Reference Guide

AudioCodes Gateways & Session Border Controllers

SNMP Alarms

Version 7.4

Notice

Date Published: January-16-2025

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.

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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

SBC-Gateway SNMP Reference Guide
SBC-Gateway Performance Monitoring Reference Guide
MP-1288 High-Density Analog Media Gateway User's Manual
Mediant 500 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 3100 Gateway & SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual

Document Revision Record

LTRT	Description
52440	Initial document release for Ver. 7.4.
52441	Alarm cleared section added.
52442	New alarms - acClockConfigurationAlarm, acMCNotSecuredAlarm, acFaultyDSPAlarm, acTLSCertificateMismatchAlarm (Ver. 7.40A.100)
52443	Source varbinds updated; acTLSCertificateMismatchAlarm text updated; acFanTrayAlarm description updated
52445	New alarm acNoReplyFromDNSServerAlarm; conditions changed for acBoardTemperatureAlarm
52446	Updated to 7.4.260; New alarm acWeakPasswordAlarm; acFeatureKeyError alarm with License Key validation period and free trial.

LTRT	Description
52447	Updated to 7.4.300; acIPv6ErrorAlarm (updated with dynamic addressing); acBoardFatalError (description); ipNetToMediaTable
52448	Note added indicating acInstallationFailureAlarm not in use.
52449	Updated to 7.40A.250.609; acTLSSocketsLimitAlarm
52450	Updated to 7.40A.400.023 (7.4.400). Typo in description of authenticationFailure; new Major alarm triggers for acHASystemFaultAlarm; acClockConfigurationAlarm (PTP); acVMMaintenaceAlarm
52452	acProxyConnectivity (typos); acMeteringAlarm (text message); acgwAdminStateChange (text)
52453	Typo (acVMMaintenanceAlarm)
52454	7.4.500: acRedundantBoardAlarm (removed); acRtpOnlyBrokenRtpConnectionAlarm (new); acAWSSecurityRoleAlarm (IAM); acBoardTemperatureAlarm (description)
52457	Typo in acDebugRecordingActivationAlarm severity
52459	Updated to 7.40A.500.357 (7.4.500-1); acCertificateExpiryAlarm with CN in description.
52467	Updated to 7.4.500-2: new alarms acIpGroupKeepAliveAlarm and acAccountRegistrationAlarm; text description updated for acHASystemFaultAlarm (maintenance event conditions)
52468	acMeteringAlarm updated
52471	PM_EnableThresholdAlarms removed (obsolete)

Table of Contents

1 Introduction

This document describes all the Simple Network Management Protocol (SNMP) traps (events and alarms) that can be sent by AudioCodes session border controllers (SBC) and media gateways (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

This section provides an overview of the SNMP traps.

For a description of the device's SNMP traps (alarms and events), refer to the *SBC-Gateway SNMP Alarm Reference Guide*.

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 EMS 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 Series)

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., events or 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)

Trap Varbind	Description
	■ critical(5)
AcBoardTrapGlobalsUniqID (5)	Consecutive number count of trap since 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)

Trap Varbind	Description
	■ degradedSignal(12) ■ dteDceInterfaceError(13) ■ 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)

Trap Varbind	Description
	■ remoteNodeTransmissionError(42) ■ resourceAtOrNearingCapacity(43) ■ 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)

Trap Varbind	Description
	■ outOfService(71) ■ proceduralError(72) ■ 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.

Trap Varbind	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.
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 the 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

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

Cleared Alarms

When the device clears an alarm, it adds the prefix "Alarm cleared:" to the alarm's original text description. For example, when an Ethernet link alarm is cleared, the following alarm description is sent: "Alarm cleared: Ethernet link alarm. LAN port number 8 is down.".

2 SNMP Trap Alarms

This section describes the device's SNMP trap alarms.

- You can customize the severity level (including suppressing alarms) of SNMP trap alarms, using the Alarms Customization table [AlarmSeverity]. For more information. refer to the device's *User's Manual*.
- For High-Availability (HA) systems, the source varbind text for alarms that are raised by the redundant device is "Redundant#1" (instead of "Board#1" for the active device).
- Currently, the acInstallationFailureAlarm trap (OID 1.3.6.1.4.1.5003.9.10.1.21.2) is not supported.

Chassis Alarms

This section describes alarms related to the device's chassis.

These alarms are applicable only to MP-1288, Mediant 1000, Mediant 2600, Mediant 4000, and Mediant 9000.

Fan Tray Alarm

This alarm is applicable only to MP-1288, Mediant 1000, Mediant 2600, Mediant 3100, Mediant 4000, and Mediant 9000.

Table 2-1: acFanTrayAlarm

Alarm	acFanTrayAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29
Description	■ The alarm is sent when a fault occurs in the fan tray or a fan tray is missing. ■ **Mediant 1000:** The alarm is sent when the fan tray module is missing (i.e., not installed). ■ **MP-1288, Mediant 3100, Mediant 2600, Mediant 4000:** The alarm is sent when the fan tray module is missing (i.e., not installed) or a fan is faulty. ■ **Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** The alarm is sent when the fan tray module is missing (i.e., not installed), entire fan tray module is faulty, or a specific fan is faulty. For example, if a failure occurs in fan #3, the alarm is sent ("Fan-Tray Alarm. Fan 3 is

<table>
<tr><th>Alarm</th><th colspan="3">acFanTrayAlarm</th></tr>
<tr><td></td><td colspan="3">faulty"). If a failure then also occurs in fan #4, the first alarm is cleared and a new alarm is sent indicating failures in fans #3 and #4 ("Fan-Tray Alarm. Fans 3,4 are faulty"). If fans #3 and #4 return to normal operation, the alarm is cleared.</td></tr>
<tr><td>Source Varbind Text</td><td colspan="3">Chassis#0/FanTray#0</td></tr>
<tr><td>Alarm Text</td><td colspan="3">Fan-Tray Alarm Text</td></tr>
<tr><td>Event Type</td><td colspan="3">equipmentAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">■ 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)</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Critical</td><td>Fan Tray module is missing (not installed in chassis).</td><td>"Fan-Tray is missing"</td><td>a. Check if the Fan Tray module is inserted in the chassis.
b. If the Fan Tray module was removed from the chassis, re-insert it.
c. 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</td></tr>
</table>

Alarm	acFanTrayAlarm		
			harm, make sure that you don't touch the fan blades.
Major	When one or more fans in the Fan Tray module are faulty. **Note:** Not applicable to Mediant 1000.	**All Except Mediant 90xx:** "Fan-Tray is faulty" **Mediant 90xx:** "Fan-Tray Alarm. Fan <#,#> <is or are> faulty"	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module is installed and all fans are working.	-	-

Power Supply Alarm

This alarm is applicable only to MP-1288, Mediant 1000, Mediant 2600, Mediant 3100, Mediant 4000, and Mediant 9000.

Table 2-2: acPowerSupplyAlarm

Alarm	acPowerSupplyAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30
Description	The alarm is sent when a fault occurs in one of the Power Supply modules or a Power Supply module is not installed in the chassis or not installed properly. **Note:** ■ The alarm is applicable only when the device is installed with dual Power Supply modules and one of them is functioning. ■ Mediant 1000: To enable the sending of this trap, configure the ini file parameter [Mediant1000DualPowerSupplySupported] to [2]. ■ MP-1288, Mediant 3100 and Mediant 9000: To enable the device to send this alarm for both Power Supply modules (PS #1 and PS #2), configure the [DualPowerSupplySupported] parameter to 2. If you configure the parameter to 1, the devicesends this alarm only for PS #1 (ignores PS #2). Therefore, If you want to use only one Power Supply module, make sure that the parameter is configured to 1; otherwise, the alarm will be sent to indicate a removed module.

Alarm	acPowerSupplyAlarm		
Default Severity	Critical		
Source Varbind Text	Chassis#0/PowerSupply#<m>, where m is the power supply's slot number		
Event Type	equipmentAlarm		
Probable Cause	powerProblem		
Severity	Condition	Text	Corrective Action
Major	Unable to detect Power Supply module (faulty or missing).	Mediant 1000/2600/4000/9000: "Power-Supply Alarm. Power-Supply is missing." MP-1288: "PS1 fault" Mediant 3100: "PS1 removed" or "PS2 removed"	1. If the Power Supply module is not installed (e.g., was removed), insert a Power Supply module in the chassis. 2. If the Power Supply module is installed, make sure that it is fully inserted into the chassis. 3. If the alarm persists, contact AudioCodes support.
Major (Mediant 3100 Only)	Power source input is faulty.	"PS1 input fault" or "PS2 input fault"	1. Make sure that your power source is on. 2. Make sure that the power cable is properly connected from your power source to the Power Supply module(s).

Alarm	acPowerSupplyAlarm		
			3. If the alarm persists, contact AudioCodes support.
Major (Mediant 3100 Only)	Power output from Power Supply module is faulty.	"PS1 output fault" or "PS2 output fault"	1. If this trap is also sent because of a "PS1/2 input fault" reason, then see above corrective actions. 2. If the alarm persists, contact AudioCodes support.
Cleared	Power Supply module is functioning.	-	-

Hardware Failure Alarm

This alarm is applicable only to Mediant 1000.

Table 2-3: acHwFailureAlarm

Alarm	acHwFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.43
Description	The alarm is sent when the device detects a hardware failure (faulty module or port) on an analog module (FXS or FXO).
Default Severity	Critical
Source Varbind Text	Chassis#0/module#<m>, where *m* is the module's number
Event Type	equipmentAlarm

Alarm	acHwFailureAlarm		
Probable Cause	equipmentMalfunction		
Severity	Condition	Text	Corrective Action
Critical	The module is faulty or has been removed incorrectly.	"Module Alarm: Faulty IF-Module"	Restart the device to clear this alarm. The alarm is not cleared.
Major	Module mismatch - module and CPU board mismatch.	"IF-Module Mismatch"	Restart the device to clear this alarm. The alarm is not cleared.

