

# Alarms Monitoring Guide

*AudioCodes One Voice Operations Center (OVOC)*

# OVOC

## Alarms

Version 8.2



**OVOC**  
one voice operation center

**ac**audiocodes

## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: November-20-2022

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

## Documentation Feedback

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

## Stay in the Loop with AudioCodes



Document Name
<b>OVOC Documents</b>
Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center
One Voice Operations Center IOM Manual
One Voice Operations Center Product Description

Document Name
One Voice Operations Center User's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Agent Installation and Configuration Guide
ARM User's Manual
<b>Documents for Managed Devices</b>
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500Li MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800 MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Microsoft Teams Direct Routing SBA Installation and Maintenance Manual

Document Name
Mediant 800B/1000B/2600B SBA for Skype for Business Installation and Maintenance Manual
Fax Server and Auto Attendant IVR Administrator's Guide
Voca Administrator's Guide
VoiceAI Connect Installation and Configuration Manual

## Document Revision Record

LTRT	Description
41810	<p>Updates for Version 8.2 and Version 8.2.1000:</p> <ul style="list-style-type: none"><li>■ Added OVOC alarm Table Partition Management Error Event.</li><li>■ Added IP Phone alarm: IPP Server SSL Certificate Could Not Be Proven</li><li>■ Added Vocanom System and Agent alarms.</li><li>■ Added SBC alarms: No Reply From DNS Server Alarm; Weak Password alarm</li><li>■ Update to Meeting Insights alarm Call Recording Error Event</li></ul>

---

## Table of Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Standard Events</b>	<b>3</b>
	Cold Start	3
	Link Down	3
	Link Up	4
	Entity Configuration Change	5
	Authentication Failure	5
<b>3</b>	<b>Management Alarms</b>	<b>7</b>
	EMS Trap Receiver Binding Error	7
	GW Connection Alarm	7
	GW Mismatch Alarm	8
	Configuration Mismatch	10
	OVOC Server Started	10
	OVOC Disk Space Alarm	11
	Software Replaced	12
	Hardware Replaced	12
	HTTP/HTTPS Access Disabled	13
	PM File Generated	14
	PM Polling Error	15
	Cold Start Missed	16
	GW Backup Event	16
	Security Alarm	17
	Security Event	18
	Topology Update Event	19
	Topology File Event	20
	Synchronizing Alarms Event	21
	Synchronizing Active Alarms Event	22
	OVOC License Key Alarm	22
	Suppressed Alarm <Name>	23
	OVOC Keep Alive Alarm	24
	Pre-provisioning Alarm	25
	Endpoint Publish Alarm	26
	Disk Space Alarm	26
	Oracle Disk Space Alarm	27
	License Alarm	28
	Synchronizing Alarms	29
	QoE Sip Message Status Alarm	30
	Floating License Extended	31
	Floating License Device Report Alarm	31
	Floating License Register Successful Event	32

Floating License Register Failure Alarm .....	32
Floating License Failure to Send Usage Report Alarm .....	33
Floating License Failure to Send Extended Usage Report Alarm .....	33
Floating License Service Shutdown Alarm .....	34
Floating License Manage Devices above Allow Maximum .....	35
Floating License Registered Devices Requests Capacity .....	35
Alarms Overflow .....	36
Alarms Forward Overflow .....	37
FQDN Resolve Event .....	37
PM Timeout Event .....	38
PM Token Pool is Empty .....	39
PM Polling Status Event .....	39
PM Batch Overflow Alarm .....	43
PM Has No SNMP Connection .....	43
FlexPool License Usage .....	44
UMP Users Scheduler Time Exceeded Alarm .....	45
Teams Connection Alarm .....	46
URI Exceeded Storing Limit Event .....	47
Low IO Rate Performance Event .....	48
Teams Subscription Alarm .....	49
Certificate Expiration Alarm .....	51
PostgreSQL Table Partition Management Error Event .....	52
<b>4 Voice Quality Package Alarms .....</b>	<b>55</b>
OVOC QoE - Failed Calls Alarm .....	55
OVOC QoE – Poor Voice Quality Alarm .....	56
OVOC QoE - Average Call Duration Alarm .....	58
OVOC QoE - License Key Alarm .....	59
OVOC QoE - System Load Alarm .....	60
Call Details Storage Level Change .....	61
Call Quality Monitoring Connection Status Alarm .....	62
OVOC QoE - Skype for Business SQL Server Connection Lost Alarm .....	63
OVOC QoE - Active Directory Server Connection Lost Alarm .....	64
OVOC QoE - Media Bandwidth Alarm .....	64
OVOC QoE - Rule Max Concurrent Calls Alarm .....	66
Report Schedulers Time Event .....	67
Report Schedulers Load Alarm .....	68
Report Schedulers Execution Event .....	69
<b>5 Device Manager Alarms .....</b>	<b>70</b>
Registration Failure Alarm .....	70
IP Phone Survivable Mode Start Alarm .....	70
IP Phone Lync Login Failure Alarm .....	71
Endpoint License Alarm .....	72

Endpoint Server Overloaded Alarm .....	73
IP Phone Speaker Firmware Download Failure .....	73
IP Phone Speaker Firmware Upgrade Failure .....	74
IP Phone Conference Speaker Connection Failure .....	75
IP Phone General Local Event .....	75
IP Phone Web Successive Login Failure .....	76
IP Phone Requires Reset .....	77
Jabra Firmware Upgrade Failed .....	78
VIP Endpoint is Not Registered or Offline .....	78
VIP Endpoint is Disconnected .....	79
Remote Control Battery Drained .....	80
Remote Control is not Connected .....	80
USB Port Shutdown due to over Current Exceeded .....	81
Peripheral Device is Missing .....	82
IPP Server SSL Certificate Could Not Be Proven .....	83
<b>6 OVOC Managed Devices Alarms .....</b>	<b>85</b>
Support Matrix .....	85
Common Device Alarms .....	94
Board Fatal Error .....	94
Entity Configuration Change .....	95
Configuration Error .....	96
Initialization Ended .....	97
Board Resetting Following Software Reset .....	97
Feature Key Related Error .....	98
Gateway Administrative State Changed .....	98
No Free Channels Available .....	100
Gatekeeper/Proxy not Found or Registration Failed .....	101
Ethernet Link Down Alarm .....	103
System Component Overloaded .....	104
Active Alarms Table Overflow .....	105
Operation State Change [Node] .....	106
Keep Alive Trap .....	107
NAT Traversal Alarm .....	108
Enhanced BIT Status Trap .....	109
Threshold of Performance Monitored Object Exceeded .....	110
HTTP Download Result .....	110
IPv6 .....	111
SAS Emergency Mode Alarm .....	112
Software Upgrade Alarm .....	113
NTP Server Status Alarm .....	113
LDAP Lost Connection .....	114
SSH Connection Status [Event] .....	115

OCSP Server Status Alarm .....	115
Media Process Overload Alarm .....	116
Ethernet Group Alarm .....	116
Media Realm BW Threshold Alarm .....	117
Certificate Expiry Notification .....	118
Web User Access Disabled .....	119
Proxy Connection Lost .....	119
IDS Policy Alarm .....	121
IDS Threshold Cross Notification .....	122
IDS Blacklist Notification .....	123
Proxy Connectivity .....	124
Web User Activity Log Trap .....	125
HTTP Proxy Service Alarm .....	126
Answer-Seizure Ratio Threshold Alarm .....	127
Average Call Duration Threshold Alarm .....	128
Network Effectiveness Ratio Threshold Alarm .....	129
IP Group No Route Alarm .....	130
TLS Certificate Expiry Alarm .....	131
NGINX Configuration is not Valid .....	133
NGINX Process is not Running .....	134
Remote Monitoring Alarm .....	134
SDR Server Alarm .....	135
KPI Threshold Crossing .....	136
Clock Configuration Alarm .....	137
Debug Recording Activation Alarm .....	137
Faulty DSP Alarm .....	138
No Reply From DNS Server Alarm .....	139
Weak Password Alarm .....	140
Specific Hardware Alarms .....	141
Temperature Alarm .....	141
Fan Tray Alarm .....	142
Power Supply Alarm .....	143
HA System Alarms .....	144
HA System Fault Alarm .....	144
HA System Configuration Mismatch Alarm .....	150
HA System Switch Over Alarm .....	151
Hitless Software Upgrade Alarm .....	152
Redundant Board Alarm .....	153
HA Network Watchdog Status Alarm .....	154
License Key Hitless Upgrade Alarm .....	155
HA Network Mismatch Alarm .....	156
HA Network Monitor Alarm .....	156
HA Ethernet Group Alarm .....	157
License Pool Alarms .....	158
License Pool Infra Alarm .....	158

License Pool Application Alarm .....	160
License Pool Over Allocation Alarm .....	161
Floating License Alarms .....	162
Floating License Alarm - Not Enough Memory to Allocate 'Custom' Profile .....	162
Cloud License Manager Alarm .....	163
Flex License Manager Alarm .....	165
Mediant 2600 E-SBC and Mediant 4000 SBC Alarms .....	166
DSP Farms Mismatch Alarm .....	166
Mediant 9000 and Software SBC Alarms .....	167
Cluster HA Alarm .....	168
Media Transcoder Network Failure .....	169
Media Transcoder Software Upgrade Failure .....	169
Media Transcoder High Temperature Failure .....	170
Media Transcoder Fan Tray Module Failure .....	171
Media Transcoder Power Supply Module Failure .....	172
Cluster Bandwidth Utilization Alarm .....	173
Media Cluster Alarm .....	174
Remote Interface Alarm .....	176
AWS Security Role Alarm .....	177
CDR Server Alarm .....	178
Metering Alarm .....	178
MC Not Secured Alarm .....	179
TLS Certificate Mismatch Alarm .....	181
Stack Manager Alarms .....	182
REST API Failure .....	182
Stack Manager Down .....	184
Stack Manager Status Error .....	186
Stack Manager Configuration Error .....	187
Stack Manager Accelerated Network Error .....	188
Stack Manager No HA .....	189
Stack Manager Activity Log .....	189
MP-1288 Alarms .....	190
Module Service Alarm .....	190
Module Operation Alarm .....	191
Port Service Alarm .....	192
MSBR Alarms .....	193
WAN Link Alarm .....	193
Power Over Ethernet Status [Event] .....	194
Wireless Cellular Modem Alarm .....	195
Wireless Cellular Modem Status Changed .....	195
Data Interface Status .....	196
NQM Connectivity Alarm .....	197
NQM RTT Alarm .....	197
NQM Jitter Alarm .....	198
NQM Packet Loss Alarm .....	199

NQM MOS CQ Alarm .....	200
NQM MOS LQ Alarm .....	201
<b>Mediant 3000 Hardware Alarms .....</b>	<b>202</b>
PEM Module Alarm .....	202
SA Module Missing Alarm .....	203
User Input Alarm .....	204
TM Inconsistency .....	204
TM Reference Status .....	205
TM Reference Change .....	206
<b>PSTN Trunk Alarms .....</b>	<b>206</b>
D-Channel Status .....	206
SONET Section LOF Alarm .....	207
SONET Section LOS Alarm .....	208
SONET Line AIS Alarm .....	209
SONET Line RDI Alarm .....	210
SONET/SDN IF Failure Alarm .....	210
Trunk LOS Alarm .....	211
Trunk LOF Alarm .....	212
Trunk AIS Alarm .....	213
Trunk RAI Alarm .....	213
V5.2 Interface Alarm .....	214
SONET Path STS LOP Alarm .....	215
SONET Path STS AIS Alarm .....	216
SONET Path STS RDI Alarm .....	216
SONET Path Unequipped Alarm .....	217
SONET Path Signal Label Alarm .....	218
DS1 Line Status Alarm .....	218
DS3 RAI Alarm .....	220
DS3 AIS Alarm .....	220
DS3 LOF Alarm .....	221
DS3 LOS Alarm .....	221
NFAS Group Alarm .....	222
B Channel Alarm .....	223
<b>Analog Port Alarms .....</b>	<b>223</b>
Analog Port SPI Out of Service .....	224
Analog Port High Temperature .....	224
Analog Port Ground Fault Out-of-Service Alarm .....	225
Dial Plan File Replaced Trap .....	225
Analog Line Left Off Hook Alarm .....	226
<b>UMP-365 and CloudBond Microsoft Platform Alarms .....</b>	<b>226</b>
Commit License Failed .....	226
Component Unreachable .....	227
Component Restart .....	228
Performance Counter General .....	229
Performance Counter Service .....	230

Component Service Status .....	231
Component Event Viewer .....	231
Component Event Viewer Past Hours .....	232
Component Event Viewer Dropped .....	233
Alarm-Admin License Expired .....	233
Certificate Expired Alarm .....	234
Alarm-Disk Space .....	235
Fax Server .....	236
System Alarms .....	236
Component Unreachable .....	236
Component Restart .....	237
Component Resource Failed .....	238
Component Resource Down .....	238
Agent Alarms .....	239
Component Performance Counter General .....	239
Performance Counter Service .....	240
Component Service Status .....	241
Component Event Viewer .....	242
Component Event Viewer Past Hours .....	243
Component Event Viewer Dropped .....	243
Certificate Expired .....	244
Disk Space .....	245
License Alarms .....	245
Admin License Expired .....	245
Admin License Violation .....	246
IVR Alarms .....	247
System Alarms .....	247
IVR Alarm – Component Unreachable .....	247
IVR Component Restart .....	248
IVR Component Resource Down .....	248
Agent Alarms .....	249
IVR Component Performance Counter General .....	249
IVR Component Performance Counter Service .....	250
IVR Component Service Status .....	251
IVR Component Event Viewer .....	252
IVR Component Event Viewer Past Hours .....	252
IVR– Component Event Viewer Dropped .....	253
IVR Certificate Expired .....	254
IVR Disk Space .....	254
License Alarms .....	255
IVR Admin License Expired .....	255
IVR Admin License Violation .....	256
Vocanom Alarms .....	257
System Alarms .....	257
Voca Alarm – Component Unreachable .....	257

Voca Component Restart .....	258
Agent Alarms .....	258
Voca Component Performance Counter General .....	258
Voca Component Service Status .....	259
Voca Certificate Expired .....	260
Voca Disk Space .....	261
Voca Agent Specific Alarms .....	262
Alarm –Wrong Operating Component .....	262
Alarm –Wrong Settings .....	263
Alarm – Connection Failure .....	264
Microsoft Teams Direct Routing SBA Alarms .....	265
System Alarms .....	265
SBA Alarm – Component Unreachable .....	265
Component Restart .....	266
System Action Failed .....	266
Alarm – System Cloud Status .....	267
Alarm – Wrong Operating .....	268
Alarm – Component Resource Down .....	268
Agent Alarms .....	269
Alarm – Component Performance Counter General .....	269
Alarm – Component Performance Counter Service .....	270
Alarm – Component Service Status .....	271
Event – Component Event Viewer .....	272
Alarm – Component Event Viewer Past Hours .....	272
Alarm – Component Event Viewer Dropped .....	273
Alarm – Certificate Expired .....	274
Alarm – Disk Space .....	274
License Alarms .....	275
Alarm – Admin License Expired .....	275
SBA Skype for Business Alarms .....	276
Alarm – CPU Status .....	276
SBA Memory Status .....	277
SBA Disk Space Alarm .....	278
SBA Certificate Expired .....	279
Alarm – Performance Counter .....	280
SBA Services Status Alarm .....	281
User Management Pack 365 (UMP) Alarms .....	282
Wrong Operating Alarm .....	282
UMP Tenant License Threshold Alarm .....	284
UMP User License Threshold Alarm .....	285
UMP Super Admin Authentication Fail Event (Service Provider) .....	285
UMP End User License Threshold Alarm .....	286
UMP Azure AD Sync Alarm .....	287
UMP Office 365 Failure Alarm .....	287
UMP Office 365 Command Execution Event .....	288

UMP User Settings Fail Event .....	289
UMP End User Authentication Fail Event .....	289
CloudBond 365 Alarms .....	290
Alarm-Admin License Expired .....	290
10SmartTAP Alarms .....	291
SmartTAP System Alarms .....	291
Alarm – Component Unreachable .....	291
SmartTAP Event – Component Restart .....	292
Event – Component Resource Failed .....	292
Alarm - Component Resource Threshold Exceeded .....	293
Alarm – Connection Failure .....	294
SmartTAP Agent Alarms .....	295
Alarm – Component Performance Counter General .....	295
Alarm – Component Service Status .....	296
Alarm – Component Event Viewer Dropped .....	297
Alarm – Certificate Expired .....	297
10Alarm – Disk Space .....	298
SmartTAP Application Server Alarms .....	298
Call Recording Error Event .....	298
Event – Configuration Error .....	299
Recording Resource Failure .....	300
Meeting Insights Alarms .....	301
Connection Failure .....	301
Call Recording Error Event .....	303
Performance Counter General .....	304
Component Service Status .....	305
Alarm Certificate Expired .....	306
Alarm Disk Space .....	307
ARM Alarms .....	308
Disk Size Illegal .....	308
Disk Space Usage .....	308
ARM License About to Expire .....	309
ARM License has Expired .....	310
ARM License Session Number .....	311
ARM License Missing .....	312
Quality Change .....	312
ARM Configurator Reload .....	313
ARM Router Reload .....	314
ARM Routing Rule Match .....	315
ARM Configuration Inconsistency .....	315
Operation State Changed (Router) .....	316
Operation Status Changed [Node] .....	318
Operation Status Changed [Peer Connection] .....	319
Operation Status Changed [LDAP Server] .....	321
Operational Status Changed [Active MQ] .....	322

Limit Reached .....	323
Router Using Other Configurator .....	323
NTP Sync Status .....	324
No Available Routers .....	325
Registration Status Resync Threshold .....	326
External Web Service .....	327
Disk Usage Alarm .....	328
CAC Usage .....	331
Calls Duration Quota Usage .....	333
VoiceAI Connect Alarms .....	335
Status DB Connection Failure Alarm .....	335
All Session Managers Down Alarm .....	336
SBC Failure Alarm .....	337
SBC Failure Per Session Manager Alarm .....	338
TTS Failure Alarm .....	339
TTS Failure Per Session Manager Alarm .....	340
Bot Failure Alarm .....	341
Bot Failure Per Session Manager Alarm .....	342
STT Failure Alarm .....	343
STT Failure Per Session Manager Alarm .....	344
Failed Calls Alarm .....	345
Failed Calls Per Session Manager Alarm .....	346
TTS Delay Alarm .....	347
Call Duration Alarm .....	348
Active Calls Per Session Manager Alarm .....	349
CPU Usage Alarm .....	350
Disk Usage Alarm .....	351
Memory Usage Alarm .....	352
Auto Update Not Working Alarm .....	353
Auto Update Failure Alarm .....	354
Session Manager Down Alarm .....	355
End-To-End Keep Alive Failed Alarm .....	356
Failed Key Retrieval per Session Manager Alarm .....	357
Remote Manager is Down Alarm .....	360
User Defined Alarms .....	360

# 1 Introduction

This document describes alarms that are raised on OVOC and its managed entities. These alarms are displayed in the One Voice Operations Center Web interface Active Alarms table. Supported alarms / events can fall into one of these three categories:

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

To determine which traps are defined as Events refer to 'Alarm Name' or 'Alarm Title' fields in the table. All the events are marked with [Event] prefix in the OVOC Active Alarms table and Alarms History windows.

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

Alarm Field	Description
Alarm Title (Name)	The alarm name, as it appears in the OVOC Active Alarms and History tables.
Description	Documented description of the alarm.
SNMP Trap Name	NOTIFICATION-TYPE Name as it appears in the MIB.
SNMP OID	NOTIFICATION-TYPE OID as it appears in the MIB. Corrective Action Possible corrective action when applicable. - 1
Alarm Source	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource
Alarm Type	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsType.
Probable Cause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.
Additional Info	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo1, tgTrapGlobalsAdditionalInfo2 and tgTrapGlobalsAdditionalInfo3. The document includes a few examples of the possible values of this field.

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

## 2 Standard Events

This section describes the Standard Events.

### Cold Start

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

### Link Down

Alarm Field	Description
Description	SNMPv2-MIB: A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
SNMP Alarm	[Event] linkDown

Alarm Field	Description
SNMP OID	1.3.6.1.6.3.1.1.5.3
Alarm Title	Link Down
Alarm Type	Communication Alarm
Alarm Source	-
Probable Cause	Other
Severity	Major
Additional Info1,2,3	-
Corrective Action	-

## Link Up

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

Alarm Field	Description
Info1,2,3	
Corrective Action	-

## Entity Configuration Change

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

## Authentication Failure

Alarm Field	Description
Description	SNMPv2-MIB: An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

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

### 3 Management Alarms

This section describes the Management alarms.

#### EMS Trap Receiver Binding Error

Alarm Field	Description
Description	This alarm is generated during server startup if an error occurs indicating that the SNMP trap receiver port is already taken.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.1
SNMP Alarm	acEMSSnmpCannotBindError
Alarm Title	[Event] EMS Trap Receiver Binding Error
Alarm Source	OVOC Mgmt
Alarm Type	Environmental Alarm
Probable Cause	Application Subsystem Failure
Severity	Critical
Additional Info	-
Corrective Action	<p>Run netstats command to verify which application uses the alarms reception port (by default UDP post 162).</p> <ul style="list-style-type: none"> <li>■ OVOC application: If it's busy, check which application uses this port. If it's not freed by OVOC application, restart the OVOC server application as described in the OVOC Server IOM.</li> <li>■ Other network management application: change OVOC application and all managed gateways' default alarm reception ports.</li> </ul>
Media Gateways	All the gateways managed by OVOC

#### GW Connection Alarm

Alarm Field	Description
Description	Originated by OVOC when an SNMP Timeout occurs for the first time

Alarm Field	Description
	in the Media Gateway.
SNMP Alarm	acEMSNodeConnectionLostAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.3
Alarm Title	GW Connection Alarm
Alarm Source	Media Gateway
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure
Severity	Critical
Additional Info	When an SBA is configured, displays the 'SBA Description' field.
Corrective Action	<p>Communication problem: Try to ping the gateway to check if there is network communication.</p> <ul style="list-style-type: none"> <li>■ Default gateway alive: Open the network screen. Check the default gateway IP address and ping it.</li> <li>■ SNMP Community Strings: Verify that the community string defined in OVOC for the gateway matches the actual gateway community strings. To check the community string, right-click on the gateway, select the 'Details' menu. Default community strings: read = public, write = private.</li> <li>■ Hardware Problem: Check that the gateway is alive according to the LEDs. Verify that network and power cables are in place and plugged in.</li> </ul>
Media Gateways	All the gateways managed by OVOC

## GW Mismatch Alarm

Alarm Field	Description
Description	<p>Activated when OVOC detects a hardware, software, predefine or configuration mismatch.</p> <ul style="list-style-type: none"> <li>■ Software Mismatch: Activated when OVOC detects a software version mismatch between the actual and the previous definition of the Media Gateway (for example, Version 4.0.353 instead of the previously defined 4.0.278). This is also the case when the new</li> </ul>

Alarm Field	Description
	<p>version is not defined in the Software Manager.</p> <ul style="list-style-type: none"> <li>■ Hardware Mismatch: Activated when OVOC detects a hardware mismatch between the actual and the previous definition of a Media Gateway.</li> <li>■ Configuration Mismatch: Activated when OVOC detects a configuration mismatch between the actual parameter values provisioned and previous parameter values provisioned.</li> </ul>
SNMP Alarm	acEMSNoMismatchNodeAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.9
Alarm Title	GW Mismatch Alarm
Alarm Source	<ul style="list-style-type: none"> <li>■ Media Gateway/Software</li> <li>■ Media Gateway/Hardware</li> <li>■ Media Gateway/Configuration</li> </ul>
Alarm Type	Equipment Alarm
Probable Cause	Other
Severity	Clear
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Software Mismatch: <ul style="list-style-type: none"> <li>✓ Define the detected version in the OVOC Software Manager</li> <li>✓ Perform a Software Upgrade on the gateway with one of the supported versions.</li> </ul> </li> <li>■ Hardware Mismatch: <ul style="list-style-type: none"> <li>✓ Perform remove / add a device in order to resync OVOC and the gateway status</li> <li>✓ Verify in the Software Manager that an appropriate version exists for the hardware type displayed in the error message</li> </ul> </li> <li>■ Configuration Mismatch: <ul style="list-style-type: none"> <li>✓ Run Configuration Verification command in order to compare OVOC configuration and actual MG configuration:</li> </ul> </li> </ul>

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

## Configuration Mismatch

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

## OVOC Server Started

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

Alarm Field	Description
SNMP OID	acEMSServerStartup- 1.3.6.1.4.1.5003.9.20.3.2.0.11
AlarmTitle	[Event] OVOC Server Started
AlarmSource	Management
Alarm Type	Communications Alarm
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	All the gateways managed by OVOC.

## OVOC Disk Space Alarm

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

Alarm Field	Description
Additional Info	
Corrective Action	Free disk space

## Software Replaced

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

## Hardware Replaced

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

Alarm Field	Description
	MAC address) to what was initially defined, while the Hardware Type remains the same. Hardware Replace is discovered by the MAC address and performed during Board Started trap.
SNMP Alarm	acEMSHardwareReplaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.15
Alarm Title	[Event] Hardware Replaced
Alarm Type	Equipment Alarm
Alarm Source	Media Gateway
Probable Cause	Other
Severity	Major
Additional Info	-
Corrective Action	-
Media Gateways	MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000

## HTTP/HTTPS Access Disabled

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

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

## PM File Generated

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

Alarm Field	Description
Media Gateways	All Gateways

## PM Polling Error

Alarm Field	Description
Description	Originated when a History PM stops collecting performance summary data from MG. Possible reasons are: NTP synchronization lost, Connection Loss, SW Mismatch, etc.
SNMP Alarm	acEMSPmHistoryAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.19
Alarm Title	[Event] PM Polling Error
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Severity	Minor
Additional Info	-
Corrective Action	<p>Verify in the 'Description' (see above) the reason why the PM history stopped.</p> <ul style="list-style-type: none"> <li>■ When the reason is 'NTP synchronization lost', verify that the gateway and the OVOC server machine are synchronized to the same NTP server and have accurate time definitions.</li> <li>■ When the reason is 'Software Mismatch', you can stop the PM history collection until the new version is added to the Software Manager.</li> <li>■ When the reason is 'Connection Loss' between the OVOC server and the gateway, polling continues automatically when the connection is re-established; the purpose of the alarm in this case is to inform users of missing samples.</li> </ul> <p>Note: The alarm continues to activate every 15 minutes unless you fix the problem or manually stop PM polling of the gateway.</p>
Media Gate-	All Gateways

Alarm Field	Description
ways	

## Cold Start Missed

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

## GW Backup Event

Alarm Field	Description
Description	This alarm is raised when an AudioCodes device configuration file cannot be retrieved due to insufficient disk space or periodic backup operation failure.
SNMP Alarm	acEMSMGBBackupEvent
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.21

Alarm Field	Description		
Alarm Title	GW Backup Event		
Alarm Source	<Device IP address>		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	Corrective Action
Minor	periodic backup failed due to insufficient disk space	Backup file from IP:{0} with MG name: {1} was not retrieved due to low OVOC Mgmt disk space.	Check disk and free some space.
Minor	periodic backupbackup failed	Periodic Backup operation failed for MG {0} with IP:{1}	
Indeterminate	periodic backup success	backup file: {file} from ip: {ip} with mg name: {name} was successfully retrieved.	

## Security Alarm

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

Alarm Field	Description
Probable Cause	Other
Severity	Minor, Major, Critical
Additional Info	-
Corrective Action	-
Media Gateways	-

## Security Event

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

Alarm Field	Description
ways	

## Topology Update Event

Alarm Field	Description
Description	<p>This event is issued by OVOC when a Gateway or Region is added/removed/updated in OVOC and includes the following information:</p> <ul style="list-style-type: none"> <li>■ Action: Add / Remove / Update GW or Region</li> <li>■ Region Name</li> <li>■ GW Name</li> <li>■ GW IP</li> </ul> <p><b>Note:</b> For opening an EMS client in the MG context, the gateway IP address should be provided.</p>
SNMP Alarm	acEMSTopologyUpdateEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.25
Alarm Title	[Event] Topology Update
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Severity	Indeterminate
Additional Info	<p>Additional Info 1 field will include following details:</p> <p>Region: X1 'X2' [GW: Y1 'Y2' 'Y3' 'Y4']</p> <p>X1 = Region ID (unique identifier in the OVOC data base used for region identification)</p> <p>X2 = Region name as it defined by OVOC operator</p> <p>Y1 = GW ID (unique identifier in the OVOC data base used for GW identification)</p> <p>Y2 = GW Name as it defined by OVOC operator</p> <p>Y3 = GW IP as it defined by OVOC operator</p> <p>Y4 = GW Type as it identified by OVOC during the first connection to the gateway. If first connection was not successful during the add operation,</p>

Alarm Field	Description
	<p>it will trigger an 'Add GW' event with Unknown GW type, and 'Update GW' event once the initial connection to the gateway has been successful. The following gateways will be supported: MP, M1K, M2K, M3K, M5K, M8K</p> <p>Region details will always be part of the alarm, while GW info will be displayed when event is gateway-related.</p> <p>All the fields related to the gateway will always be displayed to allow easy parsing.</p> <p>Examples:</p> <p>(Description=Add Region)      Region: 7 'Test Lab'</p> <p>(Description=Update Region)      Region: 7 'My Updated Region'</p> <p>(Description=Add GW)      Region: 7 'My Updated Region', GW: 22 'MG14' '1.2.3.4' 'Unknown', PM Polling: disabled</p> <p>(Description=Update GW)      Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7' 'M3K'</p> <p>(Description=Update GW)      Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7', PM Polling: enabled</p> <p>(Description=Remove GW)      Region: 7 'My Updated Region', GW: 22 'My MG 15' '4.5.6.7' 'M3K', Polling: enabled</p> <p>(Description=Remove Region)      Region: 7 'My Updated Region'</p>
Corrective Action	-
Media Gateways	-

## Topology File Event

Alarm Field	Description
Description	This event is issued by OVOC when the Topology File is updated on the OVOC server machine. The Topology file is automatically updated upon the addition /removal of a Media Gateway or upon updates to the Media Gateway properties. For more information, refer to the Northbound Integration Guide.
SNMP Name	acEMSTopologyFileEvent-
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.26

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

## Synchronizing Alarms Event

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

Alarm Field	Description
Corrective Action	-
Media Gateways	-

## Synchronizing Active Alarms Event

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

## OVOC License Key Alarm

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

Alarm Field	Description		
SNMP Alarm	acEMSLicenseKeyAlarm		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.29		
Alarm Title	OVOC License Key Alarm		
Alarm Source	OVOC Mgmt/license		
Alarm Type	other		
Probable Cause	keyexpired		
Additional Info	In case the OVOC license expires: OVOC license key expiration date: <expiration date>		
Corrective Action	In case the OVOC license expires: ■ Contact AudioCodes for new license  In case of the missing license in device: ■ If required, contact AudioCodes for new license		
Alarm Severity	Condition	Text	Corrective Action
Critical	expired	OVOC Mgmt Application License is expired	
Major	Month before	OVOC Mgmt Application License will be expired within one month	
Critical	Device not have OVOC management license	GW management is not covered by current OVOC Mgmt Application License	

## Suppressed Alarm <Name>

Alarm Field	Description
Description	This alarm is sent when the OVOC suppresses alarms (of the same alarm type and alarm source), once the number of such alarms reaches a configured threshold level in a configured interval (configured in the

Alarm Field	Description
	OVOC Alarms Settings screen). When this alarm is sent, such alarms are not added to the OVOC database and are not forwarded to configured destinations.
SNMP Alarm	acEMSAAlarmSuppression
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.42
Alarm Title	The name of the suppressed alarm
Alarm Source	OVOC Mgmt or OVOC QoE/<IP address_Managed Entity>
Alarm Text	Alarm Suppression activated
Alarm Type	Other
Probable Cause	Threshold crossed.
Severity	Indeterminate
Status Changes	The alarm is cleared when in the subsequent interval, the number of such alarms falls below the configured threshold. Once the alarm is cleared, then these alarms are once more added to the OVOC database and forwarded to configured destinations.
Additional Info	-
Corrective Action	Investigate the recurrence of such alarms.

## OVOC Keep Alive Alarm

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

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

## Pre-provisioning Alarm

Alarm Field	Description
Description	This alarm is generated when the operation for pre-provisioning the device upon initial connection to OVOC fails.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.46
AlarmTitle	Pre-Provisioning
AlarmSource	OVOC Mgmt
AlarmType	operational/Violation
Probable Cause	The template file could not be applied to the device because there was a mismatch between the template file and the device's existing ini file or there was a mismatch between the device type and the firmware file applied to the device.
Severity	Critical
Additional Info	-
Corrective Action	<p>■ When this alarm is raised, you cannot reload configuration or firmware files to the device as it has already been connected to OVOC. Instead download these files to the device using the Software Manager and then use the 'Software Upgrade' action.</p> <p>OR</p>

Alarm Field	Description
	<ul style="list-style-type: none"> <li>■ Remove the device from OVOC and then reconnect it i.e. repeat the pre-provisioning process.</li> </ul>
Media Gateways	All gateways managed by OVOC.

