Reference Guide

AudioCodes Multi-Service Business Router Series

SNMP Alarms

MSBR Series

Version 7.2

audiocodes

Notice

Date Published: June-15-2023

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
MSBR Series Release Notes
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual

Document Name
Mediant 800 MSBR User's Manual
MSBR CLI Reference Guide

Document Revision Record

LTRT	Description
52374	Initial document release for Ver. 7.2.
52378	Typos.
52380	MP-1288 added; number of trap varbinds (13); acBoardTrapGlobalsSystemSerialNumber (new); acLicensePoolInfraAlarm (updated); acLicensePoolApplicationAlarm (updated); acLicensePoolOverAllocationAlarm (updated); acTrackIdStateChangeAlarm (new); acModuleServiceAlarm; acClusterBandwidthAlarm (new); acSBAServicesStatusAlarm (updated); acKeepAlive (updated); acProxyConnectivity (updated)
52381	SBA-related SNMP removed (added to SBA documents).
52383	Typos; varbinds increased to 16 (new - acBoardTrapGlobalsDeviceName, acBoardTrapGlobalsDeviceInfo, acBoardTrapGlobalsDeviceDescription); acLicensePoolInfraAlarm (description updated); acLicensePoolApplicationAlarm (description updated); acLicenseKeyHitlessUpgradeAlarm (new)
52384	Source names added for PM MIB names; event source added to acPerformanceMonitoringThresholdCrossing; description updated for entConfigChange
52385	Source name for acPMSBCIPGroupInCallEstablishedDurationTable; Media Transcoding Cluster removed
52386	Updated descriptions: acPowerSupplyAlarm; acHwFailureAlarm; acHASystemFaultAlarm; acHASystemSwitchOverAlarm New alarm -acHANetworkMonitorAlarm
52389	Updated to Ver. 7.20A.200.019 New traps: acHAEthernetGroupAlarm; acHANetworkMismatchAlarm; acNGINXConfigurationIsInvalidAlarm; acNGINXPprocessIsNotRunningAlarm Updated traps: acHwFailureAlarm; acHASystemFaultAlarm; acHANetworkMonitorAlarm (OID); acHTTPProxyServiceAlarm

LTRT	Description
52391	Updated to Ver. 7.20A.202.112 Updated traps: AcPowerSupplyAlarm; acBoardTemperatureAlarm; acCertificateExpiryNotification changed to acCertificateExpiryAlarm; acLicensePoolApplicationAlarm; acIpGroupNoRouteAlarm; acIDSPolicyAlarm; acKeepAlive New traps: acCloudLicenseManagerAlarm; acFloatingLicenseAlarm Performance Monitoring - updated
52392	Updated to Ver. 7.20A.204.115 acAWSSecurityRoleAlarm
52393	acDataInterfaceStatus removed; acNATTraversalAlarm removed
52394	OIDs of performance monitoring MIBs; acProxyConnectionLost updated (severity); SNMPSysName updated
52395	Updated for Ver. 7.20A.252 Configuring performance monitoring thresholds; coder enums for acPMChannelsPerCoderTable; new acAnalogLineLeftOffhookAlarm; acIpGroupNoRouteAlarm (description updated); new PM MIBs (acPMActiveContextCountTable, acPMSBCInAttemptedCallsTable, acPMSBCOutAttemptedCallsTable, acPMSBCInEstablishedCallsTable, acPMSBCOutEstablishedCallsTable, acPMSBCMediaBrokenConnectionCallsTable, acPMSBCInShortCallsTable, acPMSBCOutShortCallsTable, acPMSBCInAttemptedRegistrationsTable, acPMSBCOutAttemptedRegistrationsTable, acPMSBCInSuccessfulRegistrationsTable, acPMSBCOutSuccessfulRegistrationsTable, acPMSBCIPGroupMediaBrokenConnectionCallsTable, acPMSBCIPGroupInShortCallsTable, acPMSBCIPGroupOutShortCallsTable, acPMSBCIPGroupInAttemptedRegistrationsTable, acPMSBCIPGroupOutAttemptedRegistrationsTable, acPMSBCIPGroupInSuccessfulRegistrationsTable, acPMSBCIPGroupOutSuccessfulRegistrationsTable, acPMSBCSRDInAttemptedCallsTable, acPMSBCSRDOutAttemptedCallsTable, acPMSBCSRDInEstablishedCallsTable, acPMSBCSRDOutEstablishedCallsTable, acPMSBCSRDMediaBrokenConnectionCallsTable, acPMSBCSRDInShortCallsTable, acPMSBCSRDOutShortCallsTable, acPMSBCSRDInAttemptedRegistrationsTable, acPMSBCSRDOutAttemptedRegistrationsTable, acPMSBCSRDInSuccessfulRegistrationsTable, acPMSBCSRDOutSuccessfulRegistrationsTable, acPMSBCInUserDefinedFailures<1-26>Table,

LTRT	Description
	acPMSBCOutUserDefinedFailures<1-26>Table, cPMSBCSRDInUserDefinedFailures<1-26>Table, acPMSBCSRDOutUserDefinedFailures<1-26>Table, acPMSBCIPGroupInUserDefinedFailures<1-26>Table, acPMSBCIPGroupOutUserDefinedFailures<1-26>Table, acPMSBCInCapsTable, acPMSBCOutCapsTable, acPMSBCSrdInCapsTable, acPMSBCSrdOutCapsTable
52396	acCDRServerAlarm alarm added
52397	Updated to Ver. 7.20A.254 AcFanTrayAlarm and acBoardTemperatureAlarm updated for Mediant 90xx; CLI command added to acBoardOverloadAlarm
52398	Typo fixed for acPMSIPSBCEstablishedCallsTable
52399	Updated to Ver. 7.20A.256.024 New PM MIB - acPMChannelsPerCoderG711Table; AcDSPFarmsMismatchAlarm (new); acRemoteMonitoringAlarm (new); acBoardEvResettingBoard (text updated); acMtcmClusterHaAlarm (updated); acMtceNetworkFailureAlarm (updated); acMtceSwUpgradeFailureAlarm (updated); acMediaClusterAlarm (new).
52428	Updated to Ver. 7.20M1.256.029; acFloatingLicenseAlarm (new); acCloudLicenseManagerAlarm (new); acWirelessCellularModemStatusChanged (updated for LTE) Miscellaneous typos; acBoardEthernetLinkAlarm (description); acEthernetGroupAlarm (description); acFeatureKeyError (not supported note removed).
52429	AcDChannelStatus moved to alarms and description updated
52461	Text updated of acNqmLqMosAlarm and acNqmCqMosAlarm.
52486	acNoReplyFromDNSServerAlarm; acSBCCallAttemptsPerSecTable; acPMCPCallAttemptsPerSecTable
52456	Dedicate alarms guide (from Ver. M9.1); acProxyConnectivity description updated

Table of Contents

1 Introduction

This document describes the Simple Network Management Protocol (SNMP) traps (events and alarms) that can be sent by AudioCodes Multi-Service Business Routers (MSBR), referred hereafter as *device*.

- The SNMP MIB manual is supplied in the Software Release Package delivered with the device.
- For configuring SNMP through the Web interface, see the device's User's Manual.

Carrier-Grade Alarm System

The basic alarm system has been extended to a carrier-grade alarm system. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account EMS outages, network outages, and transport mechanism such as SNMP over UDP.

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

- The device allows an EMS to determine which alarms are currently active in the device. That is, the device maintains an active alarm table.
- The device allows an EMS to detect lost alarms and clear notifications [sequence number in trap, current sequence number MIB object]
- The device allows an EMS to recover lost alarm raise and clear notifications [maintains a log history]
- The device sends a cold start trap to indicate that it is starting. This allows the EMS to synchronize its view of the device's active alarms.

When the SNMP alarm traps are sent, the carrier-grade alarm system does not add or delete alarm traps as part of the feature. This system provides the mechanism for viewing of history and current active alarm information.

Active Alarm Table

The device maintains an active alarm table to allow an EMS to determine which alarms are currently active in the device. Two views of the active alarm table are supported by the agent:

- acActiveAlarmTable in the enterprise AcAlarm
- alarmActiveTable and alarmActiveVariableTable in the IETF standard AcAlarm MIB (rooted in the MIB tree)

The acActiveAlarmTable is a simple, one-row per alarm table that is easy to view with a MIB browser.

Alarm History

The device maintains a history of alarms that have been sent and traps that have been cleared to allow an EMS to recover any lost raise or clear traps. Two views of the alarm history table are supported by the agent:

- acAlarmHistoryTable in the enterprise AcAlarm - a simple, one-row per alarm table, that is easy to view with a MIB browser.
- nlmLogTable and nlmLogVariableTable in the standard NOTIFICATION-LOG-MIB

SNMP Traps Overview

This section provides an overview of the SNMP traps.