DSP Farms Mismatch Alarm

This alarm is applicable only to Mediant 2600 and Mediant 4000.

Table 2-4: AcDSPFarmsMismatchAlarm

Alarm	AcDSPFarmsMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.143		
Description	The 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. The alarm and the parameter are used to check that all required MPMs are present and correctly installed in the device's chassis.		
Default Severity	Major		
Source Varbind Text	Board#1/ClusterManager#1/MT#2		
Event Type	equipmentAlarm		
Probable Cause	Underlying Resource Unavailable		
Severity	Condition	Text	Corrective Action
Major	The number of MPMs configured by the	"Missing DSP farm	1. Check if the MPM module(s) is fully inserted

Alarm	AcDSPFarmsMismatchAlarm		
	DspFarmsInstalledNum parameter is greater than the number of MPMs installed on the chassis. This could result in a faulty or missing MPM module(s).	was detected."	into the chassis slot. 2. If an MPM module(s) was removed from the chassis, re-install it. 3. Make sure that the DspFarmsInstalledNum parameter is configured to the correct number of physical MPM modules. 4. If you have performed all the above and the alarm still exists, send a Return Merchandise Author-ization (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.	-	-

Trunk Alarms

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

These alarms are applicable only to products supporting digital interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Trunk Near-End LOS Alarm

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-5: acTrunksAlarmNearEndLOS

Alarm	acTrunksAlarmNearEndLOS
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.49

Alarm	acTrunksAlarmNearEndLOS		
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.
Cleared	End of LOS	-	-

Trunk Near-End LOF Alarm

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-6: 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

Alarm	acTrunksAlarmNearEndLOF		
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

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-7: 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)

Alarm	acTrunksAlarmRcvAIS		
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

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-8: 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		
Severity	Condition	Text	Corrective Action
Critical	RAI	"Trunk RAI Alarm"	Make sure that transmission is correct.
Cleared	End of RAI	-	-

DS1 Line Status Alarm

This alarm is applicable only to products supporting digital PRI interfaces (Mediant 500, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-9: 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 ■ 2 - dsx1RcvFarEndLOF: Far end LOF (also known as Yellow Alarm) ■ 4 - dsx1XmtFarEndLOF: Near end sending LOF Indication ■ 8 - dsx1RcvAIS: Far end sending AIS

Alarm	dsx1LineStatusChange	
		■ 16 - dsx1XmtAIS: Near end sending AIS ■ 32 - dsx1LossOfFrame: Near end LOF (also known as 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

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-10: 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

This alarm is applicable only to products supporting digital (BRI or PRI) interfaces (Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-11: 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

Alarm	acDChannelStatus		
Major	ISDN D-channel goes down (fails)	"D-Channel 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

This alarm is applicable only to products supporting digital PRI interfaces (Mediant 500, Mediant 800, Mediant 1000 and Mediant 3100).

Table 2-12: 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

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

High-Availability Alarms

This section describes the alarms concerned with the High Availability (HA) system.

These alarms are applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

HA System Fault Alarm

This alarm is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-13: acHASystemFaultAlarm

Alarm	acHASystemFaultAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33

Alarm	acHASystemFaultAlarm		
Description	The alarm is sent when the High Availability (HA) system is faulty (i.e., no HA functionality).		
Default Severity	Critical		
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Severity	Condition	Text	Corrective Action
Critical	HA has failed to initialize because of a configuration error.	"SYS_HA: HA Remote address not configured, No HA system."	Configure a valid 'HA Remote Address'.
		"SYS_HA: HA Remote address and Maintenance IF address are not on the same subnet, No HA system."	Configure a valid Maintenance network interface and 'HA Remote Address'.
		"SYS_HA: HA Remote address and Maintenance IF address should be different, No HA system."	Configure a valid Maintenance network interface and 'HA Remote Address'.
	HA is active, but the system is not operating in HA mode.	"Switch-Over: Reason = Fatal exception error"	HA was lost because of a switchover and should return

Alarm	acHASystemFaultAlarm		
			automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = SW WD exception error"	HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = System error"	HA was lost because of a switchover caused by a general system error and should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = Eth link error"	HA was lost because of a switchover. Reconnect the Ethernet link.
		"Switch-Over: Reason = Network Monitor error. Failed table rows index: <id	HA was lost because of a switchover caused by the HA Network

Alarm	acHASystemFaultAlarm		
		1> … up to <id 10>"	Monitor feature as the threshold of unreachable rows (in the HA Network Monitor table) was exceeded. The indices of these unreachable rows are provided in the alarm's text. The HA mode should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = Keep Alive error"	HA was lost due because of a switchover and should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = DSP error"	HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required.

Alarm	acHASystemFaultAlarm		
			Note: Applicable only to Mediant 4000.
		"Switch-Over: Reason = Software upgrade"	HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = Software upgrade - switch back"	HA was lost because of a switchover caused by the Hitless Software Upgrade process that switched from active to redundant device, and should return automatically. Corrective action isn't required.
		"Switch-Over: Reason = Fk upgrade"	HA was lost because of a switchover caused by a Hitless License Upgrade process and should return automatically after a few

Alarm	acHASystemFaultAlarm		
			minutes. Corrective action isn't required.
		"Switch-Over: Reason = Manual switch over"	HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required.
		"Switch-Over: Reason = Higher HA priority"	HA was lost because of a switchover to the device with the higher HA priority and should return automatically after a few minutes. Corrective action isn't required.
Major	HA feature is active, but the system is not operating in HA mode.	"SYS_HA: Invalid Network configuration, fix it and reboot Redundant unit - no HA system!"	HA synchronization process failed. Correct invalid network configuration and then restart the Redundant device to trigger HA synchronization again.

Alarm	acHASystemFaultAlarm		
		"SYS_HA: Offline configuration was changed, HA is not available until next system reboot."	HA synchronization process failed. Changing configuration that requires a device restart to apply the new configuration must be done before the standalone system can become HA again.
		"SYS_HA: Redundant is not reconnecting after deliberate restart, No HA system."	HA synchronization process failed. Manually restart the Redundant device.
	The system is no longer in HA mode because the redundant device is restarting or disconnected from the active device. For example, this can occur during a hitless software upgrade when the redundant device burns the new firmware and then restarts to apply it.	"HA is not operational: redundant unit error/reset reason - <fault description, e.g., Software Upgrade>."	-
	The redundant device disconnected from the HA system and the active device is now in standalone mode.	"HA is not operational: Redundant unit is disconnected."	-
	The active device is in standalone mode and then the redundant device joins HA and synchronizes with the active device.	"HA is not operational: synchronizing redundant	-

Alarm	acHASystemFaultAlarm		
		unit's state and configuration."	
	The active device is in standalone mode and then the redundant device joins HA, but they are running different software versions (.cmp). Therefore, the redundant device gets the .cmp file from the active device (so that they run the same software version).	"HA is not operational: updating redundant unit's software version."	-
	An offline parameter (i.e., requires a device restart) is modified on the active device. An HA switchover occurs, the redundant device (previously active device) restarts to apply the new settings, and synchronization between active and redundant devices occur.	"HA is not operational: redundant unit is restarting to apply new configuration."	-
Minor	The HA Network Monitor feature isn't the cause of an HA switchover because the 'Preempt Mode' parameter is configured to **Enable** and the 'Preempt Priority' is configured to a level.	"Network Monitor switch-over is blocked when HA Preemptive mode and Priority is configured"	-
	The HA Network Monitor feature isn't the cause of an HA switchover because the number of Ethernet Groups (Ethernet links) in the redundant device in "up" status is less than on the active device.	"Network Monitor switch-over is blocked when status of Ethernet links on redundant is worse than on active unit"	-
	The Maintenance Events Monitoring feature is enabled (MaintenanceEventsMonitoringEnable) and the cloud platform performs a	"HA is not operational: switch-over from Active to	-

Alarm	acHASystemFaultAlarm		
	maintenance event on the virtual machine hosting the active device, causing an HA switchover to the redundant device. **Note:** This condition is applicable only to Mediant VE SBC and when it's [MaintenanceEventsMonitoringEnable] parameter is enabled and [MaintenanceEventsTreatmentEnable] disabled.	Redundant unit, Switch over reason - VM maintenance event"	
	The Ethernet Group associated with the Maintenance IP interface (used for HA systems) is configured with two ports, but one of them is down (i.e., no 1+1 Ethernet port redundancy).	"SYS_HA: Maintenance redundant link is down - no HA maintenance link redundancy"	■ Make sure that the network cable is firmly plugged into the Ethernet port. ■ Make sure that the other end of the network cable is correctly connected to the network.
Cleared	The HA system is active and operational.	"HA is operational"	-

HA System Configuration Mismatch Alarm

This alarm is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-14: acHASystemConfigMismatchAlarm

Alarm	acHASystemConfigMismatchAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34

Alarm	acHASystemConfigMismatchAlarm		
Description	The alarm is sent when the License Keys of the two units in the High Availability (HA) system is not identical, causing instability.		
Default Severity	Major		
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot number		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	Text	Corrective Action
Major	License Keys of Active and Redundant units are different.	"Configuration mismatch in the system: Active and Redundant modules have different feature keys."	Update the License Keys of the Active and Redundant units.
	The Active unit was unable to pass on to the Redundant unit the License Key.	"Configuration mismatch in the system: Fail to update the redundant with feature key."	Replace the License Key of the Redundant unit because it may be invalid.
	License key of the Redundant unit is invalid.	"Configuration mismatch in the system: Feature key did not update in redundant module."	Replace the License Key of the Redundant unit because it may be invalid.
Cleared	Successful License Key update	"The feature key was successfully updated in the redundant module"	-

