Alarms Monitoring Guide

AudioCodes One Voice Operations Center (OVOC)

OVOC

Alarms

Version 7.8
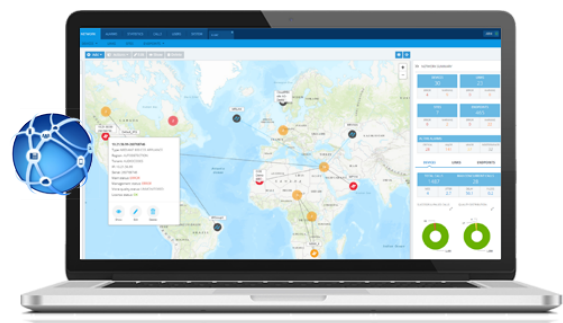
acaudiocodes

Notice

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual

Document Name
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
Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center
One Voice Operations Center IOM Manual
One Voice Operations Center Product Description
One Voice Operations Center User's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Agent Installation and Configuration Guide
ARM User's Manual

Document Revision Record

LTRT	Description
41613	■ Added Device Alarms: DSP Farms Mismatch Alarm; Metering alarm; Flex License Manager alarm ■ Added OVOC Alarms: FlexPool License Usage; Report Schedulers Time Event; Report Schedulers Load Alarm; Report Schedulers Execution Event ■ Added Device Manager Pro alarms: VIP Endpoint is not Registered or Offline and "VIP Endpoint is Disconnected ■ Added SmartTAP alarm: Call Recording Error Event ■ Added ARM alarms: Registration Status Resync Threshold and External Web Service; Changed name for General Alarm to"No Available Routers" ■ Added User Management Pack 365 (UMP) alarms: UMP Tenant License Threshold Alarm; UMP User License Threshold Alarm; UMP Super Admin Authentication Fail Event; UMP Azure AD Sync Alarm; UMP Office 365 Failure Alarm; UMP Office 365 Command Execution Event; UMP User Settings Fail Event; UMP End User Authentication Fail Event
41614	■ Added Device alarm: Remote Monitoring Alarm ■ Updated: Board Resetting Following Software Reset; Media Transcoder Software Upgrade Failure; Media Cluster Alarm ■ Correction to OID for the following alarms: FlexPool License Usage; PM Has No SNMP Connection
41615	■ ARM: Update to alarms Operation State Changed (Router); External Web Service ■ ARM: Added alarm Operation Status Changed (Active MQ) ■ SBC: Added the following SBC alarms: Metering alarm; SDR Server alarm; KPI Threshold Crossing; Clock Configuration alarm; Debug Recording Activation alarm
41616	■ Update to SmartTAP: Call Recording Error Event ■ Added ARM: Disk Space Usage Alarm

Table of Contents

1   Introduction

This document describes alarms that are raised on OVOC and its managed entities. These alarms are displayed in the One Voice Operations Center Web interface Active Alarms table. 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.

■ OVOC alarms / events: traps originated by OVOC application and defined in the OVOC proprietary MIB.

To determine 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 in the OVOC Active Alarms table and Alarms History windows.

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

Alarm Field	Description
Alarm Title (Name)	The alarm name, as it appears in the OVOC Active Alarms and History tables.
Description	Documented description of the alarm.
SNMP Trap Name	NOTIFICATION-TYPE Name as it appears in the MIB.
SNMP OID	NOTIFICATION-TYPE OID as it appears in the MIB. Corrective Action Possible corrective action when applicable. - 1
Alarm Source	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource
Alarm Type	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsType.
Probable Cause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.
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

Alarm Field	Description		
	examples of the possible values of this field.		
Alarm Severity	Condition	Text	Corrective Action
Possible severity value . This value is displayed from the variable-binding tgTrapGlobalsSeverity.	Condition upon which the alarm is raised for the specific severity. There may be several conditions for each severity.	Textual description of specific problem. This value is displayed from the variablebinding tgTrapGlobalsTextualDescription. The document includes a few examples of the possible values of this field.	Possible corrective action when applicable.

2   Standard Events

Cold Start

Alarm Field	Description
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 Source	-
Alarm Type	Communication Alarm
Probable Cause	Other
Severity	Clear
Additional Info1,2,3	-
Corrective Action	-

Link Down

Alarm Field	Description
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

Alarm Field	Description
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	-

Link Up

Alarm Field	Description
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 Source	-
Alarm Type	Communication Alarm
Probable Cause	Other
Severity	Clear
Additional	-

Alarm Field	Description
Info1,2,3	
Corrective Action	-

Entity Configuration Change

Alarm Field	Description
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	-

Authentication Failure

Alarm Field	Description
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.

Alarm Field	Description
SNMP Alarm	[Event] authenticationFailure
SNMP OID	1.3.6.1.6.3.1.1.5.5
Alarm Title	Authentication Failure
Alarm Source	-
Alarm Type	Communication Alarm
Probable Cause	Other
Severity	Major
Additional Info1,2,3	-
Corrective Action	-

3   Management Alarms

EMS Trap Receiver Binding Error

Alarm Field	Description
Description	This alarm is generated during server startup if an error occurs indicating that the SNMP trap receiver port is already taken.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.1
SNMP Alarm	acEMSSnmpCannotBindError
Alarm Title	[Event] EMS Trap Receiver Binding Error
Alarm Source	OVOC Mgmt
Alarm Type	Environmental Alarm
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). ■ OVOC application: If it's busy, check which application uses this port. If it's not freed by OVOC application, restart the OVOC server application as described in the OVOC Server IOM. ■ Other network management application: change OVOC application and all managed gateways' default alarm reception ports.
Media Gateways	All the gateways managed by OVOC

GW Connection Alarm

Alarm Field	Description
Description	Originated by OVOC when an SNMP Timeout occurs for the first time in the Media Gateway.

Alarm Field	Description
SNMP Alarm	acEMSNodeConnectionLostAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.3
Alarm Title	GW Connection Alarm
Alarm Source	Media Gateway
Alarm Type	Communications Alarm
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 OVOC 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 OVOC

GW Mismatch Alarm

Alarm Field	Description
Description	Activated when OVOC detects a hardware, software, predefine or configuration mismatch. ■ Software Mismatch: Activated when OVOC 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.

Alarm Field	Description
	■ Hardware Mismatch: Activated when OVOC detects a hardware mismatch between the actual and the previous definition of a Media Gateway. ■ Configuration Mismatch: Activated when OVOC detects a configuration mismatch between the actual parameter values provisioned and previous parameter values provisioned.
SNMP Alarm	acEMSNoMismatchNodeAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.9
Alarm Title	GW Mismatch Alarm
Alarm Source	■ Media Gateway/Software ■ Media Gateway/Hardware ■ Media Gateway/Configuration
Alarm Type	Equipment Alarm
Probable Cause	Other
Severity	Clear
Additional Info	-

Corrective Action	■ Software Mismatch:
	
	  ✔ Define the detected version in the OVOC Software Manager
	
	  ✔ Perform a Software Upgrade on the gateway with one of the supported versions.
	
	■ Hardware Mismatch:
	
	  ✔ Perform remove / add a device in order to resync OVOC 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 OVOC configuration and actual MG configuration:
	
	    -MG configuration is incorrect: use configuration download to update MG with correct configuration saved in OVOC database.

Alarm Field	Description
	-MG is correct, OVOC is not updated: use configuration upload to save a correct MG configuration in OVOC database. ■ Check the Actions Journal for recent updates of the gateway.
Media Gateways	All the gateways managed by OVOC.

Configuration Mismatch

Alarm Field	Description
Description	This alarm is raised when there are missing or incorrect parameters values received from a managed entity.
SNMP Alarm	acEMSConfigurationMismatchNodeAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.7
Alarm Title	Configuration Mismatch
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Severity	Minor
Additional Info	-
Corrective Action	-

OVOC Server Started

Alarm Field	Description
Description	Event raised each time the OVOC server is started or restarted (warm boot/reboot) by the OVOC Watchdog Process.
SNMP OID	acEMSServerStartup- 1.3.6.1.4.1.5003.9.20.3.2.0.11

Alarm Field	Description
AlarmTitle	[Event] OVOC Server Started
AlarmSource	Management
Alarm Type	Communications Alarm
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	All the gateways managed by OVOC.

OVOC Disk Space Alarm

Alarm Field	Description
Description	The usage size (in %) on the disk partition of the #application type #application name is 'Dangerously High' or 'Almost Full'.
SNMP Alarm	acEMSNotEnoughDiskSpaceAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.12
AlarmTitle	Disk Space Alarm
AlarmType	Equipment Alarm
AlarmSource	OVOC Mgmt
Probable Cause	Storage Capacity Problem
Severity	■ More than 70% - minor ■ 80-90 – major ■ More than 90 - critical
Alarm Text	{0}% of the disk is used in data partition. Free some disk space to avoid system failure.

Alarm Field	Description
Additional Info	
Corrective Action	Free disk space

Software Replaced

Alarm Field	Description
Description	Originates when OVOC 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 OVOC). Software Replace old version : <old version> new version <new version>.
SNMP Alarm	acEMSSoftwareReplaceAlarm-
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.14
Alarm Title	[Event] Software Replaced
Alarm Source	OVOC Mgmt
Alarm Type	Communications Alarm
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 OVOC.

Hardware Replaced

Alarm Field	Description
Description	Originated when OVOC discovers a different gateway (according to the

Alarm Field	Description
	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 Alarm	acEMSHardwareReplaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.15
Alarm Title	[Event] Hardware Replaced
Alarm Type	Equipment Alarm
Alarm Source	Media Gateway
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000

HTTP/HTTPS Access Disabled

Alarm Field	Description
Description	Originated when HTTP access is disabled by OVOC hardening; however OVOC manages media gateways that require HTTP access for software upgrade. Originated on server startup.
SNMP Alarm	acEMSHTTPDisabled
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.16
Alarm Title	[Event] HTTP/HTTPS Access Disabled
Alarm Type	Environmental Alarm

Alarm Field	Description
Alarm Source	OVOC Mgmt
Probable Cause	Application Subsystem Failure
Severity	Major
Additional Info	-
Corrective Action	Separate the gateways between two OVOC servers (secured & unsecured)
Media Gateways	Gateways using the HTTP server for the software upgrade procedure: MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000

PM File Generated

Alarm Field	Description
Description	Originated when a PM file is generated in the OVOC server, and it can be retrieved by a higher level management system.
SNMP Alarm	acEMSPmFileGenerate
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.18
Alarm Title	[Event] PM File Generated
Alarm Source	OVOC Mgmt
Alarm Type	Other
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	-

Alarm Field	Description
Media Gateways	All Gateways

PM Polling Error

Alarm Field	Description
Description	Originated when a History PM stops collecting performance summary data from MG. Possible reasons are: NTP synchronization lost, Connection Loss, SW Mismatch, etc.
SNMP Alarm	acEMSPmHistoryAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.19
Alarm Title	[Event] PM Polling Error
Alarm Source	OVOC Mgmt
Alarm Type	Other
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 OVOC 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 OVOC 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.

Alarm Field	Description
Media Gate-ways	All Gateways

Cold Start Missed

Alarm Field	Description
Description	Originated when Carrier Grade Alarm System recognizes coldStart trap has been missed.
SNMP Alarm	acEMSNodeColdStartMissedEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.20
Alarm Title	[Event] Cold Start Missed
Alarm Source	-
Alarm Type	Other
Probable Cause	Receive failure
Severity	Clear
Additional Info	-
Corrective Action	-
Media Gateways	All the managed Gateways

GW Backup Event

Alarm Field	Description
Description	This alarm is raised when an AudioCodes device configuration file cannot be retrieved due to insufficient disk space or periodic backup operation failure.
SNMP Alarm	acEMSMGBackupEvent

Alarm Field	Description
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.21
Alarm Title	GW Backup Event
Alarm Source	<Device IP address>
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Severity	Condition	Text	Corrective Action
Minor	periodic backup failed due to insufficient disk space	Backup file from IP:{0} with MG name: {1} was not retrieved due to low OVOC Mgmt disk space.	Check disk and free some space.
Minor	periodic backupbackup failed	Periodic Backup operation failed for MG {0} with IP:{1}	
Indeterminate	periodic backup success	backup file: {file} from ip: {ip} with mg name: {name} was successfully retrieved.	

Security Alarm

Alarm Field	Description
Description	Activated when one or more RADIUS servers are not reachable. When none of the RADIUS servers can be reached, a Critical Severity alarm is generated.
SNMP Alarm	acEMSSecurityAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.23
Alarm Title	Security Alarm
Alarm Source	OVOC Mgmt/ Radius <#>

Alarm Field	Description
Alarm Type	Processing Error Alarm
Probable Cause	Other
Severity	Minor, Major, Critical
Additional Info	-
Corrective Action	-
Media Gate- ways	-

Security Event

Alarm Field	Description
Description	This event is generated when a specific user is blocked after reaching the maximum number of login attempts, or when the OVOC failed to sync OVOC and Mediant 5000 / 8000 users.
SNMP Alarm	acEMSSecurityEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.24
Alarm Title	[Event] Security Event
Alarm Source	OVOC Mgmt/ User Name, OVOC Mgmt/ User Sync
Alarm Type	Other
Probable Cause	Other
Severity	Indeterminate
Additional Info	-
Corrective Action	-

Alarm Field	Description
Media Gate-ways	-

Topology Update Event

Alarm Field	Description
Description	This event is issued by OVOC when a Gateway or Region is added/removed/updated in OVOC 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 Alarm	acEMSTopologyUpdateEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.25
Alarm Title	[Event] Topology Update
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Severity	Indeterminate
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 OVOC data base used for region identification) X2 = Region name as it defined by OVOC operator Y1 = GW ID (unique identifier in the OVOC data base used for GW identification) Y2 = GW Name as it defined by OVOC operator Y3 = GW IP as it defined by OVOC operator Y4 = GW Type as it identified by OVOC during the first connection to the

Alarm Field	Description
	gateway. 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 gateway has been success full. The following gateways 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 gateway-related. All the fields related to the gateway 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 Gate-ways	-

Topology File Event

Alarm Field	Description
Description	This event is issued by OVOC when the Topology File is updated on the OVOC 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 Northbound Integration Guide.
SNMP Name	acEMSTopologyFileEvent-
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.26

Alarm Field	Description
Alarm Title	[Event] Topology File
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Severity	Indeterminate
Additional Info	File Name: MGsTopologyList.csv
Corrective Action	-
Media Gate-ways	-

Synchronizing Alarms Event

Alarm Field	Description
Description	This event is issued when the OVOC 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 OVOC failed to retrieve is provided in the Additional Info field.
SNMP Alarm	acEMSSyncAlarmEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.27
Alarm Title	[Event] Synchronizing Alarms
Alarm Source	OVOC Mgmt
Alarm Type	Other
Severity	Indeterminate
Probable Cause	Other
Additional Info	Retrieved x missed alarms, failed to retrieve y alarms.

Alarm Field	Description
Corrective Action	-
Media Gateways	-

Synchronizing Active Alarms Event

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

OVOC License Key Alarm

Alarm Field	Description
Description	This alarm is raised when the OVOC License key has expired or the OVOC management license (License key) on the device is missing.

Alarm Field	Description
SNMP Alarm	acEMSLicenseKeyAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.29
Alarm Title	OVOC License Key Alarm
Alarm Source	OVOC Mgmt/license
Alarm Type	other
Probable Cause	keyexpired
Additional Info	In case the OVOC license expires: OVOC license key expiration date: <expiration date>
Corrective Action	In case the OVOC license expires: ■ Contact AudioCodes for new license In case of the missing license in device: ■ If required, contact AudioCodes for new license

Alarm Severity	Condition	Text	Corrective Action
Critical	expired	OVOC Mgmt Application License is expired	
Major	Month before	OVOC Mgmt Application License will be expired within one month	
Critical	Device not have OVOC management license	GW management is not covered by current OVOC Mgmt Application License	

Suppressed Alarm <Name>

Alarm Field	Description
Description	This alarm is sent when the OVOC 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

Alarm Field	Description
	OVOC Alarms Settings screen). When this alarm is sent, such alarms are not added to the OVOC database and are not forwarded to configured destinations.
SNMP Alarm	acEMSAlarmSuppression
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.42
Alarm Title	The name of the suppressed alarm
Alarm Source	OVOC Mgmt or OVOC QoE/<IP address_Managed Entity>
Alarm Text	Alarm Suppression activated
Alarm Type	Other
Probable Cause	Threshold crossed.
Severity	Indeterminate
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 OVOC database and forwarded to configured destinations.
Additional Info	-
Corrective Action	Investigate the recurrence of such alarms.

OVOC Keep Alive Alarm

Alarm Field	Description
Description	This alarm indicates that an SNMP Keep-alive trap has been sent from OVOC to a third-party destination such as a Syslog server to indicate OVOC liveness (configured in the OVOC Alarms Settings window).
SNMP Alarm	EMSKeepAliveAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.45
Alarm Title	OVOC Keep Alive Alarm

Alarm Field	Description
Alarm Source	OVOC Mgmt
Alarm Text	Management Keep-Alive
Default Severity	Indeterminate
Alarm Type	Other
Probable Cause	Other
Corrective Action	-

Pre-provisioning Alarm

Alarm Field	Description
Description	This alarm is generated when the operation for pre-provisioning the device upon initial connection to OVOC fails.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.46
AlarmTitle	Pre-Provisioning
AlarmSource	OVOC Mgmt
AlarmType	operational/Violation
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 OVOC. Instead download these files to the device using the Software Manager and then use the 'Software Upgrade' action. OR

Alarm Field	Description
	■ Remove the device from OVOC and then reconnect it i.e. repeat the pre-provisioning process.
Media Gate-ways	All gateways managed by OVOC.