Standard Traps

The device also supports the following standard traps:

- authenticationFailure
- coldStart: The device supports a cold start trap to indicate that the device is starting up. This allows the OVOC to synchronize its view of the device's active alarms. In fact, two different traps are sent at start-up:
  - Standard coldStart trap: iso(1).org(3).dod(6).internet(1). snmpV2(6). snmpModules(3). snmpMIB(1). snmpMIBObjects(1). snmpTraps(5). coldStart(1) sent at system initialization.
  - Enterprise acBoardEvBoardStarted: generated at the end of system initialization. This is more of an "application-level" cold start sent after all the initializing process is over and all the modules are ready
- linkDown
- linkup
- entConfigChange
- dsx1LineStatusChange (Applicable only to digital interfaces)

Proprietary Traps

This section provides information on proprietary SNMP traps supported by the device. There is a separation between traps that are alarms and traps that are not (i.e., logs). All traps have the same structure made up of the same 16 varbinds (Variable Binding), i.e., 1.3.6.1.4.1.5003.9.10.1.21.1. For a list of the varbinds, see Trap Varbinds on the next page.

The source varbind is composed of a string that details the device component from which the trap is being sent (forwarded by the hierarchy in which it resides). For example, an alarm from an SS7 link has the following string in its source varbind: acBoard#1/SS7#0/SS7Link#6. The SS7 link number is specified as 6 and is part of the only SS7 module in the device that is placed in

slot number 1 (in a chassis) and is the module to which this trap relates. For devices where there are no chassis options, the slot number is always 1.

Full proprietary trap definitions and trap varbinds are found in AcBoard MIB and AcAlarm MIB.

All traps are sent from the SNMP port (default 161).

Trap Varbinds

Trap varbinds are sent with each proprietary SNMP trap. Refer to the AcBoard MIB for more information on these varbinds.

Table 1-1: Trap Varbinds for Proprietary SNMP Traps

Trap Varbind	Description
acBoardTrapGlobalsName (1)	Alarm or event number. The number value is obtained from the last digit(s) of the OID of the sent trap, and then subtracted by 1. For example, for the trap acBoardEthernetLinkAlarm, which has an OID of 1.3.6.1.4.1.5003.9.10.1.21.2.0.10, the value of the varbind is 9 (i.e., 10 – 1). The value is an integer from 0 to 1000.
acBoardTrapGlobalsTextualDescription (2)	Description of the reported issue. The value is an octet string of up to 200 characters.
acBoardTrapGlobalsSource (3)	The source of the issue. For example, Trunk#1 or Entity1#x. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsSeverity (4)	Active alarm severity on the device: ■ noAlarm(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5)
AcBoardTrapGlobalsUniqID (5)	Consecutive number count of trap since

Trap Varbind	Description
	device was powered on. The number is managed separately for alarms and events. For example, you may have an alarm whose value is 1 and an event whose value is 1. The value is an integer from 0 to 32000.
acBoardTrapGlobalsType (6)	■ other(0) ■ communicationsAlarm(1) ■ qualityOfServiceAlarm(2) ■ processingErrorAlarm(3) ■ equipmentAlarm(4) ■ environmentalAlarm(5) ■ integrityViolation(6) ■ operationalViolation(7) ■ physicalViolation(8) ■ securityServiceOrMechanismViolation(9) ■ timeDomainViolation(10)
acBoardTrapGlobalsProbableCause (7)	■ other(0) ■ adapterError(1) ■ applicationSubsystemFailure(2) ■ bandwidthReduced(3) ■ callEstablishmentError(4) ■ communicationsProtocolError(5) ■ communicationsSubsystemFailure(6) ■ configurationOrCustomizationError(7) ■ congestion(8) ■ corruptData(9) ■ cpuCyclesLimitExceeded(10) ■ dataSetOrModemError(11) ■ degradedSignal(12) ■ dteDceInterfaceError(13)

Trap Varbind	Description
	■ enclosureDoorOpen(14) ■ equipmentMalfunction(15) ■ excessiveVibration(16) ■ fileError(17) ■ fireDetected(18) ■ floodDetected(19) ■ framingError(20) ■ heatingVentCoolingSystemProblem(21) ■ humidityUnacceptable(22) ■ inputOutputDeviceError(23) ■ inputDeviceError(24) ■ lanError(25) ■ leakDetected(26) ■ localNodeTransmissionError(27) ■ lossOfFrame(28) ■ lossOfSignal(29) ■ materialSupplyExhausted(30) ■ multiplexerProblem(31) ■ outOfMemory(32) ■ ouputDeviceError(33) ■ performanceDegraded(34) ■ powerProblem(35) ■ pressureUnacceptable(36) ■ processorProblem(37) ■ pumpFailure(38) ■ queueSizeExceeded(39) ■ receiveFailure(40) ■ receiverFailure(41) ■ remoteNodeTransmissionError(42) ■ resourceAtOrNearingCapacity(43)

Trap Varbind	Description
	■ responseTimeExecessive(44) ■ retransmissionRateExcessive(45) ■ softwareError(46) ■ softwareProgramAbnormallyTerminated (47) ■ softwareProgramError(48) ■ storageCapacityProblem(49) ■ temperatureUnacceptable(50) ■ thresholdCrossed(51) ■ timingProblem(52) ■ toxicLeakDetected(53) ■ transmitFailure(54) ■ transmitterFailure(55) ■ underlyingResourceUnavailable(56) ■ versionMismatch(57) ■ authenticationFailure(58) ■ breachOfConfidentiality(59) ■ cableTamper(60) ■ delayedInformation(61) ■ denialOfService(62) ■ duplicateInformation(63) ■ informationMissing(64) ■ informationModificationDetected(65) ■ informationOutOfSequence(66) ■ intrusionDetection(67) ■ keyExpired(68) ■ nonRepudiationFailure(69) ■ outOfHoursActivity(70) ■ outOfService(71) ■ proceduralError(72)

Trap Varbind	Description
	■ unauthorizedAccessAttempt(73) ■ unexpectedInformation(74)
acBoardTrapGlobalsAdditionalInfo1 (8)	Provides additional information regarding the reported trap. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsAdditionalInfo2 (9)	Provides additional information regarding the reported trap. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsAdditionalInfo3 (10)	Provides additional information regarding the reported trap. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsDateAndTime (11)	Date and time the trap was sent.
acBoardTrapGlobalsSystemSeverity (12)	The highest alarm severity sent by the device when the trap was sent: ■ cleared(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5)
acBoardTrapGlobalsDeviceName (13)	Name of the device. The value is an octet string of up to 100 characters. **Note:** The device sends an empty string "\0". AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsDeviceInfo (14)	Device information. The value is an octet string of up to 100 characters. **Note:** The device sends an empty string "\0".

Trap Varbind	Description
	AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsDeviceDescription (15)	Device description. The value is an octet string of up to 100 characters. **Note:** The device sends an empty string "\0". AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsSystemSerialNumber (16)	The Serial Number of the device that sent the trap. The value is an octet string of up to 255 characters.

Customizing Trap's Enterprise OID

You can change the enterprise value in the device's SNMP Traps to a variable value, using the ini file parameter [SNMPTrapEnterpriseOid]. This parameter replaces the Traps' OID prefix from 'AcTrap' (1.3.6.1.4.1.5003.9.10.1.21) to user-defined root. All other OIDs remain the same.

For example, the current acBoardEvBoardStarted parameter's OID is '1.3.6.1.4.1.5003.9.10.1.21.2.0.4'. Its prefix ('1.3.6.1.4.1.5003.9.10.1.21') can be changed, and all other OIDs remain the same.

SNMP Alarms in Syslog

SNMP alarms are sent to the Syslog server using the following format.

- **Sent alarms:** RAISE-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >.

  If additional information exists in the alarm, the following are also added: Additional Info1:/ Additional Info2:/ Additional Info3

  The message severity is as follows:

Table 1-2: Message Severity

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
Critical	RecoverableMsg
Major	RecoverableMsg

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
Minor	RecoverableMsg
Warning	Notice
Indeterminate	Notice
Cleared	Notice

- **Cleared alarm:**

  CLEAR-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >; If exists Additional Info1:/ Additional Info2:/ Additional Info3:

2 SNMP Trap Alarms

The tables in the following subsections provide information on alarms triggered as a result of a generated SNMP trap. The component name (described in each of the following headings) refers to the string provided in the acBoardTrapGlobalsSource trap varbind. To clear a generated alarm, the same notification type is sent but with the severity set to 'Cleared'.

- You can customize the severity level of SNMP trap alarms using the Alarms Customization table [AlarmSeverity]. This table also lets you suppress alarms.
- Currently, the acInstallationFailureAlarm trap alarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2) is not supported.