HA System Switch Over Alarm

This alarm is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-15: acHASystemSwitchOverAlarm

Alarm	acHASystemSwitchOverAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35		
Description	The alarm is sent when a switchover occurs from active to redundant device in a High Availability (HA) system.		
Default Severity	Critical		
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Severity	Condition	Text	Corrective Action
Critical	A switchover from the active to the redundant unit has occurred	(See acHASystemFaultAlarm)	See HA System Configuration Mismatch Alarm on page 32 for details.
	A switchover occurred due to the HA Network Monitor feature as the threshold of unreachable rows (in the HA Network Monitor table) was exceeded. The indices of these unreachable rows are provided in the alarm's text.	"Reason = Network Monitor error. Failed table rows index: <id 1> … up to <id 10>"	
Cleared	10 seconds have passed since the switchover	-	-

HA Network Monitor Alarm

This alarm is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-16: acHANetworkMonitorAlarm

Alarm	acHANetworkMonitorAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.136		
Description	The 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*.		
Default Severity	Major		
Source Varbind Text	Board#1/NetworkMonitor#X		
Event Type	communicationsAlarm		
Probable Cause	connectionEstablishmentError		
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

This alarm is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-17: acHAEthernetGroupAlarm

Alarm	acHAEthernetGroupAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.137		
Description	The 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.		
Default Severity	Minor		
Source Varbind Text	system#0		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
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	-	-

HA Network Mismatch Alarm

This alarm is applicable only to Mediant Software.

Table 2-18: acHANetworkMismatchAlarm

Alarm	acHANetworkMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.135		
Description	Mismatch of network devices in the cloud High Availability (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). In other words, 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 and Redundant) must be identical in terms of ENIs.		
Default Severity	Major		
Alarm Title	HA Network Mismatch Alarm		
Source Varbind Text	SystemMo		
Event Type	communicationsAlarm		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	Text	Corrective Action
Major	ENI configuration of both instances does not match.	"Cloud network devices do not match"	Correct the ENI configuration

Board Alarms

The source varbind text for all alarms under this component is System#0<n>, where *n* (always has the value 1 for MP-1288 and Mediant 1000) is the slot number in which the blade resides in the chassis.

Fatal Error Alarm

Table 2-19: acBoardFatalError

Alarm	acBoardFatalError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Description	The alarm is sent when a fatal problem occurs in the device's internal logic, and the device automatically restarts to resolve this problem,

Alarm	acBoardFatalError		
	bringing it back to service.		
Default Severity	Critical		
Source Varbind Text	Board#1		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Severity	Condition	Text	Corrective Action
Critical	Fatal problem in internal logic occurs.	"Board Fatal Error: A run-time specific string describing the fatal error"	The device automatically restarts to resolve the internal logic problem. Send the syslog file and the Debug file (with the Core Dump file, if enabled) to AudioCodes support to diagnose the problem.
Cleared (although 'Clear' trap not sent)	After restart.	-	

Configuration Error Alarm

Table 2-20: 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	"Board Config	1. Check the run-

Alarm	acBoardConfigurationError		
	error was detected	Error: A run-time specific string describing the configuration error"	time specific string to determine the nature of the configuration error. 2. Fix the configuration error using the appropriate tool: Web interface, OVOC, or ini file. 3. Save the configuration and if necessary restart the device. **Note:** The alarm remains in Critical severity until a device restart. A Clear trap is not sent.
	After configuration error	-	

Temperature Alarm

This alarm is applicable only to Mediant 1000, Mediant 3100, Mediant 2600, Mediant 4000, and Mediant 9000.

Table 2-21: acBoardTemperatureAlarm

Alarm	acBoardTemperatureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3
Description	The alarm is sent when the device exceeds its temperature limits (threshold).
Source Varbind Text	System#0
Event Type	equipmentAlarm
Probable Cause	■ The air filter is saturated.

Alarm	acBoardTemperatureAlarm		
	■ One of the fans work slower than expected. temperatureUnacceptable (50)		
Alarm Severity	Condition	Text	Corrective Action
Critical	Internal temperature is too high for normal operation. **Mediant 9000:** Temperature threshold of CPU has been exceeded. The threshold is configured by the ini file parameter [HighTemperatureThreshold]. The default is 70°C (158°F). **Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** Temperature threshold at a specific sensor(s) has been exceeded. The threshold is configured by the ini file parameter [HighTemperatureThreshold]. For example, if the temperature threshold is exceeded at sensor 1, the alarm is sent ("Board Temperature Alarm: Sensor #1 is 88 degrees Celsius. Exceeded threshold of 70"). If the temperature threshold at sensor 2 is then exceeded as well, the first alarm is cleared and a new alarm is sent indicating exceeded temperature at both sensors ("Board Temperature Alarm: Sensors #1,#2 are 88,90 degrees Celsius. Exceeded	"Board temperature too high" **Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** "Board Temperature Alarm: Sensors <#,#> <is or are> <temperature,temperature> degrees Celsius. Exceeded threshold of <threshold>"	1. 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. 2. 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,

Alarm	acBoardTemperatureAlarm		
	threshold of 70"). **Mediant 4000:** At least one temperature sensor detects temperature increase to critical threshold minus 5 (or greater).		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.
Cleared	Temperature returns to normal operating values. **Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** All sensors detect normal temperature. **Mediant 4000:** All sensors detect temperature reduced to below critical threshold minus 5 degrees for at least 60 seconds.	-	-

Software Reset Alarm

Table 2-22: 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 restarts.
Default Severity	Critical
Source Varbind Text	Board#1
Event Type	equipmentAlarm
Probable Cause	outOfService (71)

Alarm	acBoardEvResettingBoard		
Severity	Condition	Text	Corrective Action
Critical	When the device is restart through the Web interface or SNMP	"Device is resetting"	A network administrator has restarted the device. Corrective action is not required. The alarm remains at Critical severity level until the device completes the restart. A Clear trap is not sent.

Software Upgrade Alarm

Table 2-23: 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 Severity	Major		
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.

Administration Status Change Alarm

Table 2-24: acgwAdminStateChange

Alarm	acgwAdminStateChange
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7

Alarm	acgwAdminStateChange		
Description	The alarm is sent when Graceful Shutdown commences and ends.		
Default Severity	Major		
Source Varbind Text	Board#1		
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: Device 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	"Network element admin state change alarm. Device is Locked"	■ No corrective action is required. ■ A network administrator took an action to lock the device, or a graceful lock timeout occurred.
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 2-25: 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

Alarm	acOperationalStateChange		
	disabled. It is cleared when the operational state of the node changes to enabled.		
Default Severity	Major		
Source Varbind Text	Board#1		
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.
Cleared	Operational state changed to enabled	-	-

Board Overload Alarm

Table 2-26: 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

<table>
<tr><th>Alarm</th><th colspan="3">acBoardOverloadAlarm</th></tr>
<tr><td></td><td colspan="3">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 <code>configure voip > sip-definition settings > overload-sensitivity-level</code>.</td></tr>
<tr><td>Default Severity</td><td colspan="3">Major</td></tr>
<tr><td>Source Varbind Text</td><td colspan="3">Board#1</td></tr>
<tr><td>Event Type</td><td colspan="3">processingErrorAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">softwareError (46)</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Major</td><td>An overload condition exists in one or more of the system components</td><td>"System CPU overload condition - IdleUtilization percentage=<percentage of available CPU resources>"</td><td>1. Make sure that the syslog level is 0 (or not high).
2. Make sure that Debug Recording is not running.
3. If the system is configured correctly, reduce traffic.</td></tr>
<tr><td>Cleared</td><td>The overload condition passed</td><td>"System CPU overload condition - IdleUtilization percentage=<percentage of available CPU resources></td><td>-</td></tr>
</table>

Faulty DSP Alarm

Table 2-27: acFaultyDSPAlarm

Alarm	acFaultyDSPAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.152		
Description	The alarm is sent when one or more of the device's DSP cores are faulty.		
Default Severity	Major		
Source Varbind	Board#1		
Event Type	equipmentAlarm		
Probable Cause	unexpectedInformation		
Severity	Condition	Text	Corrective Action
Major	Failure detected in on one or more of the device's DSP cores during bootup	"At least one faulty DSP detected during boot"	Perform diagnostics on the DSP cores.
Cleared	The faulty DSP core(s) has been repaired or replaced and the device has subsequently restarted	-	-

Call Resources Alarm

Table 2-28: 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

Alarm	acBoardCallResourcesAlarm		
Source Varbind Text	Board#1		
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) ■ Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	

Controller Failure Alarm

Table 2-29: 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: ■ **FXO-supporting products only:** 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.) ■ **Digital-supporting products only:** 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.