Endpoint Publish Alarm

Alarm Field	Description
Description	This alarm is raised when problems arise with the SIP Publish reporting for voice quality metrics (port 5060) from endpoints (RFC 6035). ■ When a SIP Publish message is missing mandatory parameter/s required by OVOC to handle this message. ■ When SIP Publish message time is not synchronized with OVOC server.
SNMP Alarm	acEndpointPublishAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.47
Alarm Title	Endpoint Publish Alarm
Alarm Source	OVOC_QoE/<Endpoint IP>
Alarm Type	Communications alarm
Alarm Text	Bad Publish Message. Device IP: {ip}, Device MAC: {mac}.
Probable Cause	Communications protocol error
Additional Info	Possible reasons: Mandatory Field/s Missing. Endpoint Server and Device Synchronization Error.
Severity	Minor

Disk Space Alarm

Alarm Fields	Description
Description	This alarm is issued in one of the following cases:

Alarm Fields	Description
	■ 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
AlarmSource	OVOC Mgmt
AlarmType	Equipment Alarm
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 Gate-ways	-

Oracle Disk Space Alarm

Alarm Field	Description
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

Alarm Field	Description
AlarmSource	OVOC Mgmt
AlarmType	Equipment Alarm
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 Gate-ways	-

License Alarm

Alarm Field	Description
Description	This alarm is issued when the OVOC License approaches or reaches it's expiration date or OVOC 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
Alarm Title	License Alarm
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Additional Info	Info1: ■ Machine ID In The License Is {0} ■ Expiration Date In The License Is {0}

Alarm Field	Description		
Alarm Severity	Condition	<text>	Corrective Action
Critical	The license expiration date is less than equal to 7 days.	■ OVOCLicense is about to expire in {0} days. ■ OVOC License is about to expire in 1 day. ■ OVOC License Will Expire Today	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.
Major	The license expiration date is more than 7 days and less than equal to 30 days.	OVOC License is about to expire in {0} days.	
Clear	The license expiration date is greater than 30 days.		

Synchronizing Alarms

Alarm Field	Description
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 Alarm	ac OCReSyncEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.58
Alarm Title	[Event] Synchronizing Alarms
Alarm Source	OVOC Mgmt
Alarm Type	Other

Alarm Field	Description
Severity	Indeterminate
Probable Cause	Other
Additional Info	-
Corrective Action	-
Media Gateways	-

QoE Sip Message Status Alarm

Alarm Field	Description
Description	Alarm is raised when device notify OVOC that it stop sending SIP messages. cleared when it notify that it continue sending SIP messages
SNMP Alarm	acSEMSipMessageStatusAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.60
AlarmTitle	QoE: Sip Message Status Alarm
AlarmType	OVOC QOE/<device name>
AlarmSource	Communications Alarm
Probable Cause	Communications Subsystem Failure
Severity	Critical
Alarm Text	Device Stopped Sending Sip Ladder Messages
Additional Info	
Corrective Action	

Floating License Extended

Alarm Field	Description
Description	This alarm is raised when IP phones are added to OVOC and as a result licenses are extended beyond the pre-existing tenant allocation; where there are insufficient licenses currently allocated to the phone's designated tenant. In this case, OVOC checks the number of free available licenses (licensees that are not assigned to any tenant) and then takes 5% of the current tenant allocation (a minimum of five, or the remaining licenses) and dynamically adds them to the phone's tenant. The licenses are taken from the OVOC License "Managed Endpoints" feature license if the endpoint is managed by IP Phone Manager Pro or from the "Voice Quality Endpoints" feature if the phones are managed in the OVOC for Voice Quality ("QOE Supported" in OVOC Web). If both of these license features are managed for the endpoint, the license is taken according to the license availability for the respective tenant license allocation. For example, if the endpoint is licensed for both of these categories and there also insufficient licenses allocated for both categories, then the dynamic license allocation is separately executed and therefore separate events are raised.
SNMP Alarm	floatingLicenseExtended
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.61
Alarm Title	Floating License Extended
Alarm Source	The tenant on which the license is extended.
Alarm Type	Other
Severity	Indeterminate (info)
Probable Cause	Other

Floating License Device Report Alarm

Alarm Field	Details
Description	This alarm is raised when the device does not send a usage report for [calc duration] minutes or more to OVOC.
SNMP Alarm	acClmDeviceReportAlarm

Alarm Field	Details
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.62
Alarm Title	Floating license Device missing report
Alarm Source	Floating license/Device#[Device Id]
Alarm Type	Communication
Severity	Major
Probable Cause	Other

Floating License Register Successful Event

Alarm Field	Description
Description	This alarm is raised when OVOC successfully registers to Floating License at [DNS address].
SNMP Alarm	acClmRegisterSuccessfulEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.63
Alarm Title	Floating license Cloud Service registration successful
Alarm Source	Floating license
Alarm Type	Communication
Severity	Info
Probable Cause	Other

Floating License Register Failure Alarm

Alarm Field	Description
Description	This alarm is raised when OVOC fails to register to Floating License Cloud Service at [DNS address], Reason: [Error description or timeout]
SNMP Alarm	acClmRegisterFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.64

Alarm Field	Description
Alarm Title	Fail to register to Cloud Service
Alarm Source	Floating license
Alarm Type	Communication
Severity	Critical
Probable Cause	Communications Protocol Error

Floating License Failure to Send Usage Report Alarm

Alarm Field	Description
Description	This alarm is raised when OVOC fails in two attempts to send usage report to Floating LIcense Cloud Service Service. This service shuts down if the problem not fixed by the configured period (default 90 days). Note: this time period is configured by AudioCodes on the Floating License Service.
SNMP Alarm	acClmFailToSendUsageReportAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.65
Alarm Title	Failed to send usage report to Cloud Service
Alarm Source	Floating license
Alarm Type	Communication
Severity	Major
Probable Cause	Communications Protocol Error

Floating License Failure to Send Extended Usage Report Alarm

Alarm Field	Description
Description	This alarm is raised when OVOC fails to send usage reports to the Floating License Cloud Service . This alarm is raised one week prior to the shutdown date (default 90 days). Note: this time period is configured by AudioCodes on the Floating

Alarm Field	Description
	License Service.
SNMP Alarm	acClmFailToSendUsageReportExtendedAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.66
Alarm Title	Failed to send usage report to Floating License Cloud Service
Alarm Source	Floating license
Alarm Type	Communication
Alarm Text	OVOC failed to send usage report to Floating License Cloud Service. Service will shutdown if problem not fixed by 90 days
Severity	Critical
Probable Cause	Communications Protocol Error

Floating License Service Shutdown Alarm

Alarm Field	Description
Description	Floating License service shutdown, reason: failure to communicate with cloud service for [(ovocNoResponseHours-144) *60/ ovocReportIntervalMin] minutes.
SNMP Alarm	acClmServiceShutdownAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.67
Alarm Title	Service Shutdown
Alarm Source	Floating license
Alarm Type	Communication
Severity	Critical
Probable Cause	Application Subsystem Failure

Floating License Manage Devices above Allow Maximum

Alarm Field	Description
Description	This alarm is raised when the maximum number of devices managed by the floating license is reduced to less than the currently registered count (the number of devices that have registered to OVOC and the Floating License service and are currently managed by the floating license). For example, if there are 30 devices registered and are currently managed by the floating license in OVOC, and then the maximum number of devices supported by the license is reduced to 20 devices, then this alarm will be raised.
SNMP Alarm	acClmMaxDeviceMismatchEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.68
Alarm Title	Floating license Manage devices above allow maximum
Alarm Source	Floating license
Alarm Type	Other
Alarm Severity	Info
Probable Cause	Other
Additional Info	-
Corrective Action	-

Floating License Registered Devices Requests Capacity

Alarm Field	Description
Description	This alarm is raised when there is an attempt to register a device for floating license management that is above the OVOC maximum floating license capacity.
SNMP Alarm	acClmMaxDeviceCapacityAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.69

Alarm Field	Description
Alarm Title	Floating license registered devices requests capacity.
Alarm Source	Floating license
Alarm Type	Other
Alarm Severity	Critical
Probable Cause	Other
Additional Info	-
Corrective Action	-

Alarms Overflow

Alarm Field	Description
Description	This alarm is raised when one of the alarm processing queues reached their threshold which prevented the receiving of new alarms.
SNMP Alarm	acAlarmsOverflow
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.71
Alarm Title	Alarms Overflow
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Threshold Crossed
Severity	Major
Additional Info	-
Corrective Action	-

Alarms Forward Overflow

Alarm Field	Description
Description	This alarm is raised when one of the alarms forwarding processing queues reached their threshold prevented the forwarding of new alarms
SNMP Alarm	acAlarmsFwOverflow
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.72
Alarm Title	Alarms Forward Overflow
Alarm Source	OVOC Mgmt
Alarm Type	Other
Severity	Major
Probable Cause	Threshold Crossed
Additional Info	-
Corrective Action	-

FQDN Resolve Event

Alarm Field	Description
Description	This alarm is raised when the FQDN for logging into the device cannot be resolved.
SNMP Alarm	acEMSFQDNResolveEvent
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.73
Alarm Title	FQDN Resolve Event
Alarm Source	Device IP
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
Additional Info	- 38 -		
Corrective Action	Check if another device with the same IP already exists in OVOC (same as the resolved configured FQDN).		

Alarm Severity	Condition	Text	Corrective Action
Major		FQDN : <fqdn> resolved to IP: <IP> . IP address already exist . IP address for node name <name> changed to empty value	
Major		FQDN : <fqdn> resolved to IP: <IP> . IP address for node name <name> changed to <IP>	

PM Timeout Event

Alarm Field	Description		
Description	This system event is raised when the polling interval has expired and not all of the parameters that were defined in the assigned PM profile were yet polled.		
SNMP Alarm	acPmTimeOutEvent		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.74		
Alarm Source	OVOC Mgmt/ PM Handler		
Alarm Title	PM Timeout Event		
Alarm Type	Other		
Probable Cause	Other		

Event Severity	Condition	<text>	Corrective Action

Alarm Field	Description		
Critical	The polling interval has expired and not all of the parameters that were defined in the PM profile were yet polled.	Message: PM Timeout ; startTime= 12:00 ; endTime= 12:15 ; currentTime= 12:14:30 ; timeout= 30 sec before endTime	Check network performance.
Cleared	-	-	

PM Token Pool is Empty

Alarm Field	Description		
Description	This system event is raised when the number of parameters polled for the current interval has reached its maximum capacity.		
SNMP Alarm	acPMTokenPooisEmpty		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.75		
Alarm Source	OVOC Mgmt/ PM Token Pool Handler		
Alarm Title	PM Token Pool is Empty-Event		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	The number of parameters polled for this interval has reached its maximum capacity.	Message: 500,000 tokens have already been used, no more DB transactions is allowed on this pm iteration.	Check the number of parameters and devices configured in the PM Profile and reduce the load accordingly.

PM Polling Status Event

Alarm Details	Description
Description	This event is raised per managed polled entity under the following

Alarm Details	Description
	circumstances:
	■ When a specific device is successfully polled.
	■ For the failure scenarios described below.
	⚠ This event is sent only when the 'Send Event per Interval' parameter is enabled in the Performance Monitoring profile.
SNMP Alarm	acDevicePmPollingEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.76
Alarm Title	PM Polling Status Event
Alarm Source	OVOC Mgmt/ PM Handle
Alarm Type	Other
Probable Cause	Other

Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	Raised when the device is successfully polled.	Success: PM polling operation was successfully finished. deviceName=Device Name ; deviceIp= 1.1.1.1 ; pollingTimeStamp= 12:15	-
Major	The time format for the device's system clock is in a different format to the time settings for the OVOC server clock.	Device time has not valid format	Synchronize the time settings.
	Device connection timeout	Device timeout	Troubleshoot the device connection.
	Device configuration is	Device is not Sync	Download updated configuration to

Alarm Details	Description		
	not synchronized		the device.
	Device is polled when the token pool did not have sufficient allocations.	Token pool has not enough allocations	Analyze the polling load.
	The device does not have a valid MIB version.	Device has not valid MIB version	Verify the device's MIB version.
	The device's MIB version is not supported for the PM parameter.	Device's MIB version is not supporting PM, current version= v7.0	Refer to the Performance Monitoring Guide for the supported MIB version for the PM parameter.
	The OVOC server Performance Monitoring SNMP process used to manage the connection with the managed device has failed.	Device has no SNMP connection with OVOC.	Check the SNMP connection between the device and the OVOC server.
	A PM profile has not been assigned to the device.	Device is not attached to any PM profile.	Assign a PM profile to the device.
	The Token pool does not have sufficient allocations.	Token pool has not enough allocations	Check the number of parameters and devices configured in the PM Profile and reduce the load accordingly.
	The device was	Device was restarted less	Wait at least 15

Alarm Details	Description		
	restarted less than 15 minutes ago.	than 15 minutes ago	minutes for the polling operation to recommence.
	The last polling reason type was unknown.	Unknown LastPollingFailReasonType failure	-
Cleared	-	-	-

PM Batch Overflow Alarm

Alarm Field	Description		
Description	This system alarm is raised when the database buffer for the polled interval has reached its maximum capacity.		
SNMP Alarm	acPmBatchOverFlowAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.77		
Alarm Source	OVOC Mgmt/ PM Batch Handler		
Alarm Title	PM Batch OverFlow Alarm		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	The PM batch handler buffer has reached maximum capacity.	PM's batch handler reached his max buffer capacity= 15000, while his current size= 15000. Polling operation will be stopped until the buffer will be cleared.	-.
Cleared	-	-	

PM Has No SNMP Connection

Alarm Field	Description
Description	This system event is raised when the internal SNMP process for managing the polling operation fails.
SNMP Alarm	acPmHasNoSnmpConnection
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.78
Alarm Source	OVOC Mgmt/ PM Token Pool Handler
Alarm Title	PM Has No SNMP Connection
Alarm Type	Other
Probable Cause	Other

Alarm Severity	Condition	<text>	Corrective Action
Critical	The internal SNMP process for managing the polling operation has failed.	PM process has no SNMP connection to the Main SNMP service ; startTime= 12:00 ; endTime= 12:15 ; currentTime= 12:01	-
Cleared	-	-	

FlexPool License Usage

Alarm Field	Description
Description	This alarm is raised when a FlexPool License parameter is approaching or has reached its maximum value.
SNMP Alarm	acFlexPoolLicenseUsage
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.85
Alarm Title	FlexPool license parameter license usage
Alarm Source	FlexPool/[license parameter name]
Alarm Type	Other

Alarm Field	Description		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Critical	FlexPool license parameter has exceeded its maximum value.	FlexPool license parameter [name] is over license limit.	Renew floating license or reduce current consumption.
Minor	FlexPool license parameter is approaching its maximum value according to the setting for the Flex Pool OVOC Web Configuration parameter "Alarm Threshold Percentage" (default 85%).	FlexPool license parameter [name] is approaching maximum utilization.	Renew floating license or reduce current consumption.

4   Voice Quality Package Alarms

OVOC QoE - Failed Calls Alarm

Alarm Field	Description
Description	This alarm is raised when the % number of failed calls for the managed node or link crosses the threshold 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. The threshold for this alarm is set in the QoE Status and Alarms Details window.
SNMP OID	acVoice QualityRuleFailedCallsAlarm
SNMP Alarm	1.3.6.1.4.1.5003.9.20.3.2.0.30
Alarm Title	Voice Quality - Failed Calls Alarm
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint
Alarm Type	Quality of service alarm.
Probable Cause	The minimum or maximum threshold is crossed.
Additional Info	Critical or Major severity threshold is Y%: ■ Critical Threshold: 10 % of calls (default) ■ Major Threshold: 2 % of calls (default) Where Y% is the % failed calls per managed node or link that is measured for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:30) and then at 15:30 (from 12:30 to 15:30) and so on.

Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when Y % of calls (rep-resenting the con-figured critical	Y% of failed calls has crossed the "Critical"	Investigate the source (device or link) of the failed

Alarm Field	Description		
	threshold) made by the managed node or link for the sampled period fail (see above).	threshold	calls.
Major	This alarm is raised when Y % of calls (representing the configured major threshold) made by the managed node or link for the sampled period fail (see above).	Y% number of failed calls for has crossed the "Major" threshold.	
Clear	Cleared when the failed calls ratio returns below the threshold value for the sampled period.		-

OVOC QoE – Poor Voice Quality Alarm

Alarm Field	Description
Description	This alarm is raised when the % number of poor quality calls polled for the managed node or link crosses the threshold 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. The threshold for this alarm is set in the QoE Status and Alarms Details window.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.31
SNMP Alarm	acVoiceQualityRulePoorQualityCallsAlarm
Alarm Title	Voice Quality – Voice Quality Alarm
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint
Alarm Type	Quality of service alarm
Probable Cause	The minimum or maximum threshold is crossed.

Alarm Field	Description
Additional Info	Critical or Major severity threshold is Y%: ◼ Critical Threshold: 10% of calls (default). ◼ Major Threshold: 2% of calls (default) Where Y% is the % poor quality calls per managed node or link that is measured for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (from 12:30 to 15:30) and so on.

Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when Y% (representing the configured critical threshold) of calls made by the managed node or link for the sampled period (see above) are of poor quality.	Y% calls have crossed the "Critical" threshold.	Investigate the source (device or link) of the poor quality calls.
Major	This alarm is raised when Y % (representing the configured major threshold) of calls by the managed node or link for the sampled period (see above) are of poor quality.	Y% calls have crossed the "Major" threshold.	
Clear	Cleared when the poor quality calls ratio returns below the threshold value for the sampled period (see above).		-

OVOC QoE - Average Call Duration Alarm

Alarm Field	Description
Description	This alarm is raised when the average call duration time threshold for the managed node or link 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 Y sec. The threshold for this alarm is set in the QoE Status and Alarms Details window.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.32
SNMP Alarm	acVoice QualityRuleAvrgCallDurationAlarm
Alarm Title	Voice Quality – Average Call Duration Alarm
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint
Alarm Type	Quality of service alarm
Probable Cause	The minimum or maximum threshold is crossed.
Additional Info	■ Critical Threshold: average call duration of 3 seconds (default). ■ Major Threshold: average call duration of 5 seconds (default) Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (for 12:30-15:30) and so on.

Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the average call duration for the managed node or link for the sampled period (see above) falls to the configured critical	Average Call Duration "Critical" threshold has been reached.	Investigate the source (device or link) reporting the excessive average call

Alarm Field	Description		
	threshold value.		duration.
Major	This alarm is raised when the average call duration for the managed node or link for the sampled period (see above) falls to the configured major threshold value.	Average Call Duration "Major" threshold has been reached.	
Clear	Cleared when the average call duration returns below the threshold value for the sampled period (see above)		-

OVOC QoE - License Key Alarm

Alarm Field	Description
Description	This alarm is sent in the following circumstances: ■ When the number of devices connected to the OVOC approaches or reaches license capacity (shown as 'Devices Number' in OVOC server Manager License screen). ■ When the number of sessions running on the OVOC approaches or reaches license capacity (shown as 'Voice Quality Sessions' in the OVOC 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
Alarms Source	OVOC QoE
Alarm Type	Other
Probable Cause	Key Expired

Alarm Field	Description
Additional Info	
Corrective Action	Contact your AudioCodes representitve to obtain the required license key.

Alarm Severity	Condition	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.	-

OVOC QoE - System Load Alarm

Alarm Field	Description
Description	This alarm is sent when the Voice Quality system capacity is high and the system consequently becomes overloaded. Three levels are supported: ■ Major -> Events are not stored. Trend Info will not be displayed. ■ Critical -> Green calls are not stored. ■ Minor - > Events are not stored for green calls. Trend Info will not be

Alarm Field	Description
	displayed.
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	OVOC QoE
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.

Call Details Storage Level Change

Alarm Field	Description
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	OVOC QoE
Alarm Type	Quality of service alarm
Probable Cause	Threshold crossed

Alarm Field	Description
Severity	Indeterminate
Additional Info	-
Corrective Action	-

Call Quality Monitoring Connection Status Alarm

Alarm Field	Description
Description	This alarm is sent when connectivity is lost between the managed device and Voice Quality Package server.
SNMP Alarm	acSEMConnectionStatusAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.36
Alarm Title	Voice Quality – OVOC QoE - Connection Status Alarm
Alarm Source	OVOC QoE/Device
Alarm Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Additional Info	One of the following reasons will appear: ■ Server Time: {0}, Device Time: {1}. ■ Please check your NTP Configuration in Device. ■ NTP Servers are not configured in the Device. ■ Please make sure that time in OVOC QoE Server and Device is properly synchronized. ■ NTP configuration is correct, please check your network conditions (Firewalls, Ports, etc .) and make sure that NTP sync of OVOC QoE Server and/or Devices is performed correctly. ■ You have complex network configuration in OVOC Mgmt/OVOC QoE server. Please refer to OVOC Mgmt client / Help menu / OVOC Mgmt Configuration frame to verify network configuration.

Alarm	Condition	Text	CorrectiveAction

Alarm Field	Description		
Severity			
Critical	Insufficient memory buffer.	There isn't enough buffer size to allocate for main messages queue of this board.	The OVOC server has reached its maximum management capacity. Contact AudioCodes Customer Support.
	Connection loss between OVOC and the device.	OVOC QoE connection lost.	Check your network configuration on both the device and OVOC server.
Clear	Server and Device are not synchronized.	Server Time: {0}, Device Time: {1}.	Check your NTP Configuration in device.
	Connection is established between the device and OVOC.	OVOC QoE connection established. Server and Device are now Synchronized.	-
	Synchronization between server and device.	Server and Device are now Synchronized.	-

OVOC QoE - Skype for Business SQL Server Connection Lost Alarm

Alarm Field	Description
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	OVOC QoE/Device
Alarm Type	Communications alarm

Alarm Field	Description
Probable Cause	Communications sub-system failure
Severity	Critical
Additional Info	-
Corrective Action	Check the Lync SQL server for problems.

OVOC QoE - Active Directory Server Connection Lost Alarm

Alarm Field	Description
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	OVOC QoE/Active Directory
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.

OVOC QoE - Media Bandwidth Alarm

Alarm Field	Description
Description	This alarm is sent when the media bandwidth for the node

Alarm Field	Description
	or link falls below or exceeds the threshold values configured in the QoE Status and Alarms Details window.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.43
SNMP Alarm	acVoice QualityRuleBandwidthAlarm
Alarm Title	Voice Quality Rule Bandwidth Alarm
Alarm Source	VOC QoE/Device/Link/Site/Endpoint
Alarm Type	Quality of service alarm
Probable Cause	Threshold crossed
Additional Info	■ Critical Threshold: 10 Kb/ sec (default). ■ Major Threshold: 5 Kb/ sec (default) Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min" For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (for 12:30-15:30) and so on.

Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the maximum bandwidth for the sampled period (see above) reaches the configured critical threshold value.	Maximum Bandwidth of X Kb/sec	Check the node's or link's maximum bandwidth capacity matches the required capacity.
Major	This alarm is raised when the maximum bandwidth for the sampled period (see above) reaches the configured major threshold value.	Maximum Bandwidth of X Kb/sec	

Alarm Field	Description		
Clear	Cleared when the maximum bandwidth for the sampled period increases above the configured thresholds for the sampled period (see above).		-

OVOC QoE - Rule Max Concurrent Calls Alarm

Alarm Field	Description		
Description	This alarm is sent when the maximum concurrent calls for the node or link falls below or exceeds the threshold values configured in QoE Status and Alarms Details window.		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.44		
SNMP Alarm	acVoice QualityRuleMaxConcurrentCallsAlarm		
Alarm Title	Rule Max Concurrent Calls Alarm		
Alarm Source	OVOC QoE/Node/Link/Site/Endpoint		
Alarm Type	Quality of service alarm		
Probable Cause	Threshold crossed		
Additional Info	■ Critical Threshold: 10 Calls (default). ■ Major Threshold: 5 Calls (default) Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (from 12:30 to 15:30) and so on.		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the number of	Max Concurrent Calls of	Check that the node's or link's

Alarm Field	Description		
	concurrent calls reaches the configured critical threshold for the sampled period (see above).	X	maximum number of concurrent calls matches the required capacity.
Major	This alarm is raised when the number of concurrent calls reaches the configured major threshold for the sampled period (see above)..	Max Concurrent Calls of X	
Clear	This alarm is raised when the number of concurrent calls falls within the configured threshold for the sampled period (see above).		-

Report Schedulers Time Event

Alarm Field	Description
Description	This event is raised when the Reports Scheduler misses a scheduled execution time.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.82
SNMP Alarm	acReportSchedulersTimeEvent
Alarm Title	Report Schedulers Time Event
Alarm Source	OVOC QoE/Report Scheduler
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Major	The scheduler misses the execution time.	Example : Scheduler ZAdmin_pre-defined Has Missed his Execution Time, Schedulers Next Run: 2019-12-22 05:00:00.0, While Current Time: Sun Dec 22 05:00:20 GMT 2019	-

Report Schedulers Load Alarm

Alarm Field	Description		
Description	This alarm is raised when the Report Scheduler's buffer reaches maximum it's capacity.		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.83		
SNMP Alarm	acReportSchedulersLoadAlarm		
Alarm Title	Report Schedulers Load Alarm		
Alarm Source	OVOC QoE/Report Scheduler		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
CRITICAL	Schedulers Execution Queue has reached maximum buffer capacity.	Schedulers Queue Has Reached His Max Buffer Capacity= <buffersize>, New Schedulers Will Not Be Executed	Reduce the number of scheduled reports.
MAJOR	Schedulers Execution Queue has reached 80% of its maximum buffer capacity.	Schedulers Queue Has Reached 80% Of His Max Buffer Capacity=<buffersize> , His Current Queue Size=<buffersize>	

Report Schedulers Execution Event

Alarm Field	Description
Description	This event is raised when the execution of the report that is attached to the Scheduler fails.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.84
SNMP Alarm	acReportSchedulersExecutionEvent
Alarm Title	Report Schedulers Execution Event
Alarm Source	OVOC QoE/Report Scheduler
Alarm Type	Other
Probable Cause	Other

Alarm Severity	Condition	Text	Corrective Action
Critical	Execution of report which is attached to the scheduler fails.	**Example:** SchedulerExecuter: Calculation of report result has been failed ; schedulerName=Test_Topology_Trend ; reportName=TestTrend_Report ; executionTime=Wed Dec 11 06:46:00 GMT 2019 ; actualRunTime=Wed Dec 11 06:46:00 GMT 2019	-

5   Device Manager Alarms

Registration Failure Alarm

Alarm Field	Description
Description	This alarm is raised when a SIP registration (with a PBX) for the IP Phone fails.
SNMP Alarm	IPPhoneRegisterFailure
SNMP 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, however 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.

IP Phone Survivable Mode Start Alarm

Alarm Fields	Description
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 Fields	Description
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.

IP Phone Lync Login Failure Alarm

Alarm Field	Description
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.

Endpoint License Alarm

Table 5-1:   Endpoint License Alarm

Alarm Field	Description		
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 OVOC Server Manager License screen) approaches or reaches its license capacity. ■ When the number of managed endpoints currently running on the OVOC server (shown in the License screen 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**	**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	Clear - Clearing	-

Alarm Field	Description	
	alarm	currently active alarm.	

Endpoint Server Overloaded Alarm

Alarm Field	Description
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
Corrective Action	Reduce the endpoint traffic load on the OVOC server.

IP Phone Speaker Firmware Download Failure

Alarm Field	Details
Description	This alarm is raised when the phone fails to download the HRS 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 Field	Details
Alarm Source	The server from which the download was attempted: OVOC, WEB, HTTP, FTP
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Major, Clear
Additional Info	-
Corrective Action	■ Ensure that the HRS speaker is connected to the Device Manager. ■ Ensure that the compatible firmware file is loaded to the Device Manager.

IP Phone Speaker Firmware Upgrade Failure

Alarm Field	Description
Description	This alarm is raised when the phone fails to load the firmware to the HRS 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	Major, Clear
Additional Info	-
Corrective Action	■ Verify the USB connection between the phone and the HRS speaker. ■ Verify the firmware file is compatible with the HRS speaker.

IP Phone Conference Speaker Connection Failure

Alarm Field	Description
Description	This alarm is raised when there is failure for the USB connection between the phone and the HRS 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	Critical, Clear
Additional Info	-
Corrective Action	Check the USB connection between the HRS speaker and the phone.

IP Phone General Local Event

Table 5-2:   IPPhone General Local Event

Alarm Field	Description
Description	This alarm provides information regarding 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)

Alarm Field	Description
Probable Cause	Other(0)
Severity	Major
Additional Info	A 4-digit code that is used for support diagnostics.
Corrective Action	This alarm is for developer purposes only for additional troubleshooting of other alarms that are raised by the phone as described in this section.

IP Phone Web Successive Login Failure

Table 5-3:   IP Phone Web Successive Login Failure

Alarm Field	Description		
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	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.

Alarm Field	Description		
		■ 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.	-	-

IP Phone Requires Reset

Alarm Field	Description
Description	This alarm is send to advise the user to restart the phone, in the event where there is new Jabra HRS Speaker firmware available forupgrade and the HRS user choses not to upgrade firmware when prompted.
SNMP Alarm	IPPhoneRequiresReset
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.70
Alarm Title	IP Phone Requires Reset
Alarm Text	IPPhone requires reset
Alarm Source	The IP Phone
Alarm Type	EquipmentAlarm(4)
Probable Cause	ConfigurationOrCustomizationError(7)
Severity	Major(4)
Additional Info	HRS IP Phone enters to limited mode and speaker is not available. To solve it, the phone has to be restarted.
Corrective Action	■ If the user chooses to upgrade, at the end of the process ,the phone is automatically restarted and the firmware is upgraded. If successful, the speaker becomes available. ■ If the user chooses not to upgrade, the phone enters into limited

Alarm Field	Description
	services mode where the HRS speaker does not function as a Jabra device.

Jabra Firmware Upgrade Failed

Alarm Field	Description		
Description	This alarm is raised when the upgrade on the Jabra device (non-HRS device) fails.		
SNMP Alarm	JabraFirmwareUpgradeFailed		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.79		
Alarm Source	Jabra Integration Service		
Alarm Title	Jabra Firmware Upgrade Failed		
Alarm Type	Communications Alarm		
Probable Cause	Communications Protocol Error		
Alarm Severity	Condition	<text>	Corrective Action
Major	-	Jabra Firmware Upgrade Failed	Verify that the firmware file that was attempted to download is a compatible with the Jabra device.
Cleared	-	-	

VIP Endpoint is Not Registered or Offline

Alarm Field	Description
Description	This alarm is raised when the VIP endpoint is not registered or is offline. For example, the password for a VIP device in a conference room has expired.
SNMP Alarm	endpointVipUnregistered

Alarm Field	Description		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.80		
Alarm Title	VIP Endpoint is Not Registered / Offline		
Alarm Source	OVOC Mgmt		
Alarm Type	Operational Violation		
Probable Cause	Authentication Failure		
Alarm Severity	Condition	\<text\>	Corrective Action
Critical	The VIP endpoint is not registered with the IP-PBX. For example, Skype for Business.	VIP endpoint is in Unregistered/Offline	Re-register the endpoint.
Clear	The VIP endpoint has re-registered with the IP-PBX.	VIP endpoint registered	

VIP Endpoint is Disconnected

Alarm Field	Description		
Description	This alarm is raised when a VIP endpoint is disconnected.		
SNMP Alarm	endpointVipDisconnected		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.81		
Alarm Source	OVOC Mgmt		
Alarm Title	VIP Endpoint is Disconnected		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Alarm Severity	Condition	\<text\>	Corrective Action
Critical	The VIP endpoint has been disconnected with the OVOC	VIP Endpoint disconnected	Troubleshoot the VIP endpoint

Alarm Field	Description		
	server.		communication.
Clear	The VIP endpoint connection with the OVOC server has been restored.	VIP Endpoint connected	

6   OVOC Managed Devices Alarms

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 Alarms are supported by all AudioCodes devices.
Specific Hardware Alarms	■ Mediant 2600 E-SBC ■ Mediant 4000 SBC ■ Mediant 1000 ■ MP-1288
Temperature Alarm on page 128	■ Mediant 1000 ■ Mediant 2600 ■ Mediant 4000
Fan Tray Alarm on page 129	■ MP-1288 ■ Mediant 1000 ■ Mediant 2600 ■ Mediant 4000
Power Supply Alarm on page 130	■ 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

Alarm Type	Supported Device Types
	■ 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 on page 132	As above
HA System Configuration Mismatch Alarm on page 137	As above
HA System Switch Over Alarm on page 138	As above
Hitless Software Upgrade Alarm on page 138	■ Mediant 2600 E-SBC ■ Mediant 4000 SBC ■ Mediant SE SBC ■ Mediant VE SBC
Redundant Board Alarm on page 139	As above
HA Network Watchdog Status Alarm on page 140	As above
HA Network Watchdog Status Alarm on page 140	As above (except Mediant 3000)
Cluster HA Alarm on page 154	■ Media Transcoding Cluster feature (Mediant 9000 SBC and Mediant VE SBC)
HA Network	■ Mediant VE SBC on AWS

Alarm Type	Supported Device Types
Mismatch Alarm on page 142	■ Mediant SE SBC on AWS
HA Network Monitor Alarm on page 143	As above
HA Ethernet Group Alarm on page 144	As above (except Mediant 3000)
License Pool Alarms	Supported by all devices from Version 7.0, except for the Mediant 2000 and Mediant 3000. In addition, the Transcoding session license is applicable only to the Mediant Virtual Edition and Mediant 9000.
License Pool Infra Alarm on page 144	As above
License Pool Application Alarm on page 146	As above
License Pool Over Allocation Alarm on page 147	As above
Floating License Alarms	Refer to the OVOC Release Notes for device support information.
Cloud License Manager Alarm on page 149	Supported for the Floating License "Cloud" mode.
Floating License Alarm - Not Enough Memory to Allocate 'Custom' Profile on page 148	Supported for the Floating License "Cloud" mode.
Flex License Manager Alarm on page 152	Supported for the Floating License "FlexPool" mode.
Mediant 2600 E-SBCand Mediant 4000 Alarms SBC	
DSP Farms Mismatch	■ Mediant 2600 E-SBC

Alarm Type	Supported Device Types
Alarm on page 153	■ Mediant 4000 SBC
Mediant 9000 and Software SBC Alarms	■ Mediant 9000 SBC ■ Mediant VE SBC ■ Mediant SE SBC ■ Mediant CE SBC
Media Transcoder Network Failure on page 155	■ Media Transcoding Cluster feature (Mediant VE SBC and Mediant 9000 SBC) ■ Elastic Media Cluster feature (Mediant CE SBC)
Media Transcoder Software Upgrade Failure on page 156	■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC) ■ Elastic Media Cluster feature (Mediant CE SBC)
Media Transcoder High Temperature Failure on page 157	■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)
Media Transcoder Fan Tray Module Failure on page 158	■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)
Media Transcoder Power Supply Module Failure on page 159	■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)
Cluster Bandwidth Utilization Alarm on page 159	■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC) ■ Elastic Media Cluster feature (Mediant CE SBC)
Media Cluster Alarm on page 161	■ Elastic Media Cluster feature (Mediant CE SBC)
Remote Interface Alarm on page 162	■ Elastic Media Cluster feature (Mediant CE SBC)
AWS Security Role Alarm on page 163	■ Mediant VE SBC and Mediant CE SBC
CDR Server Alarm on page 164	■ As above

Alarm Type	Supported Device Types
Metering Alarm on page 165	■ Mediant VE when deployed through the AWS Marketplace
MP-1288 Alarms	■ MP-1288 (not supported by the OVOC License Pool Manager)
Module Service Alarm on page 166	As above
Module Operation Alarm on page 167	As above
Port Service Alarm on page 168	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])' Mediant 500Li MSBR
WAN Link Alarm on page 170	As above
Power Over Ethernet Status [Event] on page 170	Mediant 800 MSBR
Wireless Cellular Modem Alarm on page 171	■ Mediant 500 MSBR ■ Mediant 500L MSBR ■ Mediant 800 MSBR
Wireless Cellular Modem Status Changed on page 172	■ Mediant 500 MSBR ■ Mediant 500L MSBR ■ Mediant 800 MSBR
Data Interface Status on page 172	As above
NQM Connectivity Alarm on page 173	Mediant 800 MSBR