Trunk Alarms

This section describes the SNMP alarms concerned with digital trunk interfaces.

Trunk Near-End LOS Alarm

Table 2-1: acTrunksAlarmNearEndLOS

Alarm	acTrunksAlarmNearEndLOS		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.49		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Severity	Condition	Text	Corrective Action
Critical	Near-end LOS	"Trunk LOS Alarm"	Loss of Signal (LOS) indicates a physical problem. 1. Check that the cable is connected on the board. 2. Check that the correct cable type is being used (crossed/straight). 3. Contact AudioCodes Support.

Alarm	acTrunksAlarmNearEndLOS		
Cleared	End of LOS	-	-

Trunk Near-End LOF Alarm

Table 2-2: acTrunksAlarmNearEndLOF

Alarm	acTrunksAlarmNearEndLOF		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.50		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Severity	Condition	Text	Corrective Action
Critical	Near end LOF	"Trunk LOF Alarm"	1. Make sure that the trunk is connected to a proper follow-up device. 2. Make sure that both sides are configured with the same (E1 / T1) link type. 3. Make sure that both sides are configured with the same framing method. 4. Make sure that both sides are configured with the same line code. 5. Make sure that the clocking setup is correct. 6. Contact AudioCodes Support.
Cleared	End of LOF	-	-

Trunk AIS Alarm

Table 2-3: acTrunksAlarmRcvAIS

Alarm	acTrunksAlarmRcvAIS		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.51		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Text	communicationsAlarm		
Event Type	PSTN provider has stopped the trunk (receiveFailure)		
Probable Cause	communicationsAlarm		
Severity	Condition	Text	Corrective Action
Critical	Receive AIS	"Trunk AIS Alarm"	1. Contact your PSTN provider to activate the trunk. 2. If the alarm persists, contact the AudioCodes Support.
Cleared	End of AIS	-	-

Trunk Far-End LOF Alarm

Table 2-4: acTrunksAlarmFarEndLOF

Alarm	acTrunksAlarmFarEndLOF
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.52
Default Severity	Critical
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk
Event Type	communicationsAlarm
Probable Cause	transmitFailure

Alarm	acTrunksAlarmFarEndLOF		
Severity	Condition	Text	Corrective Action
Critical	RAI	"Trunk RAI Alarm"	Make sure that transmission is correct.
Cleared	End of RAI	-	-

DS1 Line Status Alarm


The alarm is applicable only to digital PSTN interfaces.

Table 2-5: dsx1LineStatusChange

Alarm	dsx1LineStatusChange	
OID	1.3.6.1.2.1.10.18.15.0.1	
Default Severity	Major on raise; Clear on clear	
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk	
Event Type	communicationsAlarm	
Probable Cause		
Severity	Text	Additional Info1,2,3
-	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: 1 dsx1NoAlarm No alarm present

Alarm	dsx1LineStatusChange	
		2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure Any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded

B-Channel Alarm

The alarm is applicable only to digital PSTN interfaces.

Table 2-6: acBChannelAlarm

Alarm	acBChannelAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.85
Default Severity	Minor
Source Varbind	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk

Alarm	acBChannelAlarm		
Text			
Event Type	communicationsAlarm		
Probable Cause	degradedSignal		
Alarm Severity	Condition	Text	Corrective Action
Major	B-channel service state changes to 'Out of Service' or 'Maintenance'	"B-Channel Alarm. %s"	Corrective action is not necessary
Clear	B-channel status changes to 'In Service'	"%s – additional information"	-

D-Channel Status Alarm

The alarm is applicable only to digital PSTN interfaces.

Table 2-7: AcDChannelStatus

Alarm	acDChannelStatus		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37		
Description	The alarm is sent at the establishment, re-establishment or release of the Link Access Protocol D-Channel (LAPD) link with its peer connection.		
Default Severity	Major		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number (0 is the first trunk)		
Event Type	communicationsAlarm		
Probable Cause	degradedSignal		
Severity	Condition	Text	Corrective Action
Major	ISDN D-channel goes down (fails)	"D-Channel	-

Alarm	acDChannelStatus		
		Alarm. D-Channel is Out Of Service"	
Minor	NFAS D-channel (primary or backup) goes down (fails)	"D-Channel Alarm. Primary NFAS D-Channel is Out Of Service" or "D-Channel Alarm. Backup NFAS D-Channel is Out Of Service"	-
Cleared	ISDN D-channel is re-established.	"D-Channel Alarm. %s"	-

NFAS Group Alarm

Table 2-8: acNFASGroupAlarm

Alarm	acNFASGroupAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.84		
Default Severity	Major		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	degradedSignal		
Severity	Condition	Text	Corrective Action
Major	An NFAS group goes	"NFAS Group Alarm. %s"	■ The alarm is sent only

Alarm	acNFASGroupAlarm		
	out-of-service		when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when both D-channels are down. ■ When at least one of the D-channels (primary or backup) returns to service, the alarm is cleared. ■ Corrective action is not necessary.
Clear	NFAS group state goes to in- service	"%s– Additional information"	-

Board Alarms

The source varbind text for all alarms under this component is System#0<n>, where *n* is the slot number in which the blade resides in the chassis.

Fatal Error Alarm

Table 2-9: acBoardFatalError

Alarm	acBoardFatalError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1		
Description	The alarm is sent whenever a fatal device error occurs.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Severity	Condition	Text	Corrective Action
Critical	Any fatal error	"Board Fatal Error: A run-time specific	1. Capture the alarm information and the Syslog clause,

Alarm	acBoardFatalError		
		string describing the fatal error"	if active. 2. Contact AudioCodes support, which will want to collect additional data from the device and perform a reset.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After fatal error	-	

No Reply From DNS Server Alarm

Table 2-10: acNoReplyFromDNSServerAlarm

Alarm	acNoReplyFromDNSServerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.155		
Description	The alarm is sent when the device queries a DNS server and no reply is received. DNS queries are done for Proxy Sets that are configured with FQDNs. The alarm indicates the IP Interface (configured in the IP Interfaces table) on which the query was sent. The device periodically (configured by [ProxyIPListRefreshTime]) queries the DNS server to resolve FQDNs, which refreshes the Proxy Set's list of DNS-resolved IP addresses. The device caches (stores) the last successful DNS resolution and if the DNS server subsequently goes offline when the device needs to do a DNS refresh query, instead of taking the Proxy Set offline, the device reuses the cached DNS-resolved addresses. In this scenario, the device continues sending DNS queries every 10 seconds. The device clears every entry in the cache 30 minutes after its time-to-live (TTL) value expires. However, if the DNS server is still offline and the device has deleted the cache, the device takes the Proxy Set offline.		
Default Severity	Minor		
Source Varbind Text	Board#1/ipInterface#<IP Interface Index>		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Severity	Condition	Text	Corrective Action
Minor	No response from DNS server.	"DNS server not responsive"	Make sure that the configured IP

Alarm	acNoReplyFromDNSServerAlarm		
			address of the DNS server is correct.
Cleared	Response received from DNS server.	-	-

Configuration Error Alarm

Table 2-11: acBoardConfigurationError

Alarm	acBoardConfigurationError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Description	The alarm is sent when the device's settings are invalid. The trap contains a message stating, detailing, and explaining the invalid setting.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Severity	Condition	Text	Corrective Action
Critical	A configuration error was detected	"Board Config Error: A run-time specific string describing the configuration error"	a. Check the run-time specific string to determine the nature of the configuration error. b. Fix the configuration error using the appropriate tool: Web interface, OVOC, or ini file. c. Save the configuration and if necessary reset the device. **Note:** The alarm remains

Alarm	acBoardConfigurationError		
			in Critical severity until a device reboot. A Clear trap is not sent.
	After configuration error	-	

Software Reset Alarm

Table 2-12: acBoardEvResettingBoard

Alarm	acBoardEvResettingBoard		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5		
Description	The alarm is sent after the device resets.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	outOfService (71)		
Severity	Condition	Text	Corrective Action
Critical	When the device is reset through the Web interface or SNMP	"Device is resetting"	A network administrator has reset the device. Corrective action is not required. The alarm remains at Critical severity level until the device completes the reboot. A Clear trap is not sent.

Software Upgrade Alarm

Table 2-13: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70
Description	The alarm is sent when an error occurs during the software upgrade process.
Default	Major

Alarm	acSWUpgradeAlarm		
Severity			
Alarms Source	System#0		
Event Type	processingErrorAlarm		
Probable Cause	softwareProgramError		
Severity	Condition	Text	Corrective Action
Major	Software upgrade errors	"SW upgrade error: Firmware burning failed. Startup system from BootP/TFTP."	Start up the system from BootP/TFTP.

