Alarms Monitoring Guide

*AudioCodes One Voice Operations Center (OVOC)*

# OVOC

## Alarms

Version 8.4

One Voice Operations Center

# Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published 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: October-30-2025

## Trademarks

©2025 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, 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.

## Security Vulnerabilities

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

## Customer Support

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

## Documentation Feedback

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

## Stay in the Loop with AudioCodes

# Related Documentation

| Document Name |
|---|
| **OVOC Documents** |
| Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center |
| One Voice Operations Center IOM Manual |
| One Voice Operations Center Product Description |
| One Voice Operations Center User’s Manual |
| Device Manager Pro Administrator's Manual |
| One Voice Operations Center Alarms Monitoring Guide |
| One Voice Operations Center Performance Monitoring Guide |
| One Voice Operations Center Security Guidelines |
| One Voice Operations Center Integration with Northbound Interfaces |
| Device Manager for Third-Party Vendor Products Administrator's Manual |
| Device Manager Deployment Guide |
| ARM User's Manual |
| **Documents for Managed Devices** |
| 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 |

| Document Name |
|---|
| 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 |
| 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 | Updates for Version 8.2 and Version 8.2.1000:<br>■ Added OVOC alarm Table Partition Management Error Event.<br>■ Added IP Phone alarm: IPP Server SSL Certificate Could Not Be Proven<br>■ Added Vocanom System and Agent alarms.<br>■ Added SBC alarms: No Reply From DNS Server Alarm; Weak Password alarm<br>■ Update to Meeting Insights alarm Call Recording Error Event |
| 41811 | ■ Update to the UMP User License Threshold alarm.<br>■ Added new IPP alarms: Device Fails to Get Certificate and Device Acquired a New Certificate Event<br>■ Added new SBC alarms: VMMaintenaceAlarm; TLS Sockets Limit Alarm<br>■ Added Alarm – Zoom Connectivity Failure alarm |
| 41812 | ■ Added: Metering Login alarm; Metering Report alarm; Metering Report event<br>■ Added Zoom alarms: |

| LTRT | Description |
|---|---|
| | ✓ Database Connectivity Failed<br>✓ Alarm - App Service Configuration failure<br>✓ Event – Ovoc Action failed<br>✓ Event – Ovoc Life Cycle<br>✓ Event – Zoom Authentication Failure<br>■ Added: Device Manager alarm Teams Pairing Required. |
| 41813 | ■ Updates to REST Formats; Updates to descriptions for SBC alarm s: the Metering Alarm, HA System Fault alarm and Temperature alarm<br>■ Added: Set Cold Start Missed Error; Failed Calls Device Alarm; Failed Calls 3rd Party Alarm; UMP Users Scheduler Suspended Alarm; UMP Users System Limit Violation Event; UCaas alarms: Event – Webhook Service Failure; Alarm – Assigned Users Count Failure; SBC Connectivity Failure; Event – SBC Action Failed; Zoom Connectivity Failure Alarm - Provider; Event – Zoom Action Failed; RTP Only Broken RTP Connection Alarm |
| 41814 | ■ Added Send CDR Destination Failure Alarm<br>■ Update to Teams Subscription Alarm on page 49<br>■ Added the following alarms:<br>✓ Outbound Calls Producer Failures per Minute Alarm on page 363<br>✓ STT Fallbacks Per Provider Alarm on page 364<br>✓ TTS Fallbacks Per Provider Alarm on page 365<br>✓ STT Delay Alarm on page 366<br>✓ Turn Delay Alarm on page 367<br>✓ TTS Delay Alarm on page 350 |
| 41815 | ■ Added the following ARM alarms:<br>✓ Certificate Expiration Alarm - ARM on page 333<br>✓ Statistics Threshold Alarm on page 334<br>✓ Blacklist Contains Numbers Alarms on page 335<br>✓ Short Calls Usage Alarm on page 336 |

# Table of Contents

# 1 Introduction

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

- Standard traps: traps originated by the device / server - all the standard traps are treated are events.
- Proprietary alarms / events: traps originated by the device / 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 managed device, 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 tgTrapGlobalsSeverity. | Condition upon which the alarm is raised for the specific severity. There may be several conditions for each severity. | Textual description of specific problem. This value is displayed from the variablebinding tgTrapGlobalsTextualDescription. The document includes a few examples of the possible values of this field. | Possible corrective action when applicable. |

# 2 Standard Events

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 no properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated. |

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

# 3 Management Alarms

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 | Run netstats command to verify which application uses the alarms reception port (by default UDP post 162).<br>■ 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.<br>■ Other network management application: change OVOC application and all managed gateways' default alarm reception ports. |
| Media Gateways | All the gateways managed by OVOC |

## GW Connection Alarm

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

| 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 | Communication problem: Try to ping the gateway to check if there is network communication.<br>■ Default gateway alive: Open the network screen. Check the default gateway IP address and ping it.<br>■ SNMP Community Strings: Verify that the community string defined in OVOC for the gateway matchs the actual gateway community strings. To check the community string, right-click on the gateway, select the 'Details' menu. Default community strings: read = public, write = private.<br>■ Hardware Problem: Check that the gateway is alive according to the LEDs. Verify that network and power cables are in place and plugged in. |
| Media Gateways | All the gateways managed by OVOC |

## GW Mismatch Alarm

| Alarm Field | Description |
|---|---|
| Description | Activated when OVOC detects a hardware, software, predefine or configuration mismatch.<br>■ 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 |

| Alarm Field | Description |
|---|---|
| | version is not defined in the Software Manager.<br>■ Hardware Mismatch: Activated when OVOC detects a hardware mismatch between the actual and the previous definition of a Media Gateway.<br>■ Configuration Mismatch: Activated when OVOC detects a configuration mismatch between the actual parameter values provisioned and previous parameter values provisioned. |
| SNMP Alarm | acEMSNoMismatchNodeAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.9 |
| Alarm Title | GW Mismatch Alarm |
| Alarm Source | ■ Media Gateway/Software<br>■ Media Gateway/Hardware<br>■ Media Gateway/Configuration |
| Alarm Type | Equipment Alarm |
| Probable Cause | Other |
| Severity | Clear |
| Additional Info | - |
| Corrective Action | ■ Software Mismatch:<br>✓ Define the detected version in the OVOC Software Manager<br>✓ Perform a Software Upgrade on the gateway with one of the supported versions.<br>■ Hardware Mismatch:<br>✓ Perform remove / add a device in order to resync OVOC and the gateway status<br>✓ Verify in the Software Manager that an appropriate version exists for the hardware type displayed in the error message<br>■ Configuration Mismatch:<br>✓ Run Configuration Verification command in order to compare OVOC configuration and actual MG configuration: |

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

## Configuration Mismatch

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

## OVOC Server Started

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

| 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 | ■ More than 70% - minor<br>■ 80-90 – major<br>■ More than 90 - critical |
| Alarm Text | {0}% of the disk is used in data partition. Free some disk space to avoid system failure. |

| Alarm Field | Description |
|---|---|
| Additional Info | |
| Corrective Action | Free disk space |

## Software Replaced

| Alarm Field | Description |
|---|---|
| Description | Originates when OVOC discovers a software version replace between board versions, for example, from V4.6.009.004 to V4.6.152.003 (when both versions are managed by OVOC). Software Replace old version : <old version> new version <new version>. |
| SNMP Alarm | acEMSSoftwareReplaceAlarm- |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.14 |
| Alarm Title | [Event] Software Replaced |
| Alarm Source | OVOCMgmt |
| 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.<br>Hardware Replace is discovered by the MAC address and performed during Board Started trap. |
| SNMP Alarm | acEMSHardwareReplaceAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.15 |
| Alarm Title | [Event] Hardware Replaced |
| Alarm Type | Equipment Alarm |
| Alarm Source | Media Gateway |
| Probable Cause | Other |
| Severity | Major |
| Additional Info | - |
| Corrective Action | - |
| Media Gateways | MediaPacks, Mediant 1000, Mediant 2000, Mediant 3000 |

## HTTP/HTTPS Access Disabled

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

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

## PM File Generated

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

| Alarm Field | Description |
|---|---|
| Media Gateways | All Gateways |

## PM Polling Error

| Alarm Field | Description |
|---|---|
| Description | Originated when a History PM stops collecting performance summary data from MG. Possible reasons are: NTP synchronization lost, Connection Loss, SW Mismatch, etc. |
| SNMP Alarm | acEMSPmHistoryAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.19 |
| Alarm Title | [Event] PM Polling Error |
| Alarm Source | OVOC Mgmt |
| Alarm Type | Other |
| Probable Cause | Other |
| Severity | Minor |
| Additional Info | - |
| Corrective Action | Verify in the 'Description' (see above) the reason why the PM history stopped.<br>■ When the reason is 'NTP synchronization lost', verify that the gateway and the OVOCserver machine are synchronized to the same NTP server and have accurate time definitions.<br>■ When the reason is 'Software Mismatch', you can stop the PM history collection until the new version is added to the Software Manager.<br>■ 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.<br>Note: The alarm continues to activate every 15 minutes unless you fix the problem or manually stop PM polling of the gateway. |
| 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 | acEMSMGBackupEvent |
| 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}<br>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 OVOCfailed 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,<br>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 | This event is issued by OVOC when a Gateway or Region is added/removed/updated in OVOC and includes the following information:<br>■ Action: Add / Remove / Update GW or Region<br>■ Region Name<br>■ GW Name<br>■ GW IP<br>**Note:** For opening an EMS client in the MG context, the gateway IP address should be provided. |
| SNMP Alarm | acEMSTopologyUpdateEvent |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.25 |
| Alarm Title | [Event] Topology Update |
| Alarm Source | OVOC Mgmt |
| Alarm Type | Other |
| Probable Cause | Other |
| Severity | Indeterminate |
| Additional Info | Additional Info 1 field will include following details:<br>Region: X1 'X2'  [GW: Y1 'Y2' 'Y3' 'Y4']<br>X1 = Region ID (unique identifier in the OVOC data base used for region identification)<br>X2 = Region name as it defined by OVOC operator<br>Y1 = GW ID (unique identifier in the OVOC data base used for GW identification)<br>Y2 = GW Name as it defined by OVOC operator<br>Y3 = GW IP as it defined by OVOC operator<br>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, |

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

## Topology File Event

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

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

## Synchronizing Alarms Event

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

| Alarm Field | Description |
|---|---|
| Corrective Action | - |
| Media Gateways | - |

## Synchronizing Active Alarms Event

| Alarm Field | Description |
|---|---|
| Description | This event is issued when OVOC is not able to perform synchronization with the History alarms table, and instead performs synchronization with the Active Alarms Table. |
| SNMP Alarm | acEMSSyncActiveAlarmEvent - |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.28 |
| Alarm Title | [Event] Synchronizing Active Alarms |
| Alarm Source | OVOC Mgmt |
| Alarm Type | Other |
| Probable Cause | Other |
| Severity | Indeterminate |
| Additional Info | - |
| Corrective Action | - |
| Media 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:<br>OVOC license key expiration date: <expiration date> |
| Corrective Action | In case the OVOC license expires:<br>■ Contact AudioCodes for new license<br>In case of the missing license in device:<br>■ If required, contact AudioCodes for new license |

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

## Suppressed Alarm <Name>

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

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

## OVOC Keep Alive Alarm

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

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

## Pre-provisioning Alarm

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

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

## Endpoint Publish Alarm

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

## Disk Space Alarm

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

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

## License Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is issued when the OVOC License approaches or reaches it's expiration date or OVOC server machine ID is no longer valid. |
| SNMP Alarm | acLicenseAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.53 |
| Alarm Title | License Alarm |
| Alarm Source | OVOC Mgmt |
| Alarm Type | Other |
| Probable Cause | Other |
| Additional Info | Info1:<br>■ Machine ID In The License Is {0}<br>■ Expiration Date In The License Is {0} |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | <text> | Corrective Action |
| Critical | The license expiration date is less than equal to 7 days. | ■ OVOC License is about to expire in {0} days.<br>■ OVOC License is about to expire in 1 day.<br>■ OVOC License Will Expire Today | Contact your AudioCodes partner ASAP. Note that when notification that this license has expired is received, the server remains connected for a few minutes in order to allow the forwarding traps to northbound destinations. |
| Major | The license expiration date is more than 7 days and less than equal to 30 days. | OVOC License is about to expire in {0} days. | |
| Clear | The license expiration date is greater than 30 days. | | |

## Synchronizing Alarms

| Alarm Field | Description |
|---|---|
| Description | This event is sent out to an SMMP NBI using user defined alarms forwarding rules once the NMS has activated the ReSync Alarms feature. |
| SNMP Alarm | ac OCReSyncEvent |

| Alarm Field | Description |
|---|---|
| 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 |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 OVOCLicense "Managed Endpoints" feature license if the endpoint is managed by IP Phone Manager Pro or from the "Voice Quality Endpoints" feature if the phones are managed in the OVOC for Voice Quality ("QOE Supported" in OVOC Web). If both of these license features are managed for the endpoint, the license is taken according to the license availability for the respective tenant license allocation. For example, if the endpoint is licensed for both of these categories and there also insufficient licenses allocated for both categories, then the dynamic license allocation is separately executed and therefore separate events are raised. |
| SNMP Alarm | floatingLicenseExtended |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.61 |
| Alarm Title | Floating License Extended |
| Alarm Source | The tenant on which the license is extended. |
| Alarm Type | Other |
| Severity | Indeterminate (info) |
| Probable Cause | Other |

## Floating License Device Report Alarm

| Alarm Field | Details |
|---|---|
| Description | This alarm is raised when the device does not send a usage report for [calc duration] minutes or more to OVOC. |
| SNMP Alarm | acClmDeviceReportAlarm |
| 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 Title | Fail to register to Cloud Service |
| Alarm Source | Floating license |
| Alarm Type | Communication |
| Severity | Critical |
| Probable Cause | Communications Protocol Error |

## Floating License Failure to Send Usage Report Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when OVOC fails in two attempts to send usage report to Floating LIcense Cloud Service Service. This service shuts down if the problem not fixed by the configured period (default 90 days).<br>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).<br>Note: this time period is configured by AudioCodes on the Floating 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 |

| Alarm Field | Description |
|---|---|
| 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 |

| Alarm Field | Description |
|---|---|
| | 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 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 |

| Alarm Field | Description |
|---|---|
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | | |
| 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> .<br>IP address already exist .<br>IP address for node name <name> changed to empty value | |
| Major | | FQDN :  <fqdn> resolved to IP: <IP> .<br>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 Field | Description | | |
|---|---|---|---|
| Alarm Source | OVOC Mgmt/ PM Handler | | |
| Alarm Title | PM Timeout Event | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Event Severity | Condition | <text> | Corrective Action |
| 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 | Message: 500,000 | Check the number of |

| Alarm Field | Description | | |
|---|---|---|---|
| | parameters polled for this interval has reached its maximum capacity. | tokens have already been used, no more DB transactions is allowed on this pm iteration. | 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 circumstances:<br>■ When a specific device is successfully polled.<br>■ For the failure scenarios described below.<br>⚠ This event is sent only when the 'Send Event per Interval' parameter is enabled in the Performance Monitoring profile. | | |
| SNMP Alarm | acDevicePmPollingEvent | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.76 | | |
| Alarm Title | PM Polling Status Event | | |
| Alarm Source | OVOC Mgmt/ PM Handle | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Indeterminate | Raised when the device is successfully polled. | Success: PM polling operation was successfully finished. deviceName=Device Name ; deviceIp= 1.1.1.1 ; pollingTimeStamp= 12:15 | - |
| Major | The time format for the device's system clock is in | Device time has not valid format | Synchronize the time settings. |

| Alarm Details | Description | | |
|---|---|---|---|
| | a different format to the time settings for the OVOC server clock. | | |
| | Device connection timeout | Device timeout | Troubleshoot the device connection. |
| | Device configuration is not synchronized | Device is not Sync | Download updated configuration to the device. |
| | Device is polled when the token pool did not have sufficient allocations. | Token pool has not enough allocations | Analyze the polling load. |
| | The device does not have a valid MIB version. | Device has not valid MIB version | Verify the device's MIB version. |
| | The device's MIB version is not supported for the PM parameter. | Device's MIB version is not supporting PM, current version= v7.0 | Refer to the Performance Monitoring Guide for the supported MIB version for the PM parameter. |
| | The OVOC server Performance Monitoring SNMP process used to manage the connection with the managed device has failed. | Device has no SNMP connection with OVOC. | Check the SNMP connection between the device and the OVOC server. |
| | A PM profile has not been assigned to the | Device is not attached to any PM profile. | Assign a PM profile to the device. |

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

## PM Batch Overflow Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| | has reached maximum capacity. | current size= 15000. Polling operation will be stopped until the buffer will be cleared. | |
| Cleared | - | - | |

## PM Has No SNMP Connection

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

## FlexPool License Usage

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when a FlexPool License parameter is approaching or has reached its maximum value. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 |
| 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 | ■ OVOC QoE/UMP User Sync<br>■ OVOC QoE/ 'name of the specific customer' |

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Alarm Title</td><td colspan="3">UMP Users Scheduler Time Exceeded Alarm</td></tr>
<tr><td>Alarm Type</td><td colspan="3">Processing Error Alarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">■ If cause type is CLEARED:<br>✓ UMP Users sync task was restarted<br>✓ UMP Users sync task for customer: 'name of the specific customer' was restarted.<br>■ If cause type is not CLEARED:<br>✓ UMP Users sync task was terminated due to exceeded time running.<br>✓ UMP Users sync task for customer: 'name of the specific customer' was failed.</td></tr>
<tr><td>Additional Info1</td><td colspan="3"></td></tr>
<tr><td>Additional Info2</td><td colspan="3"></td></tr>
<tr><td>Alarm Severity</td><td>Condition</td><td>Alarm Text</td><td>Corrective Action</td></tr>
<tr><td>Minor</td><td>■ UMP users synchronization timeout<br>■ UMP users synchronization for a specific customer failed</td><td>■ UMP Users sync task was terminated due to exceeded time running<br>■ UMP Users sync task for customer: 'name of the specific customer' was failed.</td><td>Check the connection with the Act-ive Directory.</td></tr>
<tr><td>Cleared</td><td>UMP User Synchronization success full</td><td>■ UMP Users sync task was restarted<br>■ UMP Users sync task for customer: 'name of the specific customer' was restarted.</td><td></td></tr>
</table>

## 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 | | |
| 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 | ■ Troubleshoot the network components such as firewall, DNS, certificates.<br>■ Verify that the client credentials configured for the device added in OVOC are identical to those defined by customer in Azure. |
| | 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 | |

| Alarm Field | Description | | |
|---|---|---|---|
| | | 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 | | |
| 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 | URI Storing Limit of 2000 was exceeded. | Reduce the storing limit. Note that this value cannot be changed by |

| Alarm Field | Description | | |
|---|---|---|---|
| | regexp has exceeded the limit. | | 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 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. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 Source | OVOC Mgmt/Device | | |
| Alarm Title | Teams Subscription Alarm | | |
| Alarm Type | Communications Alarm | | |
| Probable Cause | Communications Subsystem Failure | | |
| Additional Info1 | MS Cloud URL: https://graph.microsoft.com; MS Tenant: <Customer tenant ID>; MS Client: <Application (Client) ID> of the Application Registration for securing retrieval using Microsoft Teams Notification Service on the customer tenant. | | |
| Additional Info2 | | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Critical | Failed to renew (create new initial) subscription, | Subscription failed. No active subscription exists | |

| Alarm Field | Description | | |
|---|---|---|---|
| | when the previously created subscription has expired. | | |
| | 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; previously created subscription has been active for less than 48 hours (between 48 and 24 hours). | Subscription failed. Previously created subscription is active for less than 48 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. |

| Alarm Field | Description | | | |
|---|---|---|---|---|
| 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 | |
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | ■ Violated partitions: <partitioned_table>_p<range_start_time><br>Where range_start_time is in format YYYYMMDDHH<br>■ Interrupted with internal error \| Violated partitions: {partition_list}<br>■ Interrupted with internal error | | |
| Additional Info2 | | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Major | Partition range could not be created in the current timing window for <component> table. | Cannot create missing partitions for <component> table. | ■ Review PgPartitioner process-related errors including issuing event in /var/log/ems/pgpartitioner.csv<br>■ Review PostgresSQL log for details on which partition's management failed.<br>■ Check the status of the PG Partitions Manager in the OVOC Server Manager.<br>■ If the same event reoccurs for the same schema and table {schema_name}.{table_name} at successive intervals (the same event is not cleared), contact AudioCodes support. |
| 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 | Cannot remove | |

| Alarm Field | Description | | |
|---|---|---|---|
| | empty partitions of {schema_ name} schema is unsuccessful. | 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 specific database table.<br>■ Empty partitions of {NAME} schema can be removed.<br>■ Partitions distribution with schemas can be initialized.<br>■ Empty partitions of {schema_ name} schema can be removed. | | |

| Alarm Field | Description | | |
|---|---|---|---|
| | - Partitions can be created for {schema_ name}.{table_ name} table.<br>- Partitions distribution with schemas can be initialized. | | |