## Endpoint Publish Alarm

Alarm Field	Description
Description	<p>This alarm is raised when problems arise with the SIP Publish reporting for voice quality metrics (port 5060) from endpoints (RFC 6035).</p> <ul style="list-style-type: none"> <li>■ When a SIP Publish message is missing mandatory parameter/s required by OVOC to handle this message.</li> <li>■ When SIP Publish message time is not synchronized with OVOC server.</li> </ul>
SNMP Alarm	acEndpointPublishAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.47
Alarm Title	Endpoint Publish Alarm
Alarm Source	OVOC_QoE/<Endpoint IP>
Alarm Type	Communications alarm
Alarm Text	Bad Publish Message. Device IP: {ip}, Device MAC: {mac}.
Probable Cause	Communications protocol error
Additional Info	<p>Possible reasons:</p> <p>Mandatory Field/s Missing.</p> <p>Endpoint Server and Device Synchronization Error.</p>
Severity	Minor

## Disk Space Alarm

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

Alarm Fields	Description
	<ul style="list-style-type: none"> <li>■ The Archive Logs directory capacity has reached {0}%.</li> <li>■ The Oracle partition capacity has reached {0}%.</li> </ul>
SNMP Alarm	acEMSDiskSpaceAlarmCheck
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.51
AlarmTitle	Disk Space Alarm
AlarmSource	OVOC Mgmt
AlarmType	Equipment Alarm
Probable Cause	Storage Capacity Problem
Severity	<ul style="list-style-type: none"> <li>■ 70% &lt; Minor</li> <li>■ 80% &lt; Major</li> <li>■ 90% &lt; Critical</li> </ul>
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>■ The Archive Logs directory: Free space in /ACEMS/NBIF/emsBackup/DBEMS/archivelog/ to avoid system failure.</li> <li>■ The Oracle partition: Free space using the command <code>rm -f /oracle/DIAG/diag/rdbms/dbems/dbems/trace/*.tr*</code> to avoid system failure.</li> </ul>
Media Gateways	-

## Oracle Disk Space Alarm

Alarm Field	Description
Description	This alarm is issued when the Oracle partition capacity has reached {0}% of its disk capacity.
SNMP Alarm	acEMSNotEnoughOracleSpaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.52
AlarmTitle	Oracle Disk Space Alarm

Alarm Field	Description
AlarmSource	OVOC Mgmt
AlarmType	Equipment Alarm
Probable Cause	Storage Capacity Problem
Severity	<ul style="list-style-type: none"> <li>■ 70% &lt; Minor</li> <li>■ 80% &lt; Major</li> <li>■ 90% &lt; Critical</li> </ul>
Additional Info	-
Corrective Action	Free space using the command <code>rm -f /oracle/DIAG/diag/rdbms/dbems/dbems/trace/*.tr*</code> to avoid system failure.
Media Gateways	-

## License Alarm

Alarm Field	Description
Description	This alarm is issued when the OVOC License approaches or reaches its expiration date or OVOC server machine ID is no longer valid.
SNMP Alarm	acLicenseAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.53
Alarm Title	License Alarm
Alarm Source	OVOC Mgmt
Alarm Type	Other
Probable Cause	Other
Additional Info	Info1: <ul style="list-style-type: none"> <li>■ Machine ID In The License Is {0}</li> <li>■ Expiration Date In The License Is {0}</li> </ul>

Alarm Field	Description		
Alarm Severity	Condition	<text>	Corrective Action
Critical	The license expiration date is less than equal to 7 days.	<ul style="list-style-type: none"> <li>■ OVOC License is about to expire in {0} days.</li> <li>■ OVOC License is about to expire in 1 day.</li> <li>■ OVOC License Will Expire Today</li> </ul>	Contact your AudioCodes partner ASAP. Note that when notification that this license has expired is received, the server remains connected for a few minutes in order to allow the forwarding traps to northbound destinations.
Major	The license expiration date is more than 7 days and less than equal to 30 days.	OVOC License is about to expire in {0} days.	
Clear	The license expiration date is greater than 30 days.		

## Synchronizing Alarms

Alarm Field	Description
Description	This event is sent out to an SMMP NBI using user defined alarms forwarding rules once the NMS has activated the ReSync Alarms feature.
SNMP Alarm	ac OCReSyncEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.58
Alarm Title	[Event] Synchronizing Alarms
Alarm Source	OVOC Mgmt
Alarm Type	Other

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

## QoE Sip Message Status Alarm

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

## Floating License Extended

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

## Floating License Device Report Alarm

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

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

## Floating License Register Successful Event

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

## Floating License Register Failure Alarm

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

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

## Floating License Failure to Send Usage Report Alarm

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

## Floating License Failure to Send Extended Usage Report Alarm

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

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

## Floating License Service Shutdown Alarm

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

## Floating License Manage Devices above Allow Maximum

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

## Floating License Registered Devices Requests Capacity

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

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

## Alarms Overflow

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

## Alarms Forward Overflow

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

## FQDN Resolve Event

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

Alarm Field	Description		
Additional Info			
Corrective Action	Check if another device with the same IP already exists in OVOC (same as the resolved configured FQDN).		
Alarm Severity	Condition	Text	Corrective Action
Major		FQDN : <fqdn> resolved to IP: <IP> . IP address already exist . IP address for node name <name> changed to empty value	
Major		FQDN : <fqdn> resolved to IP: <IP> . IP address for node name <name> changed to <IP>	

## PM Timeout Event

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

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

## PM Token Pool is Empty

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

## PM Polling Status Event

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

Alarm Details	Description		
	<div>circumstances:</div> <div><div><div></div></div> When a specific device is successfully polled.</div> <div><div><div></div></div> For the failure scenarios described below.</div> <div><div><div><div><div></div></div></div><div>This event is sent only when the 'Send Event per Interval' parameter is enabled in the Performance Monitoring profile.</div></div></div>		
SNMP Alarm	acDevicePmPollingEvent		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.76		
Alarm Title	PM Polling Status Event		
Alarm Source	OVOC Mgmt/ PM Handle		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	Raised when the device is successfully polled.	Success: PM polling operation was successfully finished. deviceName=Device Name ; deviceIp= 1.1.1.1 ; pollingTimeStamp= 12:15	-
Major	The time format for the device's system clock is in a different format to the time settings for the OVOC server clock.	Device time has not valid format	Synchronize the time settings.
	Device connection timeout	Device timeout	Troubleshoot the device connection.
	Device configuration is	Device is not Sync	Download updated configuration to

Alarm Details	Description		
	not synchronized		the device.

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

Alarm Details	Description		
Cleared	The last polling reason type was unknown.	Unknown LastPollingFailReasonType failure	-
	-	-	-

## PM Batch Overflow Alarm

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

## PM Has No SNMP Connection

Alarm Field	Description
Description	This system event is raised when the internal SNMP process for managing the polling operation fails.

Alarm Field	Description		
SNMP Alarm	acPmHasNoSnmpConnection		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.78		
Alarm Source	OVOC Mgmt/ PM Token Pool Handler		
Alarm Title	PM Has No SNMP Connection		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	The internal SNMP process for managing the polling operation has failed.	PM process has no SNMP connection to the Main SNMP service ; startTime= 12:00 ; endTime= 12:15 ; currentTime= 12:01	-
Cleared	-	-	

## FlexPool License Usage

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

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

## UMP Users Scheduler Time Exceeded Alarm

Alarm Field	Description
Description	This alarm is raised when there is a timeout for the Active Directory connection and when this action fails for UMP for a specific customer.
SNMP Alarm	acUMPUsersSchedulerAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.86
Alarm Source	<ul style="list-style-type: none"> <li>■ OVOC QoE/UMP User Sync</li> <li>■ OVOC QoE/ 'name of the specific customer'</li> </ul>
Alarm Title	UMP Users Scheduler Time Exceeded Alarm
Alarm Type	Processing Error Alarm
Probable Cause	<ul style="list-style-type: none"> <li>■ If cause type is CLEARED: <ul style="list-style-type: none"> <li>✓ UMP Users sync task was restarted</li> <li>✓ UMP Users sync task for customer: 'name of the specific customer' was restarted.</li> </ul> </li> <li>■ If cause type is not CLEARED: <ul style="list-style-type: none"> <li>✓ UMP Users sync task was terminated due to exceeded time running.</li> <li>✓ UMP Users sync task for customer: 'name of the specific customer' was failed.</li> </ul> </li> </ul>

Alarm Field	Description		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Minor	<ul style="list-style-type: none"> <li>■ UMP users synchronization timeout</li> <li>■ UMP users synchronization for a specific customer failed</li> </ul>	<ul style="list-style-type: none"> <li>■ UMP Users sync task was terminated due to exceeded time running</li> <li>■ UMP Users sync task for customer: 'name of the specific customer' was failed.</li> </ul>	Check the connection with the Active Directory.
Cleared	UMP User Synchronization success full	<ul style="list-style-type: none"> <li>■ UMP Users sync task was restarted</li> <li>■ UMP Users sync task for customer: 'name of the specific customer' was restarted.</li> </ul>	

## Teams Connection Alarm

Alarm Field	Description
Description	This alarm is raised when calls notifications cannot be received from MS Cloud due to connection and Calls Notifications subscription issues.
SNMP Alarm	acTeamsConnectionAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.89
Alarm Source	OVOC Mgmt/Device
Alarm Title	Teams Connection Alarm
Alarm Type	Communications Alarm
Probable Cause	Communications Subsystem Failure

Alarm Field	Description		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Any network connection issue with Microsoft Teams	Connection to MS Teams Cloud Has Been Lost	<ul style="list-style-type: none"> <li>■ Troubleshoot the network components such as firewall, DNS, certificates.</li> <li>■ Verify that the client credentials configured for the device added in OVOC are identical to those defined by customer in Azure.</li> </ul>
	Failure of MS Token creation from Microsoft Graph API		
	The Subscription does not exist or the expired Connection to Microsoft Teams Cloud has been lost		
Clear	The network issue is solved	Connection to MS Teams Cloud Has Been Established	
	MS Token created successfully after failed attempts		
	New subscription created/renewed successfully		

## URI Exceeded Storing Limit Event

Alarm Field	Description
Description	This alarm is raised when the URI Storing Limit of 2000 has been exceeded.
SNMP Alarm	acURIExceededStoringLimitEvent

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.87		
Alarm Source	OVOC Mgmt/URI Summary		
Alarm Title	URI Exceeded Storing Limit Event		
Alarm Type	Processing Error Alarm		
Probable Cause	Other		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Warning	Count of Caller and Callee URI's that matched the provided regexp has exceeded the limit.	URI Storing Limit of 2000 was exceeded.	Reduce the storing limit. Note that this value cannot be changed by users as it is a system property value.

## Low IO Rate Performance Event

Alarm Field	Description
Description	This alarm is raised when the I/O rate falls below the expected rate and as a result reduces disk speed. For example, an I/O rate decreases to 27.9 MB/s. The OVOC server runs dd command each watchdog iteration (every 30 sec) in case the I/O rate falls below the expected I/O rate.
SNMP Alarm	acLowIORatePerformanceEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.88

Alarm Field	Description		
Alarm Source	OVOC Mgmt		
Alarm Title	Low IO Rate Performance Event		
Alarm Type	Communications Alarm		
Probable Cause	Other		
Additional Info1	Example: Expected I/O rate 160 MB/s sent from 10.3.180.194		
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	The I/O rate( calculated by the dd command) fell 10% below the expected I/O rate.	I/O rate decreased to xx MB/	Check network and storage performance.
Major	The I/O rate( calculated by the dd command) fell 40% below the Expected /IO rate.	I/O rate decreased to xx MB/s	Check network and storage performance.

## Teams Subscription Alarm

Alarm Field	Description
Description	This alarm is raised when the Teams Calls Notifications subscription creation or renewal process fails for any reason.
SNMP Alarm	acTeamsSubscriptionAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.90

Alarm Field	Description		
Alarm Source	OVOC Mgmt/Device		
Alarm Title	Teams Subscription Alarm		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Failed to renew (create new initial) subscription, when the previously created subscription has expired.	Subscription failed. No active subscription exists	
	Failed to create initial subscription		
Major	Failed to renew subscription; previously created subscription has been active for less than 24 hours (between 0 to 24 hours) .	Subscription failed. Previously created subscription is active for less than 24 hours. Expires at DATETIME	
Minor	Failed to renew	Subscription failed. Previously created subscription is active for less than 48	

Alarm Field	Description		
	subscription; previously created subscription has been active for less than 48 hours (between 48 and 24 hours).	hours. Expires at DATETIME	
Clear	Subscription successfully created or renewed.	Subscription created successfully. Expires at DATETIME	

## Certificate Expiration Alarm

Alarm Field	Description		
Description	This alarm is raised when the OVOC server certificate expires.		
SNMP Alarm	acCertificateExpirationAlarm		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.94		
Alarm Title	Certificate Expiration Alarm		
Alarm Source	OVOC Server		
Alarm Type	Other		
Probable Cause	Other		
Additional Info1	Expiration date is : {0}		
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Certificate is expired	Certificate is expired	Update Certificate

Alarm Field	Description		
Major	7 Days before expiration	OVOC server certificate will expire today	Update Certificate
Minor	30 Days before expiration	OVOC server certificate will expire in {0} days	Update Certificate
Clear	Certificate is updated.		

## PostgreSQL Table Partition Management Error Event

Alarm Field	Description		
Description	This alarm is raised when problems arise during PG partitions management operations such as partitions creation and removal.		
SNMP Alarm	acPgTablePartitionManagementErrorEvent		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.97		
Alarm Title	PostgreSQL Table Partition Management Error Event		
Alarm Source	OVOC_Mgmt		
Alarm Type	Other		
Probable Cause	Other		
Additional Info1	<ul style="list-style-type: none"> <li>■ Violated partitions: &lt;partitioned_table&gt;_p&lt;range_start_time&gt; Where range_start_time is in format YYYYMMDDHH</li> <li>■ Interrupted with internal error   Violated partitions: {partition_list}</li> <li>■ Interrupted with internal error</li> </ul>		
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action

Alarm Field	Description		
Major	Partition range could not be created in the current timing window for <component> table.	Cannot create missing partitions for <component> table.	<ul style="list-style-type: none"> <li>■ Review PgPartitioner process-related errors including issuing event in /var/log/ems/pgpartitioner.csv</li> <li>■ Review PostgreSQL log for details on which partition's management failed.</li> <li>■ Check the status of the PG Partitions Manager in the OVOC Server Manager.</li> </ul>
Major	Purging of empty partition of {NAME} schema is unsuccessful.	Cannot remove empty partition of {NAME} schema.	
Major	Partitions distribution with schemas cannot be initialized.	Cannot initialize partitions distribution with schemas.	
Major	Purging of empty partitions of {schema_name} schema is unsuccessful.	Cannot remove empty partitions of {schema_name} schema.	
Major	Partition range could not be created in the current timing window for {schema_name}. {table_name} table.	Cannot create missing partitions for {schema_name}. {table_name} table.	
Major	Partitions distribution with schemas cannot be initialized.	Cannot initialize partitions distribution with schemas.	
Clear	■ Partitions can be created for		

Alarm Field	Description		
	<p>specific database table.</p> <ul style="list-style-type: none"><li>■ Empty partitions of {NAME} schema can be removed.</li><li>■ Partitions distribution with schemas can be initialized.</li><li>■ Empty partitions of {schema_name} schema can be removed.</li><li>■ Partitions can be created for {schema_name}. {table_name} table.</li><li>■ Partitions distribution with schemas can be initialized.</li></ul>		

## 4 Voice Quality Package Alarms

This section describes the Voice Quality Package alarms.

### OVOC QoE - Failed Calls Alarm

Alarm Field	Description		
Description	<p>This alarm is raised when the % number of failed calls for the managed node or link crosses the threshold and is cleared when the failed calls ratio returns below the threshold value. The description field includes the info: Failed X1% of calls, X2 of X3 calls.</p> <p>The threshold for this alarm is set in the QoE Status and Alarms Details window.</p>		
SNMP OID	acVoice QualityRuleFailedCallsAlarm		
SNMP Alarm	1.3.6.1.4.1.5003.9.20.3.2.0.30		
Alarm Title	Voice Quality - Failed Calls Alarm		
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint		
Alarm Type	Quality of service alarm.		
Probable Cause	The minimum or maximum threshold is crossed.		
Additional Info	<p>Critical or Major severity threshold is Y%:</p> <ul style="list-style-type: none"> <li>■ Critical Threshold: 10 % of calls (default)</li> <li>■ Major Threshold: 2 % of calls (default)</li> </ul> <p>Where Y% is the % failed calls per managed node or link that is measured for a total time of 180 minutes period (three hours) and according to “Monitoring Frequency Min”. For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:30) and then at 15:30 (from 12:30 to 15:30) and so on.</p>		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when Y % of calls (rep-	Y% of failed calls has	Investigate the source (device or link) of the

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

## OVOC QoE – Poor Voice Quality Alarm

Alarm Field	Description
Description	This alarm is raised when the % number of poor quality calls polled for the managed node or link crosses the threshold and is cleared when the poor quality calls ratio returns below the threshold value. The description field includes the info: Poor Quality X1% of calls, X2 of X3 calls. The threshold for this alarm is set in the QoE Status and Alarms Details window.
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.31
SNMP Alarm	acVoiceQualityRulePoorQualityCallsAlarm
Alarm Title	Voice Quality – Voice Quality Alarm
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint
Alarm Type	Quality of service alarm

Alarm Field	Description		
Probable Cause	The minimum or maximum threshold is crossed.		
Additional Info	<p>Critical or Major severity threshold is Y%:</p> <ul style="list-style-type: none"> <li>■ Critical Threshold: 10% of calls (default).</li> <li>■ Major Threshold: 2% of calls (default)</li> </ul> <p>Where Y% is the % poor quality calls per managed node or link that is measured for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (from 12:30 to 15:30) and so on.</p>		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when Y% (representing the configured critical threshold) of calls made by the managed node or link for the sampled period (see above) are of poor quality.	Y% calls have crossed the "Critical" threshold.	Investigate the source (device or link) of the poor quality calls.
Major	This alarm is raised when Y % (representing the configured major threshold) of calls by the managed node or link for the sampled period (see above) are of poor quality.	Y% calls have crossed the "Major" threshold.	
Clear	Cleared when the poor quality calls ratio returns below the threshold value for the sampled period (see above).		-

## OVOC QoE - Average Call Duration Alarm

Alarm Field	Description		
Description	<p>This alarm is raised when the average call duration time threshold for the managed node or link is crossed and is cleared when the average call duration time ratio returns below the threshold value. The description field includes the info: Average Call Duration is Y sec.</p> <p>The threshold for this alarm is set in the QoE Status and Alarms Details window.</p>		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.32		
SNMP Alarm	acVoice QualityRuleAvrgCallDurationAlarm		
Alarm Title	Voice Quality – Average Call Duration Alarm		
Alarm Source	OVOC QoE/Device/Link/Site/Endpoint		
Alarm Type	Quality of service alarm		
Probable Cause	The minimum or maximum threshold is crossed.		
Additional Info	<ul style="list-style-type: none"> <li>■ Critical Threshold: average call duration of 3 seconds (default).</li> <li>■ Major Threshold: average call duration of 5 seconds (default)</li> </ul> <p>Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to “Monitoring Frequency Min”. For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (for 12:30-15:30) and so on.</p>		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the average call duration for the managed node or link for the sampled period (see above) falls to the configured critical	Average Call Duration "Critical" threshold has been reached.	Investigate the source (device or link) reporting the excessive average call

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

## OVOC QoE - License Key Alarm

Alarm Field	Description
Description	<p>This alarm is sent in the following circumstances:</p> <ul style="list-style-type: none"> <li>■ When the number of devices connected to the OVOC approaches or reaches license capacity (shown as 'Devices Number' in OVOC server Manager License screen).</li> <li>■ When the number of sessions running on the OVOC approaches or reaches license capacity (shown as 'Voice Quality Sessions' in the OVOC Server Manager License screen).</li> </ul>
SNMP Alarm	acVoice QualityLicenseKeyAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.33
Alarm Title	Voice Quality License key alarm
Alarms Source	OVOC QoE
Alarm Type	Other
Probable Cause	Key Expired

Alarm Field	Description		
Additional Info			
Corrective Action	Contact your AudioCodes representative to obtain the required license key.		
Alarm Severity	Condition	Text	Corrective Action
Critical	The number of currently running sessions/devices has reached 100% of the Voice Quality servers license capacity.	Current server load reached 100% of VOICE QUALITY License capacity.	-
Major	The number of currently running sessions/devices has reached 80% of Voice Quality servers license capacity.	Current server load reached 80% of Voice Quality License capacity.	-
Clear	The number of currently running sessions/devices has dropped below 80% of Voice Quality servers license capacity.	Clearing currently active device alarm.	-

## OVOC QoE - System Load Alarm

Alarm Field	Description
Description	<p>This alarm is sent when the Voice Quality system capacity is high and the system consequently becomes overloaded. Three levels are supported:</p> <ul style="list-style-type: none"> <li>■ Major -&gt; Events are not stored. Trend Info will not be displayed.</li> <li>■ Critical -&gt; Green calls are not stored.</li> <li>■ Minor -&gt; Events are not stored for green calls. Trend Info will not be</li> </ul>

Alarm Field	Description
	displayed.
SNMP Alarm	acVoice QualityCallDroppedAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.34
Alarm Title	■ Voice Quality – System Load Alarm
Alarm Source	OVOC QoE
Alarm Type	Quality of service alarm
Probable Cause	AlarmProbableCauseType.THRESHOLDCROSSED
Severity	MINOR/ MAJOR/ CRITICAL
Additional Info	<ul style="list-style-type: none"> <li>■ Medium load level is reached - {0}%, {1} calls of {2}. /</li> <li>■ High load level is reached - {0}%, {1} calls of {2}. /</li> <li>■ Approaching maximal system capacity - {0}%, {1} calls of {2}.</li> </ul>
Corrective Action	Reduce the system load.

## Call Details Storage Level Change

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

Alarm Field	Description
Severity	Indeterminate
Additional Info	-
Corrective Action	-

## Call Quality Monitoring Connection Status Alarm

Alarm Field	Description		
Description	This alarm is sent when connectivity is lost between the managed device and Voice Quality Package server.		
SNMP Alarm	acSEMConnectionStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.36		
Alarm Title	Voice Quality – OVOC QoE - Connection Status Alarm		
Alarm Source	OVOC QoE/Device		
Alarm Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Additional Info	<p>One of the following reasons will appear:</p> <ul style="list-style-type: none"><li>■ Server Time: {0}, Device Time: {1}.</li><li>■ Please check your NTP Configuration in Device.</li><li>■ NTP Servers are not configured in the Device.</li><li>■ Please make sure that time in OVOC QoE Server and Device is properly synchronized.</li><li>■ NTP configuration is correct, please check your network conditions (Firewalls, Ports, etc .) and make sure that NTP sync of OVOC QoE Server and/or Devices is performed correctly.</li><li>■ You have complex network configuration in OVOC Mgmt/OVOC QoE server. Please refer to OVOC Mgmt client / Help menu / OVOC Mgmt Configuration frame to verify network configuration.</li></ul>		
Alarm	Condition	Text	CorrectiveAction

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

## OVOC QoE - Skype for Business SQL Server Connection Lost Alarm

Alarm Field	Description
Description	This alarm is sent when there is no connectivity with the Lync SQL Server database.
SNMP Alarm	acMSLyncConnectionAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.37
Alarm Title	Voice Quality AD Lync Connection Alarm
Alarm Source	OVOC QoE/Device
Alarm Type	Communications alarm

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

## OVOC QoE - Active Directory Server Connection Lost Alarm

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

## OVOC QoE - Media Bandwidth Alarm

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

Alarm Field	Description		
	or link falls below or exceeds the threshold values configured in the QoE Status and Alarms Details window.		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.43		
SNMP Alarm	acVoice QualityRuleBandwidthAlarm		
Alarm Title	Voice Quality Rule Bandwidth Alarm		
Alarm Source	VOC QoE/Device/Link/Site/Endpoint		
Alarm Type	Quality of service alarm		
Probable Cause	Threshold crossed		
Additional Info	<ul style="list-style-type: none"> <li>■ Critical Threshold: 10 Kb/ sec (default).</li> <li>■ Major Threshold: 5 Kb/ sec (default)</li> </ul> <p>Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to “Monitoring Frequency Min” For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (for 12:30-15:30) and so on.</p>		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the maximum bandwidth for the sampled period (see above) reaches the configured critical threshold value.	Maximum Bandwidth of X Kb/sec	Check the node's or link's maximum bandwidth capacity matches the required capacity.
Major	This alarm is raised when the maximum bandwidth for the sampled period (see above) reaches the configured major threshold value.	Maximum Bandwidth of X Kb/sec	

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

## OVOC QoE - Rule Max Concurrent Calls Alarm

Alarm Field	Description		
Description	This alarm is sent when the maximum concurrent calls for the node or link falls below or exceeds the threshold values configured in QoE Status and Alarms Details window.		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.44		
SNMP Alarm	acVoice QualityRuleMaxConcurrentCallsAlarm		
Alarm Title	Rule Max Concurrent Calls Alarm		
Alarm Source	OVOC QoE/Node/Link/Site/Endpoint		
Alarm Type	Quality of service alarm		
Probable Cause	Threshold crossed		
Additional Info	<ul style="list-style-type: none"> <li>■ Critical Threshold: 10 Calls (default).</li> <li>■ Major Threshold: 5 Calls (default)</li> </ul> <p>Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to "Monitoring Frequency Min". For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (from 12:30 to 15:30) and so on.</p>		
Alarm Severity	Condition	Text	Corrective Action
Critical	This alarm is raised when the number of	Max Concurrent Calls of	Check that the node's or link's

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

## Report Schedulers Time Event

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

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

## Report Schedulers Load Alarm

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

## Report Schedulers Execution Event

Alarm Field	Description		
Description	This event is raised when the execution of the report that is attached to the Scheduler fails.		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.84		
SNMP Alarm	acReportSchedulersExecutionEvent		
Alarm Title	Report Schedulers Execution Event		
Alarm Source	OVOC QoE/Report Scheduler		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Critical	Execution of report which is attached to the scheduler fails.	<b>Example:</b> SchedulerExecuter: Calculation of report result has been failed ; schedulerName=Test_Topology_Trend ; reportName=TestTrend_Report ; executionTime=Wed Dec 11 06:46:00 GMT 2019 ; actualRunTime=Wed Dec 11 06:46:00 GMT 2019	-

## 5 Device Manager Alarms

This section describes the Device Manager alarms.

### Registration Failure Alarm

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

### IP Phone Survivable Mode Start Alarm

Alarm Fields	Description
Description	This alarm is raised when the IP Phone enters Survivable mode state with limited services in the Microsoft Lync environment.
SNMP Alarm	IPPhoneSurvivableModeStart
OID	1.3.6.1.4.1.5003.9.20.3.2.0.40

Alarm Fields	Description
Alarm Title	Survivable Mode Start
Alarm Source	IP Phone
Alarm Type	Other(0)
Probable Cause	other (0)
Severity	Major
Corrective Action	The problem is typically not related to the phone, but to the server or network. Make sure all servers in the enterprise's network are up. If one is down, limited service will result.

## IP Phone Lync Login Failure Alarm

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

## Endpoint License Alarm

**Table 5-1: Endpoint License Alarm**

Alarm Field	Description		
Description	<p>This alarm is issued for the following scenarios:</p> <ul style="list-style-type: none"> <li>■ When the number of endpoints currently running on the Voice Quality server (shown as 'IP Phones Number' under 'Voice Quality' in the OVOC Server Manager License screen) approaches or reaches its license capacity.</li> <li>■ When the number of managed endpoints currently running on the OVOC server (shown in the License screen License screen) approaches or reaches its license capacity.</li> </ul>		
SNMP Alarm	acEndpointLicenseAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.48		
Alarm Title	Endpoint License Alarm		
Alarm Source	Voice Quality/Management		
Alarm Type	Other		
Probable Cause	Key Expired		
Additional Info	Endpoint License capacity {0} devices.		
Corrective Action	Contact your AudioCodes partner ASAP		
Alarm Severity	Condition	Text	Corrective Action
Critical	Currently connected devices are equivalent to 100% of Endpoints License capacity.	Currently running devices reached 100% of Endpoints License capacity.	-
Major	Currently connected devices are equivalent to reached 80% of Endpoints License capacity.	Currently running devices reached 80% of Endpoints License capacity.	-
Clear	Clearing currently active	Clear - Clearing	-

Alarm Field	Description		
	alarm	currently active alarm.	

## Endpoint Server Overloaded Alarm

Alarm Field	Description
Description	This alarm is issued when the Voice Quality Endpoint server process is overloaded with RFC 6035 Publish messages. This causes new RFC 6035 SIP PUBLISH messages ( ) to be dropped from the queue for this process.
SNMP Alarm	acEndpointServerOverloadAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.49
Alarm Title	Endpoint Server Overloaded Alarm
Alarm Text	Voice Quality Endpoint Server Overloaded! New Publish Messages Dropped
Alarm Source	Voice Quality
Alarm Type	Other
Probable Cause	Queue Size exceeded
Severity	Critical
Corrective Action	Reduce the endpoint traffic load on the OVOC server.

## IP Phone Speaker Firmware Download Failure

Alarm Field	Details
Description	This alarm is raised when the phone fails to download the HRS speaker firmware from the server (see Alarm Source).
SNMP Alarm	IPPhoneSpeakerFirmDownloadFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.54
Alarm Title	IP Phone Speaker Firmware Download Failure

Alarm Field	Details
Alarm Source	The server from which the download was attempted: OVOC, WEB, HTTP, FTP
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Major, Clear
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Ensure that the HRS speaker is connected to the Device Manager.</li> <li>■ Ensure that the compatible firmware file is loaded to the Device Manager.</li> </ul>

## IP Phone Speaker Firmware Upgrade Failure

Alarm Field	Description
Description	This alarm is raised when the phone fails to load the firmware to the HRS speaker.
SNMP Alarm	IP PhoneSpeakerFirmUpgradeFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.55
Alarm Title	IP Phone Speaker Firmware Upgrade Failure
Alarm Source	The IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Major, Clear
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Verify the USB connection between the phone and the HRS speaker.</li> <li>■ Verify the firmware file is compatible with the HRS speaker.</li> </ul>

## IP Phone Conference Speaker Connection Failure

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

## IP Phone General Local Event

**Table 5-2: IPPhone General Local Event**

Alarm Field	Description
Description	This alarm provides information regarding the IP Phones internal operation.
SNMP Alarm	IPPhoneGeneralLocalEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.57
Alarm Title	IP Phone General Local Event
Alarm Source	The IP Phone
Alarm Type	Other(0)

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

## IP Phone Web Successive Login Failure

**Table 5-3: IP Phone Web Successive Login Failure**

Alarm Field	Description		
Description	This alarm is raised when there are five successive failed login attempts to an IP phone's Web interface.		
SNMP Alarm	IPPhoneWebSuccessiveLoginFailure		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.59		
Alarm Title	IP Phone Web Successive Login Failure		
Alarm Source	The IP Phone		
Alarm Type	SecurityServiceOrMechanismViolation(9)		
Probable Cause	UnauthorizedAccessAttempt(73)		
Additional Info	-		
Alarm Severity	Condition	Text	Corrective Action
Major	Issued on the fifth successive failed attempt to log in to the phone's Web interface	-	<ul style="list-style-type: none"> <li>After the alarm is cleared, try to login to the Web interface using the correct username and password.</li> </ul>

Alarm Field	Description		
			<ul style="list-style-type: none"> <li>If you forget the login credentials, inform the network administrator.</li> </ul>
Clear	There are no additional WEB login failed trials during a specific time period (60 seconds) after sending the alarm.	-	-

## IP Phone Requires Reset

Alarm Field	Description
Description	This alarm is send to advise the user to restart the phone, in the event where there is new Jabra HRS Speaker firmware available forupgrade and the HRS user choses not to upgrade firmware when prompted.
SNMP Alarm	IPPhoneRequiresReset
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.70
Alarm Title	IP Phone Requires Reset
Alarm Text	IPPhone requires reset
Alarm Source	The IP Phone
Alarm Type	EquipmentAlarm(4)
Probable Cause	ConfigurationOrCustomizationError(7)
Severity	Major(4)
Additional Info	HRS IP Phone enters to limited mode and speaker is not available. To solve it, the phone has to be restarted.
Corrective Action	<ul style="list-style-type: none"> <li>If the user chooses to upgrade, at the end of the process ,the phone is automatically restarted and the firmware is upgraded. If successful, the speaker becomes available.</li> <li>If the user chooses not to upgrade, the phone enters into limited</li> </ul>

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

## Jabra Firmware Upgrade Failed

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

## VIP Endpoint is Not Registered or Offline

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

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

## VIP Endpoint is Disconnected

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

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

## Remote Control Battery Drained

Alarm Field	Description		
Description	This alarms is raised when the battery life of the Remote-Control for the RXV80 android device is under 20%.		
SNMP Alarm	ippRemoteControlBatteryDrained		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.91		
Alarm Source	IPPhone/<mac address>		
Alarm Title	Remote control Battery drained		
Alarm Type	Equipment Alarm		
Probable Cause	Equipment Malfunction		
Alarm Severity	Condition	<text>	Corrective Action
Warning	The battery life of the remote control for the Android device is under 20 %.	This Alarm is activated upon Remote-Control battery drained under 20 %	Replace the batteries.
Clear	The battery is replaced.		

## Remote Control is not Connected

Alarm Field	Description
Description	This alarm is raised when the wireless connection between the RXV80 android device and its remote control is disconnected.

Alarm Field	Description		
SNMP Alarm	ippRemoteControlsNotConnected		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.92		
Alarm Source	IPPhone/<mac address>		
Alarm Title	Remote control is not connected		
Alarm Type	Equipment Alarm		
Probable Cause	Equipment Malfunction		
Alarm Severity	Condition	Alarm Text	Corrective Action
Warning	The wireless connection between the android device and its remote control is disconnected.	This alarm is activated upon Remote-Control was disconnected	Refer to the RXV80 manual and try to re-pair the remote controller.
Clear	The wireless connection is restored.		

## USB Port Shutdown due to over Current Exceeded

Alarm Field	Description
Description	This alarm is raised when the USB port on the android device shuts down for 30 seconds, due to a current surge.
SNMP Alarm	ippUSBPortShutdownDueToOverCurrentExceeded
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.93
Alarm Source	IPPhone/<mac address>
Alarm Title	USB port shutdown due to over current exceeded
Alarm Type	Physical Violation
Probable Cause	Input Device Error

Alarm Field	Description		
Additional Info1	Disconnect the USB device from the phone and press OK to re enable the USB port.		
Additional Info2	Make sure that the USB port is used for USB headset only.		
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	This alarm is activated when the USB port on the android device shuts down for 30 seconds, due to a current surge.	This alarm is activated upon USB shutdown for 30 seconds, due to over current exceeded.	See above
Clear	USB port connection is restored.		

## Peripheral Device is Missing

Alarm Field	Description
Description	<p>When the bundle device parameter is set on either the RXV80 Video Collaboration Bar or RXV100 Meeting Room solution main devices, and then the peripheral device is disconnected from one of these main devices, an alarm is raised.</p> <p>This alarm is relevant for the following bundled peripherals:</p> <ul style="list-style-type: none"> <li>■ RX50</li> <li>■ RXVCAM50L</li> <li>■ RXVCAM50M</li> <li>■ RXVCAM10</li> <li>■ RX10</li> <li>■ RX15</li> </ul>
SNMP Alarm	ippPeripheralDeviceIsMissing

Alarm Field	Description		
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.96		
Alarm Title	Peripheral Device is Missing		
Alarm Source	IPPhone/<missing_peripheral_devicename>/<primary_device_mac> For example: IPPhone/*HD Camera RXVCam50M*/<mac_address>		
Alarm Type	EquipmentAlarm		
Probable Cause	OtherProbCause		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Major	A bundled defined peripheral device is disconnected from the main device.	<missing device> device is missing, please plug it in.	Connect the missing device.
Clear	Device is reconnected.		

## IPP Server SSL Certificate Could Not Be Proven

Alarm Field	Description
Description	This alarm is raised for peer server security errors when the IP phone does not trust the SSL certificate when attempting to establish a TLS connection with an external server.
SNMP Alarm	ippServerSslCertificateCouldNotBeProven
SNMP OID	.1.3.6.1.4.1.5003.9.20.3.2.0.98
Alarm Title	ipp Server Ssl Certificate Could Not Be Proven
Alarm Source	IPPhone/<server>/<mac>
Alarm Type	CommunicationsAlarm

Alarm Field	Description		
Probable Cause	CommunicationsProtocolError		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Device does not trust the SSL certificate	<server> could not be proven. Its security certificate is not trusted by the device. certificate Information: Issued to: _____ Issued by: _____ Valid from _____ to _____	Verify the device certificate.
Cleared			

## 6 OVOC Managed Devices Alarms

This section describes the OVOC Managed Devices alarms.