Call Resources Alarm

Table 2-14: acBoardCallResourcesAlarm

Alarm	acBoardCallResourcesAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8		
Description	The alarm is sent when no free channels are available. **Note:** To enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated, by configuring the [EnableRAI] parameter to [1].		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Severity	Condition	Text	Corrective Action
Major	Percentage of busy channels exceeds the predefined RAI high threshold	"Call resources alarm"	Do one of the following: ■ Expand system capacity by adding more channels (trunks)

Alarm	acBoardCallResourcesAlarm		
			■ Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	

All SIP Proxies Connection Lost per Proxy Set Alarm

Table 2-15: acProxyConnectionLost

Alarm	acProxyConnectionLost		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94		
Description	The alarm is sent when all or some proxy servers in a Proxy Set are offline.		
Source Varbind Text	System#0		
Alarm Text	Proxy Set Alarm Text		
Event Type	communicationsAlarm		
Probable Cause	■ Network issue (connection fail due to network/routing failure). ■ Proxy issue (proxy is down). ■ AudioCodes device issue.		
Severity	Condition	Text	Corrective Action
Major	Connection to all the proxy servers in the Proxy Set are lost (offline) and the 'Proxy Load Balancing Method' parameter is disabled.	"Proxy Set <ID>: Proxy lost. looking for another proxy"	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.

Alarm	acProxyConnectionLost		
			3. 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. 4. Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue. 5. Contact AudioCodes support center and send a syslog and network capture for this issue.
	The number of online proxy servers in the Proxy Set is less than the number configured for the 'Min. Active Servers for Load Balancing' parameter and the 'Proxy Load Balancing Method' parameter is enabled (Round Robin or Random Weights).	"Proxy Set <ID>: Proxy lost. looking for another proxy"	
Major	Connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table (IsFallbackUsed parameter). **Note:** Applicable only to the Gateway application.	"Proxy Set <ID>: Proxy not found. Use internal routing"	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.

Alarm	acProxyConnectionLost		
			3. 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. 4. Check that routing using the device's routing table is functioning correctly. 5. Contact AudioCodes support and send a syslog and network capture for this issue.
Minor	All proxy servers were online and now at least one proxy server in the Proxy Set is offline (and at least one proxy server is still online)	"Proxy Set <ID> ("<Name>"): Server <IP address>:<port> is down - one or more servers in the proxy set are offline"	
	All proxy servers were offline and now at least one proxy server in the Proxy Set is online (and at least one proxy server is still offline)	"Proxy Set <ID> ("<Name>"): Server <IP address>:<port> is up, one or more servers in the proxy set are still offline"	
Cleared	All proxy servers in the	"Proxy found.	-

Alarm	acProxyConnectionLost		
	Proxy Set are online	ip:<IP address>:<port #> Proxy Set ID <ID>"	

Controller Failure Alarm

Table 2-16: acBoardControllerFailureAlarm

Alarm	acBoardControllerFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.9		
Description	The alarm is sent in the following scenarios: ■ For Mediant 500L, Mediant 800, and Mediant 1000: 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.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Severity	Condition	Text	Additional Information
Major	Failure in a Proxy Set	"Proxy Set ID n" Where *n* represents	

Alarm	acBoardControllerFailureAlarm		
		the Proxy Set ID.	
	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 TDM-over-IP call	"BusyOut Trunk n TDM over IP failure (Active calls x Min y)" Where *n* represents the 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 / PRI trunk ID.	-
	FXO physical port is down	"BusyOut Line n Link failure" Where *n* represents the FXO port number	Verify that the FXO line is securely cabled to the device's FXO port.

Alarm	acBoardControllerFailureAlarm		
		(0 for the first port).	
	BRI or PRI physical port is down	"BusyOut Trunk n Link failure" Where *n* represents the BRI / PRI trunk port number (0 for the first port).	Verify that the digital trunk is securely cabled to the device's digital port.
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	-

Board Overload Alarm

Table 2-17: acBoardOverloadAlarm

Alarm	acBoardOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Description	The alarm is sent when there is an overload in one or some of the system's components. An overload occurs when a specific percentage of CPU resources is available. You can configure the percentage of available resources to trigger the raising of this alarm, by using the CLI command `configure voip > sip-definition settings > overload-sensitivity-level`.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Severity	Condition	Text	Corrective Action
Major	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	a. Make sure that the syslog level is 0 (or not high). b. Make sure that DebugRecording is

Alarm	acBoardOverloadAlarm		
		available CPU resources remaining.	not running. c. If the system is configured correctly, reduce traffic.
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	-

Administration Status Change Alarm

Table 2-18: acgwAdminStateChange

Alarm	acgwAdminStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7		
Description	The alarm is sent when Graceful Shutdown commences and ends.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Severity	Condition	Text	Corrective Action
Major	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 occurred.

Alarm	acgwAdminStateChange		
Cleared	Admin state changed to unlocked	-	■ No corrective action is required. ■ A network administrator has taken an action to unlock the device.

Operational Status Change Alarm

Table 2-19: acOperationalStateChange

Alarm	acOperationalStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15		
Description	The alarm is sent if the operational state of the node changes to disabled. It is cleared when the operational state of the node changes to enabled.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Severity	Condition	Text	Corrective Action
Major	Operational state changed to disabled	"Network element operational state change alarm. Operational state is disabled."	■ The alarm is cleared when the operational state of the node changes to enabled. ■ In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the device fails to properly initialize. ■ Look for other alarms and Syslogs that might provide additional information about the error.

Alarm	acOperationalStateChange		
Cleared	Operational state changed to enabled	-	-

Remote Monitoring Alarm

Table 2-20: acRemoteMonitoringAlarm

Alarm	acRemoteMonitoringAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.145		
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.		
Default Severity	Warning		
Source Varbind Text	Board#1		
Event 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.	-	-

TLS Certificate Expiry Alarm

Table 2-21: acCertificateExpiryAlarm

Alarm	acCertificateExpiryAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.128		
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.		
Default Severity	Minor		
Source Varbind Text	Board#1/CertificateExpiry#X		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
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	

Alarm	acCertificateExpiryAlarm		
		"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.
Cleared	A new certificate is installed.	-	

License Key Alarms

This section describes the alarms concerned with the device's License Key.

Feature Key Error Alarm

The alarm is applicable only to the local License Key.

Table 2-22: acFeatureKeyError

Alarm	acFeatureKeyError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Description	The alarm is sent when an error occurs in the local License Key.
Default Severity	Critical
Source Varbind Text	
Event Type	processingErrorAlarm
Probable Cause	configurationOrCustomizationError (7)

Alarm	acFeatureKeyError		
Alarm Severity	Condition	Text	Corrective Action
Critical	License Key error.	"Feature key error"	-

License Pool Application Alarm

The alarm is applicable only to the Fixed License.

Table 2-23: acLicensePoolApplicationAlarm

Alarm	acLicensePoolApplicationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.107		
Description	The alarm is sent when the device receives new SBC licenses from the OVOC License Pool and any of the following conditions exist: ■ The device needs to reset or perform a Hitless Upgrade to apply the license. ■ The device is currently undergoing a local License Key upgrade.		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	New License pool		
Alarm Severity	Condition	Text	Corrective Action
Major	The device has received a new SBC License from the OVOC License Pool, but requires a reset for it to be applied.	"License Pool Alarm. New license pool allocations received"	Perform one of the following actions in the OVOC License Pool to apply the new license: ■ Standalone: Reset the device.

Alarm	acLicensePoolApplicationAlarm		
	The device is configured to be managed by the OVOC License Pool, but it is not listed in the License Pool.	"License pool synchronization failed, Device is not listed in the License Server"	Check if the device is expected to be listed in the OVOC License Pool. If yes, then add it to the OVOC License Pool. If not, then remove the device from the License Pool.
	The device is configured to be managed by the OVOC License Pool and is listed in the License Pool, but not managed by it.	"License pool synchronization failed, Device is not managed by License Server "	Check if the device is expected to be managed by the OVOC License Pool. If yes, then add it to the License Pool. If not, then remove the device from the License Pool.
	The device failed to configure the parameters of the OVOC License Pool.	"Device License pool server configuration failed "	Re-send the License Pool from the OVOC License Pool to the device.
Minor	■ Standalone: The device receives a new SBC License from the License Pool Manager, but the device is undergoing a local License Key upgrade.	■ Standalone: "Local License Key was loaded. License Pool requests are ignored until License Key is installed."	Do one of the following in the License Pool Manager to install the local License Key: ■ Standalone: Reset the device.

License Pool Over-Allocation Alarm

The alarm is applicable only to the Fixed License.

