync connection alarm
Corrective Action	Check the MS Lync AD server for problems.

4.9 Rule Bandwidth Alarm

Description	This alarm is sent when the media bandwidth for the node or link falls below or exceeds the threshold values configured in the Voice Quality Quality Alerts window.
SNMP Alarm	acVoice QualityRuleBandwidthAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.43
Alarm Title	Voice Quality Rule Bandwidth Alarm
Alarm Source	Voice Quality
Alarm Type	Quality of service alarm
Probable Cause	Threshold crossed
Severity	According to provisioned thresholds: critical, major or clear.
Alarm Text	Maximum Bandwidth of X Kb/sec
Status Changes	-
Additional Info	-
Corrective Action	Check the node's or link's maximum bandwidth capacity matches the required capacity.

4.10 Rule Max Concurrent Calls Alarm

Description	This alarm is sent when the maximum concurrent calls for the node or link falls below or exceeds the threshold values configured in Voice Quality Quality Alerts window.
SNMP Alarm	acVoice QualityRuleMaxConcurrentCallsAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.44
Alarm Title	Rule Max Concurrent Calls Alarm
Alarm Source	Voice Quality
Alarm Type	Quality of service alarm
Probable Cause	Threshold crossed.
Severity	According to provisioned thresholds: critical, major or clear
Alarm Text	Max Concurrent Calls of X
Status Changes	-
Additional Info	-
Corrective Action	Check that the node's or link's maximum number of concurrent calls matches the required capacity.

This page is intentionally left blank.

5 Endpoint Alarms

5.1 Registration Failure Alarm

IP Phone Registration Failure Alarm

Description	This alarm is raised when a SIP registration (with a PBX) for the IP Phone fails.
SNMP Alarm	IPPhoneRegisterFailure
OID	1.3.6.1.4.1.5003.9.20.3.2.0.39
Alarm Title	Registration Failure
Alarm Source	IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Corrective Action	The problem is typically not related to the phone, but to the server. The user/phone may not be defined, or may be incorrectly defined, or may previously have been defined but the username (for example) may have been changed, causing the registration to fail. Make sure the username and password credentials are identical in the server and phone, and weren't changed; server-phone credentials must be synchronized. Make sure the server is responsive.

5.2 Lync Survivable Mode Start Alarm

IP Phone Survivable Mode Start Alarm

Description	This alarm is raised when the IP Phone enters Survivable mode state with limited services in the Microsoft Lync environment.
SNMP Alarm	IPPhoneSurvivableModeStart
OID	1.3.6.1.4.1.5003.9.20.3.2.0.40
Alarm Title	Survivable Mode Start
Alarm Source	IP Phone
Alarm Type	Other(0)
Probable Cause	other (0)
Severity	Major
Corrective Action	The problem is typically not related to the phone, but to the server or network. Make sure all servers in the enterprise's network are up. If one is down, limited service will result.

5.3 Lync Login Failure Alarm

IP Phone Lync Login Failure Alarm

Description	This alarm is raised when the IP Phone fails to connect to Microsoft Lync Server during sign in.
SNMP Alarm	IPPhoneLyncLoginFailure
OID	1.3.6.1.4.1.5003.9.20.3.2.0.41
Alarm Title	Lync Login Failure
Alarm Source	IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Additional Info	TlsConnectionFailure NtpServerError
Corrective Action	This alarm may typically occur if the user is not registered - or is registered incorrectly - in the Lync Server. Make sure that username, password and PIN code are correctly configured and valid in the Lync Server. Try resetting them. Try redefining the user.

5.4 Endpoint License Alarm

Endpoint License Alarm

Description	This alarm is issued for the following scenarios: • When the number of endpoints currently running on the Voice Quality server (shown as 'IP Phones Number' under 'Voice Quality' in the EMS Server Manager License screen) approaches or reaches its license capacity. • When the number of endpoints currently running on the EMS server (shown as 'IP Phones Number' under 'EMS for IP Phones' in the EMS Server Manager License screen) approaches or reaches its license capacity.
SNMP Alarm	acEndpointLicenseAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.48
Alarm Title	Endpoint License Alarm
Alarm Source	Voice Quality/Management
Alarm Type	Other
Probable Cause	Key Expired
Additional Info	Endpoint License capacity {0} devices.
Corrective Action	Contact your AudioCodes partner ASAP

Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Currently connected devices are equivelant to 100% of Endpoints License capacity.	Currently running devices reached 100% of Endpoints License capacity.	-
Major	Currently connected devices are equivelant to reached 80% of Endpoints License capacity.	Currently running devices reached 80% of Endpoints License capacity.	-
Clear	Clearing currently active alarm	Clear - Clearing currently active alarm.	-

5.5 Endpoint Server Overloaded Alarm

Endpoint Server Overloaded Alarm

Description	This alarm is issued when the Voice Quality Endpoint server process is overloaded with RFC 6035 Publish messages. This causes new RFC 6035 SIP PUBLISH messages () to be dropped from the queue for this process.
SNMP Alarm	acEndpointServerOverloadAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.49
Alarm Title	Endpoint Server Overloaded Alarm
Alarm Text	Voice Quality Endpoint Server Overloaded! New Publish Messages Dropped
Alarm Source	Voice Quality
Alarm Type	Other
Probable Cause	Queue Size exceeded
Severity	Critical
Additional Info	Maximum Endpoint Server waiting queue size {0}.

Description	This alarm is issued when the Voice Quality Endpoint server process is overloaded with RFC 6035 Publish messages. This causes new RFC 6035 SIP PUBLISH messages () to be dropped from the queue for this process.
SNMP Alarm	acEndpointServerOverloadAlarm
Corrective Action	Reduce the endpoint traffic load on the EMS server.

5.5.1 IP Phone Speaker Firmware Download Failure

IP Phone Speaker Firmware Download Failure

Description	This alarm is raised when the phone fails to download the Jabra speaker firmware from the server (see Alarm Source).
SNMP Alarm	IPPhoneSpeakerFirmDownloadFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.54
Alarm Title	IP Phone Speaker Firmware Download Failure
Alarm Source	The server from which the download was attempted: EMS, WEB, HTTP, FTP
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

5.6 IP Phone Speaker Firmware Upgrade Failure

IP Phone Speaker Firmware Upgrade Failure

Description	This alarm is raised when the phone fails to load the Jabra firmware to the speaker.
SNMP Alarm	IP PhoneSpeakerFirmUpgradeFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.55
Alarm Title	IP Phone Speaker Firmware Upgrade Failure
Alarm Source	The IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

5.7 IP Phone Conference Speaker Connection Failure

IP Phone Conference Speaker Connection Failure

Description	This alarm is raised when there is failure for the USB connection between the phone and the Jabra speaker.
SNMP Alarm	IPPhone Conference Speaker Connection Failure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.56
Alarm Title	IP Phone Conference Speaker Connection Failure
Alarm Source	The IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

5.8 IP Phone General Local Event

IPPhone General Local Event

Description	This alarm provides information about the IP Phones internal operation.
SNMP Alarm	IPPhoneGeneralLocalEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.57
Alarm Title	IP Phone General Local Event
Alarm Source	The IP Phone
Alarm Type	Other(0)
Probable Cause	Other(0)
Severity	Major
Additional Info	4 digit code
Corrective Action	-

5.9 IP Phone Web Successive Login Failure

IP Phone Web Successive Login Failure

Description	This alarm is raised when there are five successive failed login attempts to an IP phone's Web interface.		
SNMP Alarm	IPPhoneWebSuccessiveLoginFailure		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.59		
Alarm Title	IP Phone Web Successive Login Failure		
Alarm Source	The IP Phone		
Alarm Type	SecurityServiceOrMechanismViolation(9)		
Probable Cause	UnauthorizedAccessAttempt(73)		
Additional Info	-		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Issued on the fifth successive failed attempt to log in to the phone's Web interface	-	• After the alarm is cleared, try to login to the Web interface using the correct username and password. • If you forget the login credentials, inform the network administrator.
Clear	There are no additional WEB login failed trials during a specific time period (60 seconds) after sending the alarm.	-	-

This page is intentionally left blank.

6 Device Alarms

6.1 Support Matrix

The table below categorizes all of the device alarms and indicates to which devices they are applicable. For each category, under the adjacent "Supported Device Types" column, all of the common supported alarms for this category are listed. For each individual alarm, under the adjacent "Supported Device Types" column, if all of the common alarms are supported "As above" is noted; however, if only specific devices support this alarm, then these device types are listed.

Alarm Type	Supported Device Types
Common Alarms	All the alarms in Section Common Device Alarms are supported by all AudioCodes devices.
Specific Hardware Alarms	• Mediant 2600 E-SBC • Mediant 4000 SBC • Mediant 1000 • MP-1288
Temperature Alarm	• Mediant 1000 • Mediant 2600 • Mediant 4000
Fan Tray Alarm	• MP-1288 • Mediant 1000 • Mediant 2600 • Mediant 4000
Power Supply Alarm	• MP-1288 • Mediant 1000 • Mediant 2600 • Mediant 4000.
HA System Alarms	▪ Mediant 500 E-SBC ▪ Mediant 800B GW & E-SBC ▪ Mediant 3000/TP-6310 ▪ Mediant 3000/TP-8410 ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC (3 x MPM) ▪ Mediant 9000 SBC ▪ Mediant VE SBC ▪ Mediant SE SBC
HA System Fault Alarm	As above
HA System Configuration Mismatch Alarm	As above

HA System Switch Over Alarm	As above
Hitless Software Upgrade Alarm	▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant SE SBC ▪ Mediant VE SBC
Redundant Board Alarm	As above
HA Network Watchdog Status Alarm	As above
Cluster HA Usage Alarm	As above
License Key Hitless Upgrade Alarm	As above except for Mediant 3000/TP-6310 and Mediant 3000/TP-8410 (these devices are not supported by the OC License Pool Manager)
Media Transcoder Alarms	▪ Mediant 9000 SBC ▪ Mediant VE SBC ▪ Mediant SE SBC
Media Transcoder Network Failure	As above
Media Transcoder Software Upgrade Failure	As above
Media Transcoder High Temperature Failure	As above
Media Transcoder Fan Tray Module Failure	As above
Media Transcoder Power Supply Module Failure	As above
MP-1288 Alarms	▪ MP-1288 (not supported by the OC License Pool Manager)
Module Service Alarm	As above
Module Operation Alarm	As above

Port Service Alarm	As above
MSBR Alarms	Mediant 1000B MSBR, Mediant 800 MSBR Mediant MSBR 500L and Mediant 500 MSBR (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform [1])
WAN Link Alarm	As above
Power Over Ethernet Status [Event]	Mediant 800 MSBR
Wireless Cellular Modem Alarm	▪ Mediant 500 MSBR ▪ Mediant 500L MSBR ▪ Mediant 800 MSBR
Data Interface Status	As above
NQM Connectivity Alarm	Mediant 800 MSBR
NQM RTT Alarm	Mediant 800 MSBR
NQM Jitter Alarm	Mediant 800 MSBR
NQM Packet Loss Alarm	Mediant 800 MSBR
NQM MOS CQ Alarm	Mediant 800 MSBR
NQM MOS LQ Alarm	Mediant 800 MSBR
Mediant 3000 Hardware Alarms	▪ Mediant 3000/TP-6310 ▪ Mediant 3000/TP-8410
PEM Module Alarm	As above
SA Module Missing Alarm	As above
User Input Alarm	As above
TM Inconsistency	As above
TM Reference Status	This alarm applies only to the Mediant 3000 using the BITs Synchronization Timing mode.
TM Reference Change	As above
PSTN Trunk Alarms	• Mediant 500 E-SBC • Mediant 500L E-SBC • Mediant 500 MSBR

[1] Refer to SBC-Gateway-MSBR Series Release Notes for details.

	• Mediant 500L MSBR • Mediant 500L GW & E-SBC • Mediant 800B Gateway & E-SBC • Mediant 800B MSBR • Mediant 850 MSBR • Mediant 1000B MSBR • Mediant 1000B GW & E-SBC • Mediant 3000/TP-6310 • Mediant 3000/TP-8410 (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform[2])
D-Channel Status	As above
SONET Section LOF Alarm	▪ Mediant 3000/TP-6310
SONET Section LOS Alarm	▪ Mediant 3000/TP-6310
SONET Line AIS Alarm	▪ Mediant 3000/TP-6310
SONET Line RDI Alarm	▪ Mediant 3000/TP-6310
SONET/SDN IF Failure Alarm	▪ Mediant 3000/TP-6310
Trunk LOS Alarm	▪ Mediant 500 E-SBC ▪ Mediant 500 MSBR ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800B MSBR ▪ Mediant 850 MSBR ▪ Mediant 1000B MSBR ▪ Mediant 1000B GW & E-SBC ▪ Mediant 3000/TP-8410
Trunk LOF Alarm	▪ Mediant 500 E-SBC ▪ Mediant 500 MSBR ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800B MSBR ▪ Mediant 850 MSBR ▪ Mediant 1000B MSBR ▪ Mediant 1000B GW & E-SBC • Mediant 3000/TP-8410
Trunk AIS Alarm	▪ Mediant 500 E-SBC ▪ Mediant 500 MSBR ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800B MSBR

[2] Refer to SBC-Gateway-MSBR Series Release Notes for details.