<table>
<tr><th>Alarm</th><th colspan="3">acBoardControllerFailureAlarm</th></tr>
<tr><td></td><td colspan="3">■ Digital-supporting products only: Failure in TDM-over-IP call - transparent E1/T1 without signalling.
■ Analog or Digital supporting products only: Connection to the Proxy Set associated with the trunk/line is up/down.
■ Analog or Digital supporting products only: Failure in server registration for the trunk/line.
■ Analog or Digital supporting products only: Failure in a Serving IP Group for the trunk.
■ Failure in a Proxy Set.</td></tr>
<tr><td>Default Severity</td><td colspan="3">Major</td></tr>
<tr><td>Source Varbind Text</td><td colspan="3">Board#1</td></tr>
<tr><td>Event Type</td><td colspan="3">processingErrorAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">softwareError (46)</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Additional Information</td></tr>
<tr><td rowspan="4">Major</td><td>Failure in a Proxy Set</td><td>"Proxy Set ID n"
Where n represents the Proxy Set ID.</td><td></td></tr>
<tr><td>Proxy has not been found or registration failure</td><td>"Proxy not found. Use internal routing"
- or -
"Proxy lost. Looking for another Proxy"</td><td>■ Check the network layer
■ Make sure that the proxy IP and port are configured correctly.</td></tr>
<tr><td>Connection to Proxy is down</td><td>"BusyOut Trunk/Line n Connectivity Proxy failure"</td><td>-</td></tr>
<tr><td>Connection to the Proxy Set associated with the trunk or line</td><td>"BusyOut Trunk/Line n Proxy Set Failure"
Where n represents</td><td>Note: Applicable only to analog and digital supporting products.</td></tr>
</table>

Alarm	acBoardControllerFailureAlarm		
	is down	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 BRI / PRI trunk.	**Note:** Applicable only to digital supporting products.
	Failure in server registration for the trunk/line	"BusyOut Trunk/Line n Registration Failure" Where *n* represents the BRI / PRI trunk or FXO line.	**Note:** Applicable only to analog and digital supporting products.
	Failure in a Serving IP Group for the trunk	"BusyOut Trunk n Serving IP Group Failure" Where *n* represents the BRI / PRI trunk ID.	**Note:** Applicable only to digital supporting products.
	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. **Note:** Applicable only to analog FXO supporting products.
	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. **Note:** Applicable only to digital supporting products.
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	-

acVMMaintenanceAlarm

This alarm is applicable only to Mediant VE /CE SBCs deployed on Azure or Google Cloud Platform.

Table 2-30: acVMMaintenanceAlarm

Alarm	acVMMaintenanceAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.157		
Description	The alarm is sent when the device receives a response (over REST API) from the cloud platform's metadata service of a scheduled maintenance event for the virtual machine on which the device is installed. The alarm indicates the type of event and the scheduled time of the event. **Note:** This feature is configured by the [MaintenanceEventsMonitoringEnable] and [MaintenanceEventsTreatmentEnable] parameters. For more information on the device's monitoring and handling of virtual machine maintenance events by the cloud platform, refer to the device's User's Manual.		
Default Severity	Warning		
Source Varbind Text	Board#1		
Event Type	Other		
Probable Cause	Other		
Severity	Condition	Text	Corrective Action
Warning	A maintenance event is scheduled for the virtual machine on which the device is installed.	"VM maintenance event was detected. Event type = “<event>”, Scheduled time = <UTC time>, Event id = <ID>."	-
Cleared	The maintenance event has completed.	-	-

CDR Server Alarm

This alarm is applicable only to Mediant 9000 and Mediant Software.

Table 2-31: acCDRServerAlarm

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

SDR Server Alarm

This alarm is applicable only to Mediant 9000 and Mediant Software.

Table 2-32: acSDRServerAlarm

Alarm	acCDRServerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.147		
Description	The alarm is sent when the device fails to send the locally stored SDRs to all the remote servers, which are configured in the SBC SDR Remote Servers table.		
Default Severity	Major		
Source Varbind Text	Board#1		
Event Type	equipmentAlarm		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Major	Device fails to send the SDR files to all the configured CDR servers.	"Failed to upload SDRs to all configured servers."	Check the network connectivity to the remote server.
Cleared	Device successfully sends the SDR files to at least one of the SDR servers.	"Files transfer succeeded to one of the SDR servers"	-

Remote Monitoring Alarm

Table 2-33: 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	Board#1

Alarm	acRemoteMonitoringAlarm		
Varbind Text			
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.	-	-

No Reply From DNS Server Alarm

Table 2-34: 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.

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

All SIP Proxies Connection Lost per Proxy Set Alarm

Table 2-35: 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	"Proxy Set <ID>: Proxy lost. looking for another proxy"	1. Ping the proxy server. If there is no ping, contact your proxy pro-

Alarm	acProxyConnectionLost		
	Load Balancing Method' parameter is disabled.		vider. 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. 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	"Proxy Set <ID>: Proxy not found. Use internal routing"	1. Ping the proxy server. If there is no ping, contact your proxy pro-

Alarm	acProxyConnectionLost		
	(IsFallbackUsed parameter). **Note:** Applicable only to the Gateway application.		vider. 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. 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	

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

acIpGroupKeepAliveAlarm

Table 2-36: acIpGroupKeepAliveAlarm

Alarm	acIpGroupKeepAliveAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.163		
Description	The alarm is sent when the device has no network connectivity (based on keep-alive messages) with an IP Group (configured in the IP Groups table).		
Default Severity	Major		
Source Varbind Text	Board#1/IPGroup#<IP Group Index>		
Event Type	qualityOfServiceAlarm		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Major	Device loses network connectivity with the IP Group.	"No connectivity with IPGroup <IPGroup name >"	Check the network connectivity to the remote IP Group.

Alarm	acIpGroupKeepAliveAlarm		
Cleared	Connectivity with the IP Group is restored.	-	-

acAccountRegistrationAlarm

Table 2-37: acAccountRegistrationAlarm

Alarm	acAccountRegistrationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.164		
Description	The alarm is sent when a registration failure occurs for an Account (configured in the Accounts table).		
Default Severity	Major		
Source Varbind Text	Board#1/IPGroup#<IP Group Index>/Account#<Account Index>		
Event Type	qualityOfServiceAlarm		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Major	Registration of the Account fails.	"Registration failure for account < Account name>"	-
Cleared	Registration of the Account is successful.	-	-

TLS Certificate Alarms

This section describes the alarms concerned with the device's TLS certificates.

TLS Certificate Expiry Alarm

Table 2-38: acCertificateExpiryAlarm

Alarm	acCertificateExpiryAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.128

<table>
<tr><th>Alarm</th><th colspan="3">acCertificateExpiryAlarm</th></tr>
<tr><td>Description</td><td colspan="3">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.
Note: In addition to the ID of the TLS Context, the alarm's description includes the certificate's Common Name (CN). However, if the certificate doesn't contain a CN, the first subject alternative name (SAN) is included in the description. If a SAN also doesn't exist, "" is included in the description.</td></tr>
<tr><td>Default Severity</td><td colspan="3">Minor</td></tr>
<tr><td>Source Varbind Text</td><td colspan="3">Board#1/CertificateExpiry#X</td></tr>
<tr><td>Event Type</td><td colspan="3">communicationsAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">communicationsSubsystemFailure</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Minor</td><td>The certificate is about to expire. This alarm is sent a user-defined number of days (TLSExpiryCheckStart) before expiration date.</td><td>"The certificate of TLS Context <ID> (CN=<Common Name>) will expire in <number> days"</td><td rowspan="2">Upload 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.</td></tr>
<tr><td>Major</td><td>The certificate is about to expire. This alarm is sent a week as well as a day before expiration date.</td><td>"The certificate of TLS Context <ID> (CN=<Common Name>) will expire in less than a week"
- Or -
"The TLS certificate of TLS Context <ID> (CN=<Common Name>) will expire in a day"
- Or -</td></tr>
</table>

Alarm	acCertificateExpiryAlarm		
		"The TLS certificate of TLS Context <ID> (CN=<Common Name>) will expire in less than a day"	
Critical	The certificate has expired.	"The certificate of TLS Context <ID> (CN=<Common Name>) has expired <number> days ago"	Upload 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.	-	

TLS Certificate Mismatch Alarm

Table 2-39: acTLSCertificateMismatchAlarm

Alarm	acTLSCertificateMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.154		
Description	This alarm is sent when a mismatch occurs between the TLS private key and the certificate (public key).		
Default Severity	Minor		
Source Varbind Text	Board#1/CertificateExpiry#X		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Severity	Condition	Text	Corrective Action

Alarm	acTLSCertificateMismatchAlarm		
Minor	A mismatch occurs between the TLS private key and the certificate.	"TLS Context <ID>: TLS Private key and Certificate in context do not match."	Load a matching private key and certificate to the device.
Cleared	Private key matches the certificate.	-	

TLS Sockets Limit Alarm

Table 2-40: acTLSSocketsLimitAlarm

Alarm	acTLSSocketsLimitAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.159		
Description	The alarm is sent when the number of allocated incoming TLS connections approaches 95% of maximum supported TLS connections. (When the number of TLS connections exceeds 80% of the maximum, the device attempts to close unused TLS connections.) For maximum supported TLS connections, refer to the *Release Notes*.		
Default Severity	Major		
Source Varbind Text	Board#1		
Event Type	communicationsAlarm		
Probable Cause	resourceAtOrNearingCapacity		
Severity	Condition	Text	Corrective Action
Major	The number of allocated incoming TLS connections approaches 95% of max. supported TLS connections.	"Number of incoming TLS connections <current number of TLS connections> is over 95% of max number allowed <max. supported TLS connections>"	-
Cleared	The number of	"Number of incoming TLS	-

Alarm	acTLSSocketsLimitAlarm		
	allocated incoming TLS connections returns to below 90% of max. supported TLS connections.	connections <current number of TLS connections> is less than 90% of max number allowed <max. supported TLS connections>"	

License Key Alarms

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

Feature Key Error Alarm

Table 2-41: acFeatureKeyError

Alarm	acFeatureKeyError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6		
Description	The alarm is sent in the following scenarios: ■ An error exists in the local License Key. ■ When the License Key has a validation period (in days) and 30 days or less remains before expiration or the period has expired. ■ When the device is operating with a free trial evaluation license (Mediant Software SBC only).		
Default Severity	Critical		
Source Varbind Text	system0Mo		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError (7)		
Alarm Severity	Condition	Text	Corrective Action
Major	When the device is operating with a free trial evaluation license.	"The device is currently operating with an evaluation license. Each call is limited	**Note:** ■ The free trial evaluation license allows up to three concurrent calls, up to three registered users, and up to three minutes per call.