Table 2-24: acLicensePoolOverAllocationAlarm

Alarm	acLicensePoolOverAllocationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.125		
Description	The alarm is sent when the SBC license received from the OVOC License Pool has exceeded the maximum capacity supported by the device.		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	Overallocation		
Severity	Condition	Text	Corrective Action
Warning	The SBC license received from the License Pool has exceeded the maximum capacity supported by the device. (Sent after the configuration has been applied in the License Pool; but prior to a device reset or hitless upgrade.)	"License Pool Alarm. Some of the license pool allocations exceed maximum capability and will not be applied"	In the OVOC License Pool, do one of the following: ■ Apply the new license (reset device or apply hitless upgrade); the device sets its SBC capacity to maximum and disregards the excess configured sessions. ■ Reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).
Warning	The SBC license received from the License Pool has exceeded the maximum capacity	"License Pool Alarm. Some of the license pool allocations will not be used because of over-	In the OVOC License Pool, reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless

Alarm	acLicensePoolOverAllocationAlarm		
	supported by the device. (Sent after a device restart.)	allocation”	upgrade).

License Pool Infrastructure Alarm


The alarm is applicable only to the Fixed License.

Table 2-25: acLicensePoolInfraAlarm

Alarm	acLicensePoolInfraAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.106		
Description	The alarm is sent if one of the following occurs: ■ The device is unable to communicate with the OVOC License Pool. ■ The device license has expired. ■ The device is no longer managed by the OVOC License Pool.		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	Condition	Text	Corrective Action
Critical	Device unable to establish an HTTPS REST connection with OVOC after successive attempts.	"License Pool Alarm. License pool validity is about to expire."	In OVOC, perform the 'MG Update' action to re-establish a REST connection with device and to send the latest license.
	The device's license has expired.	"License Pool Alarm. The device license has expired! Use of this device is	

Alarm	acLicensePoolInfraAlarm		
		strictly prohibited."	
Major	The last attempt to establish an HTTPS REST connection with OVOC was not successful.	"License Pool Alarm. Device was unable to access the License Server."	■ Wait for the next connection attempt. ■ In OVOC, perform the 'MG Update' action to re-establish a REST connection with device and to send the current license.
	The device has been configured as Non-Managed in the OVOC License Pool. If there are active licensed sessions for this device, the device automatically performs a reset or hitless upgrade.	"License Pool Alarm. Device is no longer managed by the SBC License Pool."	If you wish, reconfigure the device to be managed by the OVOC License Pool.
Clear	The alarm is cleared when: ■ Connection has been re-established with the OVOC License Pool. An updated license has been loaded to the device and an apply-reset has been performed. ■ The device has been reconfigured to be managed by the OVOC License Pool. A new license has been loaded to the device, and an apply-reset has been performed.	-	-

Cloud License Manager Alarm

The alarm is applicable to the Floating License.

Table 2-26: acCloudLicenseManagerAlarm

Alarm	acCloudLicenseManagerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.132		
Description	The alarm is sent in any of the following scenarios: ■ Disconnection between the device and OVOC. ■ Device fails to send usage reports to OVOC. ■ The Fixed License Pool is enabled and an attempt was made to enable the Floating License.		
Source Varbind Text	Board#1		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomisationError		
Severity	Condition	Text	Corrective Action
Major	There is no connection between the device and OVOC either prior to initial handshake or due to long disconnection time (default is 3 months, but it can be overridden by OVOC)	"No connection with OVOC"	■ Check TCP/TLS connectivity. ■ Check that device is registered with OVOC.
	The device did not send usage reports to OVOC for a specified number of days.	"Failed to send usage report to OVOC for X days."	Check TCP/TLS connectivity.
	The Fixed License Pool is enabled and an attempt was made to enable the Floating License.	"Floating license cannot be enabled when device is managed by License Pool."	Disable the Floating License on the device. Remove the device from the Fixed License Pool in OVOC.

Alarm	acCloudLicenseManagerAlarm		
Critical	The device couldn't connect to OVOC (handshake).	"Connection with OVOC failed, response code <XXX>"	■ <Forbidden 403>: Contact AudioCodes support. ■ <unauthorized 401>: Check username and password. Possible HTTP response codes and reasons: ■ 4xx-6xx responses: The device retries the request using the value in the Retry-After header if specified, or immediately following an update of the OVOC Product Key. ■ OVOC response to Register requests: ■ 200: If 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 device ID that is not identified by OVOC

Alarm	acCloudLicenseManagerAlarm		
			■ 500: Server is not able to handle the request due to server-side error (no resources, internal component failure etc.) ■ Server may response with 4xx or 5xx error as defined in HTTP RFC, when appropriate
	The device couldn't connect to OVOC (handshake).	"Connection with OVOC failed. Failed initialize connection"	Check TCP/TLS connectivity.
	The device couldn't initialize connection with OVOC (handshake).	"Device was rejected by OVOC while trying to fetch device id"	<Forbidden 403>: Contact AudioCodes support.
Cleared	■ Connection with OVOC is established. ■ Reports are sent successfully. ■ Floating License is disabled on the device or the device is removed from the Fixed License Pool on OVOC. The alarm is cleared upon the next device reset.	-	-

Network Alarms

This section describes alarms concerned with the network.

Clock Configuration Alarm

Table 2-27: acClockConfigurationAlarm

Alarm	acClockConfigurationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.149		
Description	The alarm is sent when device clock synchronization by NTP server and SIP Date header (in response message to SIP REGISTER) are both enabled. In this configuration scenario, NTP is used as the source of the clock synchronization.		
Default Severity	Minor		
Source Varbind Text	Board#1		
Event Type	operationalViolation		
Probable Cause	configurationOrCustomizationError		
Alarm Text	Board Configuration Error: DateHeaderTimeSync would be ignored as NTP is enabled.		
Severity	Condition	Text	Corrective Action
Minor	Clock synchronization by NTP and SIP Date header are both enabled.	"Clock Synchronization from SIP Date header ignored as NTP is enabled"	Disable one of the clock synchronization methods.
Cleared	One of the clock synchronization methods is disabled.	-	-

NTP Server Status Alarm

Table 2-28: acNTPServerStatusAlarm

Alarm	acNTPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71
Description	The alarm is sent when the connection to the NTP server is lost. Cleared when the connection is reestablished. Unset time (because

Alarm	acNTPServerStatusAlarm		
	of no connection to NTP server) may result with functionality degradation and failure in device. If the device receives no response from the NTP server, it polls the NTP server for 10 minutes for a response. If there is still no response after this duration, the device declares the NTP server as unavailable, by sending this alarm. The failed response could be due to incorrect configuration.		
Default Severity	Major		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Severity	Condition	Text	Corrective Action
Major	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.	-	-

Ethernet Link Alarm

Table 2-29: acBoardEthernetLinkAlarm

Alarm	acBoardEthernetLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Description	The alarm is sent when an Ethernet link(s) is down. The alarm is sent regardless of the number of ports configured in an Ethernet Group; as soon as an Ethernet port (link) goes down, the alarm is sent.
Default Severity	Critical
Source Varbind Text	Board#<n>/EthernetLink#0 (where n is the slot number) This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).

Alarm	acBoardEthernetLinkAlarm		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Severity	Condition	Text	Corrective Action
Minor	Ethernet Group with two Ethernet ports and only one is down.	"Ethernet link alarm. LAN port number <n> link is down" (where *n* is the port number)	1. Ensure that the Ethernet cables are plugged into the chassis. 2. Check the device's Ethernet link LEDs to determine which interface is failing. 3. Reconnect the cable or fix the network problem
Minor	Ethernet Group with two Ethernet ports and both are down, or Ethernet Group with a single port and the port is down.	"No Ethernet link"	
Cleared	Ethernet Group with two Ethernet ports and both are up, or Ethernet Group with a single port and the port is up again.	-	

WAN Link Alarm

Table 2-30: acBoardWanLinkAlarm

Alarm	acBoardWanLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.79
Description	The alarm is sent when the WAN Link is down (and cleared when link is up again).

Alarm	acBoardWanLinkAlarm		
Default Severity	Major / Clear		
Event Type	equipmentAlarm		
Source Varbind Text	Board#x/WanLink#y		
Probable Cause	underlyingResourceUnavailable		
Severity	Condition	Text	Corrective Action
Major	WAN link down	-	Connect the WAN port
Clear	WAN link up	-	-

Wireless Cellular Modem Alarm

Table 2-31: acWirelessCellularModemAlarm

Alarm	acWirelessCellularModemAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.82		
Description	The alarm is sent when either the wireless modem is down or in backup mode, and cleared when modem is up.		
Default Severity	Major / Clear		
Source Varbind Text	Board#x/WanLink#y		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Severity	Condition	Text	Corrective Action
Major	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.