## Metering Login

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when OVOC is unable to login to the Metering service. | | |
| SNMP Alarm | acMeteringLoginAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.99 | | |
| Alarm Title | Metering Login | | |
| Alarm Source | Metering | | |
| Alarm Type | meteringLogin | | |
| Probable Cause | | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | Failed to verify server authenticity. | Authentication Header Not Valid. | |
| | Login Error | Login failed with error code | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | | <response code>. | |
| | Timeout | Metering server request timeout. | |

## Metering Report Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when OVOC fails to report to the Metering server. | | |
| SNMP Alarm | acMeteringReportalarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.100 | | |
| Alarm Title | Metering Report | | |
| Alarm Source | Metering | | |
| Alarm Type | meteringReport | | |
| Probable Cause | | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | OVOCfails to report to the Metering server. | Failure to report to Metering server on date [xxx], failure reason [Response Code, response text] | |

## Metering Report Event

| Alarm Field | Description |
|---|---|
| Description | This event is raised when OVOC fails to report to the Metering Server. |

| Alarm Field | Description | | |
|---|---|---|---|
| SNMP Alarm | acMeteringReportEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.101 | | |
| Alarm Title | Metering Report | | |
| Alarm Source | Metering | | |
| Alarm Type | meteringReport | | |
| Probable Cause | | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Cleared | OVOC fails to report to the Metering server. | Failure to report to metering server on date [xxx], failure reason [Response Code, response text]. | |

## Set Cold Start Missed Error

| Alarm Field | Description |
|---|---|
| Description | This event is raised when OVOC recognizes that a coldstart trap has not been sent from the device. |
| SNMP Alarm | emsAlarmsDictionaryMibNameToOID.put (acSetColdstartMissedErrorEvent) |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.108 |
| Alarm Title | ColdStart Event |
| Alarm Source | OVOC Mgmt |
| Alarm Type | Communications Alarm |
| Probable Cause | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Cleared | | Failed to reset ColdStartMissed flag on device | |

## UMP Users Scheduler Suspended Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when UMP Users sync task was suspended due to the number of users exceeding the limit of 50,000 (default) users for customer's Direct Routing or Operator Connect service. | | |
| SNMP Alarm | acUMPUsersSuspendSchedulerAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.112 | | |
| Alarm Title | UMP Users Scheduler Suspended Alarm | | |
| Alarm Source | OVOC Mgmt/Service Name | | |
| Alarm Type | Processing Error Alarm | | |
| Probable Cause | - | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | The UMP user's Sync task was suspended because the number of users exceeds the limit for the customer's service (Direct Routing and Operator Connect). | UMP Users sync task was suspended due to users amount limit violation for customer's service. The current amount of X users exceeds the limit of 50,000 (default) users. | Delete the number of users to within the limit. |

## UMP Users System Limit Violation Event

| Alarm Field | Description | | | |
|---|---|---|---|---|
| Description | This alarm is raised when the number of UMP users exceeds the valid limit for the customer service. | | | |
| SNMP Alarm | acUMPUsersSystemLimitViolationEvent | | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.113 | | | |
| Alarm Title | UMP Users System Limit Violation Event | | | |
| Alarm Source | OVOC Mgmt | | | |
| Alarm Type | Other | | | |
| Probable Cause | Other | | | |
| Additional Info | - | | | |
| Alarm Severity | Condition | Text | Corrective Action | |
| Major | The number of UMP users exceeds the valid limit for the Direct Routing or Operator Connect service. | UMP Users entire count exceeds the permitted limit. | Reduce the number of users to the valid limit. | |

# 4 Voice Quality Package Alarms

This section describes the Voice Quality Package alarms.

## OVOC QoE - Failed Calls Alarm

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Description</td><td colspan="3">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.<br>The threshold for this alarm is set in the QoE Status and Alarms Details window.</td></tr>
<tr><td>SNMP OID</td><td colspan="3">acVoice QualityRuleFailedCallsAlarm</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">1.3.6.1.4.1.5003.9.20.3.2.0.30</td></tr>
<tr><td>Alarm Title</td><td colspan="3">Voice Quality - Failed Calls Alarm</td></tr>
<tr><td>Alarm Source</td><td colspan="3">OVOC QoE/Device/Link/Site/Endpoint</td></tr>
<tr><td>Alarm Type</td><td colspan="3">Quality of service alarm.</td></tr>
<tr><td>Probable Cause</td><td colspan="3">The minimum or maximum threshold is crossed.</td></tr>
<tr><td>Additional Info</td><td colspan="3">Critical or Major severity threshold is Y%:<br>- Critical Threshold: 10 % of calls (default)<br>- Major Threshold: 2 % of calls (default)<br>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.</td></tr>
<tr><td>Alarm Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Critical</td><td>This alarm is raised when Y % of calls (rep-</td><td>Y% of failed calls has</td><td>Investigate the source (device or link) of the</td></tr>
</table>

| Alarm Field | Description | | |
|---|---|---|---|
| | representing 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.<br>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 | Critical or Major severity threshold is Y%:<br>■ Critical Threshold: 10% of calls (default).<br>■ Major Threshold: 2% of calls (default)<br>Where Y% is the % poor quality calls per managed node or link that is measured for a total time of 180 minutes period (three hours) and according to “Monitoring Frequency Min”. For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (from 12:30 to 15:30) and so on. | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | This alarm is raised when Y% (representing the configured critical threshold) of calls made by the managed node or link for the sampled period (see above) are of poor quality. | Y% calls have crossed the "Critical" threshold. | Investigate the source (device or link) of the poor quality calls. |
| Major | This alarm is raised when Y % (representing the configured major threshold) of calls by the managed node or link for the sampled period (see above) are of poor quality. | Y% calls have crossed the "Major" threshold. | |
| Clear | Cleared when the poor quality calls ratio returns below the threshold value for the sampled period (see above). | | - |

## OVOC QoE - Average Call Duration Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the average call duration time threshold for the managed node or link is crossed and is cleared when the average call duration time ratio returns below the threshold value. The description field includes the info: Average Call Duration is Y sec.<br>The threshold for this alarm is set in the QoE Status and Alarms Details window. | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.32 | | |
| SNMP Alarm | acVoice QualityRuleAvrgCallDurationAlarm | | |
| Alarm Title | Voice Quality – Average Call Duration Alarm | | |
| Alarm Source | OVOC QoE/Device/Link/Site/Endpoint | | |
| Alarm Type | Quality of service alarm | | |
| Probable Cause | The minimum or maximum threshold is crossed. | | |
| Additional Info | ■ Critical Threshold: average call duration of 3 seconds (default).<br>■ Major Threshold: average call duration of 5 seconds (default)<br>Where measured per managed node or link for a total time of 180 minutes period (three hours) and according to “Monitoring Frequency Min”. For example, if this parameter is set to 15 minutes, sampling is performed at 15:15 (from 12:15 to 15:15) and then at 15:30 (for 12:30-15:30) and so on. | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | This alarm is raised when the average call duration for the managed node or link for the sampled period (see above) falls to the configured critical | Average Call Duration "Critical" threshold has been reached. | Investigate the source (device or link) reporting the excessive average call |

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

## OVOC QoE - License Key Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is sent in the following circumstances:<br>■ When the number of devices connected to the OVOC approaches or reaches license capacity (shown as 'Devices Number' in OVOC server Manager License screen).<br>■ When the number of sessions running on the OVOC approaches or reaches license capacity (shown as 'Voice Quality Sessions' in the OVOC Server Manager License screen). |
| SNMP Alarm | acVoice QualityLicenseKeyAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.33 |
| Alarm Title | Voice Quality License key alarm |
| Alarms Source | OVOC QoE |
| Alarm Type | Other |
| Probable Cause | Key Expired |

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

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

## OVOC QoE - System Load Alarm

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

| Alarm Field | Description |
|---|---|
| | displayed. |
| SNMP Alarm | acVoice QualityCallDroppedAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.34 |
| Alarm Title | ■ Voice Quality – System Load Alarm |
| Alarm Source | OVOC QoE |
| Alarm Type | Quality of service alarm |
| Probable Cause | AlarmProbableCauseType.THRESHOLDCROSSED |
| Severity | MINOR/ MAJOR/ CRITICAL |
| Additional Info | ■ Medium load level is reached - {0}%, {1} calls of {2}. /<br>■ High load level is reached - {0}%, {1} calls of {2}. /<br>■ Approaching maximal system capacity - {0}%, {1} calls of {2}. |
| Corrective Action | Reduce the system load. |

## Call Details Storage Level Change

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

| Alarm Field | Description |
|---|---|
| Severity | Indeterminate |
| Additional Info | - |
| Corrective Action | - |

## Call Quality Monitoring Connection Status Alarm

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Description</td><td colspan="3">This alarm is sent when connectivity is lost between the managed device and Voice Quality Package server.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">acSEMConnectionStatusAlarm</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.20.3.2.0.36</td></tr>
<tr><td>Alarm Title</td><td colspan="3">Voice Quality – OVOC QoE - Connection Status Alarm</td></tr>
<tr><td>Alarm Source</td><td colspan="3">OVOC QoE/Device</td></tr>
<tr><td>Alarm Type</td><td colspan="3">communicationsAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">communicationsSubsystemFailure</td></tr>
<tr><td>Additional Info</td><td colspan="3">One of the following reasons will appear:<br>■ Server Time: {0}, Device Time: {1}.<br>■ Please check your NTP Configuration in Device.<br>■ NTP Servers are not configured in the Device.<br>■ Please make sure that time in OVOC QoE Server and Device is properly synchronized.<br>■ 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.<br>■ 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.</td></tr>
<tr><td>Alarm</td><td>Condition</td><td>Text</td><td>CorrectiveAction</td></tr>
</table>

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

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

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

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

## OVOC QoE - Active Directory Server Connection Lost Alarm

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

## OVOC QoE - Media Bandwidth Alarm

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

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

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

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

## OVOC QoE - Rule Max Concurrent Calls Alarm

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

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

## Report Schedulers Time Event

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

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

## Report Schedulers Load Alarm

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

## Report Schedulers Execution Event

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

## Failed Calls 3rd Party Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the % number of failed calls for the managed **3rd Party** device crosses the threshold and is cleared when the failed calls ratio returns below the threshold value. The description field includes the info: Failed X1% of calls, X2 of X3 calls. The alarm is raised according to the configuration of the list of the Failed Called Reason originated by 3rd party devices (see Failed Call Reasons).<br>The custom threshold for **3rd Party** devices is set in the QoE Status and Alarms Details window. See QoE Status |

| Alarm Field | Description | | |
|---|---|---|---|
| | and Alarms. | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.111 | | |
| SNMP Alarm | acSEMRuleFailedCalls3rdPartyAlarm | | |
| Alarm Title | Failed Calls 3rd Party Alarm | | |
| Alarm Source | OVOC QoE/Device | | |
| Alarm Type | Quality Of Service Alarm | | |
| Probable Cause | Threshold Crossed | | |
| Additional Info 1 | 0} severity threshold is {1}. | | |
| Additional Info 2 | Time interval: {0} - {1}. | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | This alarm is raised when Y % of calls (representing the configured critical threshold) made by the managed device for the sampled period fail (see above). | Y% of failed calls has crossed the "Critical" threshold | Investigate the source of the failed calls according to the list of Failed Call Reasons originated by 3rd party devices. |
| Major | This alarm is raised when Y % of calls (representing the configured major threshold) made by the managed device for the sampled period fail (see above). | Y% number of failed calls for has crossed the "Major" threshold. | Investigate the source of the failed calls according to the list of Failed Call Reasons originated by 3rd party devices. |
| Clear | Cleared when the | | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | failed calls ratio returns below the threshold value for the sampled period. | | |

## Failed Calls Device Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the % number of failed calls for the managed **AudioCodes** device crosses the threshold and is cleared when the failed calls ratio returns below the threshold value. The description field includes the info: Failed X1% of calls, X2 of X3 calls. The alarm is raised according to the configuration of the Failed Called Reason Originated by Device (AudioCodes device). See Failed Call Reasons.<br>The custom threshold for **AudioCodes** devices is set in the QoE Status and Alarms Details window. See QoE Status and Alarms. | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.110 | | |
| SNMP Alarm | SEMRuleFailedCallsDeviceAlarm | | |
| Alarm Title | QoE: Failed Calls Device Alarm | | |
| Alarm Source | OVOC QoE/Device | | |
| Alarm Type | Quality Of Service Alarm | | |
| Probable Cause | Threshold Crossed | | |
| Additional Info 1 | {0} severity threshold is {1}. | | |
| Additional Info 2 | Time interval: {0} - {1}. | | |
| Alarm Severity | Condition | Text | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Critical | This alarm is raised when Y % of calls (representing the configured critical threshold) made by the managed device for the sampled period fail (see above). | Y% of failed calls has crossed the "Critical" threshold | Investigate the source of the failed calls according to the list of Failed Call Reasons originated by the device. |
| Major | This alarm is raised when Y % of calls (representing the configured major threshold) made by the managed device for the sampled period fail (see above). | Y% number of failed calls for has crossed the "Major" threshold. | Investigate the source of the failed calls according to the list of Failed Call Reasons by the device. |
| Clear | Cleared when the failed calls ratio returns below the threshold value for the sampled period. | | - |

# 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<br>NtpServerError |
| Corrective Action | This alarm may typically occur if the user is not registered - or is registered incorrectly - in the Lync Server. Make sure that username, password and PIN code are correctly configured and valid in the Lync Server. Try resetting them. Try redefining the user. |

## Endpoint License Alarm

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

| Alarm Field | Description |
|---|---|
| Description | This alarm is issued for the following scenarios:<br>■ 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.<br>■ When the number of managed endpoints currently running on the OVOC server (shown in the License screen License screen) approaches or reaches its license capacity. |
| SNMP Alarm | acEndpointLicenseAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.48 |
| Alarm Title | Endpoint License Alarm |
| Alarm Source | Voice Quality/Management |
| Alarm Type | Other |
| Probable Cause | Key Expired |
| Additional Info | Endpoint License capacity {0} devices. |
| Corrective Action | Contact your AudioCodes partner ASAP |

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

| Alarm Field | Description | | |
|---|---|---|---|
| | alarm | currently active alarm. | |

## Endpoint Server Overloaded Alarm

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

## IP Phone Speaker Firmware Download Failure

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

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

## IP Phone Speaker Firmware Upgrade Failure

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the phone fails to load the firmware to the HRS speaker. |
| SNMP Alarm | IP PhoneSpeakerFirmUpgradeFailure |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.55 |
| Alarm Title | IP Phone Speaker Firmware Upgrade Failure |
| Alarm Source | The IP Phone |
| Alarm Type | communicationsAlarm(1) |
| Probable Cause | communicationsProtocolError(5) |
| Severity | Major, Clear |
| Additional Info | - |
| Corrective Action | ■ Verify the USB connection between the phone and the HRS speaker.<br>■ Verify the firmware file is compatible with the HRS speaker. |

## IP Phone Conference Speaker Connection Failure

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

## IP Phone General Local Event

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

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

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

## IP Phone Web Successive Login Failure

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

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when there are five successive failed login attempts to an IP phone's Web interface. | | |
| SNMP Alarm | IPPhoneWebSuccessiveLoginFailure | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.59 | | |
| Alarm Title | IP Phone Web Successive Login Failure | | |
| Alarm Source | The IP Phone | | |
| Alarm Type | SecurityServiceOrMechanismViolation(9) | | |
| Probable Cause | UnauthorizedAccessAttempt(73) | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | Issued on the fifth successive failed attempt to log in to the phone's Web interface | - | ■ After the alarm is cleared, try to login to the Web interface using the correct username and password. |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | ■ If you forget the login credentials, inform the network administrator. |
| Clear | There are no additional WEB login failed trials during a specific time period (60 seconds) after sending the alarm. | - | - |

## IP Phone Requires Reset

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

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

## Jabra Firmware Upgrade Failed

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

## VIP Endpoint is Not Registered or Offline

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

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

## VIP Endpoint is Disconnected

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

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

## 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 | ippRemoteControlIsNotConnected | | |
| 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 dis-connected | Refer to the RXV80 manual and try to re-pair the remote con-troller. |
| 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 | 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.<br>This alarm is relevant for the following bundled peripherals:<br>- RX50<br>- RXVCAM50L<br>- RXVCAM50M<br>- RXVCAM10<br>- RX10<br>- RX15 |
| 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><br>For example:<br>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 | | | |

## Device Acquired a New Certificate Event

| Alarm Field | Description |
|---|---|
| Description | Device acquired a new Device_Certificate, CA_Certificate or Root_CA_Certificate by SCEP provisioning. |
| SNMP Alarm | ippAcquiredANewSignedCertificate |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.102 |
| Alarm Title | Device Acquired a New Certificate [Event] |
| Alarm Source | ■ source format: IPPhone/<source_component>/<MAC><br>■ source_component part 1: Device_Certificate, CA_Certificate, Root_CA_Certificate<br>■ source_component part 2: /SCEP/, /Provisioning/ |
| Alarm Type | Other |
| Probable Cause | Other |
| Additional | Certificate details: Subject, Issuer, SN, Expiration date |

| Alarm Field | Description |
|---|---|
| Info1 | |
| Additional Info2 | |
| Severity | Indeterminate |

## Device Fails to Get Certificate

| Alarm Field | Description |
|---|---|
| Description | Device fails to acquire Device_Certificate, CA_Certificate or Root_CA_Certificate by SCEP due to Client error. |
| SNMP Alarm | ippFailsToGetASignedCertificate |
| SNMP OID | .1.3.6.1.4.1.5003.9.20.3.2.0.103 |
| Alarm Title | Device fails to get certificate |
| Alarm Source | ■ source format: IPPhone/<source_component>/<MAC><br>■ source_component part 1: Device_Certificate, CA_Certificate, Root_CA_Certificate (future)<br>■ source_component part 2: /SCEP/, /Provisioning/ |
| Alarm Type | CommunicationsAlarm |
| Probable Cause | CommunicationsProtocolError |
| Additional Info1 | Failure reason:<br>■ Wrong root certificate fingerprint<br>■ NDES Server failed to verify the request<br>■ Gotten local cert is not valid<br>■ NDES server error. Response code is X<br>■ Client Error. Response code is X<br>■ Reject response. Return code: X (in case of provisioning) |
| Additional Info2 | |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Major | Device fails to acquire a new CA certificate by SCEP due to Client error. | Device fails to acquire CA Certificate by SCEP due to Client Error. Response Code is 600 | |
| Major | Device fails to acquire CA_Certificate by provisioning due to problems with Root_CA_Certificate, CA_Certificate, and Device_Certificate. | Device fails to acquire CA_Certificate by provisioning due to"Root_CA_Certificate" "CA_Certificate" "Device_Certificate" "Reject response. Return code: nnn" | |

## Teams Pairing Required

| Alarm Field | Description |
|---|---|
| Description | Console device e.g. RX-PAD is not paired with its Host model. |
| SNMP Alarm | ippTeamsPairingRequired |
| SNMP OID | 1.3.6.1.4.1.5003.9.20.3.2.0.109 |
| Alarm Title | Teams pairing Required |
| Alarm Source | PhoneProxyTeams |
| Alarm Type | Communication Alarm |
| Probable Cause | COMMUNICATIONS_PROTOCOL_ERROR |
| Additional Info1 | PhoneProxyTeams |
| Additional Info2 | |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Major | Teams console is not paired with its Host model. | Teams console is not paired with <Host_ Model) e.g. RXV200/RXV81 in Teams-Level. Please pair console with <Host Model> serial number < HostModel serial number > | Pair console with it’s Host model. |
| Cleared | | | |

# 6 OVOC Managed Devices Alarms

This section describes the OVOC Managed Devices alarms.