Alarm	acFeatureKeyError		
		to 3 minutes."	■ The free trial evaluation license is applicable only to Mediant Software SBC.
Major	When 30 days or less remain until License Key validation expiration (i.e., License Key about to expire).	"The device's local license is about to expire. Please obtain and activate a new license."	Purchase and obtain a License Key with required features.
Critical	When the License Key validation period has expired.	"The device's local license has expired. Each call is limited to 3 minutes."	Purchase and obtain a License Key with required features. **Note:** ■ Once the validity period expires, the device restricts all calls to three minutes (maximum number of call sessions is according to License Key). The device automatically ends calls exceeding this duration. ■ The validation period is based on system uptime. If the device is powered off at any time or restart, validation count pauses, and then resumes when the device is up and running again. ■ The validation period is supported by devices in High-Availability (HA) mode. Validation period countdown is done independently between each device (active and redundant), based on the system uptime of each device. ■ License Key validation period is

Alarm	acFeatureKeyError		
			supported by all licensing models (e.g., Local, Fixed, Floating and Flex).
Critical	An error exists in the local License Key.	"Feature key error"	Contact AudioCodes support.
Cleared	A valid License Key with all required features is purchased and installed on the device.	-	-

License Key Hitless Upgrade Alarm

This alarm is applicable only to the local License Key and products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 2-42: acLicenseKeyHitlessUpgradeAlarm

Alarm	acLicenseKeyHitlessUpgradeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.129
Description	The alarm is sent when installing a local License Key using the Hitless Upgrade method when the device operates in High-Availability (HA) mode, and installation fails due to a failure in the HA switchover process.
Default Severity	Major
Source Varbind Text	system0Mo
Event Type	communicationsAlarm
Probable Cause	keyExpired

Alarm	acLicenseKeyHitlessUpgradeAlarm		
Alarm Severity	Condition	Text	Corrective Action
Major	License Key Hitless Upgrade failed due to failure in HA switchover process.	"Feature key hitless upgrade failed due to failure of switchover process"	Reload the License Key, and then perform the Hitless Upgrade process.

License Pool Application Alarm

The alarm is applicable only to devices supporting the Fixed License.

Table 2-43: 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 restart 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 restart 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		
			■ HA: Apply a Hitless Upgrade or restart the device.
	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	■ Standalone: "Local License Key was loaded. License Pool requests are ignored until License Key is installed." ■ HA: "Local License Key was loaded. License	Do one of the following in the License Pool Manager to install the local License Key: ■ Standalone: Reset the

Alarm	acLicensePoolApplicationAlarm		
	a local License Key upgrade. ■ HA: The device receives a new SBC License from the License Pool Manager, but the devices are currently undergoing a local License Key upgrade.	Pool requests are ignored until License Key is installed."	device. ■ HA: Apply a Hitless Upgrade to the local License Key or restart the device.

License Pool Over-Allocation Alarm

The alarm is applicable only to devices supporting the Fixed License.

Table 2-44: 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	"License Pool Alarm. Some of the license pool allocations exceed maximum	In the OVOC License Pool, do one of the following: ■ Apply the new license (restart device or apply

Alarm	acLicensePoolOverAllocationAlarm		
	capacity supported by the device. (Sent after the configuration has been applied in the License Pool; but prior to a device restart or hitless upgrade.)	capability and will not be applied"	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 (restart device or apply hitless upgrade).
Warning	The SBC license received from the License Pool has exceeded the maximum capacity supported by the device. (Sent after a device restart.)	"License Pool Alarm. Some of the license pool allocations will not be used because of over-allocation"	In the OVOC License Pool, reconfigure the license sessions with values that fall within the device capacity and then apply the new license (restart device or apply hitless upgrade).

License Pool Infrastructure Alarm

The alarm is applicable only to devices supporting the Fixed License.

Table 2-45: 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

Alarm	acLicensePoolInfraAlarm		
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 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 restart 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.

Alarm	acLicensePoolInfraAlarm		
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-restart 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-restart has been performed.	-	-

Flex License Manager Alarm

The alarm is applicable only to the Flex License and to the following products: Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software.

Table 2-46: acFlexLicenseManagerAlarm

Alarm	acFlexLicenseManagerAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.144
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.
Default Severity	Warning
Source Varbind Text	Board#1
Event Type	processingErrorAlarm

Alarm	acFlexLicenseManagerAlarm		
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 status changed to "ok").	-	-

Cloud License Manager Alarm

The alarm is applicable to the Floating License and Flex License.

Table 2-47: 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 or Flex License.
Source Varbind Text	Board#1

Alarm	acCloudLicenseManagerAlarm		
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 or Flex License.	"Floating license cannot be enabled when device is managed by License Pool."	Disable the Floating License or Flex License on the device. Remove the device from the Fixed License Pool in OVOC.
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

Alarm	acCloudLicenseManagerAlarm		
			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 ■ 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	Check TCP/TLS connectivity.

Alarm	acCloudLicenseManagerAlarm		
		connection"	
	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 or Flex 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 restart.	-	-

Floating License Alarm

The alarm is applicable only to the Flex License and Floating License and to the following products: Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software.

Table 2-48: acFloatingLicenseAlarm

Alarm	acFloatingLicenseAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.138
Description	The alarm is sent when insufficient memory resources (physical memory) exist for the capacity of the user-defined (Custom) Allocation Profile configured for the Floating License on the Floating License page.
Default Severity	Warning
Source Varbind Text	Board#1

Alarm	acFloatingLicenseAlarm		
Event Type	processingErrorAlarm		
Additional Info	Detailed explanation of the problematic parameter, requested and actual value. For example: "SignalingSessions – requested 10000, allocated 1000"		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Warning	An attempt was made to configure a customized Allocation Profile with values that exceed the device's capacity support based on physical memory.	"Not enough memory to allocate for 'custom' profile."	Configure an Allocation Profile within the bounds of the device's capacity support.

Metering Alarm

The alarm is applicable only to Mediant VE.

Table 2-49: acMeteringAlarm

Alarm	acMeteringAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.146		
Description	The alarm is sent when the device fails to communicate with the 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).		
Default Severity	Warning		
Source Varbind Text	Board#1 (SystemMO)		
Event Type	communicationsAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	The device is unable	"No connection to	Check the network

Alarm	acMeteringAlarm		
	to send a usage report to the metering service after it initially connected to it.	metering API – service will be down in <hours> hours"	configuration and make sure that the device has the appropriate environment as required for the metering offer.
Critical	■ The device is unable to establish an initial connection with the metering API. - or - ■ The device 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.
Critical	The device is blocked by the metering license server.	“Service is blocked by metering license server”	-
Cleared	The device successfully communicates with the metering API.	"Device succeeds to communicate with metering API"	-

Network Alarms

This section describes alarms concerned with the network.

Clock Configuration Alarm

Table 2-50: acClockConfigurationAlarm

Alarm	acClockConfigurationAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.149

Alarm	acClockConfigurationAlarm		
Description	The alarm is sent when multiple source clock synchronization methods are enabled (NTP, SIP Date header, and/or PTP) for the device. In this scenario, the device uses the clock synchronization method in this order of priority: NTP, then SIP Date header, and then PTP. For example, if you enable both NTP and SIP Date header, the device uses NTP (ignoring SIP Date header settings). If you enable both SIP Date header and PTP, the device uses SIP Date header (ignoring PTP settings). **Note:** PTP is applicable only to Mediant VE/CE SBCs deployed on Azure or Hyper-V.		
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 enabled.	"Clock Synchronization from SIP Date header ignored as NTP is enabled"	Disable one of the clock synchronization methods.
Minor	Clock synchronization by PTP and NTP are enabled.	"Clock Synchronization from PTP ignored as NTP is enabled."	Disable one of the clock synchronization methods.
Minor	Clock synchronization by SIP Date header, PTP, and NTP are enabled.	"Clock Synchronization from SIP Date header and PTP ignored as NTP is enabled."	Disable two of the clock synchronization methods.
Minor	Clock synchronization by	"Clock Synchronization	Disable one of the clock

Alarm	acClockConfigurationAlarm		
	SIP Date header and NTP are enabled.	from SIP Date header ignored as NTP is enabled."	synchronization methods.
Minor	Clock synchronization by SIP Date header and PTP are enabled.	"Clock Synchronization from PTP ignored as SIP is enabled."	Disable one of the clock synchronization methods.
Cleared	Only one clock synchronization method is enabled.	-	-

NTP Server Status Alarm

Table 2-51: 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 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		
Source Varbind Text	Board#1		
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

Alarm	acNTPServerStatusAlarm		
			configured incorrectly in the device).
Minor	No communication to NTP server after the time was already set once.	-	-

Ethernet Link Alarm

Table 2-52: 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).		
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 inter-

Alarm	acBoardEthernetLinkAlarm		
			face 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.	-	**Note:** For High-Availability (HA) systems, the alarm's behavior is different when sent from the redundant or active device. The alarm from the redundant is sent 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.

Ethernet Group Alarm

This alarm is applicable only to Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 3100, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software.

