Release Notes

*AudioCodes Session Border Controllers and Media Gateway Series*

# SBCs and Media Gateways

*Long Term Support (LTS) Versions*

Version 7.40A.500

# Table of Contents

# List of Tables

## 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: July-03-2025

## 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.

## Stay in the Loop with AudioCodes

## Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual, unless otherwise specified, the term *device* refers to the AudioCodes products.

## Related Documentation

| Document Name |
|---|
| Mediant 500L Gateway and E-SBC Hardware Installation Manual |
| Mediant 500L Gateway and E-SBC User's Manual |
| Mediant 500 E-SBC Hardware Installation Manual |
| Mediant 500 E-SBC User's Manual |
| Mediant 800 Gateway and E-SBC Hardware Installation Manual |
| Mediant 800 Gateway and E-SBC User's Manual |
| Mediant 1000B Gateway and E-SBC Hardware Installation Manual |
| Mediant 1000B Gateway and E-SBC User's Manual |
| MP-1288 High-Density Analog Media Gateway Hardware Installation Manual |
| MP-1288 High-Density Analog Media Gateway User's Manual |

| Document Name |
|---|
| Mediant 3100 Gateway & E-SBC User's Manual |
| Mediant 3100 Gateway & E-SBC Hardware Installation Manual |
| Mediant 2600 E-SBC Hardware Installation Manual |
| Mediant 2600 E-SBC User's Manual |
| Mediant 4000 SBC Hardware Installation Manual |
| Mediant 4000 SBC User's Manual |
| Mediant 9000 SBC User's Manual |
| Mediant 9000 SBC Hardware Installation Manual |
| Mediant Software SBC User's Manual |
| SBC-Gateway CLI Reference Guide |
| SBC-Gateway Performance Monitoring Reference Guide |
| SBC-Gateway SNMP Alarms Reference Guide |

## Document Revision Record

| LTRT | Description |
|---|---|
| 27765 | Ver. 7.40A.502.090 |
| 27757 | Ver. 7.40A.501.871 |
| 27755 | Ver. 7.40A.501.869 |
| 27754 | Note about DS1_v2; typo (D4ds_v5) for Mediant CE SC on Azure; Mediant 3100 T1 capacity |
| 27751 | Ver. 7.40A.501.863 |
| 27750 | Ver. 7.40A.501.858 |
| 27747 | Ver. 7.40A.501.841 |
| 27746 | Resolved constraint re Master user level (obsolete). |
| 27742 | Ver. 7.40A.501.661 |
| 27741 | Ver. 7.40A.501.649 |
| 27737 | Ver. 7.40A.501.392 |
| 27734 | Ver. 7.40A.501.384 |
| 27731 | Ver. 7.40A.501.158 |
| 27727 | Versions 7.40A.501.149 and 7.40A.501.150; V.150.1 removed |
| 27725 | More fixed bugs added to Resolved Constraints of Ver. 7.40A.501.141 |
| 27723 | Ver. 7.40A.501.141 |
| 27722 | Mediant VE Hyper-V 4 vCPU and GCP n2-standard-2 registered users capacity updated; Mediant 800C non-hybrid SBC capacity updated |
| 27717 | SRTP capacity update for Mediant 800C |
| 27714 | Ver. 7.40A.500.786 |

| LTRT | Description |
|---|---|
| 27712 | New LTS stream - baseline 7.4.0A.500.781 (from LR); TLS capacity updated for Mediant 2600/Mediant 4000; Azure capacity updated for Mediant CE; MSRP capacity added |
| 27707 | Ver. 7.40A.500.781 |
| 27705 | Ver. 7.40A.500.775; SRTP capacity updated for GCP n2-standard-4 (Mediant VE) |
| 27691 | Ver. 7.40A.500.357; 7.20A.259.* added for 7.2-to-7.4 upgrade; Mediant VE capacity updated for Azure (D2ds_v5, D4ds_v5, and D8ds_v5); Mediant VE note for 5,000 sessions |
| 27686 | Ver. 7.40A.500.019 |
| 27676 | Mediant 3100 gateway capacity updated |
| 27673 | Typo - 8-GB RAM for GCP Media Components (Mediant CE) |
| 27670 | Ver. 7.40A.500.017 |
| 27666 | Ver. 7.40A.500.010 |
| 27665 | Version 7.40A.400.067 and 7.40A.260.313 |
| 27661 | Typo (GCP capacity) |
| 27659 | Ver. 7.40A.400.063 |
| 27652 | Ver. 7.40A.400.042; 7.2-to-7.4 upgrade note updated (7.20A.258.919 removed); feature added to Ver. 7.40A.400.023 for Mediant VE/CE Ddsv5 support; Mediant VE on Azure capacity (D2ds_v5 / D4ds_v5 / D8ds_v5) |
| 27647 | Ver. 7.40A.300.021 |
| 27644 | Ver. 7.40A.400.023; know constraint SBC-42301 added to Ver. 7.40A.260.007 |
| 27641 | WebRTC capacity note updated. |
| 27637 | Ver. 7.40A.260.152. |
| 27635 | Ver. 7.40A.300.013. |
| 27627 | Ver. 7.40A.300.012; GCP capacity; Access List table and Proxy Sets capacity; trademarks and USA address. |
| 27621 | Capacity updated for Forward On Busy Trunk Destination. |
| 27620 | Initial document release for Version 7.4. |

# 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.

# 1 Introduction

This document describes the Long Term Support (LTS) versions for Release 7.4 of AudioCodes' Session Border Controllers (SBC) and Media Gateways.

**Note:**

- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available License Keys that can be purchased, please contact your AudioCodes sales representative.
- Open-source software may have been added and/or amended. For further information, contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in this release documentation. Click here to check for an updated document version on AudioCodes website.

## 1.1 Software Revision Record

The following table lists the LTS versions for Release 7.4.

**Note:** The latest software versions can be downloaded from AudioCodes' Services Portal (registered Customers only).

**Table 1-1: Software Revision Record of LTS Versions**

| LTS Version | Released Date |
|---|---|
| 7.40A.502.090 (7.4.500-7) | June 20, 2025 |
| 7.40A.501.871 (7.4.500-6.03b) | May 12, 2025 |
| 7.40A.501.869 (7.4.500-6.03) | April 29, 2025 |
| 7.40A.501.863 (7.4.500-6.02) | March 23, 2025 |
| 7.40A.501.858 (7.4.500-6.01) | February 26, 2025 |
| 7.40A.501.841 (7.4.500-6) | February 3, 2025 |
| 7.40A.501.661 (7.4.500-5.01) | December 24, 2024 |
| 7.40A.501.649 (7.4.500-5) | December 4, 2024 |
| 7.40A.501.392 (7.4.500-4.01) | September 11, 2024 |
| 7.40A.501.384 (7.4.500-4) | August 22, 2024 |
| 7.40A.501.158 (7.4.500-3.02) | July 16, 2024 |
| 7.40A.501.150 (7.4.500-3.01-1) | June 16, 2024 |
| 7.40A.501.149 (7.4.500-3.01) | June 16, 2024 |
| 7.40A.501.141 (7.4.500-3) | May 26, 2024 |

| LTS Version | Released Date |
|---|---|
| 7.40A.500.786 (7.4.500-2.02) | March 26, 2024 |
| 7.40A.500.781 (7.4.500-2.01)<br>**Note:** This is the initial LTS version. | January 31, 2024 |
| **Previous LR Versions** | |
| 7.40A.500.775 (7.4.500-2) | January 14, 2024 |
| 7.40A.500.357 (7.4.500-1) | October 10, 2023 |
| 7.40A.500.019 (7.4.500-02) | August 29, 2023 |
| 7.40A.500.017 (7.4.500-01) | June 5, 2023 |
| 7.40A.500.010 (7.4.500) | May 18, 2023 |
| 7.40A.400.067 (7.4.400-04) | May 15, 2023 |
| 7.40A.260.313 (7.4.260-03) | May 1, 2023 |
| 7.40A.400.063 (7.4.400-03) | April 13, 2023 |
| 7.40A.400.042 (7.4.400-02) | March 6, 2023 |
| 7.40A.300.021 (7.4.300-04) | February 14, 2023 |
| 7.40A.400.023 (7.4.400-01) | January 19, 2023 |
| 7.40A.260.152 (7.4.260-1) | November 3, 2022 |
| 7.40A.300.013 (7.4.300-02) | October 26, 2022 |
| 7.40A.300.012 (7.4.300-01) | September 5, 2022 |
| 7.40A.260.007 | May 3, 2022 |

## 1.2 Supported Products

The following table lists the SBC and Media Gateway products supported in this release.

**Note:**

- Product support and hardware configurations may change without notice. Currently available hardware configurations are listed in AudioCodes Price Book. For further enquiries, please contact your AudioCodes sales representative.
- Figures shown in the tables in this section are maximum values per interface. For available hardware configurations including combinations of supported interfaces, contact your AudioCodes sales representative.

**Table 1-2: SBC and Media Gateway Products Supported in Release 7.4**

| Product | Telephony Interfaces | | | Ethernet Interfaces | USB | OSN |
|---|---|---|---|---|---|---|
| | FXS/FXO | BRI | E1/T1 | | | |
| Hybrid SBC and Gateway Series | | | | | | |
| Mediant 500 Gateway & E-SBC | - | - | 1/1 | 4 GE | 1 | - |
| Mediant 500L Gateway & E-SBC | 4/4 | 4 | - | 4 GE | 1 | - |
| Mediant 800B Gateway & E-SBC | 12/12 | 8 | 2 | 4 GE / 8 FE | 2 | √ |
| Mediant 800C Gateway & E-SBC | 12/12 | 8 | 4 | 4 GE / 8 FE | 2 | √ |
| Mediant 1000B Gateway & E-SBC | 24/24 | 20 | 6/8 | 7 GE | - | √ |
| MP-1288 Gateway & E-SBC | 288/0 | - | - | 2 GE | 1 | - |
| Mediant 3100 Gateway & E-SBC | - | - | 64 | 8 GE | 1 | - |
| SBC Series | | | | | | |
| Mediant 2600 E-SBC | - | - | - | 8 GE | - | - |
| Mediant 4000 SBC | - | - | - | 8 GE | - | - |
| Mediant 4000B SBC | - | - | - | 8 GE | - | √ |
| Mediant 9030 SBC | - | - | - | 12 GE | - | - |
| Mediant 9080 SBC | - | - | - | 12 GE | - | - |
| Mediant SE SBC | - | - | - | 12 GE | - | - |
| Mediant VE SBC | - | - | - | 12 GE | - | - |
| Mediant CE SBC | - | - | - | 12 GE | - | - |

## 1.3 Terms Representing Product Groups

Throughout this document, the following terms are used to refer to groups of AudioCodes products for feature applicability. Where applicability is specific to a product, the name of the product is used.

**Table 1-3: Terms Representing Product Groups**

| Term | Product |
|---|---|
| *Analog* | Products with analog interfaces (FXS or FXO):<br>▪ MP-1288<br>▪ Mediant 500L Gateway & E-SBC<br>▪ Mediant 800 Gateway & E-SBC (Rev. B and C)<br>▪ Mediant 1000B Gateway & E-SBC |
| *Device* | All products |
| *Digital* | Products with digital PSTN interfaces (ISDN BRI or PRI):<br>▪ Mediant 500 Gateway & E-SBC<br>▪ Mediant 500L Gateway & E-SBC<br>▪ Mediant 800 Gateway & E-SBC (Rev.<br>▪ Mediant 1000B Gateway & E-SBC B and C)<br>▪ Mediant 3100 Gateway & E-SBC |
| *Mediant 90xx* | ▪ Mediant 9000<br>▪ Mediant 9000 Rev. B<br>▪ Mediant 9030<br>▪ Mediant 9080 |
| *Mediant Software* | Software-based products:<br>▪ Mediant SE SBC<br>▪ Mediant VE SBC<br>▪ Mediant CE SBC |

# 2 Long Term Support (LTS) Versions

This chapter describes the LTS versions of Release 7.4.

## 2.1 Version 7.40A.502.090

This version includes resolved new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**
  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.8.9 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.4 (8.4.591, or 8.4.3068 and later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

## 2.1.1 New Features

This section describes the new features introduced in this version.

### 2.1.1.1 Pause and Resume SIPREC Sessions through REST API

SIPREC (SIP Recording) sessions can now be paused and resumed through the device's REST API. This enhancement enables greater control and flexibility over recording sessions.

This feature uses the following new REST API commands:

- **Pause SIPREC session:**

```
POST /api/v1/sip/sipRecording?command=pause&callKey=<key>
```

- **Resume SIPREC session:**

```
POST /api/v1/sip/sipRecording?command=resume&callKey=<key>
```

**Applicable Applications:** All

**Applicable Products:** All (except Mediant 1000)

### 2.1.1.2 Increased Number of Proxy Servers Attempted for Proxy Hot Swap

When the Hot Swap feature is enabled for a Proxy Set, the device now can try up to nine proxy servers (IP addresses) in the Proxy Set when a failure happens in sending the SIP dialog-initiating message. Previously (and still supported by devices not mentioned in 'Applicable Products' below), the device attempted up to four IP addresses in the Proxy Set.

This change improves resiliency and failover handling, by allowing the device to attempt more alternate proxy servers during call setup.

**Note:** This enhancement affects only the number of IP addresses the device attempts to contact during call setup when Hot Swap is enabled. It doesn't change the number of IP addresses that can be configured per Proxy Set.