	▪ Mediant 850 MSBR ▪ Mediant 1000B MSBR ▪ Mediant 1000B GW & E-SBC • Mediant 3000/TP-8410
Trunk RAI Alarm	▪ Mediant 500 E-SBC ▪ Mediant 500 MSBR ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800B MSBR ▪ Mediant 850 MSBR ▪ Mediant 1000B MSBR ▪ Mediant 1000B GW & E-SBC • Mediant 3000/TP-8410
V5.2 Interface Alarm	▪ Mediant 3000/TP-8410
SONET Path STS LOP Alarm	▪ Mediant 3000/TP-6310
SONET Path STS AIS Alarm	▪ Mediant 3000/TP-6310
SONET Path STS RDI Alarm	▪ Mediant 3000/TP-6310
SONET Path Unequipped Alarm	▪ Mediant 3000/TP-6310
SONET Path Signal Label Alarm	▪ Mediant 3000/TP-6310
DS3 RAI Alarm	▪ Mediant 3000/TP-6310
DS3 AIS Alarm	▪ Mediant 3000/TP-6310
DS3 LOF Alarm	▪ Mediant 3000/TP-6310
DS3 LOS Alarm	▪ Mediant 3000/TP-6310
NFAS Group Alarm	As above
B Channel Alarm	As above
Analog Port Alarms	• Mediant 500 E-SBC • Mediant 500L E-SBC • Mediant 500 MSBR • Mediant 500L MSBR • Mediant 500L GW & E-SBC • Mediant 800B Gateway & E-SBC

	• Mediant 800B MSBR • Mediant 850 MSBR • Mediant 1000B MSBR ▪ Mediant 1000B GW & E-SBC (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform[3])
Analog Port SPI Out of Service	As above
Analog Port High Temperature	As above
Analog Port Ground Fault Out-of-Service Alarm	As above
CloudBond 365	• CloudBond Mediant 800B • CloudBond Mediant Server
Commit License Failed	As above
Component Unreachable	As above
Component Restart	As above
Component Performance Counter General	As above
Component Performance Counter Service	As above
Component Service Status	As above
Component Event Viewer	As above
Component Event Viewer Past Hours	As above
Component Event Viewer Dropped	As above
Admin License Expired	As above
Alarm – Certificate Expired	As above
Alarm –Disk Space	As above

[3] Refer to SBC-Gateway-MSBR Series Release Notes for details.

CCE Appliance Alarms	• CCE Appliance Mediant 800B • CCE Appliance Mediant Server
Component Unreachable	As above
Event – Component Restart	As above
Component Performance Counter General	As above
Component Performance Counter Service	As above
Component Service Status	As above
Alarm – Admin System Cloud Status	As above
Alarm – Certificate Expired	As above
Alarm – CCE Wrong Operating	As above
Alarm – CCE Wrong Settings	As above
Alarm – CCE Disk Space	As above
Alarm – CCE Windows License	As above
SBA Alarms	• Mediant 800B Gateway & E-SBC • Mediant 1000B Gateway & E-SBC
SBA Services Status Alarm	As above
Alarm – CPU Status	As above
Alarm – Memory Status	As above
Alarm – Disk Space	As above
Alarm – Certificate Expired	As above
Alarm – Performance Counter	As above

6.2 Common Device Alarms

6.2.1 Board Fatal Error

Board Fatal Error

Description	Sent whenever a fatal device error occurs.		
SNMP Alarm	acBoardFatalError		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1		
Alarm Title	Board Fatal Error		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	Any fatal error	Board Fatal Error: A run-time specific string describing the fatal error	▪ Capture the alarm information and the Syslog clause, if active. ▪ Contact AudioCodes' Support Center at support@audiocodes.com which will want to collect additional data from the device and perform a reset.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After fatal error	-	

6.2.2 Configuration Error

Configuration Error

Description	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.		
SNMP Alarm	acBoardConfigurationError		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Alarm Title	[Event] Configuration Error		
AlarmType	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical(default)	A configuration error was detected	Board Config Error: A run-time specific string describing the configuration error	▪ Check the run-time specific string to determine the nature of the configuration error. ▪ Fix the configuration error using the appropriate tool: Web interface, EMS, or *ini* file. ▪ Save the configuration and if necessary reset the device.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After configuration error	-	

6.2.3 Initialization Ended

Initialization Ended

Description	This alarm is sent when the device is initialized and ready to run.
SNMP Alarm	acBoardEvBoardStarted
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Alarm Title	[Event] Initialization Ended
Alarm Type	Equipment Alarm
Alarm Source	-
Probable Cause	Other
Severity	Major
Additional Info1,2,3	NULL

6.2.4 Board Resetting Following Software Reset

Board Resetting Following Software Reset

Description	This alarm indicates that the device has started the reset process - following a software reset.
SNMP Alarm	acBoardEvResettingBoard
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5
Alarm Title	Board Resetting Following Software Reset
Alarm Type	Other
Alarm Source	-
Probable Cause	Other
Severity	Critical
Additional Info1,2,3	'AdditionalInfo1', 'AdditionalInfo2', 'AdditionalInfo3',
Corrective Action	A network administrator has taken action to reset the device. No corrective action is needed.

6.2.5 Feature Key Related Error

Feature Key Related Error

Description	Sent to relay Feature Key errors etc.
SNMP Alarm	acFeatureKeyError
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Alarm Title	Feature Key Related Error
Severity	Critical
Alarm Type	processingErrorAlarm
Probable Cause	configurationOrCustomizationError (7)
Alarm Text	Feature key error
Note	Support for this alarm is pending.

6.2.6 Gateway Administrative State Changed

Gateway Administrative State Changed

Description	This alarm indicates that the administrative state of the gateway has been changed to a new state. Note that all state changes are instigated by the parameter acgwAdminState. ▪ Time limit set in the parameter acgwAdminStateLockControl - 'GateWay shutting down. Max time to LOCK %d sec' ▪ No time limit in the parameter acgwAdminStateLockControl - 'GateWay is shutting down. No time limit.' ▪ When reaching lock state - 'GateWay is locked' • When the gateway is SET to unlocked - 'GateWay is unlocked (fully active again)'
SNMP Alarm	acgwAdminStateChange
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7
Alarm Title	Administrative State Change
Alarm Type	processingErrorAlarm
Probable Cause	outOfService (71)

Alarm Severity	Condition	<text>	Corrective Action
Major (default)	Admin state changed to shutting down	Network element admin state change alarm: Gateway is shutting down. No time limit.	No corrective action is required. A network administrator took an action to gracefully lock the device.
Major	Admin state changed to locked	Locked	No corrective action is required. A network administrator took an action to lock the device, or a graceful lock timeout occured.
Cleared	Admin state changed to unlocked	-	No corrective action is required. A network administrator has taken an action to unlock the device.

6.2.7 No Free Channels Available

No Free Channels Available

Description	This alarm indicates that almost no free resources for the call are available. Activated only if the parameter EnableRai is set. The threshold is determined according to parameters RAIHIGHTHRESHOLD and RAILOWTHRESHOLD.		
SNMP Alarm	acBoardCallResourcesAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8		
Alarm Title	No Free Channels Available		
AlarmType	processingErrorAlarm		
Alarm Source	'GWAPP'		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major(default)	Percentage of busy channels exceeds the predefined RAI high threshold	Call resources alarm	Expand system capacity by adding more channels (trunks) -OR- Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	Note that to enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated (EnableRAI = **1**).

6.2.8 Gatekeeper/Proxy not Found or Registration Failed

Proxy not Found or Registration Failed

Description	The alarm is sent in the following scenarios: ▪ Physical FXO port is up or down (Out-of-Service or OOS). The FXO line can be down due to, for example, port disconnected or insufficient current and voltage. (Syslog message event is ANALOG_IF_LINE_DISCONNECTED.) ▪ Physical BRI or PRI (E1/T1) port is up or down (OOS). ▪ Proxy is not found or registration fails. In such a case, the device's routing table may be used for routing instead of the Proxy. ▪ Connection to the Proxy is up or down. ▪ Failure in TDM-over-IP call - transparent E1/T1 without signalling. ▪ Connection to the Proxy Set associated with the trunk/line is up/down. ▪ Failure in server registration for the trunk/line. ▪ Failure in a Serving IP Group for the trunk. ▪ Failure in a Proxy Set.		
SNMP Alarm	acBoardControllerFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.9		
Alarm Source	'GWAPP'		
Alarm Title	Proxy not Found or Registration Failed		
Alarm Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Additional Information**
Major(default)	FXO physical port is down	"BusyOut Line *n* Link failure" Where *n* represents the FXO port number (0 for the first port).	▪ Verify that the FXO line is securely cabled to the device's FXO port.
	BRI or PRI physical port is down	"BusyOut Trunk *n* Link failure" Where *n* represents the BRI or PRI port number (0 for the first port).	Verify that the digital trunk is securely cabled to the device's digital port.
	Proxy has not been found or registration failure	"Proxy not found. Use internal routing" -OR- "Proxy lost. Looking for another Proxy"	▪ Check the network layer ▪ Make sure that the proxy IP and port are configured correctly.

	Connection to Proxy is down	"BusyOut Trunk/Line *n* Connectivity Proxy failure"	-
	Connection to the Proxy Set associated with the trunk or line is down	"BusyOut Trunk/Line *n* Proxy Set Failure" Where *n* represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Proxy Set	"Proxy Set ID *n*" Where *n* represents the Proxy Set ID.	-
	Failure in TDM-over-IP call	"BusyOut Trunk *n* TDM over IP failure (Active calls x Min y)" Where *n* represents the BRI/ PRI trunk.	-
	Failure in server registration for the trunk/line	"BusyOut Trunk/Line *n* Registration Failure" Where *n* represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Serving IP Group for the trunk	"BusyOut Trunk *n* Serving IP Group Failure" Where *n* represents the BRI or PRI trunk ID.	-
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	-

6.2.9 Ethernet Link Down Alarm

Ethernet Link Down Alarm

Description	This alarm indicates that the Ethernet link is down or remote Ethernet link is down and the board has no communication to any other host. • No link at all. • Link is up again. • Primary link is down only - 'Primary Link is lost. Switching to Secondary Link'		
SNMP Alarm	acBoardEthernetLinkAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10		
Alarm Title	Ethernet Link Down Alarm		
Alarm Source	All except Mediant 3000: Board#<n>/EthernetLink#0 (where n is the slot number) Mediant 3000: Chassis#0/Module#<n>/EthernetLink#0 (where n is the blade's slot number) This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Fault on single interface	Ethernet link alarm: Redundant link is down	▪ Ensure that both Ethernet cables are plugged into the back of the system. ▪ Observe the system's Ethernet link lights to determine which interface is failing. ▪ Reconnect the cable or fix the network problem
Critical(default)	Fault on both interfaces	No Ethernet link	
Cleared	Both interfaces are operational	-	Note that the alarm behaves differently when coming from the redundant or the active modules of a High Availability (HA) system. The alarm from the redundant is raised when there is an operational HA configuration in the system. There is no critical severity for the redundant module losing both its Ethernet links as that is conveyed in the no HA alarm that follows such a case.

6.2.10 System Component Overloaded

System Component Overloaded

Description	This alarm is raised when there is an overload in one or more of the system's components.		
SNMP Alarm	acBoardOverloadAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Severity	Major		
Alarm Type	processingErrorAlarm		
Alarm Source	'GWAPP'		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major(default)	An overload condition exists in one or more of the system components	"System CPU overload condition - IdleUtilization percentage=%d" Where *%d* is the percentage of available CPU resources remaining	▪ Make sure that the syslog level is 0 (or not high). ▪ Make sure that DebugRecording is not running. ▪ If the system is configured correctly, reduce traffic.
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	-

6.2.11 Active Alarms Table Overflow

Active Alarms Table Overflow

Description	This alarm is raised when there are too many alarms to fit into the active alarm table. The status stays major until reboot as it denotes a possible loss of information until the next reboot. If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.
SNMP Alarm	acActiveAlarmTableOverflow
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.12
Alarm Title	[Event] Active Alarm Table Overflow
Alarm Type	Processing Error Alarm
Alarm Source	MG
Probable Cause	resourceAtOrNearingCapacity (43)
Severity	Major
Additional Info1,2,3	-
Corrective Action	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

6.2.12 Operational State Change

Operational State Change

Description	This alarm is raised if the operational state of the node is disabled. The alarm is cleared when the operational state of the node is enabled.		
SNMP Alarm	acOperationalStateChange		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15		
Alarm Title	Operational State Change		
Alarm Source	-		
Alarm Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major(default)	Operational state changed to disabled	Network element operational state change alarm. Operational state is disabled.	▪ The alarm is cleared when the operational state of the node goes to enabled. ▪ In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the device fails to properly initialize. ▪ Look for other alarms and Syslogs that might provide additional information about the error.
Cleared	Operational state changed to enabled	-	-

6.2.13 Keep Alive Trap

Keep Alive Trap

Description	Part of the NAT traversal mechanism. If the STUN application in the device detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the device.
SNMP Alarm	acKeepAlive
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Alarm Title	[Event] Keep Alive Trap
Alarm Source	-
Alarm Type	other (0)
Probable Cause	other (0)
Default Severity	Indeterminate
Event Text	Keep alive trap
Status Changes	-
Condition	The STUN client is enabled and identified as a NAT device or doesn't locate the STUN server. The *ini* file contains the following line 'SendKeepAliveTrap=1'
Trap Status	Trap is sent
Note	Keep-alive is sent every 9/10 of the time defined in the parameter NatBindingDefaultTimeout.