---

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

Alarm Type	Supported Device Types
NQM RTT Alarm on page 174	Mediant 800 MSBR
NQM Jitter Alarm on page 174	Mediant 800 MSBR
NQM Packet Loss Alarm on page 175	Mediant 800 MSBR
NQM MOS CQ Alarm on page 176	Mediant 800 MSBR
NQM MOS LQ Alarm on page 177	Mediant 800 MSBR
Mediant 3000 Hardware Alarms	■ Mediant 3000/TP-6310 ■ Mediant 3000/TP-8410
PEM Module Alarm on page 178	As above
SA Module Missing Alarm on page 179	As above
User Input Alarm on page 180	As above
TM Inconsistency on page 180	As above
TM Reference Status on page 181	This alarm applies only to the Mediant 3000 using the BITs Synchronization Timing mode.
TM Reference Change on page 182	As above
PSTN Trunk Alarms	■ Mediant 500 Gateway & E-SBC ■ Mediant 500 MSBR ■ Mediant 800B Gateway & E-SBC ■ Mediant 800B MSBR ■ Mediant 1000B Gateway & E-SBC

Alarm Type	Supported Device Types
	■ Mediant 3000 ⚠ For version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform[1])
D-Channel Status on page 182	As above
SONET Section LOS Alarm on page 184	■ Mediant 3000/TP-6310
SONET Line AIS Alarm on page 185	■ Mediant 3000/TP-6310
SONET Line RDI Alarm on page 186	■ Mediant 3000/TP-6310
SONET/SDN IF Failure Alarm on page 186	■ Mediant 3000/TP-6310
Trunk LOS Alarm on page 187	■ 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 on page 188	■ Mediant 500 E-SBC ■ Mediant 500 MSBR ■ Mediant 800B Gateway & E-SBC ■ Mediant 800B MSBR ■ Mediant 850 MSBR

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

Alarm Type	Supported Device Types
	■ Mediant 1000B MSBR ■ Mediant 1000B GW & E-SBC ■ Mediant 3000/TP-8410
Trunk AIS Alarm on page 189	■ 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 RAI Alarm on page 189	■ 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 on page 190	■ Mediant 3000/TP-8410
SONET Path STS LOP Alarm on page 191	■ Mediant 3000/TP-6310
SONET Path STS AIS Alarm on page 192	■ Mediant 3000/TP-6310
SONET Path STS RDI Alarm on page 192	■ Mediant 3000/TP-6310
SONET Path Unequipped Alarm on page 193	■ Mediant 3000/TP-6310

Alarm Type	Supported Device Types
SONET Path Signal Label Alarm on page 194	■ Mediant 3000/TP-6310
SONET Path Signal Label Alarm on page 194	■ Mediant 3000/TP-6310
DS1 Line Status Alarm on page 194	As above
DS3 AIS Alarm on page 196	■ Mediant 3000/TP-6310
DS3 LOF Alarm on page 197	■ Mediant 3000/TP-6310
DS3 LOS Alarm on page 197	■ Mediant 3000/TP-6310
NFAS Group Alarm on page 198	As above
B Channel Alarm on page 199	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

Alarm Type	Supported Device Types
	applications that reside on the same host platform[1])
Analog Port SPI Out of Service on page 200	As above
Analog Port High Temperature on page 200	As above
Analog Port Ground Fault Out-of-Service Alarm on page 201	As above
Dial Plan File Replaced Trap on page 201	As above
Analog Line Left Off Hook Alarm on page 202	As above
Microsoft Platform Alarms	■ CloudBond Mediant 800B ■ CloudBond Mediant Server ■ CCE Appliance Mediant 800B ■ CCE Appliance Mediant Server
Component Unreachable on page 203	As above
Component Restart on page 203	As above
Component Performance Counter General on page 204	As above
Component Performance Counter Service on page 205	As above
Component Service	As above

---

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

Alarm Type	Supported Device Types
Status on page 206	
Component Event Viewer on page 207	As above
Component Event Viewer Past Hours on page 207	As above
Component Event Viewer Dropped on page 208	As above
Certificate Expired on page 209	As above
CloudBond Disk Space on page 210	As above
UMP Alarms	■ User Management Pack 365 (UMP)
UMP Tenant License Threshold Alarm on page 211	As above
UMP User License Threshold Alarm on page 211	As above
UMP Super Admin Authentication Fail Event on page 212	As above
UMP Azure AD Sync Alarm on page 213	As above
UMP Office 365 Failure Alarm on page 214	As above
UMP Office 365 Command Execution Event on page 214	As above
UMP User Settings	As above

Alarm Type	Supported Device Types
Fail Event on page 215	
UMP End User Authentication Fail Event on page 216	As above
CloudBond 365	■ CloudBond Mediant 800B ■ CloudBond Mediant Server
Commit License Failed on page 216	As above
Admin License Expired on page 217	As above
CCE Appliance Alarms	■ CCE Appliance Mediant 800B ■ CCE Appliance Mediant Server
Component Unreachable on page 203	As above
Event – Component Restart	As above
Component Performance Counter General on page 204	As above
Component Performance Counter Service on page 205	As above
Component Service Status on page 206	As above
Alarm – Admin System Cloud Status on page 218	As above
CCE Appliance Certificate Expired Alarm on page 219	As above

Alarm Type	Supported Device Types
CCE Wrong Operating Alarm on page 220	As above
CCE Wrong Settings Alarm on page 221	As above
CCE Disk Space Alarm on page 222	As above
CCE Windows License Alarm on page 223	As above
SBA Alarms	■ Mediant 800B Gateway & E-SBC ■ Mediant 1000B Gateway & E-SBC
SBA Services Status Alarm on page 229	As above
Alarm – CPU Status on page 224	As above
Alarm – Memory Status	As above
SBA Disk Space Alarm on page 226	As above
SBA Certificate Expired on page 227	As above
Alarm – Performance Counter on page 228	As above
SmartTAP Alarms	
Alarm - Component Resource Threshold Exceeded on page 234	-
Alarm – Component Unreachable on page 230	-
Alarm – Connection	-

Alarm Type	Supported Device Types
Failure on page 236	
Event – Component Resource Failed on page 231	-
SmartTAP Event – Component Restart on page 231	-
Component Performance Counter General on page 204	-
Alarm – Component Service Status on page 244	-
Alarm – Component Event Viewer Dropped on page 241	Agent alarm
Alarm – Certificate Expired on page 241	Agent alarm
Alarm – Disk Space on page 246	Agent alarm
Call Recording Error Event on page 238	-

Common Device Alarms

Board Fatal Error

Alarm Field	Description
Description	This alarm is 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 Field	Description		
Alarm Source			
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
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.	Any fatal error	-	-

Entity Configuration Change

Alarm Field	Description
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	Other

Alarm Field	Description
Cause	
Severity	Info
Additional Info1,2,3	-
Corrective Action	-

Configuration Error

Alarm Field	Description		
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, OVOC, 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	-	

Initialization Ended

Alarm Field	Description
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

Board Resetting Following Software Reset

Alarm Fields	Description		
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 Source	-		
Alarm Type	equipmentAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	Condition	Text	Corrective Action
Critical	When the device is reset through the	"Device is resetting"	A network administrator has reset the device. Corrective action is not required. The alarm remains at Critical severity

Alarm Fields	Description	
	Web interface or SNMP	level until the device completes the reboot. A Clear trap is not sent.

Feature Key Related Error

Table 6-1:   Feature Key Related Error

Alarm Field	Description
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
Alarm Type	processingErrorAlarm
Severity	Critical
Probable Cause	configurationOrCustomizationError (7)
Alarm Text	Feature key error
Note	Support for this alarm is pending.

Gateway Administrative State Changed

Alarm Field	Description
Description	This alarm indicates that the administrative state of the gateway has been changed to a new state. ⚠️ 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.'

Alarm Field	Description		
	■ 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

Alarm Field	Description		
		- 90 -	administrator has taken an action to unlock the device.

No Free Channels Available

Alarm Field	Description		
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).

Gatekeeper/Proxy not Found or Registration Failed

Alarm Field	Description
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.

Alarm Field	Description		
	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	-

Alarm Field	Description		
		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.	-	-

Ethernet Link Down Alarm

Alarm Field	Description
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 Field	Description
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.

System Component Overloaded

Alarm Field	Description
Description	This alarm is raised when there is an overload in one or more of the

Alarm Field	Description
	system's components.
SNMP Alarm	acBoardOverloadAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11
Alarm Title	System Component Overloaded
Alarm Source	'GWAPP'
Alarm Type	processingErrorAlarm
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=%"	-

Active Alarms Table Overflow

Table 6-2:   Active Alarms Table Overflow

Alarm Field	Description
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

Alarm Field	Description
	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.

Operation State Change [Node]

Table 6-3:   Operational State Change

Alarm	Condition	Text	Corrective Action
Description	This alarm is raised when node state has changed.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarm Source	Node # elementName		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		

Severity			
Major (default)	Operational state changed to disabled	Node {elementName} was marked as {status}	■ 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 available	-	In case state is unavailable: ■ Validate that Node is available in WEB interface / OVOC ■ Check device network connectivity ■ Check the device's network connectivity to the ARM Configurator ■ Validate that proper Node credentials updated in ARM In case state is logged out: ■ Check the ARM configuration in the device In case state is Unrouteable: ■ Check the device network connectivity to the ARM routers ■ Check router status and availability

Keep Alive Trap

Alarm Field	Description
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

Alarm Field	Description
	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.

NAT Traversal Alarm

Alarm Field	Description
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 Field	Description
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

Enhanced BIT Status Trap

Alarm Field	Description
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
Alarm Source	BIT
Alarm Type	Other
Severity	Indeterminate
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their

Alarm Field	Description
	status.
Corrective Action	-

Threshold of Performance Monitored Object Exceeded

Alarm Field	Description
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 Source	MO Path
Alarm Type	Other
Probable Cause	Other
Severity	Indeterminate (this is a notification; it's not automatically cleared)
Additional Info1,2,3	-
Corrective Action	-

HTTP Download Result

Alarm Field	Description
Description	This is a log message (not alarm) indicating both sucessful and failed HTTP Download result.

Alarm Field	Description
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	-

IPv6

Alarm Field	Description
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
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 Field	Description		
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.	-	-

SAS Emergency Mode Alarm

Alarm Field	Description
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

Software Upgrade Alarm

Alarm Field	Description
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.

NTP Server Status Alarm

Alarm Field	Description
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 Field	Description
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.	-	-

LDAP Lost Connection

Alarm Field	Description
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	-

Alarm Field	Description
Corrective Action	-

SSH Connection Status [Event]

Alarm Field	Description
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	-

OCSP Server Status Alarm

Alarm Field	Description
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

Alarm Field	Description
Severity	Major / Clear
Additional Information	-
Corrective Action	■ Repair the Online Certificate Status Protocol (OCSP) server -OR- ■ Correct the network configuration

Media Process Overload Alarm

Alarm Field	Description
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	-

Ethernet Group Alarm

Alarm Field	Description
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.

Alarm Field	Description
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	-

Media Realm BW Threshold Alarm

Alarm Field	Description
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	-

Alarm Field	Description
Corrective Action	-

Certificate Expiry Notification

Alarm Field	Description
Description	This alarm is sent before the expiration of the installed certificate and after it has expired.
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 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.

Web User Access Disabled

Alarm Field	Description
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.

Proxy Connection Lost

Alarm Field	Description
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

Alarm Field	Description
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 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.

Alarm Field	Description		
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	

IDS Policy Alarm

Alarm Field	Description
Description	The alarm is raised whenever a threshold is crossed in the IDS system. The alarm is associated with the MO pair IDSMatch & IDSRule.

Alarm Field	Description
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.

IDS Threshold Cross Notification

Alarm Field	Description
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

Alarm Field	Description
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

IDS Blacklist Notification

Alarm Field	Description
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.

Alarm Field	Description
	⚠️ 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.

Proxy Connectivity

Alarm Field	Description		
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 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

Alarm Field	Description		
		- 115	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	

Web User Activity Log Trap

Alarm Field	Description
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
Alarm Title	Web User Activity Log Trap
Alarm Type	other (0)
Probable Cause	other (0)
Default Severity	Indeterminate
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]

Alarm Field	Description
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.

HTTP Proxy Service Alarm

Alarm Fields	Description		
Description	Sent when an HTTP host specified in the Upstream Groups table is down. The trap is cleared when the host is back up.		
SNMP Alarm	acHTTPProxyServiceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.108		
Alarm Title	HTTP Proxy Service Alarm		
Alarm Source	System#0/HTTPProxyService#<num> System#0/EMSService#<num>		
Alarm Type	communicationsAlarm		
Probable Cause	■ Network issue (connection fail due to network/routing failure) ■ Host issue (host is down) ■ Device issue		
Severity	Condition	Text	Corrective Action
Major	When connection to the Upstream Host is lost.	"HTTP Proxy Upstream Host IP:Port (Host #n in Upstream Group name) is OFFLINE"	1. Ping the host. If there is no ping, contact your provider. The probable reason is that the host is down. 2. Ping between the host and the device. If there is no ping, the problem could be a network/router issue. 3. Check that routing using the

Alarm Fields	Description		
		-	device's (internal) routing table is functioning correctly. **4.** Contact AudioCodes support center (sup-port@AudioCodes.com) and send a syslog and network capture for this issue.
Clear	When connection to service is available again.	-	-

Answer-Seizure Ratio Threshold Alarm

Alarm Field	Description		
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 Type	QualityOfServiceAlarm		
Probable Cause	ThresholdCrossed		
Severity	Condition	\<text\>	Corrective Action
Major	ASR is equal or less than the configured Major threshold.	"ASR threshold crossed."	

Alarm Field	Description		
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.	-	

Average Call Duration Threshold Alarm

Alarm Field	Description		
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 Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction

Alarm Field	Description		
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.		

Network Effectiveness Ratio Threshold Alarm

Alarm Field	Description
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.

Alarm Field	Description		
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.	-	-

IP Group No Route Alarm

Alarm Fields	Description
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

Alarm Fields	Description
	■ Bandwidth ■ ASR (see acASRThresholdAlarm) ■ ACD (see acACDThresholdAlarm) ■ NER (see acNERThresholdAlarm)
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).	-	-

TLS Certificate Expiry Alarm

Alarm Field	Description
Description	The alarm is sent to indicate that the installed TLS certificate belonging to a configured TLS Context is about to expire (which cannot be renewed automatically) or has expired.
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.128
SNMP Alarm	acCertificateExpiryAlarm
Alarm Title	TLS Certificate Expiry Alarm
Alarm Source	Board#1/CertificateExpiry#X
Alarm Type	communicationsAlarm
Probable	communicationsSubsystemFailure

Alarm Field	Description		
Cause			
Alarm Severity	Condition	Text	Corrective Action
Minor	The certificate is about to expire. This is sent a user-defined number of days (TLSExpiryCheckStart) before the expiration date.	"The certificate of TLS context %d will expire in %d days"	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 User's Manual.
Major	The certificate is about to expire. This is sent a week as well as a day before the expiration date.	"The certificate of TLS context %d will expire in less than a week" Or "The TLS certificate of TLS context %d will expire in a day" Or "The TLS certificate of TLS context %d will expire in less than a day"	
Critical	The certificate has expired.	"The certificate of TLS context %d has expired %d days ago"	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 User's Manual.

Alarm Field	Description		
Cleared	A new certificate is installed.	-	-

NGINX Configuration is not Valid

Alarm Field	Description
Description	This alarm is raised when NGINX Directives Sets have been configured with invalid syntax. NGINX continues to run with the previous, valid configuration unless the SBC is restarted, in which case, the NGINX process is stopped and the NGINX Process is not Running alarm is raised (see below).
SNMP Alarm	acNGINXConfigurationIsInvalidAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.130
Alarm Title	NGINX configuration is not valid
Alarm Source	operationalViolation
Alarm Type	alarmTrap
Probable Cause	configurationOrCustomizationError

Alarm Severity	Condition	Text	Corrective Action
Minor		NGINX Configuration file is not valid.	Identify and resolve NGINX Directives Sets syntax errors to ensure an uninterrupted HTTP Proxy service. You can run the CLI commands for troubleshooting: ■ "show network http-proxy conf new" to display the Directives Set configuration that generated the errors. ■ "show network http-proxy conf errors" to display the errors

Alarm Field	Description
	resulting from the invalid Directives Set configuration.

NGINX Process is not Running

Alarm Field	Description		
Description	This alarm is raised when the SBC is restarted with an erroneous NGINX configuration i.e. after alarm 'NGINX Configuration is not Valid' is raised (see NGINX Configuration is not Valid on the previous page).		
SNMP Alarm	acNGINXPprocessIsNotRunningAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.131		
Alarm Title	NGINX process could not be started		
Alarm Source	communicationsAlarm		
Alarm Type	alarmTrap		
Probable Cause	applicationSubsystemFailure		
Alarm Severity	Condition	Text	Corrective Action
Major		NGINX process is not running.	Correct the NGINX Directives syntax and then the NGINX process is restarted automatically.

Remote Monitoring Alarm

Alarm Field	Description
Description	The alarm is sent when the device loses connection with the remote monitoring server (configured on the device as a Remote Web Service) for remote monitoring of the device when it is located behind a NAT.
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.145

Alarm Field	Description		
SNMP Alarm	acRemoteMonitoringAlarm		
Alarm Title	Remote Monitoring Alarm		
Alarm Source	Board#1		
Alarm Type	communicationsAlarm		
Probable Cause	callEstablishmentError		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Warning	The device receives an HTTP failure response (4xx/5xx/6xx) when it sends the monitoring report.	"No connection with Remote Monitoring server"	Check that the configuration of the Remote Web Service is correct.
Cleared	The device receives an HTTP successful response (2xx) when it sends the monitoring report.	-	-

SDR Server Alarm

Alarm Field	Description		
Description	This alarm is sent when SBC failed to upload SDRs to all configured servers.		
SNMP Alarm	acSDRServerAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.147		
Alarm Title	SDR Server Alarm		
Alarm Source	processingErrorAlarm		
Alarm Type	alarmTrap		
Probable Cause	communicationsProtocolError		
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Warning	Device fails to upload SDRs to all remote servers	Failed to upload SDRs to all configured servers	Check that IP address of server is correct

KPI Threshold Crossing

Alarm Field	Description
Description	The alarm is sent every time the threshold of a performance monitoring parameter (object) is crossed. The thresholds to raise or clear an alarm, the severity levels, and the alarm messages are configured in the Alarm Thresholds table (Setup menu > Administration tab > Performance Monitoring folder).
SNMP Alarm	acKpiThresholdCrossing
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.148
Alarm Title	KPI Threshold Crossing
Alarm Source	The object for which the threshold is crossed.
Alarm Type	processingErrorAlarm
Probable Cause	thresholdCrossed

Alarm Severity	Condition	Text	Corrective Action
Raised alarm (severity depends on con-figuration)	Threshold crossed to raise alarm	<kpi_name> value <value> is too <high|low> (Note: Text is con-figurable.)	Verify the con-figuration of the related Per-formance Mon-itoring object and adjust loads accordingly.
Cleared alarm (severity depends on con-figuration)	Threshold crossed to clear alarm	"<kpi_name> value <value> is back to normal" (Note: Text is	

Alarm Field	Description	
	configurable.)	