**Applicable Applications:** SBC

**Applicable Products:** Mediant Software; Mediant 90xx

### 2.1.1.3 New KPIs for SBC Call Failure Rate

The device now supports the measurement of SBC call failure rates, providing enhanced visibility into call performance. The failure rate is expressed as a percentage, calculated using the formula:

*Failed Call Rate (%) = Number of Failed Calls / Total Number of Calls × 100*

These new Key Performance Indicators (KPIs) are available at three levels: Global, Per IP Group, and Per SRD, enabling detailed performance monitoring across different network segments.

- **Global:**
  - acKpiSbcCallStatsCurrentGlobalFailedCallsInRatio
  - acKpiSbcCallStatsCurrentGlobalFailedCallsOutRatio
  - acKpiSbcCallStatsIntervalGlobalFailedCallsOutRatioAvg
  - acKpiSbcCallStatsIntervalGlobalFailedCallsInRatioAvg
- **Per IP Group:**
  - acKpiSbcCallStatsCurrentIpGroupFailedCallsOutRatio
  - acKpiSbcCallStatsCurrentIpGroupFailedCallsInRatio
  - acKpiSbcCallStatsIntervalIpGroupFailedCallsInRatioAvg
  - acKpiSbcCallStatsIntervalIpGroupFailedCallsOutRatioAvg
- **Per SRD:**
  - acKpiSbcCallStatsCurrentSrdFailedCallsOutRatio
  - acKpiSbcCallStatsCurrentSrdFailedCallsInRatio
  - acKpiSbcCallStatsIntervalSrdFailedCallsInRatioAvg
  - acKpiSbcCallStatsIntervalSrdFailedCallsOutRatioAvg

**Applicable Application:** SBC

**Applicable Products:** All

### 2.1.1.4 Miscellaneous

- The CLI command `dns-fallback-policy` has been relocated to `configure network > dns settings`.
- Importing a Dial Plan file through the Web interface now displays a confirmation message to clearly inform users of the differences between importing to the parent page (Dial Plan table) and importing to the child page (Dial Plan Rules table).

### 2.1.2 Known Constraints

This section lists known constraints.

**Table 2-1: Known Constraints in Version 7.40A.502.090**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-58156 | OVOC Version 8.4 doesn't connect to the device when TLS 1.3 is used (only connects for TLS 1.2). | OVOC Version 8.4 doesn't connect to device | Low | All | - |

### 2.1.3 Resolved Constraints

This section lists resolved constraints.

**Table 2-2: Resolved Constraints in Version 7.40A.502.090**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-56231 | The device sends the SIP ACK request to the wrong destination when it contains multiple SIP Record-Route headers. | Call failure | Medium | All | n/a |
| SBC-56586 | The variable for message manipulation is limited to 1,500 characters, preventing users from copying and storing values of long headers. | Message Manipulation limitation | Low | All | n/a |
| SBC-56595 | The device loses some DTMFs for a transcoding call because of a bug in the DSP. | Missing DTMFs | Medium | All | n/a |
| SBC-56623 | The device disconnects a call because of a bug in the session-timer mechanism for specific scenarios. | Call disconnection | Medium | All | n/a |
| SBC-56667 | The device excludes the SIP Content-Length header in multi-part SDP body. | Incorrect SDP size | Medium | All | n/a |
| SBC-56684 | The parameters [VerifyRecievedRequestUri] and [RegistrarProxySetID] don't function correctly when the SIP Interface is different to the registrar Proxy Set, causing the device to reject the incoming SIP INVITE request. | Call failure | Medium | All | n/a |
| SBC-56735<br>SBC-56737 | Device exposed to security vulnerabilities SYSS-2025-12 (possible to change HTTP from POST to GET) and SYSS-2025- | Vulnerabilities | High | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | 13 (CSRF token can be bypassed). | | | | |
| SBC-56763 | The device mistakenly considers a registered user as not behind NAT, causing call failure | Call failure | Medium | All | N\A |
| SBC-56785 | The device fails to include the Authorization header for REST CDR. | REST CDR failure | Medium | All | n/a |
| SBC-56865 | The device rejects SIP messages that contain more than 100 headers. | Call failure | Medium | All | n/a |
| SBC-56871 | The device adds spaces to CDR fields (causing them to be unreadable for the user) when the user-part contains special characters like “,”. | CDR corrupted fields | Medium | All | n/a |
| SBC-56909 | The device supports only four IP addresses resolved by NAPTR record, ignoring the rest of the resolved IP addresses. | Incorrect DNS resolved | Medium | All | n/a |
| SBC-56926 | The device doesn’t send identical SDP offers for direct media (different incoming SDP offer and outgoing SDP offer). | SDP differences for direct media | Medium | All | n/a |
| SBC-57020<br>SBC-57799 | The device is exposed to a cross-site scripting vulnerability on the Topology View page of the Web interface. | Vulnerability | Medium | All | n/a |
| SBC-57175 | The device doesn't support SFTP connection using CyberDuck | SFTP connection failure | Medium | All | n/a |
| SBC-57205 | The device doesn’t release the HTTP buffer upon releasing a call and sending REST CDR HTTP POST messages with STOP but not getting any response. | Resource pool leak | Medium | All | n/a |
| SBC-57227 | The device doesn’t send a SIP re-INVITE for media sync, causing a Teams LMO call to fail for a specific call scenario. | LMO call failure | Medium | All | n/a |
| SBC-57239 | The device fails to decrypt SRTP packets during a call because of incorrect detection of ROC changes. | No voice | Medium | All | n/a |
| SBC-57242 | The device fails to increase the SDP version in the SIP 200 OK response for session-timer refresh. | Incorrect SDP version | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-57259 | The device fails to establish an SSH connection from OVOC over the tunnelling interface. | Failed SSH connection | Low | All | n/a |
| SBC-57296 | The device closes the TLS connection when handling SIP OPTIONS requests based on destination type "Internal" in the IP-to-IP Routing table, even though the global parameters [RELIABLECONNECTIONPERSISTENTMODE] and [FAKETCPALIAS] are enabled. | Device terminates connection | Medium | All | n/a |
| SBC-57345 | The device restarts with exception message “Signal 10, Task WEBS” when using Azure AD login. | Device restarts | Medium | All | n/a |
| SBC-57430 | Security vulnerability CVE-2024-50302. | Vulnerability | Medium | All | n/a |
| SBC-57443<br>SBC-58042 | The device decreases its SRTP packet sequence during hold-retrieve, causing one-way voice. | One-way voice | Medium | All | n/a |
| SBC-57452<br>SBC-57784<br>SBC-58455 | The device sends unexpected SIP UPDATE requests during call establishment, causing a possible call failure. | Call failure | Medium | All | n/a |
| SBC-57571 | The device’s Web Service authentication fails when authentication type is digest. | Web Service authentication failure | Medium | All | n/a |
| SBC-57575 | One-way voice occurs after call transfer because the one call leg remains in hold and the device fails to perform media sync. | One-way voice | Medium | All | n/a |
| SBC-57704 | The device is not reachable over SSH after an HA switchover. | SSH disabled | Medium | HA | n/a |
| SBC-57751 | The device fails to be configured with KPI type average (such as Failed Calls In and Failed Calls Out (Ratio) in the Alarms Thresholds table. | KPI limitations | Medium | All | n/a |
| SBC-57783 | The device rejects a SIP re-INVITE with a 488 response and disconnects the call when the IP Profile’s parameter 'Generate SRTP Keys Mode' is configured with 'Keep original' and the Teams side sends a new crypto suite. | Call failure | Medium | All | n/a |
| SBC-57842 | The device creates an incorrect SIP User-to-User header. | Incorrect header format | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-57901 | The device sends the syslog error message "SYSTEM ERROR: core 0, Id - 21, Counter - 1, errno - 145 [Code:0x2002d]". | Syslog error | Low | All | n/a |
| SBC-58025 | The device fails to add a SIP header which was added to the original outgoing INVITE by message manipulation, to the authenticated INVITE (in case server challenges with 401/407). | SIP INVITE missing header | Medium | All | n/a |
| SBC-58036 | The Web user status changes from "valid" to "inactivity" after a device restart. | Web user not active | Medium | All | n/a |
| SBC-58105 | The device fails to send an alternative HTTP get request, causing call failure. | Call failure | Medium | All | n/a |
| SBC-58135 | A re-INVITE failure for WebRTC calls causes call failure in a specific call scenario involving DNS resolved addresses and Poxy Hot Swap feature. | Call failure | Medium | All | n/a |
| SBC-58148 | The device fails to send the correct call status messages to the ARM for consultive transfer, causing the transfer to fail. | Transfer failure | Medium | All | n/a |
| SBC-58176 | The device undergoes an HA switchover with the exception "Signal 11, Task SPMR", caused by the device attempting to access a resource that was already deallocated. | Device restarts | Medium | All | n/a |
| SBC-58307 | The device restarts with the exception "Signal 904, Task WEBS" when adding a new row in the Alarm Customization table that has the same name as an existing row, only with a different severity. | Device restarts | Medium | All | n/a |
| SBC-58404 | The device's CLI command update-frequency-sec is not saved after an HA switchover. | CLI command value not applied after a switchover | Low | All | n/a |
| SBC-58406 | The device rejects SIP UPDATE requests on a race condition with a SIP 500 response instead of rejecting it with a 491 response. | Incorrect SIP response | Low | All | n/a |

## 2.2 Version 7.40A.501.871

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.8.9 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.2.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-3: Resolved Constraints in Version 7.40A.501.871**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-58106<br>SBC-58126 | The device can’t establish a connection with the Floating license server (OVOC). | No connection with Floating license server | High | All | n/a |

## 2.3 Version 7.40A.501.869

This version includes new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.8.9 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.3.1 New Features

This section describes the new features introduced in this version.

#### 2.3.1.1 Configurable Retries for TCP/TLS Connection Failures

The number of retry attempts that the device makes when attempting to reconnect to a server (Proxy Set) after a TCP/TLS connection failure can now be configured. Previously, the maximum number of retries was hardcoded (5). Now it can be configured from 1 to 20.

This feature is configured by the new ini file parameter [ReliableConnectionFailureRetries].

**Applicable Applications:** All

**Applicable Products:** All

### 2.3.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-4: Resolved Constraints in Version 7.40A.501.869**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-56780 | Calls are disconnected because of an issue with SIP UPDATE messages after upgrading to 7.40A.501.841. | Call failure | High | All | VMware |
| SBC-56780<br>SBC-57087<br>SBC-57110<br>SBC-57235 | SBC call failure occurs because of incorrect handling of an incoming SIP UPDATE message | Call failure | High | All | n/a |
| SBC-57087 | Calls fail because of incorrect handling of SIP UPDATE messages. | Call failure | High | All | ARM |
| SBC-57110 | The device generates the message "All medias are not supported" when refreshing (SIP UPDATE) both ends. | Call ends | High | All | AWS |
| SBC-57235 | The device rejects the second SIP UPDATE message with a 488 response. | Call failure | High | All | - |
| SBC-57252 | The device's WebSocket tunnel with OVOC fails when using FQDN and a specific Imperva router (device sends both FQDN and IP address, while Imperva router expects only FQDN). | WebSocket tunnel with OVOC failure | High | All | n/a |
| SBC-57342 | SBC Reliable (TCP) Connection Failure Retry should be configurable | Parameter to control the TCP connection reuse | Medium | All | n/a |
| SBC-57568<br>SBC-57834<br>SBC-56265 | The device's connection with ARM is unstable because the device handles a "chunked body" from ARM incorrectly. | Unstable ARM connection | High | All | n/a |
| SBC-57650<br>SBC-57693<br>SBC-57754<br>SBC-58004 | SBC Call failure as a result SBC incorrectly sending SIP UPDATE message in the middle of the call | SBC call failure | High | All | n/a |

## 2.4 Version 7.40A.501.863

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.7.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.4.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-5: Resolved Constraints in Version 7.40A.501.863**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-56317 | The device's connection to ARM is unstable after the device is upgraded. | Unstable ARM connection | High | All | AudioCodes ARM |
| SBC-56656 | The device can't be added to ARM. | No ARM functionality | High | All | AWS |
| SBC-56801 | The device becomes unresponsive and restarts. | Device restart | High | Mediant 4000 | - |
| SBC-56987 | ARM nodes go down after testing a fallback scenario. | No routing by ARM | High | All | AudioCodes ARM |
| SBC-57001 | The device's connection to the ARM routers are lost upon a switchover. | No connection to ARM | High | All | AWS |

## 2.5 Version 7.40A.501.858

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.7.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.5.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-6: Resolved Constraints in Version 7.40A.501.858**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53963<br>SBC-55073 | The device has insufficient resources (syslog message "no more free id") due to incorrect handling of SIP CANCEL requests for forking calls, causing call processing failure for new calls. | Device stops handling new calls | High | All | n/a |
| SBC-56466 | The 'Default Access Level' parameter has value of sec-admin in 7.4.500 instead of block, causing a security breach. | Vulnerability | High | All | n/a |
| SBC-56480<br>SBC-56587<br>SBC-56685 | The device sends an incorrect SDP answer, containing two identical DTMF payload types on a transcoding call that involves both SILK NB and WB. | Device sends incorrect SDP answer | Medium | All | n/a |
| SBC-56583 | The device restarts because of using S3 URLs in cloud-init. | Device restarts | High | All | AWS |
| SBC-56610 | The device restarts with the error message "Signal 11, Task SPMR" because of incorrect media channel handling after a restart. | Device restarts | Medium | All | Azure |
| SBC-56742 | The device sends a SIP re-INVITE to the SIPREC server with incorrect crypto keys. | SRS decryption error | Medium | All | n/a |

## 2.6 Version 7.40A.501.841

This version includes new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.7.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

## 2.6.1 New Features

This section describes the new features introduced in this version.