## Support Matrix for AudioCodes SBC Alarms

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

| Alarm Type | Supported Device Types |
|---|---|
| Common Alarms | All the alarms in Section Common Alarms are supported by all AudioCodes devices. |
| Specific Hardware Alarms | ■ Mediant 2600 E-SBC<br>■ Mediant 4000 SBC<br>■ Mediant 1000<br>■ MP-1288 |
| Temperature Alarm | ■ Mediant 1000<br>■ Mediant 2600<br>■ Mediant 4000 |
| Fan Tray Alarm on page 155 | ■ MP-1288<br>■ Mediant 1000<br>■ Mediant 2600<br>■ Mediant 4000 |
| Power Supply Alarm on page 156 | ■ MP-1288<br>■ Mediant 1000<br>■ Mediant 2600<br>■ Mediant 4000. |
| HA System Alarms | ■ Mediant 500 E-SBC<br>■ Mediant 800B GW & E-SBC<br>■ Mediant 3000/TP-6310 |

| Alarm Type | Supported Device Types |
|---|---|
| | ■ Mediant 3000/TP-8410<br>■ Mediant 2600 E-SBC<br>■ Mediant 4000 SBC<br>■ Mediant 4000B SBC (3 x MPM)<br>■ Mediant 9000 SBC<br>■ Mediant VE SBC<br>■ Mediant SE SBC |
| HA System Fault Alarm | As above |
| HA System Configuration Mismatch Alarm on page 166 | As above |
| HA System Switch Over Alarm on page 167 | As above |
| Hitless Software Upgrade Alarm on page 168 | ■ Mediant 2600 E-SBC<br>■ Mediant 4000 SBC<br>■ Mediant SE SBC<br>■ Mediant VE SBC |
| Redundant Board Alarm on page 169 | As above |
| HA Network Watchdog Status Alarm on page 170 | As above |
| HA Network Watchdog Status Alarm on page 170 | As above (except Mediant 3000) |
| Cluster HA Alarm on page 184 | ■ Media Transcoding Cluster feature (Mediant 9000 SBC and Mediant VE SBC) |
| HA Network Mismatch Alarm on page 172 | ■ Mediant VE SBC on AWS |

| Alarm Type | Supported Device Types |
|---|---|
| | ■ Mediant SE SBC on AWS |
| HA Network Monitor Alarm on page 172 | As above |
| HA Ethernet Group Alarm on page 173 | As above (except Mediant 3000) |
| License Pool Alarms | Supported by all devices from Version 7.0, except for the Mediant 2000 and Mediant 3000. In addition, the Transcoding session license is applicable only to the Mediant Virtual Edition and Mediant 9000. |
| License Pool Infra Alarm on page 174 | As above |
| License Pool Application Alarm on page 176 | As above |
| License Pool Over Allocation Alarm on page 177 | As above |
| Floating License Alarms | Refer to the OVOC Release Notes for device support information. |
| Cloud License Manager Alarm on page 179 | Supported for the Floating License "Cloud" mode. |
| Floating License Alarm - Not Enough Memory to Allocate 'Custom' Profile on page 178 | Supported for the Floating License "Cloud" mode. |
| Flex License Manager Alarm on page 181 | Supported for the Floating License "FlexPool" mode. |
| Mediant 2600 E-SBCand Mediant 4000 Alarms SBC | |
| DSP Farms Mismatch Alarm on page 182 | ■ Mediant 2600 E-SBC<br>■ Mediant 4000 SBC |

| Alarm Type | Supported Device Types |
|---|---|
| Mediant 9000 and Software SBC Alarms | ■ Mediant 9000 SBC<br>■ Mediant VE SBC<br>■ Mediant SE SBC<br>■ Mediant CE SBC |
| Media Transcoder Network Failure on page 185 | ■ Media Transcoding Cluster feature (Mediant VE SBC and Mediant 9000 SBC)<br>■ Elastic Media Cluster feature (Mediant CE SBC) |
| Media Transcoder Software Upgrade Failure on page 186 | ■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)<br>■ Elastic Media Cluster feature (Mediant CE SBC) |
| Media Transcoder High Temperature Failure on page 186 | ■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC) |
| Media Transcoder Fan Tray Module Failure on page 187 | ■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC) |
| Media Transcoder Power Supply Module Failure on page 188 | ■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC) |
| Cluster Bandwidth Utilization Alarm on page 189 | ■ Media Transcoding Cluster feature (Mediant 9000 and Mediant VE SBC)<br>■ Elastic Media Cluster feature (Mediant CE SBC) |
| Media Cluster Alarm on page 191 | ■ Elastic Media Cluster feature (Mediant CE SBC) |
| Remote Interface Alarm on page 192 | ■ Elastic Media Cluster feature (Mediant CE SBC) |
| AWS Security Role Alarm on page 193 | ■ Mediant VE SBC and Mediant CE SBC |
| CDR Server Alarm on page 194 | ■ As above |
| Metering Alarm | ■ Mediant VE when deployed through the AWS Marketplace |

| Alarm Type | Supported Device Types |
|---|---|
| MC Not Secured Alarm on page 196 | ■ Mediant CE SBC |
| TLS Certificate Mismatch Alarm on page 198 | ■ Mediant CE SBC |
| MP-1288 Alarms | ■ MP-1288 (not supported by the OVOC License Pool Manager) |
| Module Service Alarm on page 207 | As above |
| Module Operation Alarm on page 208 | As above |
| Port Service Alarm on page 209 | As above |
| MSBR Alarms | Mediant 1000B MSBR, Mediant 800 MSBR Mediant MSBR 500L and Mediant 500 MSBR (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform [1])' Mediant 500Li MSBR |
| WAN Link Alarm on page 210 | As above |
| Power Over Ethernet Status [Event] on page 211 | Mediant 800 MSBR |
| Wireless Cellular Modem Alarm on page 212 | ■ Mediant 500 MSBR<br>■ Mediant 500L MSBR<br>■ Mediant 800 MSBR |
| Wireless Cellular Modem Status Changed on page 212 | ■ Mediant 500 MSBR<br>■ Mediant 500L MSBR<br>■ Mediant 800 MSBR |
| Data Interface Status on page 213 | As above |

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

| Alarm Type | Supported Device Types |
|---|---|
| NQM Connectivity Alarm on page 214 | Mediant 800 MSBR |
| NQM RTT Alarm on page 214 | Mediant 800 MSBR |
| NQM Jitter Alarm on page 215 | Mediant 800 MSBR |
| NQM Packet Loss Alarm on page 216 | Mediant 800 MSBR |
| NQM MOS CQ Alarm on page 217 | Mediant 800 MSBR |
| NQM MOS LQ Alarm on page 218 | Mediant 800 MSBR |
| Mediant 3000 Hardware Alarms | ■ Mediant 3000/TP-6310<br>■ Mediant 3000/TP-8410 |
| PEM Module Alarm on page 219 | As above |
| SA Module Missing Alarm on page 220 | As above |
| User Input Alarm on page 221 | As above |
| TM Inconsistency on page 221 | As above |
| TM Reference Status on page 222 | This alarm applies only  to the Mediant 3000 using the BITs Synchronization Timing mode. |
| TM Reference Change on page 223 | As above |
| PSTN Trunk Alarms | ■ Mediant 500 Gateway & E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 800B Gateway & E-SBC |

| Alarm Type | Supported Device Types |
|---|---|
| | ■ Mediant 800B MSBR<br>■ Mediant 1000B Gateway & E-SBC<br>■ Mediant 3000<br>⚠ For version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform[1]) |
| D-Channel Status on page 223 | As above |
| SONET Section LOS Alarm on page 225 | ■ Mediant 3000/TP-6310 |
| SONET Line AIS Alarm on page 226 | ■ Mediant 3000/TP-6310 |
| SONET Line RDI Alarm on page 227 | ■ Mediant 3000/TP-6310 |
| SONET/SDN IF Failure Alarm on page 227 | ■ Mediant 3000/TP-6310 |
| Trunk LOS Alarm on page 228 | ■ Mediant 500 E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 800B Gateway & E-SBC<br>■ Mediant 800B MSBR<br>■ Mediant 850 MSBR<br>■ Mediant 1000B MSBR<br>■ Mediant 1000B GW & E-SBC<br>■ Mediant 3000/TP-8410 |
| Trunk LOF Alarm on page 229 | ■ Mediant 500 E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 800B Gateway & E-SBC |

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

| Alarm Type | Supported Device Types |
|---|---|
| | ■ Mediant 800B MSBR<br>■ Mediant 850 MSBR<br>■ Mediant 1000B MSBR<br>■ Mediant 1000B GW & E-SBC<br>■ Mediant 3000/TP-8410 |
| Trunk AIS Alarm on page 230 | ■ Mediant 500 E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 800B Gateway & E-SBC<br>■ Mediant 800B MSBR<br>■ Mediant 850 MSBR<br>■ Mediant 1000B MSBR<br>■ Mediant 1000B GW & E-SBC<br>■ Mediant 3000/TP-8410 |
| Trunk RAI Alarm on page 230 | ■ Mediant 500 E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 800B Gateway & E-SBC<br>■ Mediant 800B MSBR<br>■ Mediant 850 MSBR<br>■ Mediant 1000B MSBR<br>■ Mediant 1000B GW & E-SBC<br>■ Mediant 3000/TP-8410 |
| V5.2 Interface Alarm on page 231 | ■ Mediant 3000/TP-8410 |
| SONET Path STS LOP Alarm on page 232 | ■ Mediant 3000/TP-6310 |
| SONET Path STS AIS Alarm on page 233 | ■ Mediant 3000/TP-6310 |
| SONET Path STS RDI Alarm on page 233 | ■ Mediant 3000/TP-6310 |

| Alarm Type | Supported Device Types |
|---|---|
| SONET Path Unequipped Alarm on page 234 | ■ Mediant 3000/TP-6310 |
| SONET Path Signal Label Alarm on page 235 | ■ Mediant 3000/TP-6310 |
| SONET Path Signal Label Alarm on page 235 | ■ Mediant 3000/TP-6310 |
| DS1 Line Status Alarm on page 235 | As above |
| DS3 AIS Alarm on page 237 | ■ Mediant 3000/TP-6310 |
| DS3 LOF Alarm on page 238 | ■ Mediant 3000/TP-6310 |
| DS3 LOS Alarm on page 238 | ■ Mediant 3000/TP-6310 |
| NFAS Group Alarm on page 239 | As above |
| B Channel Alarm on page 240 | As above |
| Analog Port Alarms | ■ Mediant 500 E-SBC<br>■ Mediant 500L E-SBC<br>■ Mediant 500 MSBR<br>■ Mediant 500L MSBR<br>■ Mediant 500L GW & E-SBC<br>■ Mediant 800B Gateway & E-SBC<br>■ Mediant 800B MSBR<br>■ Mediant 850 MSBR<br>■ Mediant 1000B MSBR<br>■ Mediant 1000B GW & E-SBC |

| Alarm Type | Supported Device Types |
|---|---|
| | ■ (for version 7.2 and later, MSBR and E-SBC are separate applications that reside on the same host platform[1]) |
| Analog Port SPI Out of Service on page 241 | As above |
| Analog Port High Temperature on page 241 | As above |
| Analog Port Ground Fault Out-of-Service Alarm on page 242 | As above |
| Dial Plan File Replaced Trap on page 242 | As above |
| Analog Line Left Off Hook Alarm on page 243 | 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 |
| Probable Cause | underlyingResourceUnavailable (56) |

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

| Alarm Field | Description | | |
|---|---|---|---|
| Additional Info | - | | |
| Alarm Severity | Condition | Text | CorrectiveAction |
| Critical (default) | Any fatal error | Board Fatal Error: A run-time specific string describing the fatal error | ■ Capture the alarm information and the Syslog clause, if active.<br>■ Contact AudioCodes' Support Center at support@AudioCodes.com which will want to collect additional data from the device and perform a restart. |
| 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 |
| Additional Info1,2,3 | - |

| Alarm Field | Description |
|---|---|
| Corrective Action | - |

## Configuration Error

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

## Initialization Ended

| Alarm Field | Description |
|---|---|
| Description | This alarm is sent when the device is initialized and ready to run. |

| Alarm Field | Description |
|---|---|
| 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 restart process - following a software restart. | | |
| 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 restart through the Web interface or SNMP | "Device is resetting" | A network administrator has restart the device. Corrective action is not required. The alarm remains at Critical severity level until the device completes the reboot. A Clear trap is not sent. |

## Feature Key Related Error

**Table 6-1: Feature Key Related Error**

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

## Gateway Administrative State Changed

| Alarm Field | Description |
|---|---|
| Description | This alarm indicates that the administrative state of the gateway has been changed to a new state.<br>⚠ All state changes are instigated by the parameter acgwAdminState.<br>■ Time limit set in the parameter acgwAdminStateLockControl - 'GateWay shutting down. Max time to LOCK %d sec'<br>■ No time limit in the parameter acgwAdminStateLockControl - 'GateWay is shutting down. No time limit.'<br>■ When reaching lock state - 'GateWay is locked'<br>■ When the gateway is SET to unlocked - 'GateWay is unlocked (fully active again)' |
| SNMP Alarm | acgwAdminStateChange |

| Alarm Field | Description | | |
|---|---|---|---|
| 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.<br>A network administrator took an action to gracefully lock the device. |
| Major | Admin state changed to locked | Locked | No corrective action is required.<br>A network administrator took an action to lock the device, or a graceful lock timeout occured. |
| Cleared | Admin state changed to unlocked | - | No corrective action is required.<br>A network 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)<br>-OR-<br>Reduce traffic |
| Cleared | Percentage of busy channels falls below the predefined RAI low threshold | - | Note that to enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated (EnableRAI = 1). |

## Gatekeeper/Proxy not Found or Registration Failed

| Alarm Field | Description |
|---|---|
| Description | The alarm is sent in the following scenarios:<br>■ 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.) |

| Alarm Field | Description | | |
|---|---|---|---|
| | ■ Physical BRI or PRI (E1/T1) port is up or down (OOS).<br>■ 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.<br>■ Connection to the Proxy is up or down.<br>■ Failure in TDM-over-IP call - transparent E1/T1 without signalling.<br>■ Connection to the Proxy Set associated with the trunk/line is up/down.<br>■ Failure in server registration for the trunk/line.<br>■ Failure in a Serving IP Group for the trunk.<br>■ Failure in a Proxy Set. | | |
| SNMP Alarm | acBoardControllerFailureAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.9 | | |
| Alarm Source | 'GWAPP' | | |
| Alarm Title | Proxy not Found or Registration Failed | | |
| Alarm Type | processingErrorAlarm | | |
| Probable Cause | softwareError (46) | | |
| Alarm Severity | Condition | Text | Additional Information |
| Major (default) | FXO physical port is down | "BusyOut Line n Link failure"<br>Where n represents the FXO port number (0 for the first port). | ■ Verify that the FXO line is securely cabled to the device's FXO port. |
| | BRI or PRI physical port is down | "BusyOut Trunk n Link failure"<br>Where n represents the BRI or PRI port | Verify that the digital trunk is securely cabled to the device's digital port. |

| Alarm Field | Description | | |
|---|---|---|---|
| | | number (0 for the first port). | |
| | Proxy has not been found or registration failure | "Proxy not found. Use internal routing"<br>-OR-<br>"Proxy lost. Looking for another Proxy" | ■ Check the network layer<br>■ Make sure that the proxy IP and port are configured correctly. |
| | Connection to Proxy is down | "BusyOut Trunk/Line n Connectivity Proxy failure" | - |
| | Connection to the Proxy Set associated with the trunk or line is down | "BusyOut Trunk/Line n Proxy Set Failure"<br>Where n represents the BRI/ PRI trunk or FXO line. | - |
| | Failure in a Proxy Set | "Proxy Set ID n"<br>Where n represents the Proxy Set ID. | - |
| | Failure in TDM-over-IP call | "BusyOut Trunk n TDM over IP failure (Active calls x Min y)"<br>Where n represents the BRI/ PRI trunk. | - |
| | Failure in server registration for | "BusyOut | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | the trunk/line | Trunk/Line n Registration Failure"<br>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"<br>Where n represents the BRI or PRI trunk ID. | - |
| Cleared | Proxy is found. The 'Cleared' message includes the IP address of this Proxy. | - | - |

## Ethernet Link Down Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm indicates that the Ethernet link is down or remote Ethernet link is down and the board has no communication to any other host.<br>■ No link at all.<br>■ Link is up again.<br>■ Primary link is down only - 'Primary Link is lost. Switching to Secondary Link' |
| SNMP Alarm | acBoardEthernetLinkAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.10 |
| Alarm Title | Ethernet Link Down Alarm |
| Alarm Source | All except Mediant 3000: Board#<n>/EthernetLink#0 (where n is the slot number)<br>Mediant 3000: Chassis#0/Module#<n>/EthernetLink#0 (where n is the blade's slot number) |

| Alarm Field | Description | | |
|---|---|---|---|
| | This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link). | | |
| Alarm Type | equipmentAlarm | | |
| Probable Cause | underlyingResourceUnavailable (56) | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | Fault on single interface | Ethernet link alarm:<br>Redundant link is down | ■ Ensure that both Ethernet cables are plugged into the back of the system.<br>■ Observe the system’s Ethernet link lights to determine which interface is failing.<br>■ Reconnect the cable or fix the network problem |
| Critical (default) | Fault on both interfaces | No Ethernet link | |
| Cleared | Both interfaces are operational | - | Note that the alarm behaves differently when coming from the redundant or the active modules of a High Availability (HA) system. The alarm from the redundant is raised when there is an operational HA configuration in the system. There is no critical severity for the redundant module losing both its Ethernet links as that is conveyed in the no HA alarm that follows such a case. |

## System Component Overloaded

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when there is an overload in one or more of the system's components. |
| SNMP Alarm | acBoardOverloadAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.11 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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”<br>Where %d is the percentage of available CPU resources remaining | ■ Make sure that the syslog level is 0 (or not high).<br>■ Make sure that DebugRecording is not running.<br>■ If the system is configured correctly, reduce traffic. |
| Cleared | The overload condition passed | “System CPU overload condition - IdleUtilization percentage=%” | - |

## Active Alarms Table Overflow

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

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when there are too many alarms to fit into the active alarm table. The status stays major until reboot as it denotes a possible loss of information until the next reboot. If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table. |
| SNMP Alarm | acActiveAlarmTableOverflow |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.12 |

| Alarm Field | Description |
|---|---|
| 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 Severity | Condition | Text | Corrective Action |
| Major (default) | Operational state changed to disabled | Node {elementName} was marked as {status} | ■ In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the |

| | | | |
|---|---|---|---|
| | | | device fails to properly initialize.<br>■ Look for other alarms and Syslogs that might provide additional information about the error. |
| Cleared | Operational state changed to available | - | In case state is unavailable:<br>■ Validate that Node is available in WEB interface / OVOC<br>■ Check device network connectivity<br>■ Check the device's network connectivity to the ARM Configurator<br>■ Validate that proper Node credentials updated in ARM<br>In case state is logged out:<br>■ Check the ARM configuration in the device<br>In case state is Unrouteable:<br>■ Check the device network connectivity to the ARM routers<br>■ Check router status and availability |

## Keep Alive Trap

| Alarm Field | Description |
|---|---|
| Description | Part of the NAT traversal mechanism. If the STUN application in the device detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the device. |
| SNMP Alarm | acKeepAlive |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.16 |

| Alarm Field | Description |
|---|---|
| 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 Type | other (0) |
| Alarm Source | MG |
| Probable Cause | other (0) |

| Alarm Field | Description |
|---|---|
| Severity | Indeterminate |
| Additional Info1,2,3 | - |
| Status Changes | The STUN client in the device is enabled and has either identified a NAT or is not finding the STUN server.<br>Keep-alive is sent out every 9/10 of the time defined in the 'NatBindingDefaultTimeout' parameter. |
| Corrective Action | See http://tools.ietf.org/html/rfc5389 |