6.2.14 NAT Traversal Alarm

NAT Traversal Alarm

Description	This alarm is sent when the NAT is placed in front of a device and is identified as a symmetric NAT. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.
SNMP Alarm	acNATTraversalAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.17
Alarm Title	NAT Traversal Alarm
Alarm Type	other (0)
Alarm Source	MG
Probable Cause	other (0)
Severity	Indeterminate
Additional Info1,2,3	-
Status Changes	The STUN client in the device is enabled and has either identified a NAT or is not finding the STUN server. Keep-alive is sent out every 9/10 of the time defined in the 'NatBindingDefaultTimeout' parameter.
Corrective Action	See http://tools.ietf.org/html/rfc5389

6.2.15 Enhanced BIT Status Trap

Enhanced BIT Status

Description	Sent for the status of the BIT (Built In Test). The information in the trap contains blade hardware elements being tested and their status. The information is presented in the Additional Info fields.
SNMP Alarm	acEnhancedBITStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Alarm Title	Enhanced BIT Status
Severity	Indeterminate
Alarm Source	BIT
Alarm Type	Other
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their status.
Status Changes	-
Additional Info-1	BIT Type: Offline, startup, periodic
Additional Info-2	BIT Results: BIT_RESULT_PASSED BIT_RESULT_FAILED
Additional Info-3	Buffer: Number of bit elements reports
Corrective Action	Not relevant

6.2.16 Threshold of Performance Monitored Object Exceeded

Threshold of Performance Monitored Object Exceeded

Description	Sent every time the threshold of a Performance Monitored object (counter or gauge) ('Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') is crossed. The severity field is 'Indeterminate' when the crossing is above the threshold and 'Cleared' when it goes back under the threshold. The 'Source' varbind in the trap indicates the object for which the threshold is being crossed.
SNMP Alarm	acPerformanceMonitoringThresholdCrossing
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Alarm Title	Threshold of Performance Monitored Object Exceeded
Alarm Type	Other
Alarm Source	MO Path
Probable Cause	Other
Severity	Indeterminate (this is a notification; it's not automatically cleared)
Additional Info1,2,3	-
Corrective Action	-

6.2.17 HTTP Download Result

HTTP Download Result

Description	This is a log message (not alarm) indicating both sucessful and failed HTTP Download result.
SNMP Alarm	acHTTPDownloadResult
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Alarm Title	[Event] HTTP Download Result
Alarm Source	-
Alarm Type	processingErrorAlarm (3) for failures and other (0) for success
Probable Cause	Other
Severity	Indeterminate
Additional Info	There are other possible textual messages describing NFS failures or success, FTP failure or success.
Corrective Action	-

6.2.18 IPv6

Description	This alarm indicates when an IPv6 address already exists or an IPv6 configuration failure has occurred. The description generated is "IP interface alarm. IPv6 Configuration failed, IPv6 will be disabled".		
SNMP Alarm	acIPv6ErrorAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.53		
Alarm Title	IPv6		
Default Severity	Critical		
Alarm Source	System#0/Interfaces#<n>.		
Alarm Type	operationalViolation		
Probable Cause	communicationsProtocolError		
Additional Info	Status stays critical until reboot. A clear trap is not sent.		
Corrective Action	▪ Find a new IPV6 address and reboot.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	Bad IPv6 address (already exists)	IP interface alarm: IPv6 configuration failed, IPv6 will be disabled.	▪ Find a new IPV6 address. ▪ Reboot the device.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After the alarm is raised.	-	-

6.2.19 SAS Emergency Mode Alarm

GW SAS Emergency Mode Alarm

Description	This alarm is sent by the Stand-Alone Survivability (SAS) application when switching from “Normal" mode to “Emergency" mode. This alarm is cleared once the SAS returns to “Normal" mode.
SNMP Alarm	acGWSASEmergencyModeAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.59
Alarm Title	GW SAS Emergency Mode Alarm
Alarm Source	-
Alarm Type	Other
Probable Cause	Other
Severity	-

Additional Info	-
Corrective Action	Check network communication with the Proxy

6.2.20 Software Upgrade Alarm

Software Upgrade Alarm

Description	This alarm is generated when the Software upgrade failure occurs.		
SNMP Alarm	acSWUpgradeAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70		
Alarm Title	Software Upgrade alarm		
Alarms Source	System#0		
Alarm Type	processingErrorAlarm		
Probable Cause	softwareProgramError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major (default)	Raised upon software upgrade errors	SW upgrade error: Firmware burning failed. Startup system from Bootp/tftp.	Start up the system from BootP/TFTP.

6.2.21 NTP server Status Alarm

NTP server Status Alarm

Description	This alarm is raised when the connection to the NTP server is lost. It is cleared when the connection is reestablished. Unset time (as a result of no connection to NTP server) may result in functionality degradation and failure in device.
SNMP Alarm	acNTPserverStatusAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71
Alarm Title	NTP server Status Alarm
Alarm Source	-
Alarm Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure

Alarm Severity	Condition	<text>	Corrective Action
Major(default)	No initial communication to Network Time Protocol (NTP) server.	NTP server alarm. No connection to NTP server.	Repair NTP communication (the NTP server is down or its IP address is configured incorrectly in the device).
Minor	No communication to NTP server after the time was already set once.	-	-

6.2.22 LDAP Lost Connection

LDAP Lost Connection

Description	This alarm is raised when there is no connection to the LDAP server.
SNMP Alarm	acLDAPLostConnection
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.75
Alarm Title	LDAP Lost Connection
Alarm Source	-
Alarm Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure If a connection is idle for more than the maximum configured time in seconds that the client can be idle before the LDAP server closes the connection, the LDAP server returns an LDAP disconnect notification and this alarm is raised.
Severity	Minor / Clear
Additional Info	-
Corrective Action	-

6.2.23 SSH Connection Status [Event]

[Event] SSH Connection Status

Description	This trap indicates the result of a recent SSH connection attempt.
SNMP Alarm	acSSHConnectionStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Alarm Title	[Event] SSH Connection Status
Alarm Source	-
Alarm Type	environmentalAlarm

Probable Cause	unauthorizedAccessAttempt/other
Severity	indeterminate
Additional Info	-
Corrective Action	-

6.2.24 OCSP Server Status Alarm

OCSP Server Status Alarm

Description	This alarm is raised when the OCSP connection is not available.
SNMP Alarm	acOCSPServerStatusAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.78
Alarm Title	OCSP server alarm.
Alarm Source	-
Alarm Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Severity	Major / Clear
Additional Information	-
Corrective Action	• Repair the Online Certificate Status Protocol (OCSP) server -OR- • Correct the network configuration

6.2.25 Media Process Overload Alarm

Media Process Overload Alarm

Description	This alarm is raised when the media process overloads and is cleared when the load returns to normal.
SNMP Alarm	acMediaProcessOverloadAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.81
Alarm Title	Media Process Overload Alarm
Alarm Source	Board#x or System#x
Alarm Type	processingErrorAlarm
Probable Cause	resourceAtOrNearingCapacity
Severity	Major / Clear
Additional Info	-
Corrective Action	-

6.2.26 Ethernet Group Alarm

Ethernet Group Alarm

Description	This alarm is raised when the in an Ethernet port-pair group (1+1) has no Ethernet port with its link up and is cleared when at least one port has established a link.
SNMP Alarm	acEthernetGroupAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86
Alarm Title	Ethernet Group alarm.
Alarm Source	Board#%d/EthernetGroup#%d
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	major
Additional Info	-
Corrective Action	-

6.2.27 Media Realm BW Threshold Alarm

Media Realm BW Threshold Alarm

Description	This alarm is raised when a BW threshold is crossed and is cleared when the BW threshold returns to normal range.
SNMP Alarm	acMediaRealmBWThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.87
Alarm Title	Media Realm BW Threshold Alarm.
Alarm Source	Board#%d/MediaRealm#%d
Alarm Type	processingErrorAlarm
Probable Cause	resourceAtOrNearingCapacity
Severity	major
Additional Info	-
Corrective Action	-

6.2.28 Certificate Expiry Notification

Certificate Expiry Notification

Description		This alarm is sent before the expiration of the installed credentials, which cannot be renewed automatically (the credentials should be updated manually).	
SNMP Alarm		acCertificateExpiryNotification	
SNMP OID		1.3.6.1.4.1.5003.9.10.1.21.2.0.92	
Alarm Title		Certificate Expiry Notification	
Alarm Source		tls#<num>	
Alarm Text		Device's TLS certificate of security context #%d will expire in %d days	
Alarm Type		environmentalAlarm	
Probable Cause		The certificate key expired (keyExpired)	
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Intermediate	The certificate key is about to expire.	Either: ▪ The device certificate has expired %d days ago ▪ The device certificate will expire in %d days ▪ The device certificate will expire in less than 1 day %d – number of days %d – TLS Context to which certificate belongs	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically). To replace certificates, refer to the device's *User's Manual*.

6.2.29 Web User Access Disabled

WEB User Access Disabled

Description	This alarm is sent when the Web user has been disabled due to inactivity.
SNMP Alarm	acWEBUserAccessDisabled
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Alarm Title	-
Alarm Source	-
Alarm Type	other
Probable Cause	The Web user was disabled due to inactivity (denialOfService).
Severity	indeterminate
Additional Info	-
Corrective Action	Contact your Web security administrator. Only the Web security administrator can unblock a user whose access to the Web interface was denied (for example, because the user made 3 unsuccessful attempts at access). The Web security administrator must: ▪ In the Web interface, access the Accounts page (**Configuration** > **System** > **Management** > **Web User Accounts**). ▪ Identify in the list of users table that user whose access has been denied. Change the status of that user from **Blocked** to **Valid** or **New**.

6.2.30 Proxy Connection Lost

Proxy Connection Lost

Description	This alarm is sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.
SNMP Alarm	acProxyConnectionLost
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94
Alarm Title	Proxy Connection Lost
Alarm Source	System#0
Alarm Text	Proxy Set Alarm <text>
Alarm Type	communicationsAlarm
Probable Cause	• Network issue (connection fail due to network/routing failure). • Proxy issue (proxy is down). • AudioCodes device issue.

Alarm Severity	Condition	<text>	Corrective Action
Major	When connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table.	Proxy Set %d: Proxy not found. Use internal routing	• Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. • Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. • If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. • Check that routing using the device's (internal) routing table is functioning correctly. • Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.

Major	When Proxy Set includes more than one proxy IP with redundancy and connection to one of them is lost.	Proxy Set %d: Proxy lost. looking for another proxy	• Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. • Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. • If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. • Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue. • Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to proxy is available again	Proxy found. ip:<IP address>:<port #> Proxy Set ID %d	-

6.2.31 IDS Policy Alarm

IDS Policy Alarm

Description	The alarm is raised whenever a threshold is crossed in the IDS system. The alarm is associated with the MO pair IDSMatch & IDSRule.
SNMP Alarm	acIDSPolicyAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Alarm Title	IDS Policy Alarm
Default Severity	-
Alarm Type	Other
Probable Cause	-
Alarm Text	Policy NUM (NAME) minor/major/critical threshold (NUM) of REASON cross in global/ip/ip+port scope (triggered by IP)
Status Changes	-
Corrective Action	• Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm. • Locate the remote hosts (IP addresses) that are specified in the traps. • Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation. • If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table.

6.2.32 IDS Threshold Cross Notification

IDS Threshold Cross Notification

Description	This notiofication is sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
SNMP Alarm	acIDSThresholdCrossNotification
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Default Severity	-
AlarmType	Other
Probable Cause	-
Alarm Text	Threshold cross for scope value IP. Severity=minor/major/critical. Current value=NUM
Status Changes	-
Corrective Action	• Identify the remote host (IP address / port) on the network which the Intrusion Detection System (IDS) has indicated is malicious. Note that the IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). • Block the malicious activity.

6.2.33 IDS Blacklist Notification

IDS Blacklist Notification

Description	This alarm notifies when an IP address has been added or removed from a blacklist.
SNMP Alarm	acIDSBlacklistNotification
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Default Severity	-
Alarm Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	Added IP * to blacklist Removed IP * from blacklist
Status Changes	-
Corrective Action	Identify the malicious remote host (IP address / port) that the Intrusion Detection System (IDS) has automatically blacklisted or removed from the blacklist. Note that a host is determined to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). The malicious source is automatically blacklisted for a user-defined period, after which it is removed from the blacklist.