### 2.6.1.1 Azure Blob Storage for Debug Recording Files

The device now supports the ability to send locally stored debug recording files directly to a Customer's Microsoft Azure Blob Storage account (container). Once the device creates a debug recording file in its local storage, it sends it to the Blob container and deletes the file from local storage.

This feature can be configured through the following new parameters, which have been added to the Debug Recording page:

- 'Storage Location': Specifies where the debug recordings are stored, either locally (existing support) or in the Blob storage container.
- 'Storage URL': Defines the URL of the Blob storage container.
- 'Container': Specifies the name of the Blob storage container.
- 'Account Key': Defines the shared access signature (SAS) token key required for secure access to the Blob storage container.

**Note:** The local storage feature must be enabled for this functionality (using the existing 'Local Storage' parameter).

**Applicable Applications:** SBC

**Applicable Products:** Mediant 9000; Mediant Software

### 2.6.1.2 Prefix for Debug Recording Files in Local and Azure Blob Storage

The file names of locally stored debug recording files, including those sent to Azure Blob storage (see previous feature) can now be customized with a user-defined prefix. The prefix is configured using the new 'File Name Prefix' parameter on the Debug Recording page.

By configuring a file name prefix, users can now easily identify and categorize their debug recordings, both locally and in Azure Blob storage.

File naming formats are now as follows:

- **Locally stored debug recording files:**

  ```
  <Prefix>_DR_<YYYY>_<Month>_<DD>__<HH_MM_SS>_<Sequence>.gz
  ```

- **Locally stored debug recording files sent to Azure Blob storage:**

  ```
  <Deployment ID>_<Prefix>_DR_<Device Serial
  Number>_<YYYY>_<Month>_<DD>__<HH_MM_SS>_<Sequence>.gz
  ```

**Note:** *Deployment ID* is used only when the device is deployed through AudioCodes Live Platform. This ID is configured by AudioCodes using the [DeploymentId] ini file parameter.

**Applicable Applications:** SBC

**Applicable Products:** 9000; Mediant Software

### 2.6.1.3 Enhanced Password Obfuscation in INI and CLI Script Files

Passwords in the device's downloaded INI and CLI Script files can now be securely obfuscated using a strong encryption algorithm. The encryption is performed using the AES-256 algorithm with a 16-bit random CFB initialization vector (IV) cipher, ensuring robust protection of sensitive data.

The obfuscated passwords appear as follows:

- **INI File:** Prefixed with "$2$", for example:

  ```
  WSTunPassword = $2$8EGYm+FG+JJT/p8ZOytU64uplPMKcw==
  ```

- **CLI Script file:** Suffixed with "encrypted", for example:

  ```
  password B55osyLT1t7+oorwkaNB3bxEX4Bl8g== encrypted
  ```

The encryption key can be configured in one of the following ways:

- **Manually through CLI:**

  ```
  configure network > security-settings > encryption-key assign
  <string>
  ```

- **Device-Generated through CLI:**

  ```
  configure network > security-settings > encryption-key
  generate
  ```

- **Manually using Configuration Package File:** This is done by uploading a Configuration Package file with a newly created *encryption.key file that contains the key. (For detailed instructions, refer to the User's Manual.)*

The encryption key must be at least 32 characters long and can contain a combination of the following characters: A-Z, a-z, 0-9, !, #, $, %, &, (, ), *, +, ,, -, ., /, <, =, >, ?, @, [, ], ^, _, `, {, }, ~. A-Z, a-z, 0-9, !, #, $, %, &, (, ), *, +, ,, -, ., /, <, =, >, ?, @, [, ], ^, _, `, {, }, and ~.

The CLI displays only part of the encryption key for security (first four characters followed by three asterisks, for example, `%3[-***`). This is displayed using the following new CLI command:

```
configure network > security-settings > encryption-key display
```

This command can be used to check if an encryption key has been configured.

The full encryption key is included in a downloaded, encrypted Configuration Package file. The key is shown in a separate file called *encryption.key* inside the archive. This allows complete backup-and-restore, if needed.

The encryprion key can be deleted, using the following new CLI command:

```
configure network > security-settings > encryption-key clear
```

**Note:**

- If you plan to downgrade the device to an earlier version that doesn't support this feature, you must first clear the encryption key; otherwise, the downgrade will fail.
- The encryption key remains unaffected during a restore to factory defaults (`write factory`).

**Applicable Applications:** All

**Applicable Products:** All

### 2.6.1.4 Configurable Presence of 'a=extmap' SDP Line

The device now allows you to configure whether to keep (default) or remove the 'a=extmap' SDP line in outgoing SIP dialog-initiating INVITE requests. This functionality is configured through the following new IP Profile parameter:

- **Web Interface:** ‘Remove EXTMAP’
- **CLI:** `sbc-remove-extmap`
- **ini File:** [IpProfile_SBCRemoveEXTMAP]

**Applicable Applications:** SBC

**Applicable Products:** All

### 2.6.1.5 Customized DNS Fallback Policy

The device now provides full customization over the DNS fallback (failover) sequence. Previously, the DNS fallback order was hardcoded and couldn’t be changed.

This new feature allows you to configure DNS fallback policies for IPv4 and IPv6 traffic.  The DNS fallback policy can include a failover priority between the following DNS servers:

- The DNS server configured for the OAM IPv4 interface in the IP Interfaces table.
- The DNS server configured for the OAM IPv6 interface in the IP Interfaces table.
- The device's default IPv4 DNS server, configured by the existing [DefaultPrimaryDnsServerIp] parameter.
- The device's default IPv6 DNS server, configured by the existing [DefaultPrimaryDnsServerIpv6] parameter.

This functionality is configured in the new DNS Fallback Policy table (**Setup** menu > **IP Network** tab > **DNS** folder > **DNS Fallback Policy**). The table allows you to configure two DNS fallback policies -- one for IPv4 traffic and another for IPv6 traffic. Each policy supports a "chain" of up to four DNS priority rules, where each rule can be one of the above listed DNS servers.

**Note:**

- Currently, the DNS fallback feature is not per IP Interface, but only for IPv4 and IPv6 OAM interfaces.
- If the device is restored to factory defaults, the new DNS Fallback Policy table maintains its current configuration.
- If the table is not configured (all rules set to **None**), the device's default (hardcoded) DNS fallback sequence is applied (as in previous releases).

**Applicable Applications:** All

**Applicable Products:** All

#### 2.6.1.6 SFTP Operations Limited to File Downloads for Enhanced Security

To further strengthen device security, the following restrictions have been implemented on the device’s internal file system and SFTP:

- **File Access via SFTP:** Users can now only read or download files through SFTP. Previously, users had the ability to rename, delete, and upload files as well.
- **Removal of** ***/downloads*** **Folder:** The */downloads* folder has been removed, eliminating the ability for users to copy files to and from this folder via SFTP.
- **Discontinuation of SCP Support:** Secure Copy Protocol (SCP) is no longer supported. Previously, SCP was used for uploading files, including those related to the Auto-Update mechanism.

**Note:** When using the SFTP Cyberduck client and downloading a file from the /configuration or /debug folder, the client may display a "Transfer incomplete" message even though the download was successful.

**Applicable Applications:** All

**Applicable Products:** All

#### 2.6.1.7 Updated Location of CLI Command `reset-srtp-upon-re-key`

The CLI command `reset-srtp-upon-re-key` (ResetSrtpStateUponRekey) has been relocated within the CLI hierarchy. It’s now available under `configure voip > media security` instead of `configure voip > sip-definition settings`. This change aligns the command with other SRTP-related settings for better consistency.

**Applicable Applications:** SBC

**Applicable Products:** All

## 2.6.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-7: Resolved Constraints in Version 7.40A.501.841**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53782 | Device restarts with exception “CMX Kernel Panic” because of a bug in an internal thread. | Device restarts | Medium | Mediant 800C | n/a |
| SBC-54186 | The Customized Access Level table doesn’t function for Administrator users and for the Firewall table. | Web Page Customization failure | Low | All | n/a |
| SBC-54309 | The device sends an alarm about DNS failure for interfaces which are not configured with DNS. | Unwarranted DNS alarm | Medium | All | n/a |
| SBC-54434 | The device doesn't reflect saving configuration using the REST API. | Save over REST API doesn't function | Medium | All | n/a |
| SBC-54594 | HA system on Azure fails to renew TCP\TLS connections after switch-over because of the long time for the Azure load balancer to detect that the active server is no longer active. | Re-connection failure after a switch-over | High | HA | Azure |
| SBC-54599 | Cyberduck SFTP client fails to download the local debug recording file from local storage. | SFTP failure | Medium | All | n/a |
| SBC-54617 | Security vulnerability CVE-2024-52884 identified on the device. | Security | Medium | All | - |
| SBC-54945<br>SBC-55629 | The device's DTLS handshake fails after certificate is changed. | DTLS errors after loading a new certificate | Medium | All | n/a |
| SBC-54947 | The device sends echo to IP side for Tel-to-IP calls after receiving a hook flash over RFC 2833 from the IP side. | Calls with echo | Medium | Gateway | n/a |
| SBC-55178 | Message Manipulation with a condition that includes an ISUP body fails on an IP Group Set. | Message manipulation fails | Medium | All | n/a |
| SBC-55338 | When an incremental CLI script is uploaded through CLI or REST API, it adds a new IP Group with the same name as | Device adds an IP Group with same name | Low | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | an existing IP Group (instead of failing). | | | | |
| SBC-55346 | The device fails to apply the User UDP Port Assignment feature for SIP messages that aren't INVITE or REGISTER (for example, MESSAGE). | User UDP Port Assignment feature doesn't function | Low | All | n/a |
| SBC-55353 | The device fails to display the values of KPIs that check the total number of network packets/bytes when the value of the KPI is large (greater than 2147483647). | Incorrect KPI values | Medium | All | n/a |
| SBC-55431 | The device ends a call during a transfer for a specific call flow scenario. | Device ends a call | Medium | All | n/a |
| SBC-55449 | The device's local IP address responds to ICMP pings even if configured on a different VLAN. | Device responds to pings even though it shouldn't | Low | All | n/a |
| SBC-55461 | The device fails to renew its IP address over DHCP. | DHCP failure | Medium | All | n/a |
| SBC-55471 | The device disconnects the call after terminating a SIP UPDATE without SDP. | Call failure | Medium | All | n/a |
| SBC-55478 | The HA system fails to Telnet the redundant device from the active device. | Telnet failure | Medium | HA | n/a |
| SBC-55535 | The device fails to route a call to the Gateway-type IP Group if it's registered to the device over TCP\TLS behind NAT. | Call failure | Medium | All | n/a |
| SBC-55614 | The HA system on Azure sends syslog error messages ("SYSTEM ERROR: core 0, Id - 13, Counter - 1, errno - 11 [Code:0x2002d]". | Syslog messages | Low | HA | Azure |
| SBC-55619 | The device tries to allocate new media ports upon receipt of a 491 response for a re-INVITE, causing call failure (because Teams side doesn't start new STUN negotiation on the new port). | Call failure | Medium | All | n/a |
| SBC-55637 | The device is exposed to vulnerability CVE-2024-36971, which affects its kernel. | Security vulnerability | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-55668 | The device sends incorrect RTCP fields when operating in SRTP tunneling mode and when the IP Profile parameter 'RTCP Mode' is not transparent. | Incorrect RTCP parameters | Medium | All | n/a |
| SBC-55670 | The device restarts with error message “Signal 11, Task TIMB” when debug capturing is activated on the terminal or to TFTP. | Device restarts | Medium | All | n/a |
| SBC-55697 | The device is exposed to the Referrer-Policy vulnerability. | Security vulnerability | Medium | All | n/a |
| SBC-55700 | The device sends SNMP traps used for the keep-alive mechanism for OVOC over SNMPv3 instead of SNMPv2. | OVOC keep-alive failure | Medium | All | n/a |
| SBC-55737 | If the SIP header Alert-Info contains the string “dr” and doesn’t specify a tone index, the device erroneously attempts to play a Distinctive Ringing tone. | Incorect tone played | Low | Gateway | n/a |
| SBC-55756 | The device doesn't remove the ‘a=extmap’ attribute in the outgoing INVITE. | Call failure | Medium | All | n/a |
| SBC-55768 | The device sometimes transmits incorrect DTMF RFC 2833 RTP Event (RTP timestamp). | Device sends incorrect DTMFs | Medium | All | n/a |
| SBC-55806 | The device sends the same SDP body in an outgoing re-INVITE but mistakenly increases the SDP version. | Device sends incorrect SDP version | Medium | All | n/a |
| SBC-55875 | The device doesn't include the Authorization header for HTTP Post requests (REST CDR) upon the receipt of a 401 response. | Missing Authorization header | Medium | All | n/a |
| SBC-55895 | The device experiences SoftDSP restarts and sends error message “System encountered a fatal error, burning CoreDump to flash and restarting”. | SoftDSP restarts | Medium | All | n/a |
| SBC-55922 | The device fails to increase its SDP version even though it sends a new SDP offer in a specific call scenario. | Device sends incorrect SDP version | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-55934 | The device breaks its transparent session expires behavior and interferes in the session expires negotiation in a specific call scenario. | Incorrect session expires behavior | Medium | All | n/a |
| SBC-55942 | The device uses the same sequence number for outgoing DTMF RFC 2833 packets because, causing the far side to fail to detect them. | DTMF detection failure | Medium | All | n/a |
| SBC-55957 | The device fails to upload an ini file through Web interface if the file contains the old format of “WebPagesAccessLevel”. | Upload failure of ini file | Medium | All | n/a |
| SBC-56085 | The 'Enable Early Media' global parameter doesn't appear in the CLI. | Missing CLI command | Low | All | n/a |
| SBC-56101<br>SBC-56109 | The device restarts because of a DSP allocation failure. | Device restarts | Medium | All | n/a |
| SBC-56108 | The device fails to connect to OVOC over tunneling when OVOC’s IP address can’t be resolved in the first five seconds after the device recovers from a restart. | Device fails to connect to OVOC over tunneling | Medium | All | n/a |
| SBC-56168 | When functioning as a Media Component (MC) over VMware, the error message “Username: In: Failed to create symbolic link '/var/log/messages.0” is displayed in the CLI after recovering from a restart caused by a network failure. | MC repeated syslog error messages | Medium | MT\MTC | VMWare |
| SBC-56196 | The device's Web interface doesn't contain the TLS Default Bundle page. | Missing page in Web interface | Low | All | n/a |
| SBC-56202 | The device rejects calls with a 488 Not Acceptable Here because of incorrect handling of a SIP UPDATE. | Call failure | Medium | All | n/a |
| SBC-56272 | The Web interface's Registration Status page doesn't display data correctly when choosing to view 20 records per page. | Web interface display error | Low | MP-1288 | n/a |
| SBC-56316 | The device fails to display correct performance | Incorrect performance monitoring data | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | monitoring data for non-Administrator users. | | | | |
| SBC-56319 | The device disconnects the call in ringing state after receiving a TCP RST. | Call failure | Medium | All | n/a |
| SBC-56459 | The device displays network interfaces configured with network mask 31 as invalid (validation error). | Invalid network interfaces | Medium | All | n/a |