## Enhanced BIT Status Trap

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

## Threshold of Performance Monitored Object Exceeded

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

## HTTP Download Result

| Alarm Field | Description |
|---|---|
| Description | This is a log message (not alarm) indicating both sucessful and failed HTTP Download result. |
| SNMP Alarm | acHTTPDownloadResult |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.28 |
| Alarm Title | [Event] HTTP Download Result |
| Alarm Source | - |

| Alarm Field | Description |
|---|---|
| Alarm Type | processingErrorAlarm (3) for failures and other (0) for success |
| Probable Cause | Other |
| Severity | Indeterminate |
| Additional Info | There are other possible textual messages describing NFS failures or success, FTP failure or success. |
| Corrective Action | - |

## IPv6

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

| Alarm Field | Description | | |
|---|---|---|---|
| Stays 'Critical' until reboot.<br>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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | | |
| Probable Cause | communicationsSubsystemFailure | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Major (default) | No initial | NTP server alarm. No connection to | Repair NTP communication (the NTP server is down or |

| Alarm Field | Description | | |
|---|---|---|---|
| | communication to Network Time Protocol (NTP) server. | NTP server. | 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<br>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 | ■ Repair the Online Certificate Status Protocol (OCSP) server<br>-OR- |

| 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. | Either:<br>■ The device certificate has expired %d days ago<br>■ The device certificate will expire in %d days<br>■ The device certificate will expire in less than 1 day<br>%d – number of days<br>%d – TLS Context to which certificate belongs | Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically).<br>To replace certificates, refer to the device's User's Manual. |

## Web User Access Disabled

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

## Proxy Connection Lost

| Alarm Field | Description |
|---|---|
| Description | This alarm is sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up. |
| SNMP Alarm | acProxyConnectionLost |
| 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 | ■ Network issue (connection fail due to network/routing failure).<br>■ Proxy issue (proxy is down).<br>■ AudioCodes device issue. | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | When connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table. | Proxy Set %d: Proxy not found. Use internal routing | ■ Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.<br>■ Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.<br>■ 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.<br>■ Check that routing using the device's (internal) routing table is functioning correctly.<br>■ Contact AudioCodes support center (support@AudioCodes.com) and send a syslog and network capture for this issue. |
| Major | When Proxy Set includes | Proxy Set %d: Proxy lost. | ■ Ping the proxy server. If there is no ping, contact your |

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

## IDS Policy Alarm

| Alarm Field | Description |
|---|---|
| Description | The alarm is raised whenever a threshold is crossed in the IDS system.<br>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 | ■ Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm.<br>■ Locate the remote hosts (IP addresses) that are specified in the traps.<br>■ Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation.<br>■ If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table. |

## IDS Threshold Cross Notification

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

| Alarm Field | Description |
|---|---|
| Alarm Text | Threshold cross for scope value IP. Severity=minor/major/critical. Current value=NUM |
| Status Changes | - |
| Corrective Action | ■ Identify the remote host (IP address / port) on the network which the Intrusion Detection System (IDS) has indicated is malicious<br>■ Note that the IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks(counter).<br>■ Block the malicious activity |

## IDS Blacklist Notification

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

| Alarm Field | Description |
|---|---|
| | ⚠ A host is determined to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). The malicious source is automatically blacklisted for a user-defined period, after which it is removed from the blacklist. |

## Proxy Connectivity

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Description</td><td colspan="3">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.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">acProxyConnectivity</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.10.1.21.2.0.102</td></tr>
<tr><td>Alarm Source</td><td colspan="3">System#0</td></tr>
<tr><td>Alarm Type</td><td colspan="3">communicationsAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">■ Network issue (connection fail due to network/routing failure).<br>■ Proxy issue (proxy is down).<br>■ AudioCodes device issue.</td></tr>
<tr><td>Alarm Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Indeterminate</td><td>When connection to the proxy server is lost.</td><td>Proxy server &lt;IP address&gt;:&lt;port&gt; is now OUT OF SERVICE</td><td>■ Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.<br>■ Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.<br>■ If you have more than one device connected to this same proxy, check if there are more AudioCodes</td></tr>
</table>

| Alarm Field | Description | | |
|---|---|---|---|
| | | | devices with the same trap event. If this is the case, this could confirm that this is not AudioCodes device issue.<br>■ Contact AudioCodes support center (support@AudioCodes.com) and send a syslog and network capture for this issue. |
| Cleared | When connection to the proxy is available again | Proxy server <IP address>:<port> is now IN SERVICE | |

## Web User Activity Log Trap

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

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

## HTTP Proxy Service Alarm

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

| Alarm Fields | Description | | |
|---|---|---|---|
| | | name) is OFFLINE" | work/router issue.<br>3. Check that routing using the device's (internal) routing table is functioning correctly.<br>4. Contact AudioCodes support center (support@AudioCodes.com) and send a syslog and network capture for this issue. |
| Clear | When connection to service is available again. | - | - |

## Answer-Seizure Ratio Threshold Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The Answer-Seizure Ratio (ASR) measures the percentage of answered calls relative to the total number of attempted calls (seizures). The alarm is raised when the configured ASR minor and major thresholds are crossed (configured in the Performance Profile table). | | |
| SNMP Alarm | acASRThresholdAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.111 | | |
| Alarm Title | ASR Threshold Crossed | | |
| Alarm Source | The object for which the threshold is crossed can be any of the following:<br>■ PM_gwSBCASR<br>■ PM_gwSBCIPGroupASR<br>■ PM_gwSBCSRDASR | | |
| 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 | The object for which the threshold is crossed can be any one of the following:<br>■ PM_gwSBCACD<br>■ PM_gwSBCIPGroupACD<br>■ PM_gwSBCSRDACD |
| 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:<br>■ PM_gwSBCNER<br>■ PM_gwSBCIPGroupNER<br>■ PM_gwSBCSRDNER |
| 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 | The alarm is raised when the device rejects calls to an IP Group due to the following reasons:<br>■ IP Group keep-alive failure (Gateway and SBC)<br>■ Poor Voice Quality - MOS (SBC only)<br>■ Bandwidth threshold has been crossed (SBC only)<br>■ ASR threshold has been crossed (SBC only)<br>■ ACD threshold has been crossed (SBC only)<br>■ NER threshold has been crossed (SBC only) |
| SNMP Alarm | acIpGroupNoRouteAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.114 |
| Alarm Title | IP Group Blocked |
| Alarm Source | The object for which the threshold is crossed according to one of the above mentioned reasons: |

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

## TLS Certificate Expiry Alarm

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

| Alarm 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).<br>To replace certificates, refer to the User's Manual. |
| Major | The certificate is about to expire. This is sent a week as well as a day before the expiration date. | "The certificate of TLS context %d will expire in less than a week"<br>Or<br>"The TLS certificate of TLS context %d will expire in a day"<br>Or<br>"The TLS certificate of TLS context %d will expire in less than a day" | |
| Critical | The certificate has expired. | "The certificate of TLS context %d has expired %d days ago" | Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically).<br>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 | Indicates that the NGINX Configuration file is not valid. | NGINX Configuration file is not valid. | Identify and resolve NGINX Directives Sets syntax errors to ensure an uninterrupted HTTP Proxy service. You can run the CLI commands for troubleshooting:<br>■ “show network http-proxy conf new” to display the Directives Set configuration that generated the errors.<br>■ “show network http- |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | proxy conf errors" to display the errors resulting from the invalid Directives Set configuration. |

## NGINX Process is not Running

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

## Remote Monitoring Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.145 | | |
| 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 Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Text | Corrective Action |
| 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><br>(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"<br>(Note: Text is | |

| Alarm Field | Description | | |
|---|---|---|---|
| | | configurable.) | |

## Clock Configuration Alarm

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

## Debug Recording Activation Alarm

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

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

## 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | 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 | 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. | | |
| 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 | Condition | Alarm Text | Corrective |

| Alarm Field | Description | | |
|---|---|---|---|
| Severity | | | Action |
| Minor | No response from DNS server. | "DNS server not responsive" | Make sure that the configured IP address of the DNS server is correct. |
| Cleared | Response received from DNS server. | | |

## 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 | acWeakPasswordAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.156 | | |
| Alarm Title | Weak Password Alarm | | |
| 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 |

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

## TLS Sockets Limit Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| | max. supported TLS connections. | supported TLS connections>" | |
| Cleared | The number of allocated incoming TLS connections returns to below 90% of max. supported TLS connections. | "Number of incoming TLS connections <current number of TLS connections> is less than 90% of max number allowed <max. supported TLS connections>" | - |

## VM Maintenace Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is sent when the OVOC receives a response (over REST API) from the cloud platform's metadata service of a scheduled maintenance event for the virtual machine on which the OVOC is installed. The alarm indicates the type of event and the scheduled time of the event.<br>This feature is configured by the [MaintenanceEventsMonitoringEnable] and [MaintenanceEventsTreatmentEnable] parameters. For more information on the OVOC's monitoring and handling of virtual machine maintenance events by the Cloud platform, refer to the OVOC's User's Manual. | | |
| SNMP Alarm | acVMMaintenaceAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.157 | | |
| Alarm Source | Board#1 | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Severity | Condition | Text | Corrective Action |
| Warning | A maintenance | "VM maintenance | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | event is scheduled for the virtual machine on which the OVOC is installed. | event was detected. Event type = “<event>”, Scheduled time = <UTC time>, Event id = <ID>." | |
| Cleared | The maintenance event has completed. | - | - |

## Specific Hardware Alarms

This section describes specific hardware alarms.

### Temperature Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is sent when the device exceeds its temperature limits (threshold). | | |
| 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.<br>■ One of the fans work slower than expected.<br>temperatureUnacceptable (50) | | |
| Alarm Severity | Condition | Text | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Critical | Internal temperature is too high for normal operation.<br>**Mediant 9000:** Temperature threshold of CPU has been exceeded. The threshold is configured by the ini file parameter [HighTemperatureThreshold]. The default is 70°C (158°F).<br>**Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** Temperature threshold at a specific sensor(s) has been exceeded. The threshold is configured by the ini file parameter [HighTemperatureThreshold]. For example, if the temperature threshold is exceeded at sensor 1, the alarm is sent ("Board Temperature Alarm: Sensor #1 is 88 degrees Celsius. Exceeded threshold of 70"). If the temperature threshold at sensor 2 is then exceeded as well, the first alarm is cleared and a new alarm is sent indicating exceeded temperature at both sensors ("Board Temperature Alarm: Sensors #1,#2 are 88,90 degrees Celsius. Exceeded threshold of 70").<br>**Mediant 4000:** At least one temperature sensor detects temperature increase to critical threshold minus 5 (or | "Board temperature too high"<br>**Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:**<br>"Board Temperature Alarm: Sensors <#,#> <is or are> <temperature,temperature> degrees Celsius. Exceeded threshold of <threshold>" | **1.** Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels.<br>**2.** Check the chassis ventilation outlet and make sure that they are not obstructed for air flow.<br>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 |

| Alarm Field | Description | | |
|---|---|---|---|
| | greater). | | case, send the faulty Fan Tray to AudioCodes as RMA. |
| Cleared | Temperature returns to normal operating values.<br>**Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080:** All sensors detect normal temperature.<br>**Mediant 4000:** All sensors detect temperature reduced to below critical threshold minus 5 degrees for at least 60 seconds. | - | - |

## Fan Tray Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is activated in one of the following cases:<br>■ Fan-Tray is missing<br>■ One or more fans in the fan-tray is faulty.<br>■ Fan tray is in place and fans are functioning. | | |
| SNMP Alarm | acFanTrayAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.29 | | |
| Alarm Title | Fan Tray Alarm | | |
| Alarm Source | Chassis#0/FanTray#0 | | |
| Alarm Type | equipmentAlarm | | |
| Probable Cause | ■ One or more fans on the Fan Tray module stopped working.<br>■ One or more fans on the Fan Tray module works slower than expected (heatingVentCoolingSystemProblem) | | |
| Alarm Severity | Condition | Text | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Critical | Fan-Tray is missing. | Fan-Tray is missing | 1. Check if the Fan Tray module is inserted in the chassis.<br>2. If the Fan Tray module was removed from the chassis, re-insert it.<br>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.<br>Warning: When removing the Fan Tray module while the power is on (or after it has recently been switched off), the blades may still be rotating at high speeds. Therefore, to avoid bodily harm, make sure that you don't touch the fan blades. |
| Major | When one or more fans in the Fan Tray are faulty. | Fan-Tray is faulty | Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes. |
| Cleared | Fan Tray module is in place and fans are working. | - | - |

## Power Supply Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is activated in one of the following cases:<br>■ The HA (High Availability) feature is active and one of the power supply units is faulty or missing.<br>■ PS unit is inserted in its location and functioning. |
| SNMP Alarm | acPowerSupplyAlarm |

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

## HA System Alarms

This section describes HA System alarms.

### HA System Fault Alarm

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

| Alarm Field | Description |
|---|---|
| Description | The alarm is sent when the High Availability (HA) system is faulty (i.e., no HA functionality). |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | | |
| Alarm Type | qualityOfServiceAlarm | | |
| Probable Cause | outOfService | | |
| Severity | Condition | Text | Corrective Action |
| Critical | HA has failed to initialize because of a configuration error. | "SYS_HA: HA Remote address not configured, No HA system." | Configure a valid 'HA Remote Address'. |
| | | "SYS_HA: HA Remote address and Maintenance IF address are not on the same subnet, No HA system." | Configure a valid Maintenance network interface and 'HA Remote Address'. |
| | | "SYS_HA: HA Remote address and Maintenance IF address should be different, No HA system." | Configure a valid Maintenance network interface and 'HA Remote Address'. |
| | HA is active, but the system is not operating in HA mode. | "Switch-Over: Reason = Fatal exception error" | HA was lost because of a switchover and should return automatically after a few minutes. |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | Corrective action isn't required. |
| | | "Switch-Over: Reason = SW WD exception error" | HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required. |
| | | "Switch-Over: Reason = System error" | HA was lost because of a switchover caused by a general system error and should return automatically after a few minutes. Corrective action isn't required. |
| | | "Switch-Over: Reason = Eth link error" | HA was lost because of a switchover. Reconnect the Ethernet link. |
| | | "Switch-Over: Reason = Network Monitor error. Failed table rows index: <id 1> ... up to <id 10>" | HA was lost because of a switchover caused by the HA Network Monitor feature as the threshold of unreachable |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | rows (in the HA Network Monitor table) was exceeded. The indices of these unreachable rows are provided in the alarm's text. The HA mode should return automatically after a few minutes. Corrective action isn't required. |
| | | "Switch-Over: Reason = Keep Alive error" | HA was lost due because of a switchover and should return automatically after a few minutes. Corrective action isn't required. |
| | | "Switch-Over: Reason = DSP error" | HA was lost because of a switchover and should return automatically after a few minutes. Corrective action isn't required.<br>**Note:** Applicable only to Mediant |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | 4000. |

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

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

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

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

| Alarm Field | Description | | |
|---|---|---|---|
| | **Note:** This condition is applicable only to Mediant VE SBC and when it's [MaintenanceEventsMonitoringEnable] parameter is enabled and [MaintenanceEventsTreatmentEnable] disabled. | event" | |
| | The Ethernet Group associated with the Maintenance IP interface (used for HA systems) is configured with two ports, but one of them is down (i.e., no 1+1 Ethernet port redundancy). | "SYS_HA: Maintenance redundant link is down - no HA maintenance link redundancy" | ■ Make sure that the network cable is firmly plugged into the Ethernet port.<br>■ Make sure that the other end of the network cable is correctly connected to the network. |
| Cleared | The HA system is active and operational. | "HA is operational" | - |

## HA System Configuration Mismatch Alarm

| 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 | configurationOrCustomizationError |

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

## HA System Switch Over Alarm

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

| Alarm Fields | Description | | |
|---|---|---|---|
| Event Type | qualityOfServiceAlarm | | |
| Probable Cause | outOfService | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical (default) | A switchover from the active to the redundant unit has occurred | Switch-over: See the acHASystemFaultAlarm table above | See HA System Configuration Mismatch Alarm on page 166 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 | Hitless Update Event | The corrective action for each condition is described below. |

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

## Redundant Board Alarm

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

| Alarm Field | Description |
|---|---|
| Severity | - |
| Additional Info | - |
| Corrective Action | - |

## HA Network Watchdog Status Alarm

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

| Alarm Field | Description | |
|---|---|---|
| use | | |
| 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).<br>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 | This alarm is raised under the following circumstances:<br>■ The device was unable to access the SBC License Pool Manager.<br>■ The device license has expired.<br>■ The device is no longer managed by the SBC License Pool Manager. |
| SNMP Alarm | acLicensePoolInfraAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.106 |
| Alarm Source | system0Mo |
| Alarm Type | communicationsAlarm |
| Probable Cause | keyExpired, fail to connect to license pool server. |

| Alarm 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. | ■ Wait for the next connection attempt.<br>■ In the SBC License Pool Manager, perform the 'MG Update' action to reestablish REST connection with device and send the current license. |
| | The device has been configured as Non-Managed in the SBC License Pool Manager. If there are active licensed sessions for this device, the device automatically performs a restart 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:<br>■ Connection has been restablished with the SBC License Pool Manager, an updated license has been loaded | - | |

| Alarm Field | Description | | |
|---|---|---|---|
| | to device and apply/restart has been performed.<br>■ 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/restart has been performed. | | |

## License Pool Application Alarm

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

## License Pool Over Allocation Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| | capacity supported by the device | allocation” | or apply hitless upgrade). |

## 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 | “Not enough memory to allocate for 'custom' pro- | Define a Custom Allocation Profile within the bounds of |

| Alarm Field | Description | | |
|---|---|---|---|
| | physical memory. | file” | the device’s capacity. |

## Cloud License Manager Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised under one of the following circumstances:<br>■ Disconnection between the device and OVOC.<br>■ Failure to send usage reports from the device to OVOC.<br>■ Fixed license is enabled and an attempt was made to enable the Floating license. | | |
| SNMP Alarm | acCloudLicenseManagerAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.132 | | |
| Alarm Title | Cloud License Manager Alarm | | |
| Alarm Source | Board#1 | | |
| Alarm Type | processingErrorAlarm | | |
| Probable Cause | configurationOrCustomisationError | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | CorrectiveAction |
| Major | There is no connection between the device and OVOC either prior to the initial handshake or due to a long disconnection time (default is three months; this time may be overriden by OVOC). | “No connection with OVOC” | ■ Check TCP/TLS connectivity.<br>■ Device should be registered on OVOC. |
| | Usage reports could | “Failed to send | Check TCP/TLS |

| Alarm Field | Description | | |
|---|---|---|---|
| | not be sent to OVOC from the device for a specified number of days. | usage report to OVOC for X days” | connectivity. |
| | The device is configured to work with the Fixed License Pool and an attempt was made to enable the Floating license. | “Floating license cannot be enabled, when device is managed by License Pool” | Disable Floating License parameter on the device.<br>Remove the device from the Fixed License Pool in OVOC. |
| Critical | Device couldn’t connect to OVOC (handshake). | “Connection with OVOC failed with response code <XXX>”. See below for more information” | <Forbidden 403>: contact AudioCodes support.<br><unauthorized 401>: check username/password |
| | Device couldn’t connect to OVOC (handshake). | ”Connection with OVOC failed, Failed initialize connection” | Check TCP/TLS connectivity. |
| | Device couldn’t initialize connection to OVOC (handshake). | ”Device was rejected by OVOC while trying to retrieve the device ID” | <Forbidden 403>: contact AudioCodes support. |
| Cleared | Connection with OVOC is established.<br>Reports are sent successfully.<br>The Floating License parameter is disabled on the device or the | - | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | device is removed from the Fixed License Pool. This alarm is cleared upon the next reboot. | | |

HTTP response code and reason:

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

## Flex License Manager Alarm

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

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Source | Board#1 | | |
| Alarm Type | processingErrorAlarm | | |
| Probable Cause | communicationsProtocolError | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Warning | OVOC Flex License pool stops the device’s service of an SBC capacity license type(s) due to pool's license capacity reached or exceeded (utilization status changed to "overlicense"). | "Service for <service name> license parameter is stopped" Where <service type> can be Signaling sessions, FEU (Far End Users), Transcoding sessions, and Media sessions | |
| Cleared | OVOC Flex License pool allows the device’s service of an SBC capacity license type(s) when sufficient licenses are restored to the pool (utilization 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| | and the parameter are used to check that all required MPMs are present and correctly installed in the device's chassis. | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.143 | | |
| SNMP Alarm | AcDSPFarmsMismatchAlarm | | |
| Alarm Title | DSP Farms Mismatch Alarm | | |
| Alarm Source | Board#1/ClusterManager#1/MT#2 | | |
| Alarm Type | equipmentAlarm | | |
| Probable Cause | Underlying Resource Unavailable | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | The number of MPMs configured by the DspFarmsInstalledNum parameter is greater than the number of MPMs installed on the chassis. This could result in a faulty or missing MPM module(s). | "Missing DSP farm was detected." | ■ Check if the MPM module(s) is fully inserted into the chassis slot.<br>■ If an MPM module(s) was removed from the chassis, re-install it.<br>■ Make sure that the DspFarmsInstalledNum parameter is configured to the correct number of physical MPM modules.<br>■ If you have performed all the above and the alarm still exists, send a Return Merchandise Authorization (RMA) request to AudioCodes |
| Cleared | The number of MPMs configured by the DspFarmsInstalledNum parameter is less than or equal to the number of MPMs installed in the chassis. | - | - |

## Mediant 9000 and Software SBC Alarms

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" | ■ Make sure all Media Transcoders are properly connected to the Cluster Manager.<br>■ Make sure all Media Transcoders in the Media Transcoders table |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | are in Admin State "Unlocked" and Status "Connected". |
| Cleared | HA usage drops to below 95% | - | - |

## Media Transcoder Network Failure

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

## Media Transcoder Software Upgrade Failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is sent upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Component. | | |
| SNMP Alarm | acMtceSwUpgradeFailureAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.117 | | |
| Alarm Title | Media Transcoder Software Upgrade Failure | | |
| Alarm Source | Board#1/clusterManager#0/MTCE#xxx | | |
| Alarm Type | processingErrorAlarm | | |
| Probable Cause | other | | |
| Severity | Condition | Text | Corrective Action |
| Major | Software upgrade (.cmp) or Auxiliary file load failure in Media Component. | ""Reset of the MTCE is required" | Reset the Media Transcoder and perform the upgrade process again.<br>If the upgrade fails again, contact your AudioCodes support representative. |
| Cleared | Upon restart 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 Field | Description | | |
|---|---|---|---|
| Alarm Type | Equipment Alarm | | |
| Probable Cause | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | Temperature of Media Transcoder reaches critical threshold | “MTCE reached high temperature threshold" | ■ Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels.<br>■ Check the chassis ventilation outlet and make sure that they are not obstructed for air flow.<br>■ Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray. |
| Cleared | Connectivity with Media Transcoder is re-established and temperature is reduced | - | - |

## 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 |

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

## Media Transcoder Power Supply Module Failure

| Alarm Field | Description |
|---|---|
| Description | The alarm is raised upon a failure in the Power Supply module of the Media Transcoder. |
| SNMP Alarm | acMtcePsuFailureAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.120 |
| Alarm Title | MT Power Supply Failure |
| Alarm Source | …./MTCE#1/powerSupply#1 |
| Alarm Type | equipmentAlarm |
| Probable Cause | powerProblem |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | Failure in Power Supply module of Media Transcoder | "MTCE power supply unit fault" | - Check if the Power Supply module is inserted in the chassis.<br>- If it was removed from the chassis, re-insert it.<br>- If the Power Supply module is inserted in the chassis and the alarm is still raised, send a Return Merchandise Authorization (RMA) request to AudioCodes. |
| Cleared | Power Supply module status returns to normal | - | - |

## Cluster Bandwidth Utilization Alarm

| Alarm Field | Description |
|---|---|
| Description | The alarm is raised when the bandwidth utilization of a Cluster interface exceeds the configured maximum bandwidth (refer to the MtcClusterNetworkMaxBandwidth parameter). |
| SNMP Alarm | acClusterBandwidthAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.126 |
| Alarm Title | Cluster Bandwidth Utilization Alarm |
| Alarm Source | Board#1/EthernetLink#<ehternet port number> |
| Alarm Type | Other |
| Probable Cause | performanceDegraded:<br>- Too many sessions processed on the specific Cluster interface.<br>- Cluster interface is being used by another application (e.g., OAMP). |
| Additional Info | - |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Text | CorrectiveAction |
| Major | Bandwidth utilization is greater than 90%. | "Cluster Bandwidth is above 90% utilization on Interface name: <name>. No more transcoding sessions will be allocated on that Cluster Interface" | Reduce the number of Media Transcoders on that Cluster interface. Alternatively, the overall permitted bandwidth for the Cluster interfaces should be increased, if possible (using the ini file parameter MtcClusterNetworkMaxBandwidth). |
| Minor | Bandwidth utilization is between 85 and 90%. Note: If a Major alarm was raised and the 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 | The alarm is sent when the Media Cluster is enabled and one of the following scenarios exist:<br>■ There are no operational Media Components in the Media Cluster.<br>■ There are no media interfaces configured for the operational Media Components.<br>⚠ Typically, using the Stack Manager to install, configure and manage Mediant CE prevents conditions (described below) that cause this alarm to be generated. However, if this alarm is generated, it is recommended to call the Healing stack operation, as described in the *Stack Manager for Mediant CE SBC User's Manual*. |
| SNMP Alarm | acMediaClusterAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.133 |
| Alarm Title | Media Cluster Alarm |
| Alarm Source | Device/clusterManager |
| Alarm Type | - |
| Probable Cause | - |

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

## Remote Interface Alarm

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

| Alarm Fields | Description | | |
|---|---|---|---|
| Description | This alarm is raised in the following circumstances:<br>■ 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.<br>■ 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.<br>■ 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.<br>Typically, using the Stack Manager to install, configure and manage Mediant CE prevents conditions (described below) that cause this alarm to be generated. However, if this alarm is generated, it is recommended to call the Healing stack operation, as described in the Stack Manager for Mediant CE SBC User's Manual. | | |
| SNMP Alarm | acMediaClusterRemoteInterfaceAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.134 | | |
| Alarm Title | Remote Interface Alarm | | |
| Alarm Source | device/clusterManager/MC | | |
| Alarm Type | Media Cluster | | |
| Probable Cause | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | According to description above. | ■ Interface <Interface id>, Name: <ethXX> - Alarm Status is | ■ Add the appropriate Media Interface |

| Alarm Fields | Description | | |
|---|---|---|---|
| | | RmifMissing<br>Interface <Interface id>, Name: <ethXX> - Alarm Status is PublicIpAddrMissing<br>Remote Interface Alarm: Interface <Interface id>, Name: <ethXX> - Alarm Status is LinkDown | ethXX<br>Configure a public IP address on the Media Cluster or remove the NAT rule.<br>Troubleshoot the Media Interface ethXX |

## AWS Security Role Alarm

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

## RTP Only Broken RTP Connection Alarm

| Alarm Fields | Description | | |
|---|---|---|---|
| Description | The alarm is sent when the RTP-Only feature is configured and a broken RTP connection exists for at least one of the RTP-only sessions (streams). For configuring the RTP-only sessions feature, see the [RtpOnly] ini file parameter in the device's User's Manual. | | |
| SNMP Alarm | acRtpOnlyBrokenRtpConnectionAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.160 | | |
| Alarm Title | RTP Only Broken RTP Connection Alarm | | |
| Alarm Source | Board#1 | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | At least one of the RTP-only sessions is in broken state. | Broken RTP connection on at least one RTP-only session | - |
| Cleared | All RTP-only sessions are in idle or connected states. | - | - |

## 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 Field | Description | | |
|---|---|---|---|
| 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

The alarm is applicable only to Mediant VE.

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is sent when the device fails to communicate with the metering API. The device needs to communicate with the Marketplace API when using AudioCodes Metered License model to license the SBC, which is based on the AudioCodes device usage (in minutes). | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.146 | | |
| Alarm Title | Metering Alarm | | |
| Alarm Source | Board#1 (SystemMO) | | |
| Alarm Type | communicationsAlarm | | |
| Probable Cause | communicationsProtocolError | | |
| Alarm Severity | Condition | Text | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Warning | The device is unable to send a usage report to the metering service after it initially connected to it. | "No connection to metering API – service will be down in <hours> 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 metering API.<br>- or -<br>■ The device has lost connectivity with the metering API for 3 hours since the last connection. | "Service down due to no connection to metering API" | Check the network configuration and make sure that the device has the appropriate environment as required for the metering offer. |
| Critical | The device is blocked by the metering license server. | “Service is blocked by metering license server” | - |
| Cleared | The device successfully communicates with the metering API. | "Device succeeds to communicate with metering API" | - |

## 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. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | ■ 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.<br>■ The MC is disconnected from the SC for unspecified reasons. | No Connection with MC | Reset the dis-connected MC. |
| Warning | The SC attempts to load the user-requested firmware to the MC and then one of the following occurs:<br>■ The upgrade is successful, however the connection cannot be established due to networking issues or to new firmware-related issues.<br>■ The upgrade process fails and the MC boots up and connects with its previous firmware version. | Failed to upgrade MC software for MC | Check the firmware, reload the firmware to the MC and restart the MC. |

| Alarm Field | Description | | |
|---|---|---|---|
| Warning | 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. | ■ MC <MTCEName> should be upgraded<br>■ MC <MTCEName> should be restarted | Upgrade and restart the MC that is currently operating in non-secure TCP mode. |
| Clear | ■ The MC successfully connects to SC in TLS secure mode.<br>■ The firmware upgrade to the MC is successful and a connection is established between SC and MC. | | |

## 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 | | |
| Probable Cause | communicationsSubsystemFailure | | |
| Alarm | Condition | Text | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Severity | | | |
| Minor | The certificate file required to secure theTLS 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 | For Mediant VE/CE stack: <stack-name><br>For Voice.AI Connect stack: <stack-name>/center or <stack-name>/sbc-X | | |
| Event Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Major | The Stack Manager can't establish connection with Mediant VE/CE stack via REST API. | Cannot connect to SBC 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | Security Group / firewall rules to allow the connection.<br>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:<br>1. Log into the Stack Manager.<br>2. Select the stack that represents specific Mediant VE/CE.<br>3. In the toolbar, click Modify<br>4. In the Advanced Config section, enter the following parameters:<br>username = <username><br>password = <password><br>5. At the bottom of the screen, click **Modify** to apply the changes. |
| 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. | Ensure that Stack Manager can access Data center management interface via HTTP protocol on port 8081. Use "curl http://<center-ip>: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. |
| Clear | Connection between the Stack Manager and | Successfully connected to Data center via REST API. | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | Voice.AI Connects’ Data center component has been restored. | | |
| 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><br>Where <component-name> is one of the following:<br>■ For Mediant VE stack: 'sbc-X'<br>■ For Mediant CE stack: 'sc-X' or 'mc-X' |

| Alarm Field | Description | | |
|---|---|---|---|
| | ■ For Voice.AI Connect stack: 'center', 'sm-X' or 'sbc-X' | | |
| Event Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Minor | ■ One of Mediant CE’s components is not in service. | ■ Signaling component 'sc-X' is 'down'<br>■ Media component 'mc-X' is 'down' | Return the component back into service. For example, start the corresponding VM. |
| Clear | ■ Mediant CE’s component is back in service. | ■ Signaling component 'sc-X' is 'up'<br>■ Media component 'mc-X' is 'up' | - |
| Minor | ■ Mediant VE’s component is not in service. | Instance 'sbc-X' is 'down' | Return the component back into service. For example, start the corresponding VM. |
| Clear | ■ Mediant VE’s component is back in service. | Instance 'sbc-X' is 'up' | - |
| Minor | ■ Voice.AI Connect’s component is not in service. | ■ Data center is 'down'<br>■ Session manager 'sm-X' is 'down'<br>■ SBC 'sbc-X' is 'down' | Return the component back into service. For example, start the corresponding VM. |
| Clear | ■ Voice.AI | ■ Data center is | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | Connect's component is back in service. | 'up'<br>■ Session manager 'sm-X' is up'<br>■ 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<br>■ 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.<br>Use "Heal" operation to fix Mediant CE configuration. |
| Clear | The Stack Manager can read the status of Mediant CE's Media Components. | Successfully read media components status | - |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 configuration. | Media component 'mc-X' is present in 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.<br>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:<br>■ Multiple FXS ports on a specific FXS blade are Out-Of-Service.<br>■ Hardware faults with the blades DSP. | | |
| SNMP Alarm | acModuleServiceAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.122 | | |
| Alarm Source | Chassis/Module# (Analog) | | |
| Alarm Type | equipmentAlarm | | |
| Probable Cause | equipmentMalfunction | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | More than five FXS ports 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 | | |
|---|---|---|---|
| | ports are Out-Of-Service on this blade.<br>■ 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. | 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 restart 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 | Decription | | |
|---|---|---|---|
| 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 | Decription | | |
|---|---|---|---|
| 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 restart 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 restart the device to return the blade to service. |
| | Clear: No hardware faults have been detected on any of the blades FXS ports. | | |

## Port Service Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when an FXS port is out of service due to the following:<br>■ The Serial Peripheral Interface (SPI) connection with the port is lost.<br>■ The temperature threshold on an FXS port has been exceeded.<br>■ An FXS port is inactive due to a ground fault. |
| SNMP Alarm | acPortServiceAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.124 |
| Alarm Source | Chassis/Module#/FXS Port # |
| Alarm Type | equipmentAlarm |
| Probable Cause | outOfService |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | The relevant FXS ports is faulty due to the reasons described above. In addition, note the following:<br>■ If the number of faulty FXS ports is above four on the same module, then the acModuleOperationAlarm alarm is raised (see above).<br>■ If there were active sessions on the device, then these calls are disconnected. No new SIP outbound calls will be initiated towards these FXS lines on this device. | "FXS Port state was changed to Out of Service" (the detailed reason will be provided in: Syslog, in the Web detailed port status description and in WEB tooltip per FXS port) | Service the faulty FXS port. |
| Clear | This alarm is cleared when:<br>■ The Serial Peripheral Interface (SPI) connection is restored.<br>■ The FXS port temperature falls within the threshold.<br>■ The ground fault is cleared.<br>■ The acModuleServiceAlarm (see above) is raised i.e. the number of faulty FXS ports on the module is above four. | | |

## 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”<br>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 | | |
|---|---|---|---|
| | ■ Vendor ID<br>■ Product ID<br>■ Cellular state (shutdown or no shutdown)<br>■ Received Signal Strength Indicator (RSSI) in dBm<br>■ Cellular dongle status ("up" or "down") | | |
| SNMP Alarm | acWirelessCellularModemStatusChanged | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.104 | | |
| Alarm Title | Wireless Cellular Modem Status Changed | | |
| Alarm Source | Board#x/WanLink#y | | |
| Alarm Type | Equipment Alarm | | |
| Probable Cause | other (0) | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Indeterminate | | MSBR cellular interface: dongle type <vendor ID>:<product ID>,modem <"on" or "off">,RSSI <dBm value> DBM. | |

## Data Interface Status

| Alarm Field | Description |
|---|---|
| Description | This alarm is sent when a DSL interface state changes to up or down. |
| SNMP Alarm | acDataInterfaceStatus |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.83 |
| Alarm Title | - |
| Alarm 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 | To correct long RTT (Round Trip Time):<br>■ Test with traceroute.<br>■ Contact your ISP with the traceroute results.<br>■ Use Wireshark or any other diagnostic tool to perform a traffic capture and determine who is contaminating the network. |

## NQM Jitter Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when high Jitter towards the NQM probe destination is detected. | | |
| SNMP Alarm | acNqmJitterAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.90 | | |
| Alarm Title | NQM Jitter Alarm | | |
| Alarm Source | Board#%d/NqmSender#%d | | |
| Alarm Type | CommunicationsAlarm | | |
| 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 | To correct high jitter:<br>■ Test with traceroute.<br>■ Contact your Internet Service Provider (ISP) with traceroute results.<br>■ Implement Quality of Service (QoS).<br>■ Note that there's no simple solution for high jitter. A systemic level solution may be required. |

## NQM Packet Loss Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when high packet loss towards the NQM probe destination is detected. | | |
| SNMP Alarm | acNqmPacketLossAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.91 | | |
| Alarm Source | Board#%d/NqmSender#%d | | |
| Alarm Type | CommunicationsAlarm | | |
| Probable Cause | Raised when Detected high Packet Loss towards NQM probe destination | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | - | Detected high PL towards NQM probe destination | To correct high packet loss (PL):<br>■ Eliminate interference problems: Distance your modem from electrical devices<br>■ Do not coil up any excess signal or power cables. |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | ■ Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring. |

## NQM MOS CQ Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when low conversational voice quality towards the NQM probe destination is detected. | | |
| SNMP Alarm | acNqmCqMosAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.95 | | |
| Alarm Title | Detected low conversational voice quality towards NQM probe destination | | |
| Alarm Source | Board#%d/NqmSender#%d | | |
| Alarm Type | communicationsAlarm | | |
| Probable Cause | Raised when Detected low conversational voice quality towards NQM probe destination | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | - | Detected low conversational voice quality towards NQM probe destination | To fix the Noise Quality Measure (NQM) result:<br>■ Perform corrective action for jitter. See NQM Jitter Alarm on page 215<br>■ Perform corrective action for Real Time Protocol (RTP) packet loss.<br>■ See NQM Packet Loss Alarm on the previous page<br>■ Perform corrective action for |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination.<br>■ See NQM RTT Alarm on page 214<br>To fix the poor Conversational Quality (CQ) that the test indicates:<br>■ Try changing the coder<br>■ Try using RTP-Redundancy<br>■ Perform corrective action for RTP packet loss.<br>■ See NQM Packet Loss Alarm on page 216 |

## NQM MOS LQ Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when low listening voice quality towards the NQM probe destination is detected. | | |
| SNMP Alarm | acNqmLqMosAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.96 | | |
| Alarm Source | Board#%d/NqmSender#%d | | |
| AlarmType | communicationsAlarm | | |
| Probable Cause | Raised when detected low listening voice quality towards NQM probe destination | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | - | Detected low listening voice quality towards NQM probe destination | To fix the Noise Quality Measure (NQM) result:<br>■ Perform corrective action for Real Time |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | Protocol (RTP) packet loss.<br>■ See NQM Packet Loss Alarm on page 216<br>To fix the poor listening quality that the test indicates:<br>■ Try changing the coder<br>■ Try using RTP-Redundancy<br>■ Perform corrective action for RTP packet loss.<br>■ See NQM Packet Loss Alarm on page 216 |

## Mediant 3000 Hardware Alarms

This section describes the Mediant 3000 Hardware alarms.

### PEM Module Alarm

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

## SA Module Missing Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is sent when the Shelf Alarm (SA) module is missing or non operational. | | |
| SNMP Alarm | acSAMissingAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.32 | | |
| Alarm Title | SA Module Missing Alarm | | |
| Alarm Source | Chassis#0/SA#<m>, where m is the shelf Alarm module’s slot number | | |
| Alarm Type | equipmentAlarm | | |
| Probable Cause | underlyingResourceUnavailable | | |
| Alarm Severity | Condition | <Text> | Corrective Action |
| Critical (default) | SA module removed or missing | SA Module Alarm. SA-Module from slot #n is missing. | ■ Reinsert the Shelf Alarm (SA) module into slot #n<br>■ Make sure it's correctly inserted |

| 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.<br>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 | 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:<br>■ D-channel synchronized<br>■ D-channel not-synchronized |

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

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

## SONET Line RDI Alarm

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Description</td><td colspan="3">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).</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">acSonetLineRDIAlarm</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.10.1.21.2.0.41</td></tr>
<tr><td>Alarm Source</td><td colspan="3">Interfaces#0/Sonet#<m>, where m is the SONET interface number</td></tr>
<tr><td>Alarm Type</td><td colspan="3">communicationsAlarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">transmitFailure</td></tr>
<tr><td>Alarm Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Critical (default)</td><td>RDI condition is present on SONET-Line #n</td><td>SONET-Line RDI</td><td>■ Check the remote site for alarm conditions.<br>■ Correct a line problem that has arisen from the remote interface.<br>Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value sonetLineRDI (4)</td></tr>
<tr><td>Cleared</td><td>RDI condition is not present.</td><td>-</td><td>-</td></tr>
</table>

## SONET/SDN IF Failure Alarm

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

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

## Trunk LOS Alarm

This alarm applies to E1/T1Trunks.