### Support Matrix

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

Alarm Type	Supported Device Types
Common Alarms	All the alarms in Section Common Alarms are supported by all AudioCodes devices.
Specific Hardware Alarms	<ul style="list-style-type: none"> <li>■ Mediant 2600 E-SBC</li> <li>■ Mediant 4000 SBC</li> <li>■ Mediant 1000</li> <li>■ MP-1288</li> </ul>
<a href="#">Temperature Alarm</a> on page 141	<ul style="list-style-type: none"> <li>■ Mediant 1000</li> <li>■ Mediant 2600</li> <li>■ Mediant 4000</li> </ul>
<a href="#">Fan Tray Alarm</a> on page 142	<ul style="list-style-type: none"> <li>■ MP-1288</li> <li>■ Mediant 1000</li> <li>■ Mediant 2600</li> <li>■ Mediant 4000</li> </ul>
<a href="#">Power Supply Alarm</a> on page 143	<ul style="list-style-type: none"> <li>■ MP-1288</li> <li>■ Mediant 1000</li> <li>■ Mediant 2600</li> <li>■ Mediant 4000.</li> </ul>
HA System Alarms	<ul style="list-style-type: none"> <li>■ Mediant 500 E-SBC</li> <li>■ Mediant 800B GW &amp; E-SBC</li> <li>■ Mediant 3000/TP-6310</li> </ul>

Alarm Type	Supported Device Types
	<ul style="list-style-type: none"> <li>■ Mediant 3000/TP-8410</li> <li>■ Mediant 2600 E-SBC</li> <li>■ Mediant 4000 SBC</li> <li>■ Mediant 4000B SBC (3 x MPM)</li> <li>■ Mediant 9000 SBC</li> <li>■ Mediant VE SBC</li> <li>■ Mediant SE SBC</li> </ul>
<a href="#">HA System Fault Alarm</a> on page 144	As above
<a href="#">HA System Configuration Mismatch Alarm</a> on page 150	As above
<a href="#">HA System Switch Over Alarm</a> on page 151	As above
<a href="#">Hitless Software Upgrade Alarm</a> on page 152	<ul style="list-style-type: none"> <li>■ Mediant 2600 E-SBC</li> <li>■ Mediant 4000 SBC</li> <li>■ Mediant SE SBC</li> <li>■ Mediant VE SBC</li> </ul>
<a href="#">Redundant Board Alarm</a> on page 153	As above
<a href="#">HA Network Watchdog Status Alarm</a> on page 154	As above
<a href="#">HA Network Watchdog Status Alarm</a> on page 154	As above (except Mediant 3000)
<a href="#">Cluster HA Alarm</a> on page 168	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 SBC and Mediant VE SBC)</li> </ul>

Alarm Type	Supported Device Types
<a href="#">HA Network Mismatch Alarm</a> on page 156	<ul style="list-style-type: none"> <li>■ Mediant VE SBC on AWS</li> <li>■ Mediant SE SBC on AWS</li> </ul>
<a href="#">HA Network Monitor Alarm</a> on page 156	As above
<a href="#">HA Ethernet Group Alarm</a> on page 157	As above (except Mediant 3000)
License Pool Alarms	Supported by all devices from Version 7.0, except for the Mediant 2000 and Mediant 3000. In addition, the Transcoding session license is applicable only to the Mediant Virtual Edition and Mediant 9000.
<a href="#">License Pool Infra Alarm</a> on page 158	As above
<a href="#">License Pool Application Alarm</a> on page 160	As above
<a href="#">License Pool Over Allocation Alarm</a> on page 161	As above
Floating License Alarms	Refer to the OVOC Release Notes for device support information.
<a href="#">Cloud License Manager Alarm</a> on page 163	Supported for the Floating License "Cloud" mode.
<a href="#">Floating License Alarm - Not Enough Memory to Allocate 'Custom' Profile</a> on page 162	Supported for the Floating License "Cloud" mode.
<a href="#">Flex License Manager Alarm</a> on page 165	Supported for the Floating License "FlexPool" mode.
Mediant 2600 E-SBC and Mediant 4000 Alarms SBC  <a href="#">DSP Farms Mismatch</a>	<ul style="list-style-type: none"> <li>■ Mediant 2600 E-SBC</li> </ul>


Alarm Type	Supported Device Types
<a href="#">Alarm</a> on page 166	<ul style="list-style-type: none"> <li>■ Mediant 4000 SBC</li> </ul>
Mediant 9000 and Software SBC Alarms	<ul style="list-style-type: none"> <li>■ Mediant 9000 SBC</li> <li>■ Mediant VE SBC</li> <li>■ Mediant SE SBC</li> <li>■ Mediant CE SBC</li> </ul>
<a href="#">Media Transcoder Network Failure</a> on page 169	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant VE SBC and Mediant 9000 SBC)</li> <li>■ Elastic Media Cluster feature (Mediant CE SBC)</li> </ul>
<a href="#">Media Transcoder Software Upgrade Failure</a> on page 169	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)</li> <li>■ Elastic Media Cluster feature (Mediant CE SBC)</li> </ul>
<a href="#">Media Transcoder High Temperature Failure</a> on page 170	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)</li> </ul>
<a href="#">Media Transcoder Fan Tray Module Failure</a> on page 171	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)</li> </ul>
<a href="#">Media Transcoder Power Supply Module Failure</a> on page 172	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)</li> </ul>
<a href="#">Cluster Bandwidth Utilization Alarm</a> on page 173	<ul style="list-style-type: none"> <li>■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)</li> <li>■ Elastic Media Cluster feature (Mediant CE SBC)</li> </ul>
<a href="#">Media Cluster Alarm</a> on page 174	<ul style="list-style-type: none"> <li>■ Elastic Media Cluster feature (Mediant CE SBC)</li> </ul>
<a href="#">Remote Interface Alarm</a> on page 176	<ul style="list-style-type: none"> <li>■ Elastic Media Cluster feature (Mediant CE SBC)</li> </ul>
<a href="#">AWS Security Role Alarm</a> on page 177	<ul style="list-style-type: none"> <li>■ Mediant VE SBC and Mediant CE SBC</li> </ul>
<a href="#">CDR Server Alarm</a> on page 178	<ul style="list-style-type: none"> <li>■ As above</li> </ul>

Alarm Type	Supported Device Types
<a href="#">Metering Alarm</a> on page 178	■ Mediant VE when deployed through the AWS Marketplace
<a href="#">MC Not Secured Alarm</a> on page 179	■ Mediant CE SBC
<a href="#">TLS Certificate Mismatch Alarm</a> on page 181	■ Mediant CE SBC
MP-1288 Alarms	■ MP-1288 (not supported by the OVOC License Pool Manager)
<a href="#">Module Service Alarm</a> on page 190	As above
<a href="#">Module Operation Alarm</a> on page 191	As above
<a href="#">Port Service Alarm</a> on page 192	As above
MSBR Alarms	Mediant 1000B MSBR, Mediant 800 MSBR Mediant MSBR 500L and Mediant 500 MSBR (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform <sup>1)</sup> ) Mediant 500Li MSBR
<a href="#">WAN Link Alarm</a> on page 193	As above
<a href="#">Power Over Ethernet Status [Event]</a> on page 194	Mediant 800 MSBR
<a href="#">Wireless Cellular Modem Alarm</a> on page 195	<ul style="list-style-type: none"> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 500L MSBR</li> <li>■ Mediant 800 MSBR</li> </ul>
<a href="#">Wireless Cellular Modem Status Changed</a> on page 195	<ul style="list-style-type: none"> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 500L MSBR</li> <li>■ Mediant 800 MSBR</li> </ul>

---

<sup>1</sup>Refer to SBC-Gateway-MSBR Series Release Notes for details.

Alarm Type	Supported Device Types
<a href="#">Data Interface Status</a> on page 196	As above
<a href="#">NQM Connectivity Alarm</a> on page 197	Mediant 800 MSBR
<a href="#">NQM RTT Alarm</a> on page 197	Mediant 800 MSBR
<a href="#">NQM Jitter Alarm</a> on page 198	Mediant 800 MSBR
<a href="#">NQM Packet Loss Alarm</a> on page 199	Mediant 800 MSBR
<a href="#">NQM MOS CQ Alarm</a> on page 200	Mediant 800 MSBR
<a href="#">NQM MOS LQ Alarm</a> on page 201	Mediant 800 MSBR
Mediant 3000 Hardware Alarms	<ul style="list-style-type: none"> <li>■ Mediant 3000/TP-6310</li> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">PEM Module Alarm</a> on page 202	As above
<a href="#">SA Module Missing Alarm</a> on page 203	As above
<a href="#">User Input Alarm</a> on page 204	As above
<a href="#">TM Inconsistency</a> on page 204	As above
<a href="#">TM Reference Status</a> on page 205	This alarm applies only to the Mediant 3000 using the BITs Synchronization Timing mode.
<a href="#">TM Reference Change</a> on page 206	As above
PSTN Trunk Alarms	<ul style="list-style-type: none"> <li>■ Mediant 500 Gateway &amp; E-SBC</li> </ul>

Alarm Type	Supported Device Types
	<ul style="list-style-type: none"> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 1000B Gateway &amp; E-SBC</li> <li>■ Mediant 3000</li> </ul> <p> For version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform<sup>1</sup>)</p>
<a href="#">D-Channel Status</a> on page 206	As above
<a href="#">SONET Section LOS Alarm</a> on page 208	■ Mediant 3000/TP-6310
<a href="#">SONET Line AIS Alarm</a> on page 209	■ Mediant 3000/TP-6310
<a href="#">SONET Line RDI Alarm</a> on page 210	■ Mediant 3000/TP-6310
<a href="#">SONET/SDN IF Failure Alarm</a> on page 210	■ Mediant 3000/TP-6310
<a href="#">Trunk LOS Alarm</a> on page 211	<ul style="list-style-type: none"> <li>■ Mediant 500 E-SBC</li> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 850 MSBR</li> <li>■ Mediant 1000B MSBR</li> <li>■ Mediant 1000B GW &amp; E-SBC</li> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">Trunk LOF Alarm</a> on page 212	■ Mediant 500 E-SBC

<sup>1</sup>Refer to SBC-Gateway-MSBR Series Release Notes for details.

Alarm Type	Supported Device Types
	<ul style="list-style-type: none"> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 850 MSBR</li> <li>■ Mediant 1000B MSBR</li> <li>■ Mediant 1000B GW &amp; E-SBC</li> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">Trunk AIS Alarm</a> on page 213	<ul style="list-style-type: none"> <li>■ Mediant 500 E-SBC</li> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 850 MSBR</li> <li>■ Mediant 1000B MSBR</li> <li>■ Mediant 1000B GW &amp; E-SBC</li> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">Trunk RAI Alarm</a> on page 213	<ul style="list-style-type: none"> <li>■ Mediant 500 E-SBC</li> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 850 MSBR</li> <li>■ Mediant 1000B MSBR</li> <li>■ Mediant 1000B GW &amp; E-SBC</li> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">V5.2 Interface Alarm</a> on page 214	<ul style="list-style-type: none"> <li>■ Mediant 3000/TP-8410</li> </ul>
<a href="#">SONET Path STS LOP Alarm</a> on page 215	<ul style="list-style-type: none"> <li>■ Mediant 3000/TP-6310</li> </ul>
<a href="#">SONET Path STS AIS Alarm</a> on page 216	<ul style="list-style-type: none"> <li>■ Mediant 3000/TP-6310</li> </ul>

Alarm Type	Supported Device Types
<a href="#">SONET Path STS RDI Alarm</a> on page 216	■ Mediant 3000/TP-6310
<a href="#">SONET Path Unequipped Alarm</a> on page 217	■ Mediant 3000/TP-6310
<a href="#">SONET Path Signal Label Alarm</a> on page 218	■ Mediant 3000/TP-6310
<a href="#">SONET Path Signal Label Alarm</a> on page 218	■ Mediant 3000/TP-6310
<a href="#">DS1 Line Status Alarm</a> on page 218	As above
<a href="#">DS3 AIS Alarm</a> on page 220	■ Mediant 3000/TP-6310
<a href="#">DS3 LOF Alarm</a> on page 221	■ Mediant 3000/TP-6310
<a href="#">DS3 LOS Alarm</a> on page 221	■ Mediant 3000/TP-6310
<a href="#">NFAS Group Alarm</a> on page 222	As above
<a href="#">B Channel Alarm</a> on page 223	As above
Analog Port Alarms	<ul style="list-style-type: none"> <li>■ Mediant 500 E-SBC</li> <li>■ Mediant 500L E-SBC</li> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 500L MSBR</li> <li>■ Mediant 500L GW &amp; E-SBC</li> <li>■ Mediant 800B Gateway &amp; E-SBC</li> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 850 MSBR</li> </ul>

Alarm Type	Supported Device Types
	<ul style="list-style-type: none"> <li>■ Mediant 1000B MSBR</li> <li>■ Mediant 1000B GW &amp; E-SBC</li> <li>■ (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform<sup>1</sup>)</li> </ul>
<a href="#">Analog Port SPI Out of Service</a> on page 224	As above
<a href="#">Analog Port High Temperature</a> on page 224	As above
<a href="#">Analog Port Ground Fault Out-of-Service Alarm</a> on page 225	As above
<a href="#">Dial Plan File Replaced Trap</a> on page 225	As above
<a href="#">Analog Line Left Off Hook Alarm</a> on page 226	As above

## Common Device Alarms

### Board Fatal Error

Alarm Field	Description
Description	This alarm is sent whenever a fatal device error occurs.
SNMP Alarm	acBoardFatalError
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Alarm Title	Board Fatal Error
Alarm Source	
Alarm Type	equipmentAlarm

<sup>1</sup>Refer to SBC-Gateway-MSBR Series Release Notes for details.

Alarm Field	Description		
Probable Cause	underlyingResourceUnavailable (56)		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Critical (default)	Any fatal error	Board Fatal Error: A run-time specific string describing the fatal error	<ul style="list-style-type: none"> <li>■ Capture the alarm information and the Syslog clause, if active.</li> <li>■ Contact AudioCodes' Support Center at <a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a> which will want to collect additional data from the device and perform a reset.</li> </ul>
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	Any fatal error	-	-

## Entity Configuration Change

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

Alarm Field	Description
Additional Info1,2,3	-
Corrective Action	-

## Configuration Error

Alarm Field	Description		
Description	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.		
SNMP Alarm	acBoardConfigurationError		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Alarm Title	[Event] Configuration Error		
AlarmType	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	Condition	Text	Corrective Action
Critical(default)	A configuration error was detected	Board Config Error: A run-time specific string describing the configuration error	<ul style="list-style-type: none"> <li>■ Check the run-time specific string to determine the nature of the configuration error.</li> <li>■ Fix the configuration error using the appropriate tool: Web interface, OVOC, or ini file.</li> <li>■ Save the configuration and if necessary reset the device.</li> </ul>
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After configuration error	-	

## Initialization Ended

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

## Board Resetting Following Software Reset

Alarm Fields	Description		
Description	This alarm indicates that the device has started the reset process - following a software reset.		
SNMP Alarm	acBoardEvResettingBoard		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5		
Alarm Title	Board Resetting Following Software Reset		
Alarm Source	-		
Alarm Type	equipmentAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	Condition	Text	Corrective Action
Critical	When the device is reset through the	"Device is resetting"	A network administrator has reset the device. Corrective action is not required. The alarm remains at Critical severity


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

## Feature Key Related Error

Table 6-1: Feature Key Related Error

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

## Gateway Administrative State Changed

Alarm Field	Description
Description	<p>This alarm indicates that the administrative state of the gateway has been changed to a new state.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  All state changes are instigated by the parameter acgwAdminState. </div> <ul style="list-style-type: none"> <li>■ Time limit set in the parameter acgwAdminStateLockControl - 'GateWay shutting down. Max time to LOCK %d sec'</li> <li>■ No time limit in the parameter acgwAdminStateLockControl - 'GateWay is shutting down. No time limit.'</li> </ul>

Alarm Field	Description		
	<ul style="list-style-type: none"> <li>■ When reaching lock state - 'GateWay is locked'</li> <li>■ When the gateway is SET to unlocked - 'GateWay is unlocked (fully active again)'</li> </ul>		
SNMP Alarm	acgwAdminStateChange		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7		
Alarm Title	Administrative State Change		
Alarm Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	Condition	Text	Corrective Action
Major (default)	Admin state changed to shutting down	Network element admin state change alarm: Gateway is shutting down. No time limit.	No corrective action is required. A network administrator took an action to gracefully lock the device.
Major	Admin state changed to locked	Locked	No corrective action is required. A network administrator took an action to lock the device, or a graceful lock timeout occurred.
Cleared	Admin state changed to unlocked	-	No corrective action is required. A network

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

## No Free Channels Available

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

## Gatekeeper/Proxy not Found or Registration Failed

Alarm Field	Description		
Description	<p>The alarm is sent in the following scenarios:</p> <ul style="list-style-type: none"> <li>■ 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.)</li> <li>■ Physical BRI or PRI (E1/T1) port is up or down (OOS).</li> <li>■ 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.</li> <li>■ Connection to the Proxy is up or down.</li> <li>■ Failure in TDM-over-IP call - transparent E1/T1 without signalling.</li> <li>■ Connection to the Proxy Set associated with the trunk/line is up/down.</li> <li>■ Failure in server registration for the trunk/line.</li> <li>■ Failure in a Serving IP Group for the trunk.</li> <li>■ Failure in a Proxy Set.</li> </ul>		
SNMP Alarm	acBoardControllerFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.9		
Alarm Source	'GWAPP'		
Alarm Title	Proxy not Found or Registration Failed		
Alarm Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	Condition	Text	Additional Information
Major (default)	FXO physical port is down	<p>"BusyOut Line n Link failure"</p> <p>Where n represents the FXO port number (0 for the first port).</p>	<ul style="list-style-type: none"> <li>■ Verify that the FXO line is securely cabled to the device's FXO port.</li> </ul>

Alarm Field	Description		
	BRI or PRI physical port is down	"BusyOut Trunk n Link failure" Where n represents the BRI or PRI port number (0 for the first port).	Verify that the digital trunk is securely cabled to the device's digital port.
	Proxy has not been found or registration failure	"Proxy not found. Use internal routing" -OR- "Proxy lost. Looking for another Proxy"	<ul style="list-style-type: none"> <li>■ Check the network layer</li> <li>■ Make sure that the proxy IP and port are configured correctly.</li> </ul>
	Connection to Proxy is down	"BusyOut Trunk/Line n Connectivity Proxy failure"	-
	Connection to the Proxy Set associated with the trunk or line is down	"BusyOut Trunk/Line n Proxy Set Failure" Where n represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Proxy Set	"Proxy Set ID n" Where n represents the Proxy Set ID.	-
	Failure in TDM-over-IP call	"BusyOut Trunk n TDM over IP failure (Active calls x	-

Alarm Field	Description		
		Min y)" Where n represents the BRI/ PRI trunk.	
	Failure in server registration for the trunk/line	"BusyOut Trunk/Line n Registration Failure" Where n represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Serving IP Group for the trunk	"BusyOut Trunk n Serving IP Group Failure" Where n represents the BRI or PRI trunk ID.	-
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	-

## Ethernet Link Down Alarm

Alarm Field	Description
Description	<p>This alarm indicates that the Ethernet link is down or remote Ethernet link is down and the board has no communication to any other host.</p> <ul style="list-style-type: none"> <li>■ No link at all.</li> <li>■ Link is up again.</li> <li>■ Primary link is down only - 'Primary Link is lost. Switching to Secondary Link'</li> </ul>
SNMP Alarm	acBoardEthernetLinkAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10

Alarm Field	Description		
Alarm Title	Ethernet Link Down Alarm		
Alarm Source	<p>All except Mediant 3000: Board#&lt;n&gt;/EthernetLink#0 (where n is the slot number)</p> <p>Mediant 3000: Chassis#0/Module#&lt;n&gt;/EthernetLink#0 (where n is the blade's slot number)</p> <p>This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).</p>		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	Condition	Text	Corrective Action
Major	Fault on single interface	Ethernet link alarm: Redundant link is down	<ul style="list-style-type: none"> <li>■ Ensure that both Ethernet cables are plugged into the back of the system.</li> <li>■ Observe the system's Ethernet link lights to determine which interface is failing.</li> <li>■ Reconnect the cable or fix the network problem</li> </ul>
Critical (default)	Fault on both interfaces	No Ethernet link	
Cleared	Both interfaces are operational	-	Note that the alarm behaves differently when coming from the redundant or the active modules of a High Availability (HA) system. The alarm from the redundant is raised when there is an operational HA configuration in the system. There is no critical severity for the redundant module losing both its Ethernet links as that is conveyed in the no HA alarm that follows such a case.

## System Component Overloaded

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

Alarm Field	Description		
	system's components.		
SNMP Alarm	acBoardOverloadAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Alarm Title	System Component Overloaded		
Alarm Source	'GWAPP'		
Alarm Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	Condition	Text	Corrective Action
Major (default)	An overload condition exists in one or more of the system components	"System CPU overload condition - IdleUtilization percentage=%d" Where %d is the percentage of available CPU resources remaining	<ul style="list-style-type: none"> <li>■ Make sure that the syslog level is 0 (or not high).</li> <li>■ Make sure that DebugRecording is not running.</li> <li>■ If the system is configured correctly, reduce traffic.</li> </ul>
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	-

## Active Alarms Table Overflow

**Table 6-2: Active Alarms Table Overflow**

Alarm Field	Description
Description	This alarm is raised when there are too many alarms to fit into the active alarm table. The status stays major until reboot as it denotes a possible loss of information until the next reboot. If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in

Alarm Field	Description
	the active alarm table.
SNMP Alarm	acActiveAlarmTableOverflow
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.12
Alarm Title	[Event] Active Alarm Table Overflow
Alarm Type	Processing Error Alarm
Alarm Source	MG
Probable Cause	resourceAtOrNearingCapacity (43)
Severity	Major
Additional Info1,2,3	-
Corrective Action	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

## Operation State Change [Node]

**Table 6-3: Operational State Change**

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

Severity			
Major (default)	Operational state changed to disabled	Node {elementName} was marked as {status}	<ul style="list-style-type: none"> <li>■ 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.</li> <li>■ Look for other alarms and Syslogs that might provide additional information about the error.</li> </ul>
Cleared	Operational state changed to available	-	<p>In case state is unavailable:</p> <ul style="list-style-type: none"> <li>■ Validate that Node is available in WEB interface / OVOC</li> <li>■ Check device network connectivity</li> <li>■ Check the device's network connectivity to the ARM Configurator</li> <li>■ Validate that proper Node credentials updated in ARM</li> </ul> <p>In case state is logged out:</p> <ul style="list-style-type: none"> <li>■ Check the ARM configuration in the device</li> </ul> <p>In case state is Unrouteable:</p> <ul style="list-style-type: none"> <li>■ Check the device network connectivity to the ARM routers</li> <li>■ Check router status and availability</li> </ul>

## Keep Alive Trap

Alarm Field	Description
Description	Part of the NAT traversal mechanism. If the STUN application in the device detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the

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

## NAT Traversal Alarm

Alarm Field	Description
Description	This alarm is sent when the NAT is placed in front of a device and is identified as a symmetric NAT. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.
SNMP Alarm	acNATTraversalAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.17
Alarm Title	NAT Traversal Alarm

Alarm Field	Description
Alarm Type	other (0)
Alarm Source	MG
Probable Cause	other (0)
Severity	Indeterminate
Additional Info1,2,3	-
Status Changes	<p>The STUN client in the device is enabled and has either identified a NAT or is not finding the STUN server.</p> <p>Keep-alive is sent out every 9/10 of the time defined in the 'NatBindingDefaultTimeout' parameter.</p>
Corrective Action	See <a href="http://tools.ietf.org/html/rfc5389">http://tools.ietf.org/html/rfc5389</a>

### Enhanced BIT Status Trap

Alarm Field	Description
Description	Sent for the status of the BIT (Built In Test). The information in the trap contains blade hardware elements being tested and their status. The information is presented in the Additional Info fields.
SNMP Alarm	acEnhancedBITStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Alarm Title	Enhanced BIT Status
Alarm Source	BIT
Alarm Type	Other
Severity	Indeterminate
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their status.

Alarm Field	Description
Corrective Action	-

### Threshold of Performance Monitored Object Exceeded

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

### HTTP Download Result

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

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Alarm Title	[Event] HTTP Download Result
Alarm Source	-
Alarm Type	processingErrorAlarm (3) for failures and other (0) for success
Probable Cause	Other
Severity	Indeterminate
Additional Info	There are other possible textual messages describing NFS failures or success, FTP failure or success.
Corrective Action	-

## IPv6

Alarm Field	Description
Description	This alarm indicates when an IPv6 address already exists or an IPv6 configuration failure has occurred. The description generated is "IP interface alarm. IPv6 Configuration failed, IPv6 will be disabled".
SNMP Alarm	acIPv6ErrorAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.53
Alarm Title	IPv6
Alarm Source	System#0/Interfaces#<n>.
Alarm Type	operationalViolation
Probable Cause	communicationsProtocolError
Additional Info	Status stays critical until reboot. A clear trap is not sent.
Corrective Action	<ul style="list-style-type: none"> <li>Find a new IPV6 address and reboot.</li> </ul>

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	Bad IPv6 address (already exists)	IP interface alarm: IPv6 configuration failed, IPv6 will be disabled.	<ul style="list-style-type: none"> <li>Find a new IPV6 address.</li> <li>Reboot the device.</li> </ul>
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After the alarm is raised.	-	-

## SAS Emergency Mode Alarm

Alarm Field	Description
Description	This alarm is sent by the Stand-Alone Survivability (SAS) application when switching from "Normal" mode to "Emergency" mode. This alarm is cleared once the SAS returns to "Normal" mode.
SNMP Alarm	acGWSASEmergencyModeAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.59
Alarm Title	GW SAS Emergency Mode Alarm
Alarm Source	-
Alarm Type	Other
Probable Cause	Other
Severity	-
Additional Info	-
Corrective Action	Check network communication with the Proxy

## Software Upgrade Alarm

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

## NTP Server Status Alarm

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

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

## LDAP Lost Connection

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

## SSH Connection Status [Event]

Alarm Field	Description
Description	This trap indicates the result of a recent SSH connection attempt.
SNMP Alarm	acSSHConnectionStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Alarm Title	[Event] SSH Connection Status
Alarm Source	-
Alarm Type	environmentalAlarm
Probable Cause	unauthorizedAccessAttempt/other
Severity	indeterminate
Additional Info	-
Corrective Action	-

## OCSP Server Status Alarm

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

Alarm Field	Description
	■ Correct the network configuration

## Media Process Overload Alarm

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

## Ethernet Group Alarm

Alarm Field	Description
Description	This alarm is raised when the in an Ethernet port-pair group (1+1) has no Ethernet port with its link up and is cleared when at least one port has established a link.
SNMP Alarm	acEthernetGroupAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86
Alarm Title	Ethernet Group alarm
Alarm Source	Board#%d/EthernetGroup#%d

Alarm Field	Description
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	major
Additional Info	-
Corrective Action	-

### Media Realm BW Threshold Alarm

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

## Certificate Expiry Notification

Alarm Field		Description	
Description		This alarm is sent before the expiration of the installed certificate and after it has expired.	
SNMP Alarm		acCertificateExpiryNotification	
SNMP OID		1.3.6.1.4.1.5003.9.10.1.21.2.0.92	
Alarm Title		Certificate Expiry Notification	
Alarm Source		tls#<num>	
Alarm Type		environmentalAlarm	
Probable Cause		The certificate key expired (keyExpired)	
Alarm Severity	Condition	Text	Corrective Action
Intermediate	The certificate key is about to expire.	<p>Either:</p> <ul style="list-style-type: none"> <li>■ The device certificate has expired %d days ago</li> <li>■ The device certificate will expire in %d days</li> <li>■ The device certificate will expire in less than 1 day</li> </ul> <p>%d – number of days            %d – TLS Context to which certificate belongs</p>	<p>Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically).</p> <p>To replace certificates, refer to the device's User's Manual.</p>

## Web User Access Disabled

Alarm Field	Description
Description	This alarm is sent when the Web user has been disabled due to inactivity.
SNMP Alarm	acWEBUserAccessDisabled
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Alarm Title	-
Alarm Source	-
Alarm Type	other
Probable Cause	The Web user was disabled due to inactivity (denialOfService).
Severity	indeterminate
Additional Info	-
Corrective Action	<p>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).</p> <p>The Web security administrator must:</p> <ul style="list-style-type: none"> <li>■ In the Web interface, access the Accounts page (Configuration &gt; System &gt; Management &gt; Web User Accounts).</li> <li>■ Identify in the list of users table that user whose access has been denied.</li> </ul> <p>Change the status of that user from Blocked to Valid or New.</p>

## Proxy Connection Lost

Alarm Field	Description
Description	This alarm is sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.
SNMP Alarm	acProxyConnectionLost
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94

Alarm Field	Description		
Alarm Title	Proxy Connection Lost		
Alarm Source	System#0		
Alarm Type	communicationsAlarm		
Probable Cause	<ul style="list-style-type: none"> <li>■ Network issue (connection fail due to network/routing failure).</li> <li>■ Proxy issue (proxy is down).</li> <li>■ AudioCodes device issue.</li> </ul>		
Alarm Severity	Condition	Text	Corrective Action
Major	When connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table.	Proxy Set %d: Proxy not found. Use internal routing	<ul style="list-style-type: none"> <li>■ Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.</li> <li>■ Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.</li> <li>■ 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.</li> <li>■ Check that routing using the device's (internal) routing table is functioning correctly.</li> <li>■ Contact AudioCodes support center (<a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a>) and send a syslog and network capture for this issue.</li> </ul>
Major	When Proxy Set includes	Proxy Set %d: Proxy lost.	<ul style="list-style-type: none"> <li>■ Ping the proxy server. If there is no ping, contact your</li> </ul>

Alarm Field	Description		
	more than one proxy IP with redundancy and connection to one of them is lost.	looking for another proxy	<p>proxy provider. The probable reason is the proxy is down.</p> <ul style="list-style-type: none"> <li>■ Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.</li> <li>■ 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.</li> <li>■ Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue.</li> <li>■ Contact AudioCodes support center (<a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a>) and send a syslog and network capture for this issue.</li> </ul>
Cleared	When connection to proxy is available again	Proxy found. ip:<IP address>:<port #> Proxy Set ID %d	

## IDS Policy Alarm

Alarm Field	Description
Description	The alarm is raised whenever a threshold is crossed in the IDS system. The alarm is associated with the MO pair IDSMATCH & IDSRULE.
SNMP Alarm	acIDSPolicyAlarm

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Alarm Title	IDS Policy Alarm
Default Severity	-
Alarm Type	Other
Probable Cause	-
Alarm Text	Policy NUM (NAME) minor/major/critical threshold (NUM) of REASON cross in global/ip/ip+port scope (triggered by IP)
Status Changes	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm.</li> <li>■ Locate the remote hosts (IP addresses) that are specified in the traps.</li> <li>■ Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation.</li> <li>■ If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table.</li> </ul>


## IDS Threshold Cross Notification

Alarm Field	Description
Description	This notification is sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
SNMP Alarm	acIDSThresholdCrossNotification
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Default Severity	-
AlarmType	Other
Probable Cause	-

Alarm Field	Description
Alarm Text	Threshold cross for scope value IP. Severity=minor/major/critical. Current value=NUM
Status Changes	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Identify the remote host (IP address / port) on the network which the Intrusion Detection System (IDS) has indicated is malicious</li> <li>■ Note that the IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks(counter).</li> <li>■ Block the malicious activity</li> </ul>

## IDS Blacklist Notification

Alarm Field	Description
Description	This alarm notifies when an IP address has been added or removed from a blacklist.
SNMP Alarm	acIDSBlacklistNotification
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Default Severity	-
Alarm Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	Added IP * to blacklist Removed IP * from blacklist
Status Changes	-
Corrective Action	Identify the malicious remote host (IP address / port) that the Intrusion Detection System (IDS) has automatically blacklisted or removed from the blacklist.

Alarm Field	Description
	 <p>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.</p>

## Proxy Connectivity

Alarm Field	Description		
Description	Sent when a connection to a specific proxy in a specific Proxy Set is down. The trap is cleared when the proxy connections is up.		
SNMP Alarm	acProxyConnectivity		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.102		
Alarm Source	System#0		
Alarm Type	communicationsAlarm		
Probable Cause	<ul style="list-style-type: none"> <li>■ Network issue (connection fail due to network/routing failure).</li> <li>■ Proxy issue (proxy is down).</li> <li>■ AudioCodes device issue.</li> </ul>		
Alarm Severity	Condition	Text	Corrective Action
Indeterminate	When connection to the proxy server is lost.	Proxy server <IP address>:<port> is now OUT OF SERVICE	<ul style="list-style-type: none"> <li>■ Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.</li> <li>■ Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.</li> <li>■ If you have more than one device connected to this same proxy, check if there are more AudioCodes</li> </ul>

Alarm Field	Description		
			<p>devices with the same trap event. If this is the case, this could confirm that this is not AudioCodes device issue.</p> <ul style="list-style-type: none"> <li>■ Contact AudioCodes support center (<a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a>) and send a syslog and network capture for this issue.</li> </ul>
Cleared	When connection to the proxy is available again	Proxy server <IP address>:<port> is now IN SERVICE	

## Web User Activity Log Trap

Alarm Field	Description
Description	Sent upon log (Syslog) generated by device indicating a Web user action (configured by ActivityListToLog). The SNMP trap notification functionality is enabled by the EnableActivityTrap parameter (refer to the User's Manual).
SNMP Alarm	acActivityLog
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.105
Alarm Title	Web User Activity Log Trap
Alarm Type	other (0)
Probable Cause	other (0)
Default Severity	Indeterminate
Trap Text	<p>[description of activity].User:&lt;username&gt;. Session: &lt;session type&gt;[IP address of client (user)].</p> <p>For example:</p> <p>“Auxiliary file loading was changed from ‘0’ to ‘1’, User:Admin. Session:</p>

Alarm Field	Description
	WEB [172.17.125.12]
Note	Activity log event is applicable to the following OAMP interfaces: SNMP, Web, CLI and REST. For SNMP activity, the username refers to the SNMP community string.