## 2.7 Version 7.40A.501.661

This version includes new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.7.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:** Starting from this version, the **Master** user level for device management is no longer supported. For more information, see this resolved constraint.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2 (8.2.3122 or later) and 8.4 (8.4.591 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

## 2.7.1 New Features

This section describes the new features introduced in this version.

### 2.7.1.1 SIPREC Session Trigger by SIP 200 OK Responses

The device can now be triggered to start a SIPREC session for a call upon the receipt of a SIP 200 OK in response to the initial INVITE request. This is achieved using AudioCodes proprietary X-AC-Action header set to the value ‘start-siprec’ (X-AC-Action: start-siprec) in the 200 OK response. Previously, triggering SIPREC by SIP messages was supported only by SIP INFO messages (with the X-AC-Action header).

Once triggered by a 200 OK response, the SIPREC session can be paused, resumed, and stopped, using the X-AC-Action header in INFO messages (as previously supported).

**Applicable Application:** SBC

**Applicable Products:** All

### 2.7.2 Resolved Constraints

This section lists resolved constraints.

Table 2-8: Resolved Constraints in Version 7.40A.501.661

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53363 | One-way voice occurs because the device deallocates a DSP resource before DTLS negotiation is completed. | One-way voice | Medium | All | n/a |
| SBC-53955 | A security vulnerability has been identified that enables regular users to elevate their privileges to that of a Master user, potentially granting unauthorized access to sensitive system functions and data. (As a result, Master user level is no longer supported from this version.) | Security | Medium | All | n/a |
| SBC-54178<br>SBC-54778<br>SBC-55128<br>SBC-55780 | The device sends an SDP answer that has missing attributes (for example, ‘a=rtcp-mux’, ‘a=sendrecv’, ‘a=ptime: x’) without changing the DSP version, causing call failure. | Call failure because of incorrect SDP | Medium | All | n/a |
| SBC-54548 | Device displays incorrect Performance Monitoring values in the SNMP ifTable. | Incorrect SNMP values | Medium | All | n/a |
| SBC-55367 | Device fails to authenticate STUN binding requests, causing calls without audio. | Calls without audio | Medium | All | n/a |
| SBC-55848<br>SBC-55862 | Device fails to connect to the LDAP server when the username contains special characters. | LDAP login failure | High | All | n/a |
| SBC-55870 | Device flags Proxy Sets and IP Groups as offline during a hitless upgrade because of initialization delays in network interfaces (especially when many interfaces are configured). | Device erroneously flags Proxy Sets and IP Groups as offline | Medium | All | n/a |
| SBC-55879 | Device sends an SDP offer with the same SDP version, even though the SDP was changed, causing the far side to reject the offer, resulting in call failure. | Call failure | Medium | All | n/a |

## 2.8 Version 7.40A.501.649

This version includes new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.7.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.3122 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

## 2.8.1 New Features

This section describes the new features introduced in this version.

### 2.8.1.1 Enhanced Security

#### 2.8.1.1.1 Enhanced Security for SSH using SHA2-based Signatures

The device's embedded SSH server used for accessing the CLI now supports SHA-256 (rsa-sha2-256) and SHA-512 (rsa-sha2-512) signature algorithms for public-key client authentication that utilizes RSA keys:

- Server host key algorithms (refer to RFC 4253, Section 7.1)
- Algorithm for client authentication (refer to RFC 8303, Section 3.1 and RFC 8332, Section 3.2).

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.2 Enhanced Username and Password Complexity

The following security enhancements for login username and password complexity policies have been introduced:

- Enforcement of username complexity. Previously, only password complexity was supported. This functionality is enabled by the following new parameter:
  - Web: 'Enforce Username Complexity'
  - CLI: `configure system > users-settings > enforce-username-complexity`
  - INI: [EnforceUsernameComplexity]
- Enforcement of username or password complexity policies by regular expressions (regex), for example, "^(?!.*\\.\\.)[\\w.-]{1,40}$". This functionality is configured by the following new parameters:
  - [PasswordComplexityCheckByRegex] – configures password complexity by a regex (default is empty).

  - [UsernameComplexityCheckByRegex] – configures username complexity by a regex (default is empty).

- The default complexity rule for usernames now allows the at "@" sign. (Complexity based on regex can contain any symbol or sign.)
- The username or password can now contain up to 100 characters (previously, was 40).

**Note:** If any of the complexity parameters (EnforcePasswordComplexity, EnforceUsernameComplexity, PasswordComplexityCheckByRegex, UsernameComplexityCheckByRegex, or MinWebPasswordLen) are modified, changes only take effect after the Web page is refreshed.

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.3 User's Web Sessions Displayed and Optionally Terminated

The device's Web interface now displays the number of currently established Web sessions of the same logged-in user and with the same access level (e.g., Security Administrator). These Web sessions may be logged in from different computers or web browsers.

In addition, this feature allows you to forcibly terminate these other active Web sessions. Therefore, this feature enables you to end unwanted or suspicious sessions, protecting your account from possible attacks.

The number of other active sessions and the option to end them are displayed in the logged-in username drop-down box, located on the top-right of the Web interface.

The existing Login Information window, which if enabled pops up each time upon user login, now also displays the number of other active Web sessions of the user.

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.4 Enhanced RADIUS Security with Message-Authenticator Attribute

The device now offers robust security for RADIUS-based user authentication, using RADIUS attribute 80 (Message-Authenticator). This attribute ensures the integrity of RADIUS packets, safeguarding against unauthorized access, for example, "man-in-the-middle" attacks.

This feature provides security for both incoming and outgoing RADIUS packets:

- **Outgoing RADIUS messages:** You can enable the device (Network Access Server / NAS) to include the Message-Authenticator attribute in all Access-Request RADIUS packets sent to the RADIUS server. This is applicable only to the Password Authentication Protocol (PAP) authentication method.

  This functionality is enabled by the following new parameter:

  - Ini file: [RadiusPapRequireMsgAuthTx]
  - CLI: `rad-pap-req-msg-auth-tx`

  **Note:** For RADIUS-based SIP message authentication, this parameter is not needed as SIP authentication uses the Digest protocol, which inherently includes the Message-Authenticator attribute.

- **Incoming RADIUS messages:** You can enable the device to require the presence of the Message-Authenticator attribute in all incoming Accept-Accept RADIUS messages from the RADIUS server. If the attribute is not present, the device rejects the message and denies user login. This is applicable to Digest and PAP authentication methods.

  This functionality is enabled by the following new parameter:

  - Ini file: [RadiusRequireMsgAuthRx]
  - CLI: `rad-req-msg-auth-rx`

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.5 Original Crypto Key Used throughout SIP Dialog for SRTP

You can now configure the device to preserve (use) the original crypto key, sent in the dialog-initiating INVITE message, for all the SIP dialog's transactions (including a re-INVITE). The key is specified in the 'a=crypto' line of the SDP body.

This feature is supported by the new optional value **Keep Original** for the existing IP Profiles table parameter 'Generate SRTP Keys Mode' (GenerateSRTPKeys).

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.6 SRTP Reset upon Key Change for Relevant Call Party Only

If a call party changes the SRTP key ('a=crypto' line in SDP body) during a call, the device can now reset the SRTP stream (roll-over counter / ROC index and other SRTP fields) of only this specific call party. The SRTP stream of the other call party is not reset. The SRTP key is typically updated by the call party using a SIP re-INVITE message (for example, due to a session refresh).

This feature is enabled by the following new global parameter:

- Ini file: [SrtpResetTxRxSeparately]
- CLI: `configure voip > media security > srtp-reset-tx-rx-separately`

**Note:**

- For this functionality, the existing parameter 'Reset SRTP Upon Re-key' (ResetSRTPStateUponRekey) must also be enabled.
- If this new feature is disabled and the existing parameter 'Reset SRTP Upon Re-key' is enabled, the device resets the SRTP stream of both call parties.

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.1.7 Enforcement of Web Interface Access via Hostname

You can now enforce access to the device's Web interface only through the device's hostname (FQDN). When enabled, all attempts to access the Web interface through the device's IP address is blocked.

You can enable (default) this feature using the following new parameter:

- Web: 'Enforce Web Host Name' (Setup > Administration > Web & CLI > Web Settings)
- CLI: `configure system > web > enforce-web-host-name`

- Ini file: [EnforceWebHostname]

The device's hostname is configured using the existing 'Web Server Name' (WebHostName) parameter.

**Note:**

- Access to the Web interface is allowed through an FQDN or IP address in any of the following configuration scenarios:
  - The 'Enforce Web Host Name' parameter is disabled.
  - The 'Web Server Name' parameter is not configured (regardless of the 'Enforce Web Host Name' parameter).
- If you're using single sign-on (SSO) with OVOC, you must disable this feature; otherwise, SSO fails.
- If you're upgrading from version 7.4.500-2 (7.40A.500.775) or later to this version and have configured the 'Web Server Name' parameter and use the device's IP address to access the Web interface, access will be blocked. If you want to retain such capability, disable the 'Enforce Web Host Name' parameter.

**Applicable Application:** All

**Applicable Products:** All

## 2.8.1.2 SIP and Call Handling

### 2.8.1.2.1 Maximum Concurrent Calls per User using Tags

You can now configure a different maximum concurrent call value (incoming or outgoing) for each user, using the device's tag functionality in Call Setup Rules and Dial Plans.

Previously (and still supported), the same maximum concurrent call value, configured in the Call Admission Control Profiles table, applied to every user associated with the SIP Interface or IP Group to which the profile was assigned.

This feature introduces a new hardcoded tag called 'cac'. The tag has the format *key*|*value*, where *key* identifies the call party (SIP URL user-part or IP address) and *value* defines maximum concurrent calls. For example, '*cac=+12345678*|*3'* (or '*cac=10.4.4.4*|*3*') limits the user (or IP address) with phone number +12345678 (or IP address *10.4.4.4)* to a maximum of three concurrent calls.

This feature is configured by a Dial Plan and Call Setup Rule (which are assigned to the relevant SIP Interface, IP Group, or IP-to-IP Routing rule):

- The Dial Plan is configured with multiple rules, where each rule defines a user's prefix number, and maximum concurrent calls using any user-defined tag (for example, "*cacMax=3*").
- The Call Setup Rule is configured to check the existence and value of your Dial Plan tag, for example:
  - Condition: SrcTags.cacMax exists And SrcTags.cac !exists
  - Action Subject: SrcTags.cac
  - Action Type: Modify
  - Action Value: Header.From.URL.User + '|' + SrcTags.cacMax

If you want all users to have the same maximum concurrent calls, only a Call Setup Rule needs to be configured. For example, the below applies a maximum concurrent incoming calls of three to each user (or IP address):

- Action Subject: SrcTags.cac
- Action Type: Modify
- Action Value: (one of following)
    - For each IP address: Param.Message.Address.Src.IP + '|3'
    - For each user: Header.From.Url.User + '|3'

This feature also introduces a new CLI command `show voip tags-cac` whose output displays a list of cac keys (users) with their current concurrent calls out of their maximum allowed concurrent calls. The command can also output information for a specific user (`show voip tags-cac key <phone number or IP address>`).

If the maximum number of concurrent calls is reached, the device rejects any new call and sends the following syslog message:

- For incoming calls: "RELEASE_BECAUSE_IN_PER_KEY_CAC_LIMIT_REACHED"
- for outgoing calls: "RELEASE_BECAUSE_OUT_PER_KEY_CAC_LIMIT_REACHED"

**Applicable Application:** SBC

**Applicable Products:** All

### 2.8.1.2.2 SDP Handling of Subsequent SIP Responses to Initial INVITE

You can now configure the device to handle (process) the SDP body of only the first SIP response to the SIP dialog-initiating INVITE request, ignoring the SDPs of all subsequent SIP responses.