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

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

## Trunk LOF Alarm

This alarm applies to E1/T1Trunks.

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

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

| 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 | ■ Contact your PSTN provider to activate the trunk.<br>■ If the alarm persists, contact the AudioCodes Support Center at support@AudioCodes.com |
| Cleared | End of AIS | - | - |

## Trunk RAI Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm indicates a loss of frame at the trunk's far end. |
| 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 | 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:<br>■ V5 interfaces ID are not equal on both sides<br>■ V5 variants are not equal on both sides<br>■ V5 link ID check timeout error occurred<br>■ Layer 2 startup failed<br>■ V5 restart failed<br>An Alarm is raised with major severity when:<br>■ Control protocol data link error<br>■ Link control protocol data link error<br>■ BCC protocol data link error<br>■ PSTN protocol data link error<br>■ Protection DL1 failure<br>■ Protection DL2 failure |
| 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 | For critical severity alarms, solve configuration mismatch (configuration does not comply to far end configuration).<br>For major severity alarms:<br>■ Ensure physical connections are in place.<br>■ Ensure links are not administratively blocked.<br>■ Resolve configuration issues. |

## SONET Path STS LOP Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is issued when the LOP condition is present on the SONET Path #m. |
| SNMP Alarm | acSonetPathSTSLOPAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.61 |
| Alarm Title | SONET Path STS LOP Alarm |
| Alarm Source | Interfaces#0/Path#<m> |
| Alarm Type | communicationsAlarm |
| Probable Cause | receiveFailure |
| 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 | acSonetPathSTSAISAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.62 |
| Alarm Title | SONET Path STS AIS Alarm |
| Alarm Source | Interfaces#0/Path#<m> |
| Alarm Type | communicationsAlarm |
| Probable Cause | receiveFailure |
| Severity | Critical / clear |
| Additional Info | - |
| Corrective Action | Check the following and correct according to the appropriate reason:<br>There is higher level failure: LOS, LOF, AIS-L<br>A Path Trace Identifier mismatch occurred<br>▪ Path is unequipped on the Far-End |

## SONET Path STS RDI Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is issued when the RDI condition is present on the SONET Path #m. |
| SNMP Alarm | acSonetPathSTSRDIAlarm |
| 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.<br>Check the following and correct on the far-end according to the appropriate reason:<br>LOS, LOF, AIS-L, AIS-P |

## SONET Path Unequipped Alarm

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

## SONET Path Signal Label Alarm

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

## DS1 Line Status Alarm

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

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

## DS3 RAI Alarm

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

## DS3 LOF Alarm

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

## DS3 LOS Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is issued when the LOF condition is present on the DS3 Interface #m. |
| SNMP Alarm | acDS3LOSAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.69 |

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

## NFAS Group Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when an NFAS group goes Out-Of-Service and is cleared when an NFAS Group is back In-Service. |
| SNMP Alarm | acNFASGroupAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.84 |
| Alarm Source | Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk |
| Alarm Type | communicationsAlarm |
| Probable Cause | degradedSignal |

| Alarm Severity | Condition | Text | Corrective Action |
|---|---|---|---|
| Major (default) | Raised when an NFAS group goes out-of-service | NFAS Group Alarm. %s | ■ The alarm is sent only when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when both D-channels are down.<br>■ When at least one of the<br>■ D-channels (primary or |

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

## B Channel Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the B-Channel service state changes and is cleared when the BChannel is back in service. | | |
| SNMP Alarm | acBChannelAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.85 | | |
| Alarm Title | B-Channel Alarm | | |
| Alarm Source | Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk | | |
| AlarmType | communicationsAlarm | | |
| Probable Cause | DegradedSignal | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major (default) | Raised when B-channel service state changes to 'Out of Service' or 'Maintenance' | B-Channel Alarm. %s | Corrective Action is not necessary. |
| Clear | B-channel status changes to 'In 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 | ■ No corrective action is required.<br>■ The device shuts down the port and tries to activate it again when the relevant alarm is over. |
| Note | Relevant to FXS only. |

## Dial Plan File Replaced Trap

| Alarm Field | Description |
|---|---|
| Description | Indicates that the dial plan file has been replaced. |
| SNMP Alarm | acDialPlanFileReplaced |
| SNMP OID | 1.3.6.1.4.1.5003.9.10.1.21.2.0.45 |
| Default Severity | Indeterminate |
| Alarm 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> | |
| 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> | a. |
| 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<br>(indicates which service is down) | |
| Major | Service is down | SERVICE_STOPPED<br>(indicates which service is down) | |
| Warning | Service is down | SERVICE_STOPPED.<br>(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 | a. |
| Major | Event Log has a Major alarm. | The event log has errors | a. |
| Warning | Event Log has a Warning alarm. | The event log has errors | a. |
| 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 | ■ License will expired in <number of days left><br>■ Days. | ■ Check the license server of update new license. |
| 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<br>renewed | - | - |

## Alarm-Disk Space

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the host machine disk space is above the predefined 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}% | ■ Free temporary files and other unnecessary files from the CCE appliance Host disk.<br>■ Validate on the HyperV machine that you can view up to two versions of the CCE Appliance. If you view more versions, clear the old CCE version VMs. |
| Clear | Pre-defined severity for percentage of used disk space. | Disk space usage is over {0}% | ■ Free temporary files and other unnecessary files from the CCE appliance Host disk.<br>■ 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. |

## 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 Field | Description | | |
|---|---|---|---|
| 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 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 Field | Description | | |
|---|---|---|---|
| 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. | | |
| 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<br><x>. | |
| Major | Pre- defined severity per counter type. | <Performance counter> high level | |

| Alarm Field | Description | | |
|---|---|---|---|
| | | <x>. | |
| Warning | Pre- defined severity per counter type. | <Performance counter> high level<br><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. | | |
| 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 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. | | | |

## Voca Certificate Expired

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

| Alarm Field | Description | | |
|---|---|---|---|
| | 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 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. | | |

## 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:<br>■ ReplicationManager\SlaveDBStatus<br>■ ReplicationManager\RemoteSlaveDBStatus |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | |
| 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:<br>- ClusterManager\NodesIds<br>- ClusterManager\NodesRoles |
| Alarm Text | TBD |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. | |
| 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:<br>■ ClusterManager\HeartBeats<br>■ ReplicationManager\DBConnection |
| Alarm Title | Alarm – Connection Failure |
| Alarm Type | Alarm |
| Probable Cause | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | |
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. | | |

## 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 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 Field | Description | | |
|---|---|---|---|
| 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 |
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. | | |

### 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| Probable Cause | | | |
| Additional Info | | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Critical | Pre-defined severity per each counter type | <Performance counter> high level <x> | ■ |
| Major | Pre-defined severity per each counter type | <Performance counter> high level <x> | ■ |
| Warning | Pre-defined severity per each counter type | <Performance counter> high level <x> | ■ |
| Cleared | When counter returns below the threshold level. | | |

### 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)<br>• TeamsSBA<br>• TeamsSbaConfig |
| Alarm Title | Component Service Status |
| Alarm Type | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. | | | |

### 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 | |

| Alarm Field | Description | | |
|---|---|---|---|
| | 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 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 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:<br>■ Self signed certificate for mTls<br>■ 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 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 | | |

| Alarm Field | Description | | |
|---|---|---|---|
| | 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 Title | Product License Expired | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Major | License is invalid/expired | ■ License will expired in <number of days left><br>■ Days. | ■ Check the license server of update new license. |
| 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 Severity | Condition | Text | Corrective Action |
| Critical | CPU > 90% | High CPU usage Above 90% | Using task manager check if the CPU load is constant or not, find the process that causes the high CPU usage and see if high CPU is reasonable (for example high CPU when performing windows updates, or running traces on the SBA), if there isn't a reason for the high CPU try to restart 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 restart the SBA and if didn't solve the issue open a call to AudioCodes |
| Cleared | CPU < 76% | - | - |

## SBA Memory Status

| Alarm Field | Description | | |
|---|---|---|---|
| Description | Memory used status alarm. Send an alarm when the level of available physical memory is below the threshold. | | |
| SNMP Alarm | acSBAMemorytatusAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.30.2.2.0.3 | | |
| Alarm Title | Alarm – Memory Status | | |
| Alarm Source | Memory/% Available MByte | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Major | Available Memory < 7% | High memory usage, available memory is Below 7% | Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. if there isn't a reason for the high memory try to restart the SBA and if didn't solve the issue open a call to AudioCodes. |
| Critical | Available Memory < 4% | High memory usage, available memory is Bellow 4% | Using task manager find the process that causes the high memory usage. SQL process can take huge amount of memory and it is normal. If you install extra tools on the SBA remove/disable them and see if solve the high memory usage. On 2G RAM SBAs the memory usage can be high but it should not have any impact on the service that the SBA provide. Perform Windows update and SQL server update. If there isn't a reason for the |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | high memory try to restart the SBA and if didn't solve the issue open a call to AudioCodes. |
| Cleared | Available Memory >8% | | |

## SBA Disk Space Alarm

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised if the disk (C) usage level exceeds configured thresholds. Thresholds can be configured in the snmp_sba.ini under C:\SBA (requires service restart for the changes to take effect). | | |
| SNMP Alarm | acSBADiskSpaceAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.30.2.2.0.4 | | |
| Alarm Title | Alarm – Disk Space | | |
| Alarm Source | C:\ | | |
| Alarm Text | Disk space usage is over {0}%<br>{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 | - | | |
| 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. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 the 'Major' threshold | Performance counter {0} is Above/Below {1}<br>{0} – Performance counter full path<br>{1} – Threshold value | |
| Critical | Monitored value crossed the 'Critical' threshold | Performance counter {0} is Above/Below {1}<br>{0} – Performance counter full path<br>{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 Field | Description | | |
|---|---|---|---|
| Alarm Source | RtcSrv/ RTCMEDSRV/ REPLICA/ RTCCLSAGT | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Severity | Condition | <text> | Corrective Action |
| Critical | Service is down | SERVICE_STOPPED | Start the service and check why the service stopped, using the event viewer. |
| Major | Service is paused | SERVICE_PAUSED | Start the service and check why the service paused, using the event viewer. |
| Cleared | Service is running | SERVICE_RUNNING | - |
| Indeterminate | Service in indeterminate state | SERVICE_CONTINUE_ PENDING SERVICE_ PAUSE_PENDING SERVICE_START_ PENDING SERVICE_ STOP_PENDING | Start the service and check why the service is in indeterminate state, using the event viewer. |

## UMP-365 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 | ▪ WebSocket |

| Alarm Field | Description | | |
|---|---|---|---|
| | ■ TunDevice | | |
| Alarm Title | Wrong Operating Alarm | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| 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 | Unable to | |

| Alarm Field | Description | | |
|---|---|---|---|
| | WebSocket service.is unable to connect to OVOC. | 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 Web Socket service correctly sends HTTPS packets to OVOC.. | Tun device written successfully | |

## UMP Tenant License Threshold Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the number of UMP tenant licenses that are active for a specific UMP virtual machine instance crosses the threshold.<br>⚠ A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition. |
| SNMP Alarm | acUmpTenantLicThresholdAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.41 |
| Alarm Title | UMP Tenant License Threshold Alarm |
| Unique ID | Unique ID in the UMP-365 SQL database. |
| Alarm Source | Virtual machine of UMP installation platform |
| Alarm Type | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| Probable Cause | Other | | |
| Additional Info | #of users/# in active | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 95 %). | Tenant License threshold (Over 95 %) | |
| Major | The number of UMP tenant licenses running on the UMP virtual machine instance crosses the threshold (above 90 %). | Tenant License threshold (Over 90 %) | |

## UMP User License Threshold Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance crosses the configured licensed threshold. The threshold is configured in the UMP Customer License settings in the UMP-365 Main Tenant License page.<br>A tenant license exists for each Microsoft Office 365 tenant and is relevant for the UMP SP Edition. |
| SNMP Alarm | acUmpUserLicThresholdAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.42 |
| Alarm Title | UMP User License Threshold Alarm |
| Unique ID | Unique ID in the UMP-365 SQL database. |
| Alarm Source | Virtual machine of UMP installation platform |

| Alarm Field | Description | | |
|---|---|---|---|
| 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 (configured in the License page in the UMP-365 Main Tenant interface). In this case, a Grace period (also configured in the Tenants page in the UMP-365 Main Tenant interface) is granted including a percentage allotment of licenses for a limited period. | User License threshold crossed (Configured License Threshold %) | |
| Major | The number of active UMP users for a specific UMP tenant on a specific UMP virtual machine instance, reaches the configured Warning threshold (configured in the License page in the UMP-365 Main Tenant interface). | User License threshold reached (Configured License Threshold %) | |
| Clear | The number of licensed users falls below the configured threshold. | | |

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

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

| Alarm Field | Description | | |
|---|---|---|---|
| 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 | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| 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 |
| Unique ID | Unique ID in the UMP-365 SQL database. |
| Alarm Source | Virtual Machine/CustomerID |
| Alarm Type | Other |
| Probable Cause | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| Additional Info | #of users/# in active | | |
| 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 | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| 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. | | |
| SNMP Alarm | acUmpO365FailureAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.46 | | |
| Alarm Title | UMP O365 Failure Alarm | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| 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 |
| Unique ID | Unique ID in the UMP-365 SQL database. |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Source | Virtual machine of UMP installation platform/CustomerID (Customer Name) | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | Execution Result | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Minor | This alarm is raised when any PowerShell command run on the UMP platform . | | |

## UMP User Settings Fail Event

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when a user editing operation fails (Field Edit user). | | |
| SNMP Alarm | acUmpUserSettingsFailEvent | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.49 | | |
| Alarm Title | UMP User Settings Fail Event | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| 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 set- | |

| Alarm Field | Description | | |
|---|---|---|---|
| | | tings fail | |

## UMP End User Authentication Fail Event

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when there is an authentication failure for the UMP Admin End User . | | |
| SNMP Alarm | acUmpEndUserAuthFailEvent | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.50 | | |
| Alarm Title | UMP End User Authentication Fail Event | | |
| Unique ID | Unique ID in the UMP-365 SQL database. | | |
| 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 | |

## UMP Operation Failed Alarm

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when UMP-365 cannot establish connection with the SMTP Mail server. |
| SNMP Alarm | acUmpOperationFailedAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.80.3.2.0.51 |
| Alarm Title | UMP Operation Failed Alarm |
| Unique ID | Unique ID in the UMP-365 SQL database. |
| Alarm Source | ■ Incorrect SMTP settings: ump/emailinit |

| Alarm Field | Description | | |
|---|---|---|---|
| | ■ Incorrect email: username/emailsend<br>Where username is the field configured in the Email Server Settings page in Multitenant interface.<br>■ SMTP Service is not running: tenantname/emailsend | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | - | | |
| Alarm Severity | Condition | Text | CorrectiveAction |
| Critical | SMTP Server Settings (Hostname and Port number) are configured incorrectly in the Email Server Settings page in the Multitenant interface (Configuration > UMP > Email > Server Settings). | Cannot initialize SMTP Settings. | Verify that the SMTP Hostname and port number are correct. |
| Critical | Email address is configured incorrectly in the Email Server Settings page in the Multitenant interface (Configuration > UMP > Email > Server Settings). | Exception Sending Email. | Verify that the email address for connecting to the SMTP server is correct. |
| Critical | The SMTP Service is not running on the UMP-365 Microsoft Windows server . | SMTP Service is not running. | Verify that the SMTP service is running on the UMP-365 Microsoft Windows server. |

# Interaction Insights Alarms

This section describes the SmarTAP alarms.

## SmartTAP System Alarms

This section describes SmartTAP Microsoft Windows Server System alarms.

### Alarm – Component Unreachable

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised in the following circumstances:<br>■ 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 Interaction Insights application server.<br>■ The Interaction Insights Application server is unable to connect to the Interaction Insights Web Admin Interface | | |
| SNMP Alarm | acVAManEnvUnreachableAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.1 | | |
| Alarm Source | SmartTapAS_<FQDN> | | |
| Alarm Title | Component Unreachable | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm | Condition | <text> | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Severity | | | |
| 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 Interaction Insights Application server is unable to connect to the Interaction Insights Web Admin interface. | Unable to Connect to Voice Application Admin | |
| Cleared | OVOC Client agent is re-available | | |

## Interaction Insights Event – Component Restart

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This event is raised when the Interaction Insights 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 Interaction Insights Application server has been restarted. | Component <Interaction Insights AS FQDN> restarted | - |

## Event – Component Resource Failed

| Alarm Field | Description |
|---|---|
| Description | This event is raised in the following circumstances:<br>■ The allocation of resources for recording licenses has been exceeded<br>■ Media Server management has failed |
| SNMP Alarm | acVaCompResFailedEvent |
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.9 |
| Alarm Source | SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following:<br>■ Licenses:<br>✓ imLicQuotaExceeded<br>✓ videoLicQuotaExceeded<br>✓ userLicQuotaExceeded<br>✓ mediaFwdLicQuotaExceeded<br>✓ licUnavailable<br>■ Media Server Resource Failure:<br>✓ Hmp - channelResourceFailure<br>✓ Hmp createFileFailed<br>✓ Hmp bindingFailure<br>✓ Hmp rtsTransferFailed<br>✓ Hmp writeFileFailed |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Title | Component Resource Error | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | - | | |
| Alarm Severity | Condition (related resource indicated in parenthesis) | <text> | Corrective Action |
| Major | The quota for the number of users targeted for Instant Messaging has been exceeded (imLicQuotaExceeded). | IM target quota exceeded | Reduce the number of users/devices targeted for Instant Messaging recording or purchase additional licenses. |
| Major | The quota for the number of users targeted for video has been exceeded (videoLicQuotaExceeded). | video target quota exceeded | Reduce the number of users/devices targeted for video recording or purchase additional licenses. |
| Major | The quota for the number of users/devices targeted for audio recording has been exceeded<br>(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<br>(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<br>(Hmp - channelResourceFailure). | Media server failed to create channel resource | - |
| Major | The Media Server failed to write to disk<br>(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 | This alarm is raised when one of the Interaction Insights component resources listed below has reached its predefined threshold. This alarm applies for the following resources:<br>■ Recording license notification thresholds (for all recording license types) triggered according to the configuration in the Interaction Insights Web interface License screen.<br>■ Media Storage notification thresholds triggered according to the following:<br>✓ **SMB/File Storage:** Configuration in the Interaction Insights Web interface Storage Statistics screen.<br>✓ **Azure Blob Storage:** Thresholds shown below for Azure Blob storage event.<br>■ The total hours of calls analyzed by the Analytics Service has exceeded the limit.<br>■ The number of licensed Analytics users has exceeded the limit. |
| SNMP Alarm | acVaResourceThresholdAlarm |

| Alarm Field | Description | | |
|---|---|---|---|
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.11 | | |
| Alarm Source | SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following:<br>- Interaction Insights License Threshold Notification value (for all recording license types)<br>- Media Storage Notification Threshold value<br>- Analytics Hours license value<br>- Analytics Users license value<br>- AzStorage | | |
| Alarm Title | Alarm - Component Resource Threshold Exceeded | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info | AzStorage:<br>- Total Space: <amount> GB<br>- Free Space Remaining: <amount> GB<br>- Estimated Recording Time Remaining:- <number of months> | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Critical/Major/Warning | The media storage location threshold has been reached. | Media Storage threshold exceeded | - 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.<br>- Add additional storage capacity to the file server to support additional media files (recordings). The file server is external to Interaction Insights. |
| | Recording License threshold has been exceeded. | Recording License threshold exceeded | - 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.<br>- Purchase additional recording licenses |
| | The total number of hours of analyzed calls by Analytics Service has exceeded the limit. | Analytics Hours license Threshold Exceeded | - 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.<br>- Purchase additional Analytics hours |
| | The number of licensed Analytics users has exceeded the limit. | Analytics Users license Threshold Exceeded | - 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.<br>- Purchase additional Analytics user licenses |
| | The threshold of a limited resource has been exceeded. | The Blob Storage usage reached 90% of available storage. | - Purchase additional storage or transfer media to another disk. |
| Cleared | - When counter returns below the threshold level.<br>- The Blob Storage usage reached 80% and below. | - | - |