Alarm	acWirelessCellularModemAlarm		
Clear	WAN link up	-	-

LDAP Lost Connection Alarm

Table 2-32: acLDAPLostConnection

Alarm	acLDAPLostConnection
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.75
Default Severity	Minor
Event 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 sent.
Alarm Text	LDAP Lost Connection
Status Changes	The alarm is sent when there is no connection to the LDAP server

OCSP Server Status Alarm

Table 2-33: acOCSPServerStatusAlarm

Alarm	acOCSPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.78
Default Severity	Major / Clear
Event Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Alarm Text	OCSP server alarm
Corrective Action	Try any of the following: ■ Repair the Online Certificate Status Protocol (OCSP) server ■ Correct the network configuration

Track ID Alarm

Table 2-34: acTrackIdStateChangeAlarm

Alarm	acTrackIdStateChangeAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.121		
Description	The alarm is sent when a Track ID goes down or up (i.e., the destination of the Track ID is no longer reachable). The alarm includes the Track ID, interface name, destination address and the new track state. To configure the tracking feature, use the track command.		
Default Severity	Minor		
Source Varbind Text	System#0/TrackIdRule#<n> (where n is the Track ID number).		
Event Type	communicationsAlarm		
Probable Cause	outOfService (71)		
Severity	Condition	Text	Corrective Action
Minor	Track ID changes from "UP" state to "DOWN".	"Track ID 1 on source interface <name> for tracked destination <address> is down"	If the problem is with the destination device or with some network element along the path, you need to resolve the problem on the point of failure (not on the MSBR device). If the problem is on the MSBR device, for example, the source interface used by the Track is down, you need to resolve the problem (by reconnecting a network cable, reconfiguring a removed interface from configuration, etc.)
Cleared	Track ID changes from "DOWN" to "UP".	" Track ID 1 on source interface <name> for tracked destination <address> is up"	--

Active Alarm Table Alarm

Table 2-35: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow		
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12		
Description	The alarm is sent when an active alarm cannot be entered into the Active Alarm table because the table is full.		
Default Severity	Major		
Source Varbind Text	System#0<n>/AlarmManager#0		
Event Type	processingErrorAlarm		
Probable Cause	resourceAtOrNearingCapacity (43)		
Alarm Severity	Condition	Text	Corrective Action
Major	Too many alarms to fit in the active alarm table	"Active alarm table overflow"	■ Some alarm information may be lost but the ability of the device to perform its basic operations is not impacted. ■ A reboot is the only way to completely clear a problem with the active alarm table. ■ Contact AudioCodes Support.
Remains 'Major' until reboot. A 'Clear' trap is not sent.	After the alarm is sent	-	Note that the status remains 'Major' until reboot as it denotes a possible loss of information until the next reboot. If an alarm is sent when the table is full, it is possible that the alarm is active, but does not appear in the active alarm table.

Analog Port Alarms

Analog Port SPI Out-of-Service Alarm

The alarm is applicable only to analog interfaces.

Table 2-36: acAnalogPortSPIOutOfService

Alarm	acAnalogPortSPIOutOfService		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.46		
Default Severity	Major		
Source Varbind Text	System#0/analogports#<n>, where n is the port number		
Event Type	physicalViolation		
Probable Cause	equipmentMalfunction		
Alarm Severity	Condition	Text	Corrective Action
Major	Analog port has gone out of service	"Analog Port SPI out of service"	■ No corrective action is required. ■ The device shuts down the port and activates it again when the Serial Peripheral Interface (SPI) connection returns.
Cleared	Analog port is back in service	-	-

Analog Port High Temperature Alarm

Table 2-37: acAnalogPortHighTemperature

Alarm	acAnalogPortHighTemperature		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.47		
Default Severity	Major		
Source Varbind Text	System#0/analogports#<n>, where n is the port number		
Event Type	physicalViolation		
Probable Cause	equipmentMalfunction		
Severity	Condition	Text	Corrective Action

Alarm	acAnalogPortHighTemperature		
Major	Analog device has reached critical temperature. Device is automatically disconnected.	"Analog Port High Temperature"	■ No corrective action is required. ■ The device shuts down the analog port and tries to activate it again later when the device's temperature drops.
Cleared	Temperature is back to normal - analog port is back in service.	-	-

Analog Port Ground Fault Out-of-Service Alarm

Table 2-38: acAnalogPortGroundFaultOutOfService

Alarm	acAnalogPortGroundFaultOutOfService
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Default Severity	Major / Clear
Source Varbind Text	System#0/analogports#<n>, where n is the port number
Event Type	physicalViolation
Probable Cause	equipmentMalfunction (this alarm is sent when the FXS port is inactive due to a ground fault)
Alarm Text	Analog Port Ground Fault Out Of Service
Corrective Action	■ No corrective action is required. ■ The device shuts down the port and tries to activate it again when the relevant alarm is over.

Analog Line Left Off-hook Alarm

Table 2-39: acAnalogLineLeftOffhookAlarm

Alarm	acAnalogLineLeftOffhookAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.141		
Description	The alarm is sent when an analog FXS phone is left off-hook for a user-defined time, configured by the FXSOffhookTimeoutAlarm parameter.		
Alarm Source	Board#1/SipAnalogEp#<id>		
Event Type	equipmentAlarm		
Probable Cause			
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.	-	-

Media Alarms

Media Process Overload Alarm

Table 2-40: acMediaProcessOverloadAlarm

Alarm	acMediaProcessOverloadAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.81
Description	The alarm is sent when there is an overload of media (RTP) processing on the device. This can occur, for example, because of malicious attacks (such as denial of service or DoS) on a specific port, or as a result of processing SRTP packets.
Default Severity	Major
Event Type	environmentalAlarm

Alarm	acMediaProcessOverloadAlarm		
Probable Cause	underlyingResourceUnavailable		
Severity	Condition	Text	Corrective Action
Major	Overload of media processing.	"Media Process Overload Alarm"	If not due to malicious attacks, reconfigure your device so that it can process the required media sessions per SIP entity according to media characteristics (e.g., SRTP, RTP and coder types). If due to malicious attacks, you should contact your network administrator.
Cleared	Resources are available for media processing.	-	-

Media Realm Bandwidth Threshold Alarm

Table 2-41: acMediaRealmBWThresholdAlarm

Alarm	acMediaRealmBWThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.87		
Default Severity			
Event Type	ProcessingErrorAlarm		
Probable Cause	The alarm is sent when a bandwidth threshold is crossed		
Severity	Condition	Text	Corrective Action
Major	-	"Media Realm BW Threshold Alarm"	Cleared when bandwidth threshold returns to normal range

Call Quality Alarms

This section describes the alarms concerned with call quality.

Answer-Seizure Ratio Threshold Alarm

Table 2-42: acASRThresholdAlarm

Alarm	acASRThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.111		
Description	The Answer-Seizure Ratio (ASR) measures the percentage of answered calls relative to the total number of attempted calls (seizures). The alarm is sent when the configured ASR minor and major thresholds are crossed (configured in the Performance Profile table).		
Source Varbind Text	The object for which the threshold is crossed can be any of the following: ■ PM_gwSBCASR ■ PM_gwSBCIPGroupASR ■ PM_gwSBCSRDASR		
Alarm Text	-		
Event Type	QualityOfServiceAlarm		
Probable Cause	ThresholdCrossed		
Severity	Condition	Text	Corrective Action
Major	ASR is equal or less than the configured Major threshold.	"ASR threshold crossed."	-
Minor	ASR is equal or less than the configured Minor threshold (but greater than the Major threshold).	"ASR threshold crossed."	-
Cleared	ASR is above the configured Minor threshold plus the hysteresis.	-	-

Average Call Duration Threshold Alarm

Table 2-43: acACDThresholdAlarm

Alarm	acACDThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.112		
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 sent when the configured ACD minor and major thresholds are crossed (configured in the Performance Profile table).		
Source Varbind Text	The object for which the threshold is crossed can be any one of the following: ■ PM_gwSBCACD ■ PM_gwSBCIPGroupACD ■ PM_gwSBCSRDACD		
Alarm Text			
Event Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Severity	Condition	Text	Corrective Action
Major	ACD is equal or less than the configured Major threshold.	"ACD threshold crossed."	-
Minor	ACD is equal or less than the configured Minor threshold (but greater than the Major threshold).	-	-
Cleared	ACD is above the configured Minor threshold plus the hysteresis.	-	-

Network Effectiveness Ratio Threshold Alarm

Table 2-44: acNERThresholdAlarm

Alarm	acNERThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.113		
Description	The NER (Network Effectiveness Ratio) measures the percentage of successfully connected calls relative to the total number of seizures. The alarm is sent when the configured NER minor and major thresholds are crossed (configured in the Performance Profile table).		
Source Varbind Text	The object for which the threshold is crossed can be one of the following: ■ PM_gwSBCNER ■ PM_gwSBCIPGroupNER ■ PM_gwSBCSRDNER		
Alarm Text			
Event Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Severity	Condition	Text	Corrective Action
Major	NER is equal or less than the configured Major threshold.	"NER threshold crossed."	
Minor	NER is equal or less than the configured Minor threshold (but greater than the Major threshold).		
Cleared	NER is above the configured Minor threshold plus the hysteresis.		