Table 2-53: acEthernetGroupAlarm

Alarm	acEthernetGroupAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86		
Description	The alarm is sent when an Ethernet port in an Ethernet Group goes down. **Note:** If an Ethernet Group is configured with two ports and only one port goes down, the alarm is not sent.		
Default Severity	Major		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Text	Ethernet Group alarm. %s		
Severity	Condition	Text	Corrective Action
Major	Ethernet Group is configured with only one port and the port is down.	"Ethernet Group alarm. Ethernet Group <ID> is Down"	-
Major	Ethernet Group is configured with two ports and both ports are down.	"Ethernet Group alarm. Ethernet Group (ID> is Down"	-
Cleared	Ethernet Group configured with only one port: alarm cleared when the port comes up again. Ethernet Group configured with two ports: alarm is cleared when at least one port comes up again.	-	-

LDAP Lost Connection Alarm

Table 2-54: acLDAPLostConnection

Alarm	acLDAPLostConnection
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.75
Default Severity	Minor
Source Varbind Text	Board#1/LdapServer#<ID>
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 2-55: acOCSPServerStatusAlarm

Alarm	acOCSPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.78
Default Severity	Major / Clear
Source Varbind Text	Board#1
Event Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Alarm Text	OCSP server alarm
Corrective Action	Try any of the following:

Alarm	acOCSPServerStatusAlarm
	■ Repair the Online Certificate Status Protocol (OCSP) server ■ Correct the network configuration

IPv6 Error Alarm

Table 2-56: acIPv6ErrorAlarm

Alarm	acIPv6ErrorAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.53		
Description	The alarm is sent when there is an issue with an IPv6 Interface in the IP Interfaces table.		
Default Severity	Critical		
Source Varbind Text	System#0/Interfaces#<n>.		
Event Type	operationalViolation		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Critical	Invalid IPv6 address configured in the IP Interfaces table (already exists).	"IP interface alarm: IPv6 configuration failed, IPv6 will be disabled."	■ Find a new IPv6 address. ■ Restart the device. **Note:** The alarm remains in Critical severity until the device restarts (a Clear trap is not sent).

Alarm	acIPv6ErrorAlarm		
Major	When the IP Interface is configured in the IP Interfaces table for dynamic IPv6 addressing (i.e., 'Interface Mode' configured to **IPv6 Stateless** or **IPv6 DHCP**) and no IP address is received within 10 seconds.	"Dynamic address not exist, no response from server"	Check that the server is online.
Cleared	A valid IPv6 address is configured, or an IPv6 address is received for dynamic IPv6 addressing, or the IP Interface is deleted.	-	-

HTTP Proxy NGINX Alarms

This section describes the alarms related to HTTP Proxy Services (NGINX).

NGINX Configuration is Invalid

Table 2-57: acNGINXConfigurationIsInvalidAlarm

Alarm	acNGINXConfigurationIsInvalidAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.130

Alarm	acNGINXConfigurationIsInvalidAlarm		
Description	The alarm is sent when NGINX Directives Sets have been configured with invalid syntax. NGINX continues to run with the previous, valid configuration unless the device is restarted, in which case, the NGINX process is stopped and the NGINX Process is not Running alarm is sent (see below).		
Alarm Title	NGINX configuration is not valid		
Alarm Source	operationalViolation		
Alarm Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	<text>	Corrective Action
Minor	NGINX Directives Sets have been configured with invalid syntax.	"NGINX Configuration file is not valid."	Identify and resolve NGINX Directives Sets syntax errors to ensure an uninterrupted HTTP Proxy service. You can run 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 resulting from the invalid Directives Set configuration.

NGINX Process Not Running

Table 2-58: acNGINXPprocessIsNotRunningAlarm

Alarm	acNGINXPprocessIsNotRunningAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.131
Description	The alarm is sent when the device is restarted with an erroneous

Alarm	acNGINXPprocessIsNotRunningAlarm		
	NGINX configuration (i.e., after the alarm "NGINX Configuration is not Valid" is sent (see above).		
Alarm Source	communicationsAlarm		
Alarm Title	NGINX process could not be started		
Alarm Type	alarmTrap		
Probable Cause	applicationSubsystemFailure		
Severity	Condition	<text>	Corrective Action
Major	The device is restarted with an erroneous NGINX configuration.	"NGINX process is not running."	Correct the NGINX Directives syntax (the NGINX process will restart automatically).

HTTP Proxy Service Alarm

Table 2-59: acHTTPProxyServiceAlarm

Alarm	acHTTPProxyServiceAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.108		
Description	The alarm is sent when an HTTP host specified in the Upstream Groups table is down. The trap is cleared when the host is back up.		
Source Varbind Text	System#0/HTTPProxyService#<num> System#0/EMSService#<num>		
Event 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	1. Ping the host. If there is no ping, contact your provider. The probable reason is that the host is down.

Alarm	acHTTPProxyServiceAlarm		
		Group name) is OFFLINE"	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 device's (internal) routing table is functioning correctly. 4. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to service is available again.	-	-

Active Alarm Table Alarm

Table 2-60: 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	"Active	■ Some alarm information may be lost

Alarm	acActiveAlarmTableOverflow		
	alarms to fit in the active alarm table	alarm table overflow"	but the ability of the device to perform its basic operations is not impacted. ■ A restart is the only way to completely clear a problem with the active alarm table. ■ Contact AudioCodes Support.
Remains 'Major' until restart. A 'Clear' trap is not sent.	After the alarm is sent	-	Note that the status remains 'Major' until restart as it denotes a possible loss of information until the next restart. 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.

AWS Security Role Alarm

This alarm is applicable only to Mediant VE and Mediant CE.

Table 2-61: acAWSSecurityRoleAlarm

Alarm	acAWSSecurityRoleAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.139		
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 resources.		
Default Severity	Major		
Source Varbind Text	Board#1		
Event Type	securityServiceOrMechanismViolation		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	Text	Corrective Action

Alarm	acAWSSecurityRoleAlarm		
Major	IAM role was not found, or access to AWS services was blocked	"AWS IAM role permissions error"	Refer to the device's *Installation Manual* for information on adding a proper IAM role to the instance.
Cleared	IAM role was found and permission to access AWS services was granted	-	-

Audio Staging from APS Server Alarm

This alarm is applicable only to Mediant 1000 (for backward compatibility).

Table 2-62: acAudioProvisioningAlarm

Alarm	acAudioProvisioningAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.14		
Description	The alarm is sent if the device is unable to provision its audio.		
Default Severity	Critical		
Source Varbind Text	System#0/AudioStaging#0		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError (7)		
Severity	Condition	Text	Corrective Action
Critical	Media server times out waiting for a successful audio distribution from the APS (Audio Provisioning Server)	"Unable to provision audio"	a. From the Audio Provisioning Server (APS) GUI, ensure that the device

Alarm	acAudioProvisioningAlarm		
			is properly configured with audio and that the device has been enabled. **b.** Ensure that the IP address for the APS has been properly specified on the device. **c.** Ensure that both the APS server and application are in-service. **d.** For more information regarding the problem, view the Syslogs from the device as well as the APS manager logs.
Cleared	After the alarm is sent, the media server is successfully provisioned with audio from the APS	-	

RTP Only Broken RTP Connection Alarm

This alarm is applicable only to Mediant VE, Mediant CE and Mediant SE.

Table 2-63: acRtpOnlyBrokenRtpConnectionAlarm

Alarm	acRtpOnlyBrokenRtpConnectionAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.160
Description	The alarm is sent when the RTP-Only feature is configured and a broken RTP connection exists for at least one of the RTP-only sessions (streams). For configuring the RTP-only sessions feature, see the [RtpOnly] ini file parameter in the device's User's Manual.

Alarm	acRtpOnlyBrokenRtpConnectionAlarm		
Default Severity	Warning		
Source Varbind Text	Board#1		
Event Type	Other		
Probable Cause	Other		
Severity	Condition	Text	Corrective Action
Major	At least one of the RTP-only sessions is in broken state.	"Broken RTP connection on at least one RTP-only session"	-
Cleared	All RTP-only sessions are in idle or connected states.	-	-

Weak Password Alarm

Table 2-64: acWeakPasswordAlarm

Alarm	acWeakPasswordAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.156		
Description	The alarm is sent when a user in the Local Users table is configured with a weak password, according to the Weak Passwords List table. (This weak passwords feature is enabled by the 'Check Weak Passwords' parameter.)		
Default Severity	Major		
Source Varbind Text	WebUsers#X (where *X* is the row index of the user in the Local Users table)		
Event Type	securityServiceOrMechanismViolation		
Probable Cause	Weak Password		
Alarm Severity	Condition	Text	Corrective Action

Alarm	acWeakPasswordAlarm		
Major	A user is configured with a weak password.	"User <username> has weak password"	Configure the user with a strong password.
Cleared	The user's password is no longer weak (or the user has been deleted in the Local Users table).	-	-

Analog Port Alarms

These alarms are applicable only to analog (FXS or FXO) interfaces (MP-1288, Mediant 500L, Mediant 800, Mediant 1000).

Analog Port SPI Out-of-Service Alarm

The alarm is applicable only to products with analog interfaces (MP-1288, Mediant 500L, Mediant 800, Mediant 1000).

Table 2-65: 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	"Analog Port SPI out of service"	■ No corrective action is required. ■ The device shuts down the port and

Alarm	acAnalogPortSPIOutOfService		
	service		activates it again when the Serial Peripheral Interface (SPI) connection returns.
Cleared	Analog port is back in service	-	-

Analog Port High Temperature Alarm

The alarm is applicable only to products with analog interfaces (MP-1288, Mediant 500L, Mediant 800, Mediant 1000).

Table 2-66: 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
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

The alarm is applicable only to FXS interfaces for the following products: Mediant 500L, Mediant 800, and Mediant 1000.

Table 2-67: 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.

FXS Blade Service Alarm

This alarm is applicable only to MP-1288.

Table 2-68: acModuleServiceAlarm

Alarm	acModuleServiceAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.122
Description	The alarm is sent due to a hardware failure on the FXS blade, due to the following: ■ Multiple FXS ports are out-of-service (due to high temperature, Serial Peripheral Interface or electrical shortage). ■ DSP failure (due to high temperature), causing FXS ports to go out-of-service.