## HTTP Proxy Service Alarm

Alarm Fields	Description		
Description	Sent when an HTTP host specified in the Upstream Groups table is down. The trap is cleared when the host is back up.		
SNMP Alarm	acHTTPProxyServiceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.108		
Alarm Title	HTTP Proxy Service Alarm		
Alarm Source	System#0/HTTPProxyService#<num> System#0/EMSService#<num>		
Alarm Type	communicationsAlarm		
Probable Cause	<ul style="list-style-type: none"> <li>■ Network issue (connection fail due to network/routing failure)</li> <li>■ Host issue (host is down)</li> <li>■ Device issue</li> </ul>		
Severity	Condition	Text	Corrective Action
Major	When connection to the Upstream Host is lost.	"HTTP Proxy Upstream Host IP:Port (Host #n in Upstream Group	<ol style="list-style-type: none"> <li>1. Ping the host. If there is no ping, contact your provider. The probable reason is that the host is down.</li> <li>2. Ping between the host and the device. If there is no ping, the problem could be a net-</li> </ol>

Alarm Fields	Description		
		name) is OFFLINE"	<p>work/router issue.</p> <ol style="list-style-type: none"> <li>3. Check that routing using the device's (internal) routing table is functioning correctly.</li> <li>4. Contact AudioCodes support center (support@AudioCodes.com) and send a syslog and network capture for this issue.</li> </ol>
Clear	When connection to service is available again.	-	-

### Answer-Seizure Ratio Threshold Alarm

Alarm Field	Description		
Description	The Answer-Seizure Ratio (ASR) measures the percentage of answered calls relative to the total number of attempted calls (seizures). The alarm is raised when the configured ASR minor and major thresholds are crossed (configured in the Performance Profile table).		
SNMP Alarm	acASRThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.111		
Alarm Title	ASR Threshold Crossed		
Alarm Source	<p>The object for which the threshold is crossed can be any of the following:</p> <ul style="list-style-type: none"> <li>■ PM_gwSBCASR</li> <li>■ PM_gwSBCIPGroupASR</li> <li>■ PM_gwSBCSRDASR</li> </ul>		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	ThresholdCrossed		
Severity	Condition	<text>	Corrective Action
Major	ASR is equal or less	"ASR threshold	

Alarm Field	Description		
	than the configured Major threshold.	crossed."	
Minor	ASR is equal or less than the configured Minor threshold (but greater than the Major threshold).	"ASR threshold crossed."	
Cleared	ASR is above the configured Minor threshold plus the hysteresis.	-	

### Average Call Duration Threshold Alarm

Alarm Field	Description
Description	The Average Call Duration (ACD) plus the SDD (Session Disconnect time) measures the average call duration from the time from when the sip Bye is sent to the time when the 200 OK is received. The alarm is raised when the configured ACD minor and major thresholds are crossed (configured in the Performance Profile table).
SNMP Alarm	acACDThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.112
Alarm Title	ACD Threshold Crossed
Alarm Source	<p>The object for which the threshold is crossed can be any one of the following:</p> <ul style="list-style-type: none"> <li>■ PM_gwSBCACD</li> <li>■ PM_gwSBCIPGroupACD</li> <li>■ PM_gwSBCSRDACD</li> </ul>
Alarm Type	Quality Of Service Alarm
Probable Cause	The threshold has been crossed.
Additional Info	-

Alarm Field	Description		
Alarm Severity	Condition	Text	CorrectiveAction
Major	ACD is equal or less than the configured Major threshold.	"ACD threshold crossed."	-
Minor	ACD is equal or less than the configured Minor threshold (but greater than the Major threshold).	-	-
Cleared	ACD is above the configured Minor threshold plus the hysteresis.		

### Network Effectiveness Ratio Threshold Alarm

Alarm Field	Description
Description	The NER (Network Effectiveness Ratio) measures the percentage of successfully connected calls relative to the total number of seizures. The alarm is raised when the configured NER minor and major thresholds are crossed (configured in the Performance Profile table).
SNMP Alarm	acNERThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.113
Alarm Title	NER Threshold Crossed
Alarm Source	The object for which the threshold is crossed, which can be one of the following: <ul style="list-style-type: none"> <li>■ PM_gwSBCNER</li> <li>■ PM_gwSBCIPGroupNER</li> <li>■ PM_gwSBCSRDNER</li> </ul>
Alarm Text	-
Alarm Type	Quality Of Service Alarm

Alarm Field	Description		
Probable Cause	The threshold has been crossed.		
Severity	Condition	Text	Corrective Action
Major	NER is equal or less than the configured Major threshold.	"NER threshold crossed."	-
Minor	NER is equal or less than the configured Minor threshold (but greater than the Major threshold).	-	-
Cleared	NER is above the configured Minor threshold plus the hysteresis.	-	-

### IP Group No Route Alarm

Alarm Fields	Description
Description	<p>The alarm is raised when the device rejects calls to an IP Group due to the following reasons:</p> <ul style="list-style-type: none"> <li>■ IP Group keep-alive failure (Gateway and SBC)</li> <li>■ Poor Voice Quality - MOS (SBC only)</li> <li>■ Bandwidth threshold has been crossed (SBC only)</li> <li>■ ASR threshold has been crossed (SBC only)</li> <li>■ ACD threshold has been crossed (SBC only)</li> <li>■ NER threshold has been crossed (SBC only)</li> </ul>
SNMP Alarm	acIpGroupNoRouteAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.114
Alarm Title	IP Group Blocked
Alarm Source	The object for which the threshold is crossed according to one of the above mentioned reasons:

Alarm Fields	Description		
	<ul style="list-style-type: none"> <li>■ IP Group keep alive failure (acProxyConnectivity trap is raised)</li> <li>■ Poor Quality of Experience</li> <li>■ Bandwidth</li> <li>■ ASR (see acASRThresholdAlarm)</li> <li>■ ACD (see acACDThresholdAlarm)</li> <li>■ NER (see acNERThresholdAlarm)</li> </ul>		
Alarm Type	Quality Of Service Alarm		
Probable Cause	One of the reasons described above.		
Severity	Condition	Text	Corrective Action
Major	When calls rejected to IP Group due to any of the above-mentioned reasons.	"IP Group is temporarily blocked."	-
Cleared	When calls are no longer rejected due to the above mentioned reasons (i.e. when none of the above reasons prevent a route to the IP Group from being established).	-	-

## TLS Certificate Expiry Alarm

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

Alarm Field	Description		
Alarm Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Alarm Severity	Condition	Text	Corrective Action
Minor	The certificate is about to expire. This is sent a user-defined number of days (TLSExpiryCheckStart) before the expiration date.	"The certificate of TLS context %d will expire in %d days"	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically).
Major	The certificate is about to expire. This is sent a week as well as a day before the expiration date.	"The certificate of TLS context %d will expire in less than a week" Or "The TLS certificate of TLS context %d will expire in a day" Or "The TLS certificate of TLS context %d will expire in less than a day"	To replace certificates, refer to the User's Manual.
Critical	The certificate has expired.	"The certificate of TLS context %d has expired %d days ago"	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically). To replace certificates,

Alarm Field	Description		
			refer to the User's Manual.
Cleared	A new certificate is installed.	-	-

## NGINX Configuration is not Valid

Alarm Field	Description		
Description	This alarm is raised when NGINX Directives Sets have been configured with invalid syntax. NGINX continues to run with the previous, valid configuration unless the SBC is restarted, in which case, the NGINX process is stopped and the NGINX Process is not Running alarm is raised (see below).		
SNMP Alarm	acNGINXConfigurationIsInvalidAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.130		
Alarm Title	NGINX configuration is not valid		
Alarm Source	operationalViolation		
Alarm Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	Condition	Text	Corrective Action
Minor		NGINX Configuration file is not valid.	<p>Identify and resolve NGINX Directives Sets syntax errors to ensure an uninterrupted HTTP Proxy service. You can run the CLI commands for troubleshooting:</p> <ul style="list-style-type: none"> <li>■ “show network http-proxy conf new” to display the Directives Set configuration that generated the errors.</li> <li>■ “show network http-proxy conf errors” to display the errors</li> </ul>

Alarm Field		Description
		resulting from the invalid Directives Set configuration.

### NGINX Process is not Running

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

### Remote Monitoring Alarm

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

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

## SDR Server Alarm

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

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

## KPI Threshold Crossing

Alarm Field	Description		
Description	The alarm is sent every time the threshold of a performance monitoring parameter (object) is crossed. The thresholds to raise or clear an alarm, the severity levels, and the alarm messages are configured in the Alarm Thresholds table (Setup menu > Administration tab > Performance Monitoring folder).		
SNMP Alarm	acKpiThresholdCrossing		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.148		
Alarm Title	KPI Threshold Crossing		
Alarm Source	The object for which the threshold is crossed.		
Alarm Type	processingErrorAlarm		
Probable Cause	thresholdCrossed		
Alarm Severity	Condition	Text	Corrective Action
Raised alarm (severity depends on configuration)	Threshold crossed to raise alarm	<kpi_name> value <value> is too <high low> (Note: Text is configurable.)	Verify the configuration of the related Performance Monitoring object and adjust loads accordingly.
Cleared alarm (severity depends on configuration)	Threshold crossed to clear alarm	"<kpi_name> value <value> is back to normal" (Note: Text is configurable.)	

## Clock Configuration Alarm

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

## Debug Recording Activation Alarm

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

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

## Faulty DSP Alarm

This alarm is relevant for all DSP-based devices.

Alarm Field	Description		
Description	This alarm is raised when one or more DSP cores on the device is faulty.		
SNMP Alarm	acFaultyDSPAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.152		
Alarm Title	Faulty DSP alarm		
Alarm Source	equipmentAlarm		
Alarm Type	alarmTrap		
Probable Cause	unexpectedInformation		
Alarm Severity	Condition	Text	Corrective Action
Major	Failure has been detected on one or more of the device DSP cores during bootup.	At least one faulty DSP detected during boot	Perform diagnostics on the DSP cores.
Major	Failure has been detected on one or more of the device DSP cores.	At least one faulty DSP detected	Perform diagnostics on the DSP cores.
Clear	Repair or replace the faulty DSP core(s) and restart the device.		

## No Reply From DNS Server Alarm

Alarm Field	Description		
Description	<p>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.</p>		
SNMP Alarm	acNoReplyFromDNSServerAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.155		
Alarm Title	No Reply From DNS Server Alarm		
Alarm Source	Board#1/ipInterface#<IP Interface Index>		
Alarm Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm 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.

Alarm Field	Description		
Cleared	Response received from DNS server.		

## Weak Password Alarm

Alarm Field	Description		
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.)		
SNMP Alarm			
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.156		
Alarm Title			
Alarm Source	WebUsers#X (where X is the row index of the user in the Local Users table)		
Alarm Type	securityServiceOrMechanismViolation		
Probable Cause	Weak Password		
Additional Info1			
Additional Info2			
Alarm Severity	Condition	Alarm Text	Corrective Action
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		

Alarm Field	Description		
	been deleted in the Local Users table).		

## Specific Hardware Alarms

This section describes specific hardware alarms.

### Temperature Alarm

Alarm Field	Description		
Description	Sent when the device exceeds its temperature limits.		
SNMP Alarm	acBoardTemperatureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3		
Alarm Title	Temperature Alarm		
Alarm Source	System#0		
Alarm Type	equipmentAlarm		
Probable Cause	The air filter is saturated. One of the fans work slower than expected. temperatureUnacceptable (50)		
Alarm Severity	Condition	Text	Corrective Action
Critical	Internal temperature is too high for normal operation	Board temperature too high	Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels.  Check the chassis ventilation outlet and make sure that they are not obstructed for air flow.

Alarm Field	Description		
			Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Temperature returns to normal operating values	-	-

## Fan Tray Alarm

Alarm Field	Description		
Description	This alarm is activated in one of the following cases: <ul style="list-style-type: none"> <li>■ Fan-Tray is missing</li> <li>■ One or more fans in the fan-tray is faulty.</li> <li>■ Fan tray is in place and fans are functioning.</li> </ul>		
SNMP Alarm	acFanTrayAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29		
Alarm Title	Fan Tray Alarm		
Alarm Source	Chassis#0/FanTray#0		
Alarm Type	equipmentAlarm		
Probable Cause	<ul style="list-style-type: none"> <li>■ One or more fans on the Fan Tray module stopped working.</li> <li>■ One or more fans on the Fan Tray module works slower than expected (heatingVentCoolingSystemProblem)</li> </ul>		
Alarm Severity	Condition	Text	Corrective Action
Critical	Fan-Tray is missing.	Fan-Tray is missing	<ol style="list-style-type: none"> <li>1. Check if the Fan Tray module is inserted in the chassis.</li> </ol>

Alarm Field	Description		
			<p>2. If the Fan Tray module was removed from the chassis, re-insert it.</p> <p>3. If the Fan Tray module has already been inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes.</p> <p>Warning: When removing the Fan Tray module while the power is on (or after it has recently been switched off), the blades may still be rotating at high speeds. Therefore, to avoid bodily harm, make sure that you don't touch the fan blades.</p>
Major	When one or more fans in the Fan Tray are faulty.	Fan-Tray is faulty	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module is in place and fans are working.	-	-

## Power Supply Alarm

Alarm Field	Description
Description	<p>This alarm is activated in one of the following cases:</p> <ul style="list-style-type: none"> <li>■ The HA (High Availability) feature is active and one of the power supply units is faulty or missing.</li> <li>■ PS unit is inserted in its location and functioning.</li> </ul>
SNMP Alarm	acPowerSupplyAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30

Alarm Field	Description		
Alarm Title	Power Supply Alarm		
Alarm Source	Chassis#0/PowerSupply#<m>, where m is the power supply's slot number		
Alarm Type	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	Condition	Text	Corrective Action
Major (default)	The HA (High Availability) feature is active (applicable only to Mediant 3000) and one of the power supply units is faulty or missing.	Power-Supply Alarm. Power-Supply is missing.	<ol style="list-style-type: none"> <li>1. Check if the unit is inserted in the chassis.</li> <li>2. If it was removed from the chassis, re-insert it.</li> <li>3. If it's inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes.</li> </ol>
Cleared	PS unit is placed and working.	-	-

## HA System Alarms

This section describes HA System alarms.

### HA System Fault Alarm

Alarm Field	Description
Description	<p>This alarm originates when:</p> <ul style="list-style-type: none"> <li>■ HA feature is active but the system is NOT working in HA mode. Reason is specified (for example: SW WD exception error, HW WD exception error, SAT device is missing, SAT device error, DSP error, BIT tests error, etc).</li> <li>■ HA feature is active and the redundant module is in start up mode but hasn't connected yet</li> </ul>

Alarm Field	Description		
	■ HA system is active		
SNMP Alarm	acHASystemFaultAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33		
Alarm Title	HA System Fault Alarm		
Alarm Source	System#0/Module#<m>, where m is the blade module's slot number		
AlarmType	qualityOfServiceAlarm		
Probable Cause	outOfService		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	HA feature is active but the system is not working in HA mode	Fatal exception error	High Availability (HA) was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.
		TCPIP exception error	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.
		Network processor exception error (applicable only to Mediant 3000)	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.
		SW WD exception error	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.

Alarm Field	Description	
		<p>HW WD exception error</p> <p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>SAT device is missing (applicable only to Mediant 3000)</p>	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>SAT device error (applicable only to Mediant 3000)</p>	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>DSP error (applicable only to Mediant 3000 and Mediant 4000)</p>	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>BIT tests error</p>	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>PSTN stack error (applicable only to Mediant 3000)</p>	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
	<p>Keep Alive error</p>	<p>HA was lost due to</p>

Alarm Field	Description		
			<p>switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
		Software upgrade	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
		Manual switch over	<p>HA was lost due to switchover and should return automatically after a few minutes.</p> <p>Corrective action is not required.</p>
		Manual reset	<p>HA was lost due to a system reset and should return automatically after few minutes. Corrective action is not required.</p>
		Board removal (applicable only to Mediant 3000)	<p>Return the removed board to the system.</p>
		TER misplaced (applicable only to Mediant 3000)	<p>Place the TER card according to the User's Manual</p>
		HW fault. TER in slot 2 or 3 is missing (applicable only to Mediant 3000)	<p>Place the TER card according to the User's Manual</p>
		HW fault. TER has old version or is not functional (applicable only to	<p>Replace the TER card.</p>

Alarm Field	Description		
		Mediant 3000)	

Alarm Field	Description		
		HW fault. invalid TER Type (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. invalid TER active/redundant state (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. Error reading GbE state (applicable only to Mediant 3000)	Replace the TER card.
		Redundant module is missing (applicable only to Mediant 3000)	<ul style="list-style-type: none"> <li>■ Insert the redundant module into the system.</li> <li>■ If the error continues, reset / replace the module.</li> </ul>
		Redundant is not connecting (applicable only to Mediant 3000)	Reset / replace the redundant module.
		Redundant is not reconnecting after deliberate restart	Reset / replace the redundant module.
		No Ethernet Link in redundant module	Connect Ethernet links to the redundant module
		SA module faulty or missing (applicable only to Mediant 3000)	Make sure the Shelf Alarm module is inserted correctly.
		Eth link error	HA was lost due to switchover, Connect the Eth link back.

Alarm Field	Description		
Minor	HA feature is active and the redundant module is in startup mode and hasn't connected yet	Higher HA priority (Not applicable to Mediant 3000)	HA was lost due to switchover to unit with higher HA priority and should return automatically after a few minutes. Corrective action is not required.
		Network watchdog error	HA was lost due to switchover, fix the network connectivity from failed unit.
		Waiting for redundant to connect (applicable only to Mediant 3000)	Corrective action is not required.
Cleared	HA system is active	-	-

## HA System Configuration Mismatch Alarm

Alarm Field	Description		
Description	HA feature is active. The active module was unable to transfer the License Key to the redundant module.		
SNMP Alarm	acHASystemConfigMismatchAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34		
Alarm Source	System#0/Module#<m>, where m is the blade module's slot number		
Alarm Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError		
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Major (default)	HA feature is active:	Configuration mismatch in the system:	The actions for the conditions are described below.
	License Keys of Active and Redundant modules are different.	Active and Redundant modules have different feature keys.	Update the Feature Keys of the Active and Redundant modules.
	The Active module was unable to pass on to the Redundant module the License Key.	Fail to update the redundant with feature key.	Replace the Feature Key of the Redundant module – it may be invalid.
	License key of the Redundant module is invalid.	Feature key did not update in redundant module.	Replace the Feature Key of the Redundant module – it may be invalid.
Cleared	Successful License Key update	The feature key was successfully updated in the redundant module	-

## HA System Switch Over Alarm

Alarm Fields	Description
Description	Sent when a switchover from the active to the redundant module has occurred.
SNMP Alarm	acHASystemSwitchOverAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35
Default Severity	Critical
Alarm Source	System#0/Module#<m>, where m is the blade module's slot number
Event Type	qualityOfServiceAlarm
Probable	outOfService

Alarm Fields	Description		
Cause			
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	A switchover from the active to the redundant unit has occurred	Switch-over: See the acHASystemFaultAlarm table above	See <a href="#">HA System Configuration Mismatch Alarm</a> on page 150 above for details.
Cleared	10 seconds have passed since the switchover	-	-

## Hitless Software Upgrade Alarm

Alarm Field	Description		
Description	A Notification trap that is sent out at the beginning and the end of a Hitless software update. Failure during the process will also instigate the trap. This alarm is only relevant for the local license key.		
SNMP Alarm	acHitlessUpdateStatus		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48		
Alarm Title	Hitless Update event		
Alarm Source	Automatic Update		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Indeterminate	A notification trap sent at the beginning and end of a hitless software update. Failure during the software update also activates the trap.	Hitless Update Event	The corrective action for each condition is described below.
	Hitless: Start software		Corrective action is not

Alarm Field	Description		
	upgrade.		required.
	Hitless fail: Invalid cmp file file - missing Version parameter.		Replace the cmp file with a valid one.
	Hitless fail: The software version stream name is too long.		Replace the cmp file with a valid one.
	Hitless fail: Invalid cmp file - missing UPG parameter.		Replace the cmp file with a valid one.
	Hitless fail: Hitless software upgrade is not supported.		Replace the cmp file with a valid one that supports hitless upgrade of the software from the current version to the new one.
	Hitless: Software upgrade ended successfully.		Corrective action is not required.

## Redundant Board Alarm

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

Alarm Field	Description
Additional Info	-
Corrective Action	-

## HA Network Watchdog Status Alarm

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

Alarm Field	Description	
Network watchdog is disabled while Redundant units has less Eth groups available	One or more of the Redundant unit's Ethernet Groups are down	-
Disabling network watchdog due to network interface error in Redundant unit	One or more of the Redundant unit's Ethernet Groups are down	-

### License Key Hitless Upgrade Alarm

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

## HA Network Mismatch Alarm

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

## HA Network Monitor Alarm

Description	Alarm Fields		
Description	This alarm is sent when all previously reachable destinations configured for a specific row in the HA Network Monitor table (for the HA Network Monitor feature) are now unreachable (i.e., none of them reply to the device's pings). For configuring the HA Network Monitor feature, refer to the User's Manual.		
SNMP Alarm	acHANetworkMonitorAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.136		

Description	Alarm Fields		
Alarm Title	HA Network Monitor Alarm		
Alarm Source	Board#1/NetworkMonitor#X		
Alarm Type	communicationsAlarm		
Probable Cause	connectionEstablishmentError		
Alarm Severity	Condition	Text	Corrective Action
Major	All destinations of a specific row in the HA Network Monitor table that replied in the past to the device's pings are now "unreachable"	"Destination/s <peer destination IP address(es)> is/are unreachable"	-
Cleared	At least one of the "unreachable" destinations replies to the device's pings and is now "reachable", or the row in the HA Network Monitor table has been deleted	-	-

## HA Ethernet Group Alarm

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

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

## License Pool Alarms

This section describes License Pool alarms.

### License Pool Infra Alarm

Alarm Field	Description
Description	<p>This alarm is raised under the following circumstances:</p> <ul style="list-style-type: none"> <li>■ The device was unable to access the SBC License Pool Manager.</li> <li>■ The device license has expired.</li> <li>■ The device is no longer managed by the SBC License Pool Manager.</li> </ul>
SNMP Alarm	acLicensePoolInfraAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.106
Alarm Source	system0Mo
Alarm Type	communicationsAlarm
Probable Cause	keyExpired, fail to connect to license pool server.

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Major	The last attempt to establish an HTTPS REST connection with OVOC SBC License Pool Manager server was not successful.	Device was unable to access the License Server.	<ul style="list-style-type: none"> <li>■ Wait for the next connection attempt.</li> <li>■ In the SBC License Pool Manager, perform the 'MG Update' action to reestablish REST connection with device and send the current license.</li> </ul>
	The device has been configured as Non-Managed in the SBC License Pool Manager. If there are active licensed sessions for this device, the device automatically performs a reset or hitless upgrade.	Device is no longer managed by the SBC License Pool.	If you wish, reconfigure the device as managed by the SBC License Pool Manager.
Critical	Device unable to establish an HTTPS REST connection with OVOC SBC License Pool Manager server after successive attempts.	License-pool is about to expire.	In the SBC License Pool Manager, perform the 'MG Update' action to reestablish REST connection with device and send the latest license.
	The device license has expired.	The device license has expired! Use of this device is strictly prohibited.	
Clear	This alarm is cleared when: <ul style="list-style-type: none"> <li>■ Connection has been reestablished with the SBC License Pool Manager, an updated license has been loaded</li> </ul>	-	

Alarm Field	Description		
	<p>to device and apply/reset has been performed.</p> <ul style="list-style-type: none"> <li>■ The device has been reconfigured as managed by the SBC License Pool Manager, a new license has been loaded to the device, and and apply/reset has been performed.</li> </ul>		

### License Pool Application Alarm

Alarm Field	Description		
Description	This alarm is raised when the device requires a reset or apply hitless upgrade after receiving a new license.		
SNMP Alarm	acLicensePoolApplicationAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.107		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	New license pool		
Alarm Severity	Condition	Text	Corrective Action
Major	SBC License key has been received from SBC License Pool Manager Server.	New license pool allocations received	<p>Perform one of the following actions in the SBC License Pool Manager to apply the new license:</p> <ul style="list-style-type: none"> <li>■ For stand-alone devices, reset the device.</li> <li>■ For HA devices, apply a hitless upgrade or reset the device.</li> </ul>

## License Pool Over Allocation Alarm

Alarm Field	Description		
Description	This alarm is raised when the SBC license received from the SBC License Pool Manager has exceeded the maximum capacity supported by the device.		
SNMP Alarm	acLicensePoolOverAllocationAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.125		
Alarm Source	system0Mo		
Alarm Type	communicationsAlarm		
Probable Cause	Overallocation		
Alarm Severity	Condition	Text	Corrective Action
Warning (displayed after the configuration has been applied in the SBC License Pool Manager; however, prior to device reset or hitless upgrade).	The SBC license received from the License Pool Manager has exceeded the maximum capacity supported by the device.	"Some of the license pool allocations exceed maximum capability and will not be applied"	<p>In the SBC License Pool Manager, do one of the following:</p> <ul style="list-style-type: none"> <li>■ Apply the new license (reset device or apply hitless upgrade); the device sets its SBC capacity to maximum and disregards the excess configured sessions.</li> <li>■ Reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).</li> </ul>
Warning (displayed after device restart).	The SBC license received from the License Pool Manager Server has exceeded the maximum capacity	"Some of the license pool allocations will not be used because of over-allocation"	In the SBC License Pool Manager, reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).

Alarm Field	Description		
	supported by the device		

## Floating License Alarms

This section describes Floating License alarms.

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

Alarm Field	Description		
Description	This alarm is raised when there are insufficient physical memory resources to allocate for configuring the “Floating License” with the configured Custom Allocation Profile in the device’s Floating License table.		
SNMP Alarm	acFloatingLicenseAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.138		
Alarm Title	Floating License Alarm - Not enough memory to allocate 'custom' profile		
Alarm Source	Board#1		
Additional Info	Detailed explanation of the License configuration parameter that resulted in this alarm, including the requested and actual value. For example, “SignalingSessions – requested 10000, allocated 1000”		
Alarm Type	processingErrorAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	An attempt was made to configure a Custom Allocation Profile with values exceeding the device’s physical memory.	“Not enough memory to allocate for 'custom' profile”	Define a Custom Allocation Profile within the bounds of the device’s capacity.

## Cloud License Manager Alarm

Alarm Field	Description		
Description	<p>This alarm is raised under one of the following circumstances:</p> <ul style="list-style-type: none"> <li>■ Disconnection between the device and OVOC.</li> <li>■ Failure to send usage reports from the device to OVOC.</li> <li>■ Fixed license is enabled and an attempt was made to enable the Floating license.</li> </ul>		
SNMP Alarm	acCloudLicenseManagerAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.132		
Alarm Title	Cloud License Manager Alarm		
Alarm Source	Board#1		
Alarm Type	processingErrorAlarm		
Probable Cause	configurationOrCustomisationError		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Major	There is no connection between the device and OVOC either prior to the initial handshake or due to a long disconnection time (default is three months; this time may be overridden by OVOC).	"No connection with OVOC"	<ul style="list-style-type: none"> <li>■ Check TCP/TLS connectivity.</li> <li>■ Device should be registered on OVOC.</li> </ul>
	Usage reports could not be sent to OVOC from the device for a specified number of days.	"Failed to send usage report to OVOC for X days"	Check TCP/TLS connectivity.

Alarm Field	Description		
	The device is configured to work with the Fixed License Pool and an attempt was made to enable the Floating license.	"Floating license cannot be enabled, when device is managed by License Pool"	<ul style="list-style-type: none"> <li>■ Disable Floating License parameter on the device.</li> <li>■ Remove the device from the Fixed License Pool in OVOC.</li> </ul>
Critical	Device couldn't connect to OVOC (handshake).	"Connection with OVOC failed with response code <XXX>". See below for more information"	<ul style="list-style-type: none"> <li>■ &lt;Forbidden 403&gt;: contact AudioCodes support.</li> <li>■ &lt;unauthorized 401&gt;: check username/password</li> </ul>
	Device couldn't connect to OVOC (handshake).	"Connection with OVOC failed, Failed initialize connection"	Check TCP/TLS connectivity.
	Device couldn't initialize connection to OVOC (handshake).	"Device was rejected by OVOC while trying to retrieve the device ID"	<Forbidden 403>: contact AudioCodes support.
Cleared	<ul style="list-style-type: none"> <li>■ Connection with OVOC is established.</li> <li>■ Reports are sent successfully.</li> <li>■ The Floating License parameter is disabled on the device or the device is removed from the Fixed License Pool. This alarm is cleared upon the next</li> </ul>	-	-

Alarm Field	Description		
	reboot.		

HTTP response code and reason:

- Other 4xx-6xx responses: the device retries the request using the value in retry-after header if specified, or immediately following an update of the OVOC Product key.
- OVOC response to Register requests:
  - 200 In case of successful request
  - 400: request format is not valid or request data is not valid, or if OVOC is in a state of initial registration required
  - 401: username or password are incorrect
  - 403: customer is blocked, or OVOC maximum capacity has been reached
  - 404: request URI contains a device ID not identified by OVOC.
  - 500: server is not able to handle the request due to server side error (no resources, internal component failure etc.)
- Server may respond with 4xx or 5xx error as defined in HTTP RFC when appropriate.

## Flex License Manager Alarm

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

Alarm Field	Description		
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").		

## Mediant 2600 E-SBC and Mediant 4000 SBC Alarms

This section describes Mediant 2600 E-SBC and Mediant 4000 SBC alarms.

### DSP Farms Mismatch Alarm

Alarm Field	Description
Description	This alarm is sent if the number of MPM modules (DSP farms) configured by the ini file parameter DspFarmsInstalledNum (default is 0) is greater than the actual MPM modules installed in the device's chassis. This alarm and the parameter are used to check that all required MPMs are present and correctly installed in the device's chassis.
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.143
SNMP Alarm	AcDSPFarmsMismatchAlarm

Alarm Field	Description		
Alarm Title	DSP Farms Mismatch Alarm		
Alarm Source	Board#1/ClusterManager#1/MT#2		
Alarm Type	equipmentAlarm		
Probable Cause	Underlying Resource Unavailable		
Alarm Severity	Condition	Text	Corrective Action
Major	The number of MPMs configured by the DspFarmsInstalledNum parameter is greater than the number of MPMs installed on the chassis. This could result in a faulty or missing MPM module(s).	"Missing DSP farm was detected."	<ul style="list-style-type: none"> <li>■ Check if the MPM module(s) is fully inserted into the chassis slot.</li> <li>■ If an MPM module(s) was removed from the chassis, re-install it.</li> <li>■ Make sure that the DspFarmsInstalledNum parameter is configured to the correct number of physical MPM modules.</li> <li>■ If you have performed all the above and the alarm still exists, send a Return Merchandise Authorization (RMA) request to AudioCodes</li> </ul>
Cleared	The number of MPMs configured by the DspFarmsInstalledNum parameter is less than or equal to the number of MPMs installed in the chassis.	-	-

## Mediant 9000 and Software SBC Alarms

This section describes Mediant 9000 and Software SBC alarms.

## Cluster HA Alarm

Alarm Field	Description		
Description	The alarm is sent by the Cluster Manager when the cluster HA usage exceeds 100%. HA usage of 100% means that if a failure occurs in a Media Component (MC or vMC), sufficient DSP resources are available on the other Media Components in the cluster to take over the transcoding sessions of the failed Media Component. HA usage exceeding 100% means that insufficient DSP resources are available on the other Media Components to take over the transcoding sessions of the failed Media Component.		
SNMP Alarm	acMtcMClusterHaAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.115		
Alarm Title	CM Cluster HA Alarm		
Alarm Source	device/clusterManager		
Alarm Type	equipmentAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Major	Cluster HA usage exceeds 100%.	"At least one of the MTCEs is inactive, MTC will now provide only partial HA"	<ul style="list-style-type: none"> <li>■ Make sure all Media Transcoders are properly connected to the Cluster Manager.</li> <li>■ Make sure all Media Transcoders in the Media Transcoders table are in Admin State "Unlocked" and Status "Connected".</li> </ul>

Alarm Field	Description		
Cleared	HA usage drops to below 95%	-	-

### Media Transcoder Network Failure

Alarm Field	Description		
Description	The alarm is sent when the Cluster Manager (Media Transcoding Cluster feature) or Signalling Component (Elastic Media Cluster feature) fails to connect to the Media Component.		
SNMP Alarm	acMtceNetworkFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.116		
Alarm Title	MT Network Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	communicationsAlarm		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	Connection failure with Media Transcoder	"No Connection with MTCE: <MTCE-name>"	For the Media Transcoding Cluster feature, ensure a physical connection exists between the Media Component and the Cluster Manager.
Cleared	Connection established / re-established with Media Transcoder	-	-

### Media Transcoder Software Upgrade Failure

Alarm Field	Description
Description	The alarm is sent upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Component.
SNMP Alarm	acMtceSwUpgradeFailureAlarm

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

### Media Transcoder High Temperature Failure

Alarm Field	Description		
Description	The alarm is raised when the temperature of the Media Transcoder chassis reaches a critical threshold.		
SNMP Alarm	acMtceHwTemperatureFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.118		
Alarm Title	MT Temperature Failure		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Alarm Type	Equipment Alarm		
Probable Cause	-		
Alarm Severity	Condition	Text	Corrective Action

Alarm Field	Description		
Major	Temperature of Media Transcoder reaches critical threshold	"MTCE reached high temperature threshold"	<ul style="list-style-type: none"> <li>■ 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.</li> <li>■ Check the chassis ventilation outlet and make sure that they are not obstructed for air flow.</li> <li>■ 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.</li> </ul>
Cleared	Connectivity with Media Transcoder is re-established and temperature is reduced	-	-

## Media Transcoder Fan Tray Module Failure

Alarm Field	Description
Description	The alarm is raised upon a failure in the Fan Tray module of the Media Transcoder.
SNMP Alarm	acMtceHwFanTrayFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.119
Alarm Title	MT HW Fan Tray Failure

Alarm Field	Description		
Alarm Source	.../MTCE#1/fanTray#1		
AlarmType	equipmentAlarm		
Probable Cause	heatingVentCoolingSystemProblem		
Alarm Severity	Condition	Text	Corrective Action
Minor	Failure in Fan Tray module of Media Transcoder	"MTCE fan tray fault"	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module status returns to normal	-	-

### Media Transcoder Power Supply Module Failure

Alarm Field	Description		
Description	The alarm is raised upon a failure in the Power Supply module of the Media Transcoder.		
SNMP Alarm	acMtcePsuFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.120		
Alarm Title	MT Power Supply Failure		
Alarm Source	.../MTCE#1/powerSupply#1		
Alarm Type	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	Condition	Text	Corrective Action
Minor	Failure in Power Supply module of	"MTCE power supply unit	<ul style="list-style-type: none"> <li>■ Check if the Power Supply module is inserted in the chassis.</li> <li>■ If it was removed from the chassis,</li> </ul>

Alarm Field	Description		
	Media Transcoder	fault"	<p>re-insert it.</p> <ul style="list-style-type: none"> <li>■ If the Power Supply module is inserted in the chassis and the alarm is still raised, send a Return Merchandise Authorization (RMA) request to AudioCodes.</li> </ul>
Cleared	Power Supply module status returns to normal	-	-


### Cluster Bandwidth Utilization Alarm

Alarm Field	Description		
Description	The alarm is raised when the bandwidth utilization of a Cluster interface exceeds the configured maximum bandwidth (refer to the MtcClusterNetworkMaxBandwidth parameter).		
SNMP Alarm	acClusterBandwidthAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.126		
Alarm Title	Cluster Bandwidth Utilization Alarm		
Alarm Source	Board#1/EthernetLink#<ehernet port number>		
Alarm Type	Other		
Probable Cause	<p>performanceDegraded:</p> <ul style="list-style-type: none"> <li>■ Too many sessions processed on the specific Cluster interface.</li> <li>■ Cluster interface is being used by another application (e.g., OAMP).</li> </ul>		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Major	Bandwidth utilization is greater than	"Cluster Bandwidth is above 90%	Reduce the number of Media Transcoders on that Cluster interface. Alternatively, the overall permitted

Alarm Field	Description		
	90%.	utilization on Interface name: <name>. No more transcoding sessions will be allocated on that Cluster Interface"	bandwidth for the Cluster interfaces should be increased, if possible (using the ini file parameter MtcClusterNetworkMaxBandwidth).
Minor	Bandwidth utilization is between 85 and 90%. Note: If a Major alarm was raised and the bandwidth later declined to between 80 and 85%, the alarm is changed to Minor.	"Cluster Bandwidth is above 85% utilization on Interface name: <name>"	
Clear	Bandwidth utilization is less than 80%.		