6.2.34 Proxy Connectivity

Proxy Connectivity

Description	Sent when a connection to a specific proxy in a specific Proxy Set is down. The trap is cleared when the proxy connections is up.
SNMP Alarm	acProxyConnectivity
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.102
Alarm Source	System#0
Alarm Text	Proxy Set Alarm <text>
Alarm Type	communicationsAlarm
Probable Cause	▪ Network issue (connection fail due to network/routing failure). ▪ Proxy issue (proxy is down). ▪ AudioCodes device issue.

Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	When connection to the proxy server is lost.	Proxy server <IP address>:<port> is now OUT OF SERVICE	• Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. • Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. • If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same trap event. If this is the case, this could confirm that this is not AudioCodes device issue. • Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to the proxy is available again	Proxy server <IP address>:<port> is now IN SERVICE	-

6.2.35 Web User Activity Log Trap

acActivityLog

Description	Sent upon log (Syslog) generated by device indicating a Web user action (configured by ActivityListToLog). The SNMP trap notification functionality is enabled by the EnableActivityTrap parameter (refer to the *User's Manual*).
SNMP Alarm	acActivityLog
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.105
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	[description of activity].User:<username>. Session: <session type>[IP address of client (user)]. For example: “Auxiliary file loading was changed from ‘0’ to ‘1’, User:Admin. Session: WEB [172.17.125.12]
Note	Activity log event is applicable to the following OAMP interfaces: SNMP, Web, CLI and REST. For SNMP activity, the username refers to the SNMP community string.

6.2.36 License Pool Infra Alarm

acLicensePoolInfraAlarm

Description	This alarm is raised under the following circumstances: • The device was unable to access the SBC License Pool Manager. • The device license has expired. • The device is no longer managed by the SBC License Pool Manager.		
SNMP Alarm	acLicensePoolInfraAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.106		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired, fail to connect to license pool server.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	The last attempt to establish an HTTPS REST connection with the EMS SBC License Pool Manager server was not successful.	Device was unable to access the License Server.	• Wait for the next connection attempt. • In the SBC License Pool Manager, perform the 'MG Update' action to reestablish REST connection with device and send the current license.
	The device has been configured as Non-Managed in the SBC License Pool Manager. If there are active licensed sessions for this device, the device automatically performs a reset or hitless upgrade.	Device is no longer managed by the SBC License Pool.	If you wish, reconfigure the device as managed by the SBC License Pool Manager.

Critical	Device unable to establish an HTTPS REST connection with the EMS SBC License Pool Manager server after successive attempts.	License-pool is about to expire.	In the SBC License Pool Manager, perform the 'MG Update' action to reestablish REST connection with device and send the latest license.
	The device license has expired.	The device license has expired! Use of this device is strictly prohibited.	
Clear	This alarm is cleared when: • Connection has been restablished with the SBC License Pool Manager, an updated license has been loaded to device and apply/reset has been performed. • The device has been reconfigured as managed by the SBC License Pool Manager, a new license has been loaded to the device, and and apply/reset has been performed.	-	

6.2.37 License Pool Application Alarm

Table 6-1: acLicensePoolApplicationAlarm

Description	This alarm is raised when the device requires a reset or apply hitless upgrade after receiving a new license.		
SNMP Alarm	acLicensePoolApplicationAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.107		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	New license pool		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	SBC License key has been received from SBC License Pool Manager Server.	New license pool allocations received	Perform one of the following actions in the SBC License Pool Manager to apply the new license: • For stand-alone devices, reset the device. • For HA devices, apply a hitless upgrade or reset the device.

6.2.38 Answer-Seizure Ratio Threshold Alarm

ASR Threshold Crossed

Description	The Answer-Seizure Ratio (ASR) measures the percentage of answered calls relative to the total number of attempted calls (seizures). The alarm is raised when the configured ASR minor and major thresholds are crossed (configured in the *Performance Profile* table).
SNMP Alarm	acASRThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.111
Alarm Title	ASR Threshold Crossed
Alarm Source	The object for which the threshold is crossed can be any of the following: ▪ PM_gwSBCASR ▪ PM_gwSBCIPGroupASR ▪ PM_gwSBCSRDASR
Alarm Text	-
Alarm Type	QualityOfServiceAlarm
Probable Cause	ThresholdCrossed

Severity	Condition	<text>	Corrective Action
Major	ASR is equal or less than the configured Major threshold.	"ASR threshold crossed."	
Minor	ASR is equal or less than the configured Minor threshold (but greater than the Major threshold).	"ASR threshold crossed."	
Cleared	ASR is above the configured Minor threshold plus the hysteresis.	-	

6.2.39 Average Call Duration Threshold Alarm

ACD Threshold Crossed

Description	The Average Call Duration (ACD) plus the SDD (Session Disconnect time) measures the average call duration from the time from when the sip Bye is sent to the time when the 200 OK is received. The alarm is raised when the configured ACD minor and major thresholds are crossed (configured in the Performance Profile table).		
SNMP Alarm	acACDThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.112		
Alarm Title	ACD Threshold Crossed		
Alarm Source	The object for which the threshold is crossed can be any one of the following: ▪ PM_gwSBCACD ▪ PM_gwSBCIPGroupACD ▪ PM_gwSBCSRDACD		
Alarm Text	-		
AlarmType	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	ACD is equal or less than the configured Major threshold.	"ACD threshold crossed."	-

Minor	ACD is equal or less than the configured Minor threshold (but greater than the Major threshold).	-	-
Cleared	ACD is above the configured Minor threshold plus the hysteresis.	-	-

6.2.40 Network Effectiveness Ratio Threshold Alarm

NER Threshold Crossed

Description	The NER (Network Effectiveness Ratio) measures the percentage of successfully connected calls relative to the total number of seizures. The alarm is raised when the configured NER minor and major thresholds are crossed (configured in the Performance Profile table).		
SNMP Alarm	acNERThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.113		
Alarm Title	NER Threshold Crossed		
Alarm Source	The object for which the threshold is crossed, which can be one of the following: ▪ PM_gwSBCNER ▪ PM_gwSBCIPGroupNER ▪ PM_gwSBCSRDNER		
Alarm Text	-		
Alarm Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Severity	**Condition**	**<text>**	**Corrective Action**
Major	NER is equal or less than the configured Major threshold.	"NER threshold crossed."	-
Minor	NER is equal or less than the configured Minor threshold (but greater than the Major threshold).	-	-

Cleared	NER is above the configured Minor threshold plus the hysteresis.	-	-

6.2.41 No Route to IP Group Alarm

IP Group Blocked

Description	The alarm is raised when the device rejects calls to an IP Group due to the following reasons: ▪ IP Group keep-alive failure (Gateway and SBC) ▪ Poor Voice Quality - MOS (SBC only) ▪ Bandwidth threshold has been crossed (SBC only) ▪ ASR threshold has been crossed (SBC only) ▪ ACD threshold has been crossed (SBC only) ▪ NER threshold has been crossed (SBC only)		
SNMP Alarm	acIpGroupNoRouteAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.114		
Alarm Title	IP Group Blocked		
Alarm Source	The object for which the threshold is crossed according to one of the above mentioned reasons: ▪ IP Group keep alive failure (acProxyConnectivity trap is raised) ▪ Poor Quality of Experience ▪ Bandwidth ▪ ASR (see acASRThresholdAlarm) ▪ ACD (see acACDThresholdAlarm) ▪ NER (see acNERThresholdAlarm)		
Alarm Text	<Alarm Description Reason> as described above.		
Alarm Type	Quality Of Service Alarm		
Probable Cause	One of the reasons described above.		
Severity	**Condition**	**<text>**	**Corrective Action**
Major	When calls rejected to IP Group due to any of the above-mentioned reasons.	"IP Group is temporarily blocked."	-

Cleared	When calls are no longer rejected due to the above mentioned reasons (i.e. when none of the above reasons prevent a route to the IP Group from being established).	-	-

6.2.42 License Pool Over Allocation Alarm

License Pool Over Allocation Alarm

Description	This alarm is raised when the SBC license received from the SBC License Pool Manager has exceeded the maximum capacity supported by the device.		
SNMP Alarm	acLicensePoolOverAllocationAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.125		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	Overallocation		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Warning (displayed after the configuration has been applied in the SBC License Pool Manager; however, prior to device reset or hitless upgrade).	The SBC license received from the License Pool Manager has exceeded the maximum capacity supported by the device.	"Some of the license pool allocations exceed maximum capability and will not be applied"	In the SBC License Pool Manager, do one of the following: • Apply the new license (reset device or apply hitless upgrade); the device sets its SBC capacity to maximum and disregards the excess configured sessions. • Reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).

Warning (displayed after device restart).	The SBC license received from the License Pool Manager Server has exceeded the maximum capacity supported by the device	“Some of the license pool allocations will not be used because of over-allocation”	In the SBC License Pool Manager, reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).

6.3 Specific Hardware Alarms

6.3.1 Temperature Alarm

Temperature Alarm

Description	Sent when the device exceeds its temperature limits.		
SNMP Alarm	acBoardTemperatureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3		
Alarm Title	Temperature Alarm		
Alarm Type	equipmentAlarm		
Alarm Source	System#0		
Probable Cause	The air filter is saturated. One of the fans work slower than expected. temperatureUnacceptable (50)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Internal temperature is too high for normal operation	Board temperature too high	Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels. Check the chassis ventilation outlet and make sure that they are not obstructed for air flow. Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Temperature returns to normal operating values	-	-

6.3.2 Fan Tray Alarm

Fan Tray Alarm

Description	This alarm is activated in one of the following cases: ▪ Fan-Tray is missing ▪ One or more fans in the fan-tray is faulty. ▪ Fan tray is in place and fans are functioning.		
SNMP Alarm	acFanTrayAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29		
Alarm Title	Fan Tray Alarm		
Alarm Source	Chassis#0/FanTray#0		
Alarm Text	Fan-Tray Alarm <text>		
Alarm Type	equipmentAlarm		
Probable Cause	▪ One or more fans on the Fan Tray module stopped working. ▪ One or more fans on the Fan Tray module works slower than expected (heatingVentCoolingSystemProblem)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Fan-Tray is missing.	Fan-Tray is missing	1. Check if the Fan Tray module is inserted in the chassis. 2. If the Fan Tray module was removed from the chassis, re-insert it. 3. If the Fan Tray module has already been inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes. **Warning:** When removing the Fan Tray module while the power is on (or after it has recently been switched off), the blades may still be rotating at high speeds. Therefore, to avoid bodily harm, make sure that you don't touch the fan blades.
Major	When one or more fans in the Fan Tray are faulty.	Fan-Tray is faulty	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module is in place and fans are working.	-	-

6.3.3 Power Supply Alarm

Power Supply Alarm

Description	This alarm is activated in one of the following cases: ▪ The HA (High Availability) feature is active and one of the power supply units is faulty or missing. ▪ PS unit is inserted in its location and functioning.		
SNMP Alarm	acPowerSupplyAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30		
Alarm Title	Power Supply Alarm		
Alarm Source	Chassis#0/PowerSupply#<m>, where *m* is the power supply's slot number		
Alarm Type	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major (default)	The HA (High Availability) feature is active (applicable only to Mediant 3000) and one of the power supply units is faulty or missing.	Power-Supply Alarm. Power-Supply is missing.	1. Check if the unit is inserted in the chassis. 2. If it was removed from the chassis, re-insert it. 3. If it's inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	PS unit is placed and working.	-	-

6.4 HA System Alarms

6.4.1 HA System Fault Alarm

HA System Fault Alarm

Description	This alarm originates when: ▪ HA feature is active but the system is NOT working in HA mode. Reason is specified (for example: SW WD exception error, HW WD exception error, SAT device is missing, SAT device error, DSP error, BIT tests error, etc). ▪ HA feature is active and the redundant module is in start up mode but hasn't connected yet ▪ HA system is active		
SNMP Alarm	acHASystemFaultAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33		
Alarm Title	HA System Fault Alarm		
Alarm Source	System#0/Module#<m>, where *m* is the blade module's slot number		
AlarmType	qualityOfServiceAlarm		
Probable Cause	outOfService		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	HA feature is active but the system is not working in HA mode	Fatal exception error	High Availability (HA) was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		TCPIP exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Network processor exception error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		HW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.