## Alarm – Connection Failure

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised in the following circumstances: |

| Alarm Field | Description |
|---|---|
| | ■ The connection between one of the Interaction Insights components and the Interaction Insights Application server is down.<br>■ The connection between other Interaction Insights components is down. |
| SNMP Alarm | acVaConnectionFailureAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.12 |
| Alarm Source | <SmartTAPComponent>@ <FQDN>:<br>■ AC-MediaProxy @<FQDN><br>■ AC-Annoucement @ <FQDN><br>■ CS@ <FQDN><br>■ CD-IP@ <FQDN><br>■ CD-SIPREC@ <FQDN><br>■ MediaDelivery@ <FQDN><br>■ Media Server@<FQDN><br>■ AC_HealthMonitor@ <FQDN><br>■ AC-Plugin@ <FQDN><br>■ RTS@ <FQDN> |
| Alarm Title | Alarm – Connection Failure |
| Alarm Type | Other |
| Probable Cause | Other |
| Additional Info | - |

| Alarm Severity | Condition | <text> | Corrective Action |
|---|---|---|---|
| Critical/Major/Warning | Communication between Interaction Insights component and Interaction Insights Application server is down | Communication Down Details: Managed Device <SmartTAPComponent>@<HostNameFQDN> failed to send heartbeat within specified time of <xxmS>.Device InfoId: <SmartTAPInternalID>HostNameType: COM_ SERVERDisplay Name: <HostName>Last heartbeat received on <yyyy-mm-dd> <hh:mm> | |
| | Connection from CallDelivery to lyncPlugInServerConnDown | Communication Down Details: Call Delivery at <HostNameFQDN> lost 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 | |

| Alarm Field | Description | | |
|---|---|---|---|
| | 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 Interaction Insights 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 Cause | Other | | |
| 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 Interaction Insights Application server is down. These services include Interaction Insights 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:<br>■ AudioCodes_CS |

| Alarm Field | Description | | |
|---|---|---|---|
| | MySQL<br>CallDelivery-IP<br>HealthMonitorSvc<br>AudioCodesMPSvc<br>HPXMedia<br>RemoteTransferService<br>AcProcDump<br>CallDeliverySR<br>CallDelivery<br>CallDeliveryLD<br>CallDeliveryAES<br>SmartTapMonitoringSvc | | |
| 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<br>(indicates which service is down) | - |
| Major | Service is down | SERVICE_ STOPPED<br>(indicates which service is down) | - |
| Warning | Service is down | SERVICE_ STOPPED.<br>(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 Field | Description |
|---|---|
| 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 Interaction Insights Application server is about to expire. | | |
| SNMP Alarm | acVaCompCertificateExpiredAlarm | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.27 | | |
| Alarm Source | SmartTapAS_<FQDN> | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Critical | Raised when the certificate will expire in less than two days | Certificate will expire in <days left> days | Verify which certificate is about to expire and renew it. |
| Major | Raised when the certificate will expire in less than 30 days. | Certificate will expire in <days left> days | Verify which certificate is about to expire and renew it. |
| Cleared | When certificate is renewed | - | - |

## Alarm – Disk Space

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the server disk space on the Interaction Insights 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 Interaction Insights 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 |
| Major | One of the following Health Monitor services reported an error to the Interaction Insights 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 | ■ Check Media location configuration in Interaction Insights<br>■ Check Azure Blob accessibility and health |
| | 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 | ■ Check Service Fabric Cluster health<br>■ Verify MSFT Graph API accessibility and responsiveness |
| Major | CdrRecoveryFailed(450) | Call Recovery Failed, file <path> has exceeded the allowed failure threshold. | Check Interaction Insights 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 | This event is raised under the following circumstances:<br>■ 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.<br>■ 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.<br>■ Problems with Azure Storage account configuration<br>■ 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.<br>■ 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.<br>■ User access to Azure Cognitive Services is unauthorized. | | |
| 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 | ■ 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 Interaction Insights. Please make sure the user is assigned to one AAD group that is mapped to a recording profile.<br>■ 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 Interaction Insights. Please make sure the user is assigned to one AAD group that is mapped only when mapping retention policies.<br>■ User <username> 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 Interaction Insights.<br>■ User <username> 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 Interaction Insights | | |
| 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 | - botNodeName@botclusterFQDN<br>- botCluster@botclusterFQDN | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | RecordingClusterNotAvailable<br>(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<br>(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 overloaded, 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 | One of the following MeetingInsights components is unreachable:<br>- BackEnd<br>- OutlookDaemon<br>- SpeechTranscriptionApp<br>- SpeakerIdApp<br>- AI Server<br>- SI server |

| Alarm Field | Description |
|---|---|
| SNMP Alarm | acVaConnectionFailureAlarm |
| SNMP OID | 1.3.6.1.4.1.5003.9.40.3.2.0.12 |
| Alarm Title | Connection Failure |
| Alarm Source | ■ MeetingInsights/<component>-<avaliablityTest><br>■ MeetingInsights/backend-<Customer>status<br>■ MeetingInsights/ -<Customer>status<br>■ MeetingInsights/speakerIdapp--<Customer> status<br>■ MeetingInsights/outlookdaemon--<Customer> status<br>■ MeetingInsightsasierver--<Customer> status<br>■ MeetingInsights/siserver--<Customer> status |
| Alarm Type | Other |
| 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. | ■ Check IIS status and try to connect from the BackEnd server on localhost http://localhost/ui<br>■ Check firewall rules.<br>■ Check EventLogs for errors. |
| 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. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. |
| 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 Field | Description | | |
|---|---|---|---|
| Alarm Source | ■ MeetingInsights/<Component>/<Condition><br>■ MeetingInsights/Backend/ PostProcessFailed<br>■ MeetingInsights/<nodename@clusterfqdn>/CreateCallFailed<br>■ MeetingInsights/<nodename@clusterfqdn>/JoinCallFailed<br>■ MeetingInsights/<nodename@clusterfqdn>/FileXferFailed | | |
| 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 from Bot.. |
| Major | JoinCallFailed | Failed answering call <call-id> scenarioId <senarioid>. | ■ Check Bot logs for errors.<br>■ Check customer admin consent for Bot application.<br>■ Check if there is firewall in front of the Bot.. |
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| | 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 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:<br>■ MongoDB<br>■ IIS<br>■ MIAlarmManager | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| 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. |

| Alarm Field | Description | | |
|---|---|---|---|
| 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. |
| 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 |

| Alarm Field | Description | | |
|---|---|---|---|
| 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

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td>Description</td><td colspan="3">This alarm is raised when the disk size defined for the ARM Configurator or Router is insufficient for ARM requirements.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">acARMDiskSize</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.70.1.2.2.0.4</td></tr>
<tr><td>Alarm Title</td><td colspan="3">Disk Size Illegal</td></tr>
<tr><td>Alarms Source</td><td colspan="3">■ Configurator<br>■ Router# <Routername></td></tr>
<tr><td>Alarm Type</td><td colspan="3">integrityViolation</td></tr>
<tr><td>Probable Cause</td><td colspan="3">storageCapacityProblem</td></tr>
<tr><th>Alarm Severity</th><th>Condition</th><th>Text</th><th>Corrective Action</th></tr>
<tr><td>Critical</td><td>The size of the hard disk of the ARM Configurator or Router is insufficient for ARM requirements.</td><td>The size of the hard disk in <Configurator or Router->/<Configurator or Router Name> was changed to an illegal size <CurrentSize>. Minimum is <MinimumSize> .</td><td>Increase VM disk size according to the requirements specified in the ARM Installation manual.</td></tr>
</table>

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

## ARM License About to Expire

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the ARM license is about to expire. |
| 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 | This alarm is initially raised 28 days before the expiration date of the license and then for each subsequent day prior to the expiration date. |

## ARM License has Expired

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

## ARM License Session Number

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

## ARM License Missing

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

## Quality Change

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

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

## ARM Configurator Reload

| Alarm Field | Description |
|---|---|
| Description | This alarm is raised when the ARM configurator was reloaded by 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 | ■ The Tomcat server was not restarted properly.<br>■ The ARM Configurator didn’t respond to the number of keep-alive requests from the watchdog. |

## ARM Router Reload

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

## ARM Routing Rule Match

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

## ARM Configuration Inconsistency

| Alarm Field | Description |
|---|---|
| Description | This event is raised when there is mismatch between a Peer connection or a Routing Interface configuration and a Node configuration. |
| SNMP Alarm | acARMConfigurationInconsistency |
| 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><br>Node#<NodeName>/RoutingInterface#<RoutingInterfaceName> |
| Alarm Type | Processing Error Alarm |
| Probable Cause | Configuration or Customization Error |
| Additional Info | ARM database was synchronized to the nodes configuration |
| Alarm Severity | Condition |
| Indeterminate | ■ An inconsistency was discovered between the ARM Topology and the SBC or gateway configuration.<br>■ The element was added to the SBC and discovered by ARM during the synchronization process. |

## Operation State Changed (Router)

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the router state has changed and when an associated Web Service is unavailable, for example call masking for DID and 911 calls. | | |
| SNMP Alarm | acARMOperationStatusChanged | | |
| SNMP OID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.1 | | |
| Alarm Title | Operation Status Changed | | |
| Alarms Source | Router#<RouterName><br>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. | In case state is unavailable:<br>■ Check router status and availability.<br>■ Network connectivity between configurator and router.<br>■ Validate that proper Router credentials updated in ARM.<br>■ Validate DNS setting in case hostname is used. |
| Major | The router is initializing with the ARM Configurator. | Router <RouterName>was marked as Initializing | |
| Major | The configured memory in the router is less than the size required by the license. | Router <RouterName> was marked as not in service due to memory requirements. | This occurs when the number of users does not match the memory requirements.<br>Refer to User's manual / Installation Guide for more information regarding how increase the memory. |
| 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 | Node#<NodeName>/Router#armServer<br>(For IP Profile issues) Node#<NodeName> | | |
| Alarm Type | Communications Alarm | | |
| Probable Cause | Communications Subsystem Failure | | |
| Additional Info | The alarm will be cleared once the status will be changed back to available.<br>Added the routing server to the node | | |
| **Alarm Severity** | **Condition** | **Text** | **Corrective Action** |
| Major | The Routing server node is unavailable. | Routing Server armServer in Node <Node Name> was marked as Unavailable | Check device network connectivity<br>Check the device's network connectivity to the ARM Configurator |

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

## Operation Status Changed [Peer Connection]

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

<table>
<tr><th>Alarm Field</th><th colspan="3">Description</th></tr>
<tr><td></td><td colspan="3">has changed.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">acARMOperationStatusChanged</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.70.1.2.2.0.1</td></tr>
<tr><td>Alarm Title</td><td colspan="3">Operation Status Changed</td></tr>
<tr><td>Alarms Source</td><td colspan="3">Node #<NodeName>/<PeerConnection#<PeerName></td></tr>
<tr><td>Alarm Type</td><td colspan="3">Communications Alarm</td></tr>
<tr><td>Probable Cause</td><td colspan="3">Communications Subsystem Failure</td></tr>
<tr><td>Additional Info</td><td colspan="3">The alarm will be cleared once the status will be changed back to available.</td></tr>
<tr><th>Alarm Severity</th><th>Condition</th><th>Text</th><th>Corrective Action</th></tr>
<tr><td>Major</td><td></td><td>Peer Connection in Node <Node Name> was marked as Unavailable</td><td>When this alarm is received from a Peer Connection and it indicates that the operative state of the Peer Connection has changed to Unavailable:<br>■ Check the configuration of the related IP Group in the specific device.<br>■ Check the device's network connectivity to the configured Proxy IP associated with that IP Group</td></tr>
</table>

| 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. | This alarm is raised when LDAP server state has turned to unavailable:<br>■ Check the LDAP server network connectivity.<br>■ Validate LDAP server credentials. |

| 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. | The ActiveMQ should be restarted automatically. If the alarm doesn't clear after a period of time:<br>■ Check that the ActiveMQ service is working properly<br>■ Collect ActiveMQ logs |

| 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<br>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> | Two configurators are trying to use the router at the same time:<br>■ Check the IP of another configurator, {otherAddress} in the description and make sure only one of them uses the router.<br>■ Restart the tomcat service in the router machine. |

## NTP Sync Status

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

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

## 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. | ■ Make sure that at least one router is configured in your system.<br>■ Check router status and availability.<br>■ Network connectivity between configurator and router.<br>■ Validate that proper Router credentials updated in ARM.<br>■ Validate DNS setting in case hostname is used. |
| 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 #ele-mentName | |
| 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 | acARMExternalWebService |
| SNMP OID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.17 |
| Alarm Title | External Web Service |
| Alarms Source | Web Service#<the name of the service> |

| Alarm 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 | ■ Node#<NodeName>/PeerConnection#<PeerConnectionName><br>■ Resource group#<ResourceGroupName> |
| 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. | ■ Make sure that the calls quota has been configured as required. If not, do one of the following:<br>✓ Delete the Calls Quota limit for the Peer Connection or Resource Group<br>✓ Adjust the Calls Quota limit or Time Scheduling for the Peer Connection or Resource Group |
| Warning | Calls quota threshold has been reached<br>The threshold is configurable, 75% by default | {elementType} {elementName} calls quota threshold has been reached. | ■ Make sure that the calls quota threshold has been configured as required. If not, do one of the following:<br>✓ Delete the Calls Quota for the Peer Connection or Resource Group<br>✓ Change the Threshold for the Peer Connection or |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | Resource Group |
| Clear | ■ Calls Quota has been deleted from the Peer Connection<br>■ Calls Quota has been deleted from the Resource Group<br>■ New time period has started (according to Time Scheduling defined in the Calls Quota)<br>■ Time Scheduling in Calls Quota definition has been modified. For example, set to “monthly” instead of “daily”<br>■ 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) | | |

## 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 | ■ Node#<NodeName>/PeerConnection#<PeerConnectionName>/incoming<br>■ Node#<NodeName>/PeerConnection#<PeerConnectionName>/outgoing<br>■ Node#<NodeName>/PeerConnection#<PeerConnectionName>/total<br>■ PeerConnection#<PeerConnectionName>/incoming<br>■ PeerConnection<PeerConnectionName>/outgoing<br>■ PeerConnection#<PeerConnectionName>/total<br>■ Customer#<CustomerName>/incoming<br>■ Customer#<CustomerName>/outgoing<br>■ Customer#<CustomerName>/total<br>■ VoIP Peer#<VoIPPeerName>/incoming<br>■ VoIP Peer#<VoIPPeerName>/outgoing<br>■ VoIP Peer#<VoIPPeerName>/total | | |
| 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}<br>{elementName} incoming/outgoing/total has exceeded 100% | Make sure that the CAC has been configured as required. If not, do one of the following:<br>- Delete the CAC from the relevant element.<br>- Adjust the CAC limit. |
| Warning | CAC alarm threshold has exceeded the defined value. | {elementType} {elementName} incoming/outgoing/total has exceeded {DefinedThreshold}% | Make sure that the CAC has been configured as required. If not, do one of the following:<br>- Delete the CAC from the relevant element.<br>- Adjust the CAC limit. |
| Clear | - CAC has been deleted from the element<br>- Number of concurrent sessions is lower than the threshold.<br>- Modifying Limit in CAC definition results in alarm clearing for specific element (i.e. for those entities with the CAC applied that fall within | | |

| 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 | ■ Node#<NodeName>/PeerConnection#<PeerConnectionName><br>■ Resource group#<ResourceGroupName> | | |
| Alarm Type | Other | | |
| Probable Cause | Threshold Crossed | | |
| Additional Info | | | |
| Alarm Severity | Condition | Text | Corrective Action |
| Critical | Calls quota limit has been reached. | {elementType} {elementName} calls quota limit/threshold has been reached. | Make sure that the calls quota has been configured as required. If not, do one of the following:<br>■ Delete the Calls Quota limit for the Peer Connection or Resource Group |

| Alarm Field | Description | | |
|---|---|---|---|
| | | | ■ Adjust the Calls Quota limit or Time Scheduling for the Peer Connection or Resource Group |
| Warning | Calls quota threshold has been reached The threshold is configurable, 75% by default | {elementType} {elementName} calls quota threshold has been reached. | ■ Make sure that the calls quota threshold has been configured as required. If not, do one of the following:<br>✓ Delete the Calls Quota for the Peer Connection or Resource Group<br>✓ Change the Threshold for the Peer Connection or Resource Group |
| Clear | ■ Calls Quota has been deleted from the Peer Connection<br>■ Calls Quota has been deleted from the Resource Group<br>■ New time period has started (according to Time Scheduling defined in the Calls Quota) | | |

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

## Certificate Expiration Alarm - ARM

| AlarmField | Description | | |
|---|---|---|---|
| Description | The configurator certificate or the router certificate is about to expire in 20 days or less. | | |
| SNMPAlarm | acARMCertificateExpiration | | |
| SNMPOID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.20 | | |
| AlarmSource | ARM | | |
| AlarmTitle | Certificate expiration | | |
| AlarmType | Equipment Alarm | | |
| Probable Cause | Key Expired | | |
| Additional Info1 | The certificate will expire in less than X days. | | |
| Additional Info2 | | | |
| Alarm Severity | Condition | AlarmText | Corrective Action |
| Critical | | | |
| Major | The certificate expires in less than 7 days. | The certificate of ARM Configurator / Router will expire on <dd/MM/YYYY HH:mm:ss>. | |

| AlarmField | Description | | |
|---|---|---|---|
| Minor | The certificate expires in less than 21 days, however more than 7 days | | |
| Clear | | | |

## Statistics Threshold Alarm

| AlarmField | Description | | |
|---|---|---|---|
| Description | This alarm is raised when a statistics threshold that was defined by an ARM user has been crossed or has returned to normal. | | |
| SNMPAlarm | acARMStatisticThreshold | | |
| SNMPOID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.21 | | |
| AlarmSource | ARM | | |
| AlarmTitle | Statistic threshold | | |
| AlarmType | Operational Violation | | |
| Probable Cause | Threshold Crossed | | |
| Additional Info1 | ■ statisticType value is higher than or equal to the user-defined trigger threshold.<br>■ statisticType can be any of the following: ARM, Router, Node, Peer Connection, Connection, Routing Rule Action, Top Routes, Routing Rule, Routing Group, Calls Quota, Resource Group, Customer, or VoIP Peer. | | |
| Additional Info2 | | | |
| Alarm Severity | Condition | AlarmText | Corrective Action |

| AlarmField | Description | | |
|---|---|---|---|
| Critical | Severity is User defined | #element #statisticName crossed the trigger threshold (#limit) defined in threshold rule #thresholdName | |
| Major | | | |
| Minor | | | |
| Clear | | #element #statisticName clear threshold (#limit) defined in threshold rule #thresholdName is back to normal | |

## Blacklist Contains Numbers Alarms

| AlarmField | Description |
|---|---|
| Description | This alarm is raised when there are numbers contained in the blacklist. |
| SNMPAlarm | acARMBlackListContainsNumbers |
| SNMPOID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.22 |
| AlarmSource | Policy Studio |
| AlarmTitle | Blacklist Contains NumbersAlarms |
| AlarmType | Other |
| Probable Cause | Other |
| Additional Info1 | |
| Additional Info2 | |

| AlarmField | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | AlarmText | Corrective Action |
| Critical | | | |
| Major | | | |
| Minor | The blacklist contains numbers. | Policy Studio <policy studio name > - blocking list contains numbers | |
| Clear | The blacklist is empty. | Policy Studio <policy studio name > - blocking list is cleared | |