## Media Cluster Alarm

Alarm Field	Description
Description	<p>The alarm is sent when the Media Cluster is enabled and one of the following scenarios exist:</p> <ul style="list-style-type: none"> <li>■ There are no operational Media Components in the Media Cluster.</li> <li>■ There are no media interfaces configured for the operational Media</li> </ul>

Alarm Field	Description		
	<p>Components.</p> <div>  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 <i>Stack Manager for Mediant CE SBC User's Manual</i>. </div>		
SNMP Alarm	acMediaClusterAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.133		
Alarm Title	Media Cluster Alarm		
Alarm Source	Device/clusterManager		
Alarm Type	-		
Probable Cause	-		
Alarm Severity	Condition	Text	Corrective Action
Major	Media Cluster is enabled, however, no media interface is configured for the operational Media Components	Media Cluster Alarm: Media Cluster <MC Name>, Remote Interface - Alarm Status is NoRmifPresent.	Configure media interfaces on the Media Components.
Clear	A media interface is configured on the Media Component, or the Media Component is removed from the Cluster Manager	Media Cluster : Media Cluster <MC Name>, Remote Interface - Alarm Status is Clear	-

## Remote Interface Alarm

**Table 6-4: Remote Interface Alarm**

Alarm Fields	Description		
Description	<p>This alarm is raised in the following circumstances:</p> <ul style="list-style-type: none"> <li>■ A Media Interface ethXX exists in the Remote Interface table, and this interface is used by one or more Media Realms; however, it is not defined in a specific Media Cluster.</li> <li>■ A Media Interface ethXX exists in the Remote Interface table of the Cluster Manager (CM) and is used by one or more Media Realms; however, it does not have a public IP address configured on the Media Cluster i.e. a NAT rule is defined for a Remote Interface which is referenced by a Media Realm, however, an MC does not have a public IP address for this interface.</li> <li>■ A Media Interface ethXX exists in the Remote Interface table of the Cluster Manager(CM) and is used by one or more Media Realms; however, it's status is link down.</li> </ul> <div>  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. </div>		
SNMP Alarm	acMediaClusterRemoteInterfaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.134		
Alarm Title	Remote Interface Alarm		
Alarm Source	device/clusterManager/MC		
Alarm Type	Media Cluster		
Probable Cause	-		
Alarm Severity	Condition	Text	Corrective Action
Major	According to description above.	<ul style="list-style-type: none"> <li>■ Interface &lt;Interface id&gt;, Name: &lt;ethXX&gt; - Alarm Status is</li> </ul>	<ul style="list-style-type: none"> <li>■ Add the appropriate Media Interface</li> </ul>

Alarm Fields	Description		
		<p>RmifMissing</p> <ul style="list-style-type: none"> <li>Interface &lt;Interface id&gt;, Name: &lt;ethXX&gt; - Alarm Status is PublicIpAddrMissing</li> <li>Remote Interface Alarm: Interface &lt;Interface id&gt;, Name: &lt;ethXX&gt; - Alarm Status is LinkDown</li> </ul>	<p>ethXX</p> <ul style="list-style-type: none"> <li>Configure a public IP address on the Media Cluster or remove the NAT rule.</li> <li>Troubleshoot the Media Interface ethXX</li> </ul>

### AWS Security Role Alarm

Alarm Field	Description
Description	The alarm is sent when the Amazon Web Services (AWS) instance has not been configured with the required IAM role to access AWS services and resources.
SNMP Alarm	acAWSSecurityRoleAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.139
Alarm Title	AWS Security Role Alarm
Alarm Source	Board#1
Alarm Type	securityServiceOrMechanismViolation
Probable Cause	configurationOrCustomizationError
Alarm Severity	Condition
Major	IAM role was not found, or access to AWS services was blocked
Cleared	IAM role was found and permission to access AWS services was granted

## CDR Server Alarm

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

## Metering Alarm

Alarm Field	Description
Description	The alarm is sent when the device fails to communicate with the Amazon Web Services (AWS) Marketplace metering API. The device needs to communicate with the Marketplace API when using AudioCodes' Metered License model to license the SBC, which is based on the device's usage (in minutes).
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.146
SNMP Alarm	acMeteringAlarm

Alarm Field	Description		
Alarm Title	Metering Alarm		
Alarm Source	Board#1 (SystemMO)		
Alarm Type	communicationsAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	The device is unable to send a usage report to the AWS metering service after it has initially connected with it.	"No connection to metering API – service will be down in 3 hours"	Check the network configuration and make sure that the device has the appropriate environment as required for the metering offer.
Critical	The device is unable to establish an initial connection with the AWS metering API, or has lost connectivity with the metering API for 3 hours since the last connection.	"Service down due to no connection to metering API"	Check the network configuration and make sure that the device has the appropriate environment as required for the metering offer.
Cleared	The device successfully communicates with the AWS metering API.	"Device succeeds to communicate with metering API"	-

## MC Not Secured Alarm

This alarm is relevant for the Mediant CE SBC.

Alarm Field	Description		
Description	This alarm is raised when the connection between the Signaling Cluster (SC) and the Media Cluster (MC) fails or when an upgrade is not successfully applied by SC to the MC.		
SNMP Alarm	acMCNotSecuredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.151		
Alarm Title	MC Not Secured		
Alarm Source	securityServiceOrMechanismViolation		
Alarm Type	alarmTrap		
Probable Cause	versionMismatch		
Alarm Severity	Condition	Text	Corrective Action
Warning	<ul style="list-style-type: none"> <li>■ When the SC is configured to work in TLS mode and then there is a switchover to the redundant SC, an MC in the cluster still connects to SC in non-secure TCP mode. As a result ,the connection between SC and MC fails.</li> <li>■ The MC is disconnected from the SC for unspecified reasons.</li> </ul>	No Connection with MC	Reset the disconnected MC.
Warning	<p>The SC attempts to load the user-requested firmware to the MC and then one of the following occurs:</p> <ul style="list-style-type: none"> <li>■ The upgrade is successful, however the connection cannot be established due to networking issues or to new firmware-related issues.</li> </ul>	Failed to upgrade MC software for MC	Check the firmware, reload the firmware to the MC and reset the MC.

Alarm Field	Description		
	<ul style="list-style-type: none"> <li>The upgrade process fails and the MC boots up and connects with its previous firmware version.</li> </ul>		
Warning	<p>Its detected that SC is configured to work in TLS and MC is configured to work in TCP mode and therefore you need to upgrade or restart the device in order for MC to retrieve the updated configuration from SC in order to synchronize connection in TLS mode.</p>	<ul style="list-style-type: none"> <li>MC &lt;MTCENName&gt; should be upgraded</li> <li>MC &lt;MTCENName&gt; should be restarted</li> </ul>	<p>Upgrade and restart the MC that is currently operating in non-secure TCP mode.</p>
Clear	<ul style="list-style-type: none"> <li>The MC successfully connects to SC in TLS secure mode.</li> <li>The firmware upgrade to the MC is successful and a connection is established between SC and MC.</li> </ul>		

## TLS Certificate Mismatch Alarm

This alarm is relevant for the Mediant CE SBC device.

Alarm Field	Description
Description	This alarm is raised when the Server Certificate file required to secure the TLS connection between the Signaling Cluster (SC )and the MC is not automatically loaded to MC and therefore there is a configuration mismatch between the Media Cluster and the SC.
SNMP Alarm	acTLSCertificateMismatchAlarm
SNMP OID	.1.3.6.1.4.1.5003.9.10.1.21.2.0.154
Alarm Title	TLS Certificate Mismatch Alarm
Alarm Source	communicationsAlarm
Alarm Type	alarmTrap

Alarm Field	Description		
Probable Cause	communicationsSubsystemFailure		
Alarm Severity	Condition	Text	Corrective Action
Minor	The certificate file required to secure the TLS connection between the SC and MC has not been automatically updated to the MC.	Private key and Certificate file do not match.	Manually load the required server certificate file to the MC.

## Stack Manager Alarms

This section describes the Stack Manager alarms.

### REST API Failure

Alarm Field	Description		
Description	This alarm is raised when the Stack Manager can't establish connection with the stack via REST API.		
SNMP Alarm	acSmRestApi		
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.1		
Alarm Title	REST API Failure		
Alarm Source	<ul style="list-style-type: none"> <li>■ For Mediant VE/CE stack: &lt;stack-name&gt;</li> <li>■ For Voice.AI Connect stack: &lt;stack-name&gt;/center or &lt;stack-name&gt;/sbc-X</li> </ul>		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	The Stack Manager can't establish connection	Cannot connect to SBC via REST API.	Ensure that Stack Manager can access the SBC management interface via HTTPS protocol. Use

Alarm Field	Description		
	with Mediant VE/CE stack via REST API.		<p>“curl -k https://&lt;sbcsip&gt;” command in Stack Manager CLI interface to verify whether HTTPS connection is working. If not, configure Network Security Group / firewall rules to allow the connection.</p> <p>If the HTTPS connection is working, however the Stack Manager still fails to connect to the REST API, update credentials used by the Stack Manager via the following procedure:</p> <ol style="list-style-type: none"> <li>1. Log into the Stack Manager.</li> <li>2. Select the stack that represents specific Mediant VE/CE.</li> <li>3. In the toolbar, click Modify</li> <li>4. In the Advanced Config section, enter the following parameters: username = &lt;username&gt; password = &lt;password&gt;</li> <li>5. At the bottom of the screen, click <b>Modify</b> to apply the changes.</li> </ol>
Clear	Connection between the Stack Manager and the Mediant VE/CE is restored.	Successfully connected to SBC via REST API.	-
Major	The Stack Manager can't establish connection with Voice.AI Connects' Data center component via REST API.	Cannot connect to Data center via REST API.	<p>Ensure that Stack Manager can access Data center management interface via HTTP protocol on port 8081. Use “curl http://&lt;center-ip&gt;:8081” command in Stack Manager CLI interface to verify whether HTTP connection is working. If not, configure network security group / firewall rules to allow the connection.</p>

Alarm Field	Description		
Clear	Connection between the Stack Manager and Voice.AI Connects' Data center component has been restored.	Successfully connected to Data center via REST API.	-
Major	Stack Manager can't establish connection with Voice.AI Connects' SBC component via REST API.	Cannot connect to SBC 'sbc-X' via REST API.	Ensure that Stack Manager can access the SBC Management interface via HTTPS protocol. Use "curl -k https://<sbc-ip>" command in Stack Manager CLI interface to verify whether HTTPS connection is working. If not, configure Network Security Group / Firewall rules to allow the connection.
Clear	Connection between the Stack Manager and Voice.AI Connects' SBC component has been restored.	Successfully connected to SBC 'sbc-X' via REST API.	-

### Stack Manager Down

Alarm Field	Description
Description	This alarm is raised when one of the stack components is not in service.
SNMP Alarm	acSmDown
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.2
Alarm Title	Stack Manager Down
Alarm Source	<stack-name>/<components-name>

Alarm Field	Description		
	Where <component-name> is one of the following: <ul style="list-style-type: none"> <li>■ For Mediant VE stack: 'sbc-X'</li> <li>■ For Mediant CE stack: 'sc-X' or 'mc-X'</li> <li>■ For Voice.AI Connect stack: 'center', 'sm-X' or 'sbc-X'</li> </ul>		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Minor	<ul style="list-style-type: none"> <li>■ One of Mediant CE's components is not in service.</li> </ul>	<ul style="list-style-type: none"> <li>■ Signaling component 'sc-X' is 'down'</li> <li>■ Media component 'mc-X' is 'down'</li> </ul>	Return the component back into service. For example, start the corresponding VM.
Clear	<ul style="list-style-type: none"> <li>■ Mediant CE's component is back in service.</li> </ul>	<ul style="list-style-type: none"> <li>■ Signaling component 'sc-X' is 'up'</li> <li>■ Media component 'mc-X' is 'up'</li> </ul>	-
Minor	<ul style="list-style-type: none"> <li>■ Mediant VE's component is not in service.</li> </ul>	Instance 'sbc-X' is 'down'	Return the component back into service. For example, start the corresponding VM.
Clear	<ul style="list-style-type: none"> <li>■ Mediant VE's component is back in service.</li> </ul>	Instance 'sbc-X' is 'up'	-
Minor	<ul style="list-style-type: none"> <li>■ Voice.AI Connect's component is not in service.</li> </ul>	<ul style="list-style-type: none"> <li>■ Data center is 'down'</li> <li>■ Session manager 'sm-X' is 'down'</li> </ul>	Return the component back into service. For example, start the corresponding VM.

Alarm Field	Description		
		■ SBC 'sbc-X' is 'down'	
Clear	■ Voice.AI Connect's component is back in service.	■ Data center is 'up' ■ Session manager 'sm-X' is up' ■ SBC 'sbc-X' is 'up'	-

### Stack Manager Status Error

Alarm Field	Description		
Description	This alarm is raised when the Stack Manager can't read the status of one of the stack components.		
SNMP Alarm	acSmStatusError		
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.3		
Alarm Title	Stack Manager Status Error		
Alarm Source	■ For Mediant CE stack: <stack-name>/mc ■ For Voice.AI Connecty stack: <stack-name>/sm-X		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	The Stack Manager can't read the status of Mediant CE's Media Components.	Cannot read media components status	Check Media Component status via Mediant CE Web management interface. Use "Heal" operation to fix Mediant CE configuration.

Alarm Field	Description		
Clear	The Stack Manager can read the status of Mediant CE's Media Components.	Successfully read media components status	-
Minor	The Stack Manager can't read the status of Voice.AI Connect's session manager.	Session manager 'sm-X' is missing from Data center	Use "Heal" operation to fix Voice.AI Connect configuration.
Clear	The Stack Manager can read the status of Voice.AI Connect's session manager.	Session manager 'sm-X' is present in Data center	-

### Stack Manager Configuration Error

Alarm Field	Description		
Description	This alarm is raised when the Stack Manager detects an error in the stacks configuration.		
SNMP Alarm	acSmConfError		
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.4		
Alarm Title	Stack Manager Configuration Error		
Alarm Source	<stack-name>/mc-X		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Minor	One of the media components is missing from Mediant CE's configuration.	Media component 'mc-X' is missing from SBC configuration.	Use "Heal" operation to fix Mediant CE configuration.
Clear	All media components are present in Mediant CE's	Media component 'mc-X' is present in	-

Alarm Field	Description		
	configuration.	SBC configuration.	

### Stack Manager Accelerated Network Error

Alarm Field	Description		
Description	This alarm is raised when one of the stack components lack the correct accelerated networking configuration.		
SNMP Alarm	acSmAccelNetwork		
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.5		
Alarm Title	Stack Manager Accelerated Network Error		
Alarm Source	<stack-name>/mc-X		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Minor	Accelerated networking is incorrectly configured on one of the Mediant CE's media components	Media component 'mc-X' lacks accelerated networking	The reason for the problem is an intermittent error in the Azure APIs (or temporary lack of resources in Azure Data center) during VM creation.  To fix the problem, use the "Rebuild" operation to rebuild the corresponding media component.
Clear	Accelerated networking is correctly configured on the specific Mediant CE's media components.	Media component 'mc-X' lacks accelerated networking	-

### Stack Manager No HA

Alarm Field	Description		
Description	This alarm is raised when specific stack components are not in “high availability” state.		
SNMP Alarm	acSmNoHa		
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.6		
Alarm Title	Stack Manager No HA		
Alarm Source	<stack-name>		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Minor	Mediant CE’s signaling components are not in “high availability” state.	Signaling components are not in HA mode.	Bring the redundant signaling component back into service. For example, start the corresponding VM.
Clear	Mediant CE’s signaling components are in “high availability” state.	Signaling components are in HA mode.	-

### Stack Manager Activity Log

Alarm Field	Description
Description	This event is raised for activities performed by the Stack Manager
SNMP Alarm	acSmActivityLog
SNMP OID	.1.3.6.1.4.1.5003.9.100.1.2.0.7
Alarm Title	Stack Manager Activity Log

Alarm Field	Description		
Alarm Source	<empty>		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	Activity performed by user – e.g. stack was created or scaled-in.	Detailed description of activity performed by user.	

## MP-1288 Alarms

This section describes the MP-1288 alarms.

### Module Service Alarm

Alarm Field	Description		
Description	This alarm is raised in the following circumstances: <ul style="list-style-type: none"> <li>■ Multiple FXS ports on a specific FXS blade are Out-Of-Service.</li> <li>■ Hardware faults with the blades DSP.</li> </ul>		
SNMP Alarm	acModuleServiceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.122		
Alarm Source	Chassis/Module# (Analog)		
Alarm Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	Condition	Text	Corrective Action
Minor	More than five FXS ports and less than 33% of FXS ports are Out-Of-Service on a this blade.	Multiple FXS ports are Out-Of-Service.	Service the faulty blade.
Major	■ More than 33% of FXS	Multiple	Service the faulty blade.

Alarm Field	Description		
	<p>ports are Out-Of-Service on this blade.</p> <p>■ There is a hardware fault on the DSP blade. If the fault is due to the exceeding of the high temperature limit, all FXS ports on this blade are Out-Of-Service.</p>	FXS ports are Out-Of-Service.	
Clear	Major to Minor: Less than 25% of FXS ports are Out-Of-Service on the blade.	-	If this alarm has been raised as a result of a high DSP temperature as described above, then you must power reset the device to return the blade to service.
	The FXS module has less than 4 FXS ports that are Out-Of-Service on the blade.		

## Module Operation Alarm

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

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

## Port Service Alarm

Alarm Field	Description
Description	<p>This alarm is raised when an FXS port is out of service due to the following:</p> <ul style="list-style-type: none"> <li>■ The Serial Peripheral Interface (SPI) connection with the port is lost.</li> <li>■ The temperature threshold on an FXS port has been exceeded.</li> <li>■ An FXS port is inactive due to a ground fault.</li> </ul>
SNMP Alarm	acPortServiceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.124
Alarm Source	Chassis/Module#/FXS Port #
Alarm Type	equipmentAlarm
Probable Cause	outOfService

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Minor	<p>The relevant FXS ports is faulty due to the reasons described above. In addition, note the following:</p> <ul style="list-style-type: none"> <li>■ If the number of faulty FXS ports is above four on the same module, then the acModuleOperationAlarm alarm is raised (see above).</li> <li>■ If there were active sessions on the device, then these calls are disconnected. No new SIP outbound calls will be initiated towards these FXS lines on this device.</li> </ul>	"FXS Port state was changed to Out of Service" (the detailed reason will be provided in: Syslog, in the Web detailed port status description and in WEB tooltip per FXS port)	Service the faulty FXS port.
Clear	<p>This alarm is cleared when:</p> <ul style="list-style-type: none"> <li>■ The Serial Peripheral Interface (SPI) connection is restored.</li> <li>■ The FXS port temperature falls within the threshold.</li> <li>■ The ground fault is cleared.</li> <li>■ The acModuleServiceAlarm (see above) is raised i.e. the number of faulty FXS ports on the module is above four.</li> </ul>		

## MSBR Alarms

This section describes the MSBR alarms.

### WAN Link Alarm

Alarm Field	Description
Description	This alarm is raised when the WAN Link is down and cleared when the link is up.

Alarm Field	Description
SNMP Alarm	acBoardWanLinkAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.79
Alarm Title	WAN Link alarm
Alarm Source	Board#x/WanLink#y
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	Major / Clear
Additional Info	-
Corrective Action	Connect the WAN port.

### Power Over Ethernet Status [Event]

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

Alarm Field	Description
	client in a PoE-enabled LAN port.
Additional Info	-
Corrective Action	-

## Wireless Cellular Modem Alarm

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

## Wireless Cellular Modem Status Changed

Alarm Field	Description
Description	Sent upon a change in the status of the 3G cellular (wireless) USB modem. A change can be in any of the following:

Alarm Field	Description		
	<ul style="list-style-type: none"> <li>■ Vendor ID</li> <li>■ Product ID</li> <li>■ Cellular state (shutdown or no shutdown)</li> <li>■ Received Signal Strength Indicator (RSSI) in dBm</li> <li>■ Cellular dongle status ("up" or "down")</li> </ul>		
SNMP Alarm	acWirelessCellularModemStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.104		
Alarm Title	Wireless Cellular Modem Status Changed		
Alarm Source	Board#x/WanLink#y		
Alarm Type	Equipment Alarm		
Probable Cause	other (0)		
Alarm Severity	Condition	Text	Corrective Action
Indeterminate		MSBR cellular interface: dongle type <vendor ID>:<product ID>,modem <"on" or "off">,RSSI <dBm value> DBM.	

## Data Interface Status

Alarm Field	Description
Description	This alarm is sent when a DSL interface state changes to up or down.
SNMP Alarm	acDataInterfaceStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.83
Alarm Title	-
Alarm Source	-
Alarm Type	communicationsAlarm

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

## NQM Connectivity Alarm

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

## NQM RTT Alarm

Alarm Fields	Description
Description	This alarm is raised when high RTT towards the NQM probe destination is detected.

Alarm Fields	Description		
SNMP Alarm	acNqmRttAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.89		
Alarm Source	Board#%d/NqmSender#%d		
AlarmType	communicationsSubsystemFailure		
Probable Cause	Raised when Detected high RTT towards NQM probe destination		
Alarm Severity	Condition	Text	Corrective Action
Minor	-	Detected high RTT towards NQM probe destination	<p>To correct long RTT (Round Trip Time):</p> <ul style="list-style-type: none"> <li>■ Test with traceroute.</li> <li>■ Contact your ISP with the traceroute results.</li> <li>■ Use Wireshark or any other diagnostic tool to perform a traffic capture and determine who is contaminating the network.</li> </ul>

## NQM Jitter Alarm

Alarm Field	Description		
Description	This alarm is raised when high Jitter towards the NQM probe destination is detected.		
SNMP Alarm	acNqmJitterAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.90		
Alarm Title	NQM Jitter Alarm		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Jitter towards NQM probe destination - thresholdCrossed		
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Minor	-	Detected high Jitter towards NQM probe destination	<p>To correct high jitter:</p> <ul style="list-style-type: none"> <li>■ Test with traceroute.</li> <li>■ Contact your Internet Service Provider (ISP) with traceroute results.</li> <li>■ Implement Quality of Service (QoS).</li> <li>■ Note that there's no simple solution for high jitter. A systemic level solution may be required.</li> </ul>

## NQM Packet Loss Alarm

Alarm Field	Description		
Description	This alarm is raised when high packet loss towards the NQM probe destination is detected.		
SNMP Alarm	acNqmPacketLossAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.91		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Packet Loss towards NQM probe destination		
Alarm Severity	Condition	Text	Corrective Action
Minor	-	Detected high PL towards NQM probe destination	<p>To correct high packet loss (PL):</p> <ul style="list-style-type: none"> <li>■ Eliminate interference problems: Distance your modem from electrical devices</li> <li>■ Do not coil up any excess signal or power cables.</li> </ul>

Alarm Field	Description		
			<ul style="list-style-type: none"> <li>■ Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring.</li> </ul>

## NQM MOS CQ Alarm

Alarm Field	Description		
Description	This alarm is raised when low conversational voice quality towards the NQM probe destination is detected.		
SNMP Alarm	acNqmCqMosAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.95		
Alarm Title	Detected low conversational voice quality towards NQM probe destination		
Alarm Source	Board#%d/NqmSender#%d		
Alarm Type	communicationsAlarm		
Probable Cause	Raised when Detected low conversational voice quality towards NQM probe destination		
Alarm Severity	Condition	Text	Corrective Action
Minor	-	Detected low conversational voice quality towards NQM probe destination	<p>To fix the Noise Quality Measure (NQM) result:</p> <ul style="list-style-type: none"> <li>■ Perform corrective action for jitter. See <a href="#">NQM Jitter Alarm</a> on page 198</li> <li>■ Perform corrective action for Real Time Protocol (RTP) packet loss.</li> <li>■ See <a href="#">NQM Packet Loss Alarm</a> on the previous page</li> <li>■ Perform corrective action for</li> </ul>

Alarm Field	Description		
			<p>long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination.</p> <ul style="list-style-type: none"> <li>■ See <a href="#">NQM RTT Alarm</a> on page 197</li> </ul> <p>To fix the poor Conversational Quality (CQ) that the test indicates:</p> <ul style="list-style-type: none"> <li>■ Try changing the coder</li> <li>■ Try using RTP-Redundancy</li> <li>■ Perform corrective action for RTP packet loss.</li> <li>■ See <a href="#">NQM Packet Loss Alarm</a> on page 199</li> </ul>

## NQM MOS LQ Alarm

Alarm Field	Description		
Description	This alarm is raised when low listening voice quality towards the NQM probe destination is detected.		
SNMP Alarm	acNqmLqMosAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.96		
Alarm Source	Board#%/NqmSender#%		
AlarmType	communicationsAlarm		
Probable Cause	Raised when detected low listening voice quality towards NQM probe destination		
Alarm Severity	Condition	Text	Corrective Action
Minor	-	Detected low listening voice quality towards NQM probe destination	<p>To fix the Noise Quality Measure (NQM) result:</p> <ul style="list-style-type: none"> <li>■ Perform corrective action for Real Time</li> </ul>

Alarm Field	Description		
			<p>Protocol (RTP) packet loss.</p> <ul style="list-style-type: none"> <li>■ See <a href="#">NQM Packet Loss Alarm</a> on page 199</li> </ul> <p>To fix the poor listening quality that the test indicates:</p> <ul style="list-style-type: none"> <li>■ Try changing the coder</li> <li>■ Try using RTP-Redundancy</li> <li>■ Perform corrective action for RTP packet loss.</li> <li>■ See <a href="#">NQM Packet Loss Alarm</a> on page 199</li> </ul>

## Mediant 3000 Hardware Alarms

This section describes the Mediant 3000 Hardware alarms.

### PEM Module Alarm

Alarm Field	Description
Description	<p>This alarm is sent in one of the following cases:</p> <ul style="list-style-type: none"> <li>■ The HA (High Availability) feature is active and one of the PEM (Power Entry Module) units is missing</li> <li>■ PEM card is in its location and both DC wires are in.</li> </ul>
SNMP Alarm	acPEMAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.31
Alarm Source	chassis#0/PemCard#<m>, where m is the power entry module's (PEM) slot number
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Critical	The HA (High Availability) feature is active and one of the PEMs (Power Entry Modules) is missing.	PEM Module Alarm. PEM card is missing.	<ul style="list-style-type: none"> <li>Make sure the PEMs are present and that they're inserted correctly.</li> <li>If it's present and inserted correctly yet the alarm remains active, send a Return Merchandise Authorization (RMA) request to AudioCodes.</li> </ul>
Cleared	PEM card is placed and both DC wires are in.		

## SA Module Missing Alarm

Alarm Field	Description		
Description	This alarm is sent when the Shelf Alarm (SA) module is missing or non operational.		
SNMP Alarm	acSAMissingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.32		
Alarm Title	SA Module Missing Alarm		
Alarm Source	Chassis#0/SA#<m>, where m is the shelf Alarm module's slot number		
Alarm Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	Condition	<Text>	Corrective Action
Critical (default)	SA module removed or missing	SA Module Alarm. SA-Module from slot #n is missing.	<ul style="list-style-type: none"> <li>Reinsert the Shelf Alarm (SA) module into slot #n</li> <li>Make sure it's correctly inserted</li> </ul>

Alarm Field	Description		
			in the slot.
Cleared	SA module is in slot 2 or 4 and working.	-	-

## User Input Alarm

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

## TM Inconsistency

Alarm Field	Description
Description	Timing Manager Alarm. This alarm is triggered when the system is in a 1+1 status and the redundant board PLL status is different to the active board PLL status.
SNMP Alarm	acTMInconsistentRemoteAndLocalPLLStatus

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.56
Alarm Title	TM Inconsistency
Alarm Source	-
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Severity	Major, Clear
Additional Info	Status stays major until reboot. A clear trap is not sent.
Corrective Action	Synchronize the timing module.

### TM Reference Status

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

Alarm Field	Description
Action	

## TM Reference Change

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

## PSTN Trunk Alarms

This section describes the PSTN Trunk alarms.

## D-Channel Status

**Table 6-5: D-Channel Status**

Alarm Field	Description
Description	<p>Non-alarm trap sent at the establishment, re-establishment or release of LAPD link with its peer connection occurs. The trap is sent with one of the following textual descriptions:</p> <ul style="list-style-type: none"> <li>■ D-channel synchronized</li> <li>■ D-channel not-synchronized</li> </ul>

Alarm Field	Description
SNMP Alarm	acDChannelStatus
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
Alarm Title	D-Channel Status
Alarm Source	Trunk no.<m> where m is the trunk number (from 0 up).
Alarm Type	Communications Alarm
Probable Cause	Communications Protocol Error
Severity	Minor on raise, Clear on clear
Additional Info	-
Corrective Action	-

### SONET Section LOF Alarm

Alarm Field	Description		
Description	This alarm indicates that a LOF condition is present on SONET no#m. The field 'sonetSectionCurrentStatus' in the sonetSectionCurrentTable will have a value of sonetSectionLOF (4).		
SNMP Alarm	acSonetSectionLOFAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.38		
Alarm Source	Interfaces#0/Sonet#<m>, where m is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Alarm Severity	Condition	Text	Corrective Action
Critical	LOF condition is present on SONET no.n	SONET-Section LOF	Make sure the framing format on the port matches the format configured on the line.  Note that the

Alarm Field	Description		
			'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value sonetSectionLOF(4)
Cleared	LOF condition is not present	LOF	-

## SONET Section LOS Alarm

Alarm Field	Description		
Description	This alarm indicates that LOS or AIS condition is present on SONET no #m. The field 'sonetSectionCurrentStatus' in the sonetSectionCurrentTable will have a value of sonetSectionLOS (2).		
SNMP Alarm	acSonetSectionLOSAAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.39		
Alarm Source	Interfaces#0/Sonet#<m>, where m is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	LOS condition is present on SONET no #n	SONET-Section LOS	<ul style="list-style-type: none"> <li>■ Make sure the fiber optic cable is plugged in correctly.</li> <li>■ Make sure it's not damaged.</li> <li>■ Make sure its remote end is correctly connected and undamaged.</li> <li>■ Make sure that configuration of the remote port is correct.</li> </ul> <p>Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value sonetSectionLOS (2)</p>

Alarm Field	Description		
Cleared	LOS condition is not present	-	-

## SONET Line AIS Alarm

Alarm Field	Description		
Description	This alarm indicates that an AIS condition is present on SONET-Line #m. The field 'sonetLineCurrentStatus' in the sonetLineCurrentTable will have a value of sonetLineAIS (2).		
SNMP Alarm	acSonetLineAISAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.40		
Alarm Source	Interfaces#0/Sonet#<m>, where m is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	AIS condition is present on SONET-Line #n	SONET-Line AIS	<p>If an Alarm Indication Signal (AIS) condition is present on a SONET line: Make sure the remote configuration is correct.</p> <ul style="list-style-type: none"> <li>■ Check the line status at the remote end of the link.</li> </ul> <p>Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value sonetLineAIS (2)</p>
Cleared	AIS condition is not present.	-	-

## SONET Line RDI Alarm

Alarm Field	Description		
Description	This alarm indicates that RDI condition is present on SONET-Line no#m. The field 'sonetLineCurrentStatus' in the sonetLineCurrentTable will have a value of sonetLineRDI (4).		
SNMP Alarm	acSonetLineRDIAAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.41		
Alarm Source	Interfaces#0/Sonet#<m>, where m is the SONET interface number		
Alarm Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	RDI condition is present on SONET-Line #n	SONET-Line RDI	<ul style="list-style-type: none"> <li>■ Check the remote site for alarm conditions.</li> <li>■ Correct a line problem that has arisen from the remote interface.</li> </ul> <p>Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value sonetLineRDI (4)</p>
Cleared	RDI condition is not present.	-	-

## SONET/SDN IF Failure Alarm

Alarm Field	Description
Description	This alarm indicates a Hardware failure on SONET-Line no#m
SNMP Alarm	acSonetIfHwFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.42
Alarm Title	SONET/SDH IF Failure Alarm

Alarm Field	Description
Alarm Source	Interfaces#0/Sonet#<m> where m is the SONET I/F number
Alarm Type	Communications Alarm
Probable Cause	Transmit failure
Severity	Critical on raise, Clear on clear
Additional Info	-
Corrective Action	-

## Trunk LOS Alarm

This alarm applies to E1/T1Trunks.

Alarm Field	Description		
Description	This alarm indicates a loss of signal at the trunk's near end.		
SNMP Alarm	acTrunksAlarmNearEndLOS		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.49		
Alarm Title	Trunk LOS Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	Near-end LOS	Trunk LOS Alarm	<p>Los of Signal (LOS) indicates a physical problem.</p> <ul style="list-style-type: none"> <li>■ Check that the cable is connected on the board.</li> <li>■ Check that the correct cable type is being used (crossed/straight).</li> <li>■ Contact AudioCodes' Support Center at</li> </ul>

Alarm Field	Description		
			<a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a> .
Cleared	End of LOS	-	-

## Trunk LOF Alarm

This alarm applies to E1/T1Trunks.

**Table 6-6: Trunk LOF Alarm**

Alarm Field	Description		
Description	This alarm indicates a loss of frame at the trunk's near end.		
SNMP Alarm	acTrunksAlarmNearEndLOF		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.50		
Alarm Title	Trunk LOF Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Alarm Severity	Condition	Text	Corrective Action
Critical (default)	Near end LOF	Trunk LOF Alarm	<p>Make sure that the trunk is connected to a proper follow-up device.</p> <p>Make sure that both sides are configured with the same (E1 / T1) link type.</p> <p>Make sure that both sides are configured with the same framing method.</p> <p>Make sure that both sides are configured with the same line code.</p> <ul style="list-style-type: none"> <li>■ Make sure that the clocking setup is correct.</li> <li>■ Contact AudioCodes' Support Center at <a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a>.</li> </ul>

Alarm Field	Description		
Cleared	End of LOF	-	-

## Trunk AIS Alarm

This alarm applies to E1/T1Trunks.