		SAT device is missing (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SAT device error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		DSP error (applicable only to Mediant 3000 and Mediant 4000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		BIT tests error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		PSTN stack error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Keep Alive error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Software upgrade	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Manual switch over	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Manual reset	HA was lost due to a *system reset* and should return automatically after few minutes. Corrective action is not required.
		Board removal (applicable only to Mediant 3000)	Return the removed board to the system.
		TER misplaced (applicable only to Mediant 3000)	Place the TER card according to the *User's Manual*
		HW fault. TER in slot 2 or 3 is missing (applicable only to Mediant 3000)	Place the TER card according to the *User's Manual*

		HW fault. TER has old version or is not functional (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. invalid TER Type (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. invalid TER active/redundant state (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. Error reading GbE state (applicable only to Mediant 3000)	Replace the TER card.
		Redundant module is missing (applicable only to Mediant 3000)	• Insert the redundant module into the system. • If the error continues, reset / replace the module.
		Redundant is not connecting (applicable only to Mediant 3000)	Reset / replace the redundant module.
		Redundant is not reconnecting after deliberate restart	Reset / replace the redundant module.
		No Ethernet Link in redundant module	Connect Ethernet links to the redundant module
		SA module faulty or missing (applicable only to Mediant 3000)	Make sure the Shelf Alarm module is inserted correctly.
		Eth link error	HA was lost due to switchover, Connect the Eth link back.
		Higher HA priority (Not applicable to Mediant 3000)	HA was lost due to switchover to unit with higher HA priority and should return automatically after a few minutes. Corrective action is not required.
		Network watchdog error	HA was lost due to switchover, fix the network connectivity from failed unit.
Minor	HA feature is active and the redundant module is in startup mode and hasn't connected yet	Waiting for redundant to connect (applicable only to Mediant 3000)	Corrective action is not required.

Cleared	HA system is active	-	-

6.4.2 HA System Configuration Mismatch Alarm

HA System Configuration Mismatch Alarm

Description	HA feature is active. The active module was unable to transfer the License Key to the redundant module.		
SNMP Alarm	acHASystemConfigMismatchAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34		
Alarm Source	System#0/Module#<m>, where *m* is the blade module's slot number		
Alarm Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major (default)	HA feature is active:	Configuration mismatch in the system:	The actions for the conditions are described below.
	License Keys of Active and Redundant modules are different.	Active and Redundant modules have different feature keys.	Update the Feature Keys of the Active and Redundant modules.
	The Active module was unable to pass on to the Redundant module the License Key.	Fail to update the redundant with feature key.	Replace the Feature Key of the Redundant module – it may be invalid.
	License key of the Redundant module is invalid.	Feature key did not update in redundant module.	Replace the Feature Key of the Redundant module – it may be invalid.
Cleared	Successful License Key update	The feature key was successfully updated in the redundant module	-

6.4.3 HA System Switch Over Alarm

HA System Switch Over Alarm

Description	Sent when a switchover from the active to the redundant module has occurred.		
SNMP Alarm	acHASystemSwitchOverAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35		
Default Severity	Critical		
Alarm Source	System#0/Module#<m>, where *m* is the blade module's slot number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	A switchover from the active to the redundant unit has occurred	Switch-over: See the acHASystemFaultAlarm table above	See Section 6.4.2 above for details.
Cleared	10 seconds have passed since the switchover	-	-

6.4.4 Hitless Software Upgrade Alarm

acHitlessUpdateStatus

Description	A Notification trap that is sent out at the beginning and the end of a Hitless SW update. Failure during the process will also instigate the trap.		
SNMP Alarm	acHitlessUpdateStatus		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48		
Alarm Title	Hitless Update event		
Alarm Source	Automatic Update		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Indeterminate	A notification trap sent at the *beginning* and *end* of a hitless software update. Failure *during* the software update also activates the trap.	Hitless Update Event	The corrective action for each condition is described below.
	Hitless: Start software upgrade.		Corrective action is not required.
	Hitless fail: Invalid cmp file file - missing Version parameter.		Replace the cmp file with a valid one.
	Hitless fail: The software version stream name is too long.		Replace the cmp file with a valid one.
	Hitless fail: Invalid cmp file - missing UPG parameter.		Replace the cmp file with a valid one.
	Hitless fail: Hitless software upgrade is not supported.		Replace the cmp file with a valid one that supports hitless upgrade of the software from the current version to the new one.
	Hitless: Software upgrade ended successfully.		Corrective action is not required.

6.4.5 Redundant Board Alarm

Redundant Board Alarm

Description	Active board sends notification when an alarm or notification is raised in the redundant board.
SNMP Alarm	acRedundantBoardAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.97
Alarm Title	Redundant Board Alarm
Alarm Source	-
Alarm Type	Notification
Probable Cause	-
Severity	-
Additional Info	-
Corrective Action	-

6.4.6 HA Network Watchdog Status Alarm

HA Network Watchdog Status Alarm

Description	This alarm indicates that the device's HA Network Reachability (network watchdog) feature is configured, but is not functioning correctly due to, for example, the Ethernet Group being down from where the ping is sent to the network entity. The device's HA Network Reachability feature is used to configure a network IP address to test reachability using pings. When the tested peer stops replying to the Active unit, a switchover is made to the Redundant unit. For configuring the HA Network Reachability feature, refer to the *User's Manual*.	
SNMP Alarm	acHANetworkWatchdogStatusAlarm	
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.98	
Alarm Title	HA Network Watchdog Status Alarm	
Alarm Source	System#0/Module#<m>, where *m* is the blade module's slot number	
Alarm Type	alarmTrap	
Probable Cause	outOfService	
Default Severity	Major	
Trap Text	**Condition**	**Corrective Action**
Failed sending ping	Some network configuration error	-
Network watchdog is disabled while HA priority is in use	When HA Priority is in use, the network watchdog module is disabled	-
Network watchdog is disabled while Redundant units has less Eth groups available	One or more of the Redundant unit's Ethernet Groups are down	-
Disabling network watchdog due to network interface error in Redundant unit	One or more of the Redundant unit's Ethernet Groups are down	-

6.4.7 Cluster HA Usage Alarm

This alarm is applicable for the Mediant 9000 SBC and the Mediant Software SBC products.

CM Cluster HA Alarm

Description	The alarm is raised by the Cluster Manager when the cluster HA usage exceeds 100%. HA usage of 100% means that if a failure occurs in a Media Transcoder, sufficient DSP resources are available on the other Media Transcoders in the cluster to take over the transcoding sessions of the failed Media Transcoder. HA usage exceeding 100% means that insufficient DSP resources are available on the other Media Transcoders to take over the transcoding sessions of the failed Media Transcoder.		
SNMP Alarm	acMtcmClusterHaAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.115		
Alarm Title	CM Cluster HA Alarm		
Alarm Source	device/clusterManager		
Alarm Type	equipmentAlarm		
Probable Cause	Other		
Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Cluster HA usage exceeds 100%.	"At least one of the MTCEs is inactive, MTC will now provide only partial HA"	Make sure all Media Transcoders are properly connected to the Cluster Manager. Make sure all Media Transcoders in the Media Transcoders table are in Admin State “Unlocked” and Status “Connected”.
Cleared	HA usage drops to below 95%	-	-

6.4.8 License Key Hitless Upgrade Alarm

License Key Hitless Upgrade Alarm

Description	Feature key hitless upgrade failed due to failure of switchover process.		
SNMP Alarm	acLicenseKeyHitlessUpgradeAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.129		
Alarm Title	License Key Hitless Upgrade Alarm		
Alarm Source	system0Mo		
Alarm Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Major	Feature key hitless upgrade failed due to failure of switchover process.	Feature key hitless upgrade failed due to failure of switchover process.	Reload the Feature key run the hitless process.

6.5 Media Transcoder Alarms

6.5.1 Media Transcoder Network Failure

This alarm is applicable for the Mediant 9000 SBC and the Mediant Software SBC products.

MT Network Failure

Description	The alarm is raised when the Cluster Manager fails to connect to the Media Transcoder.		
SNMP Alarm	acMtceNetworkFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.116		
Alarm Title	MT Network Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	communicationsAlarm		
Probable Cause	Other		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Connection failure with Media Transcoder	“No Connection with MTCE: <MTCE-name>"	Make sure a physical connection exists between the Media Transcoder and the Cluster Manager.
Cleared	Connection established / re-established with Media Transcoder	-	-

6.5.2 Media Transcoder Software Upgrade Failure

MT SW Upgrade Failure

Description	The alarm is raised upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Transcoder.		
SNMP Alarm	acMtceSwUpgradeFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.117		
Alarm Title	MT SW Upgrade Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	processingErrorAlarm		
Probable Cause	other		
Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Software upgrade (.cmp) or Auxiliary file load failure in Media Transcoder	""Reset of the MTCE is required"	Reset the Media Transcoder and perform the upgrade process again. If the upgrade fails again, contact your AudioCodes support representative.
Cleared	Upon reset of Media Transcoder	-	-

6.5.3 Media Transcoder High Temperature Failure

Media Transcoder High Temperature Failure

Description	The alarm is raised when the temperature of the Media Transcoder chassis reaches a critical threshold.		
SNMP Alarm	acMtceHwTemperatureFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.118		
Alarm Title	MT Temperature Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	Equipment Alarm		
Probable Cause	-		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Temperature of Media Transcoder reaches critical threshold	"MTCE reached high temperature threshold"	▪ Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels. ▪ Check the chassis ventilation outlet and make sure that they are not obstructed for air flow. ▪ Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Connectivity with Media Transcoder is re-established and temperature is reduced	-	-

6.5.4 Media Transcoder Fan Tray Module Failure

This alarm is applicable for the Mediant 9000 SBC and the Mediant Software SBC products.

MT HW Fan Tray Failure

Description	The alarm is raised upon a failure in the Fan Tray module of the Media Transcoder.		
SNMP Alarm	acMtceHwFanTrayFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.119		
Alarm Title	MT HW Fan Tray Failure		
Alarm Source	…./MTCE#1/fanTray#1		
AlarmType	equipmentAlarm		
Probable Cause	heatingVentCoolingSystemProblem		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Minor	Failure in Fan Tray module of Media Transcoder	"MTCE fan tray fault"	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module status returns to normal	-	-

6.5.5 Media Transcoder Power Supply Module Failure

MT Power Supply Failure

Description	The alarm is raised upon a failure in the Power Supply module of the Media Transcoder.		
SNMP Alarm	acMtcePsuFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.120		
Alarm Title	MT Power Supply Failure		
Alarm Source	…./MTCE#1/powerSupply#1		
AlarmType	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Minor	Failure in Power Supply module of Media Transcoder	"MTCE power supply unit fault"	• Check if the Power Supply module is inserted in the chassis. • If it was removed from the chassis, re-insert it. • If the Power Supply module is inserted in the chassis and the alarm is still raised, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Power Supply module status returns to normal	-	-

6.6 MP-1288 Alarms

6.6.1 Module Service Alarm

acModuleServiceAlarm

Description	This alarm is raised in the following circumstances: • Multiple FXS ports on a specific FXS blade are Out-Of-Service. • Hardware faults with the blades DSP.		
SNMP Alarm	acModuleServiceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.122		
Alarm Source	Chassis/Module# (Analog)		
Event Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	More than five FXS ports and less than 33% of FXS ports are Out-Of-Service on a this blade.	Multiple FXS ports are Out-Of-Service.	Service the faulty blade.
Major	• More than 33% of FXS ports are Out-Of-Service on this blade. • There is a hardware fault on the DSP blade. If the fault is due to the exceeding of the high temperature limit, all FXS ports on this blade are Out-Of-Service.	Multiple FXS ports are Out-Of-Service.	Service the faulty blade.
Clear	*Major to Minor:* Less than 25% of FXS ports are Out-Of-Service on the blade.	-	If this alarm has been raised as a result of a high DSP temperature as described above, then you must power reset the device to return the blade to service.

	The FXS module has less than 4 FXS ports that are Out-Of-Service on the blade.		

6.6.2 Module Operation Alarm

acModuleOperationAlarm

Description	This alarm is raised when there is operational hardware failure on FXS port or the blades DSP/CPU.		
SNMP Alarm	acModuleOperationalAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.123		
Alarm Source	Chassis/Module# (Analog / CPU)		
Event Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	An operational hardware failure has been detected on between one port to 33% of FXS ports on a specific blade.	Operational failure was detected on Analog/CPU blade.	Service the faulty blade.

Major	An operational hardware failure has been detected on more than 33% of FXS ports on the blade.	Operational failure was detected on Analog/CPU blade.	Service the faulty blade.
	An operational hardware failure has been detected on the blades DSP/CPU. The problem could not be resolved after successive reset attempts.	"Blade is out-of-service due to operational failure"	
Clear	*Major to Minor:* hardware faults have been detected on less than 25% of the blades FXS ports.		If this alarm has been raised as a result of DSP or CPLD failure as described above, then you must power reset the device to return the blade to service.
	Clear: No hardware faults have been detected on any of the blades FXS ports.		

6.6.1 Port Service Alarm

acPortServiceAlarm

Description	This alarm is raised when an FXS port is out of service due to the following: • The Serial Peripheral Interface (SPI) connection with the port is lost. • The temperature threshold on an FXS port has been exceeded. • An FXS port is inactive due to a ground fault.		
SNMP Alarm	acPortServiceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.124		
Alarm Source	Chassis/Module#/FXS Port #		
Event Type	equipmentAlarm		
Probable Cause	outOfService		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	The relevant FXS ports is faulty due to the reasons described above. In addition, note the following: • If the number of faulty FXS ports is above four on the same module, then the acModuleOperationAlarm alarm is raised (see above). • If there were active sessions on the device, then these calls are disconnected. No new SIP outbound calls will be initiated towards these FXS lines on this device.	"FXS Port state was changed to Out of Service" (the detailed reason will be provided in: Syslog, in the Web detailed port status description and in WEB tooltip per FXS port)	Service the faulty FXS port.