Alarm	acModuleServiceAlarm		
Alarm Source	Chassis/Module# (Analog)		
Event Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Severity	Condition	Alarm Text	Corrective Action
Major	■ More than 33% of FXS ports on the FXS blade are out-of-service. ■ Hardware failure (DSP) on the FXS blade. If the fault is due to exceeding 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. If the alarm is sent as a result of a high DSP temperature, you must cold restart the device (power off and then power on) to return the blade to service.
Minor	More than five FXS ports but less than 33% of FXS ports are out-of-service on the FXS blade. Major to Minor: Less than 25% of FXS ports are out-of-service on the FXS blade.	"Multiple FXS ports are Out-Of-Service"	Service the faulty blade.
Clear	Less than 4 FXS ports are out-of-service on the FXS blade.	-	-

FXS Blade Operation Alarm

This alarm is applicable only to MP-1288.

Table 2-69: acModuleOperationAlarm

Alarm	acModuleOperationalAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.123		
Description	The alarm is sent when an operational hardware failure occurs on the FXS ports or on the FXS blades (DSP and CPU).		
Alarm Source	Chassis/Module# (Analog / CPU)		
Event Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Severity	Condition	Text	Corrective Action
Major	Operational hardware failure on more than 33% of FXS ports on the FXS blade.	"Operational failure was detected on Analog/CPU blade"	Service the faulty FXS blade.
	Operational DSP/CPU hardware failure on the FXS blade and the problem could not be resolved after successive restart attempts.	"Blade is out-of-service due to operational failure"	Cold restart (power off and then on) the device to return the blade to service.
Minor	Operational hardware failure on up to 33% of FXS ports on the FXS blade. Major to Minor: hardware failure on less than 25% of the FXS ports on the FXS blade.	"Operational failure was detected on Analog/CPU blade"	Service the faulty blade.
Clear	No hardware failure on any of the FXS ports on the FXS blade.		

Port Service Alarm

This alarm is applicable only to MP-1288.

Table 2-70: acPortServiceAlarm

Alarm	acPortServiceAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.124		
Description	The alarm is sent when an FXS port is out of service due to one of the following: ■ The Serial Peripheral Interface (SPI) connection with the port is lost. ■ The temperature of the port has exceeded the temperature threshold. ■ The port is inactive due to a ground fault.		
Alarm Source	Chassis/Module#/FXS Port #		
Event Type	equipmentAlarm		
Probable Cause	outOfService		
Severity	Condition	Text	Corrective Action
Minor	The FXS port is faulty due to the reasons described above. **Note:** ■ If the number of faulty FXS ports is greater than four on the same FXS blade, the acModuleOperationAlarm alarm is sent. ■ If there were active call sessions on the device, these calls are disconnected. No new SIP outbound calls will be initiated towards the FXS line.	"FXS Port state was changed to Out of Service" **Note:** Detailed reason is provided in the Syslog and Web interface (detailed port status description and tooltip per FXS port).	Service the faulty FXS port.
Clear	The alarm is cleared when: ■ The Serial Peripheral Interface (SPI) connection is restored. ■ The FXS port temperature falls below the threshold.	-	-

Alarm	acPortServiceAlarm		
	■ The ground fault is cleared. ■ The acModuleServiceAlarm alarm is sent (i.e. the number of faulty FXS ports on the blade is greater than four).		

Analog Line Left Off-hook Alarm

This alarm is applicable only to FXS interfaces (MP-1288, Mediant 500L, Mediant 800, and Mediant 1000).

Table 2-71: 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

This section describes the media-related SNMP alarms.

Media Process Overload Alarm

This alarm is applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.

Table 2-72: 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		
Source Varbind Text	Board#1		
Event Type	environmentalAlarm		
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 2-73: 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

No Route to IP Group Alarm

Table 2-74: 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	Board#1 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

Alarm	acIpGroupNoRouteAlarm		
	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-mentioned reasons.	"IP Group is temporarily 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).		-

IDS Policy Alarm

Table 2-75: acIDSPolicyAlarm

Alarm	acIDSPolicyAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99

Alarm	acIDSPolicyAlarm		
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)."		
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.

Media Cluster Alarms

This section describes the alarms for the Media Cluster feature.

These alarms are applicable only to Mediant 9000 and Mediant Software.

Cluster Bandwidth Utilization Alarm

This alarm is applicable to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE) and the Elastic Media Cluster feature (Mediant CE).

Table 2-76: acClusterBandwidthAlarm

Alarm	acClusterBandwidthAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.126		
Description	The alarm is sent when the bandwidth utilization of a Cluster interface exceeds the configured maximum bandwidth (refer to the MtcClusterNetworkMaxBandwidth parameter).		
Default Severity	Minor		
Source Varbind Text	Board#1/EthernetLink#<ethernet port number>		
Event 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).		
Severity	Condition	Text	Corrective Action
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	Reduce the number of Media Components on the Cluster interface. Alternatively, the overall permitted bandwidth for the Cluster interfaces should be increased, if possible, using the ini file parameter [MtcClusterNetworkMaxBandwidth].

Alarm	acClusterBandwidthAlarm		
		Interface"	
Minor	Bandwidth utilization is between 85 and 90%. Note: If a Major alarm was sent and the bandwidth later declined to between 80 and 85%, the alarm is changed to Minor.	"Cluster Bandwidth is above 85% utilization on Interface name: <name>"	
Cleared	Bandwidth utilization is less than 80%.	-	-

Cluster HA Usage Alarm

This alarm is applicable only to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC).

Table 2-77: acMtcmClusterHaAlarm

Alarm	acMtcmClusterHaAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.115
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.

Alarm	acMtcmClusterHaAlarm		
Default Severity	Major		
Alarm Source	device/clusterManager		
Event Type	equipmentAlarm		
Probable Cause	Other		
Severity	Condition	Alarm Text	Corrective Action
Major	Cluster HA usage exceeds 100%.	"At least one of the MTCEs is inactive, MTC will now provide only partial HA"	■ Make sure all Media Components are properly connected to the Cluster Manager. ■ Make sure all Media Components in the Media Components table show "Unlocked" for the Admin State field and "Connected" for the Status field.
Cleared	HA usage drops to below 95%	-	-

Media Cluster Alarm

- This alarm is applicable only to the Elastic Media Cluster feature (Mediant CE).
- 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.

Table 2-78: acMediaClusterAlarm

Alarm	acMediaClusterAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.133		
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.		
Default Severity	Major		
Alarm Source	Device/clusterManager		
Event Type	-		
Probable Cause	-		
Severity	Condition	Text	Corrective Action
Major	Media Cluster is enabled, but 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.
Cleared	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	-

Media Component Fan Tray Module Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE).

Table 2-79: acMtceHwFanTrayFailureAlarm

Alarm	acMtceHwFanTrayFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.119		
Description	The alarm is sent upon a failure in the Fan Tray module of the Media Component (MC type).		
Default Severity	Minor		
Alarm Source	…./MTCE#1/fanTray#1		
Event Type	equipmentAlarm		
Probable Cause	heatingVentCoolingSystemProblem		
Severity	Condition	Alarm Text	Corrective Action
Minor	Failure in Fan Tray module of Media Component	"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 Component High Temperature Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE).

Table 2-80: acMtceHwTemperatureFailureAlarm

Alarm	acMtceHwTemperatureFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.118
Description	The alarm is sent when the temperature of the Media Component (MC type) chassis reaches a critical threshold.
Default Severity	Major
Alarm Source	Board#1/clusterManager#0/MTCE#xxx

Alarm	acMtceHwTemperatureFailureAlarm		
Event Type			
Probable Cause			
Severity	Condition	Alarm Text	Corrective Action
Major	Temperature of Media Component reaches critical threshold	"MTCE reached high temperature threshold"	1. 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. 2. Check the chassis ventilation outlet and make sure that they are not obstructed for air flow. 3. Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Connectivity with Media Component is re-established and temperature is reduced	-	-

Media Component Network Failure Alarm

This alarm is applicable to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE) and the Elastic Media Cluster feature (Mediant CE).

Table 2-81: acMtceNetworkFailureAlarm

Alarm	acMtceNetworkFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.116		
Description	The alarm is sent when the Cluster Manager (Media Transcoding Cluster feature) or Signaling Component (Elastic Media Cluster feature) fails to connect to the Media Component.		
Default Severity	Major		
Source Varbind Tex	Board#1/clusterManager#0/MTCE#xxx		
Event Type	communicationsAlarm		
Probable Cause	Other		
Severity	Condition	Alarm Text	Corrective Action
Major	Connection failure with Media Component	"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 Component	-	-

Media Component Power Supply Module Failure Alarm

This alarm is applicable only to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE).

Table 2-82: acMtcePsuFailureAlarm

Alarm	acMtcePsuFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.120		
Description	The alarm is sent upon a failure in the Power Supply module of the Media Component (MC type).		
Default Severity	Minor		
Alarm Source	…./MTCE#1/powerSupply#1		
Event Type	equipmentAlarm		
Probable Cause	powerProblem		
Severity	Condition	Alarm Text	Corrective Action
Minor	Failure in Power Supply module of Media Component	"MTCE power supply unit fault"	1. Check if the Power Supply module is inserted in the chassis. 2. If it was removed from the chassis, re-insert it. 3. If the Power Supply module is inserted in the chassis and the alarm is still sent, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Power Supply module status returns to normal	-	-

Media Component Software Upgrade Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature (Mediant 9000 and Mediant VE) and the Elastic Media Cluster feature (Mediant CE).

Table 2-83: acMtceSwUpgradeFailureAlarm

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

Remote Media Interface Alarm

- This alarm is applicable only to the Elastic Media Cluster feature (Mediant CE).
- 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.