Alarm Field	Description		
Description	This alarm indicates that an AIS is received from the trunk's far end.		
SNMP Alarm	acTrunksAlarmRcvAIS		
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.51		
Alarm Title	Trunk AIS Alarm		
Alarm Source	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Type	communicationsAlarm		
Probable Cause	PSTN provider has stopped the trunk (receiveFailure)		
Alarm Severity	Condition	Text	Corrective Action
Critical	Receive AIS	Trunk AIS Alarm	<ul style="list-style-type: none"> <li>■ Contact your PSTN provider to activate the trunk.</li> <li>■ If the alarm persists, contact the AudioCodes Support Center at <a href="mailto:support@AudioCodes.com">support@AudioCodes.com</a></li> </ul>
Cleared	End of AIS	-	-

## Trunk RAI Alarm

Alarm Field	Description
Description	This alarm indicates a loss of frame at the trunk's far end.
SNMP Alarm	acTrunksAlarmFarEndLOF
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.52

Alarm Field	Description
Alarm Title	Trunk RAI Alarm
Alarm Source	Port#<n> where n is the digital trunk number
Alarm Type	communicationsAlarm
Probable Cause	transmitFailure
Severity	Critical
Additional Info	-
Corrective Action	Check trunk's connectivity

## V5.2 Interface Alarm

**Table 6-7: V5.2 Interface Alarm**

Alarm Field	Description
Description	<p>A V5.2 Interface alarm is raised in one of the following cases. For detailed V5.2 Interface condition, refer to the V5.2 Interfaces status table. An Alarm is raised with critical severity when:</p> <ul style="list-style-type: none"> <li>■ V5 interfaces ID are not equal on both sides</li> <li>■ V5 variants are not equal on both sides</li> <li>■ V5 link ID check timeout error occurred</li> <li>■ Layer 2 startup failed</li> <li>■ V5 restart failed</li> </ul> <p>An Alarm is raised with major severity when:</p> <ul style="list-style-type: none"> <li>■ Control protocol data link error</li> <li>■ Link control protocol data link error</li> <li>■ BCC protocol data link error</li> <li>■ PSTN protocol data link error</li> <li>■ Protection DL1 failure</li> <li>■ Protection DL2 failure</li> </ul>
SNMP Alarm	acV52InterfaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.60

Alarm Field	Description
Alarm Title	V5.2 Interface Alarm.
Alarm Source	V5.2IF#
Alarm Type	Communications Alarm
Probable Cause	Communications Protocol Error
Severity	Critical, Major, Clear
Additional Info	-
Corrective Action	<p>For critical severity alarms, solve configuration mismatch (configuration does not comply to far end configuration).</p> <p>For major severity alarms:</p> <ul style="list-style-type: none"> <li>■ Ensure physical connections are in place.</li> <li>■ Ensure links are not administratively blocked.</li> <li>■ Resolve configuration issues.</li> </ul>

### SONET Path STS LOP Alarm

Alarm Field	Description
Description	This alarm is issued when the LOP condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTSLOPAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.61
Alarm Title	SONET Path STS LOP Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-

Alarm Field	Description
Corrective Action	Correct the SONET mapping on either side ( the Gateway and the far end).

### SONET Path STS AIS Alarm

Alarm Field	Description
Description	This alarm is issued when the AIS condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTS AISAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.62
Alarm Title	SONET Path STS AIS Alarm
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure
Severity	Critical / clear
Additional Info	-
Corrective Action	<p>Check the following and correct according to the appropriate reason:</p> <p>There is higher level failure: LOS, LOF, AIS-L</p> <p>A Path Trace Identifier mismatch occurred</p> <ul style="list-style-type: none"> <li>■ Path is unequipped on the Far-End</li> </ul>

### SONET Path STS RDI Alarm

Alarm Field	Description
Description	This alarm is issued when the RDI condition is present on the SONET Path #m.
SNMP Alarm	acSonetPathSTS RDIAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.63
Alarm Title	SONET Path STS RDI Alarm

Alarm Field	Description
Alarm Source	Interfaces#0/Path#<m>
Alarm Type	communicationsAlarm
Probable Cause	transmitFailure
Severity	Critical / Cleared
Additional Info	-
Corrective Action	This indication only reflects a failure detected on the far-end. Check the following and correct on the far-end according to the appropriate reason: LOS, LOF, AIS-L, AIS-P

### SONET Path Unequipped Alarm

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

## SONET Path Signal Label Alarm

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

## DS1 Line Status Alarm

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

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

## DS3 RAI Alarm

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

## DS3 AIS Alarm

Alarm Field	Description
Description	This alarm is issued when the AIS condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3AISAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.67
Alarm Title	DS3 AIS Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	receiveFailure

Alarm Field	Description
Severity	Critical / Cleared
Additional Info	-
Corrective Action	Check the following and correct according to the appropriate reason: There is a SONET level failure: LOS, LOF, AIS-L, AIS-P, UNEQ-P, TIM-P The far-end (e.g., MUX) sends a DS3 AIS

### DS3 LOF Alarm

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

### DS3 LOS Alarm

Alarm Field	Description
Description	This alarm is issued when the LOF condition is present on the DS3 Interface #m.
SNMP Alarm	acDS3LOSAAlarm
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.69

Alarm Field	Description
Alarm Title	DS3 LOS Alarm
Alarm Source	Interfaces#0/DS3#<m>
Alarm Type	communicationsAlarm
Probable Cause	lossOfFrame
Severity	Critical / Cleared
Additional Info	-
Corrective Action	Check the cable connections or cable length

## NFAS Group Alarm

Alarm Field		Description	
Description		This alarm is raised when an NFAS group goes Out-Of-Service and is cleared when an NFAS Group is back In-Service.	
SNMP Alarm		acNFASGroupAlarm	
SNMP OID		1.3.6.1.4.1.5003.9.10.1.21.2.0.84	
Alarm Source		Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk	
Alarm Type		communicationsAlarm	
Probable Cause		degradedSignal	
Alarm Severity	Condition	Text	Corrective Action
Major (default)	Raised when an NFAS group goes out-of-service	NFAS Group Alarm. %s	<div><div></div> 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.</div> <div><div></div> When at least one of the</div> <div><div></div> D-channels (primary or</div>

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

## B Channel Alarm

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

## Analog Port Alarms

This section describes the Analog port alarms.

## Analog Port SPI Out of Service

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

## Analog Port High Temperature

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

## Analog Port Ground Fault Out-of-Service Alarm

Alarm Field	Description
Description	This alarm indicates that there is a ground fault in the analog port.
SNMP Alarm	acAnalogPortGroundFaultOutOfService
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Alarm Title	Analog Port Ground Fault Out Of Service
Alarm Source	System#0/analogports#<n>, where n is the port number
Alarm Text	Analog Port Ground Fault Out Of Service
Alarm Type	physicalViolation
Probable Cause	equipmentMalfunction (this alarm is raised when the FXS port is inactive due to a ground fault)
Default Severity	Major / Clear
Corrective Action	<ul style="list-style-type: none"> <li>■ No corrective action is required.</li> <li>■ The device shuts down the port and tries to activate it again when the relevant alarm is over.</li> </ul>
Note	Relevant to FXS only.

## Dial Plan File Replaced Trap

Alarm Field	Description
Description	Indicates that the dial plan file has been replaced.
SNMP Alarm	acDialPlanFileReplaced
SNMP OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.45
Default Severity	Indeterminate
Alarm Type	Other (0)
Probable Cause	Other (0)
Status Change	

Alarm Field	Description
Condition	Successful dial plan file replacement
Trap Text	Dial plan file replacement complete.

### Analog Line Left Off Hook Alarm

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

### UMP-365 and CloudBond Microsoft Platform Alarms

This section describes the Microsoft platform alarms for the UMP-365 and CloudBond products.

#### Commit License Failed

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

Alarm Field	Description		
SNMP Alarm	acCbManLicenseCommitAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.1		
Alarm Title	Commit License Failed		
Alarm Source	N/A		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Major	Unable to store the license in the Active Directory	Unable to commit the license in Active Directory.	Verify that OVOC Agent can access the local Active Directory. Verify that the local Active Directory contains the contact 'CbLicense'.
Cleared	The license has been successfully stored in the Active Directory.	-	

## Component Unreachable

Alarm Field	Description
Description	This alarm is raised when the Ovoc Main Agent is unable to connect to one of the client agents in the environment.
SNMP Alarm	acCbManEnvUnreachableAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.2
Alarm Source	<n> (where n is the component IP and port or unique name )
Alarm Title	Component Unreachable

Alarm Field	Description		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Client agent is unavailable	Unable to connect to the client agent on <component name>.	
Cleared	Client agent is available again.		

## Component Restart

Alarm Field	Description		
Description	This alarm is raised when a CloudBond or UMP-365 component has restarted.		
SNMP Alarm	acCbManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.3		
Alarm Title	Event – Component Restart		
Alarm Source	<n> (where n is the component name)		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	Text	Corrective Action
Major	Indeterminate	CCE Appliance component <component name> restarted	-
Cleared	-	-	

## Performance Counter General

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

## Performance Counter Service

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

## Component Service Status

Alarm Field	Description		
Description	This alarm is raised when a CloudBond or UMP-365 component service is down.		
SNMP Alarm	acCbCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.13		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service’s importance to system functionality.			

## Component Event Viewer

Alarm Field	Description
Description	This alarm is raised when report is generated in the Event Viewer for a CloudBond or UMP-365 component error.

Alarm Field	Description		
SNMP Alarm	acCbCompEventViewer		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.14		
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))		
Alarm Title	Component Event Viewer		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type "Info".		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate		The text of the event	

### Component Event Viewer Past Hours

Alarm Field	Description		
Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.		
SNMP Alarm	acCbCompEventLogAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.15		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action

Alarm Field	Description		
Critical	Event Log has a Critical alarm.	The event log has errors	<b>a.</b>
Major	Event Log has a Major alarm.	The event log has errors	<b>a.</b>
Warning	Event Log has a Warning alarm.	The event log has errors	<b>a.</b>
Cleared	No errors have occurred in the past hours.		

### Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the OVOC after the sending rate threshold has been exceeded.
SNMP Alarm	acCbCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.16
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Additional Info	
Alarm Severity	Indeterminate

### Alarm-Admin License Expired

Alarm Field	Description
Description	This alarm is raised when the product license is invalid or has expired.

Alarm Field	Description		
SNMP Alarm	acCbAdminLicInvalidAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.21		
Alarm Title	Product License Expired		
Alarm Source	N/a		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> <li>License will expired in &lt;number of days left&gt;</li> <li>Days.</li> </ul>	<ul style="list-style-type: none"> <li>Check the license server of update new license.</li> </ul>
Cleared	License is valid		

## Certificate Expired Alarm

Alarm Field	Description
Description	This alarm is raised when a certificate of a Cloudbond or UMP-365 component is about to expire.
SNMP Alarm	acCceAdminCertificateExpiredAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.32
Alarm Title	Certificate Expired Alarm
Alarm Source	N/A
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
Additional Info	-		
Alarm Severity	Condition	Text	Corrective Action
Critical	Pre-defined severity per threshold	Certificate will expires in <days left> days	Open certificate manager. Find the expired certificate and renew it.
Major	Pre-defined severity per threshold	Certificate will expires in <days left> days	Open certificate manager. Find the expired certificate and renew it.
Warning	Pre-defined severity per threshold	Certificate will expires in <daysleft> days	Open certificate manager. Find the expired certificate and renew it.
Cleared	When certificate renewed	-	-

## Alarm-Disk Space

Alarm Field	Description
Description	This alarm is raised when the host machine disk space is above the pre-defined threshold.
SNMP Alarm	acCceDiskSpaceAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.36
Alarm Title	Disk Space Alarm
Alarm Source	Host/C:\
Alarm Type	Other
Probable Cause	Other
Additional Info	-

Alarm Field	Description		
Alarm Severity	Condition	Text	CorrectiveAction
Major	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	<ul style="list-style-type: none"> <li>Free temporary files and other unnecessary files from the CCE appliance Host disk.</li> <li>Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs.</li> </ul>
Clear	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	<ul style="list-style-type: none"> <li>Free temporary files and other unnecessary files from the CCE appliance Host disk.</li> <li>Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs.</li> </ul>

## Fax Server

This section describes the Fax Server alarms.

## System Alarms

This section describes the Fax server System alarms.

### Component Unreachable

Alarm Field	Description
Description	This alarm is raised when the Ovoc Main Agent is unable to connect to one of the client agents in the environment.
SNMP Alarm	acGaManEnvUnreachableAlarm
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.1
Alarm Source	<n> (where n is the component IP and port or unique name )
Alarm Title	Component Unreachable

Alarm Field	Description		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Client agent is unavailable	Unable to connect to the client agent on <component name>.	
Major	Fax Server is unavailable	Unable to connect to admin.	
Cleared	Client agent is available again.		

### Component Restart

Alarm Field	Description		
SNMP Alarm	acGaManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	component <component name> restarted		<b>a.</b>

### Component Resource Failed

Alarm Field	Description		
Description	This event sent when a resource allocation on a component fails.		
SNMP Alarm	acGaCompResFailedEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.9		
Alarm Source	<n><rn> (where n is the name of the component or ip:port and rn is the resource name)		
Alarm Title	Component Resource Error		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Minor	Fax channel reached timeout.	Fax server channel reached timeout	

### Component Resource Down

Alarm Field	Description		
Description	This alarm is raised when a resource is down and can't be used.		
SNMP Alarm	acGaCompResDownAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.10		
Alarm Source	FaxCall		
Alarm Title			
Alarm Type	Other		
Probable Cause	Other		

Alarm Field	Description		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	Failed to execute a test call.	Fax call failure	Check Commetrex fax service
Cleared	Test call succeed.		

## Agent Alarms

This section describes the Fax server Agent alarms.

### Component Performance Counter General

Alarm Field	Description		
Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory/CPU/disk.		
SNMP Alarm	acGaCompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.21		
Alarm Source	<n>\<g>\<p> (where n is the component name or ip:port, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	<b>a.</b>

Alarm Field	Description		
Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	a.
Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	
Cleared	When counter returns below the threshold level.		

### Performance Counter Service

Alarm Field	Description		
Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. Related to activity of windows services usually taken from KHI.		
SNMP Alarm	acGaCompPcServAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.22		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause			
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per each counter type	<Performance counter> high level <x>	a.
Major	Pre-defined severity	<Performance	a.

Alarm Field	Description		
	per each counter type	counter> high level <x>	
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	a.
Cleared	When counter returns below the threshold level.		

### Component Service Status

Alarm Field	Description		
Description	This alarm is raised when a component service is down.		
SNMP Alarm	acGaCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.23		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name) <ul style="list-style-type: none"> <li>• BladeWare</li> <li>• FaxAlarmsManager</li> <li>• F2M</li> <li>• F2MW</li> <li>• Fax_Receiver</li> <li>• M2FHM</li> <li>• Apache2.4</li> </ul>		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	a.

Alarm Field	Description		
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	a.
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service’s importance to system functionality.			

### Component Event Viewer

Alarm Field	Description		
Description	This event sent when report is generated in the Event Viewer for a component error.		
SNMP Alarm	acGaCompEventViewer		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.24		
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))		
Alarm Title	Component Event Viewer		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type "Info".		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate		The text of the event	

### Component Event Viewer Past Hours

Alarm Field	Description		
Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.		
SNMP Alarm	acGaCompEventLogAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.25		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Event Log has a Critical alarm.	The event log has errors	<b>a.</b>
Major	Event Log has a Major alarm.	The event log has errors	<b>a.</b>
Warning	Event Log has a Warning alarm.	The event log has errors	<b>a.</b>
Cleared	No errors have occurred in the past hours.		

### Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the OVOC after the sending rate threshold has been exceeded.
SNMP Alarm	acGaCompEventViewerDropped

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.26
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Additional Info	
Alarm Severity	Indeterminate

### Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when the certificate in the component is about to expire.		
SNMP Alarm	acGaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.27		
Alarm Source	<n> (where n is the component name)		
Alarm Text	Certificate will expires in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Cleared	When certificate is renewed		

## Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on the component is above pre-defined threshold.		
SNMP Alarm	acGaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.28		
Alarm Source	<n>/<e> (where n is the component name and e is drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.		

## License Alarms

This section describes the Fax server License alarms.

### Admin License Expired

Alarm Field	Description
Description	This alarm is raised when the product license is invalid/ expired.
SNMP Alarm	acGaManLicInvalidAlarm
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.42
Alarm Source	N/a
Alarm Title	Product License Expired
Alarm Type	Other

Alarm Field	Description		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> <li>■ License will expired in &lt;number of days left&gt;</li> <li>■ Days.</li> </ul>	<ul style="list-style-type: none"> <li>a. Check the license server of update new license.</li> </ul>
Cleared	License is valid		

### Admin License Violation

Alarm Field	Description		
Description	This event sent when the administrator attempts to define users/resources exceeding the maximum capacity set by license.		
SNMP Alarm	acGaManLicViolationEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.43		
Alarm Source	N/A		
Alarm Title	Admin License Violation		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Minor		
Alarm Severity	Condition	<text>	Corrective Action

Alarm Field	Description		
Minor	The number of users exceed the limitation in the license.	■ Exceed number of users limitation in license	■ Check the license server of update new license.

## IVR Alarms

This section describes the IVR alarms.


### System Alarms

This section describes the IVR System alarms.

#### IVR Alarm – Component Unreachable

Alarm Field	Description		
Description	his alarm is raised when the EMS Main Agent is unable to connect to one of the client agents in the environment.		
SNMP Alarm	acVAManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.1		
Alarm Source	<n> (where n is the component IP and port or unique name )		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Client agent is unavailable	Unable to connect to the client agent on <component name>.	-
Major	IVR is unavailable	Unable to connect to admin.	-
Cleared	Client agent is available again.		

### IVR Component Restart

Alarm Field	Description		
Description	This alarm is raised when a client agent on component has restarted.		
SNMP Alarm	acVAManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	component <component name> restarted		

### IVR Component Resource Down

Alarm Field	Description		
Description	This alarm is raised when a resource is down and can't be used.		
SNMP Alarm	acVaCompResDownAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.10		
Alarm Source	ApplicationEndPoint UserEndPoint		
Alarm Text	<r> can't start.		
Alarm Type	Other		
Probable Cause	Other		

Alarm Field	Description		
Alarm Severity	Condition	<text>	Corrective Action
Major	Application endpoint is down	Application End Point can't start	Check frontend
Cleared	Application Endpoint is up		
Major	One or more of the User endpoint are down	User End Point can't start	Check frontend
Cleared	All User Endpoints are up		

## Agent Alarms

This section describes the IVR Agent alarms.


### IVR Component Performance Counter General

Alarm Field	Description		
Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory/CPU/disk.		
SNMP Alarm	acVACompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.21		
Alarm Source	<n>\<g>\<p> (where n is the component name or ip:port, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	<Performance counter> high level	■


Alarm Field	Description		
		<x>.	
Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	■
Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	■
Cleared	When counter returns below the threshold level.		


### IVR Component Performance Counter Service

Alarm Field	Description		
Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. Related to activity of windows services usually taken from KHI.		
SNMP Alarm	acVaCompPcServAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.22		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause			
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per each counter type	<Performance counter> high level	■

Alarm Field	Description		
		<x>	
Major	Pre-defined severity per each counter type	<Performance counter> high level <x>	
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	
Cleared	When counter returns below the threshold level.		

### IVR Component Service Status

Alarm Field	Description		
Description	This alarm is raised when a component service is down.		
SNMP Alarm	acVaCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.23		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	

Alarm Field	Description		
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

### IVR Component Event Viewer

Alarm Field	Description		
Description	This event sent when report is generated in the Event Viewer for a component error.		
SNMP Alarm	acVaCompEventViewer		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.24		
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))		
Alarm Title	Component Event Viewer		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type "Info".		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate		The text of the event	

### IVR Component Event Viewer Past Hours

Alarm Field	Description
Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.
SNMP Alarm	acVaCompEventLogAlarm

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.25		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Event Log has a Critical alarm.	The event log has errors	
Major	Event Log has a Major alarm.	The event log has errors	
Warning	Event Log has a Warning alarm.	The event log has errors	
Cleared	No errors have occurred in the past hours.		

#### IVR– Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the EMS after the sending rate threshold has been exceeded.
SNMP Alarm	acVaCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.26
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other

Alarm Field	Description
Probable Cause	Other
Additional Info	
Alarm Severity	Indeterminate

### IVR Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when the certificate in the component is about to expire.		
SNMP Alarm	acVaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.27		
Alarm Source	<n> (where n is the component name)		
Alarm Text	Certificate will expires in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Cleared	When certificate is renewed		

### IVR Disk Space

Alarm Field	Description
Description	This alarm is raised when the server disk space on the component is above pre-defined threshold.

Alarm Field	Description		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.28		
Alarm Source	<n>/<e> (where n is the component name and e is drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.		

## License Alarms

This section describes the IVR License alarms.

### IVR Admin License Expired

Alarm Field	Description
Description	This alarm is raised when the product license is invalid/ expired.
SNMP Alarm	acVaManLicInvalidAlarm
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.42
Alarm Source	N/a
Alarm Title	Product License Expired
Alarm Type	Other
Probable Cause	Other
Additional	

Alarm Field	Description		
Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> <li>License will expired in &lt;number of days left&gt;</li> <li>Days.</li> </ul>	<ul style="list-style-type: none"> <li>Check the license server of update new license.</li> </ul>
Cleared	License is valid		

### IVR Admin License Violation

Alarm Field	Description		
Description	This event sent when the administrator attempts to define users/resources exceeding the maximum capacity set by license.		
SNMP Alarm	acVaManLicViolationEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.43		
Alarm Source	N/A		
Alarm Title	Admin License Violation		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Minor		
Alarm Severity	Condition	<text>	Corrective Action
Major	The number of concurrent calls	<ul style="list-style-type: none"> <li>Call rejected due to</li> </ul>	<ul style="list-style-type: none"> <li>Update the license with increased number of</li> </ul>

Alarm Field	Description		
	exceeded the license.	license limitation	concurrent calls.

## Vocanom Alarms

This section describes the Vocanom alarms.

## System Alarms

This section describes the Voca System alarms.

### Voca Alarm – Component Unreachable

Alarm Field	Description		
Description	This alarm is raised when the EMS Main Agent is unable to connect to one of the client agents in the environment.		
SNMP Alarm	acVAManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.1		
Alarm Source	<n> (where n is the component IP and port or unique name)		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Client agent is unavailable.	Unable to connect to the client agent on <component name>.	
Major	Voca Alarms agent is unavailable.	Unable to connect to admin.	
Cleared	Client agent is		

Alarm Field	Description		
	available again.		

### Voca Component Restart

Alarm Field	Description		
Description	This alarm is raised when a client agent on component has been restarted.		
SNMP Alarm	acVAManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable	Other		
Cause			
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	component <component name> restarted		

### Agent Alarms

This section describes the IVR Agent alarms.

### Voca Component Performance Counter General

Alarm Field	Description
Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory/CPU/disk.

Alarm Field	Description		
SNMP Alarm	acVACompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.21		
Alarm Source	<n>\<g>\<p> (where n is the component name or ip:port, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre- defined severity per counter type.	<Performance counter> high level <x>.	
Major	Pre- defined severity per counter type.	<Performance counter> high level <x>.	
Warning	Pre- defined severity per counter type.	<Performance counter> high level <x>.	
Cleared	When counter returns below the threshold level.		

### Voca Component Service Status

Alarm Field	Description
Description	This alarm is raised when a component service is down.

Alarm Field	Description		
SNMP Alarm	acVaCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.23		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service down	is SERVICE_STOPPED(indicates which service is down).	
Major	Service down	is SERVICE_STOPPED(indicates which service is down).	
Warning	Service down	is SERVICE_STOPPED(indicates which service is down).	
Cleared	Service running	SERVICE_RUNNING	
Note: the severity is determined according to the service’s importance to system functionality.			

### Voca Certificate Expired

Alarm Field	Description
Description	This alarm is raised when the component certificate is about to expire.
SNMP Alarm	acVaCompCertificateExpiredAlarm

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.27		
Alarm Source	<n> (where n is the component name)		
Alarm Text	Certificate will expire in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity per threshold.	Certificate will expires in <days left> days	Verify which certificate is about to expire and renew it.
Cleared	When certificate is renewed.		

### Voca Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on the component is above the pre-defined threshold.		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.28		
Alarm Source	<n>/<e> (where n is the component name and e is drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of	Disk space usage is	Free temporary files and other unnecessary

Alarm Field	Description		
	used disk space.	over {0}%	file from the disk.
Cleared	Used disk space is below threshold.		

## Voca Agent Specific Alarms

This section describes the Voca-specific alarms.

### Alarm –Wrong Operating Component

Alarm Field	Description		
Description	This alarm is raised when the service specified in the source is in an incorrect mode.		
SNMP Alarm	acVaWrongOperatingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.7		
Alarm Source	Based on alarm source: <ul style="list-style-type: none"> <li>■ ReplicationManager\SlaveDBStatus</li> <li>■ ReplicationManager\RemoteSlaveDBStatus</li> </ul>		
Alarm Title	Alarm –Wrong Operating Component		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	The slave db is not running based on specific DB parameters.	slave DB not running	
Cleared	Slave db is running without errors.	slave DB running	

Alarm Field	Description		
Major	Remote slave db is not running based on specific DB parameters.	Remote slave is not connected to the master.	
Cleared	Remote Slave db is running without errors.	Remote slave is now connected to the master.	

### Alarm –Wrong Settings

Alarm Field	Description		
Description	This alarm is raised when the parameter specified in the source has incorrect settings.		
SNMP Alarm	acVaWrongSettingsAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.8		
Alarm Source	Based on alarm source: <ul style="list-style-type: none"> <li>■ ClusterManager\NodesIds</li> <li>■ ClusterManager\NodesRoles</li> </ul>		
Alarm Text	TBD		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Incomplete or incorrect configuration.	Incomplete configuration - missing nodes.	
Critical	Incomplete or incorrect configuration.	Incomplete configuration - nodes ids do not match.	
Critical	Node role mismatch.	Incomplete configuration - nodes roles do not match.	

Alarm Field	Description		
Cleared	Mismatch resolved.	Incomplete configuration - mismatch resolved.	

### Alarm – Connection Failure

Alarm Field	Description		
Description	This alarm is raised when the connection between system components is down.		
SNMP Alarm	acVaConnectionFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.12		
Alarm Source	Based on alarm source: <ul style="list-style-type: none"> <li>■ ClusterManager\HeartBeats</li> <li>■ ReplicationManager\DBConnection</li> </ul>		
Alarm Title	Alarm – Connection Failure		
Alarm Type	Alarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Missed heartbeats (allowed missed heartbeats).	Missing heartbeats	
Critical	The system component has been in failure mode for more than one day.	In failure mode for {0} days	
Critical	Grace time has been exceeded.	Missing heartbeats - Grace ended	
Cleared	Incoming consecutive Heartbeats (recovery threshold)	Recovery detected - Entering normal mode	

Alarm Field	Description		
Major	Cannot connect to replication DB.	Failed to connect to DB.	
Cleared	Connection to DB has been restored.	Connection to replication DB restored	

## Microsoft Teams Direct Routing SBA Alarms


This section describes the Microsoft Teams Direct Routing SBA alarms.

### System Alarms


This section describes the Teams SBA system alarms.

#### SBA Alarm – Component Unreachable

Alarm Field	Description		
Description	This alarm is raised when the EMS Main Agent is unable to connect to one of the client agents in the environment.		
SNMP Alarm	acGaManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.1		
Alarm Source	<n> (where n is the component IP and port or unique name )		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Client agent is unavailable	Unable to connect to the client agent on <component name>.	■

Alarm Field	Description		
Major	IVR is unavailable	Unable to connect to admin.	
Cleared	Client agent is available again.		

### Component Restart

Alarm Field	Description		
Description	This alarm is raised when a client agent on component has restarted.		
SNMP Alarm	acGaManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	component <component name> restarted		

### System Action Failed

Alarm Field	Description		
Description	The voice application fails to execute a system action.		
SNMP Alarm	acGaSysActionFailedEvent		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.4		

Alarm Field	Description		
Alarm Source	TeamsSba		
Alarm Title	System Action Failed		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	Error executing an action in Microsoft Teams SBA service	Failed to execute settings in Microsoft Teams SBA service due to {0}	■

### Alarm – System Cloud Status

Alarm Field	Description		
Description	This alarm is raised when there is a problem Office365 cloud.		
SNMP Alarm	acGaSystemCloudStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.6		
Alarm Source	Teams SBA Status		
Alarm Title	System Cloud Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	Status is not OK	Teams SBA service status is {0}.	■

### Alarm – Wrong Operating

Alarm Field	Description		
Description	The service that specified in the source's varbind is operated in a wrong mode.		
SNMP Alarm	acGaWrongOperatingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.7		
Alarm Source	• Teams SBA State		
Alarm Title	Wrong Operating		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	State is not Ready	Teams SBA service state is {0}.	■

### Alarm – Component Resource Down

Alarm Field	Description		
Description	This alarm is raised when a resource is down and can't be used.		
SNMP Alarm	acGaCompResDownAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.10		
Alarm Source	Teams SBA		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action

Alarm Field	Description		
Major	Failed to connect to Microsoft Teams SBA Service	Can't connect to Microsoft Teams SBA service	Check Microsoft Teams SBA service
Cleared	Microsoft Teams SBA service is available.		

## Agent Alarms

This section describes the Teams SBA Agent alarms.


### Alarm – Component Performance Counter General

Alarm Field	Description		
Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory/CPU/disk.		
SNMP Alarm	acGaCompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.21		
Alarm Source	<n>\<g>\<p> (where n is the component name or ip:port, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	
Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	

Alarm Field	Description		
Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	
Cleared	When counter returns below the threshold level.		

### Alarm – Component Performance Counter Service

Alarm Field	Description		
Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. Related to activity of windows services usually taken from KHI.		
SNMP Alarm	acGaCompPcServAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.22		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause			
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per each counter type	<Performance counter> high level <x>	■
Major	Pre-defined severity per each counter type	<Performance counter> high level <x>	■

Alarm Field	Description		
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	
Cleared	When counter returns below the threshold level.		

### Alarm – Component Service Status

Alarm Field	Description		
Description	This alarm is raised when a component service is down.		
SNMP Alarm	acGaCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.23		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name) <ul style="list-style-type: none"> <li>TeamsSBA</li> <li>TeamsSbaConfig</li> </ul>		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	

Alarm Field	Description		
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

### Event – Component Event Viewer

Alarm Field	Description		
Description	This event sent when report is generated in the Event Viewer for a component error.		
SNMP Alarm	acGaCompEventViewer		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.24		
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))		
Alarm Title	Component Event Viewer		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type "Info".		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate		The text of the event	

### Alarm – Component Event Viewer Past Hours

Alarm Field	Description		
Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.		
SNMP Alarm	acGaCompEventLogAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.25		
Alarm Source	<n> (where n is the component name)		

Alarm Field	Description		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Event Log has a Critical alarm.	The event log has errors	■
Major	Event Log has a Major alarm.	The event log has errors	■
Warning	Event Log has a Warning alarm.	The event log has errors	■
Cleared	No errors have occurred in the past hours.		

### Alarm – Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the EMS after the sending rate threshold has been exceeded.
SNMP Alarm	acGaCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.26
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Additional	

Alarm Field	Description
Info	
Alarm Severity	Indeterminate

### Alarm – Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when the certificate in the component is about to expire. Only the certificates that used by Teams SBA are monitored:  ■ Self signed certificate for mTls  ■ Signed certificate that upload by admin with tenant name.		
SNMP Alarm	acGaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.27		
Alarm Source	<n> (where n is the component name)		
Alarm Text	Certificate will expires in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Cleared	When certificate is renewed		

### Alarm – Disk Space

Alarm Field	Description
Description	This alarm is raised when the server disk space on the component is above pre-defined

Alarm Field	Description		
	threshold.		
SNMP Alarm	acGaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.28		
Alarm Source	<n>/<e> (where n is the component name and e is drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.		

## License Alarms

This section describes the Teams SBA License alarms.

### Alarm – Admin License Expired

Alarm Field	Description
Description	This alarm is raised when the product license is invalid/ expired.
SNMP Alarm	acGaManLicInvalidAlarm
SNMP OID	1.3.6.1.4.1.5003.9.110.3.2.0.42
Alarm Source	N/a

Alarm Field	Description		
Alarm Title	Product License Expired		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> <li>License will expired in &lt;number of days left&gt;</li> <li>Days.</li> </ul>	<ul style="list-style-type: none"> <li>Check the license server of update new license.</li> </ul>
Cleared	License is valid		

## SBA Skype for Business Alarms

This section describes the SBA Skype for Business alarms.

### Alarm – CPU Status

Alarm Field	Description		
Description	CPU usage status alarm. Send alarm when CPU usage is above the threshold		
SNMP Alarm	acSBACpuStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.2		
Alarm Title	Alarm – CPU Status		
Alarm Source	Processor Information/%Processor Time/_Total		
Alarm Type	Other		
Probable Cause	Other		
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Critical	CPU > 90%	High CPU usage Above 90%	Using task manager check if the CPU load is constant or not, find the process that causes the high CPU usage and see if high CPU is reasonable (for example high CPU when performing windows updates, or running traces on the SBA), if there isn't a reason for the high CPU try to reset the SBA and if didn't solve the issue open a call to AudioCodes
Major	CPU > 80%	High CPU usage Above 80%	Using task manager check if the CPU load is constant or not, find the process that causes the high CPU usage and see if high CPU is reasonable (for example high CPU when performing windows updates, or running traces on the SBA), if there isn't a reason for the high CPU try to reset the SBA and if didn't solve the issue open a call to AudioCodes
Cleared	CPU < 76%	-	-

### SBA Memory Status

Alarm Field	Description		
Description	Memory used status alarm. Send an alarm when the level of available physical memory is below the threshold.		
SNMP Alarm	acSBAMemorytatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.3		
Alarm Title	Alarm – Memory Status		
Alarm Source	Memory/% Available MByte		
Alarm Type	Other		
Probable Cause	Other		
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Major	Available Memory < 7%	High memory usage, available memory is Below 7%	Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. if there isn't a reason for the high memory try to reset the SBA and if didn't solve the issue open a call to Audi-oCodes.
Critical	Available Memory < 4%	High memory usage, available memory is Bellow 4%	Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. If there isn't a reason for the high memory try to reset the SBA and if didn't solve the issue open a call to Audi-oCodes.
Cleared	Available Memory >8%		

### SBA Disk Space Alarm

Alarm Field	Description
Description	This alarm is raised if the disk (C) usage level exceeds configured thresholds. Thresholds can be configured in the snmp_sba.ini under C:\SBA (requires service restart for the changes to take effect).
SNMP Alarm	acSBADiskSpaceAlarm

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.4		
Alarm Title	Alarm – Disk Space		
Alarm Source	C:\		
Alarm Text	Disk space usage is over {0}% {0} – Threshold value		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	Disk 'C' usage level is over 90%	"Disk space usage is over 90%"	Remove unnecessary files from disk. Clean log files.
Critical	Disk 'C' usage level is between 80% and 90%	"Disk space usage is over 80%"	
Cleared	Disk 'C' usage level is below 76%	-	

### SBA Certificate Expired

Alarm Field	Description
Description	This alarm is raised when the certificate that is used to secure the connection between the SBA and the Datacenter is about to expire. The alarm is sent when the number of days to certificate expiration is below the threshold.
SNMP Alarm	acSbaCertificateExpiredAlarm
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.5
Alarm Title	Alarm – Certificate Expired
Alarm Type	Other
Alarm Source	-

Alarm Field	Description		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	Number of day to expiration < 30	Certificate will expire in 30 days.	Using windows mmc tool, check the expiration date of the certificates and find the expired certificate. Sign the expired certificate and install it on the machine.
Critical	Number of day to expiration < 2	Certificate will expire in 2 days.	Using windows mmc tool, check the expiration date of the certificates and find the expired certificate. Sign the expired certificate and install it on the machine.
Cleared	New valid certificate is installed.	-	-

### Alarm – Performance Counter

Alarm Field	Description		
Description	This alarm is raised when the configured performance counter's value is above/below the configured threshold.		
SNMP Alarm	acSbaPerfCounterAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.6		
Alarm Title	Alarm – Performance Counter		
Alarm Source	{Performance counter full path}		
Event Type	Other		
Probable Cause	Other		
Severity	Condition	<text>	Corrective Action
Major	Monitored value crossed	Performance counter	

Alarm Field	Description		
	the 'Major' threshold	{0} is Above/Below {1} {0} – Performance counter full path {1} – Threshold value	
Critical	Monitored value crossed the 'Critical' threshold	Performance counter {0} is Above/Below {1} {0} – Performance counter full path {1} – Threshold value	
Cleared	Monitored value falls below the 'Major' threshold		

### SBA Services Status Alarm

Alarm Field	Description		
Description	Services status alarm. The services are Front End server, Mediation server, Replica server, and Centralized Logging Service for Microsoft Lync 2013 (Centralized Logging is not available for Lync 2010).		
SNMP Alarm	acSBAServicesStatusAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.30.2.2.0.1		
Alarm Title	SBA Services Status Alarm		
Alarm Source	RtcSrv/ RTCMEDSRV/ REPLICA/ RTCCLSAGT		
Alarm Type	Other		
Probable Cause	Other		
Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED	Start the service and check why the service stopped, using the event viewer.
Major	Service is paused	SERVICE_PAUSED	Start the service and

Alarm Field	Description		
			check why the service paused, using the event viewer.
Cleared	Service is running	SERVICE_RUNNING	-
Indeterminate	Service in indeterminate state	SERVICE_CONTINUE_PENDING SERVICE_PAUSE_PENDING SERVICE_START_PENDING SERVICE_STOP_PENDING	Start the service and check why the service is in indeterminate state, using the event viewer.