Clock Configuration Alarm

Alarm Field	Description		
Description	This alarm is sent when both NTP and Date Header Time Sync options have been enabled in the Time & Date page of the device's Web server.		
SNMP Alarm	acClockConfigurationAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.149		
Alarm Title	Clock Configuration Alarm		
Alarm Source	operationalViolation		
Alarm Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	Condition	Text	Corrective Action
Minor	Both the NTP Server and Data Header Time Sync options have been configured in the Time & Date page of the device's Web server.	Clock Synchronization from SIP Date header ignored as NTP is enabled.	Disable one of these configuration options.

Debug Recording Activation Alarm

Alarm Field	Description
Description	This alarm is sent when Debug Recording is enabled on the device.
SNMP Alarm	acDebugRecordingActivationAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.150
Alarm Title	Debug Recording Activation Alarm
Alarm Source	operationalViolation

Alarm Field	Description		
Alarm Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	Condition	Text	Corrective Action
Minor	Debug recording is activated on the device	Debug Recording is active	-
Clear	Cleared when Debug Recording stops working and no longer captures any packets.		

Specific Hardware Alarms

Temperature Alarm

Alarm Field	Description		
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 Source	System#0		
Alarm Type	equipmentAlarm		
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	Board temperature too high	Check that the ambient environment around the chassis was not changed (room

Alarm Field	Description		
	normal operation	- 129 -	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	-	-

Fan Tray Alarm

Alarm Field	Description
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 Type	equipmentAlarm

Alarm Field	Description
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.	-	-

Power Supply Alarm

Alarm Field	Description
Description	This alarm is activated in one of the following cases:

Alarm Field	Description
	■ 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.	-	-

HA System Alarms

HA System Fault Alarm

Alarm Field	Description
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.

Alarm Field		Description	
		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

Alarm Field	Description		
			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.

Alarm Field		Description	
		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.

Alarm Field		Description	
		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	-	-

HA System Configuration Mismatch Alarm

Alarm Field	Description		
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	-

HA System Switch Over Alarm

Alarm Fields	Description
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 HA System Configuration Mismatch Alarm on the previous page above for details.
Cleared	10 seconds have passed since the switchover	-	-

Hitless Software Upgrade Alarm

Alarm Field	Description
Description	A Notification trap that is sent out at the beginning and the end of a Hitless software update. Failure during the process will also instigate the trap. This alarm is only relevant for the local license key.
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 Field	Description
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.

Redundant Board Alarm

Alarm Field	Description
Description	Active board sends notification when an alarm or notification is raised in the redundant board.

Alarm Field	Description
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	-

HA Network Watchdog Status Alarm

Alarm Field	Description
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

Alarm Field	Description	
Probable Cause	outOfService	
Default Severity	Major	

Alarm Severity	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	-

License Key Hitless Upgrade Alarm

Alarm Field	Description
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	keyExpired

Alarm Field	Description		
Cause			
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.

HA Network Mismatch Alarm

Alarm Field	Description		
Description	Mismatch of network devices in the cloud HA system (AWS) between active and redundant instances. There is a mismatch in the configuration of the AWS instances for the ENI (Elastic Network Interface), i.e. a different number of ENIs are configured, and/or different Subnet IDs, or the same ENIs however in the incorrect order. When working on an AWS HA system, both systems (Active & Redundant) must be identical in terms of ENIs.		
SNMP Alarm	acHANetworkMismatchAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.135		
Alarm Title	HA Network Mismatch Alarm		
Alarm Source	SystemMo		
Alarm Type	communicationsAlarm		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	Condition	Text	Corrective Action
Major	ENI configuration of both instances do not match	Cloud network devices do not match"	Fix the ENI con-figuration

HA Network Monitor Alarm

Description	Alarm Fields
Description	This alarm is sent when all previously reachable destinations configured for a specific row in the HA Network Monitor table (for the HA Network Monitor feature) are now unreachable (i.e., none of them reply to the device's pings). For configuring the HA Network Monitor feature, refer to the User's Manual.
SNMP Alarm	acHANetworkMonitorAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.136
Alarm Title	HA Network Monitor Alarm
Alarm Source	Board#1/NetworkMonitor#X
Alarm Type	communicationsAlarm
Probable Cause	connectionEstablishmentError

Alarm Severity	Condition	Text	Corrective Action
Major	All destinations of a specific row in the HA Network Monitor table that replied in the past to the device's pings are now "unreachable"	"Destination/s <peer destination IP address(es)> is/are unreachable"	-
Cleared	At least one of the "unreachable" destinations replies to the device's pings and is now "reachable", or the row in the HA Network Monitor table has been deleted	-	-

HA Ethernet Group Alarm

Alarm Field	Description
Description	This alarm is sent when the Ethernet link of at least one port in the Ethernet Group that is associated with the HA Maintenance interface is down.
SNMP Alarm	acHAEthernetGroupAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.137
Alarm Source	system#0
Alarm Type	qualityOfServiceAlarm
Probable Cause	outOfService

Alarm Severity	Condition	Text	Corrective Action
Minor	At least one of the Ethernet port links in the Ethernet Group associated with the HA Maintenance interface is down	"SYS_HA: Maintenance Group - One of the links is down - NO HA of maintenance link redundancy"	Check that the Ethernet cables are connected securely to the ports. Check that the ports at the other end are up (working).
Cleared	All Ethernet ports in the Ethernet Group associated with the HA Maintenance interface become up again	-	-

License Pool Alarms

License Pool Infra Alarm

Alarm Field	Description
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.

Alarm Field	Description
	■ 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
Alarm 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 OVOC 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 OVOC 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

Alarm Field	Description		
	The device license has expired.	The device license has expired! Use of this device is strictly prohibited.	device and send the latest license.
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.	-	

License Pool Application Alarm

Alarm Field	Description		
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

Alarm Field	Description		
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.

License Pool Over Allocation Alarm

Alarm Field	Description		
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		
Alarm 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

Alarm Field	Description		
			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).

Floating License Alarms

Floating License Alarm - Not Enough Memory to Allocate 'Custom' Profile

Alarm Field	Description
Description	This alarm is raised when there are insufficient physical memory resources to allocate for configuring the "Floating License" with the configured Custom Allocation Profile in the device's Floating License table.
SNMP Alarm	acFloatingLicenseAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.138
Alarm Title	Floating License Alarm - Not enough memory to allocate 'custom' profile
Alarm Source	Board#1
Additional Info	Detailed explanation of the License configuration parameter that resulted in this alarm, including the requested and actual value. For example, "SignalingSessions – requested 10000, allocated 1000"

Alarm Field	Description		
Alarm Type	processingErrorAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	An attempt was made to configure a Custom Allocation Profile with values exceeding the device's physical memory.	"Not enough memory to allocate for 'custom' profile"	Define a Custom Allocation Profile within the bounds of the device's capacity.

Cloud License Manager Alarm

Alarm Field	Description		
Description	This alarm is raised under one of the following circumstances: ■ Disconnection between the device and OVOC. ■ Failure to send usage reports from the device to OVOC. ■ Fixed license is enabled and an attempt was made to enable the Floating license.		
SNMP Alarm	acCloudLicenseManagerAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.132		
Alarm Title	Cloud License Manager Alarm		
Alarm Source	Board#1		
Alarm Type	processingErrorAlarm		
Probable Cause	configurationOrCustomisationError		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction

Alarm Field	Description		
Major	There is no connection between the device and OVOC either prior to the initial handshake or due to a long disconnection time (default is three months; this time may be overriden by OVOC).	"No connection with OVOC"	■ Check TCP/TLS connectivity. ■ Device should be registered on OVOC.
	Usage reports could not be sent to OVOC from the device for a specified number of days.	"Failed to send usage report to OVOC for X days"	Check TCP/TLS connectivity.
	The device is configured to work with the Fixed License Pool and an attempt was made to enable the Floating license.	"Floating license cannot be enabled, when device is managed by License Pool"	■ Disable Floating License parameter on the device. ■ Remove the device from the Fixed License Pool in OVOC.
Critical	Device couldn't connect to OVOC (handshake).	"Connection with OVOC failed with response code <XXX>". See below for more information"	■ <Forbidden 403>: contact AudioCodes support. ■ <unauthorized 401>: check username/password
	Device couldn't connect to OVOC (handshake).	"Connection with OVOC failed, Failed initialize connection"	Check TCP/TLS connectivity.
	Device couldn't initialize connection to OVOC (handshake).	"Device was rejected by OVOC while trying to	<Forbidden 403>: contact AudioCodes support.

Alarm Field	Description		
		retrieve the device ID"	
Cleared	■ Connection with OVOC is established. ■ Reports are sent successfully. ■ The Floating License parameter is disabled on the device or the device is removed from the Fixed License Pool. This alarm is cleared upon the next reboot.	-	-

HTTP response code and reason:

■ Other 4xx-6xx responses: the device retries the request using the value in retry-after header if specified, or immediately following an update of the OVOC Product key.

■ OVOC response to Register requests:

- 200 In case of successful request

- 400: request format is not valid or request data is not valid, or if OVOC is in a state of initial registration required

- 401: username or password are incorrect

- 403: customer is blocked, or OVOC maximum capacity has been reached

- 404: request URI contains a device ID not identified by OVOC.

- 500: server is not able to handle the request due to server side error (no resources, internal component failure etc.)

■ Server may respond with 4xx or 5xx error as defined in HTTP RFC when appropriate.

Flex License Manager Alarm

Alarm Field	Description
Description	The alarm is sent when a change in status occurs in one or more SBC capacity license types that are managed by OVOC Flex License. The status change can be from "ok" to "overlicense" or vice versa. The SBC capacity license types include Signaling Sessions, FEU (Far End Users), Transcoding Sessions, and Media Sessions.
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.144
SNMP Alarm	acFlexLicenseManagerAlarm
Alarm Title	Flex License Manager Alarm
Alarm Source	Board#1
Alarm Type	processingErrorAlarm
Probable Cause	communicationsProtocolError

Alarm Severity	Condition	Text	Corrective Action
Warning	OVOC Flex License pool stops the device's service of an SBC capacity license type(s) due to pool's license capacity reached or exceeded (utilization status changed to "overlicense").	"Service for <service name> license parameter is stopped" Where <service type> can be Signaling sessions, FEU (Far End Users), Transcoding sessions, and Media sessions	
Cleared	OVOC Flex License pool allows the device's service of an SBC capacity license type(s) when sufficient licenses are restored to the pool (utilization		

Flex License Manager Alarm

Alarm Field	Description	
	status changed to "ok").	

Mediant 2600 E-SBCand Mediant 4000 Alarms SBC

DSP Farms Mismatch Alarm

Alarm Field	Description		
Description	This alarm is sent if the number of MPM modules (DSP farms) configured by the ini file parameter DspFarmsInstalledNum (default is 0) is greater than the actual MPM modules installed in the device's chassis. This alarm and the parameter are used to check that all required MPMs are present and correctly installed in the device's chassis.		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.143		
SNMP Alarm	AcDSPFarmsMismatchAlarm		
Alarm Title	DSP Farms Mismatch Alarm		
Alarm Source	Board#1/ClusterManager#1/MT#2		
Alarm Type	equipmentAlarm		
Probable Cause	Underlying Resource Unavailable		
Alarm Severity	Condition	Text	Corrective Action
Major	The number of MPMs configured by the DspFarmsInstalledNum parameter is greater than the number of MPMs installed on the chassis. This could result in a faulty or missing MPM module(s).	"Missing DSP farm was detected."	■ Check if the MPM module(s) is fully inserted into the chassis slot. ■ If an MPM module(s) was removed from the chassis, re-install it. ■ Make sure that the DspFarmsInstalledNum parameter is configured to the correct number of physical MPM modules.

Alarm Field	Description		
		- 154 -	■ If you have performed all the above and the alarm still exists, send a Return Merchandise Authorization (RMA) request to AudioCodes
Cleared	The number of MPMs configured by the DspFarmsInstalledNum parameter is less than or equal to the number of MPMs installed in the chassis.	-	-

Mediant 9000 and Software SBC Alarms

Cluster HA Alarm

Alarm Field	Description
Description	The alarm is sent by the Cluster Manager when the cluster HA usage exceeds 100%. HA usage of 100% means that if a failure occurs in a Media Component (MC or vMC), sufficient DSP resources are available on the other Media Components in the cluster to take over the transcoding sessions of the failed Media Component. HA usage exceeding 100% means that insufficient DSP resources are available on the other Media Components to take over the transcoding sessions of the failed Media Component.
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
Additional	-

Alarm Field	Description		
Info			
Alarm Severity	Condition	Text	CorrectiveAction
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%	-	-

Media Transcoder Network Failure

Alarm Field	Description
Description	The alarm is sent when the Cluster Manager (Media Transcoding Cluster feature) or Signalling Component (Elastic Media Cluster feature) fails to connect to the Media Component.
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 Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Major	Connection failure with Media Transcoder	"No Connection with MTCE: <MTCE-name>"	For the Media Transcoding Cluster feature, ensure a physical connection exists between the Media Component and the Cluster Manager.
Cleared	Connection established / re-established with Media Transcoder	-	-

Media Transcoder Software Upgrade Failure

Alarm Field	Description		
Description	The alarm is sent upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Component.		
SNMP Alarm	acMtceSwUpgradeFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.117		
Alarm Title	Media Transcoder Software Upgrade Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	processingErrorAlarm		
Probable Cause	other		
Severity	Condition	Text	Corrective Action
Major	Software upgrade (.cmp) or Auxiliary file load failure in Media Component.	""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	-	-

Media Transcoder High Temperature Failure

Alarm Field	Description
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	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.

Alarm Field	Description		
Cleared	Connectivity with Media Transcoder is re-established and temperature is reduced	-	-

Media Transcoder Fan Tray Module Failure

Alarm Field	Description		
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	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	-	-

Media Transcoder Power Supply Module Failure

Alarm Field	Description
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
Alarm Type	equipmentAlarm
Probable Cause	powerProblem

Alarm Severity	Condition	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	-	-

Cluster Bandwidth Utilization Alarm

Alarm Field	Description
Description	The alarm is raised when the bandwidth utilization of a Cluster interface exceeds the configured maximum bandwidth (refer to the MtcClusterNetworkMaxBandwidth parameter).

Alarm Field	Description
SNMP Alarm	acClusterBandwidthAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.126
Alarm Title	Cluster Bandwidth Utilization Alarm
Alarm Source	Board#1/EthernetLink#<ehternet port number>
Alarm Type	Other
Probable Cause	performanceDegraded: ■ Too many sessions processed on the specific Cluster interface. ■ Cluster interface is being used by another application (e.g., OAMP).
Additional Info	-

Alarm Severity	Condition	Text	CorrectiveAction
Major	Bandwidth utilization is greater than 90%.	"Cluster Bandwidth is above 90% utilization on Interface name: <name>. No more transcoding sessions will be allocated on that Cluster Interface"	Reduce the number of Media Transcoders on that Cluster interface. Alternatively, the overall permitted bandwidth for the Cluster interfaces should be increased, if possible (using the ini file parameter MtcClusterNetworkMaxBandwidth).
Minor	Bandwidth utilization is between 85 and 90%. Note: If a Major alarm was raised and the	"Cluster Bandwidth is above 85% utilization on Interface name: <name>"	

Alarm Field	Description		
	bandwidth later declined to between 80 and 85%, the alarm is changed to Minor.	- 161 -	
Clear	Bandwidth utilization is less than 80%.		

Media Cluster Alarm

Alarm Field	Description
Description	The alarm is sent when the Media Cluster is enabled and one of the following scenarios exist: ■ There are no operational Media Components in the Media Cluster. ■ There are no media interfaces configured for the operational Media Components. ⚠ Typically, using the Stack Manager to install, configure and manage Mediant CE prevents conditions (described below) that cause this alarm to be generated. However, if this alarm is generated, it is recommended to call the Healing stack operation, as described in the *Stack Manager for Mediant CE SBC User's Manual*.
SNMP Alarm	acMediaClusterAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.133
Alarm Title	Media Cluster Alarm
Alarm Source	Device/clusterManager
Alarm Type	-
Probable Cause	-

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Major	Media Cluster is enabled, however, no media interface is configured for the operational Media Components	Media Cluster Alarm: Media Cluster <MC Name>, Remote Interface - Alarm Status is NoRmifPresent.	Configure media interfaces on the Media Components.
Clear	A media interface is configured on the Media Component, or the Media Component is removed from the Cluster Manager	Media Cluster : Media Cluster <MC Name>, Remote Interface - Alarm Status is Clear	-

Remote Interface Alarm

Table 6-4:   Remote Interface Alarm

Alarm Fields	Description
Description	This alarm is raised in the following circumstances: ■ A Media Interface ethXX exists in the Remote Interface table, and this interface is used by one or more Media Realms; however, it is not defined in a specific Media Cluster. ■ A Media Interface ethXX exists in the Remote Interface table of the Cluster Manager (CM) and is used by one or more Media Realms; however, it does not have a public IP address configured on the Media Cluster i.e. a NAT rule is defined for a Remote Interface which is referenced by a Media Realm, however, an MC does not have a public IP address for this interface. ■ A Media Interface ethXX exists in the Remote Interface table of the Cluster Manager(CM) and is used by one or more Media Realms; however, it's status is link down.