This feature is configured by the following new parameter in the IP Profiles table:

- Web: ‘SDP Subsequent Responses Mode’
- CLI: `sdp-origin-same-session-ver`
- Ini: [SDPSubsequentResponses]

By default, the device handles SDPs of all the subsequent SIP responses.

**Applicable Application:** SBC

**Applicable Products:** All

### 2.8.1.2.3 New SDR Field Indicating Call Termination Side

The device provides a new optional SDR field called ‘Termination Side’. This field indicates the call party (entity) that terminated the call ("ingress", "egress", or "internal").

The field is applicable to both ATTEMPT and STOP SDR record types. You can include the field in SDRs by configuring the existing SBC SDR Format table.

In addition to the above, the existing ‘Release Time’ optional field is now also applicable to ATTEMPT SDR record types. Previously, it was applicable only to STOP record types.

**Applicable Application:** SBC

**Applicable Products:** Mediant 90xx; Mediant Software

### 2.8.1.2.4 Proxy Set Homing with Dedicated TCP Connection Mode

You can now use Proxy Set homing in conjunction with the Dedicated Connection mode. Previously, when the Dedicated Connection mode was used, Proxy Set homing wasn't functional.

In Proxy Set homing, the device always tries to connect with the proxy server that has the highest priority. In Dedicated Connection mode, the device uses a dedicated TCP / TLS connection (source port) with the proxy server per user defined in the SBC User Information table, or per trunk endpoint (MP-1288 only).

**Applicable Application:** All

**Applicable Products:** All

### 2.8.1.2.5 Alternative Routing upon Loss of SIP Signaling Path

You can now configure the device to re-route calls when it detects a disconnection in the associated SIP signaling path (SIP socket).

Even when the SIP connection is lost, the call (RTP media) is maintained. However, for some services such as emergency calls (E-9-1-1), it's critical that a SIP connection exists so that other call functionalities (for example, call transfer to another PSAP operator) can be done.

This feature enables the device to re-route the call to an alternative destination (for example, different PSAP or police) upon the detection of a loss in the SIP signaling path. A new SIP signaling path for the alternative destination is established, ensuring full call functionality.

The feature is configured by the following new IP Profile parameter:

- Web: 'Broken Signaling Connection Mode'
- Ini file: [DisconnectOnBrokenSignalingConnection]
- CLI: `disconnect-on-broken-signaling-connection`

**Note:** This feature is applicable only to calls whose SIP signaling is over TCP.

**Applicable Application:** SBC

**Applicable Products:** All

### 2.8.1.3 Networking

#### 2.8.1.3.1 Default IPv6-based DNS Servers

You can now configure default IPv6 DNS servers (primary and secondary). Previously, only default IPv4 DNS server configuration was supported (DefaultPrimaryDnsServerIp and DefaultSecondaryDnsServerIp parameters).

The default DNS servers ensure that applications such as the Automatic Update feature, which may require DNS lookups, run seamlessly even when DNS servers haven't been configured (in the device's Internal DNS table and IP Interfaces table). In other words, the device uses the default DNS servers as the last resort.

The default IPv6 DNS servers are configured by the following new parameters:

- Primary default DNS server:
  - Web: 'Default Primary DNS Server IPv6'
  - Ini fie: [DefaultPrimaryDnsServerIpv6]
  - CLI: `configure network > dns settings > dns-default-primary-server-ipv6`
- Secondary default DNS server:
  - Web: 'Default Secondary DNS Server IPv6'
  - Ini file: [DefaultSecondaryDnsServerIpv6]
  - CLI: `configure network > dns settings > dns-default-secondary-server-ipv6`

The following lists the default IP addresses of the default IPv6 DNS servers:

- Primary DNS server: 2001:4860:4860::8888
- Secondary DNS server: 2001:4860:4860::8844

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.3.2 Configurable Second Port for RPCAP Server

You can now configure the second port of the device's embedded RPCAP server. Previously, the device dynamically allocated the number for this port.

The first port (configurable and by default, 2002) is an always-open listening port that's used for initial connections. The second port (now configurable and by default, dynamically allocated) is sent to the client during the initial connection to open a new TCP connection for the captured packets.

You can configure the second port using the following existing CLI command:

```
# debug capture rpcap-server start <First Port> <Second Port>
```

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.3.3 Configurable ARP Reply Timeout

You can now configure a maximum time (timeout) that the device waits for an Address Resolution Protocol (ARP) reply. By default, the device waits up to three seconds for an ARP response. If no reply is received within this time, the device terminates the call.

You can configure this timeout by the following new global parameter:

- CLI: `configure voip > media settings > arp-manager-timeout`
- Ini file: [ArpManagerTimeout]

**Note:** The device first checks its internal ARP table for a matching MAC address associated with the destination IP. It only sends an ARP request if no match is found.

**Applicable Application:** All

**Applicable Products:** All

### 2.8.1.4 Parameter Updates

#### 2.8.1.4.1 CLI Commands Changed for Auto-Update of INI File

New CLI commands for specifying the ini file (incremental or regular) for the Auto-Update mechanism have been introduced, replacing the previous commands for this functionality:

- [IncrementalIniFileURL] ini file:

  `voice-configuration-incr` replaced by `incremental-ini-file`
- [IniFileURL] ini file:

  `voice-configuration` replaced by `ini-file`

The names of these new commands more accurately reflect the type of ini file and are aligned with other commands (e.g., `copy`) that are used to specify the ini file type.

**Applicable Application:** All

**Applicable Products:** All

#### 2.8.1.4.2 CLI Location Changed for `enforce-media-order`

The CLI command `enforce-media-order` (EnforceMediaOrder ini file parameter) for the Gateway application has been moved under `configure voip > gateway advanced`.

**Applicable Application:** Gateway

**Applicable Products:** Gateway

#### 2.8.1.4.3 Value Range Updated for Auto-Update File Transfer Timeout

The valid configuration value for the [AUPDMaxTransferTime] parameter, which defines the file transfer timeout (minutes) for the Auto-Update mechanism has been updated. The range is now 1 to 5 (instead of 1 to 1,000) and the default is now 5 (instead of 10).

**Applicable Application:** All

**Applicable Products:** All

### 2.8.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-9: Resolved Constraints in Version 7.40A.501.649**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51048<br>SBC-55364 | Device doesn't send RTP packets because of a DSP issue, resulting in one-way voice. | One-way voice | Medium | All | n/a |
| SBC-52401 | Device stops playing playback upon a coder change because of a DSP issue, resulting in no voice. | Call transcoding failure causing no voice | Medium | All | n/a |
| SBC-53289 | Media Component (MC) fails to connect to the device after a software upgrade to Version 7.4.500 when no client defaults are defined. | MC connection failure | Medium | Mediant CE | n/a |
| SBC-53321<br>SBC-54361 | Device restarts because of a DSP issue, generating the error message "System encountered a fatal error, burning CoreDump to flash and restarting, this can take several minutes". | Device restart | Medium | All | n/a |
| SBC-53714<br>SBC-53729<br>SBC-54800 | The device fails to decrypt the SRTP stream after the far end SRTP key changes (device didn't change crypto). | One-way voice | Medium | All | n/a |
| SBC-53717 | Security vulnerability concerning RADIUS was identified because the device doesn't enforce the presence of the Message-Authenticator attribute (CVE-2024-3596). | Vulnerability | Medium | All | n/a |
| SBC-53910 | Hitless software upgrade fails when the Firewall table includes rules that block HA Maintenance packets. | Hitless upgrade failure (HA system becomes standalone) | Medium | HA | n/a |
| SBC-54035 | Device restarts upon an IP-to-Tel call connection because of an interworking issue between the device and ARM. | Device restart | Medium | Gateway | n/a |
| SBC-54097 | The device has a two to five seconds delay on getting a dial tone when pulse dial detection is enabled (EnablePulseDialDetection)s. | Dial tone delay | Medium | MP-1288 | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-54139 | The device sends Call Setup Rules with Signing Certificate Request (CSR) Version 3, causing the far side to reject it (as expecting Version 1). | Call Setup Rules failure | Medium | All | n/a |
| SBC-54140 | The device restarts, (exception "Signal 11, Task SPMR") because of an internal issue that allows access to a resource pool with an invalid id. | Device restart | Medium | All | n/a |
| SBC-54165 | If the device is configured with a primary syslog server that uses TLS and with additional syslog servers (Syslog Servers table) that use UDP or TCP, after about 1,024 syslog messages, syslog freezes. | Device sends syslog messages with big delay | Low | All | n/a |
| SBC-54220 | The device times out an ARP request after only three seconds, causing delayed (more than three seconds) ARP answers to be ignored and resulting in call failure (media destination unreachable). | Device disconnects call | Medium | All | n/a |
| SBC-54237 | The device loses its AudioCodes production certificate chain and reverts to the single self-signed certificate when upgrading from version 7.2 to 7.4. | Certificate error | Medium | All | n/a |
| SBC-54288 | If an OAuth server in the OAuth Servers table is configured with ‘Verify Certificate’ enabled but without an assigned TLS Context, the device doesn’t use the default TLS Context (#0). | TLS error | Medium | All | n/a |
| SBC-54297 | Basic authentication for Web Services doesn’t function as expected (device sends multiple requests after 401 without waiting for a response). | Incorrect device behavior after receiving a 401 response | Medium | All | n/a |
| SBC-54320 | The device flags Proxy Sets and IP Groups as offline during a hitless upgrade due to initialization delays in network interfaces (especially | Device erroneously flags Proxy Sets and IP Groups as offline | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | when many interfaces are configured). | | | | |
| SBC-54350 | The device disconnects a call (SIP BYE with Reason: SIP ;cause=400 ;text="local") during media synchronization (EnableSBCMediaSync disabled and no transcoding license or DSP). | Device disconnects calls | Medium | All | n/a |
| SBC-54351 | The device sends an RTP stream with SSRC 0x0 after a Teams call transfer that requires DSPs, causing call failure. | Call failure | Medium | All | n/a |
| SBC-54353 | When the device performs message manipulation on a received SIP INVITE with multipart bodies, it miscalculates the SDP's Content-Length field in the outgoing leg. | Device sends INVITE with incorrect SDP | Medium | All | n/a |
| SBC-54435 | The device doesn't forward the voice stream (RTP packets) in scenarios where it first starts playing the ringback tone without DSP, and then reopens the channel with DSP on SIP 183 (due to SBCFaxReroutingMode) while the tone is still being played. | Call failure due to no voice | Medium | All | n/a |
| SBC-54452<br>SBC-54928<br>SBC-55181 | The device's OAMP network interface becomes unreachable after the IP address is changed of another interface in the IP Interfaces table, because of an issue in the Firewall table. | Device becomes unreachable | High | All | n/a |
| SBC-54469 | The device fails to handle a 401 challenge response for a SIP REGISTER (refresh) for a user because of a mismatch with the CSeq number, resulting in misalignment with the SIP request-response dialog transaction of the specific user. | Device fails to handle user registration refresh | Medium | All | n/a |
| SBC-54587 | When in HA mode, the device fails to resolve the FQDN in the Firewall table after a switchover, causing the Proxy Set \ IP Groups to go offline. | Proxy Set \ IP Groups go offline after a switchover | Medium | HA | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-54604 | The device fails to run two consecutive SSH sessions if the gap between them is too small. | Second SSH session fails | Low | All | n/a |
| SBC-54636 | The CLI command `fxs-line-testing` outputs "failed" results for all CIDs. | CLI command doesn't function | Low | MP-1288 | n/a |
| SBC-54637 | The device fails to negotiate the same bandwidth for the telephone event as the negotiated codec. | Device sends incorrect SDP answer | Medium | All | n/a |
| SBC-54638<br>SBC-54837<br>SBC-55180 | LDAP connection over TLS (1.2) creates an overload on the LDAP task and the device goes into overload state. | Device delays responses | High | All | n/a |
| SBC-54689 | The device offers both IPv4 and IPv6 for audio\video using the ANAT feature, instead of offering only one media and one video. | Device rejects SDP answer | Medium | All | n/a |
| SBC-54711 | The device restarts when the CLI command `show voip calls active` is run. | Device restart | Medium | All | n/a |
| SBC-54753 | The device restarts because of a SoftDSP restart ("fatal error"). | Device restart | Medium | All | n/a |
| SBC-54806 | Device doesn't display all the entries in the Account table on the Web interface's Monitor page (Registration Status). | Monitor page missing entries | Low | All | n/a |
| SBC-54840 | The device restarts upon a scan test. | Device restart | Medium | All | n/a |
| SBC-54869 | The device's MIB files fail to compile. | MIB files fail to compile | Low | All | n/a |
| SBC-54915<br>SBC-54923 | The duration of RFC 2833 DTMF packets doesn't increase according to the OPUS sample rate, resulting in a DTMF transcoding failure. | DTMF transcoding failure | Medium | All | n/a |
| SBC-54920 | The device erroneously increases its SDP version. | Device sends incorrect SDP version | Medium | All | n/a |
| SBC-54954 | The device fails to exclude VND fax coders from the outgoing SDP offer, even though they weren't defined in the Allowed Coders List. | Device includes incorrect coders | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-54962<br>SBC-54963<br>SBC-55490 | The HA device fails to maintain SNMP v3 users after a switchover, causing an invalid SNMP v3 Users table. | SNMP v3 Users table becomes invalid after second switchover | Medium | HA | n/a |
| SBC-54992 | The device fails to decrypt SRTP packets if RTP validation fails due to an SSRC (SRTP) error, causing a WebRTC call video freeze. | WebRTC call video freeze | Medium | All | n/a |
| SBC-55025 | MgmtLDAPLogin functions even if the incorrect Admin username is used (with correct password) | Vulnerability | High | All | n/a |
| SBC-55032 | The device restarts because of a bug in the DNS mechanism when trying to access an FQDN from the Firewall table. | Device restart | Medium | All | n/a |
| SBC-55053 | The HA device's "DeploymentSecret" parameter changes after a switchover. | Parameter changes after a switchover | Medium | HA | n/a |
| SBC-55069 | The device terminates a SIP re-INVITE request and disconnects the call with a 500 response. | Device disconnects call | Medium | All | n/a |
| SBC-55110 | The device restarts ("CMX Kernel Panic") because of an internal bug caused by two overlapped memory segments. | Device restart | Medium | Mediant 800C | n/a |
| SBC-55124 | Device failed to get upgraded by the Stack Manager because of a certificate replacement bug. | Device restart | Medium | Mediant CE | n/a |
| SBC-55129 | The device fails to connect to OVOC over tunneling when OVOC's IP address can't be resolved in the first 5 seconds after a device restart. | Device fails to connect to OVOC over tunneling | Medium | All | n/a |
| SBC-55141 | The device sends the incorrect media line (instead of "RTP/SAVP") in the SIP 200 OK SDP answer, causing call failure. | Device sends incorrect SDP, causing call failure | Medium | All | n/a |
| SBC-55146 | The device's Web interface displays "LDAP Connection Broken" status even though LDAP server is ok. | Device displays incorrect LDAP status | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-55159 | The device's IP Profile parameter setting 'Header For Transfer' to **Remote-Party-ID** doesn't function as expected, (device doesn't send re-INVITE with Remote-Party-Id header after transfer). | 'Header For Transfer' to **Remote-Party-ID** doesn't function | Medium | All | n/a |
| SBC-55179 | The device's IP Profile parameter 'Generate SRTP Keys Mode' doesn't provide an option to keep the original key. | Device doesn't support enforcement of original crypto key | Medium | All | n/a |
| SBC-55183 | The device rejects a DTLS call with a SIP 488 response because of a bug in DTLS fingerprints and setup. | Call failure | Medium | All | n/a |
| SBC-55241 | The device has incorrect varbinds in SNMP traps. | Device has incorrect varbinds in SNMP traps | Medium | All | n/a |
| SBC-55277 | Call has clicking noises originating from the device when using No-Op mechanism for RTP. | Voice quality | Medium | All | n/a |
| SBC-55357 | The device selects the port from the last received SDP answer, even though the SDP version didn't change. | Device selects incorrect RTP port | Medium | All | n/a |
| SBC-55370 | The device restarts because of a failure in how it handles a SIP INVITE with Replaces. | Device restarts | Medium | All | n/a |
| SBC-55413 | The device rejects a call with "Board command failed - Internal error" because of a call that involves two CIDs connected as an SBC session. | Call failure | Medium | All | n/a |
| SBC-55450 | The device sends the syslog message "!!! Repeated 10 times" when running a message manipulation set that contains many rules. | Device sends syslog messages | Low | All | n/a |
| SBC-55463 | The device restarts ("Signal 901 Task MCIE" because it was accessed through curl. | Device restart | Medium | All | n/a |
| SBC-55467 | IP Group Set tags used for classification (which is not allowed) create issues with IP Group(s) that have the same tag (IP Group Set should have precedence over IP Group) | IP Group Set Tags don't function properly | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-55474 | The call-status packet sent from the device to ARM after receiving a 404 should have ‘0’ for "routeSeq" for the first route in both call-status packets. | Device sends incorrect value to ARM | Medium | All | n/a |
| SBC-55538 | The device restarts when it doesn’t find a route by destination tag to a self-initiated SIP REGISTER. | Device restarts | Medium | All | n/a |