Clear	This alarm is cleared when: • The Serial Peripheral Interface (SPI) connection is restored. • The FXS port temperature falls within the threshold. • The ground fault is cleared. • The acModuleServiceAlarm (see above) is raised i.e. the number of faulty FXS ports on the module is above four.		

6.7 MSBR Alarms

6.7.1 WAN Link Alarm

WAN Link Alarm

Description	This alarm is raised when the WAN Link is down and cleared when the link is up.
SNMP Alarm	acBoardWanLinkAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.79
Alarm Title	WAN Link alarm
Alarm Source	Board#x/WanLink#y
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	Major / Clear
Additional Info	-
Corrective Action	Connect the WAN port.

6.7.2 Power Over Ethernet Status [Event]

Power over Ethernet Status [Event]

Description	This event is sent when Power over Ethernet (PoE) for a specific port is disabled.
SNMP Alarm	acPowerOverEthernetStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.80
Alarm Title	[Event] Power over Ethernet Status
Alarm Source	-
Alarm Type	-
Probable Cause	underlyingResourceUnavailable
Event Text	"POE Port %d Was Not Powered Due To Power Management" where %d is the Ethernet port number
Default Severity	Indeterminate
Condition	This trap is sent when insufficient power is available for a plugged-in PoE client in a PoE-enabled LAN port.
Additional Info	-
Corrective Action	-

6.7.3 Wireless Cellular Modem Alarm

Wireless Cellular Modem Alarm

Description	This alarm is raised when either the wireless modem is down or in backup mode and is cleared when the wireless modem is up.		
SNMP Alarm	acWirelessCellularModemAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.82		
Alarm Title	Wireless Cellular Modem Alarm		
Default Severity	Major / Clear		
Source Varbind Text	Board#x/WanLink#y		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised when either the wireless modem is down or in backup mode, and cleared when modem is up.	WAN wireless cellular modem alarm	Get the link up. Investigate the possibility of an electronics failure or a problem with the radio frequency (RF) path.
Clear	WAN link up	-	-

6.7.4 Data Interface Status

Data Interface Status

Description	This alarm is sent when a DSL interface state changes to up or down.
SNMP Alarm	acDataInterfaceStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.83
Alarm Title	-
Alarm Source	-
Alarm Type	communicationsAlarm
Probable Cause	communicationsProtocolError
Severity	indeterminate
Additional Info	-
Corrective Action	-

6.7.5 NQM Connectivity Alarm

NQM Connectivity Alarm

Description	This alarm is raised when connectivity with the NQM probe destination is lost and cleared when connectivity with the NQM probe destination is re-established.		
SNMP Alarm	acNqmConnectivityAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.88		
Alarm Title	Connectivity with NQM probe destination is lost.		
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsSubsystemFailure		
Probable Cause	Raised when Connectivity with NQM probe destination is lost		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Connectivity with NQM probe destination is lost	Cleared when connectivity with the Noise Quality Measure (NQM) probe destination is re-established

6.7.6 NQM RTT Alarm

NQM RTT Alarm

Description	This alarm is raised when high RTT towards the NQM probe destination is detected.		
SNMP Alarm	acNqmRttAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.89		
Alarm Source	Board#%d/NqmSender#%d		
AlarmType	communicationsSubsystemFailure		
Probable Cause	Raised when Detected high RTT towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected high RTT towards NQM probe destination	To correct long RTT (Round Trip Time): ▪ Test with traceroute. ▪ Contact your ISP with the traceroute results. ▪ Use Wireshark or any other diagnostic tool to perform a traffic capture and determine who is contaminating the network.

6.7.7 NQM Jitter Alarm

NQM Jitter Alarm

Description	This alarm is raised when high Jitter towards the NQM probe destination is detected.		
SNMP Alarm	acNqmJitterAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.90		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Jitter towards NQM probe destination - thresholdCrossed		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected high Jitter towards NQM probe destination	To correct high jitter: ▪ Test with traceroute. ▪ Contact your Internet Service Provider (ISP) with traceroute results. ▪ Implement Quality of Service (QoS). ▪ Note that there's no simple solution for high jitter. A systemic level solution may be required.

6.7.8 NQM Packet Loss Alarm

NQM Packet Loss Alarm

Description	This alarm is raised when high packet loss towards the NQM probe destination is detected.		
SNMP Alarm	acNqmPacketLossAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.91		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Packet Loss towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected high PL towards NQM probe destination	To correct high packet loss (PL): ▪ Eliminate interference problems: Distance your modem from electrical devices ▪ Do not coil up any excess signal or power cables. ▪ Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring.

6.7.9 NQM MOS CQ Alarm

NQM MOS CQ Alarm

Description	This alarm is raised when low conversational voice quality towards the NQM probe destination is detected.		
SNMP Alarm	acNqmCqMosAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.95		
Alarm Title	Detected low conversational voice quality towards NQM probe destination		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	communicationsAlarm		
Probable Cause	Raised when Detected low conversational voice quality towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected low conversational voice quality towards NQM probe destination	To fix the Noise Quality Measure (NQM) result: ▪ Perform corrective action for jitter. See Section 6.7.7 ▪ Perform corrective action for Real Time Protocol (RTP) packet loss. See Section 6.7.8 ▪ Perform corrective action for long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination. See Section 6.7.6 To fix the poor Conversational Quality (CQ) that the test indicates: ▪ Try changing the coder ▪ Try using RTP-Redundancy ▪ Perform corrective action for RTP packet loss. See Section 6.7.8

6.7.10 NQM MOS LQ Alarm

NQM MOS LQ Alarm

Description	This alarm is raised when low listening voice quality towards the NQM probe destination is detected.		
SNMP Alarm	acNqmLqMosAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.96		
Alarm Source	Board#%d/NqmSender#%d		
AlarmType	communicationsAlarm		
Probable Cause	Raised when detected low listening voice quality towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected low listening voice quality towards NQM probe destination	To fix the Noise Quality Measure (NQM) result: ▪ Perform corrective action for Real Time Protocol (RTP) packet loss. See Section 6.7.8 To fix the poor listening quality that the test indicates: ▪ Try changing the coder ▪ Try using RTP-Redundancy ▪ Perform corrective action for RTP packet loss. See Section 6.7.8

6.8 Mediant 3000 Hardware Alarms

6.8.1 PEM Module Alarm

PEM Module Alarm

Description	This alarm is sent in one of the following cases: ▪ The HA (High Availability) feature is active and one of the PEM (Power Entry Module) units is missing ▪ PEM card is in its location and both DC wires are in.		
SNMP Alarm	acPEMAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.31		
Default Severity	Critical		
Alarm Source	hassis#0/PemCard#<m>, where *m* is the power entry module's (PEM) slot number		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	The HA (High Availability) feature is active and one of the PEMs (Power Entry Modules) is missing.	PEM Module Alarm. PEM card is missing.	• Make sure the PEMs are present and that they're inserted correctly. • If it's present and inserted correctly yet the alarm remains active, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	PEM card is placed and both DC wires are in.	-	-

6.8.2 SA Module Missing Alarm

SA Module Missing Alarm

Description	This aalrm is sent when the Shelf Alarm (SA) module is missing or non operational.		
SNMP Alarm	acSAMissingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.32		
Alarm Title	SA Module Missing Alarm		
Alarm Source	Chassis#0/SA#<m>, where *m* is the shelf Alarm module's slot number		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	SA module removed or missing	SA Module Alarm. SA-Module from slot #n is missing.	▪ Reinsert the Shelf Alarm (SA) module into slot #n ▪ Make sure it's correctly inserted in the slot.
Cleared	SA module is in slot 2 or 4 and working.	-	-

6.8.3 User Input Alarm

User Input Alarm

Description	Sent when the input dry contact is short circuited; cleared when the circuit is reopened.		
SNMP Alarm	acUserInputAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.36		
Alarm Source	Chassis#0		
Alarm Type	equipmentAlarm		
Probable Cause	inputDeviceError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	Input dry contact is short circuited.	User input Alarm. User's Input-Alarm turn on.	Reopen the input dry contact.
Cleared	Input dry contact circuit is reopened.	-	-

6.8.4 TM Inconsistency

TM Inconsistency

Description	Timing Manager Alarm. This alarm is triggered when the system is in a 1+1 status and the redundant board PLL status is different to the active board PLL status.
SNMP Alarm	acTMInconsistentRemoteAndLocalPLLStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.56
Alarm Title	TM Inconsistency
Alarm Source	-
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	Major, Clear
Additional Info	Status stays major until reboot. A clear trap is not sent.
Corrective Action	Synchronize the timing module.

6.8.5 TM Reference Status

TM Reference Status

Description	Timing Manager Alarm. This alarm is triggered when either the primary or secondary BITs reference or both BITs references are not responding.
SNMP Alarm	acTMReferenceStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.57
Alarm Title	TM Reference Status
Alarm Source	-
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	Major, Critical, Clear
Additional Info	When the primary and secondary BITs clock references do not respond in more than 24 hours, an alarm will be escalated to critical. The status of this alarms stays major until reboot. A clear trap is not sent.
Corrective Action	Synchronize the timing module.

6.8.6 TM Reference Change

TM Reference Change

Description	The Timing Manager sends a log message upon PLL Status change.
SNMP Alarm	acTMReferenceChange
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.58
Alarm Title	[Event] TM Reference Change
Alarm Source	-
Alarm Type	Other
Probable Cause	Other
Severity	indeterminate
Additional Info	-
Corrective Action	-

6.9 PSTN Trunk Alarms

6.9.1 D-Channel Status

D-Channel Status

Description	Non-alarm trap sent at the establishment, re-establishment or release of LAPD link with its peer connection occurs. The trap is sent with one of the following textual descriptions: • D-channel synchronized • D-channel not-synchronized
SNMP Alarm	acDChannelStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
Alarm Title	D-Channel Status
Alarm Source	Trunk no.<m> where m is the trunk number (from 0 up).
Alarm Type	Communications Alarm
Probable Cause	Communications Protocol Error
Severity	Minor on raise, Clear on clear
Additional Info	-
Corrective Action	-

6.9.2 SONET Section LOF Alarm

SONET Section LOF Alarm

Description	This alarm indicates that a LOF condition is present on SONET no#m. The field 'sonetSectionCurrentStatus' in the sonetSectionCurrentTable will have a value of sonetSectionLOF (4).		
SNMP Alarm	acSonetSectionLOFAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.38		
Default Severity	Critical		
Alarm Source	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	LOF condition is present on SONET no.n	SONET-Section LOF	Make sure the framing format on the port matches the format configured on the line. Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value **sonetSectionLOF(4)**
Cleared	LOF condition is not present	LOF	-

6.9.3 SONET Section LOS Alarm

SONET Section LOS Alarm

Description	This alarm indicates that LOS or AIS condition is present on SONET no #m. The field 'sonetSectionCurrentStatus' in the sonetSectionCurrentTable will have a value of sonetSectionLOS (2).		
SNMP Alarm	acSonetSectionLOSAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.39		
Alarm Source	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	LOS condition is present on SONET no #n	SONET-Section LOS	▪ Make sure the fiber optic cable is plugged in correctly. ▪ Make sure it's not damaged. ▪ Make sure its remote end is correctly connected and undamaged. ▪ Make sure that configuration of the remote port is correct. Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value **sonetSectionLOS (2)**
Cleared	LOS condition is not present	-	-

6.9.4 SONET Line AIS Alarm

SONET Line AIS Alarm

Description	This alarm indicates that an AIS condition is present on SONET-Line #m. The field 'sonetLineCurrentStatus' in the sonetLineCurrentTable will have a value of sonetLineAIS (2).		
SNMP Alarm	acSonetLineAISAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.40		
AlarmSource	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	AIS condition is present on SONET-Line #n	SONET-Line AIS	If an Alarm Indication Signal (AIS) condition is present on a SONET line: • Make sure the remote configuration is correct. • Check the line status at the remote end of the link. Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value **sonetLineAIS (2)**
Cleared	AIS condition is not present.	-	-

6.9.5 SONET Line RDI Alarm

SONET Line RDI Alarm

Description	This alarm indicates that RDI condition is present on SONET-Line no#m. The field 'sonetLineCurrentStatus' in the sonetLineCurrentTable will have a value of sonetLineRDI (4).		
SNMP Alarm	acSonetLineRDIAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.41		
Alarm Source	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	RDI condition is present on SONET-Line #n	SONET-Line RDI	• Check the *remote site* for alarm conditions. • Correct a line problem that has arisen from the *remote interface*. Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value **sonetLineRDI (4)**
Cleared	RDI condition is not present.	-	-

6.9.6 SONET/SDN IF Failure Alarm

SONET/SDN IF Failure Alarm

Description	This alarm indicates a HW failure on SONET-Line no#m
SNMP Alarm	acSonetIfHwFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.42
Alarm Title	SONET/SDH IF Failure Alarm
Alarm Source	Interfaces#0/Sonet#<m> where m is the SONET I/F number
Alarm Type	Communications Alarm
Probable Cause	Transmit failure
Severity	Critical on raise, Clear on clear
Additional Info	-
Corrective Action	-

6.9.7 Trunk LOS Alarm

This alarm applies to E1/T1Trunks.