## Short Calls Usage Alarm

| AlarmField | Description | | |
|---|---|---|---|
| Description | This alarm is raised when short call profile was crossed on peer connection. | | |
| SNMPAlarm | acARMShortCallsUsage | | |
| SNMPOID | 1.3.6.1.4.1.5003.9.70.1.2.2.0.24 | | |
| AlarmSource | Peer Connection | | |
| AlarmTitle | Short Calls Usage | | |
| AlarmType | Other | | |
| Probable Cause | thresholdCrossed | | |
| Additional Info1 | | | |
| Additional Info2 | | | |
| Alarm | Condition | AlarmText | Corrective |

| AlarmField | Description | | |
|---|---|---|---|
| Severity | | | Action |
| Critical | | Peer connection <peer connection name> limit has been reached. | |
| Major | | | |
| Minor | | | |
| Clear | Any of the following:<br>- Short calls profile has been changed<br>- New time period has started<br>- Short calls profile has been deleted from the Peer Connection | Peer connection <peer connection name> cleared. | |

## 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 |

| Alarm Field | Description |
|---|---|
| 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 | - |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 | - |

| Alarm Field | Description |
|---|---|
| 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 | > |

| Alarm Field | Description |
|---|---|
| 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 |

| Alarm Field | Description |
|---|---|
| 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 |

| Alarm Field | Description |
|---|---|
| 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 description | true |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 {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 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 |
| 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 | true |

| Alarm Field | Description |
|---|---|
| device 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 |
| metrics | (CallEndingsPerMinute - SuccessfulCallsPerMinute) / CallEndingsPerMinute if 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 |

| Alarm Field | Description |
|---|---|
| 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 name | 12 |
| metrics | (CallEndingsPerMinute - SuccessfulCallsPerMinute) / CallEndingsPerMinute if 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 | - |

| Alarm Field | Description |
|---|---|
| level | |
| groupId whitelist | - |

## TTS Delay Alarm

| Alarm Field | Description |
|---|---|
| SNMP | |
| Description | This alarm is sent when the average text-to-speech (TTS) delay over the past 5 minutes 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 name | 13 |
| metrics | AverageTTSDelayMilliseconds if TTSRequestsPerMinute > 10 else 0 |
| group by | ttsProviderId |
| 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 |
| use secondary device description | true |

| Alarm Field | Description |
|---|---|
| MINOR level | 500 |
| MAJOR level | 1000 |
| CRITICAL level | |
| 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 |
| 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" |

| Alarm Field | Description |
|---|---|
| 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 |
| 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}" |

| Alarm Field | Description |
|---|---|
| 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 |
| 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}%" |

| Alarm Field | Description |
|---|---|
| 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.

| Alarm Field | Description |
|---|---|
| SNMP | |
| SNMP Alarm | acVoiceAIDiskUsage |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 |
| 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 |

| Alarm Field | Description |
|---|---|
| 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 |
| 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 |
| 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. |

| Alarm Field | Description |
|---|---|
| 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 |
| 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 | acVoiceAIEndToEndKeepAliveFailed |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.22 |
| Configuration Parameters | |
| alarm name | 22 |

| Alarm Field | Description |
|---|---|
| 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}" |
| 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 |

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

## Remote Manager is Down Alarm

| 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 | Connection with remote manager X is | Check that the configured ovoc connection parameters are correct. Check that the OVOC is up and |

| Alarm Field | Description | | |
|---|---|---|---|
| | down | down | 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 | |

## Send CDR Destination Failure Alarm

| SNMP | |
|---|---|
| Description | This alarm is sent when there is a failure by the Session Manager to send CDRs using the REST API. |
| SNMP Alarm | acVoiceAISendCDRDestinationFailure |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.26 |
| Alarm Title | Send CDR Destination Failure Alarm |
| Configuration Parameters | |
| alarm name | 26 |
| metrics | SendCdrDestinations.FailedRequests |
| group by | sessionManagerId |
| time interval minutes | 10 |
| logical operator | > |
| message | "Send CDR destination request failure on session manager {groupId}" |
| clear message | "Send CDR connection restored on session manager {groupId}" |
| additional info | - |
| MINOR level | - |
| MAJOR level | 0.1 |

| SNMP | |
|---|---|
| CRITICAL level | - |
| groupId whitelist | - |

## Outbound Calls Producer Failures per Minute Alarm

| SNMP | |
|---|---|
| Description | This alarm is sent when the number of failed outbound calls per minute over the last 10 minutes is higher than the threshold. The following includes examples of failed outbound calls:<br>■ Session Manager returns a response that is not 200<br>■ Timeout waiting for response from Session Manager (504)<br>■ Dialout message validation failure (400)<br>■ No such bot exists (400)<br>■ Caller not in allowed callers list (400)<br>■ Authentication error with dialer app (403)<br>■ Error sending message on RabbitMQ (500) |
| SNMP Alarm | acVoiceAIOutboundCallProducerFailure |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.27 |
| Configuration Parameters | |
| alarm name | 27 |
| metrics | ServicesMngr.OutboundCallsProducerFailuresPerMinute |
| group by | none |
| time interval minutes | 10 |
| logical operator | > |
| message | "Outbound calls producer failures per minute is higher than \ {threshold}" |
| clear message | "Outbound calls producer failures per minute over the past {interval} minutes is no longer higher than {threshold}" |
| additional info | "Outbound calls producer failures per minute over the past {interval} minutes is higher than {threshold}, Current value: {current}" |
| MINOR level | - |

| SNMP | |
|---|---|
| MAJOR level | 10 |
| CRITICAL level | - |
| groupId whitelist | - |

## STT Fallbacks Per Provider Alarm

| SNMP | |
|---|---|
| Description | This alarm is sent when the ratio of calls that had speech-to-text (STT) fallbacks over the last 5 minutes on the speech-to-text provider is higher than the threshold. |
| SNMP Alarm | acVoiceAISTTFallbacksPerProvider |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.28 |
| Configuration Parameters | |
| alarm name | 28 |
| metrics | STTFallbacksPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0 |
| group by | sttProviderId |
| time interval minutes | 5 |
| logical operator | > |
| message | "STT provider \{groupId} fallbacks rate is higher than {threshold}" |
| clear message | "Ratio of STT fallbacks per minute over the past {interval} minutes on STT provider {groupId} is lower than {threshold}" |
| additional info | "Ratio of STT fallbacks 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 | - |

| SNMP | |
|---|---|
| groupId whitelist | - |

## TTS Fallbacks Per Provider Alarm

| SNMP | |
|---|---|
| Description | This alarm is sent when the ratio of calls that had text-to-speech (TTS) fallbacks over the last 5 minutes on the speech-to-text provider is higher than the threshold. |
| SNMP Alarm | acVoiceAITTSFallbacksPerProvider |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.29 |
| Configuration Parameters | |
| alarm name | 29 |
| metrics | TTSFallbacksPerMinute / CallEndingsPerMinute if CallEndingsPerMinute > 2 else 0 |
| group by | ttsProviderId |
| time interval minutes | 5 |
| logical operator | > |
| message | "TTS provider \{groupId} fallbacks rate is higher than {threshold}" |
| clear message | "Ratio of TTS fallbacks per minute over the past {interval} minutes on STT provider {groupId} is lower than {threshold}" |
| additional info | "Ratio of TTS fallbacks 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 | - |
| groupId whitelist | - |

## STT Delay Alarm

| SNMP | |
|---|---|
| Description | This alarm is sent when the average speech-to-text (STT) delay over the past 5 minutes on the STT provider is higher than the threshold. |
| SNMP Alarm | acVoiceAISTTDelay |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.30 |
| Configuration Parameters | |
| alarm name | 30 |
| metrics | AverageSTTDelayMilliseconds if STTRequestsWithDelayPerMinute > 10 else 0 |
| group by | sttProviderId |
| time interval minutes | 5 |
| logical operator | > |
| message | "Average STT delay is higher than \{threshold} milliseconds" |
| clear message | "Average STT delay over the past {interval} minutes on STT provider {groupId} is no longer higher than {threshold} milliseconds" |
| additional info | "Average STT delay over the past {interval} minutes on STT provider {groupId} is higher than {threshold} milliseconds, Current value: {current} milliseconds" |
| MINOR level | 1000 |
| MAJOR level | 2000 |
| CRITICAL level | - |
| groupId whitelist | - |

## Turn Delay Alarm

| Alarm Field | Description |
|---|---|
| SNMP | |
| Description | This alarm is sent when the average turn delay over the past 5 minutes on the bot is higher than the threshold. |
| SNMP Alarm | acVoiceAITurnDelay |
| SNMP OID | 1.3.6.1.4.1.5003.9.90.1.2.0.31 |
| Configuration Parameters | |
| alarm name | 31 |
| metrics | AverageTurnDelayMilliseconds if TurnsWithDelayPerMinute > 10 else 0 |
| group by | botId |
| time interval minutes | 5 |
| logical operator | > |
| message | "Average turn delay is higher than \{threshold} milliseconds" |
| clear message | "Average turn delay over the past {interval} minutes on bot {groupId} is no longer higher than {threshold} milliseconds" |
| additional info | "Average turn delay over the past {interval} minutes on bot {groupId} is higher than {threshold} milliseconds, Current value: {current} milliseconds" |
| MINOR level | 1500 |
| MAJOR level | 2500 |
| CRITICAL level | - |
| groupId whitelist | - |

## 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 |
| | acVoiceAIUserDefined2 | 1.3.6.1.4.1.5003.9.90.1.2.0.201 | User defined 2 |
| | acVoiceAIUserDefined 3 | 1.3.6.1.4.1.5003.9.90.1.2.0.202 | User defined 3 |
| | acVoiceAIUserDefined 4 | 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 | |
| Warning | User defined | User defined | |
| Indeterminate | User defined | User defined | |
| Cleared | User defined | User defined | |

## Multi-UCaaS Alarms

Multi-UCaaS alarms are raised for the following products:

- Zoom Phone Provider Exchange
- Live CX
- Webex Cloud Connect
- Webex LGW
- Live Essentials

## Database Connectivity Failed

| Alarm Field | Description | | |
|---|---|---|---|
| Description | This alarm is raised when the Zoom Connect service is unable to access the Azure service of CosmosDB database. | | |
| SNMP Alarm | acZmDbConnectivityFailAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.1 | | |
| Alarm Title | Database Connectivity Failed | | |
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Critical | Cosmos DB service in Azure is not accessible. | <Failed operation> CosmosDB <Database name> err: <error> | Verify Azure service is accessible from the Azure portal. |
| Cleared | Cosmos DB service in Azure is available again. | CosmosDB <Database name> is accessible again. | - |

## Event - App Service Failed

| Alarm Field | Description |
|---|---|
| Description | This event is raised when the Zoom Connect app service fails to perform the following:<br>■ Retrieve the SBC device information from OVOC.<br>■ Execute SBC CLI script. |
| SNMP Alarm | acZmAppServiceFailEvent |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.2 |
| Alarm Title | App Service Failed |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Minor | Failed to generate SBC script. | Empty SBC output for script <SBC Template Name> | ■ The SBC template is corrupted. |
| Minor | Failed to retrieve details from OVOC of the SBC device that is connected to the Zoom Phone system. | Error: Failed to retrieve SBC info from OVOC | Troubleshoot OVOC network connections. |

## Alarm - App Service Configuration failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is raised when the Zoom Connect service configuration is missing or wrong. | | |
| SNMP Alarm | acZmAppServiceCfgFailAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.3 | | |
| Alarm Title | App Service Configuration failure | | |
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Major | Provider | GetCustomerRequestPageInfo: | ■ Add the |

| Alarm Field | Description | | |
|---|---|---|---|
| | configuration is not found in ‘ProvidersInfo’ container. | provider <ProviderName> not found in 'ProvidersInfo' container | provider name specifying that the alarms exists in the CosmosDb ‘ProvidersInfo’ container.<br>■ Restart the Zoom Connect App service. The alarm will be cleared upon restart. |
| Cleared | No cleared message are sent to OVOC since all the alarms are cleared upon App Service restart. | | |

## Alarm – OVOC Connectivity Failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is raised when Zoom Connect service fails to connect to OVOC. | | |
| SNMP Alarm | acZmOvocConnectivityFailAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.11 | | |
| Alarm Title | Ovoc Connectivity failure | | |
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |

| Alarm Field | Description | | |
|---|---|---|---|
| Major | OVOC is not accessible from Zoom Phone Connect | <Failure Message> | ■ Check that OVOC is accessible.<br>■ Verify that app settings OVOC__ BaseUrl is the correct IP address.<br>■ Verify that app settings OVOC__ UserName and OVOC__Password are adjusted to OVOC 'Zoom' operator credentials. |
| Cleared | OVOC is accessible again | OVOC is accessible again | |

## Event – OVOC Action Failed

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The event is sent when Zoom Connect service fails to execute an action on OVOC. | | |
| SNMP Alarm | acZmOvocActionFailEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.12 | | |
| Alarm Title | OVOC Action failed | | |
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Indeterminate | An action executed on the OVOC failed. | <Action description>, Err=<Failure Message> | In case the failure is not the result of connectivity issues, check failure message for the cause. |

## Event – OVOC Life Cycle

| Alarm Field | Description |
|---|---|
| Description | This event is raised when the Zoom Connect service starts when OVOC |

| Alarm Field | Description | | |
|---|---|---|---|
| | clears all the active alarms for this service. | | |
| SNMP Alarm | acZmOvocLifeCycleEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.13 | | |
| Alarm Title | OVOC Life Cycle | | |
| Alarm Source | N/A | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Indeterminate | Zoom Connect service starting. | Zoom Service Started | |

## SBC Connectivity Failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is raised when the Zoom Connect service fails to connect to the SBC device. | | |
| SNMP Alarm | acZmSbcConnectivityFailAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.21 | | |
| Alarm Title | SBC Connectivity failure | | |
| Alarm Source | <SBC Name> | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Major | The SBC is not accessible from the Zoom Connect | A connection attempt failed because the | Verify that the IP address that specified in the alarm is |

| Alarm Field | Description | | |
|---|---|---|---|
| | | connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond. (<SBC IP Address>). | accessible from the Zoom Connect network. |
| Major | Invalid SBC credentials | Error while copying content to a stream. | Verify that the SBC credentials in the OVOC are the correct one. |
| Major | SBC Credentials missing | The SBC credentials in the OVOC are missing. | Verify the ‘Zoom’ operator in the OVOC has enough privileges to retrieve the SBC password in the response of Get SBC Info. |
| Cleared | SBC is accessible again | SBC is accessible again. | |

## Event – SBC Action Failed

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The event is sent when Zoom Connect service failed to execute an action on SBC. | | |
| SNMP Alarm | acZmSbcActionFailEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.22 | | |
| Alarm Title | SBC Action Failed | | |
| Alarm Source | <SBC Name> | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Alarm Severity | Condition | <text> | Corrective Action |
| Minor | Any action failure on SBC | <Failure message> | |

## Zoom Connectivity Failure Alarm - Carrier Exchange

| Alarm Field | Description |
|---|---|
| Description | The alarm is raised when the Zoom Connect service fails to connect to the Zoom Phone system. |
| SNMP Alarm | acZmZoomConnectivityAlarm |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.21 |
| Alarm Title | Alarm – Zoom Connectivity Failure |
| Alarm Source | <Carrier Exchange name> |
| Alarm Type | Other |
| Probable Cause | Other |
| Additional Info1 | |

| Alarm Field | Description | | |
|---|---|---|---|
| Additional Info2 | | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Major | The Zoom API is not accessible from the Zoom Connect ACV APP. | Zoom is not accessible at <zoom url> | Verify network connections. |
| Major | Invalid Carrier Exchange credentials. | Zoom access failed due to invalid Carrier Exchange credentials. | Verify that Carrier Exchange credentials in systemConfig container are modified according to Carrier Exchange ‘application’ at Zoom market place. Restart of the server running the Zoom Connect ACV APP is required to apply the update. |
| Cleared | Zoom is accessible again. | Zoom is accessible again at <zoom url> | |

## Zoom Connectivity Failure Alarm - Provider

| Alarm Field | Description |
|---|---|
| Description | The alarm is raised when Zoom Connect service failed to connect to Zoom system |

| Alarm Field | Description | | |
|---|---|---|---|
| SNMP Alarm | acZmZoomConnectivityAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.31 | | |
| Alarm Title | Zoom Connectivity failure | | |
| Alarm Source | <provider name> | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info1 | | | |
| Additional Info2 | | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Major | The Zoom api is not accessible from the Zoom Connect | Zoom is not accessible at <zoom url> | |
| Major | Invalid provider credentials | Zoom access failed due to invalid provider credentials | Verify that provider's credentials in systemConfig container are adjusted to provider 'application' at Zoom market place.<br>Need to restart after change. |
| Cleared | Zoom is accessible again | Zoom is accessible again at <zoom url> | |

## Event – Zoom Action Failed

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The event is sent when the Zoom Connect service failed to execute an action on the Zoom environment. | | |
| SNMP Alarm | acZmZoomActionFailEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.32 | | |
| Alarm Title | Zoom Action Failed | | |
| Alarm Source | - | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info1 | - | | |
| Additional Info2 | - | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Indeterminate | Customer action failed | Customer <customer name> failed to <action name> in zoom | |

## Event – Zoom Authentication Failure

| Alarm Field | Description |
|---|---|
| Description | The event is sent when the Zoom Connect service fails to execute an action on the Zoom environment. |
| SNMP Alarm | acZmZoomAuthFailEvent |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.33 |
| Alarm Source | <SBC Name> |
| Alarm Title | Zoom Authentication failure |
| Alarm Type | Other |
| Probable Cause | Other |

| Alarm Field | Description | | |
|---|---|---|---|
| Alarm Severity | Condition | <text> | Corrective Action |
| Indeterminate | Customer action failed due to an authentication failure | Customer <customer name> authentication failed during <action name> in zoom action | Customer user should handle it independently. Logout from service, close tab, relogin and execute the action again. |

## Event – Webhook Service Failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The event is sent when Zoom Connect service failed to send a request to webhook service | | |
| SNMP Alarm | acZmWebhookActionFailEvent | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.5 | | |
| Alarm Title | Webhook action failure | | |
| Alarm Source | - | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info1 | - | | |
| Additional Info2 | - | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Indeterminate | Failed to send notification request to webhook service. | Webhook request to {notification url} failed. | Provider or channel should check:<br>1. Request details are current.<br>2. Webhook service is using the request body as describes in the documentation. |

## Alarm – Assigned Users Count Failure

| Alarm Field | Description | | |
|---|---|---|---|
| Description | The alarm is raised when the Zoom Connect service fails to retrieve and count the assigned users from the Zoom service. | | |
| SNMP Alarm | acZmAssignedUsersCountFailAlarm | | |
| SNMP OID | .1.3.6.1.4.1.5003.9.120.3.2.0.4 | | |
| Alarm Title | Assigned users count failure | | |
| Alarm Source | ■ <provider name> - when the failure related to a provider<br>■ Empty – when the task was not running in the past 24 hours | | |
| Alarm Type | Other | | |
| Probable Cause | Other | | |
| Additional Info1 | - | | |
| Additional Info2 | - | | |
| Alarm Severity | Condition | Alarm Text | Corrective Action |
| Minor | The assigned users count task was not triggered by the Azure triggered function. Updates were not sent to the Zoom-Connect service for more than 24 hours. | The assigned users count task was not run more than {configurable threshold} hours. | Need to go to Azure Function App and look for errors in the log of $$$$$. |
| Clear | The assigned users count task run | The assigned users count task is run successfully. | - |

| Alarm Field | Description | | |
|---|---|---|---|
| | successfully | | |
| Minor | Failed to run the assigned users count task for specific provider | Failed to run assigned users task for {providername} | Check that the credentials in Server 2 Server OAuth application of the provider are aligned with the configuration of the provider in Zoom-Connect systemConfig. |
| Clear | The assigned users count task for specific provider was run successfully. | Calculate the assigned users for provider {providername} succeed. | - |

**This page is intentionally left blank.**

**International Headquarters**

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

Document #: LTRT-41815