## 2.9 Version 7.40A.501.392

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.

- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.5.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.3122 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.9.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-10: Resolved Constraints in Version 7.40A.501.392**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53042 | The CLI command output of `fxs-line-testing` displays "failed" results for all CIDs. | CLI command doesn't function | Low | All | n/a |
| SBC-54019<br>SBC-54108 | Some HA settings (HA Remote Address, HA Device Name, HA Remote Device Name) change after an HA switchover, causing HA failure. | Loss in HA | High | Mediant CE | AWS |
| SBC-54037 | Fax calls fail when the device receives a SIP re-INVITE with delayed offer (no SDP) because the device replies with 'a=inactive'. | Fax failure | Medium | All | n/a |
| SBC-54116 | When the device is configured to translate a SIP UPDATE message to re-INVITE, it fails to handle the re-INVITE, rejecting it with a SIP 491 response and generating the error message "!! [ERROR] SBCOfferAnswerMngr(#563)::HandleSDPUpdateFromCore - Can't handle new UPDATE. Re-INVITE is in progress". | Call failure | Medium | All | n/a |

## 2.10 Version 7.40A.501.384

This version includes new features, known constraints and resolved constraints.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.5.1 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.3122 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.10.1 New Features

This section describes the new features introduced in this version.

#### 2.10.1.1 Enhanced Control of Debug Recording

The device's debug recording feature has been enhanced to provide the user with more control of the process:

- Starting and stopping debug recording is now done explicitly by the user. Previously, as soon as a rule was added to the Logging Filters table, the device automatically started debug recording (if the 'Mode' parameter was set to **Enable**). Debug recording continued until the user deleted the rule or changed the rule's 'Mode' to **Disable**.
- The debug recording process now has a maximum duration (configurable), after which it automatically stops.

This feature is supported by the following new parameters on the Debug Recording page (Troubleshoot menu > Troubleshoot tab > Logging folder > Debug Recording):

- 'Status' field: Displays if debug recording is currently running (started) or not (stopped).
- Start and Stop buttons: Starts and stops debug recording.
- 'Maximum Duration' field: Configures the maximum duration (in minutes) of the debug recording process (by default, 60 minutes).
- 'End Time' field: Displays the date and time when debug recording will stop.

This is also supported in the CLI by the following new commands under `configure troubleshoot > logging settings`:

- `dbg-rec-timeout`: Configures the maximum debug recording duration.
- `dbg-rec-status {start|stop|timer-restart}`: Displays the current debug recording status, starts or stops debug recording, and resets the maximum duration.

**Note:**

- This feature affects only rules in the Logging Filters table whose 'Mode' is **Enable**.
- The maximum debug recording timer is reset to the configured duration upon the following:
  - Configuration (new or modified rule) of Logging Filters table

- Device restart
- HA switchover

**Applicable Application:** All

**Applicable Products:** All

### 2.10.1.2 Restriction of Management Client Access per Management Interface

The Management Access List table (formerly called the *Access List* table) has been enhanced to provide users with precise control over who can access which management interface. This feature allows users to permit (allow) access of a client (IP address) to a specific (or all) management interface type (Web interface, REST API, SSH, or Telnet).

To support this feature, the table's design has been aligned with the other configuration tables, and includes a new parameter called 'Type'. This parameter defines the management interface (All, Web, REST, SSH, or Telnet) that the specified client (IP address) can access.

**Applicable Application:** All

**Applicable Products:** All

### 2.10.1.3 Insert Row Capability for Firewall Table

The Firewall table now allows the user to insert new rules at any position. Since firewall rules are processed from top to bottom, this flexibility lets users prioritize specific rules as needed.

This feature is supported by the new **Insert** button and `insert` command in the Web interface and CLI, respectively.

**Applicable Application:** All

**Applicable Products:** All

### 2.10.1.4 Syslog Capturing of HTTP Client Requests and Responses

The device now provides a method to track HTTP interactions, by capturing requests and responses sent by HTTP clients in syslog messages (like curl's verbose output).

By default, the device logs received requests and responses from all HTTP clients. However, the user can configure the device to log requests and responses from specific HTTP clients only.

This feature is configured by the following new parameters (ini and CLI only):

- [EnableHttpClientDbgMsg] / `configure troubleshoot > logging settings > enable-http-client-dbg-msg`: Enables this logging feature (by default, disabled).
- [HTTPLogFilter] / `configure troubleshoot > logging settings > http-log-filter`: Defines a string of characters that must be present in the HTTP client's URL in order to trigger the device to log the client's requests and responses.

**Applicable Application:** All

**Applicable Products:** All

#### 2.10.1.5 Elastic and Virtual IP Addresses for AWS Deployments Configurable through Web

Elastic and Virtual IP addresses in multi-zone HA deployments on AWS can now be configured through the Web interface. Previously, they could only be configured through ini file (AwsElasticIPs and AwsVirtualIPs) and CLI (aws-elastic-ips and aws-virtual-ips).

To support this feature, the following new tables have been added to the Web interface:

- AWS Elastic IPs table (Setup menu > IP Network tab > Advanced folder > AWS Elastic IPs)
- AWS Virtual IPs table (Setup menu > IP Network tab > Advanced folder > AWS Virtual IPs)

**Note:**

- Configuration of Elastic and Virtual IP addresses is typically (and recommended) configured through AudioCodes **Stack Manager**. Therefore, these tables should be used for viewing only.
- These tables are only visible when the following conditions are fulfilled:
  - The deployment is in an AWS environment.
  - The [HAPreserveIPAddresses] parameter is configured to a non-zero value (i.e., multizone deployment).

**Applicable Application:** SBC

**Applicable Products:** Mediant CE (AWS)

#### 2.10.1.6 Miscellaneous Updates

The location of the `prefix-to-ext-line` command in the CLI has changed to `configure voip > gateway analog fxs-setting`.

**Applicable Application:** Gateway

**Applicable Products:** Gateway

### 2.10.2 Known Constraints

This section lists known constraints.

**Table 2-11: Known Constraints in Version 7.40A.501.384**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53129 | During a hitless upgrade, warnings in syslog and alarms may be raised about an NGINX issue, even though NGINX is functioning normally. The alarm is cleared within a few seconds. | None | Low | Mediant 800 | HA |

### 2.10.3 Resolved Constraints

This section lists resolved constraints.