Trunk LOS Alarm

Description	This alarm indicates a loss of signal at the trunk's near end.		
SNMP Alarm	acTrunksAlarmNearEndLOS		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.49		
Alarm Title	Trunk LOS Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	Near-end LOS	Trunk LOS Alarm	Los of Signal (LOS) indicates a physical problem. • Check that the cable is connected on the board. • Check that the correct cable type is being used (crossed/straight). • Contact AudioCodes' Support Center at support@audiocodes.com.
Cleared	End of LOS	-	-

6.9.8 Trunk LOF Alarm

This alarm applies to E1/T1Trunks.

Trunk LOF Alarm

Description	This alarm indicates a loss of frame at the trunk's near end.		
SNMP Alarm	acTrunksAlarmNearEndLOF		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.50		
Alarm Title	Trunk LOF Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical (default)	Near end LOF	Trunk LOF Alarm	Make sure that the trunk is connected to a proper follow-up device. • Make sure that both sides are configured with the same (E1 / T1) link type. • Make sure that both sides are configured with the same framing method. • Make sure that both sides are configured with the same line code. • Make sure that the clocking setup is correct. • Contact AudioCodes' Support Center at support@audiocodes.com.
Cleared	End of LOF	-	-

6.9.9 Trunk AIS Alarm

This alarm applies to E1/T1Trunks.

Trunk AIS Alarm

Description	This alarm indicates that an AIS is received from the trunk's far end.		
SNMP Alarm	acTrunksAlarmRcvAIS		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.51		
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Title	Trunk AIS Alarm		
Alarm Type	communicationsAlarm		
Probable Cause	PSTN provider has stopped the trunk (receiveFailure)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Receive AIS	Trunk AIS Alarm	• Contact your PSTN provider to activate the trunk. • If the alarm persists, contact the AudioCodes Support Center at support@audiocodes.com
Cleared	End of AIS	-	-

6.9.10 Trunk RAI Alarm

Trunk RAI Alarm

Description	This alarm indicates a loss of frame at the trunk's far end.
SNMP Alarm	acTrunksAlarmFarEndLOF
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.52
Alarm Title	Trunk RAI Alarm
Alarm Source	Port#<n> where n is the digital trunk number
Alarm Type	communicationsAlarm
Probable Cause	transmitFailure
Severity	Critical
Additional Info	-
Corrective Action	Check trunk's connectivity

6.9.11 V5.2 Interface Alarm

V5.2 Interface Alarm

Description	A V5.2 Interface alarm is raised in one of the following cases. For detailed V5.2 Interface condition, refer to the V5.2 Interfaces status table. An Alarm is raised with critical severity when: ▪ V5 interfaces ID are not equal on both sides ▪ V5 variants are not equal on both sides ▪ V5 link ID check timeout error occurred ▪ Layer 2 startup failed ▪ V5 restart failed An Alarm is raised with major severity when: ▪ Control protocol data link error ▪ Link control protocol data link error ▪ BCC protocol data link error ▪ PSTN protocol data link error ▪ Protection DL1 failure ▪ Protection DL2 failure
SNMP Alarm	acV52InterfaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.60
Alarm Title	V5.2 Interface Alarm.
Alarm Source	V5.2IF#
Alarm Type	Communications Alarm
Probable Cause	Communications Protocol Error
Severity	Critical, Major, Clear
Additional Info	-
Corrective Action	For critical severity alarms, solve configuration mismatch (configuration does not comply to far end configuration). For major severity alarms: ▪ Ensure physical connections are in place. ▪ Ensure links are not administratively blocked. ▪ Resolve configuration issues.

6.9.12 SONET Path STS LOP Alarm

SONET Path STS LOP Alarm

Description	This alarm is issued when the LOP condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTSLOPAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.61
Alarm Title	SONET Path STS LOP Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-
Corrective Action	Correct the SONET mapping on either side (the Gateway and the far end).

6.9.13 SONET Path STS AIS Alarm

SONET Path STS AIS Alarm

Description	This alarm is issued when the AIS condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTSAISAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.62
Alarm Title	SONET Path STS AIS Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-
Corrective Action	Check the following and correct according to the appropriate reason: There is higher level failure: LOS, LOF, AIS-L A Path Trace Identifier mismatch occurred • Path is unequipped on the Far-End

6.9.14 SONET Path STS RDI Alarm

SONET Path STS RDI Alarm

Description	This alarm is issued when the RDI condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTSRDIAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.63
Alarm Title	SONET Path STS RDI Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	transmitFailure
Severity	Critical / Cleared
Additional Info	-
Corrective Action	This indication only reflects a failure detected on the far-end. Check the following and correct on the far-end according to the appropriate reason: LOS, LOF, AIS-L, AIS-P

6.9.15 SONET Path Unequipped Alarm

SONET Path Unequipped Alarm

Description	This alarm is issued when the Unequipped condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathUnequippedAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.64
Alarm Title	SONET Path Unequipped Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-
Corrective Action	Equip the path on the far-end

6.9.16 SONET Path Signal Label Alarm

SONET Path Signal Label Alarm

Description	This alarm is issued when the Signal Label condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSignalLabelMismatchAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.65
Alarm Title	SONET Path Signal Label Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-
Corrective Action	Set the transmit path signal label on the far-end to either "VT Structured STS1 SPE" (02) or "Asynchronous Mapping DS3" (04).

6.9.17 DS3 RAI Alarm

DS3 RAI Alarm

Description	This alarm is issued when the RAI condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3RAIAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.66
Alarm Title	DS3 RAI Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	transmitFailure
Severity	Critical / Cleared
Additional Info	-
Corrective Action	This indication only reflects a failure detected on the far-end. Check the following and correct on the far-end according to the appropriate reason: LOS, LOF, AIS-L, AIS-P, DS3 LOS, DS3 LOF, DS3 AIS

6.9.18 DS3 AIS Alarm

DS3 AIS Alarm

Description	This alarm is issued when the AIS condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3AISAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.67
Alarm Title	DS3 AIS Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / Cleared
Additional Info	-
Corrective Action	Check the following and correct according to the appropriate reason: There is a SONET level failure: LOS, LOF, AIS-L, AIS-P, UNEQ-P, TIM-P The far-end (e.g., MUX) sends a DS3 AIS

6.9.19 DS3 LOF Alarm

DS3 LOF Alarm

Description	This alarm is issued when the LOF condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3LOFAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.68
Alarm Title	DS3 LOF Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / Cleared
Additional Info	-
Corrective Action	Check and correct the DS3 framing

6.9.20 DS3 LOS Alarm

DS3 LOS Alarm

Description	This alarm is issued when the LOF condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3LOSAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.69
Alarm Title	DS3 LOS Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	lossOfFrame
Severity	Critical / Cleared
Additional Info	-
Corrective Action	Check the cable connections or cable length

6.9.21 NFAS Group Alarm

NFAS Group Alarm

Description	This alarm is raised when an NFAS group goes Out-Of-Service and is cleared when an NFAS Group is back In-Service.		
SNMP Alarm	acNFASGroupAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.84		
Alarm Source	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	degradedSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major (default)	Raised when an NFAS group goes out-of-service	NFAS Group Alarm. %s	▪ The alarm is sent only when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when *both* D-channels are down. ▪ When at least one of the D-channels (primary or backup) returns to service, the alarm is cleared. ▪ Corrective action is not necessary.
Clear	NFAS group state goes to in- service	%s– Additional information	-

6.9.22 B Channel Alarm

B Channel Alarm

Description	This alarm is raised when the B-Channel service state changes and is cleared when the B-Channel is back in service.		
SNMP Alarm	acBChannelAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.85		
Alarm Title	B-Channel Alarm.		
Alarm Source	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
AlarmType	communicationsAlarm		
Probable Cause	degradedSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major (default)	Raised when B-channel service state changes to 'Out of Service' or 'Maintenance'	B-Channel Alarm. %s	Corrective action is not necessary
Clear	B-channel status changes to 'In Service'	%s – additional information	-

6.10 Analog Port Alarms

6.10.1 Analog Port SPI Out of Service

Analog Port SPI Out of Service

Description	This alarm indicates that an analog port out of service.
SNMP Alarm	acAnalogPortSPIOutOfService
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.46
Alarm Title	Analog Port SPI out of service
Alarm Source	Port#<m> where m is the analog port number
Alarm Type	Physical Violation
Probable Cause	Equipment Malfunction
Severity	Major on raise, Clear on clear
Additional Info	-
Corrective Action	-

6.10.2 Analog Port High Temperature

Analog Port High Temperature

Description	This alarm indicates that an analog FXS port has a high temperature.
SNMP Alarm	acAnalogPortHighTemperature
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.47
Alarm Title	Analog Port High Temperature
Alarm Source	Port#<m> where m is the analog port number
Alarm Type	Physical Violation
Probable Cause	Equipment Malfunction
Severity	Major on raise, Clear on clear
Additional Info	-
Corrective Action	-

6.10.3 Analog Port Ground Fault Out-of-Service Alarm

Table 6-2: acAnalogPortGroundFaultOutOfService

Description	This alarm indicates that there is a ground fault in the analog port.
SNMP Alarm	acAnalogPortGroundFaultOutOfService
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Alarm Title	Analog Port Ground Fault Out Of Service
Alarm Source	System#0/analogports#<n>, where *n* is the port number
Alarm Type	physicalViolation
Default Severity	Major / Clear
Probable Cause	equipmentMalfunction (this alarm is raised when the FXS port is inactive due to a ground fault)
Alarm Text	Analog Port Ground Fault Out Of Service
Corrective Action	▪ No corrective action is required. ▪ The device shuts down the port and tries to activate it again when the relevant alarm is over.
Note	Relevant to FXS only.

6.11 CloudBond 365 Alarms

6.11.1 Commit License Failed

Commit License Failed

Description	This alarm is raised when the EMS Main Agent is unable to store the license in the Active Directory.		
SNMP Alarm	acCbManLicenseCommitAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.1		
Alarm Source	N/A		
Alarm Title	Commit License Failed		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Unable to store the license in the Active Directory	Unable to commit the license in Active Directory.	Verify that EMS Agent can access the local Active Directory. Verify that the local Active Directory contains the contact ‘CbLicense’.

Cleared	The license has been successfully stored in the Active Directory.	-	

6.11.2 Component Unreachable

Component Unreachable

Description	This alarm is raised when the EMS Main Agent is unable to connect to one of the client agents in the CloudBond environment.		
SNMP Alarm	acCbManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Client agent is unavailable	Unable to connect to the client agent on <CloudBond component name>.	
Cleared	Client agent is available again.	-	

6.11.3 Component Restart

Component Restart

Description	This alarm is raised when a CloudBond component has restarted.
SNMP Alarm	acCbManEnvRestartEvent
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.3
Alarm Source	<n> (where n is the component name)
Alarm Title	Component Restart
Alarm Type	Other
Probable Cause	Other
Additional Info	The restart reason

Alarm Severity	Condition	<text>	Corrective Action
Major	Indeterminate	CloudBond component <component name> restarted	-
Cleared	-	-	

6.11.4 Component Performance Counter General

Component Performance Counter General

Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory, CPU and disk space.		
SNMP Alarm	acCbCompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.11		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-
Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-
Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-
Cleared	When counter returns below the threshold level.	-	

6.11.5 Component Performance Counter Service

Component Performance Counter Service

Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. This alarm is related to activity of Skype for Business/Lync services.		
SNMP Alarm	acCbCompPcServAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.12		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	-		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Major	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Cleared	When counter returns below the threshold level.	-	

6.11.6 Component Service Status

Component Service Status

Description	This alarm is raised when a component service is down.		
SNMP Alarm	acCbCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.13		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	-
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

6.11.7 Component Event Viewer

Component Event Viewer

Description	This alarm is raised when report is generated in the Event Viewer for a component error.
SNMP Alarm	acCbCompEventViewer
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.14
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))
Alarm Title	Component Event Viewer
Alarm Type	Other
Probable Cause	Other

Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type “Info”.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Indeterminate	-	The text of the event	-

6.11.8 Component Event Viewer Past Hours

Component Event Viewer Past Hours

Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.		
SNMP Alarm	acCbCompEventLogAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.15		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Event Log has a Critical alarm.	The event log has errors	-
Major	Event Log has a Major alarm.	The event log has errors	-
Warning	Event Log has a Warning alarm.	The event log has errors	-
Cleared	No errors have occurred in the past hours.	-	