No Route to IP Group Alarm

Table 2-45: acIpGroupNoRouteAlarm

Alarm	acIpGroupNoRouteAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.114		
Description	The alarm is sent when the device rejects calls to the destination IP Group due to any of the following reasons: ■ Server-type IP Group is not associated with a Proxy Set, or it's associated with a Proxy Set that is not configured with any addresses, or the associated Proxy Set experiences a proxy 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)		
Source Varbind Text	The object for which the threshold is crossed according to one of the above-mentioned reasons. The text displayed for this alarm can be one of the following: ■ "No Working Proxy" (acProxyConnectivity trap is sent) ■ "Poor Quality of Experience" ■ "Bandwidth" ■ "ASR" (see acASRThresholdAlarm) ■ "ACD" (see acACDThresholdAlarm) ■ "NER" (see acNERThresholdAlarm)		
Alarm Text	<Alarm Description Reason> as described above.		
Event 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-	"IP Group is temporarily	-

Alarm	acIpGroupNoRouteAlarm		
	mentioned reasons.	blocked. IPGroup(<name>) Blocked Reason: <reason – see Source Varbind Text>"	
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).		-

Network Quality Monitoring

This section describes the alarms concerned with the Network Quality Monitoring (NQM) feature.

NQM Connectivity Alarm

Table 2-46: acNqmConnectivityAlarm

Alarm	acNqmConnectivityAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.88		
Description	The alarm is sent when the device loses connectivity with the Network Quality Monitoring (NQM) probe destination.		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsSubsystemFailure		
Probable Cause	The alarm is sent when connectivity with the 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

Alarm	acNqmConnectivityAlarm		
			destination is re-established

NQM High RTT Alarm

Table 2-47: acNqmRttAlarm

Alarm	acNqmRttAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.89		
Description	The alarm is sent when the device detects high round-trip delay time (RTT) towards the Network Quality Monitoring (NQM) probe destination.		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsSubsystemFailure		
Probable Cause	The alarm is sent when high RTT is detected towards the 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 High Jitter Alarm

Table 2-48: acNqmJitterAlarm

Alarm	acNqmJitterAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.90		
Description	The alarm is sent when the device detects high jitter towards the Network Quality Monitoring (NQM) probe destination.		
Default Severity	Minor		
Alarm Source	Board#%d/NqmSender#%d		
Event Type	CommunicationsAlarm		
Probable Cause	The alarm is sent when high jitter is detected towards the 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:** There's no simple solution for high jitter. A systemic level solution may be required.

NQM High Packet Loss Alarm

Table 2-49: acNqmPacketLossAlarm

Alarm	acNqmPacketLossAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.91
Description	The alarm is sent when the device detects high packet loss towards the Network Quality Monitoring (NQM) probe destination.

Alarm	acNqmPacketLossAlarm		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	CommunicationsAlarm		
Probable Cause	The alarm is sent when high packet loss is detected towards the NQM probe destination.		
Alarm Severity	Condition	Text	Corrective Action
Minor	-	"Detected high PL towards NQM probe destination"	To correct high packet loss (PL): ■ Eliminate interference problems: Distance your modem from electrical devices ■ Do not coil up any excess signal or power cables. ■ Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring.

NQM Low Conversational MOS Alarm

Table 2-50: acNqmCqMosAlarm

Alarm	acNqmCqMosAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.95
Description	The alarm is sent when the device detects low conversational voice quality towards the Network Quality Monitoring (NQM) probe destination.
Default Severity	
Alarm Source	Board#%d/NqmSender#%d

Alarm	acNqmCqMosAlarm		
Event Type	communicationsAlarm		
Probable Cause	The alarm is sent when low conversational voice quality is detected towards the NQM probe destination.		
Severity	Condition	Text	Corrective Action
Minor	-	"Detected low conversational voice quality towards NQM probe destination Index <index>. Target IP address: <IP>, Conversation MOS: <score>"	To fix the Noise Quality Measure (NQM) result: ■ Perform corrective action for jitter. See NQM High Jitter Alarm on page 58. ■ Perform corrective action for Real Time Protocol (RTP) packet loss. See NQM High Packet Loss Alarm on page 58. ■ Perform corrective action for long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination. See NQM High RTT Alarm on page 57. To fix the poor Conversational Quality (CQ) that the test indicates: ■ Try changing the coder ■ Try using RTP-Redundancy

Alarm	acNqmCqMosAlarm		
			■ Perform corrective action for RTP packet loss. See NQM High Packet Loss Alarm on page 58.

NQM Low Listening MOS Alarm

Table 2-51: acNqmLqMosAlarm

Alarm	acNqmLqMosAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.96		
Description	The alarm is sent when the device detects low listening voice quality towards the Network Quality Monitoring (NQM) probe destination.		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsAlarm		
Probable Cause	The alarm is sent when low listening voice quality is detected towards the NQM probe destination.		
Severity	Condition	Text	Corrective Action
Minor	-	"Detected low listening voice quality towards NQM probe destination index <index>. Target IP address: <IP>, Listener MOS: <score>"	To fix the Noise Quality Measure (NQM) result, perform corrective action for Real Time Protocol (RTP) packet loss. To fix the poor listening quality that the test indicates: ■ Try changing the coder ■ Try using RTP-Redundancy

Alarm	acNqmLqMosAlarm		
			■ Perform corrective action for RTP packet loss For more information on packet loss corrective action, see NQM High Packet Loss Alarm on page 58.

Intrusion Detection Alarms

This section describes the alarms concerned with the device's Intrusion Detection System (IDS) feature.

IDS Policy Alarm

Table 2-52: acIDSPolicyAlarm

Alarm	acIDSPolicyAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Description	The alarm is sent when a threshold of a specific IDS Policy rule is crossed for the Intrusion Detection System (IDS) feature. The alarm displays the crossed severity threshold (Minor or Major), IDS Policy and IDS Rule, and the IDS Policy-Match index. The alarm is associated with the MO pair IDSMatch and IDSRule.
Default Severity	-
Event Type	Other
Probable Cause	
Alarm Text	"<Severity> (enum severity) cross. Policy: <Name> (<Index>), Rule: <Name>, Last event: <Name>, Source: <IP Address:portprotocol>, SIP Interface: <Name> (<Index>)" For example: "Major threshold (3) cross. Policy: My Policy (3), Rule: Malformed messages, Last event: SIP parser error, Source: 10.33.5.111:62990udp, SIP Interface: SIPInterface_0 (0)."

Alarm	acIDSPolicyAlarm		
Severity	Condition	Text	Corrective Action
Minor or Major (depending on crossed threshold)	Threshold of a specific IDS Policy rule is crossed.	(see Alarm Text above)	1. Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm. 2. Locate the remote hosts (IP addresses) that are specified in the traps. 3. Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation. 4. If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table.

3 SNMP Trap Events (Notifications)

This section describes the device's SNMP trap events (logs).

These traps are sent with the severity varbind value of 'Indeterminate'. These traps don't 'Clear' and they don't appear in the Alarm History table or Active Alarm table. The only log trap that does send 'Clear' is acPerformanceMonitoringThresholdCrossing.

Intrusion Detection System (IDS)

This section describes the trap events concerned with the Intrusion Detection System (IDS) feature.

IDS Threshold Cross Notification Trap

Table 3-1: acIDSThresholdCrossNotification

Event	acIDSThresholdCrossNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Description	The alarm is sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
Description	The trap is sent for each scope (IP or IPport) crossing a threshold of an active alarm.
Default Severity	
Event Type	Other
Probable Cause	
Alarm Text	Threshold crossed for scope value IP. Severity=minor/major/critical. Current value=NUM
Status Changes	
Corrective Action	1. Identify the remote host (IP address / port) on the network that the Intrusion Detection System (IDS) has indicated as malicious. The IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). 2. Block the malicious activity.

IDS Blacklist Notification Trap

Table 3-2: acIDSBlacklistNotification

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

Web User Access Denied due to Inactivity Trap

Table 3-3: acWebUserAccessDisabled

Event	acWebUserAccessDisabled
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Default Severity	Indeterminate
Event Type	
Probable Cause	The alarm is sent when Web user was disabled due to inactivity
Alarm Text	

Event	acWebUserAccessDisabled
Status Changes	
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: 1. In the Web interface, access the Local Users table (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Local Users**). 2. Identify in the table those users whose access has been denied. 3. Change the status of that user from Blocked to **Valid** or **New**.