**Table 2-12: Resolved Constraints in Version 7.40A.501.384**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51461 | The device stops sending Floating license reports because of no socket timeout. | Device stops sending reports to Floating License server | Medium | All | n/a |
| SBC-51820 | The device generates a parsing for the colon symbol error in syslog for no known reason. | Device sends unknown error message in syslog | Low | All | n/a |
| SBC-51830 | The device's FXS endpoints stops ringing after one ring when both an incoming call and voicemail are activated. | Device fails to receive an incoming call | Medium | MP-1288 | n/a |
| SBC-51855 | The device fails to disconnect an established call after an HA switchover because of a timing issue with the newly active unit binding the IP address. | Device fails to release a call after a switch over. | Medium | HA | HA |
| SBC-51935 | The device isn't accessible over Telnet and SSH for some IP network interfaces because of SSH\Telnet binding issues with IP interfaces. | Device isn't accessible over Telnet\SSH | Medium | HA | HA |
| SBC-52107 | The device ends a TLS connection when OCSP is enabled with the default response Allow. | Device ends calls | Medium | All | n/a |
| SBC-52394 | Suppression of the AcProxyConnectionLost alarm (configured in the Alarms Customization table) doesn’t function properly because it has two severity types (Minor for loss of single IP address in Proxy Set, and Major for loss of all addresses in Proxy Set). | Alarm suppression failure | Low | All | n/a |
| SBC-52412 | The device loses configuration of the third and fourth IP interfaces after uploading a CLI script file containing the same configuration. | Device fails to save configuration | Low | Mediant 500 (with four Ethernet ports) | n/a |
| SBC-52415 | The device rejects a WebRTC call ("HandleOfferSDPFromCore - All mediums are rejected") when the incoming leg is WebRTC and the outgoing leg | Device rejects a call | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | has 'SBC Media Security Behavior' configured to **As Is** and 'SBC Media Security Method' to **SDES**. | | | | |
| SBC-52437 | The device's CLI command `show voip register db sbc list` displays only up to the first 500 users in its registration database. | CLI command output limit | Low | All | n/a |
| SBC-52466 | The device's Gateway application can't make a call (to or from the trunk) because of a resource leak ("ConnID") caused by an alternative routing issue with ARM. | Device can't make calls | High | Gateway | n/a |
| SBC-52531 | The device's clock isn't synchronized with the NTP server because of sampling in seconds instead of milliseconds. | Device's NTP time is inaccurate | Medium | All | n/a |
| SBC-52687<br>SBC-52790<br>SBC-52885 | TLS mutual authentication ('Require Client Certificates for HTTPS connection' configured to **Enable**) doesn't function properly because of an NGINX validation issue. | Device inaccessible over Web HTTPS | Medium | All | n/a |
| SBC-52705 | The device sends different responses for UPDATE and re-INVITE SIP messages on race conditions (500 or 488 for UPDATE, instead of 491 for both). | Device sends incorrect SIP response | Low | All | n/a |
| SBC-52707 | The device truncates the SIP From header's display name to 60 bytes (and in a bad UTF-8 format). | Device sends incorrect HTTP request to ARM | Low | All | n/a |
| SBC-52720 | The device's Gateway application doesn't send a new SIP SUBSCRIBE request for a registration event after a proxy rediscovery. | Device doesn't send new SIP SUBSCRIBE | Low | Gateway | n/a |
| SBC-52727<br>SBC-52729 | The device's debug recording to local storage is inaccessible because of an extra backslash ("\") added to each file and directory. | Debug recording to local storage is inaccessible over SFTP | Medium | All | n/a |
| SBC-52738 | The device restarts (error message "Signal 904, Task WEBS") when uploading a Linux-formatted User | Device restarts | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | Information file over REST API. | | | | |
| SBC-52799 | When in HA mode, the automatic update parameters for the Dial Plan (DialPlanCSVFileUrl and DialPlanFileUrl) aren't saved on the redundant device, causing an automatic update failure for the Dial Plan after an HA switchover. | Automatic update for Dial Plan fails after switchover | Medium | HA | HA |
| SBC-52805 | The device sometimes fails to forward the SIP Content-Disposition header's custom values. | Device sometimes fails to forward the SIP Content-Disposition header | Low | All | n/a |
| SBC-52824 | The device forwards RTP packets with unsupported payload types even though the parameter 'RTPFWInvalidPacketHandling' is configured to 2 (Drop Packets and Issue Warnings). | Device forwards RTP packets with unsupported payload types | Medium | All | n/a |
| SBC-52841 | The device fails to fallback to an alternative proxy IP address when in-dialog upon a resolved IP address from DNS. | Device disconnects call when proxy goes down | Medium | All | n/a |
| SBC-52896 | When in HA mode, the device loses Proxy Set connectivity upon an HA switchover because it fails to check if the IP interface is up. | Device loses Proxy Set connectivity upon switchover | Medium | HA | HA |
| SBC-52905 | A device management user with Security Administrator level can't access SFTP directories and files when using SSH key authentication (instead of password). | Device files are inaccessible over SFTP | Medium | All | n/a |
| SBC-52933<br>SBC-54009 | The device restarts when running out of SIPREC resources (caused by a miscalculation of SBC and SIPREC licenses). | Device restarts | Medium | All | n/a |
| SBC-52944 | For Proxy Set load balancing, the device doesn't adhere to NAPTR priority and doesn't send SIP messages to the proxy IP addresses with the highest priority. | Device sends SIP messages to the wrong proxy IP address | Medium | All | n/a |
| SBC-52956 | Device kernel upgrade failure causes a delay in RTP | Poor voice quality. | Medium | Mediant 90xx | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | packets, causing poor voice quality calls. | | | | |
| SBC-52978 | The device's SNMP walk enters a loop after reaching the performance monitoring MIB rtcpXrHistoryGroupName (OID 1.3.6.1.2.1.255.1.4.1.2). | Device's SNMP walk enters an endless loop | Low | All | n/a |
| SBC-52987<br>SBC-53125<br>SBC-53378 | Upon the receipt of a SIP re-INVITE without SDP and the far side supports re-INVITE only with SDP, the device sends an SDP Offer based on the recent far side state (inactive, sendonly, recvonly, or sendrecv), causing one-way voice. | One-way voice | Medium | All | n/a |
| SBC-53083 | The device fails to activate media of real-time text (RTT) when the first coder in the 'm=text' SDP line is the redundancy (RED) coder instead of the voice coder, causing call failure. | Call failure | Medium | All | n/a |
| SBC-53113 | The device sometimes fails a new SSH session if there was no delay after the previous session. | Device's SSH session fails | Medium | All | n/a |
| SBC-53142 | When the device's CLI filter `grep` or `egrep` is used with the `show ini-File` command, its output displays only up to the first 21 lines. | Incorrect CLI output | Low | All | n/a |
| SBC-53213 | The device fails to route the call from the SBC to Gateway application when an async LDAP operation is assigned to the IP-to-IP Routing rule. | SBC-to-Gateway call routing failure | Medium | Hybrid (SBC and Gateway) | n/a |
| SBC-53287 | The device's HTTP basic authentication for Web Services doesn’t function properly (sends multiple requests after HTTP 401 without waiting for a response). | Device faulty behavior after receiving a 401 response | Medium | All | n/a |
| SBC-53325 | The device restarts (error message "Signal 6, Task cli1") when an attempt is made to delete a non-existing call through CLI. | Device restarts | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-53339 | When the device receives a SIP INVITE with multipart bodies and applies message manipulation, it miscalculates the body length (Content-Length header) in the outgoing leg. | Device sends INVITE with incorrect SDP | Medium | All | n/a |
| SBC-53359 | The device sends RTP with an unsupported payload type because of incorrect NoOp payload type value. | Device sends RTP packets with unsupported payload types | Medium | All | n/a |
| SBC-53415 | The device sends a CDR report for a SIP INVITE that received a 422 Session Interval Too Short response, causing a mismatch between the number of calls and OVOC's report of max. number of calls. | Device calculates incorrect maximum of number of calls | Medium | All | n/a |
| SBC-53478 | Deletion of an LDAP Server Group through the SBC Routing Policies table causes the device to lose this Routing Policy, which causes all calls belonging to this Routing Policy to fail. | Call failure | Medium | All | n/a |
| SBC-53479<br>SBC-54027 | When receiving an incoming delayed offer (INVITE without SDP) and receiving a 18x without SDP from the outgoing side, the device doesn't add SDP to the outgoing 18x (even if the parameter 'Remote Can Play Ringback' is disabled) unless PRACK is required. This is because the SDP is an offer and unless PRACK is sent, there is no way to answer it. | Call failure | Medium | All | n/a |
| SBC-53480 | The device fails to apply the value of the 'Web Server Name' field if it's greater than 64 characters. | Device's Web interface is inaccessible | Medium | Mediant VE/CE | n/a |
| SBC-53483 | Login to the device's Web interface via Proxy API Google Chrome fails because the device can't handle requests containing long headers. | Device's Web interface is inaccessible | Medium | Mediant VE/CE | Google Cloud |
| SBC-53524 | The device sends an error message ("IsDataReady: Internal timer expired | Device sends repeated syslog warning messages | Low | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | (errorCode = EWOULDBLOCK)". | | | | |
| SBC-53539 | An Ethernet Group can't be added and then used in the Ethernet Devices table without a device restart. | Device restart required to apply changes | Medium | All | n/a |
| SBC-53566 | When the device sends a SIP INVITE request for alternative routing, the Via header still uses the transport type of the initial outgoing INVITE. | Device sends INVITE with incorrect Via header (transport type) | Medium | All | n/a |
| SBC-53625 | The 'Enable DHCP' parameter is missing from the device's Web interface. | Can't enable or disable DHCP through Web interface | Low | All | n/a |
| SBC-53697 | Security vulnerabilities have been identified on the device that allow users with Monitor level to configure the Configuration Wizard and access the License Key page. | Device vulnerability | High | All | n/a |
| SBC-53727<br>SBC-53775 | The Trunk Groups table cannot be modified through the device's Web interface. | Web interface limitation | Medium | MP-1288 | n/a |
| SBC-53770<br>SBC-54118 | The device issues kernel warnings in syslog ("kern.warning [S=11070] kernel: [ 5721.214218] malformed skb eth4: len 567 data_len 527"). | Devices issues repeated syslog warning messages | Low | Mediant 90xx / Mediant Software | n/a |
| SBC-53888 | Voice call fails upon a SIP re-INVITE request for fax to T.38 and the UdpPortSpacing parameter is configured to 2. | Fax call failure | Low | All | n/a |
| SBC-54050 | The device fails to apply the value of the IP Profile parameter 'RTCP Encryption' upon a SIP re-INVITE request. | Call failure | Medium | All | n/a |

## 2.11 Version 7.40A.501.158

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:** This SBC version is compatible with Stack Manager Version 3.4.2 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

> **Note:**
>
> - **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
>   - √ This version is compatible only with OVOC Version 8.2.1382 or later.
>   - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
> - **Using this SBC version with a centralized license pool:**
>
>   Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.
>
>   When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

### 2.11.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-13: Resolved Constraints in Version 7.40A.501.158**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-52290 | The device's DSPs restart because of a network load, causing PSTN calls to end. | Call failure | High | HA | n/a |
| SBC-52626<br>SBC-53368 | The device restarts with an error message ("Signal 11, Task SPMR") because of a failure in handling long SDP lists. | Device restart | High | All | n/a |
| SBC-52711<br>SBC-53220 | The device truncates the end of the SDP body when it operates in ICE-Full mode and receives a long SDP list. | Device truncates SDP body | High | All | n/a |
| SBC-52832<br>SBC-52954<br>SBC-52984<br>SBC-53283 | The device "cuts" the voice stream because of incorrect handling of SIP re-INVITE messages, causing one-way voice. | One-way voice | High | All | n/a |
| SBC-52989 | The device exhibits incorrect behavior during user network failures, resulting in the inability to re-establish SIP user registration with the proxy server upon network recovery. | User unable to re-register to SIP server | Medium | All | n/a |
| SBC-53068 | The device fails to load the SBC Use Information file after | SBC User Information validation failure | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | a restart when using Flex License Pool. | | | | |
| SBC-53380 | The device restarts with an error message ("Signal 11, Task SPMR") because of running out of buffer resources when many INVITE requests are received at the same time. | Device restart | High | HA | n/a |

## 2.12 Version 7.40A.501.150

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1382 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.4.2 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.12.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-14: Resolved Constraints in Version 7.40A.501.150**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-52903 | When deployed in Microsoft Azure, the device fails to match HA configuration with the virtual machine's configuration, generating error messages ("cloudAPI: failed to get Azure resource name: ERROR: cannot GET http://<IP address>/metadata/instance?api-version=2021-05-01"). | Device fails to connect and synchronize with Azure metadata | High | Mediant CE | Azure |

## 2.13 Version 7.40A.501.149

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1382 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.4.2 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.13.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-15: Resolved Constraints in Version 7.40A.501.149**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-52247 | The device fails to send SDR files to the SFTP server running on Windows. | Device fails to send SDR | High | All | n/a |
| SBC-52276 | The device fails to send QoE data to OVOC whose address is defined by an FQDN and a port. | Device fails to send QoE | High | All | n/a |
| SBC-52592 | The device fails to end the SSH session when the session is disconnected on the client side at the same time as the device is disconnected from the network. | Device can't be connected over SSH | High | All | n/a |
| SBC-52712 | The device restarts because of incorrect TLS Context configuration (error message "Signal 11, Task TIMB"). | Device restart | High | All | n/a |
| SBC-52731 | The device responds with a SIP 491 to a re-INVITE, causing the call to end. | Call failure | High | All | n/a |
| SBC-52867 | The HA device doesn't end all TCP connections upon a switchover. | Incorrect MAC address of TCP connection | High | HA | n/a |

## 2.14 Version 7.40A.501.141

This version includes new features and resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1382 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.4.2 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

## 2.14.1 New Features

This section describes the new features introduced in this version.

### 2.14.1.1 Improved Configuration of Information Type for Syslog Servers

The configuration of the type of information (i.e., syslog, CDRs, or SDRs) that is sent to a remote syslog server has been improved. The optional values of the existing 'Information Type' parameter in the Syslog Servers table now provides more specific control:

- **All**: Sends all information types (syslog, CDRs, and SDRs). Previously, this option sent only syslog messages.
- **Syslog**: (New) Sends only syslog messages.
- **CDR**: (Existing and no change) Sends only CDRs.
- **SDR**: (Existing and no change) Sends only SDRs.

**Applicable Application:** All

**Applicable Products:** All

### 2.14.1.2 HTTP Client Requests and Responses Captured to Syslog

The device now provides a method to track HTTP interactions for troubleshooting. It can capture detailed information to syslog messages (like curl's verbose output) of requests and responses sent by HTTP clients.

By default, the device logs the received requests and responses from all HTTP clients. However, it can be configured to log requests and responses from only specific HTTP clients. This is done by defining a string(s) that must be present in their URLs.

This feature is configured by the following new parameters (ini and CLI only):

- [EnableHttpClientDbgMsg] / `configure troubleshoot > logging settings > enable-http-client-dbg-msg`: Enables this feature (by default, disabled).
- [HTTPLogFilter] / `configure troubleshoot > logging settings > http-log-filter`: Defines which HTTP clients to log, based on URL filter strings. By default, the device logs requests and responses from all HTTP clients.

**Applicable Application:** All

**Applicable Products:** All

### 2.14.1.3 FQDN for OVOC WebSocket Tunnel Address

The address of the OVOC WebSocket tunnel can now be specified as an FQDN, using the existing parameter 'OVOC WebSocket Tunnel Server Address'. Previously, only an IP address could be specified. This feature is required, for example, when a web application firewall (WAF) is implemented to protect the device's Web interface.

**Applicable Application:** All

**Applicable Products:** All

### 2.14.1.4 Location Updated for SIP TLS Performance Monitoring Parameters

The SIP TLS performance monitoring (KPI) parameters (listed below) are now located in the correct path, network.tlsStats.sipTlsStats.

- acKpiDdosStatsCurrentGlobalRejectedSipTlsConnTotal
- acKpiDdosStatsCurrentGlobalAttemptedSipTlsConnTotal
- acKpiDdosStatsCurrentGlobalActiveSipTlsConn
- acKpiDdosStatsIntervalGlobalRejectedSipTlsConn
- acKpiDdosStatsIntervalGlobalAttemptedSipTlsConn
- acKpiDdosStatsIntervalGlobalActiveSipTlsConnAvg
- acKpiDdosStatsIntervalGlobalActiveSipTlsConnMax

**Note:** For backward compatibility, these performance monitoring parameters still appear in the incorrect path (network.ddosStats.global).

**Applicable Application:** All

**Applicable Products:** All

### 2.14.1.5 Mid-Call SIP Messages Sent to Currently Active Proxy

When a Proxy Set is configured with multiple proxies (IP addresses), the device can now send in-call SIP messages (e.g., re-INVITE and BYE) to the currently active proxy if the proxy server that received the dialog-initiating INVITE message is currently offline. This occurs even if the currently active proxy was offline when the call was initially established.