Alarm Fields	Description
	⚠️ Typically, using the Stack Manager to install, configure and manage Mediant CE prevents conditions (described below) that cause this alarm to be generated. However, if this alarm is generated, it is recommended to call the Healing stack operation, as described in the Stack Manager for Mediant CE SBC User's Manual.
SNMP Alarm	acMediaClusterRemoteInterfaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.134
Alarm Title	Remote Interface Alarm
Alarm Source	device/clusterManager/MC
Alarm Type	Media Cluster
Probable Cause	-

Alarm Severity	Condition	Text	Corrective Action
Major	According to description above.	■ Interface <Interface id>, Name: <ethXX> - Alarm Status is RmifMissing ■ Interface <Interface id>, Name: <ethXX> - Alarm Status is PublicIpAddrMissing ■ Remote Interface Alarm: Interface <Interface id>, Name: <ethXX> - Alarm Status is LinkDown	■ Add the appropriate Media Interface ethXX ■ Configure a public IP address on the Media Cluster or remove the NAT rule. ■ Troubleshoot the Media Interface ethXX

AWS Security Role Alarm

Alarm Field	Description
Description	The alarm is sent when the Amazon Web Services (AWS) instance has not been configured with the required IAM role to access AWS services and

Alarm Field	Description
	resources.
SNMP Alarm	acAWSSecurityRoleAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.139
Alarm Title	AWS Security Role Alarm
Alarm Source	Board#1
Alarm Type	securityServiceOrMechanismViolation
Probable Cause	configurationOrCustomizationError
Alarm Severity	Condition
Major	IAM role was not found, or access to AWS services was blocked
Cleared	IAM role was found and permission to access AWS services was granted

CDR Server Alarm

Alarm Field	Description		
Description	The alarm is sent when the device fails to send a locally stored CDR file to all the remote CDR (SFTP) servers, which are configured in the SBC CDR Remote Servers table.		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.142		
SNMP Alarm	acCDRServerAlarm		
Alarm Title	CDR Server Alarm		
Alarm Source	Board#1		
Alarm Type	equipmentAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Major	Device failed to send	"Device failed to send	Check the

Alarm Field	Description		
	the CDR local storage file to all the configured CDR servers.	CDR local storage files to all configured SFTP servers"	network connectivity to the remote server.
Cleared	Device successfully sent the CDR file to at least one of the CDR servers.	"Files transfer succeeded to one of the CDR servers"	-

Metering Alarm

Alarm Field	Description		
Description	The alarm is sent when the device fails to communicate with the Amazon Web Services (AWS) Marketplace metering API. The device needs to communicate with the Marketplace API when using AudioCodes' Metered License model to license the SBC, which is based on the device's usage (in minutes).		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.146		
SNMP Alarm	acMeteringAlarm		
Alarm Title	Metering Alarm		
Alarm Source	Board#1 (SystemMO)		
Alarm Type	communicationsAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	The device is unable to send a usage report to the AWS metering service after it has initially connected with it.	"No connection to metering API – service will be down in 3 hours"	Check the network configuration and make sure that the device has the appropriate environment as required for the

Alarm Field	Description		
			metering offer.
Critical	The device is unable to establish an initial connection with the AWS metering API, or has lost connectivity with the metering API for 3 hours since the last connection.	"Service down due to no connection to metering API"	Check the network configuration and make sure that the device has the appropriate environment as required for the metering offer.
Cleared	The device successfully communicates with the AWS metering API.	"Device succeeds to communicate with metering API"	-

MP-1288 Alarms

Module Service Alarm

Alarm Field	Description		
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)		
Alarm Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	Condition	Text	Corrective Action
Minor	More than five FXS ports	Multiple	Service the faulty blade.

Alarm Field	Description		
	and less than 33% of FXS ports are Out-Of-Service on a this blade.	FXS ports are Out-Of-Service.	
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. The FXS module has less than 4 FXS ports that 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.

Module Operation Alarm

Alarm Field	Description		
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)		
Alarm Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	Condition	Text	Corrective Action

Alarm Field	Decription		
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.		

Port Service Alarm

Alarm Field	Description
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 Field	Description		
Alarm Source	Chassis/Module#/FXS Port #		
Alarm 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.		

MSBR Alarms

WAN Link Alarm

Alarm Field	Description
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.

Power Over Ethernet Status [Event]

Alarm Field	Description
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

Alarm Field	Description
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	-

Wireless Cellular Modem Alarm

Alarm Field	Description		
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		
Alarm Source	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	-	-

Wireless Cellular Modem Status Changed

Alarm Field	Description
Description	Sent upon a change in the status of the 3G cellular (wireless) USB modem. A change can be in any of the following: ■ Vendor ID ■ Product ID ■ Cellular state (shutdown or no shutdown) ■ Received Signal Strength Indicator (RSSI) in dBm ■ Cellular dongle status ("up" or "down")
SNMP Alarm	acWirelessCellularModemStatusChanged
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.104
Alarm Title	Wireless Cellular Modem Status Changed
Alarm Source	Board#x/WanLink#y
Alarm Type	Equipment Alarm
Probable Cause	other (0)

Alarm Severity	Condition	Text	Corrective Action
Indeterminate		MSBR cellular interface: dongle type <vendor ID>:<product ID>,modem <"on" or "off">,RSSI <dBm value> DBM.	

Data Interface Status

Alarm Field	Description
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 Field	Description
Alarm Source	-
Alarm Type	communicationsAlarm
Probable Cause	communicationsProtocolError
Severity	indeterminate
Additional Info	-
Corrective Action	-

NQM Connectivity Alarm

Alarm Field	Description		
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		
Alarm 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

NQM RTT Alarm

Alarm Fields	Description
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.

NQM Jitter Alarm

Alarm Field	Description
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 Title	NQM Jitter Alarm
Alarm Source	Board#%d/NqmSender#%d
Alarm Type	CommunicationsAlarm

Alarm Field	Description		
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.

NQM Packet Loss Alarm

Alarm Field	Description		
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	To correct high packet loss (PL): ■ Eliminate interference problems:

Alarm Field	Description	
	destination	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.

NQM MOS CQ Alarm

Alarm Field	Description		
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 NQM Jitter Alarm on page 174 ■ Perform corrective action for Real Time Protocol (RTP) packet loss.

Alarm Field	Description
	■ See NQM Packet Loss Alarm on page 175 ■ Perform corrective action for long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination. ■ See NQM RTT Alarm on page 174 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 NQM Packet Loss Alarm on page 175

NQM MOS LQ Alarm

Alarm Field	Description		
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	To fix the Noise Quality

Alarm Field	Description	
	voice quality towards NQM probe destination	Measure (NQM) result: ■ Perform corrective action for Real Time Protocol (RTP) packet loss. 　■ See NQM Packet Loss Alarm on page 175 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 NQM Packet Loss Alarm on page 175

Mediant 3000 Hardware Alarms

PEM Module Alarm

Alarm Field	Description
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
Alarm Source	chassis#0/PemCard#<m>, where m is the power entry module's (PEM) slot number
Alarm Type	equipmentAlarm

Alarm Field	Description		
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.		

SA Module Missing Alarm

Alarm Field	Description		
Description	This alarm 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		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	Condition	<Text>	Corrective Action
Critical (default)	SA module removed or	SA Module Alarm. SA-Module from slot #n is	■ Reinsert the Shelf Alarm (SA) module

Alarm Field	Description		
	missing	missing.	into slot #n ■ Make sure it's correctly inserted in the slot.
Cleared	SA module is in slot 2 or 4 and working.	-	-

User Input Alarm

Alarm Field	Description		
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 Title	User Input Alarm		
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.	-	-

TM Inconsistency

Alarm Field	Description
Description	Timing Manager Alarm. This alarm is triggered when the system is in a 1+1

Alarm Field	Description
	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.

TM Reference Status

Alarm Field	Description
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

Alarm Field	Description
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.

TM Reference Change

Alarm Field	Description
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	-

PSTN Trunk Alarms

D-Channel Status

Table 6-5:   D-Channel Status

Alarm Field	Description
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

Alarm Field	Description
	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	-

SONET Section LOF Alarm

Alarm Field	Description		
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		
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

Alarm Field	Description		
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	-

SONET Section LOS Alarm

Alarm Field	Description		
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.

Alarm Field	Description		
			Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value sonetSectionLOS (2)
Cleared	LOS condition is not present	-	-

SONET Line AIS Alarm

Alarm Field	Description		
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		
Alarm Source	Interfaces#0/Sonet#<m>, where m is the SONET interface number		
Alarm 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.	-	-

SONET Line RDI Alarm

Alarm Field	Description
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
Alarm 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.	-	-

SONET/SDN IF Failure Alarm

Alarm Field	Description
Description	This alarm indicates a Hardware 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 Field	Description
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	-

Trunk LOS Alarm

This alarm applies to E1/T1Trunks.

Alarm Field	Description		
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

Alarm Field	Description		
			support@AudioCodes.com.
Cleared	End of LOS	-	-

Trunk LOF Alarm

This alarm applies to E1/T1Trunks.

Table 6-6:   Trunk LOF Alarm

Alarm Field	Description		
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

Alarm Field	Description		
			Center at support@AudioCodes.com.
Cleared	End of LOF	-	-

Trunk AIS Alarm

This alarm applies to E1/T1Trunks.

Alarm Field	Description		
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 Title	Trunk AIS Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
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	-	-

Trunk RAI Alarm

Alarm Field	Description
Description	This alarm indicates a loss of frame at the trunk's far end.

Alarm Field	Description
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

V5.2 Interface Alarm

Table 6-7:   V5.2 Interface Alarm

Alarm Field	Description
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

Alarm Field	Description
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.

SONET Path STS LOP Alarm

Alarm Field	Description
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

Alarm Field	Description
Severity	Critical / clear
Additional Info	-
Corrective Action	Correct the SONET mapping on either side (the Gateway and the far end).

SONET Path STS AIS Alarm

Alarm Field	Description
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

SONET Path STS RDI Alarm

Alarm Field	Description
Description	This alarm is issued when the RDI condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTSRDIAlarm

Alarm Field	Description
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

SONET Path Unequipped Alarm

Alarm Field	Description
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

SONET Path Signal Label Alarm

Alarm Field	Description
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).

DS1 Line Status Alarm

Alarm Field	Description	
Description	Indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information.	
SNMP Alarm	ds1LineStatus	
SNMP OID	1.3.6.1.2.1.10.18.15.0.1	
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk	
Alarm Type	communicationsAlarm	
Probable Cause	-	
Alarm Severity	Text	Additional Info1,2,3

Alarm Field		Description
-	DS1 Line Status	Updated DS1 Line Status.
		This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information.
		dsx1LineStatus is a bitmap represented as a sum, so it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set.
		If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are:
		1dsx1NoAlarmNo alarm present
		2dsx1RcvFarEndLOFFar end LOF (a.k.a., Yellow Alarm)
		4dsx1XmtFarEndLOFNear end sending LOF Indication
		8dsx1RcvAISFar end sending AIS
		16dsx1XmtAISNear end sending AIS
		32dsx1LossOfFrameNear end LOF (a.k.a., Red Alarm)
		64dsx1LossOfSignalNear end Loss Of Signal
		128dsx1LoopbackStateNear end is looped
		256dsx1T16AISE1 TS16 AIS
		512dsx1RcvFarEndLOMFFar End Sending TS16 LOMF
		1024dsx1XmtFarEndLOMFNear End Sending TS16 LOMF
		2048dsx1RcvTestCodeNear End detects a test code
		4096dsx1OtherFailureAny line status not defined here
		8192dsx1UnavailSigStateNear End in Unavailable Signal State
		16384dsx1NetEquipOOSCarrier Equipment Out of Service
		32768dsx1RcvPayloadAISDS2 Payload AIS
		65536dsx1Ds2PerfThresholdDS2 Performance Threshold Exceeded

DS3 RAI Alarm

Alarm Field	Description
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

DS3 AIS Alarm

Alarm Field	Description
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

Alarm Field	Description
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

DS3 LOF Alarm

Alarm Field	Description
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

DS3 LOS Alarm

Alarm Field	Description
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 Field	Description
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

NFAS Group Alarm

Alarm Field	Description		
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

Alarm Field	Description	
		backup) returns to service, the alarm is cleared. ■ Corrective action is not necessary.
Clear	NFAS group state goes to in- service	%s– Additional information -

B Channel Alarm

Alarm Field	Description		
Description	This alarm is raised when the B-Channel service state changes and is cleared when the BChannel 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		
Additional Info	-		
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 Ser-vice'	%s – additional information	

Analog Port Alarms

Analog Port SPI Out of Service

Alarm Field	Description
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	-

Analog Port High Temperature

Alarm Field	Description
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	-

Alarm Field	Description
Corrective Action	-

Analog Port Ground Fault Out-of-Service Alarm

Alarm Field	Description
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 Text	Analog Port Ground Fault Out Of Service
Alarm Type	physicalViolation
Probable Cause	equipmentMalfunction (this alarm is raised when the FXS port is inactive due to a ground fault)
Default Severity	Major / Clear
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.

Dial Plan File Replaced Trap

Alarm Field	Description
Description	Indicates that the dial plan file has been replaced.
SNMP Alarm	acDialPlanFileReplaced
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.45
Default Severity	Indeterminate

Alarm Field	Description
Alarm Type	Other (0)
Probable Cause	Other (0)
Status Change	
Condition	Successful dial plan file replacement
Trap Text	Dial plan file replacement complete.

Analog Line Left Off Hook Alarm

Alarm Field	Description		
Description	The alarm is sent when an analog FXS phone is left off-hook for a user-defined time, configured by the FXSOffhookTimeoutAlarm parameter.		
SNMP Alarm	acAnalogLineLeftOffhookAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.141		
Alarm Source	Board#1/SipAnalogEp#<id>		
Event Type	equipmentAlarm		
Probable Cause			
Alarm Severity	Condition	Text	Corrective Action
Major	FXS phone is left off-hook for a user-defined time (configured by the FXSOffhookTimeoutAlarm parameter)	"Left Offhook Line N"	Place the phone's handset on the hook (on-hook position).
Clear	FXS phone returns to on-hook position or the phone's hook-flash button is pressed.	-	-

Microsoft Platform Alarms

The alarms described in this section are raised for the following products:

■ CloudBond

■ CCE Appliance

■   UMP (User Management Pack)

Component Unreachable

Alarm Field	Description
Description	This alarm is raised when the OVOC Main Agent is unable to connect to one of the client agents.
SNMP Alarm	acCbManEnvUnreachableAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.2
Alarm Title	Component Unreachable
Alarm Source	<n> (where n is the component name)
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Severity	Condition	Text	Corrective Action
Major	Client agent is unavailable	Unable to connect to the client agent on <component name>.	-
Cleared	Client agent is available again.	-	-

Component Restart

Alarm Field	Description
Description	This alarm is raised when a component is restarted.
SNMP Alarm	acCbManEnvRestartEvent
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.3
Alarm Title	Component Restart
Alarm Source	<n> (where n is the component name)

Alarm Field	Description		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-The restart reason		
Alarm Severity	Condition	Text	Corrective Action
Major	Indeterminate	Component <component name> restarted	-
Cleared	-		-

Component Performance Counter General

Alarm Field	Description		
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 Title	Component Performance Counter General		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-

Alarm Field	Description		
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.	-	-

Component Performance Counter Service

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

Alarm Field	Description		
	per each counter type	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.	-	-

Component Service Status

Alarm Field	Description		
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 Title	Component Service Status		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Critical	Service is down	SERVICE_ STOPPED (indicates which service is down)	Note: the severity is determined according to the service's importance to system functionality.
Major	Service is down	SERVICE_ STOPPED (indicates which	

Alarm Field	Description		
		service is down)	
Warning	Service is down	SERVICE_ STOPPED (indicates which service is down)	

Component Event Viewer

Alarm Field	Description
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 Title	Component Event Viewer
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))
Alarm Type	Other
Probable Cause	Other
Additional Info	Contains the original severity of the event. This event is displayed in OVOC as type "Info".
Alarm Severity	Condition
Indeterminate	The event text

Component Event Viewer Past Hours

Alarm Field	Description
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 Field	Description		
Alarm Title	Component Event Viewer Past Hours		
Alarm Source	<n> (where n is the component name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
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.	The event log has errors	-

Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when event from the Event Viewer are dropped and not sent to OVOC after the sending rate threshold has been exceeded; preventing a burst of events being raised on the Windows server for a specific component.
SNMP Alarm	acCbCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.16
Alarm Title	Component Event Viewer Dropped
Alarm Source	N/A
Alarm Type	Other

Alarm Field	Description
Probable Cause	Other
Alarm Text	Events from Event Viewer dropped due to high sent rate.
Additional Info	-
Severity	Indeterminate

Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when the certificate for the component is about to expire.		
SNMP Alarm	acCceAdminCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.32		
Alarm Title	CloudBond Certificate Expired		
Alarm Source	<n> (where n is the component name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
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.