## User Management Pack 365 (UMP) Alarms

This section describes the UMP 365 alarms.


### Wrong Operating Alarm

Alarm Field	Description		
Description	This alarm is raised when the UMP is unable to establish either a WebSocket or internal network adapter connection with OVOC.		
SNMP Alarm	acCceWrongOperatingAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.33		
Alarm Source	<div> <div></div> WebSocket         </div> <div> <div></div> TunDevice         </div>		
Alarm Title	Wrong Operating Alarm		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action


Alarm Field	Description		
Major	UMP is unable to establish a Web Socket connection with OVOC.	Unable to establish Web Socket connection to OVOC	
	The Web Socket connection with OVOC has been disconnected.	Web Socket disconnected from OVOC	
	Packets cannot be sent to OVOC over the Web Socket connection.	Web Socket failed to sent packets	
Clear	The Web Socket connection with OVOC has been successfully reestablished.	Web Socket connected to OVOC	
	Packets are successfully sent to OVOC over the Web Socket connection.	Web Socket sent successfully	
	The Web Socket connection with OVOC communicates successfully.	Web Socket read successfully	
Major	The internal network adapter for the WebSocket service.is unable to connect to OVOC.	Unable to connect to tun device	
	The internal network adapter for the Web Socket service cannot read incoming packets from OVOC.	Tun device read error	
	The tun device cannot send HTTPS packets to OVOC.	Tun device write error	
Clear	The internal network adapter for the Web Socket service is able to reconnect to OVOC.	Tun device connected successfully	
	The internal network adapter for the Web Socket service reads incoming HTTPS packets from OVOC correctly.	Tun device read successfully	
	The internal network adapter for the	Tun device	

Alarm Field	Description		
	Web Socket service correctly sends HTTPS packets to OVOC..	written successfully	

## UMP Tenant License Threshold Alarm

Alarm Field	Description		
Description	<p>This alarm is raised when the number of UMP tenant licenses that are active for a specific UMP virtual machine instance crosses the threshold.</p> <div>  <p>A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition.</p> </div>		
SNMP Alarm	acUmpTenantLicThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.41		
Alarm Title	UMP Tenant License Threshold Alarm		
Alarm Source	Virtual machine of UMP installation platform		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	#of users/# in active		
Alarm Severity	Condition	Text	Corrective Action
Critical	The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 95 %).	Tenant License threshold (Over 95 %)	
Major	The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 90 %).	Tenant License threshold (Over 90 %)	

## UMP User License Threshold Alarm

Alarm Field	Description		
Description	<p>This alarm is raised when the number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance crosses the licensed threshold.</p> <div>  <p>A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition.</p> </div>		
SNMP Alarm	acUmpUserLicThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.42		
Alarm Title	UMP User License Threshold Alarm		
Alarm Source	Virtual machine of UMP installation platform		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	#of users/# in active-		
Alarm Severity	Condition	Text	Corrective Action
Critical	The number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance, crosses the licensed threshold (above 95 %).	User License threshold (Over 95 %)	
Major	This alarm is raised when the number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance, crosses the threshold (above 90 %).	User License threshold (Over 90 %)	

## UMP Super Admin Authentication Fail Event (Service Provider)

Alarm Field	Description
Description	This alarm is raised when there is an authentication failure for the

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

### UMP End User License Threshold Alarm

Alarm Field	Description
Description	This alarm is raised when the number of users on the virtual machine crosses the threshold.
SNMP Alarm	acUmpEndUserLicThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.44
Alarm Title	UMP User License Threshold Alarm
Alarm Source	Virtual Machine/CustomerID
Alarm Type	Other
Probable Cause	Other
Additional	#of users/# in active

Alarm Field	Description		
Info			
Alarm Severity	Condition	Text	Corrective Action
Major	The number of users on the virtual machine has crossed the threshold (above 90%)	User License threshold (Over 90%)	

### UMP Azure AD Sync Alarm

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

### UMP Office 365 Failure Alarm

Alarm Field	Description		
Description	This alarm is raised when the UMP virtual machine loses the connection with the Office 365 platform i.e. Office 365 credentials failure.		

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

### UMP Office 365 Command Execution Event

Alarm Field	Description
Description	This alarm is raised when any PowerShell command run on the UMP platform fails.
SNMP Alarm	acUmpO365CommandExEvent
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.48
Alarm Title	Ump O365 Command Ex Event
Alarm Source	Virtual machine of UMP installation platform/CustomerID (Customer Name)
Alarm Type	Other
Probable Cause	Other
Additional	Execution Result

Alarm Field	Description		
Info			
Alarm Severity	Condition	Text	Corrective Action
Minor	This alarm is raised when any PowerShell command run on the UMP platform .		

### UMP User Settings Fail Event

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

### UMP End User Authentication Fail Event

Alarm Field	Description		
Description	This alarm is raised when there is an authentication failure for the UMP Admin End User .		

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

## CloudBond 365 Alarms

This section describes the CloudBond 365 alarms.

### Alarm-Admin License Expired

Alarm Field	Description
Description	This alarm is raised when the product license is invalid or has expired.
SNMP Alarm	acCbAdminLicInvalidAlarm
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.21
Alarm Title	Product License Expired
Alarm Source	N/a
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> <li>License will expired in &lt;number of days left&gt;</li> <li>Days.</li> </ul>	<ul style="list-style-type: none"> <li>Check the license server of update new license.</li> </ul>
Cleared	License is valid		

## 10SmartTAP Alarms

This section describes the SmartTAP alarms.

### SmartTAP System Alarms

This section describes SmartTAP Microsoft Windows Server System alarms.

#### Alarm – Component Unreachable

Alarm Field	Description		
Description	<p>This alarm is raised in the following circumstances:</p> <ul style="list-style-type: none"> <li>The OVOC Main Agent is unable to connect to one of the OVOC Client agents. Note that currently the Client agent is only installed on the SmartTAP application server.</li> <li>The SmartTAP Application server is unable to connect to the SmartTAP Web Admin Interface</li> </ul>		
SNMP Alarm	acVAManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.1		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	The OVOC Main Agent is unable to connect to one of the installed OVOC Client agents.	Unable to connect to client agent on <SmartTapAS_FQDN>	
	The SmartTAP Application server is unable to connect to the SmartTAP Web Admin interface.	Unable to Connect to Voice Application Admin	
Cleared	OVOC Client agent is re-available		

## SmartTAP Event – Component Restart

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

## Event – Component Resource Failed

Alarm Field	Description		
Description	This event is raised in the following circumstances: <ul style="list-style-type: none"> <li>■ The allocation of resources for recording licenses has been exceeded</li> <li>■ Media Server management has failed</li> </ul>		
SNMP Alarm	acVaCompResFailedEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.9		
Alarm Source	SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following: <ul style="list-style-type: none"> <li>■ Licenses:               <ul style="list-style-type: none"> <li>✓ imLicQuotaExceeded</li> <li>✓ videoLicQuotaExceeded</li> <li>✓ userLicQuotaExceeded</li> <li>✓ mediaFwdLicQuotaExceeded</li> <li>✓ licUnavailable</li> </ul> </li> <li>■ Media Server Resource Failure:               <ul style="list-style-type: none"> <li>✓ Hmp - channelResourceFailure</li> <li>✓ Hmp createFileFailed</li> <li>✓ Hmp bindingFailure</li> <li>✓ Hmp rtsTransferFailed</li> <li>✓ Hmp writeFileFailed</li> </ul> </li> </ul>		
Alarm Title	Component Resource Error		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition (related resource indicated in parenthesis)	<text>	Corrective Action

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

## Alarm - Component Resource Threshold Exceeded

Alarm Field	Description
Description	<p>This alarm is raised when one of the SmartTAP component resources listed below has reached its pre-defined threshold. This alarm applies for the following resources:</p> <ul style="list-style-type: none"> <li>■ Recording license notification thresholds (for all recording license types) triggered according to the configuration in the SmartTAP Web interface License screen.</li> <li>■ Media Storage notification thresholds triggered according to the configuration in the SmartTAP Web interface Storage Statistics screen.</li> <li>■ The number of total hours of analyzed calls by Analytics Service has exceeded the limit.</li> <li>■ The number of licensed Analytics users has exceeded the limit.</li> </ul>
SNMP Alarm	acVaResourceThresholdAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.11
Alarm Source	<p>SmartTapAS_&lt;FQDN&gt;_&lt;resource&gt;, where &lt;resource&gt; is one of the following:</p> <ul style="list-style-type: none"> <li>■ SmartTAP License Threshold Notification value (for all recording license types)</li> <li>■ Media Storage Notification Threshold value</li> <li>■ Analytics Hours license value</li> <li>■ Analytics Users license value</li> </ul>
Alarm Title	Alarm - Component Resource Threshold Exceeded
Alarm Type	Other

Alarm Field	Description		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	The media storage location threshold has been reached.	Media Storage threshold exceeded	<ul style="list-style-type: none"> <li>Verify the Notification Threshold setting configuration in the Storage Statistics screen. It's possible that there is sufficient storage and that the threshold needs to be adjusted.</li> <li>Add additional storage capacity to the file server to support additional media files (recordings). The file server is external to SmartTAP.</li> </ul>
	Recording License threshold exceeded	Recording License threshold exceeded	<ul style="list-style-type: none"> <li>Verify the Notification Threshold setting configuration in the License screen. It's possible that there are sufficient licenses and that the threshold needs to be adjusted.</li> <li>Purchase additional recording licenses</li> </ul>
	The total number of hours of analyzed calls by Analytics Service has exceeded the limit.	Analytics Hours license Threshold Exceeded	<ul style="list-style-type: none"> <li>Verify the Notification Threshold setting configuration in the License screen. It's possible that there are sufficient licenses and that the threshold needs to be adjusted.</li> <li>Purchase additional analytics hours</li> </ul>
	The number of licensed Analytics users has exceeded the limit	Analytics Users license Threshold Exceeded	<ul style="list-style-type: none"> <li>Verify the Notification Threshold setting configuration in the License screen. It's possible that there are sufficient licenses and that the threshold needs to be adjusted.</li> <li>Purchase additional analytics user licenses</li> </ul>
Cleared	When counter returns below the threshold level.	-	-

## Alarm – Connection Failure

Alarm Field	Description
Description	<p>This alarm is raised in the following circumstances:</p> <ul style="list-style-type: none"> <li>The connection between one of the SmartTAP components and the SmartTAP Application server is down.</li> <li>The connection between other SmartTAP components is down.</li> </ul>
SNMP Alarm	acVaConnectionFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.12
Alarm Source	<p>&lt;SmartTAPComponent&gt;@ &lt;FQDN&gt;:</p> <ul style="list-style-type: none"> <li>AC-MediaProxy @&lt;FQDN&gt;</li> <li>AC-Annoucement @ &lt;FQDN&gt;</li> <li>CS@ &lt;FQDN&gt;</li> <li>CD-IP@ &lt;FQDN&gt;</li> <li>CD-SIPREC@ &lt;FQDN&gt;</li> <li>MediaDelivery@ &lt;FQDN&gt;</li> <li>Media Server@&lt;FQDN&gt;</li> <li>AC_HealthMonitor@ &lt;FQDN&gt;</li> <li>AC-Plugin@ &lt;FQDN&gt;</li> <li>RTS@ &lt;FQDN&gt;</li> </ul>
Alarm Title	Alarm – Connection Failure
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description	
Additional Info	-	
Alarm Severity	Condition	Corrective Action
Critical/Major/Warning	Communication between SmartTAP component and SmartTAP Application server is down	Communication Down Details: Managed Device <SmartTAPComponent>@<HostNameFQDN> failed to send heartbeat within specified time of <xxmS>.Device Infold: <SmartTAPInternalID>HostNameType: COM_SERVERDisplay Name: <HostName>Last heartbeat received on <yyyy-mm-dd> <hh:mm>
	Connection from CallDelivery to lyncPlugInServerConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to FE Plug-using TCP
	Connection from CallDelivery to lyncPlugInSWConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to SmartWorks Plug-using TCP
	Connection from CallDelivery to communication server	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to communication server Plug-using TCP
	Connection from CallDelivery to Media delivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to Media delivery using TCP
	Connection between Media Proxy and Calldelivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to Media Proxy	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to CallDelivery	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to Call Delivery at <HostNameFQDN> using TCP
	Connection from Lync plugin to ann	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to Annoucement Server at <HostNameFQDN> using TCP
Cleared	-	The connection is up again -

## SmartTAP Agent Alarms

This section describes SmartTAP Microsoft Windows Server Agent alarms.

### Alarm – Component Performance Counter General

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

Alarm Field	Description		
Cause			
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Major	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Warning	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Cleared	When counter returns below the threshold level.	-	

## Alarm – Component Service Status

Alarm Field	Description		
Description	This alarm is raised when a component service on the SmartTAP Application server is down. These services include SmartTAP components, for example, HealthMonitorSvc and core Windows components, for example, AcProcDump.		
SNMP Alarm	acVaCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.23		
Alarm Source	SmartTapAS_<FQDN>/<servicename> is one of the following: <ul style="list-style-type: none"> <li>■ AudioCodes_CS</li> <li>■ MySQL</li> <li>■ CallDelivery-IP</li> <li>■ HealthMonitorSvc</li> <li>■ AudioCodesMPSvc</li> <li>■ HPXMedia</li> <li>■ RemoteTransferService</li> <li>■ AcProcDump</li> <li>■ CallDeliverySR</li> <li>■ CallDelivery</li> <li>■ CallDeliveryLD</li> <li>■ CallDeliveryAES</li> <li>■ SmartTapMonitoringSvc</li> </ul>		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_	-

Alarm Field	Description		
		STOPPED (indicates which service is down)	
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	-
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

### Alarm – Component Event Viewer Dropped

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

### Alarm – Certificate Expired

Alarm Field	Description
Description	This alarm is raised when one of the Microsoft Windows-certificates installed on the SmartTAP Application server is about to expire.
SNMP Alarm	acVaCompCertificateExpiredAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.27
Alarm Source	SmartTapAS_<FQDN>
Alarm Type	Other

Alarm Field	Description		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Raised when the certificate will expire in less than two days	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Major	Raised when the certificate will expire in less than 30 days.	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Cleared	When certificate is renewed	-	-

## 10Alarm – Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on the SmartTAP Application Server drive is above the pre-defined threshold.		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.28		
Alarm Source	SmartTAPAS_<FQDN>/DriveName:\\		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.	-	-

## SmartTAP Application Server Alarms

This section describes SmartTAP Application Server alarms.

### Call Recording Error Event

Alarm Field	Description		
Description	This event is raised when errors are reported by the Health Monitor to the SmartTAP Application server.		
SNMP Alarm	acVaCallRecordingErrorEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.13		
Alarm Title	Call Recording Error Event		
Alarm Source	SmartTAPAS_FQDN		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action

Alarm Field	Description		
Major	One of the following Health Monitor services reported an error to the SmartTAP Application server	as below	
	NoMediaFile(301)	Call not recorded or recorded with errors	Check ST configuration and health
	NoFileOnDisk(302)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallWarning(303)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallNotRecorded(304)	Call not recorded or recorded with errors	Check ST configuration and health
	FileXferFailed(204)	Error: Can't upload file to blob	<ul style="list-style-type: none"> <li>Check Media location configuration in SmartTAP</li> <li>Check Azure Blob accessibility and health</li> </ul>
	ComplianceRecordedButNotAssignedToRecProfile (209)	User is targeted but has no recording profile in ST	Assign Recording Profile to user under Compliance Recording Policy
	JoinCallFailed(210)	Bot failed to join the call	<ul style="list-style-type: none"> <li>Check Service Fabric Cluster health</li> <li>Verify MSFT Graph API accessibility and responsiveness</li> </ul>
Major	CdrRecoveryFailed(450)	Call Recovery Failed, file <path> has exceeded the allowed failure threshold.	Check SmartTAP and CD-Live configuration
Major	CdrRecoveryFailed(450)	Call Recovery Failed with status code <statusCode>, file <path>	Check faulty CDR file

## Event – Configuration Error

Alarm Field	Description
Description	<p>This event is raised under the following circumstances:</p> <ul style="list-style-type: none"> <li>A user is mapped to two or more Retention Policies groups via AAD mapping. In this case, the user is not assigned to any retention policy.</li> <li>A user is mapped to two or more Recording Profile groups via AAD mapping. In this case, the user is not be assigned to any recording profile.</li> <li>Problems with Azure Storage account configuration</li> <li>A user is mapped to two or more media locations groups via AAD mapping. In this case the user will not be assigned to any media location.</li> <li>A user is mapped to two or more analytics profiles groups via AAD mapping. In that case the user will not be assigned to any analytics profile.</li> <li>User access to Azure Cognitive Services is unauthorized.</li> </ul>
SNMP Alarm	acVaConfigErrorEvent
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.14
Alarm Source	<n><un> (where n is the name of the component or ip:port and un is the user name)
Additional Information	<ul style="list-style-type: none"> <li>User xxx will not be recorded. A user can not be assigned to two or more AAD groups that are mapped to recording profiles in SmartTAP. Please make sure the user is assigned to one AAD group that is mapped to a recording profile.</li> <li>User xxx is not assigned to a mapped retention policy and will be assigned to the default retention policy. A user can not be assigned to two or more AAD groups that are mapped to retention policies in SmartTAP. Please make sure the user is assigned to one AAD group that is mapped only when mapping retention policies.</li> </ul>

Alarm Field	Description		
	<ul style="list-style-type: none"> <li>User &lt;username&gt; will be assigned to the default Media Location. A user can not be assigned to multiple Media Locations. Make sure the user is assigned to only one Media Location mapped in SmartTAP.</li> <li>User &lt;username&gt; will be assigned to the default Analytics profile. A user can not be assigned to multiple Analytics profiles, make sure the user is assigned to only one Analytics profile mapped in SmartTAP</li> </ul>		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	A user cannot be assigned to multiple AAD groups for Recording Profiles.	Failed to assign a Recording Profile to a user	Check AAD Configuration
Major	A user cannot be assigned to multiple AAD groups for Retention Policies.	Failed to assign a Retention Policy to a user	Check AAD Configuration
Major	Failed to assign a recording location to a Teams Bot node	A recording location is not assigned for Teams Bot node <src>.	Check Recording Location Configuration
Major	A user cannot be mapped to two or more media locations groups via AAD mapping.	Failed to assign a Media Location to a user	Check the Media Location Group assignments.
Major	A user is mapped to two or more analytics profiles groups via AAD mapping; the user will not be assigned to any analytics profile.	Failed to assign an Analytics Profile to a user	Check the analytics profiles groups assignments.
Major	Access to Azure Cognitive Services is unauthorized.	CognitiveServiceMisconfiguration	Check the permissions authorizations to Azure Cognitive Services.

## Recording Resource Failure

Alarm Field	Description		
Description	This alarm is raised when the recording resource is not available		
SNMP Alarm	acVaRecordingResourceFailureAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.15		
Alarm Title	Recording Resource Failure		
Alarm Source	<ul style="list-style-type: none"> <li>botNodeName@botclusterFQDN</li> <li>botCluster@botclusterFQDN</li> </ul>		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Critical	RecordingClusterNotAvailable (Teams Bot cluster is not available): The cluster is overloaded and further calls won't be recorded.	Teams Bot cluster - no recording resource available Alarm.	Increase cluster size immediately.
Warning	RecordingNodeNotAvailable (Teams Bot node is not available): The reporting node is overloaded, bot is still might record further calls if there is another node which is not overloaded.	Teams Bot node - no recording resource available Alarm.	Monitor the system if more than 60% percent of the nodes are over-

Alarm Field	Description		
			loaded, consider increasing cluster size.
Cleared	Teams Bot node is available again	Teams Bot node - no recording resource available Cleared.	
Cleared	Teams Bot cluster is available again	Teams Bot cluster - no recording resource available Cleared.	

## Meeting Insights Alarms

This section describes the Meeting Insights alarms.

### Connection Failure

Alarm Field	Description
Description	<p>One of the following MeetingInsights components is unreachable:</p> <ul style="list-style-type: none"> <li>■ BackEnd</li> <li>■ OutlookDaemon</li> <li>■ SpeechTranscriptionApp</li> <li>■ SpeakerIdApp</li> <li>■ AI Server</li> <li>■ SI server</li> </ul>
SNMP Alarm	acVaConnectionFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.12
Alarm Title	Connection Failure
Alarm Source	<ul style="list-style-type: none"> <li>■ MeetingInsights/&lt;component&gt;--&lt;availabilityTest&gt;</li> <li>■ MeetingInsights/backend-&lt;Customer&gt;status</li> <li>■ MeetingInsights/ -&lt;Customer&gt;status</li> <li>■ MeetingInsights/speakerIdapp--&lt;Customer&gt; status</li> <li>■ MeetingInsights/outlookdaemon--&lt;Customer&gt; status</li> <li>■ MeetingInsightsasierver--&lt;Customer&gt; status</li> <li>■ MeetingInsights/siserver--&lt;Customer&gt; status</li> </ul>
Alarm Type	Other

Alarm Field	Description		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Critical	BackEnd component is down.	BackEnd component is not responding to http request. Service is down.	<ul style="list-style-type: none"> <li>■ Check IIS status and try to connect from the BackEnd server on localhost <a href="http://localhost/ui">http://localhost/ui</a></li> <li>■ Check firewall rules.</li> <li>■ Check EventLogs for errors.</li> </ul>
Critical	OutlookDaemon is down.	OutlookDaemon component is not responding to http request. Bot won't join calls. Service is down.	Check the service status and logs.
Major	SpeechTranscriptionApp is down.	SpeechApp component is not responding to http request. Highlights and meeting transcription are not available.	Check the service status and logs.
Major	SpeakerIdApp is down.	SpeakerIdApp component is not responding to http request. Audc speaker identification is not available.	Check the service status and logs.

Alarm Field	Description		
Critical	AI Server is down.	AI server component is not responding to http request. VoiceCommands are not available.	Check the service status and logs.
Major	SI server is down.	SI server is not responding to http request. Audc speaker identification is not available.	Check the service status and logs.

## Call Recording Error Event

Alarm Field	Description		
Description	This event is raised when errors are reported by either the BackEnd or TeamsBot components.		
SNMP Alarm	acVaCallRecordingErrorEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.13		
Alarm Title	Call Recording Error Event		
Alarm Source	<ul style="list-style-type: none"> <li>■ MeetingInsights/&lt;Component&gt;/&lt;Condition&gt;</li> <li>■ MeetingInsights/Backend/ PostProcessFailed</li> <li>■ MeetingInsights/&lt;nodename@clusterfqdn&gt;/CreateCallFailed</li> <li>■ MeetingInsights/&lt;nodename@clusterfqdn&gt;/JoinCallFailed</li> <li>■ MeetingInsights/&lt;nodename@clusterfqdn&gt;/FileXferFailed</li> </ul>		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	Text	CorrectiveAction
Major	PostProcessFailed	Failed to create final mp4 file.	Check if all media files were uploaded

Alarm Field	Description		
			from Bot..
Major	JoinCallFailed	Failed answering call <call-id> scenarioid <senarioid>.	<ul style="list-style-type: none"> <li>■ Check Bot logs for errors.</li> <li>■ Check customer admin consent for Bot application.</li> <li>■ Check if there is firewall in front of the Bot..</li> </ul>
Major	CreateCallFailed	Teams BOT failed to Post meeting to Backend call-id.	Examine Bot logs.
Major	FileXferFailed	Teams Bot failed to transfer media files to Backend	Examine Bot logs.
Cleared			

## Performance Counter General

Alarm Field	Description
Description	This alarm is raised when the generic performance counter on one of the MeetingInsights servers has reached a pre-defined threshold for memory/CPU.
SNMP Alarm	acVACompPcGenAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.21
Alarm Title	Component Performance Counter General
Alarm Source	MeetingInsights_FQDN/<Performance Monitor Group>/< Performance Monitor Name>/< NetworkAdapterName >
Alarm Type	QualityOfServiceAlarm
Probable Cause	Other
Additional	-

Alarm Field	Description		
Info			
Alarm Severity	Condition	Text	Corrective Action
Critical	Pre-defined severity per counter type has been reached and therefore calls won't be recorded.	GeneralCounter performance counter /is Above threshold	Increase cluster size immediately.
Major	Pre-defined severity per counter type has been reached and therefore calls won't be recorded.	GeneralCounter performance counter /is Above threshold	Increase cluster size immediately.
Warning	Pre-defined severity per counter type has been reached and therefore calls won't be recorded.	GeneralCounter performance counter /is Above threshold	Increase cluster size immediately.
Cleared	When counter returns below the threshold level.		

## Component Service Status

Alarm Field	Description
Description	This alarm is raised when a component service on the MeetingInsights server is down.
SNMP Alarm	acVaCompSrvAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.23
Alarm Title	Component Service Status
Alarm Source	MeetingInsights_MachineName/<service>/ is one of the following: <ul style="list-style-type: none"> <li>■ MongoDB</li> <li>■ IIS</li> <li>■ MIAAlarmManager</li> </ul>
Alarm Type	Other
Probable	Other

Alarm Field	Description		
Cause			
Additional Info	-		
Alarm Severity	Condition	Text	CorrectiveAction
Critical	One of the above mentioned services is down.	SERVICE_STOPPED (indicates which service is down).	Check corresponding service log.
Major	One of the above mentioned services is down.	SERVICE_STOPPED (indicates which service is down).	Check corresponding service log.
Cleared	Service is running.		

## Alarm Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when one of the Microsoft Windows-certificates installed on the MeetingInsights server is about to expire.		
SNMP Alarm	acVaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.27		
Alarm Title	Component Service Status		
Alarm Source	MeetingInsights _MachineName		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	Text	CorrectiveAction
Critical	Raised when the certificate will expire in less than seven days.	Certificate will expire in <days left> days.	Verify which certificate is about to expire and renew it.

Alarm Field	Description		
Major	Raised when the certificate will expire in less than 60 days.	Certificate will expire in <days left> days.	Verify which certificate is about to expire and renew it.
Cleared			

## Alarm Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on any MeetingInsights Servers drive is above the pre-defined threshold.		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.28		
Alarm Title	Disc space		
Alarm Source	MeetingInsights_MachineName /DriveName:\\		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	Text	CorrectiveAction
Critical	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Major	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.	-	-

## ARM Alarms

This section describes the ARM alarms.

### Disk Size Illegal

Alarm Field	Description		
Description	This alarm is raised when the disk size defined for the ARM Configurator or Router is insufficient for ARM requirements.		
SNMP Alarm	acARMDiskSize		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.4		
Alarm Title	Disk Size Illegal		
Alarms Source	<div> <div></div> Configurator         </div> <div> <div></div> Router# &lt;Routername&gt;         </div>		
Alarm Type	integrityViolation		
Probable Cause	storageCapacityProblem		
Alarm Severity	Condition	Text	Corrective Action
Critical	The size of the hard disk of the ARM Configurator or Router is insufficient for ARM requirements.	The size of the hard disk in <Configurator or Router- >/<Configurator or Router Name> was changed to an illegal size <CurrentSize>. Minimum is <MinimumSize>.	Increase VM disk size according to the requirements specified in the ARM Installation manual.

### Disk Space Usage

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

Alarm Field	Description		
Alarm Title	Disk space usage		
Alarms Source	ARM / Partition #partitionName or Router #routerName / Partition #partitionName		
Alarm Type	Environmental Alarm		
Probable Cause	Storage Capacity Problem		
Alarm Severity	Condition	Text	Corrective Action
Indeterminate	<ul style="list-style-type: none"> <li>■ 'Almost full' is sent when the usage is more than 95% (Critical).</li> <li>■ 'Dangerously high' is sent when the usage is more than 80% (Warning).</li> </ul>	The disk usage of {elementType} {elementName} is dangerously high / almost full (in %) {elementType} can be Configurator or router.	<ul style="list-style-type: none"> <li>■ Clean disk from obsolete data.</li> <li>■ Delete old and unused logs and backup files</li> <li>■ In case of watchdog reload delete the created heap file (/tomcat/tmp).</li> <li>■ If the calls feature is enabled and the size of the calls is large according to the logs (log cdr) or check the Mongo DB folder in your VM (/var/lib/mongo), disable the feature, reduce the number of CDR calls in Calls Settings and contact your AudioCodes representative.</li> </ul>

## ARM License About to Expire

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

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.5
Alarm Title	ARM License about to expire
Alarms Source	Configurator
Alarm Type	Operational Violation
Probable Cause	Key Expired
Alarm Severity	Condition
Major	<ul style="list-style-type: none"> <li>This alarm is initially raised 28 days before the expiration date of the license and then for each subsequent day prior to the expiration date.</li> </ul>

### ARM License has Expired

Alarm Field	Description
Description	The ARM license has expired.
SNMP Alarm	acARMLicenseHasExpired
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.6
AlarmTitle	ARM License has expired
AlarmSource	Configurator
AlarmType	Operational Violation
Probable Cause	Key Expired
Alarm Text	<ul style="list-style-type: none"> <li>Alarm License has expired</li> <li>Alarm License is OK</li> </ul>
Severity	Critical
Additional Info	-
Corrective Action	Contact your AudioCodes representative to update your ARM license.

## ARM License Session Number

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

## ARM License Missing

Alarm Field	Description
Description	This alarm is raised when the ARM license is not found.
SNMP Alarm	acARMLicenseMissing
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.10
AlarmTitle	ARM License Missing
AlarmSource	Configurator
AlarmType	Operational Violation
Probable Cause	Key Expired
Alarm Text	<ul style="list-style-type: none"> <li>■ Alarm License was not found</li> <li>■ Alarm License was found</li> </ul>
Severity	Major
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>■ Contact your AudioCodes representative</li> <li>■ Install an ARM license</li> </ul>

## Quality Change

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

Alarm Field	Description
Alarm Text	<p>The Quality of Peer Connection&lt;PeerConnectionName&gt; or Node Connection&lt;NodeConnectionName&gt; was changed to one of the following:</p> <ul style="list-style-type: none"> <li>■ Good</li> <li>■ Fair</li> <li>■ Bad</li> <li>■ Unknown</li> </ul>
Alarm Severity	Major
Corrective Action	<ul style="list-style-type: none"> <li>■ Make sure quality thresholds are configured correctly in the ARM settings</li> <li>■ Validate your network quality in data layer.</li> <li>■ Contact your network administrator.</li> <li>■ If you know that you have a problem with a specific element (Connection or Peer Connection) and you don't wish to receive an alarm for this element, you can configure the element to ignore MOS/ASR and not use the global quality definitions in the Peer or Connection properties in the ARM Web interface.</li> </ul>

## ARM Configurator Reload


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

Alarm Field	Description
Alarm Severity	Condition
Major	<ul style="list-style-type: none"> <li>■ The Tomcat server was not restarted properly.</li> <li>■ The ARM Configurator didn't respond to the number of keep-alive requests from the watchdog.</li> </ul>

## ARM Router Reload

Alarm Field	Description		
Description	This alarm is raised when the router was not reloaded successfully.		
SNMP Alarm	acARMRouterReloaded		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.14		
Alarm Title	ARM router reload		
Alarms Source	Router # routerName		
Alarm Type	Operational Violation		
Probable Cause	Application subsystem failure		
Additional Info	Memory dump in /opt/tomcat/temp/		
Alarm Severity	Condition	Text	Corrective Action
Major	<ul style="list-style-type: none"> <li>■ Tomcat server was not restarted properly</li> <li>■ Router didn't respond to number of keep-alive requests from the watchdog</li> </ul>	ARM router {routerName} was reloaded by watchdog.	<ul style="list-style-type: none"> <li>■ Collect logs</li> <li>■ Contact your AudioCodes representative</li> </ul>

## ARM Routing Rule Match

Alarm Field	Description
Description	<p>This event is raised when a Routing rule for a specific element is matched.</p> <div>  <p>These events are sent when the "Notify When activated" check box is selected for the Routing Rule in the ARM Web interface (Advanced Conditions tab).</p> </div>
SNMP Alarm	acARMRoutingRuleMatch
SNMP OID	.1.3.6.1.4.1.5003.9.70.1.2.2.0.13
Alarm Title	Routing Rule match
Alarms Source	Router#<RouterName>
Alarm Type	Other
Probable Cause	Other
Additional Info	<ul style="list-style-type: none"> <li>■ Routing Rule &lt;ruleName&gt; of Group &lt;groupName&gt; is matched.</li> <li>■ Call from Pcon &lt;PeerConnectionName&gt;, Node &lt;nodeName&gt; – From number &lt;fromNumber&gt;, to &lt;toNumber&gt;.</li> </ul>
Alarm Text	Routing Rule <rule name> was matched
Alarm Severity	indeterminate
Corrective Action	Disable the notification in the routing rule if you don't wish to view this event.