Table 2-84: acMediaClusterRemoteInterfaceAlarm

Alarm	acMediaClusterAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.134		
Description	For each Media Component, the alarm is sent in the following scenarios: 1. A remote media interface (eth…) exists (configured in the Remote Media Interface table) and is used by one or more Media Realms, but is not configured on the Media Component. 2. A remote media interface (eth…) exists, and is used by one or more Media Realms, and a NAT rule is configured (in the NAT Translation table) for this remote media interface, but a public IP address for this remote media interface is not configured on the Media Component. 3. A remote media interface (eth…) exists and is used by one or more Media Realms, but its status on the Media Component is link down.		
Default Severity	Major		
Alarm Source	device/clusterManager/MC		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Severity	Condition	Text	Corrective Action
Major	According to description #1 above.	"Interface <Interface ID>, Name: <eth…> - Alarm Status is RmifMissing"	Configure the appropriate remote media interface (eth…) in the Remote Media Interface table.
	According to description #2 above.	"Interface <Interface ID>, Name: <eth…> - Alarm Status is PublicIpAddrMissing"	Allocate a public IP address for the media interface (eth…) on the Media Component or remove the NAT

Alarm	acMediaClusterAlarm		
			rule (from the NAT Translation table).
	According to description #3 above.	"Remote Interface Alarm: Interface <Interface ID>, Name: <eth…> - Alarm Status is LinkDown"	Troubleshoot the media interface (eth…) on the Media Component.

MC Not Secured Alarm

The alarm is applicable only to the Media Transcoding Cluster feature (Mediant VE) and the Elastic Media Cluster feature (Mediant CE).

Table 2-85: acMCNotSecuredAlarm

Alarm	acMCNotSecuredAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.151		
Description	This alarm is sent when the connection between the Signaling Component (SC) and at least one of the Media Components (MC) remains unsecured when the upgrade of all the MCs by SC does not fully complete. This typically happens when SC failover occurs during the upgrade of the MCs from an unsecured media cluster version to a secured (TLS) one.		
Default Severity	Warning		
Source Varbind Text	Board#1/clusterManager#0/MTCE#xxx		
Event Type	securityServiceOrMechanismViolation		
Probable Cause	versionMismatch		
Severity	Condition	Text	Corrective Action
Warning	When the SC is configured to operate in the secured (TLS) mode and then a switchover to the redundant SC occurs,	"MC <MTCEName> should be upgraded" "MC <MTCEName>	Reset or upgrade the MC.

Alarm	acMCNotSecuredAlarm		
	an MC in the cluster still connects to SC in an unsecured (TCP) mode. As a result, the connection between SC and MC remains unsecured.	should be restarted"	
	SC is configured to operate in the secured (TLS) mode and MC is configured to operate in the unsecured (TCP) mode. However, there is no MC image in the SC repository and therefore, the MC cannot be upgraded and is still connected in the unsecured mode.	"MC <MTCEName> should be upgraded"	Upload an MC image to the SC repository and then upgrade the MC that is currently connected in the unsecured mode.
Cleared	■ The MC successfully connects to SC in the secured (TLS) mode. ■ The firmware upgrade of the MC is successful and a secured connection (TLS) is established between the SC and MC.	-	-

3 SNMP Trap Events (Notifications)

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

These trap events are sent with a severity varbind value of "Indeterminate". These traps don't 'Clear' and don't appear in the Alarms History table or Active Alarms table. The only trap event that sends a 'Clear' is acKpiThresholdCrossing.

For High-Availability (HA) systems, the source varbind text for alarms that are raised by the redundant device is "Redundant#1" (instead of "Board#1" for the active device).

Authentication Failure Trap

Table 3-1: authenticationFailure

Event	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB
Description	The alarm is sent if the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated.

Board Initialization Completed Trap

This is the AudioCodes Enterprise application cold start trap.

Table 3-2: 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 restart.
MIB	AcBoard
Severity	cleared
Event Type	equipmentAlarm
Probable	Other(0)

Event	acBoardEvBoardStarted
Cause	
Alarm Text	Initialization Ended

Dial Plan File Replaced Trap

This trap event is applicable only to analog and digital interfaces (MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000 and Mediant 3100).

Table 3-3: 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	
Condition	Successful dial plan file replacement
Trap Text	"Dial plan file replacement complete."

Cold Start Trap

Table 3-4: 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.

Configuration Change Trap

Table 3-5: 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.

Debug Recording Activation Alarm

Table 3-6: acDebugRecordingActivationAlarm

Alarm	acDebugRecordingActivationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.150		
Description	The trap event is sent when Debug Recording is enabled on the device ('Debug Recording Destination IP' parameter)		
Default Severity	Warning		
Source Varbind	Board#1		
Event Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	Text	Corrective Action
Minor	Debug recording is activated on the device.	"Debug Recording is active"	-
Cleared	Debug recording is stopped.	-	-

Enhanced BIT Status Trap

Table 3-7: 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
Additional Info-2	BIT Results: ■ BIT_RESULT_PASSED ■ BIT_RESULT_FAILED
Additional Info-3	Buffer: Number of bit elements reports
Corrective Action	Not relevant

High-Availability (HA)

This section describes the SNMP trap events concerned with the High-Availability (HA) system.

Hitless Software Upgrade Status Trap

This trap event is applicable only to products supporting HA (Mediant 500, Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant Software).

Table 3-8: acHitlessUpdateStatus

Event	acHitlessUpdateStatus	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48	
Description	The notification trap is sent at the beginning and end of a Hitless Software Upgrade, which is used in the High Availability system. Failure during the software upgrade also activates the trap.	
Default Severity	Indeterminate	
Event Type	Other (0)	
Probable Cause	Other (0)	
Source	Automatic Update	
Trap Text	Condition	Corrective Action
"Hitless: Start software upgrade."	Hitless Upgrade has begun.	Corrective action is not required
"Hitless: SW upgrade ended successfully."	Successful Hitless Upgrade.	Corrective action is not required
"Hitless: Invalid cmp file - missing Ver parameter."	Hitless Upgrade failed because the cmp file is invalid. The cmp file's version parameter is incorrect.	Replace the cmp file with a valid one.
"Hitless fail: SW ver stream name too long."	Hitless Upgrade failed because the cmp file is invalid. The number of characters defining the software version stream name in the cmp file has been exceeded.	Replace the cmp file with a valid one
"Hitless fail: Invalid cmp file - missing UPG parameter."	Hitless Upgrade failed because the cmp file is invalid. An upgrade parameter is missing from the file.	Replace the cmp file with a valid one.
"Hitless fail: Hitless SW upgrade not supported."	Hitless Upgrade failed because the cmp file is invalid. The cmp file does not support Hitless Upgrade of the current software version to the new	Replace the cmp file with a valid one that supports hitless upgrade of the software from the current

Event	acHitlessUpdateStatus	
	software version.	version to the new one.

HTTP Download Result Trap

Table 3-9: 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.

Intrusion Detection System (IDS)

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

IDS Threshold Cross Notification Trap

Table 3-10: acIDSThresholdCrossNotification

Event	acIDSThresholdCrossNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100

Event	acIDSThresholdCrossNotification
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 IP+port) crossing a threshold of an active alarm.
Event Type	Other
Alarm Text	Threshold crossed for scope value IP. Severity=minor/major/critical. Current value=NUM
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 3-11: 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.
Event Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	"Added IP * to blacklist" "Removed IP * from blacklist"
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.

Keep-Alive Trap

Table 3-12: 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. For HA-supporting products: If the device is also in High-Availability mode (HA) and the active and redundant devices are synchronized with one another, the trap is sent by the active device with the acBoardTrapGlobalsAdditionalInfo3 varbind, which contains the redundant device's serial number (S/N). **Note:** Keep-alive is sent every 9/10 of the time configured by the [NatBindingDefaultTimeout] parameter.
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

KPI Performance Monitoring Threshold Crossing Trap

Table 3-13: acKpiThresholdCrossing

Alarm	acKpiThresholdCrossing		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.148		
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).		
Default Severity	Depends on the configured severity level (in the Alarm Thresholds table).		
Source Varbind Text	The source varbind indicates the performance monitoring parameter object for which the threshold is being crossed.		
Event Type	logTrap		
Probable Cause	thresholdCrossed		
Trap Text	Depends on the configured message (in the Alarm Thresholds table).		
Severity	Condition	Text	Corrective Action
Raised alarm (severity depends on configuration)	Configured threshold to raise alarm has been crossed.	"<Performance Monitoring Parameter Name> value <Value> is too <High or Low>" (**Note:** Text is configurable.)	-
Cleared alarm (severity depends on configuration)	Configured threshold to clear alarm has been crossed.	"<Performance Monitoring Parameter Name> value <Value> is back to normal" (**Note:** Text is configurable.)	-

Link Down Trap

This trap event is applicable only to MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 3100, Mediant 2600, and Mediant 4000.

Table 3-14: 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”.

Link Up Trap

This trap event is applicable only to MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 3100, Mediant 2600, and Mediant 4000.

Table 3-15: 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 changes from “down”. Categorized by the RFC as an “enterprise-specific trap”.

Secure Shell (SSH) Connection Status Trap

Table 3-16: acSSHConnectionStatus

Event	acSSHConnectionStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Default Severity	indeterminate

Event	acSSHConnectionStatus
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 3-17: acProxyConnectivity

Event	acProxyConnectivity
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.103
Description	The trap is sent when the device loses connectivity with a specific proxy IP address of a Proxy Set. The trap is cleared when the proxy connection is up.
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

Event	acProxyConnectivity		
Severity	Condition	Text	Corrective Action
Indeterminate	Connectivity to the proxy server is lost.	"Proxy Server <IP address>:<port> is now OUT OF SERVICE"	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.
Cleared	Connectivity to the proxy is available again.	"Proxy Server <IP address>:<port> is now IN SERVICE"	-

Web User Access Denied due to Inactivity Trap

Table 3-18: acWebUserAccessDisabled

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

Event	acWebUserAccessDisabled
Cause	
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 3-19: 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,

Event	acActivityLog
	Web, CLI and REST. For SNMP activity, the username refers to the SNMP community string.

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, 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-52471