Web User Activity Log Trap

Table 3-4: acActivityLog

Event	acActivityLog
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.105
Description	The alarm is 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).
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	"[description of activity].User:<username>. Session: <session type>[IP address of client (user)]." For example: “Auxiliary file loading was changed from ‘0’ to ‘1’, User:Admin. Session: WEB [172.17.125.12]"
Note	Activity log event is applicable to the following OAMP interfaces: SNMP, Web, CLI and REST. For SNMP activity, the username refers to the SNMP community string.

Power-Over-Ethernet Status Trap

Table 3-5: acPowerOverEthernetStatus

Event	acPowerOverEthernetStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.80
Description	The alarm is sent when Power over Ethernet (PoE) for a specific port is disabled.
Default Severity	Indeterminate
Event Type	environmentalAlarm
Probable Cause	underlyingResourceUnavailable
Trap Text	"POE Port %d Was Not Powered Due To Power Management" where %d is the Ethernet port number
Condition	This trap is sent when insufficient power is available for a plugged-in PoE client in a PoE-enabled LAN port.
Trap Status	Trap is sent

Keep-Alive Trap

Table 3-6: acKeepAlive

Event	acKeepAlive
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Description	Part of the NAT traversal mechanism. If the device's STUN application detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the device. If the device is configured for SNMPv3, the trap is sent with acBoardTrapGlobalsAdditionalInfo2: SNMPVersion=SNMPv3. If the device is configured for SNMPv2, the trap is sent with acBoardTrapGlobalsAdditionalInfo2: SNMPVersion= SNMPv2c. **Note:** Keep-alive is sent every 9/10 of the time configured by the [NatBindingDefaultTimeout] parameter.

Event	acKeepAlive
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	Keep alive trap
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

Performance Monitoring Threshold-Crossing Trap

Table 3-7: acPerformanceMonitoringThresholdCrossing

Event	acPerformanceMonitoringThresholdCrossing
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Description	The alarm is sent every time the threshold of a Performance Monitored object ('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. **Note:** To enable this trap functionality, set the ini file parameter [PM_EnableThresholdAlarms] to [1].
Default Severity	Indeterminate
Event Source	<Performance Monitoring name> #<Managed Object ID> For example: PM_gwIPGroupINVITEDialogs#7, refers to SIP INVITE messages of IP Group ID 7.
Event Type	other (0)
Probable Cause	other (0)
Trap Text	"Performance: Threshold trap was set", with source = name of

Event	acPerformanceMonitoringThresholdCrossing
	performance counter or gauge which caused the trap
Status Changes	
Condition	A performance counter or gauge (for the attributes 'Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') has crossed the high threshold.
Trap Status	Indeterminate
Condition	A performance counter or gauge has returned to under the threshold
Trap Status	Cleared

HTTP Download Result Trap

Table 3-8: acHTTPDownloadResult

Event	acHTTPDownloadResult
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Description	The alarm is sent upon success or failure of the HTTP Download action.
Default Severity	Indeterminate
Event Type	processingErrorAlarm (3) for failures and other (0) for success.
Probable Cause	other (0)
Status Changes	
Condition	Successful HTTP download.
Trap Text	HTTP Download successful
Condition	Failed download.
Trap Text	HTTP download failed, a network error occurred.
Note	There are other possible textual messages describing NFS failures or success, FTP failure or success.

Wireless Cellular Modem Status Changed Trap

Table 3-9: acWirelessCellularModemStatusChanged

Event	acWirelessCellularModemStatusChanged
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.104
Description	The alarm is sent upon a change in the status of the 3G cellular (wireless) USB modem or integrated LTE (4G cellular) 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")
Default Severity	Indeterminate
Event Type	Equipment Alarm
Probable Cause	other (0)
Trap Text	"MSBR cellular interface: dongle type <vendor ID>:<product ID>,modem <"on" or "off">,RSSI <dBm value> DBM."

Dial Plan File Replaced Trap

Table 3-10: acDialPlanFileReplaced

Event	acDialPlanFileReplaced
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.45
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Status Change	

Event	acDialPlanFileReplaced
Condition	Successful dial plan file replacement
Trap Text	"Dial plan file replacement complete."

Secure Shell (SSH) Connection Status Trap

Table 3-11: acSSHConnectionStatus

Event	acSSHConnectionStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Default Severity	indeterminate
Event Type	environmentalAlarm
Probable Cause	other
Alarm Text	■ "SSH logout from IP address <IP>, user <user>" ■ "SSH successful login from IP address <IP>, user <user> at: <IP>:<port>" ■ "SSH unsuccessful login attempt from IP address <IP>, user <user> at: <IP>:<port>. <reason>" ■ "WEB: Unsuccessful login attempt from <IP> at <IP>:<port>. <reason>"
Status Changes	
Condition	SSH connection attempt
Text Value	%s – remote IP %s – user name
Condition	SSH connection attempt – success of failure

SIP Proxy Connectivity Loss Trap

Table 3-12: acProxyConnectivity

Event	acProxyConnectivity
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.103

<table>
<tr><th>Event</th><th colspan="3">acProxyConnectivity</th></tr>
<tr><td>Description</td><td colspan="3">The trap is sent when the device loses connectivity with a specific proxy IP of a Proxy Set. The trap is cleared when the proxy connection is up.</td></tr>
<tr><td>Source Varbind Text</td><td colspan="3">System#0</td></tr>
<tr><td>Alarm Text</td><td colspan="3">Proxy Set Alarm Text</td></tr>
<tr><td>Event Type</td><td colspan="3">communicationsAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">■ Network issue (connection fail due to network/routing failure).
■ Proxy issue (proxy is down).
■ AudioCodes device issue.</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Indeterminate</td><td>When connection to the proxy server is lost.</td><td>"Proxy Server <IP address>:<port> is now OUT OF SERVICE"</td><td>1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.
2. Ping between the proxy and the device. If there is no ping, the problem could be a network or router issue.
3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same trap event. If this is the case, this could confirm that this is not an issue with the device.
4. Contact AudioCodes support and send a syslog and network capture for this issue.</td></tr>
<tr><td>Cleared</td><td>When connection to</td><td>"Proxy Server <IP address>:<port> is</td><td>-</td></tr>
</table>

Event	acProxyConnectivity		
	the proxy is available again	now IN SERVICE"	

Cold Start Trap

Table 3-13: coldStart

Event	ColdStart
OID	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Description	The alarm is sent if the device reinitializes following, for example, a power failure, crash, or CLI `reload` command. Categorized by the RFC as a "generic trap".
Note	This is a trap from the standard SNMP MIB.

Authentication Failure Trap

Table 3-14: authenticationFailure

Event	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB
Description	The trap is sent if the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated. **Note:** You can disable the sending of this SNMP trap, using the [EnableSnmpAuthenticationTrap] parameter.

Board Initialization Completed Trap

This is the AudioCodes Enterprise application cold start trap.

Table 3-15: acBoardEvBoardStarted

Event	acBoardEvBoardStarted
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Description	The alarm is sent after the device is successfully restored and initialized following reset.
MIB	AcBoard
Severity	cleared
Event Type	equipmentAlarm
Probable Cause	Other(0)
Alarm Text	Initialization Ended

Configuration Change Trap

Table 3-16: entConfigChange

Event	entConfigChange
OID	1.3.6.1.2.1.4.7.2
MIB	ENTITY-MIB
Description	The alarm is sent if a change in the device's hardware is detected, for example, when a module is removed from the chassis.

Link Up Trap

Table 3-17: linkUp

Event	linkUp
OID	1.3.6.1.6.3.1.1.5.4
MIB	IF-MIB
Description	The alarm is sent if the operational status of a communication link (e.g., an Ethernet port interface) changes from “down”. Categorized by the RFC as an “enterprise-specific trap”. By default, the index of the interface is included in the trap. If you want to disable the inclusion of the index, configure the

Event	linkUp
	[LinkUpDownTrapIfIndexSuffixEnable] parameter to 0.

Link Down Trap

Table 3-18: linkDown

Event	linkDown
OID	1.3.6.1.6.3.1.1.5.3
MIB	IF-MIB
Description	The alarm is sent if a communication link failure is detected. Categorized by the RFC as an "enterprise-specific trap". By default, the index of the interface is included in the trap. If you want to disable the inclusion of the index, configure the [LinkUpDownTrapIfIndexSuffixEnable] parameter to 0.

Enhanced BIT Status Trap

Table 3-19: acEnhancedBITStatus

Event	acEnhancedBITStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Description	The alarm is 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.
Default Severity	Indeterminate
Source Varbind Text	BIT
Event Type	Other
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their status.
Status Changes	
Additional Info-1	BIT Type: Offline, startup, periodic

Event	acEnhancedBITStatus
Additional Info-2	BIT Results: ■ BIT_RESULT_PASSED ■ BIT_RESULT_FAILED
Additional Info-3	Buffer: Number of bit elements reports
Corrective Action	Not relevant

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-52456