Alarm Field	Description		
Cleared	When certificate is renewed.	-	-

CloudBond Disk Space

Alarm Field	Description		
Description	This alarm is raised when the 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 Title	CloudBond Disk Space		
Alarm Source	<e> (drive letter 'c:')		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		

Alarm Severity	Condition	Text	CorrectiveAction
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.	-	-

User Management Pack 365 (UMP) Alarms

UMP Tenant License Threshold Alarm

Alarm Field	Description
Description	This alarm is raised when the number of UMP tenant licenses that are active for a specific UMP virtual machine instance crosses the threshold. ⚠️ A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition.
SNMP Alarm	acUmpTenantLicThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.41
Alarm Title	UMP Tenant License Threshold Alarm
Alarm Source	Virtual machine of UMP installation platform
Alarm Type	Other
Probable Cause	Other
Additional Info	#of users/# in active

Alarm Severity	Condition	Text	Corrective Action
Critical	The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 95 %).	Tenant License threshold (Over 95 %)	
Major	The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 90 %).	Tenant License threshold (Over 90 %)	

UMP User License Threshold Alarm

Alarm Field	Description
Description	This alarm is raised when the number of active UMP users for a specific

Alarm Field	Description
	UMP tenant on a specific UMP virtual machine instance crosses the licensed threshold. ⚠️ A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition.
SNMP Alarm	acUmpUserLicThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.42
Alarm Title	UMP User License Threshold Alarm
Alarm Source	Virtual machine of UMP installation platform
Alarm Type	Other
Probable Cause	Other
Additional Info	#of users/# in active-

Alarm Severity	Condition	Text	Corrective Action
Critical	The number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance, crosses the licensed threshold (above 95 %).	User License threshold (Over 95 %)	
Major	This alarm is raised when the number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance, crosses the threshold (above 90 %).	User License threshold (Over 90 %)	

UMP Super Admin Authentication Fail Event

Alarm Field	Description
Description	This alarm is raised when there is an authentication failure for the UMP Super Admin user.
SNMP Alarm	acUmpSuAdminAuthFailEvent

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.43		
Alarm Title	UMP Super Admin Authentication Fail Event		
Alarm Source	Virtual machine of UMP installation platform		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	Corrective Action
Critical	There is a user authentication failure for the UMP Super Admin user.	SuperAdmin authen-tication failure (Service Provider)	

UMP Azure AD Sync Alarm

Alarm Field	Description		
Description	This alarm is raised when synchronization between the UMP virtual machine and the Azure Active Directory fails.		
SNMP Alarm	acUmpAzureADSyncAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.45		
Alarm Title	UMP Azure ADSync Alarm		
Alarm Source	Virtual machine of UMP installation platform/CustomerID (Customer Name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Customer ID		
Alarm	Condition	Text	CorrectiveAction

Alarm Field	Description		
Severity			
Major	Synchronization with the Azure Active Directory fails.	Azure AD sync alarms	

UMP Office 365 Failure Alarm

Alarm Field	Description		
Description	This alarm is raised when the UMP virtual machine loses the connection with the Office 365 platform i.e. Office 365 credentials failure.		
SNMP Alarm	acUmpO365FailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.46		
Alarm Title	UMP O365 Failure Alarm		
Alarm Source	Virtual machine of UMP installation platform/CustomerID (Customer Name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Customer ID		
Alarm Severity	Condition	Text	Corrective Action
Major	The UMP loss the connection with Office 365 platform i.e. Office 365 credentials failure.	O365 Alarm (Connection failure & Sync)	

UMP Office 365 Command Execution Event

Alarm Field	Description
Description	This alarm is raised when any PowerShell command run on the UMP platform fails.
SNMP Alarm	acUmpO365CommandExEvent

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.48		
Alarm Title	Ump O365 Command Ex Event		
Alarm Source	Virtual machine of UMP installation platform/CustomerID (Customer Name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Execution Result		
Alarm Severity	Condition	Text	Corrective Action
Minor	This alarm is raised when any PowerShell command run on the UMP platform .		

UMP User Settings Fail Event

Alarm Field	Description		
Description	This alarm is raised when a user editing operation fails (Field Edit user).		
SNMP Alarm	acUmpUserSettingsFailEvent		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.49		
Alarm Title	UMP User Settings Fail Event		
Alarm Source	Virtual machine of UMP installation platform /CustomerID (Customer Name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Execution result		
Alarm Severity	Condition	Text	Corrective Action

Alarm Field	Description		
Minor	A user editing operation fails.	User set-tings fail	

UMP End User Authentication Fail Event

Alarm Field	Description		
Description	This alarm is raised when there is an authentication failure for the UMP Admin End User .		
SNMP Alarm	acUmpEndUserAuthFailEvent		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.50		
Alarm Title	UMP End User Authentication Fail Event		
Alarm Source	Virtual machine of UMP installation platform /CustomerID (Customer Name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Admin User Name		
Alarm Severity	Condition	Text	Corrective Action
Minor	Authentication failure (reject or fail) for UMP Admin user.	Admin authentication failure	

CloudBond 365 Alarms

Commit License Failed

Alarm Field	Description
Description	This alarm is raised when the OVOC Main Agent is unable to store the license in the Active Directory.

Alarm Field	Description
SNMP Alarm	acCbManLicenseCommitAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.1
Alarm Title	Commit License Failed
Alarm Source	N/A
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Severity	Condition	Text	CorrectiveAction
Major	Unable to store the license in the Active Directory	Unable to commit the license in Active Directory.	Verify that OVOC 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.	-	

Admin License Expired

Alarm Field	Description
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 Title	Admin License Expired
Alarm Source	N/a

Alarm Field	Description		
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	-	-

CCE Appliance Alarms

Alarm – Admin System Cloud Status

Alarm Field	Description		
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 Title	Alarm – Admin System Cloud Status		
Alarm Source	N/A		
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}	-

Alarm Field	Description		
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	-

CCE Appliance Certificate Expired Alarm

Alarm Field	Description		
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 Title	CCE Appliance Certificate Expired Alarm		
Alarm Source	N/A		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		

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 <daysleft> days	Open certificate manager. Find the expired certificate and renew it.
Cleared	When cer-	-	-

Alarm Field	Description	
	tificate renewed	

CCE Wrong Operating Alarm

Alarm Field	Description		
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 Title	CCE Wrong Operating Alarm		
Alarm Source	<s> (service name {Running Version/OsUpdate/Deployment/VhdFile})		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
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.
	Service returns to operate in the correct mode.	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

Alarm Field	Description		
			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.	-	-

CCE Wrong Settings Alarm

Alarm Field	Description		
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 Title	CCE Wrong Settings Alarm		
Alarm Source	<p> (parameter name {UpdatesMode/MaintenanceMode})		
Alarm Type	Other		-
Probable Cause	Other		-
Alarm Severity	Condition	Text	Corrective Action

Alarm Field	Description		
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 another 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	-	-

CCE Disk Space Alarm

Alarm Field	Description
Description	This alarm is raised when the CCE Application 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 Title	CCE Disk Space Alarm
Alarm Source	Host/C:\
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Field	Description		
Alarm Severity	Condition	Text	CorrectiveAction
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.
Clear	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.

CCE Windows License Alarm

Alarm Field	Description		
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 Title	CCE Windows License Alarm		
Alarm Source	<e> (component name {Ad/Edge/Cms/MS/Host})		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm	Condition	Text	CorrectiveAction

Alarm Field	Description		
Severity			
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'	-	-

SBA Alarms

Alarm – CPU Status

Alarm Field	Description		
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 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

Alarm Field	Description		
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%	-	-

SBA Memory Status

Alarm Field	Description		
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 MByte		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	Available Memory < 7%	High memory usage, available memory is Below 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

Alarm Field	Description		
			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%		

SBA Disk Space Alarm

Alarm Field	Description
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

Alarm Field	Description		
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%	-	

SBA Certificate Expired

Alarm Field	Description		
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 the 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 Type	Other		
Alarm Source	-		
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

Alarm Field	Description		
			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.	-	-

Alarm – Performance Counter

Alarm Field	Description	
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	
SNMP Alarm	acSbaPerfCounterAlarm	
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	-

SBA Services Status Alarm

Alarm Field	Description
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 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.

SBA Services Status Alarm

SmartTAP Alarms

Alarm – Component Unreachable

Alarm Field	Description		
Description	This alarm is raised in the following circumstances: ■ The OVOC Main Agent is unable to connect to one of the OVOC Client agents. Note that currently the Client agent is only installed on the SmartTAP application server. ■ The SmartTAP Application server is unable to connect to the SmartTAP Web Admin Interface		
SNMP Alarm	acVAManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.1		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	The OVOC Main Agent is unable to connect to one of the installed OVOC Client agents.	Unable to connect to client agent on <SmartTapAS_ FQDN>	
	The SmartTAP Application server is unable to connect to the SmartTAP Web Admin interface.	Unable to Connect to Voice Application Admin	
Cleared	OVOC Client agent is re-available		

SmartTAP Event – Component Restart

Alarm Field	Description		
Description	This event is raised when the SmartTAP Application server has been restarted.		
SNMP Alarm	acVAManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.2		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	The SmartTAP Application server has been restarted.	Component <SmartTap AS FQDN> restarted	-

Event – Component Resource Failed

Alarm Field	Description
Description	This event is raised in the following circumstances: ■ The allocation of resources for recording licenses has been exceeded ■ Media Server management has failed
SNMP Alarm	acVaCompResFailedEvent
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.9
Alarm Source	SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following: ■ Licenses: ✔ imLicQuotaExceeded

Alarm Field	Description
	✔ videoLicQuotaExceeded ✔ userLicQuotaExceeded ✔ mediaFwdLicQuotaExceeded ✔ licUnavailable ■ Media Server Resource Failure: ✔ Hmp - channelResourceFailure ✔ Hmp createFileFailed ✔ Hmp bindingFailure ✔ Hmp rtsTransferFailed ✔ Hmp writeFileFailed
Alarm Title	Component Resource Error
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Severity	Condition (related resource indicated in parenthesis)	<text>	Corrective Action
Major	The quota for the number of users targeted for Instant Messaging has been exceeded (imLicQuotaExceeded).	IM target quota exceeded	Reduce the number of users/devices targeted for Instant Messaging recording or purchase additional licenses.
Major	The quota for the number of users targeted for video has been exceeded (videoLicQuotaExceeded).	video target quota exceeded	Reduce the number of users/devices targeted for video recording or purchase additional licenses.

Alarm Field	Description		
Major	The quota for the number of users/devices targeted for audio recording has been exceeded (userLicQuotaExceeded).	Audio User target license exceeded	Reduce the number of users/devices targeted for audio recording or purchase additional licenses.
Major	The quota for the number of users/devices targeted for audio recording has been exceeded (mediaFwdLicQuotaExceeded).	Recording license exceeded	Reduce the number of users/devices targeted for audio recording or purchase additional licenses.
Major	No license is available. All licenses are currently consumed (licUnavailable).	-	-
Major	The Media server failed to create a channel resource (Hmp - channelResourceFailure).	Media server failed to create channel resource	-
Major	The Media Server failed to write to disk (Hmp createFileFailed).	-	Check available disk space. Check that Media Server has read/write permissions on the local disk.
Major	Media Server cannot bind to ports in order to open media channels (Hmp bindingFailure).	-	Verify that other applications are not using UDP ports in the range of 40000 – 50000. Restart Media Server.
Warning	Transfer Server failed to copy files from temporary, local recording location to remote storage (Hmp	Transfer service failed to copy	Verify that the Remote Transfer Service is running

Alarm Field	Description		
	rtsTransferFailed).		with permissions that grant it read/write access to the media storage volume.
Major	The Media server failed to create a file with recorded media (Hmp writeFileFailed)	Media server failed to create a file	Check available disk space. Check that Media Server has read/write permissions on the local disk.

Alarm - Component Resource Threshold Exceeded

Alarm Field	Description
Description	This alarm is raised when one of the SmartTAP component resources listed below has reached its pre-defined threshold. This alarm applies for the following resources: ■ Recording license notification thresholds (for all recording license types) triggered according to the configuration in the SmartTAP Web interface License screen. ■ Media Storage notification thresholds triggered according to the configuration in the SmartTAP Web interface Storage Statistics screen.
SNMP Alarm	acVaResourceThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.11
Alarm Source	SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following: ■ SmartTAP License Threshold Notification value (for all recording license types) ■ Media Storage Notification Threshold value
Alarm Title	Alarm - Component Resource Threshold Exceeded
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
Additional Info	-		
Alarm Severity	Condition	\<text\>	Corrective Action
Critical/Major/Warning	The media storage location threshold has been reached.	Media Storage threshold	■ Verify the Notification Threshold setting configuration in the Storage Statistics screen. It's possible that there is sufficient storage and that the threshold needs to be adjusted. ■ Add additional storage capacity to the file server to support additional media files (recordings). The file server is external to SmartTAP.
	License threshold exceeded	licThresholdExceeded	■ Verify the Notification Threshold setting configuration in the License screen. It's possible that there are sufficient licenses and

Alarm Field	Description		
		that the threshold needs to be adjusted. ■ Purchase additional recording licenses	
Cleared	When counter returns below the threshold level.	-	-

Alarm – Connection Failure

Alarm Field	Description
Description	This alarm is raised in the following circumstances: ■ The connection between one of the SmartTAP components and the SmartTAP Application server is down. ■ The connection between other SmartTAP components is down.
SNMP Alarm	acVaConnectionFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.12
Alarm Source	<SmartTAPComponent>@ <FQDN>: ■ AC-MediaProxy @<FQDN> ■ AC-Annoucement @ <FQDN> ■ CS@ <FQDN> ■ CD-IP@ <FQDN> ■ CD-SIPREC@ <FQDN> ■ MediaDelivery@ <FQDN> ■ Media Server@<FQDN> ■ AC_HealthMonitor@ <FQDN>

Alarm Field	Description
	■ AC-Plugin@ <FQDN> ■ RTS@ <FQDN>
Alarm Title	Alarm – Connection Failure
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Communication between SmartTAP component and SmartTAP Application server is down	Communication Down Details: Managed Device <SmartTAPComponent>@<HostNameFQDN> failed to send heartbeat within specified time of <xxmS>.Device InfoId: <SmartTAPInternalID>HostNameType: COM_SERVERDisplay Name: <HostName>Last heartbeat received on <yyyy-mm-dd> <hh:mm>	
	Connection from CallDelivery to lyncPlugInServerConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost con-nection to FE Plug-using TCP	
	Connection from CallDelivery to lyncPlugInSWConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost con-nection to SmartWorks Plug-using TCP	
	Connection from CallDelivery to communication server	Communication Down Details: Call Delivery at <HostNameFQDN> lost con-nection to communication server Plug-using TCP	

Alarm Field		Description
	Connection from CallDelivery to Media delivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to Media delivery using TCP
	Connection between Media Proxy and Calldelivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to Media Proxy	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to CallDelivery	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to Call Delivery at <HostNameFQDN> using TCP
	Connection from Lync plugin to ann	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to Annoucement Server at <HostNameFQDN> using TCP
Cleared	-	The connection is up again -

Call Recording Error Event

Alarm Field	Description
Description	This event is raised when errors are reported by the Health Monitor to the SmartTAP Application server.
SNMP Alarm	acVaCallRecordingErrorEvent
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.13

Alarm Field	Description		
Alarm Title	Call Recording Error Event		
Alarm Source	SmartTAPAS_FQDN		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	One of the following Health Monitor services reported an error to the SmartTAP Application server	as below	-
	NoMediaFile(301)	Call not recorded or recorded with errors	Check ST configuration and health
	NoFileOnDisk(302)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallWarning(303)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallNotRecorded(304)	Call not recorded	Check ST configuration

Alarm Field	Description		
	or recorded with errors		and health
FileXferFailed(204)		Error: Can't upload file to blob	■ Check Media location configuration in SmartTAP ■ Check Azure Blob accessibility and health
CreateCallFailed (207)		Start call event did not reach AS after retries	Check connectivity to AS
TerminateCallFailed(208)		Release event did not reach AS after retries	Check connectivity to AS
Com-pli-anceRecordedButNotAssignedToRecProfile (209)		User is targeted but has no recordin g profile in ST	Assign Recording Profile to user under Compliance Recording Policy
JoinCallFailed(210)		Bot failed to join the call	■ Check Service Fabric Cluster health ■ Verify MSFT Graph API accessibility

Alarm Field	Description		
			and responsiveness
Clear			

Alarm – Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when one of the Microsoft Windows-certificates installed on the SmartTAP Application server is about to expire.		
SNMP Alarm	acVaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.27		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Raised when the certificate will expire in less than two days	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Major	Raised when the certificate will expire in less than 30 days.	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Cleared	When certificate is renewed	-	-

Alarm – Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped

Alarm Field	Description
	after the sending rate threshold has been exceeded; preventing a burst of events being raised for a specific component.
SNMP Alarm	acVaCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.26
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Alarm Text	Events from Event Viewer dropped due to high sent rate
Additional Info	-
Alarm Severity	Indeterminate

Alarm – Component Performance Counter General

Alarm Field	Description
Description	This alarm is raised when the generic performance counter on the SmartTAP Application server has reached a pre-defined threshold for memory/CPU/disk.
SNMP Alarm	acVACompPcGenAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.21
Alarm Source	SmartTapAS_<FQDN>/<Performance Monitor Group>/<Performance Monitor Name>/<NetworkAdapterName>
Alarm Title	Component Performance Counter General

Alarm Field	Description			
Alarm Type	QualityOfServiceAlarm			
Probable Cause	Other			
Additional Info	-			
Alarm Severity	Condition	<text>		Corrective Action
Critical	Pre-defined severity per counter type.	GeneralCounter performance counter <Per-form-anceCoun-ter-Group/<Per-formanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>		-
Major	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>		-
Warning	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>		-
Cleared	When counter	-		

Alarm Field	Description	
returns below the threshold level.		

Alarm – Component Service Status

Alarm Field	Description
Description	This alarm is raised when a component service on the SmartTAP Application server is down. These services include SmartTAP components, for example, HealthMonitorSvc and core Windows components, for example, AcProcDump.
SNMP Alarm	acVaCompSrvAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.23
Alarm Source	SmartTapAS_<FQDN>/<servicename> is one of the following: ■ AudioCodes_CS ■ MySQL ■ CallDelivery-IP ■ HealthMonitorSvc ■ AudioCodesMPSvc ■ HPXMedia ■ RemoteTransferService ■ AcProcDump ■ CallDeliverySR ■ CallDelivery ■ CallDeliveryLD ■ CallDeliveryAES ■ SmartTapMonitoringSvc

Alarm Field	Description		
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.			

Alarm – Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on the SmartTAP Application Server drive is above the pre-defined threshold.		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.28		
Alarm Source	SmartTAPAS_<FQDN>/DriveName:\\		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/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.	-	-

Alarm – Disk Space

7   ARM Alarms

Disk Size Illegal

Alarm Field	Description
Description	This alarm is raised when the disk size defined for the ARM Configurator or Router is insufficient for ARM requirements.
SNMP Alarm	acARMDiskSize
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.4
Alarm Title	Disk Size Illegal
Alarms Source	■ Configurator ■ Router# <Routername>
Alarm Type	integrityViolation
Probable Cause	storageCapacityProblem

Alarm Severity	Condition	Text	Corrective Action
Critical	The size of the hard disk of the ARM Configurator or Router is insufficient for ARM requirements.	The size of the hard disk in <Configurator or Router->/<Configurator or Router Name> was changed to an illegal size <CurrentSize>. Minimum is <Min-imumSize> .	Increase VM disk size according to the requirements specified in the ARM Installation manual.