## ARM Configuration Inconsistency

Alarm Field	Description
Description	This event is raised when there is mismatch between a Peer connection or a Routing Interface configuration and a Node configuration.
SNMP Alarm	acARMConfigurationInconsistency
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.1.0.1

Alarm Field	Description
Alarm Title	Configuration Inconsistency
Alarms Source	Node #<NodeName>/PeerConnection#<PeerConnectionName> Node#<NodeName>/RoutingInterface#<RoutingInterfaceName>
Alarm Type	Processing Error Alarm
Probable Cause	Configuration or Customization Error
Additional Info	ARM database was synchronized to the nodes configuration
Alarm Severity	Condition
Indeterminate	<ul style="list-style-type: none"> <li>■ An inconsistency was discovered between the ARM Topology and the SBC or gateway configuration.</li> <li>■ The element was added to the SBC and discovered by ARM during the synchronization process.</li> </ul>

### Operation State Changed (Router)

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

Alarm Field	Description		
Major	The router is not synchronized with the ARM Configurator.	Router <RouterName> was marked as Not_Sync.	<p>In case state is unavailable:</p> <ul style="list-style-type: none"> <li>■ Check router status and availability.</li> <li>■ Network connectivity between configurator and router.</li> <li>■ Validate that proper Router credentials updated in ARM.</li> <li>■ Validate DNS setting in case hostname is used.</li> </ul>
Major	The router is initializing with the ARM Configurator.	Router <RouterName> was marked as Initializing	
Major	The configured memory in the router is less than the size required by the license.	Router <RouterName> was marked as not in service due to memory requirements.	<p>This occurs when the number of users does not match the memory requirements.</p> <p>Refer to User's manual / Installation Guide for more information regarding how increase the memory.</p>
Major	An external Web Service associated with this	Web Service <Web service name> was	

Alarm Field	Description		
	router is unavailable.	marked as Unavailable	
Cleared	The router is re-available	Router <RouterName>was marked as Available.	

### Operation Status Changed [Node]

Alarm Field	Description		
Description	This alarm is raised when the operative state of a specific Node has changed.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarms Source	<ul style="list-style-type: none"> <li>■ Node#&lt;NodeName&gt;/Router#armServer</li> <li>■ (For IP Profile issues) Node#&lt;NodeName&gt;</li> </ul>		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info	<p>The alarm will be cleared once the status will be changed back to available.</p> <p>Added the routing server to the node</p>		
Alarm Severity	Condition	Text	Corrective Action
Major	The Routing server node is unavailable.	Routing Server armServer in Node <Node Name> was marked as Unavailable	<ul style="list-style-type: none"> <li>■ Check device network connectivity</li> <li>■ Check the device's network connectivity to the ARM Configurator</li> </ul>

Alarm Field	Description		
	The Routing server node is Unrouteable.	Routing Server armServer in Node <Node Name> was marked as Unrouteable	<ul style="list-style-type: none"> <li>■ Check the device's network connectivity to the ARM routers</li> <li>■ Check the routers' status and availability</li> </ul>
	The Routing server node is Logged out.	Routing Server armServer in Node <Node Name> was marked as Logout.	<ul style="list-style-type: none"> <li>■ Check the configuration of the device's ARM service.</li> </ul>
	The ARM IP Profile is marked as unavailable.	IP Profile ARM_IP_Profile in <Node Name> Node was marked as Unavailable	<ul style="list-style-type: none"> <li>■ Check if the IP Profile exists on the device node specified in the Alarm text. If yes, remove it and resync the node.</li> <li>■ Check the syslog and ARM log files for the error and contact support.</li> </ul>
Cleared		Node <NodeName> was marked as <Status>	

### Operation Status Changed [Peer Connection]

Alarm Field	Description
Description	This alarm is raised when the operative state of the VoIP Peer Connection

Alarm Field	Description		
	has changed.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarms Source	Node #<NodeName>/<PeerConnection#<PeerName>		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info	The alarm will be cleared once the status will be changed back to available.		
Alarm Severity	Condition	Text	Corrective Action
Major		Peer Connection in Node <Node Name> was marked as Unavailable	<p>When this alarm is received from a Peer Connection and it indicates that the operative state of the Peer Connection has changed to Unavailable:</p> <ul style="list-style-type: none"> <li>■ Check the configuration of the related IP Group in the specific device.</li> <li>■ Check the device's network connectivity to the configured Proxy IP associated with that IP Group</li> </ul>

Alarm Field	Description		
Cleared		Peer<PeerName> was marked as Available	

### Operation Status Changed [LDAP Server]

Alarm Field	Description		
Description	This alarm is generated when the LDAP server is disconnected or reconnected.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarms Source	LDAP server # <LDAPServerName>		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info	The alarm will be cleared once the status is changed back to available.		
Alarm Severity	Condition	Text	Corrective Action
Major		LDAP Server <LDAPServerName> was marked as Unavailable.	<p>This alarm is raised when LDAP server state has turned to unavailable:</p> <ul style="list-style-type: none"> <li>■ Check the LDAP server network connectivity.</li> <li>■ Validate LDAP server credentials.</li> </ul>

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

### Operational Status Changed [Active MQ]

Alarm Field	Description		
Description	This alarm is generated when there is a problem with the JMS broker on the ARM Configurator.		
SNMP Alarm	acARMOperationStatusChanged		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.1		
Alarm Title	Operation Status Changed		
Alarms Source	Configurator		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info	Failed sending three consecutive messages to the JMS, going to reload		
Alarm Severity	Condition	Text	Corrective Action
Critical	Configurator could not send three consecutive messages to the ActiveMQ broker.	ActiveMQ Connection was marked as Unavailable.	<p>The ActiveMQ should be restarted automatically. If the alarm doesn't clear after a period of time:</p> <ul style="list-style-type: none"> <li>■ Check that the ActiveMQ service is working properly</li> <li>■ Collect ActiveMQ logs</li> </ul>

Alarm Field	Description		
			■ Contact your AudioCodes representative

## Limit Reached

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

## Router Using Other Configurator

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

Alarm Field	Description		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.7		
Alarm Title	Router Using Other Configurator		
Alarms Source	Router #<RouterName>		
Alarm Type	Operational Violation		
Probable Cause	Denial Of Service		
Additional Info	Contact your AudioCodes representative.		
Alarm Severity	Condition	Text	Corrective Action
Critical		Router <RouterName> is already connected to another configurator <otherIPAddress>	<p>Two configurators are trying to use the router at the same time:</p> <ul style="list-style-type: none"> <li>■ Check the IP of another configurator, {otherAddress} in the description and make sure only one of them uses the router.</li> <li>■ Restart the tomcat service in the router machine.</li> </ul>

## NTP Sync Status

Alarm Field	Description
Description	<p>This alarm is raised when the clock on the ARM Configurator or Router is not synchronized with the NTP server. The NTP clock is critical for ARM services as it impacts license, routing (time conditions) and statistics:</p> <ul style="list-style-type: none"> <li>■ IP connectivity to the NTP server</li> </ul>

Alarm Field	Description
	<ul style="list-style-type: none"> <li>Firewall configuration</li> <li>NTP server configuration</li> </ul>
SNMP Alarm	acARMNTPSyncStatus
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.8
AlarmTitle	NTP sync status
AlarmType	Time Domain Violation
AlarmSource	<ul style="list-style-type: none"> <li>Configurator#&lt;Configuratorname&gt;</li> <li>Router #&lt;Routername&gt;</li> </ul>
Probable Cause	Timing Problem
Alarm Text	<ul style="list-style-type: none"> <li>The NTP clock on the ARM Configurator is not synchronized with NTP server</li> <li>The NTP clock on ARM Configurator is synchronized with NTP server</li> </ul>
Severity	Major
Additional Info	-
Corrective Action	<ul style="list-style-type: none"> <li>Check the NTP configuration in the ARM Web interface.</li> <li>Check for connectivity issues with the NTP server configured in the NTP Servers tab in the ARM Web interface.</li> </ul>

## No Available Routers

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

Alarm Field	Description		
Alarm Type	Communications Alarm		
Probable Cause	Communications Subsystem Failure		
Additional Info			
Alarm Severity	Condition	Text	Corrective Action
Critical	When there are no routers in the system or when all defined routers are unavailable	Currently there are no available routers in the system.	<ul style="list-style-type: none"> <li>■ Make sure that at least one router is configured in your system.</li> <li>■ Check router status and availability.</li> <li>■ Network connectivity between configurator and router.</li> <li>■ Validate that proper Router credentials updated in ARM.</li> <li>■ Validate DNS setting in case hostname is used.</li> </ul>
Clear	When there is at least one available router		

### Registration Status Resync Threshold

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

Alarm Field	Description		
SNMP Alarm	acARMRegistrationStatusResyncThreshold		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.16		
Alarm Title	Registration Status Resync Threshold		
Alarms Source	ARM		
Alarm Type	communicationsAlarm		
Probable Cause	softwareProgramError		
Additional Info			
Alarm Severity	Condition	Text	Corrective Action
major	The number of registered user resync attempts is over the default limit of three.	The number of registration users resync attempts crossed the threshold for node #elementName	
clear			

## External Web Service

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

Alarm Field	Description		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	Text	Corrective Action
Minor	Raised when an external web service is unavailable.	“Web Service <Web service name> was marked as Unavailable”	
Clear	External Web Service becomes available.		

## Disk Usage Alarm

Alarm Field	Description
Description	This alarm is raised when the cumulative duration of all calls for a peer connection or resource group reaches the limit defined in the Calls Quota that is attached to these entities. In addition, a warning is raised when the duration reaches the user-defined threshold.
SNMP Alarm	acARMCallsDurationQuotaUsage
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.18
Alarm Title	Calls duration quota usage
Alarms Source	<ul style="list-style-type: none"> <li>■ Node#&lt;NodeName&gt;/PeerConnection#&lt;PeerConnectionName&gt;</li> <li>■ Resource group#&lt;ResourceGroupName&gt;</li> </ul>
Alarm Type	Other
Probable Cause	Threshold Crossed
Additional Info	

Alarm Field	Description		
Alarm Severity	Condition	Text	Corrective Action
Critical	Calls quota limit has been reached.	{elementType} {elementName} calls quota limit/threshold has been reached.	<ul style="list-style-type: none"> <li>■ Make sure that the calls quota has been configured as required. If not, do one of the following: <ul style="list-style-type: none"> <li>✓ Delete the Calls Quota limit for the Peer Connection or Resource Group</li> <li>✓ Adjust the Calls Quota limit or Time Scheduling for the Peer Connection or Resource Group</li> </ul> </li> </ul>
Warning	Calls quota threshold has been reached The threshold is configurable, 75% by default	{elementType} {elementName} calls quota threshold has been reached.	<ul style="list-style-type: none"> <li>■ Make sure that the calls quota threshold has been configured as required. If not, do one of the following: <ul style="list-style-type: none"> <li>✓ Delete the Calls Quota for the Peer Connection or Resource Group</li> <li>✓ Change the Threshold for the Peer Connection or</li> </ul> </li> </ul>

Alarm Field	Description		
			Resource Group
Clear	<ul style="list-style-type: none"> <li>■ Calls Quota has been deleted from the Peer Connection</li> <li>■ Calls Quota has been deleted from the Resource Group</li> <li>■ New time period has started (according to Time Scheduling defined in the Calls Quota)</li> <li>■ Time Scheduling in Calls Quota definition has been modified. For example, set to “monthly” instead of “daily”</li> <li>■ Modifying Limit in Calls Quota definition results in alarm clearing for specific peer connections or resource groups (i.e. for those entities with the Calls Quota applied that fall within limit/threshold when its extended)</li> </ul>		

## CAC Usage

Alarm Field	Description		
Description	This alarm is raised when the number concurrent sessions of an element reaches the limit defined in the CAC that is attached to these elements. In addition, a warning is raised when the number of concurrent sessions reaches the user-defined threshold		
SNMP Alarm	acARMCAC		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.19		
Alarm Title	CAC usage		
Alarms Source	<ul style="list-style-type: none"> <li>■ Node#&lt;NodeName&gt;/PeerConnection#&lt;PeerConnectionName&gt;/incoming</li> <li>■ Node#&lt;NodeName&gt;/PeerConnection#&lt;PeerConnectionName&gt;/outgoing</li> <li>■ Node#&lt;NodeName&gt;/PeerConnection#&lt;PeerConnectionName&gt;/total</li> <li>■ PeerConnection#&lt;PeerConnectionName&gt;/incoming</li> <li>■ PeerConnection#&lt;PeerConnectionName&gt;/outgoing</li> <li>■ PeerConnection#&lt;PeerConnectionName&gt;/total</li> <li>■ Customer#&lt;CustomerName&gt;/incoming</li> <li>■ Customer#&lt;CustomerName&gt;/outgoing</li> <li>■ Customer#&lt;CustomerName&gt;/total</li> <li>■ VoIP Peer#&lt;VoIPPeerName&gt;/incoming</li> <li>■ VoIP Peer#&lt;VoIPPeerName&gt;/outgoing</li> <li>■ VoIP Peer#&lt;VoIPPeerName&gt;/total</li> </ul>		
Alarm Type	Operational Violation		
Probable Cause	Threshold Crossed		
Additional Info			
Alarm	Condition	Text	Corrective Action

Alarm Field	Description		
Severity			
Critical	CAC has exceeded the defined value.	{elementType} {elementName} incoming/outgoing/total has exceeded 100%	<p>Make sure that the CAC has been configured as required. If not, do one of the following:</p> <ul style="list-style-type: none"> <li>■ Delete the CAC from the relevant element.</li> <li>■ Adjust the CAC limit.</li> </ul>
Warning	CAC alarm threshold has exceeded the defined value.	{elementType} {elementName} incoming/outgoing/total has exceeded {DefinedThreshold}%	<p>Make sure that the CAC has been configured as required. If not, do one of the following:</p> <ul style="list-style-type: none"> <li>■ Delete the CAC from the relevant element.</li> <li>■ Adjust the CAC limit.</li> </ul>
Clear	<ul style="list-style-type: none"> <li>■ CAC has been deleted from the element</li> <li>■ Number of concurrent sessions is lower than the threshold.</li> <li>■ Modifying Limit in CAC definition results in alarm clearing for specific element (i.e. for those entities with the CAC applied that fall within</li> </ul>		

Alarm Field	Description		
	limit/threshold when its extended)		

## Calls Duration Quota Usage

Alarm Field	Description		
Description	This alarm is raised when the cumulative duration of all calls for a peer connection or resource group reaches the limit defined in the Calls Quota that is attached to these entities. In addition, a warning is raised when the duration reaches the user-defined threshold		
SNMP Alarm	acARMCallsDurationQuotaUsage		
SNMP OID	1.3.6.1.4.1.5003.9.70.1.2.2.0.18		
Alarm Title	Calls duration quota usage		
Alarms Source	<ul style="list-style-type: none"> <li>■ Node#&lt;NodeName&gt;/PeerConnection#&lt;PeerConnectionName&gt;</li> <li>■ Resource group#&lt;ResourceGroupName&gt;</li> </ul>		
Alarm Type	Other		
Probable Cause	Threshold Crossed		
Additional Info			
Alarm Severity	Condition	Text	Corrective Action
Critical	Calls quota limit has been reached.	{elementType} {elementName} calls quota limit/threshold has been reached.	<p>Make sure that the calls quota has been configured as required. If not, do one of the following:</p> <ul style="list-style-type: none"> <li>■ Delete the Calls Quota limit for the Peer Connection or Resource Group</li> </ul>

Alarm Field	Description		
			<ul style="list-style-type: none"> <li>■ Adjust the Calls Quota limit or Time Scheduling for the Peer Connection or Resource Group</li> </ul>
Warning	Calls quota threshold has been reached The threshold is configurable, 75% by default	{elementType} {elementName} calls quota threshold has been reached.	<ul style="list-style-type: none"> <li>■ Make sure that the calls quota threshold has been configured as required. If not, do one of the following:               <ul style="list-style-type: none"> <li>✓ Delete the Calls Quota for the Peer Connection or Resource Group</li> <li>✓ Change the Threshold for the Peer Connection or Resource Group</li> </ul> </li> </ul>
Clear	<ul style="list-style-type: none"> <li>■ Calls Quota has been deleted from the Peer Connection</li> <li>■ Calls Quota has been deleted from the Resource Group</li> <li>■ New time period has started (according to Time Scheduling defined in the Calls Quota)</li> </ul>		

Alarm Field	Description		
	■ Time Scheduling in Calls Quota definition has been modified. For example, set to “monthly” instead of “daily”		

## VoiceAI Connect Alarms

This section describes the VoiceAI Connect alarms.

### Status DB Connection Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the connection with the statusDB server is lost.
SNMP Alarm	acVoiceAIStatusDBConnectionFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.1
Configuration Parameters	
alarm name	1
metrics	-
group by	db
time interval minutes	2
logical operator	<
message	"Connection with 'status' database is down"
clear message	"Connection with 'status' database is no longer down"
additional info	-
MINOR level	-

Alarm Field	Description
MAJOR level	
CRITICAL level	1
groupId whitelist	-

### All Session Managers Down Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when all the Session Managers are down.
SNMP Alarm	acVoiceAISessionManagersDown
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.2
Configuration Parameters	
alarm name	2
metrics	none
group by	none
time interval minutes	2
logical operator	<
message	"All session managers are down"
clear message	"All session managers are no longer down"
additional info	-
MINOR level	-
MAJOR level	-
CRITICAL level	1
groupId whitelist	-

## SBC Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of SBC call attempt failures per minute over the past interval is higher than the threshold.
SNMP Alarm	acVoiceAISBCFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.3
Configuration Parameters	
alarm name	3
metrics	SBCFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	none
time interval minutes	5
logical operator	-
message	>
clear message	"SBC's Calls attempts Failure Ratio is higher than {threshold}"
additional info	"Ratio of SBC's calls attempts failures per minute over the past {interval} minutes is lower than {threshold}"
MINOR level	"Ratio of SBC's Calls attempts failures per minute over the past {interval} minutes is higher than {threshold}, Current ratio: {current}"
MAJOR level	0.2
CRITICAL level	0.5
groupId whitelist	-

## SBC Failure Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of SBC call attempt failures per Session Manager is higher than the threshold.
SNMP Alarm	acVoiceAISBCFailurePerSessionManager
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.4
Configuration Parameters	
alarm name	4
metrics	SBCFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	sessionManagerId
time interval	5
minutes	
logical operator	>
message	"SBC's Calls attempts per Session Manager Failure Ratio is higher than {threshold}"
clear message	"Ratio of SBC's calls attempts failures per minute over the past {interval} minutes is lower than {threshold}"
additional info	"Ratio of SBC's Calls attempts failures per minute over the past {interval} minutes is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
groupId whitelist	-

## TTS Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of TTS failures per minute over the past interval on the TTS provider is higher than the threshold.
SNMP Alarm	acVoiceAITTSFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.5
Configuration Parameters	
alarm name	5
metrics	TTSFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	ttsProviderId
time interval minutes	5
logical operator	>
message	"TTS provider {groupId} Failures is higher than {threshold}"
clear message	"Ratio of TTS failures per minute over the past {interval} minutes on TTS provider {groupId} is lower than {threshold}"
additional info	"Ratio of TTS failures per minute over the past {interval} minutes on TTS provider {groupId} is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
use secondary device description	true
groupId whitelist	-

## TTS Failure Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of TTS failures per minute over the past interval per Session Manager for all TTS providers is higher than the threshold.
SNMP Alarm	acVoiceAITTSFailurePerSessionManager
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.6
Configuration Parameters	
alarm name	6
metrics	TTSFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	sessionManagerId
time interval minutes	5
logical operator	>
message	"TTS (All) failures on session manager is higher than {threshold}"
clear message	"Ratio of TTS failures per minute over the past {interval} minutes on session manager {groupId} on all TTS providers together is lower than {threshold}"
additional info	"Ratio of TTS failures per minute over the past {interval} minutes on session manager {groupId} on all TTS providers together is higher than {threshold},Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
use secondary device	true

Alarm Field	Description
description	
groupId whitelist	-

## Bot Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of bot failures per minute over the past interval on the specific bot is higher than the threshold.
SNMP Alarm	acVoiceAIBotFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.7
Configuration Parameters	
alarm name	7
metrics	BotFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	botId
time interval minutes	5
logical operator	>
message	"BOT id {groupId} Failures is higher than {threshold}"
clear message	"Ratio of Bot failures per minute over the past {interval} minutes on bot id {groupId} is lower than {threshold}"
additional info	"Ratio of Bot failures per minute over the past {interval} minutes on bot id {groupId} is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5

Alarm Field	Description
CRITICAL level	-
use secondary device description	true
groupId whitelist	-

### Bot Failure Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of bot failures per minute over the past interval per Session Manager for all bots is higher than the threshold.
SNMP Alarm	acVoiceAIBotFailurePerSessionManager
Name	
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.8
Configuration Parameters	
alarm name	8
metrics	BotFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	sessionManagerId
time interval minutes	5
logical operator	>
message	"BOT (All) failures on session manager is higher than {threshold}"
clear message	"Ratio of Bot failures per minute over the past {interval} minutes on session manager {groupId} on all bots together is lower than {threshold}"
additional info	"Ratio of Bot failures per minute over the past {interval} minutes on session manager {groupId} on all bots together is higher than

Alarm Field	Description
	{threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
use secondary device description	true
groupId whitelist	-

## STT Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of STT failures per minute over the past interval on the STT provider is higher than the threshold.
SNMP Alarm	acVoiceAISTTFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.9
Configuration Parameters	
alarm name	9
metrics	STTFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	sttProviderId
time interval minutes	5
logical operator	>
message	"STT provider {groupId} Failures is higher than {threshold}"
clear message	"Ratio of STT failures per minute over the past {interval} minutes on

Alarm Field	Description
	STT provider {groupId} is lower than {threshold}"
additional info	"Ratio of STT failures per minute over the past {interval} minutes on STT provider {groupId} is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
use secondary device description	true
groupId whitelist	-

### STT Failure Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of STT failures per minute over the past interval on the Session Manager for all STT providers is higher than the threshold.
SNMP Alarm Name	acVoiceAISTTFailurePerSessionManager
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.10
Configuration Parameters	
alarm name	10
metrics	STTFailuresPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0
group by	sessionManagerId
time interval minutes	5

Alarm Field	Description
logical operator	>
message	"STT (All) failures on session manager is higher than {threshold}"
clear message	"Ratio of STT failures per minute over the past {interval} minutes on session manager {groupId} on all STT providers together is lower than {threshold}"
additional info	"Ratio of STT failures per minute over the past {interval} minutes on session manager {groupId} on all STT providers together is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL level	-
use secondary device	true
description	
groupId whitelist	-

## Failed Calls Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of failed calls over the past interval is higher than the threshold.
SNMP Alarm	acVoiceAIFailedCalls
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.11
Configuration Parameters	
alarm name	11

Alarm Field	Description
metrics	$(\text{CallEndingsPerMinute} - \text{SuccessfulCallsPerMinute}) / \text{CallEndingsPerMinute}$ if $\text{CallEndingsPerMinute} > 2$ else 0
group by	none
time interval minutes	5
logical operator	>
message	"Calls Failure Ratio is higher than {threshold}"
clear message	"Ratio of failed calls over the past {interval} minutes is no longer higher than {threshold}"
additional info	"Ratio of failed calls over the past {interval} minutes is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL	-
level	
groupId whitelist	-

### Failed Calls Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the ratio of failed calls over the past interval on the Session Manager is higher than the threshold.
SNMP Alarm	acVoiceAIFailedCallsPerSessionManager
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.12
Configuration Parameters	

Alarm Field	Description
alarm name	12
metrics	$(\text{CallEndingsPerMinute} - \text{SuccessfulCallsPerMinute}) / \text{CallEndingsPerMinute}$ if $\text{CallEndingsPerMinute} > 2$ else 0
group by	sessionManagerId
time interval minutes	5
logical operator	>
message	"Calls per Session Manager Failure Ratio is higher than {threshold}"
clear message	"Ratio of failed calls over the past {interval} minutes on session manager {groupid} is no longer higher than {threshold}"
additional info	"Ratio of failed calls over the past {interval} minutes on session manager {groupid} is higher than {threshold}, Current ratio: {current}"
MINOR level	0.2
MAJOR level	0.5
CRITICAL	-
level	
groupid whitelist	-

## TTS Delay Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the average TTS delay over the past interval on the TTS provider is higher than the threshold.
SNMP Alarm	acVoiceAITTSDelay
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.13
Configuration Parameters	

Alarm Field	Description
alarm name	13
metrics	AverageTTSDelayMilliseconds
group by	AverageTTSDelayMilliseconds
time interval minutes	5
logical operator	>
message	"Average TTS delay is higher than {threshold} milliseconds"
clear message	"Average TTS delay over the past {interval} minutes on TTS provider {groupId} is no longer higher than {threshold} milliseconds"
additional info	"Average TTS delay over the past {interval} minutes on TTS provider {groupId} is higher than {threshold} milliseconds, Current value: {current} milliseconds"
MINOR level	500
MAJOR level	1000
CRITICAL level	-
use secondary device description	true
groupId whitelist	-

## Call Duration Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the average call duration over the past interval on the bot is lower than the threshold.
SNMP Alarm	acVoiceAICallDuration

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.14
Configuration Parameters	
alarm name	14
metrics	AverageCallDurationSeconds if SuccessfulCallsPerMinute > 2 else 1000
group by	botId
time interval minutes	5
logical operator	<
message	"Average BOT call duration is lower than {threshold} seconds"
clear message	"Average call duration over the past {interval} minutes on bot {groupId} is no longer lower than {threshold} seconds"
additional info	"Average call duration over the past {interval} minutes on bot {groupId} is lower than {threshold} seconds, Current value: {current} seconds"
MINOR level	10
MAJOR level	5
CRITICAL level	-
groupId whitelist	-

### Active Calls Per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the active calls over the past interval on the Session Manager is higher than the threshold.
SNMP Alarm	acVoiceAIActiveCallsPerSessionManager

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.15
Configuration Parameters	
alarm name	15
metrics	ActiveCalls
group by	sessionManagerId
time interval minutes	5
logical operator	>
message	"Active calls is higher than {threshold}"
clear message	"Active calls over the past {interval} minutes on session manager {groupid} is no longer higher than {threshold}"
additional info	"Active calls over the past {interval} minutes on session manager {groupid} is higher than {threshold}, Current value: {current}"
MINOR level	200
MAJOR level	300
CRITICAL level	-
groupid whitelist	-

## CPU Usage Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when CPU usage on the host over the past interval has been idle for a duration that is lower than the threshold.
SNMP Alarm	acVoiceAICPUUsage

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.16
Configuration Parameters	
alarm name	16
metrics	cpu.usage_idle
group by	host
time interval minutes	5
logical operator	<
message	"CPU idle is lower than {threshold}%"
clear message	"CPU idle over the past {interval} minutes on host {groupid} is no longer lower than {threshold}%"
additional info	"CPU idle over the past {interval} minutes on host {groupid} is lower than {threshold}%, Current value: {current}%"
MINOR level	10
MAJOR level	5
CRITICAL	-
level	
groupid whitelist	-

## Disk Usage Alarm

This alarm is sent when host's disk usage over the past interval is higher than the threshold.

**Table 7-1: Disk Usage Alarm**

Alarm Field	Description
SNMP	
SNMP Alarm	acVoiceAIDiskUsage

Alarm Field	Description
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.17
Configuration Parameters	
alarm name	17
metrics	disk.used_percent
group by	host
time interval minutes	5
logical operator	>
message	"Disk usage is higher than {threshold}%"
clear message	"Disk usage over the past {interval} minutes on host {groupId} is no longer higher than {threshold}%"
additional info	"Disk usage over the past {interval} minutes on host {groupId} is higher than {threshold}%, Current value: {current}%"
MINOR level	80
MAJOR level	90
CRITICAL level	-
groupId whitelist	-

## Memory Usage Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when available RAM is lower than the threshold.
SNMP Alarm	acVoiceAIMemoryUsage
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.18

Alarm Field	Description
Configuration Parameters	
alarm name	18
metrics	mem.available_percent
group by	host
time interval minutes	5
logical operator	<
message	"Available RAM is lower than {threshold}%"
clear message	"Available RAM over the past {interval} minutes on host {groupId} is no longer lower than {threshold}%"
additional info	"Available RAM over the past {interval} minutes on host {groupId} is lower than {threshold}%, Current value: {current}%"
MINOR level	20
MAJOR level	10
CRITICAL level	-
groupId whitelist	-

### Auto Update Not Working Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the Auto-update process is not working.
SNMP Alarm	acVoiceAIAutoUpdateNotWorking
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.19

Alarm Field	Description
Configuration Parameters	
alarm name	19
metrics	AutoUpdate.none
group by	none
time interval minutes	2
logical operator	<
message	"Auto-update process is not working"
clear message	"Auto-update process is back to work"
additional info	-
MINOR level	-
MAJOR level	-
CRITICAL level	-
groupId whitelist	-

## Auto Update Failure Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when there is a failure in the Auto-update process.
SNMP Alarm	acVoiceAIAutoUpdateFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.20
Configuration Parameters	
alarm name	20
metrics	AutoUpdate.SuccessfulRun

Alarm Field	Description
group by	none
time interval minutes	2
logical operator	<
message	"Failure of auto-update process"
clear message	"Auto-update process is back to normal"
additional info	-
MINOR level	-
MAJOR level	1
CRITICAL level	-
groupId whitelist	-

### Session Manager Down Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the Session Manager is down.
SNMP Alarm	acVoiceAISessionManagerDown
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.21
Configuration Parameters	
alarm name	21
metrics	none
group by	sessionManagerId
time interval minutes	2

Alarm Field	Description
logical operator	<
message	"Session manager {groupId} is down"
clear message	"Session manager {groupId} is no longer down"
additional info	-
MINOR level	-
MAJOR level	-
CRITICAL level	1
groupId whitelist	-

## End-To-End Keep Alive Failed Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when the Session Manager is down.
SNMP Alarm	acVoiceAEndToEndKeepAliveFailed
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.22
Configuration Parameters	
alarm name	22
metrics	SuccessfulCallsPerMinute
group by	botId
time interval minutes	5
logical operator	<
message	"End to end keep alive failed on on bot {groupId}"
clear message	"successful end to end keep alive on bot {groupId}"

Alarm Field	Description
additional	"number of successful end to end keep alive per minute in the past
info	{interval} minutes on bot {groupId} is lower than {threshold}, Current value: {current}"
MINOR level	-
MAJOR level	-
CRITICAL level	0.2
groupId whitelist	-

### Failed Key Retrieval per Session Manager Alarm

Alarm Field	Description
SNMP	
Description	This alarm is sent when a key retrieval attempt on the Session Manager fails.
SNMP Alarm	acVoiceAIKeyRetrievalFailure
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.23
Configuration Parameters	
alarm name	23
metrics	Secrets.FailedKeyAttempts
group by	sessionManagerId
time interval minutes	3
logical operator	>
message	"Failed key retrieval on session manager {groupId}"
clear message	"Successful key retrieval on session manager {groupId}"
additional info	""

Alarm Field	Description
MINOR level	-
MAJOR level	0.9
CRITICAL level	-
groupId whitelist	-

Table 7-2: User Defined

Alarm Field	Description		
Description	The following alarms can be defined by the user:		
	SNMP Alarm	SNMP OID	Alarm Title
	acVoiceAIUserDefined1	1.3.6.1.4.1.5003.9.90.1.2.0.200	User defined 1
	acVoiceAIUserDefined2	1.3.6.1.4.1.5003.9.90.1.2.0.201	User defined 2
	acVoiceAIUserDefined3	1.3.6.1.4.1.5003.9.90.1.2.0.202	User defined 3
	acVoiceAIUserDefined4	1.3.6.1.4.1.5003.9.90.1.2.0.203	User defined 4
	acVoiceAIUserDefined5	1.3.6.1.4.1.5003.9.90.1.2.0.204	User defined 5
	acVoiceAIUserDefined6	1.3.6.1.4.1.5003.9.90.1.2.0.205	User defined 6

	acVoiceAIUserDefined7	1.3.6.1.4.1.5003.9.90.1.2.0.206	User defined 7
	acVoiceAIUserDefined8	1.3.6.1.4.1.5003.9.90.1.2.0.207	User defined 8
	acVoiceAIUserDefined9	1.3.6.1.4.1.5003.9.90.1.2.0.208	User defined 9
	acVoiceAIUserDefined10	1.3.6.1.4.1.5003.9.90.1.2.0.209	User defined 10
AlarmType	communicationsAlarm		
Alarm Source	User defined		
Probable Cause	other (0)		
Alarm Severity	Condition	Text	Corrective Action
Critical	User defined	User defined	
Major	User defined	User defined	
Major	User defined	User defined	
Warning	User defined	User defined	
Indeterminate	User defined	User defined	
Cleared	User defined	User defined	

## Remote Manager is Down Alarm

Delete this text and replace it with your own content.

Alarm Field	Description		
Description	This alarm indicates that the VAIC failed to connect to the OVOC		
SNMP Alarm	acVoiceAIRemoteManagerConnectionDown		
SNMP OID	1.3.6.1.4.1.5003.9.90.1.2.0.24		
Alarm Title	Connection with remote manager is down		
Alarm Source	ovoc		
Alarm Type	communicationsAlarm		
Probable Cause	other (0)		
Alarm Severity	Condition	Text	Corrective Action
Major	Connection with remote manager X is down	Connection with remote manager X is down	Check that the configured ovoc connection parameters are correct. Check that the OVOC is up and visible from the VAIC over the network.
Cleared	Connection with remote manager X is no longer down	Connection with remote manager X is no longer down	

## User Defined Alarms

Alarm Field	Description		
Description	The following alarms can be defined by the user:		
	SNMP	OID	Alarm Title
	acVoiceAIUserDefined1	1.3.6.1.4.1.5003.9.90.1.2.0.200	User defined 1

Alarm Field	Description		
	acVoiceAIUserDefined2	1.3.6.1.4.1.5003.9.90.1.2.0.20 1	User defined 2
	acVoiceAIUserDefined 3	1.3.6.1.4.1.5003.9.90.1.2.0.20 2	User defined 3
	acVoiceAIUserDefined 4	1.3.6.1.4.1.5003.9.90.1.2.0.20 3	User defined 4
	acVoiceAIUserDefined5	1.3.6.1.4.1.5003.9.90.1.2.0.20 4	User defined 5
	acVoiceAIUserDefined6	1.3.6.1.4.1.5003.9.90.1.2.0.20 5	User defined 6
	acVoiceAIUserDefined7	1.3.6.1.4.1.5003.9.90.1.2.0.20 6	User defined 7
	acVoiceAIUserDefined8	1.3.6.1.4.1.5003.9.90.1.2.0.20 7	User defined 8
	acVoiceAIUserDefined9	1.3.6.1.4.1.5003.9.90.1.2.0.20 8	User defined 9
	acVoiceAIUserDefined10	1.3.6.1.4.1.5003.9.90.1.2.0.209	User defined 10
AlarmType	communicationsAlarm		
Alarm Source	User defined		
Probable Cause	other (0)		
Alarm Severity	Condition	Text	Corrective Action
Critical	User defined	User defined	
Major	User defined	User defined	
Warning	User defined	User defined	

Alarm Field	Description		
Indeterminate	User defined	User defined	
Cleared	User defined	User defined	

**This page is intentionally left blank.**

**International Headquarters**

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

**AudioCodes Inc.**

80 Kingsbridge Rd  
Piscataway, NJ 08854, USA  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

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

**Website:** <https://www.audiocodes.com/>

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

©2022 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-41810