6.11.9 Component Event Viewer Dropped

Component Event Viewer Dropped

Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the EMS after the sending rate threshold has been exceeded.
SNMP Alarm	acCbCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.16

Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Additional Info	-
Alarm Severity	Indeterminate

6.11.10 Admin License Expired

Admin License Expired

Description	This alarm is raised by the CloudBond administrator when the CloudBond user license is invalid.		
SNMP Alarm	acCbAdminLicInvalidAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.21		
Alarm Source	N/a		
Alarm Title	Admin License Expired		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	License is invalid/expired	▪ License expired on <Data of the license> ▪ Invalid license or missing license in Active Directory	-
Cleared	License is valid	-	-

6.11.11 Alarm – Certificate Expired

Description	This alarm is raised when the certificate in the CloudBond component is about to expire.
SNMP Alarm	acCceAdminCertificateExpiredAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.32
Alarm Source	<n> (where n is the component name)
Alarm Text	Certificate will expires in <days left> days
Alarm Type	Other

Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Major	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Cleared	When certificate is renewed.	-	-

6.11.12 Alarm –Disk Space

Description	This alarm is raised when the CloudBond component's disk space is above the pre-defined threshold.		
SNMP Alarm	acCceDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.36		
Alarm Source	<e> (drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Major	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.	-	-

6.12 CCE Appliance Alarms

6.12.1 Component Unreachable

Component Unreachable

Description	This alarm is raised when the CCE Monitor Service is unable to connect to one of the component of the CCE Appliance.		
SNMP Alarm	acCbManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Appliance component is unavailable	Unable to connect to component <CCE Appliance component name>.	Verify that CCE appliance component is running and accessible via cceService user (use the password that the following powerShell return: Get-CcCredential -AccountType CceService -d). Check the CCE management service log under C:\Program Files\Skype for Business Cloud Connector Edition\ManagementService.
Cleared	Appliance component is available again.	-	

6.12.2 Event – Component Restart

Event – Component Restart

Description	This alarm is raised when a CCE Appliance component has restarted.		
SNMP Alarm	acCbManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.3		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Event – Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Indeterminate	CCE Appliance component <component name> restarted	-
Cleared	-	-	

6.12.3 Component Performance Counter General

Component Performance Counter General

Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory/CPU/disk.		
SNMP Alarm	acCbCompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.11		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	Diagnose the memory/CPU/disk on your CCE platform.
Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	Diagnose the memory/CPU/disk on your CCE platform.

Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	Diagnose the memory/CPU/disk on your CCE platform.
Cleared	When counter returns below the threshold level.	-	

6.12.4 Component Performance Counter Service

Component Performance Counter Service

Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. Related to activity of SfB/Lync services.		
SNMP Alarm	**acCbCompPcServAlarm**		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.12		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	-		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per each counter type	<Performance counter> high level <x>	Diagnose the SfB/Lync services on your CCE platform.
Major	Pre-defined severity per each counter type	<Performance counter> high level <x>	Diagnose the SfB/Lync services on your CCE platform.
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	Diagnose the SfB/Lync services on your CCE platform.
Cleared	When counter returns below the threshold level.	-	

6.12.5 Component Service Status

Component Service Status

Description	This alarm is raised when a component service is down.		
SNMP Alarm	acCbCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.13		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	Start the service and check why the service stopped, using the event viewer.
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	Start the service and check why the service stopped, using the event viewer.
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	Start the service and check why the service stopped, using the event viewer.
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

6.12.6 Alarm – Admin System Cloud Status

Description	This alarm is raised when the CCE status on the Office 365 Cloud platform is not 'Running' mode.		
SNMP Alarm	acCceAdminSystemCloudStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.31		
Alarm Source	N/A		
Alarm Text	CCE status in the O365 Cloud is <status> ***		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**

Major	All other modes	CCE status in the Office 365 Cloud is {status}	-
Warning	Status is 'Maintenance'	CCE status in the Office 365 Cloud is Maintenance	-
Cleared	Status is 'Running'	CCE status in the Office 365 Cloud is Running	-

6.12.7 Alarm – Certificate Expired

Description	This alarm is raised when a certificate in the CCE Appliance Host has almost expired.		
SNMP Alarm	acCceAdminCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.32		
Alarm Source	N/A		
Alarm Text	Certificate will expires in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Pre-defined severity per threshold	Certificate will expires in <days left> days	Open certificate manager. Find the expired certificate and renew it.
Major	Pre-defined severity per threshold	Certificate will expires in <days left> days	Open certificate manager. Find the expired certificate and renew it.
Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Open certificate manager. Find the expired certificate and renew it.
Cleared	When certificate renewed	-	-

6.12.8 Alarm – CCE Wrong Operating

Description	This alarm is raised when the service specified in the source is not in the correct mode.		
SNMP Alarm	acCceWrongOperatingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.33		
Alarm Source	<s> (service name {Running Version/OsUpdate/Deployment/VhdFile})		
Alarm Text	• The latest CCE version is not running (when source is RunningVersion) • CCE deployment error (source is Deployment) • OS update error (source is OsUpdate) • Vhd file was not updated over {0} days. (source is VhdFile)		
Alarm Type	Other		-
Probable Cause	Other		-
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	A newer version of CCE is deployed; however CCE is using an older version.	Not last CCE version is running.	Check the CCE management service log under C:\Program Files\Skype for Business Cloud Connector Edition\ManagementService View the error and determine why CCE didn't switch to a newer version and then perform required actions accordingly.
	OS Update failed	OS update error: {error}.	Check which VM failed to upgrade and validate that it has access to the internet or to the local Windows Server Update Service. Check the CCE management service log under C:\Program Files\Skype for Business Cloud Connector Edition\ManagementService
	CCE deployment failed	CCE deployment error: {error}.	Check the logs under C:\cce\appliance\Log
Minor	Vhd file not updated over pre-defined threshold	Vhd file was not updated over {threshold value} days.	Download from Audio Codes an updated VHDX file
Cleared	Service returns to operate in the correct mode.	-	-

6.12.9 Alarm – CCE Wrong Settings

Description	This alarm is raised when the parameter specified in the source has incorrect settings.		
SNMP Alarm	acCceWrongSettingsAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.34		
Alarm Source	<p> (parameter name {UpdatesMode/MaintenanceMode})		
Alarm Text	• Maintenance mode is enabled. (When source is MaintenanceMode) • CCE updates are disabled (When source is UpdatesMode)		
Event Type	Other		-
Probable Cause	Other		-
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	CCE updates are disabled	CCE updates are disabled	Validate that Auto Update was not disabled by mistake. If required, you can enable it via the dashboard.
	Maintenance mode is enabled	Maintenance mode is enabled	Verify why the CCE is in Maintenance mode. Maybe the CCE is in a middle of an upgrade or some other operation needs to be in Maintenance mode. Wait untll the operation has ended and validate that the alarm is cleared. If the alarm is not cleared, check the CCE management service log under C:\Program Files\Skype for Business Cloud Connector Edition\ManagementService.
Cleared	Parameter has correct settings again	-	-

6.12.10 Alarm – CCE Disk Space

Description	This alarm is raised when the CCE host machine disk space is above the pre-defined threshold.
SNMP Alarm	acCceDiskSpaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.36
Alarm Source	Host/C:\
Alarm Text	Disk space usage is over {0}%
Event Type	Other
Probable Cause	Other

Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary files from the CCE appliance Host disk. Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs.
Major	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary files from the CCE appliance Host disk. Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs.
Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary files from the CCE appliance Host disk. Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs.
Cleared	Used disk space is below the threshold.	-	-

6.12.11 Alarm – CCE Windows License

Description	This alarm is raised when a CCE component specified in the 'source' field does not have an active Windows license.		
SNMP Alarm	acCceWindowsLicenseAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.37		
Alarm Source	<e> (component name {Ad/Edge/Cms/MS/Host})		
Alarm Text	Windows license status is {0}		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Pre-defined severity for license status.	Windows license status is {0}	Active the license in the component that is specified in the alarm's source.
Cleared	License status is 'Licensed'.	-	-

6.13 SBA Alarms

6.13.1 SBA Services Status Alarm

SBA Services Status Alarm

Description	Services status alarm. The services are Front End server, Mediation server, Replica server, and Centralized Logging Service for Microsoft Lync 2013 (Centralized Logging is not available for Lync 2010).		
SNMP Alarm	acSBAServicesStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.1		
Alarm Title	SBA Services Status Alarm		
Alarm Source	RtcSrv/ RTCMEDSRV/ REPLICA/ RTCCLSAGT		
Alarm Text	Service {0} stopped {0} – Service name		
Alarm Type	Other		
Probable Cause	Other		
Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Service is down	SERVICE_STOPPED	Start the service and check why the service stopped, using the event viewer.
Major	Service is paused	SERVICE_PAUSED	Start the service and check why the service paused, using the event viewer.
Cleared	Service is running	SERVICE_RUNNING	-
Indeterminate	Service in indeterminate state	SERVICE_CONTINUE_PENDING SERVICE_PAUSE_PENDING SERVICE_START_PENDING SERVICE_STOP_PENDING	Start the service and check why the service is in indeterminate state, using the event viewer.

6.13.2 Alarm – CPU Status

Description	CPU usage status alarm. Send alarm when CPU usage is above the threshold		
SNMP Alarm	acSBACpuStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.2		
Alarm Title	Alarm – CPU Status		
Alarm Source	Processor Information/%Processor Time/_Total		
Alarm Text	High CPU usage Above {0} {0} – Threshold value		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	CPU > 90%	High CPU usage Above 90%	Using task manager check if the CPU load is constant or not, find the process that causes the high CPU usage and see if high CPU is reasonable (for example high CPU when performing windows updates, or running traces on the SBA), if there isn't a reason for the high CPU try to reset the SBA and if didn't solve the issue open a call to AudioCodes
Major	CPU > 80%	High CPU usage Above 80%	Using task manager check if the CPU load is constant or not, find the process that causes the high CPU usage and see if high CPU is reasonable (for example high CPU when performing windows updates, or running traces on the SBA), if there isn't a reason for the high CPU try to reset the SBA and if didn't solve the issue open a call to AudioCodes
Cleared	CPU < 76%	-	-

6.13.3 Alarm – Memory Status

Description	Memory used status alarm. Send an alarm when the level of available physical memory is below the threshold.		
SNMP Alarm	acSBAMemorytatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.3		
Alarm Title	Alarm – Memory Status		
Alarm Source	Memory/% Available MBytes		
Alarm Text	High memory usage		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Available Memory < 7%	High memory usage, available memory is Bellow 7%	Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. if there isn't a reason for the high memory try to reset the SBA and if didn't solve the issue open a call to AudioCodes

Critical	Available Memory < 4%	High memory usage, available memory is Bellow 4%	Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. if there isn't a reason for the high memory try to reset the SBA and if didn't solve the issue open a call to AudioCodes
Cleared	Available Memory >8%		

6.13.4 Alarm – Disk Space

Description	This alarm is raised if the disk (C) usage level exceeds configured thresholds. Thresholds can be configured in the snmp_sba.ini under C:\SBA (requires service restart for the changes to take effect).		
SNMP Alarm	acSBADiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.4		
Alarm Title	Alarm – Disk Space		
Alarm Source	C:\		
Alarm Text	Disk space usage is over {0}% {0} – Threshold value		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Disk ‘C’ usage level is over 90%	"Disk space usage is over 90%"	Remove unnecessary files from disk. Clean log files.

Critical	Disk 'C' usage level is between 80% and 90%	"Disk space usage is over 80%"	
Cleared	Disk 'C' usage level is below 76%	-	

6.13.5 Alarm – Certificate Expired

Description	This alarm is raised when the certificate that is used to secure the connection between the SBA and the Datacenter is about to expire. The alarm is sent when the number of days to certificate expiration is below threshold.		
SNMP Alarm	acSbaCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.5		
Alarm Title	Alarm – Certificate Expired		
Alarm Text	Certificate will expire in {0} days.		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Number of day to expiration < 30	Certificate will expire in 30 days.	Using windows mmc tool, check the expiration date of the certificates and find the expired certificate. Sign the expired certificate and install it on the machine.
Critical	Number of day to expiration < 2	Certificate will expire in 2 days.	Using windows mmc tool, check the expiration date of the certificates and find the expired certificate. Sign the expired certificate and install it on the machine.
Cleared	New valid certificate is installed.	-	-

6.13.6 Alarm – Performance Counter

Alarm	acSbaPerfCounterAlarm	
Description	This alarm is raised when the configured performance counter's value is above/below the configured threshold.	
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.6	
Alarm Source	{Performance counter full path}	
Alarm Text	Performance counter {0} is Above/Below {1} {0} – Performance counter full path {1} – Threshold value	
Event Type	Other	
Probable Cause	Other	
Alarm Severity	**Condition**	**Corrective Action**
Major	Monitored value crossed the 'Major' threshold	-
Critical	Monitored value crossed the 'Critical' threshold	-
Cleared	Monitored value falls below the 'Major' threshold	-

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

Document #: LTRT-41606