Disk Space Usage

Alarm Field	Description
Description	This alarm is raised when the disk usage reaches a high level
SNMP Alarm	SNMP Alarm acARMDiskSpaceUsage
SNMP OID	SNMP OID 1.3.6.1.4.1.5003.9.70.1.2.2.0.3

Alarm Field	Description
Alarm Title	Disk space usage
Alarms Source	ARM / Partition #partitionName or Router #routerName / Partition #partitionName
Alarm Type	Environmental Alarm
Probable Cause	Storage Capacity Problem

Alarm Severity	Condition	Text	Corrective Action
Indeterminate	■ 'Almost full' is sent when the usage is more than 95% (Critical). ■ 'Dangerously high' is sent when the usage is more than 80% (Warning).	The disk usage of {elementType} {elementName} is dangerously high / almost full (in %) {elementType} can be Configurator or router.	■ Clean disk from obsolete data. ■ Delete old and unused logs and backup files ■ In case of watchdog reload delete the created heap file (/tomcat/tmp). ■ If the calls feature is enabled and the size of the calls is large according to the logs (log cdr) or check the Mongo DB folder in your VM (/var/lib/mongo), disable the feature, reduce the number of CDR calls in Calls Settings and contact your AudioCodes representative.

ARM License About to Expire

Alarm Field	Description
Description	This alarm is raised when the ARM license is about to expire.

Alarm Field	Description
SNMP Alarm	acARMLicenseAboutToExpire
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.5
Alarm Title	ARM License about to expire
Alarms Source	Configurator
Alarm Type	Operational Violation
Probable Cause	Key Expired
Alarm Severity	Condition
Major	■ This alarm is initially raised 28 days before the expiration date of the license and then for each subsequent day prior to the expiration date.

ARM License has Expired

Alarm Field	Description
Description	The ARM license has expired.
SNMP Alarm	acARMLicenseHasExpired
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.6
AlarmTitle	ARM License has expired
AlarmSource	Configurator
AlarmType	Operational Violation
Probable Cause	Key Expired
Alarm Text	■ Alarm License has expired ■ Alarm License is OK
Severity	Critical
Additional Info	-
Corrective Action	Contact your AudioCodes representative to update your ARM license.

ARM License Session Number

Alarm Field	Description		
Description	This alarm is raised when the number of sessions is approaching the licensed limit and when the limit has been exceeded.		
SNMP Alarm	acARMLicenseSessionNumber		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.9		
Alarm Title	ARM License session number		
Alarms Source	Configurator		
Alarm Type	Operational Violation		
Probable Cause	Threshold Crossed		
Alarm Severity	Condition	Text	Corrective Action
Major	The number of utilized licenses has reached 90% of the licensed limit.	Number of sessions in ARM has exceeded 90%	Contact your AudioCodes representative to update your ARM license.
Critical	Raised when the number of active sessions has exceeded the licensed limit according to percentage.	Number of active sessions has exceeded #sessions% of the number allowed by the ARM license.	Contact your AudioCodes representative to update your ARM license.
Clear		Number of sessions in ARM is normal	

ARM License Missing

Alarm Field	Description
Description	This alarm is raised when the ARM license is not found.
SNMP Alarm	acARMLicenseMissing
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.10
AlarmTitle	ARM License Missing
AlarmSource	Configurator
AlarmType	Operational Violation
Probable Cause	Key Expired
Alarm Text	■ Alarm License was not found ■ Alarm License was found
Severity	Major
Additional Info	-
Corrective Action	■ Contact your AudioCodes representative ■ Install an ARM license

Quality Change

Alarm Field	Description
Description	This alarm is raised when the quality threshold for a Node connection or a VoIP Peer connection has been crossed.
SNMP Alarm	acARMQualityChanged
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.11
Alarm Title	Quality Change
Alarms Source	Node # <NodeName>/PeerConnection# <PeerName>
Alarm Type	Quality of Service Alarm
Probable Cause	Performance Degraded

Alarm Field	Description
Alarm Text	The Quality of Peer Connection<PeerConnectioName> or Node Connection<NodeConnectioName> was changed to one of the following: ■ Good ■ Fair ■ Bad ■ Unknown
Alarm Severity	Major
Corrective Action	■ Make sure quality thresholds are configured correctly in the ARM settings ■ Validate your network quality in data layer. ■ Contact your network administrator. ■ If you know that you have a problem with a specific element (Connection or Peer Connection) and you don't wish to receive an alarm for this element, you can configure the element to ignore MOS/ASR and not use the global quality definitions in the Peer or Connection properties in the ARM Web interface.

ARM Configurator Reload

Alarm Field	Description
Description	This alarm is raised when the ARM configurator was reloaded by watch-dog.
SNMP Alarm	acARMTopologyReloaded
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.12
Alarm Title	ARM Configurator Reloaded
Alarms Source	Configurator#<Configuratorname>
Alarm Type	operationalViolation
Probable Cause	Application subsystem failure
Additional	memory dump in /opt/tomcat/temp/-

Alarm Field	Description
Info	
Alarm Severity	Condition
Major	■ The Tomcat server was not restarted properly. ■ The ARM Configurator didn't respond to the number of keep-alive requests from the watchdog.

ARM Router Reload

Alarm Field	Description		
Description	This alarm is raised when the router was not reloaded successfully.		
SNMP Alarm	acARMRouterReloaded		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.14		
Alarm Title	ARM router reload		
Alarms Source	Router # routerName		
Alarm Type	Operational Violation		
Probable Cause	Application subsystem failure		
Additional Info	Memory dump in /opt/tomcat/temp/		
Alarm Severity	Condition	Text	Corrective Action
Major	■ Tomcat server was not restarted properly ■ Router didn't respond to number of keep-alive requests from the watchdog	ARM router {routerName} was reloaded by watchdog.	■ Collect logs ■ Contact your AudioCodes representative

ARM Routing Rule Match

Alarm Field	Description
Description	This event is raised when a Routing rule for a specific element is matched. ⚠️ These events are sent when the "Notify When activated"check box is selected for the Routing Rule in the ARM Web interface (Advanced Conditions tab).
SNMP Alarm	acARMRoutingRuleMatch
SNMP OID	.1.3.6.1.4.1.5003.9.70.1.2.2.0.13
Alarm Title	Routing Rule match
Alarms Source	Router#<RouterName>
Alarm Type	Other
Probable Cause	Other
Additional Info	■ Routing Rule <ruleName> of Group <groupName> is matched. ■ Call from Pcon <PeerConnectionName>, Node <nodeName> – From number <fromNumber>, to <toNumber>.
Alarm Text	Routing Rule <rule name> was matched
Alarm Severity	indeterminate
Corrective Action	Disable the notification in the routing rule if you don't wish to view this event.

ARM Configuration Inconsistency

Alarm Field	Description
Description	This event is raised when there is mismatch between a Peer connection or a Routing Interface configuration and a Node configuration.
SNMP Alarm	acARMConfigurationInconsistency

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.1.0.1
Alarm Title	Configuration Inconsistency
Alarms Source	Node #<NodeName>/PeerConnection#<PeerConnectionName> Node#<NodeName>/RoutingInterface#<RoutingInterfaceName>
Alarm Type	Processing Error Alarm
Probable Cause	Configuration or Customization Error
Additional Info	ARM database was synchronized to the nodes configuration
Alarm Severity	Condition
Indeterminate	■ An inconsistency was discovered between the ARM Topology and the SBC or gateway configuration. ■ The element was added to the SBC and discovered by ARM during the synchronization process.

Operation State Changed (Router)

Alarm Field	Description
Description	This alarm is raised when the router state has changed and when an associated Web Service is unavailable, for example call masking for DID and 911 calls.
SNMP Alarm	acARMOperationStatusChanged
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1
Alarm Title	Operation Status Changed
Alarms Source	Router#<RouterName> Router#<router name>/Web Service#<the name of the service>
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure
Additional Info	The alarm is cleared once the status is changed back to available.

Alarm Field	Description		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Major	The router is not synchronized with the ARM Configurator.	Router <RouterName>was marked as Not_Sync.	In case state is unavailable: ■ Check router status and availability. ■ Network connectivity between configurator and router. ■ Validate that proper Router credentials updated in ARM. ■ Validate DNS setting in case hostname is used.
Major	The router is initializing with the ARM Configurator.	Router <RouterName>was marked as Initializing	
Major	The configured memory in the router is less than the size required by the license.	Router <RouterName> was marked as not in service due to memory requirements.	This occurs when the number of users does not match the memory requirements. Refer to User's manual / Installation Guide for more information regarding how increase the memory.

Alarm Field	Description		
Major	An external Web Service associated with this router is unavailable.	Web Service <Web service name> was marked as Unavailable	
Cleared	The router is re-available	Router <RouterName>was marked as Available.	

Operation Status Changed [Node]

Alarm Field	Description		
Description	This alarm is raised when the operative state of a specific Node has changed.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarms Source	■ Node#<NodeName>/Router#armServer ■ (For IP Profile issues) Node#<NodeName>		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info	The alarm will be cleared once the status will be changed back to available. Added the routing server to the node		

Alarm Severity	Condition	Text	Corrective Action
Major	The Routing server node is unavailable.	Routing Server armServer in Node <Node Name> was marked as Unavailable	■ Check device network connectivity ■ Check the device's network connectivity to

Alarm Field	Description	
		the ARM Configurator
	The Routing server node is Unrouteable.	Routing Server armServer in Node <Node Name> was marked as Unrouteable	■ Check the device's network connectivity to the ARM routers ■ Check the routers' status and availability
	The Routing server node is Logged out.	Routing Server armServer in Node <Node Name> was marked as Logout.	■ Check the configuration of the device's ARM service.
	The ARM IP Profile is marked as unavailable.	IP Profile ARM_ IP_Profile in <Node Name> Node was marked as Unavailable	■ Check if the IP Profile exists on the device node specified in the Alarm text. If yes, remove it and resync the node. ■ Check the syslog and ARM log files for the error and contact support.
Cleared		Node <NodeName> was marked as <Status>	

Operation Status Changed [Peer Connection]

Alarm Field	Description
Description	This alarm is raised when the operative state of the VoIP Peer Connection has changed.
SNMP Alarm	acARMOperationStatusChanged
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1
Alarm Title	Operation Status Changed
Alarms Source	Node #<NodeName>/<PeerConnection#<PeerName>
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure
Additional Info	The alarm will be cleared once the status will be changed back to available.

Alarm Severity	Condition	Text	Corrective Action
Major		Peer Connection in Node <Node Name> was marked as Unavailable	When this alarm is received from a Peer Connection and it indicates that the operative state of the Peer Connection has changed to Unavailable: ■ Check the configuration of the related IP Group in the specific device. ■ Check the device's network connectivity to the configured

Alarm Field	Description		
	- 260 -		Proxy IP associated with that IP Group
Cleared		Peer<PeerName> was marked as Available	

Operation Status Changed [LDAP Server]

Alarm Field	Description
Description	This alarm is generated when the LDAP server is disconnected or reconnected.
SNMP Alarm	acARMOperationStatusChanged
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1
Alarm Title	Operation Status Changed
Alarms Source	LDAP server # <LDAPServerName>
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure
Additional Info	The alarm will be cleared once the status is changed back to available.

Alarm Severity	Condition	Text	Corrective Action
Major		LDAP Server <LDAPServerName> was marked as Unavailable.	This alarm is raised when LDAP server state has turned to unavailable: ■ Check the LDAP server network connectivity. ■ Validate LDAP server

Alarm Field	Description		
		credentials.	
Cleared		LDAP Server <LDAPServerName> was marked as Available.	

Operational Status Changed [Active MQ]

Alarm Field	Description
Description	This alarm is generated when there is a problem with the JMS broker on the ARM Configurator.
SNMP Alarm	acARMOperationStatusChanged
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1
Alarm Title	Operation Status Changed
Alarms Source	Configurator
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure
Additional Info	Failed sending three consecutive messages to the JMS, going to reload

Alarm Severity	Condition	Text	Corrective Action
Critical	Configurator could not send three consecutive messages to the ActiveMQ broker.	ActiveMQ Connection was marked as Unavailable.	The ActiveMQ should be restarted automatically. If the alarm doesn't clear after a period of time: ■ Check that the ActiveMQ service is working properly

Alarm Field	Description
	■ Collect ActiveMQ logs ■ Contact your AudioCodes representative

Limit Reached

Alarm Field	Description
Description	This alarm is raised when the number of users has exceeded the maximum allowed number (250000).
SNMP Alarm	acARMLimitReached
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.2
Alarm Title	Limit reached
Alarms Source	Configurator/users
Alarm Type	Operational Violation
Probable Cause	Threshold Crossed
Alarm Text	Maximum users <MaximumUsers> is Reached Maximum users <MaximumUsers> is OK
Additional Info	
Alarm Severity	Major

Router Using Other Configurator

Description	This alarm is raised when the ARM router is connected to an incorrect Configurator.
SNMP Alarm	acARMRouterUsingOtherConfigurator

SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.7
Alarm Title	Router Using Other Configurator
Alarms Source	Router #<RouterName>
Alarm Type	Operational Violation
Probable Cause	Denial Of Service
Additional Info	Contact your AudioCodes representative.

Alarm Severity	Condition	Text	Corrective Action
Critical		Router <RouterName> is already connected to another configurator <otherIPAddress>	Two configurators are trying to use the router at the same time: ■ Check the IP of another configurator, {otherAddress} in the description and make sure only one of them uses the router. ■ Restart the tomcat service in the router machine.

NTP Sync Status

Alarm Field	Description
Description	This alarm is raised when the clock on the ARM Configurator or Router is not synchronized with the NTP server. The NTP clock is critical for ARM services as it impacts license, routing (time conditions) and statistics: ■ IP connectivity to the NTP server ■ Firewall configuration

Alarm Field	Description
	■ NTP server configuration
SNMP Alarm	acARMNTPSyncStatus
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.8
AlarmTitle	NTP sync status
AlarmType	Time Domain Violation
AlarmSource	■ Configurator#<Configuratorname> ■ Router #<Routername>
Probable Cause	Timing Problem
Alarm Text	■ The NTP clock on the ARM Configurator is not synchronized with NTP server ■ The NTP clock on ARM Configurator is synchronized with NTP server
Severity	Major
Additional Info	-
Corrective Action	■ Check the NTP configuration in the ARM Web interface. ■ Check for connectivity issues with the NTP server configured in the NTP Servers tab in the ARM Web interface.

No Available Routers

Description	This alarm is raised if all preconfigured ARM Routers become unavailable or disconnected. The alarm is cleared when at least one ARM Router returns to service.
SNMP Alarm	acARMNoAvailableRouter
SNMP OID	3.6.1.4.1.5003.9.70.1.2.2.0.15
Alarm Title	No available routers
Alarms Source	Configurator
Alarm Type	Communications Alarm

Probable Cause	Communications Subsystem Failure		
Additional Info			
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	When there are no routers in the system or when all defined routers are unavailable	Currently there are no available routers in the system.	■ Make sure that at least one router is configured in your system. ■ Check router status and availability. ■ Network connectivity between configurator and router. ■ Validate that proper Router credentials updated in ARM. ■ Validate DNS setting in case hostname is used.
Clear	When there is at least one available router		

Registration Status Resync Threshold

Description	This alarm is raised when the number of registered user resync attempts is over the defined limit (three attempts).
SNMP Alarm	acARMRegistrationStatusResyncThreshold
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.16

Alarm Title	Registration Status Resync Threshold		
Alarms Source	ARM		
Alarm Type	communicationsAlarm		
Probable Cause	softwareProgramError		
Additional Info			
Alarm Severity	Condition	Text	Corrective Action
major	The number of registered user resync attempts is over the default limit of three.	The number of registration users resync attempts crossed the threshold for node #elementName	
clear			

External Web Service

Description	This alarm is raised when an external web service is unavailable. For example, call masking for DID and 911 calls.
SNMP Alarm	acARMExternalWebService
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.17
Alarm Title	External Web Service
Alarms Source	Web Service#<the name of the service>
Alarm Type	Other
Probable Cause	Other
Additional Info	

Alarm Severity	Condition	Text	Corrective Action
Minor	Raised when an external web service is unavailable.	"Web Service <Web service name> was marked as Unavailable"	
Clear	External Web Service becomes available.		

Disk Usage Alarm

Description	This alarm is raised when the cumulative duration of all calls for a peer connection or resource group reaches the limit defined in the Calls Quota that is attached to these entities. In addition, a warning is raised when the duration reaches the user-defined threshold		
SNMP Alarm	acARMCallsDurationQuotaUsage		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.18		
Alarm Title	Calls duration quota usage		
Alarms Source	■ Node#<NodeName>/PeerConnection#<PeerConnectionName> ■ Resource group#<ResourceGroupName>		
Alarm Type	Other		
Probable Cause	Threshold Crossed		
Additional Info			
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Calls quota limit has been reached.	{elementType} {elementName} calls quota limit/threshold has been reached.	■ Make sure that the calls quota has been configured as required. If not, do one of the following:

			✔ Delete the Calls Quota limit for the Peer Connection or Resource Group ✔ Adjust the Calls Quota limit or Time Scheduling for the Peer Connection or Resource Group
Warning	Calls quota threshold has been reached The threshold is configurable, 75% by default	{elementType} {elementName} calls quota threshold has been reached.	■ Make sure that the calls quota threshold has been configured as required. If not, do one of the following: ✔ Delete the Calls Quota for the Peer Connection or Resource Group ✔ Change the Threshold for the Peer Connection or Resource Group
Clear	■ Calls Quota has been deleted from the Peer Connection ■ Calls Quota has been deleted from the		

	Resource Group ■ New time period has started (according to Time Scheduling defined in the Calls Quota) ■ Time Scheduling in Calls Quota definition has been modified. For example, set to "monthly" instead of "daily" ■ Modifying Limit in Calls Quota definition results in alarm clearing for specific peer connections or resource groups (i.e. for those entities with the Calls Quota applied that fall within limit/threshold when its extended)		

This page is intentionally left blank.

Document #: LTRT-41616