This feature is enabled (by default, disabled) by the following new Proxy Sets table parameter: 'In-Call Route Mode' / `configure voip > proxy-set > in-call-route-mode` / [InCallRouteMode]

**Note:**

- For this functionality, all proxies in the Proxy Set must have the same transport type (e.g., all TCP); otherwise, unexpected behavior may occur (e.g., call failure).
- The device's CDR displays only the proxy that was used for the dialog-initiating INVITE message.

**Applicable Application:** All

**Applicable Products:** All

### 2.14.1.6 Blocking ICMP Timestamp Requests

The device can now be configured to block incoming ICMP timestamp requests. This prevents it from replying to such requests.

The ICMP protocol allows for network timing measurements, by sending an ICMP timestamp request to a remote peer and receiving an ICMP timestamp in reply. However, sending ICMP timestamp replies may expose the device to certain security vulnerabilities.

This feature is configured by the new ini file parameter [BlockIcmpTimeStamp]. By default, the device accepts ICMP timestamps and replies accordingly.

**Applicable Application:** SBC

**Applicable Products:** Mediant Software

## 2.14.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-16: Resolved Constraints in Version 7.40A. 501.141**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51052<br>SBC-51891 | The device fails to add the 'a=rtcp-mux' attribute to the SDP body. | Call failure | Medium | All | n/a |
| SBC-51352 | The device restarts because of an internal buffer overrun ("Trap Message - TPApp Exception: Linux Signal Board Was Crashed: Signal 11, Task SPMR, FaultAddr: 0x40"). | Device restart | Medium | All | n/a |
| SBC-51356<br>SBC-51643<br>SBC-51835<br>SBC-51843 | The device sends an SDP answer to Teams without candidates in response to an SDP offer from Teams with 'a=ice-lite'. | Call failure | Medium | All | n/a |
| SBC-51470<br>SBC-51812<br>SBC-51894<br>SBC-51955<br>SBC-52149 | The device fails to handle SIP UPDATE messages that don't contain an SDP before call establishment, causing call failure. | Call failure | Medium | All | n/a |
| SBC-51492 | The device rejects (SIP 500 Server Error response) an incoming SIP NOTIFY request in a scenario in which the user unregisters an Account. | Device rejects SIP NOTIFY request. | Medium | All | n/a |
| SBC-51519 | The device restarts during recovery from an initiated restart (user restarts or switchover) because of an erroneous DSP restart. | Device restart | Medium | Mediant Software | Azure |
| SBC-51525 | The performance monitoring parameters for TLS connections doesn't function with REST API. | Partial support of performance monitoring | Medium | Mediant 2600; Mediant 4000/B | n/a |
| SBC-51568 | AudioCodes Syslog Viewer fails to receive syslog messages from the device when the SDR sequence is | No messages in Syslog Viewer | Low | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | disabled (i.e., SdrSyslogSeqNum parameter set to 0). | | | | |
| SBC-51632 | The device terminates the MSRP connection when timer expires, instead of keeping the other leg opened. | MSRP connection failure | Medium | All | n/a |
| SBC-51633<br>SBC-51984<br>SBC-52198 | The device disconnects the call upon receiving a SIP 200 OK, after a false attempt to perform media sync when receiving a SIP UPDATE without SDP before call establishment. | Call failure | Medium | All | n/a |
| SBC-51634 | No audio in Teams calls when the device uses ICE-Full mode and rtcp mux is disabled. | No audio | Medium | All | n/a |
| SBC-51635 | The device restarts with the error message "no more release descriptors" because of calls using RTP redundancy and no DSP and play RFC 2833. | Device restarts | Medium | All | n/a |
| SBC-51636 | The device fails to reconnect to the syslog server (Kafka / Event Hub) after a switchover. | No connection to Kafka syslog | Medium | All | n/a |
| SBC-51637 | The device may be exposed to a vulnerability because of ICMP timestamp reply on the AWS Stack Manager. | Vulnerability | Medium | Mediant CE | AWS |
| SBC-51639 | The device discards the RestCDRHttpServer parameter value upon a restart (or switchover), causing it to stop sending CDRs to the server. | No CDR messages sent after restart | Medium | All | n/a |
| SBC-51640 | The device fails to re-establish the MSRP connection with the UAC after connection failure. | MSRP connection failure | Medium | All | n/a |
| SBC-51641 | The device doesn't send SIP re-INVITE to the SIPREC Server when a call is put on hold and the device is configured to play a held tone. | Devices doesn’t send re-INVITE to SRS | Medium | All | n/a |
| SBC-51642 | The device's fragmented UDP packets don’t have an identifier per RFC 791 and don't have an offset, causing | WebRTC call failure | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | DTLS negotiation to fail for WebRTC calls. | | | | |
| SBC-51645 | The device considers a Proxy Set and an IP Group as still offline even when a keep-alive using SIP REGISTER message succeeds. | Routing failure | Medium | All | n/a |
| SBC-51646 | The device runs out of Message Manipulation resources during high traffic. | Call failure | Medium | All | n/a |
| SBC-51647 | The device fails to receive calls because of fragmented IP protocol errors (IPv4 total length exceeds packet length). | Call failure | Medium | Mediant VE/CE | Cloud |
| SBC-51650 | The device fails to send syslog messages to the Kafka syslog server. | Device doesn't send syslog | Medium | Mediant VE/CE | Cloud |
| SBC-51748<br>SBC-51846<br>SBC-52177 | The HA device becomes standalone upon a switchover because the IP address of the active device wasn't saved on the redundant device's Access List table. | No HA | Medium | HA | n/a |
| SBC-51750 | The device switches to a different proxy server after an SRV query with changed weight and priority. | Device switches to incorrect SIP proxy server | Medium | All | n/a |
| SBC-51764 | The device uses an old jQuery version (3.4.1) which is exposed to a vulnerability (attacks using XSS). | Vulnerability | Medium | All | n/a |
| SBC-51768<br>SBC-51934<br>SBC-51949<br>SBC-52431<br>SBC-52389 | The device receives a SIP INVITE from Teams with an SDP that has 14 ICE candidates, but it can handle only up to 6. | Call failure | Medium | All | n/a |
| SBC-51776 | The device sends SIP REGISTER messages to all IP addresses in the Tel-to-IP Routing table when alternative routing is enabled (AltRoutingTel2IpMode). | Device sends SIP REGISTER messages | Medium | Gateway | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51845 | When a Condition in a Message Manipulation rule contains more than five Boolean terms (OR / AND), the message manipulation fails. | Message Manipulation failure | Medium | All | n/a |
| SBC-51860 | The device's OAuth feature of single sign-on (SSO) authentication stops functioning because of a buffer overrun. | OAuth doesn't function | Medium | All | n/a |
| SBC-51862 | The device changes the SIP code 452 in the Reason header because it's an unknown and unsupported SIP reason. | SIP reason changed | Low | All | n/a |
| SBC-51865 | The device fails to display the Registration Status page in the Web interface (Bad Request 400). | Web interface page not displayed | Low | All | n/a |
| SBC-51896 | The device restarts because of a race condition ("Signal 11, Task SPMR") when processing an incoming SIP SUBSCRIBE message and a connection teardown simultaneously. | Device restart | Medium | All | n/a |
| SBC-51904 | The device fails to establish calls, generating error messages "ARPMgrAddReq(): Failed to send Arp Request" and "ArpMgrSendArpReq(): Source address wasn't found in any of the interfaces". | Call failure | Medium | All | n/a |
| SBC-51909 | A Monitor user can't view additional Trunk Group rows in the Web interface's Trunk Groups table, using the drop-down list of indices. | Web interface limitation | Low | All | n/a |
| SBC-51939 | The device fails to accept the SIP 200 OK’s SDP when it contains a shorthand name for Content-Length (l) and the SIP message itself is received in a buffer containing two SIP messages. | Call failure | High | All | n/a |
| SBC-51940 | The device doesn't show the username of the user of the logged SSH session in the Activity Log. | Missing information in Activity Log | Low | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51946<br>SBC-51964 | The device fails to increase the SDP version in an outgoing SDP when the username in the SDP origin ('o=') field was modified. | Device sends incorrect SDP | Medium | All | n/a |
| SBC-51947 | The device sends an incorrect RouteSeq value to ARM for a call that was terminated due to a REFER\3xx. | Device sends incorrect information to ARM | Medium | All | n/a |
| SBC-51951 | The device restarts ("Reset Reason: DSP loading failure") because of an internal bug in the recovery mechanism. | Device restart | Medium | All | n/a |
| SBC-51958<br>SBC-52173 | The device fails to report a logical network failure that exists for less than two seconds. | Device doesn't send an alarm for network failure | Medium | All | n/a |
| SBC-51961 | The device fails to send a SIP re-INVITE to the SIPREC server if the coder changes of the recorded call, causing distorted voice in the SRS. | Device sends distorted voice to SRS | Medium | All | n/a |
| SBC-51965 | The device sends multiple SIP OPTIONS keep-alive retransmissions to unreachable servers, causing a network flood. | Device flooding network | Medium | All | n/a |
| SBC-51977 | The device sends a SIP INVITE to the outgoing leg with the incorrect Content-Length header, causing the far side to reject the SDP offer and the call. | Call failure | Medium | All | n/a |
| SBC-52028 | The device doesn't escape special characters (e.g., "&") in SIPREC metadata body sent to the SRS. | Device sends incorrect metadata body to SRS. | Medium | All | n/a |
| SBC-52029 | The device fails to connect to OVOC over WebSocket when accessed from OVOC with SSO. | No connection to OVOC | Medium | All | n/a |
| SBC-52039<br>SBC-52043 | The device sends a SIP re-INVITE with RTT ('m=text' media line in SDP) when RTP Broken Connection is detected. | Device sends incorrect SDP in re-INVITE, causing call failure | Medium | All | n/a |
| SBC-52066 | The device performs X-AC-Action message manipulation on SIP INVITE messages | Call failure | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | (even though not supported), causing call failure. | | | | |
| SBC-52120<br>SBC-52505 | The device restarts because of an internal bug in the token mechanism ("Exception Reason: TPApp Exception: Linux Signal"). | Device restarts | Medium | All | n/a |
| SBC-52122 | The device replies with a SIP 491 response to a re-INVITE request when the other leg sends an UPDATE without SDP. | Call failure | Medium | All | n/a |
| SBC-52124 | The device sends an incorrect SDP (partial RTT payload type) to the SIPREC server. | Device sends incorrect SDP to SRS | Medium | All | n/a |
| SBC-52142 | The HA device displays incorrect information in the output of the `show system utilization` CLI command upon a switchover during high traffic. | Device displays incorrect utilization data | Medium | HA | n/a |
| SBC-52143 | The device restarts because its cookies tokenizer mechanism fails to parse cookies correctly. | Device restart | Medium | All | n/a |
| SBC-52151 | The device doesn't do alternative routing for in-dialog SIP messages such as re-INVITE and BYE. | Alternative routing for in-dialog messages doesn't function | Medium | All | n/a |
| SBC-52191 | The device stops sending reports to the Floating License server. | Device stops sending reports to Floating License server | Medium | All | n/a |
| SBC-52284 | The device fails to add itself to ARM using the Additional Management Interfaces. | ARM connection failure | Medium | All | n/a |
| SBC-52333 | The device fails to handle an incoming SIP Via header (from ARM) whose 'branch' contains more than 129 characters, causing a routing error. | Routing error | Medium | All | n/a |
| SBC-52350 | The device sends a SIP re-INVITE message for media synchronization without incrementing the SDP version ('o=' line). | Device sends SDP offer with incorrect SDP version | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-52361 | The device restarts ("Signal 901, Task LIBT" and "CHashMap::CIterator ListIndex =") because of a failure in the channel closure mechanism upon the disconnection of a Media Component. | Device restart | Medium | All | n/a |
| SBC-52470 | The device re-registers to a new SIP proxy server IP address when enabled for *Registrar Stickiness* in the Accounts table and the proxy server IP list is refreshed to the same IP addresses. | Device losses stickiness of Accounts table | Medium | All | n/a |
| SBC-52490 | The device's `where` and `find-by` CLI commands are not functioning correctly. | Incorrect CLI output | Medium | All | n/a |

## 2.15 Version 7.40A.500.786

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.2.4 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.15.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-17: Resolved Constraints in Version 7.40A.500.786**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-51484 | The device doesn't send a SIP re-INVITE request to the SIPREC SRS server when the call is on hold and the device plays music on hold (MoH). | SRS error | High | All | n/a |
| SBC-51850<br>SBC-51882 | The device sends an SDP answer to Teams without candidates in response to an SDP offer from Teams with 'a=ice-lite'. | Call failure | High | All | n/a |
| SBC-51861<br>SBC-51856 | The device fails to re-open the channel when moving from SRTP tunneling and RTP forwarding to mediation, causing a loss of voice. | No voice after SIP re-INVITE | Medium | All | n/a |

## 2.16 Version 7.40A.500.781

This version includes resolved constraints only.

Version 7.40A.500.781 is the baseline version for the Long Term Support (LTS) 7.4 releases.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.2.4 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.16.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-18: Resolved Constraints in Version 7.40A.500.781**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-50787 | Provisioning the local user account in CLI causes the session to terminate. | CLI session terminates | Medium | All | n/a |
| SBC-50792 | The device restarts upon a search in the Web interface when the 'LDAP Authentication Filter' is configured with a long string (~460 characters). | Device restarts | Medium | All | n/a |
| SBC-50827 | The device doesn’t send syslog messages to the syslog server without disabling and then enabling syslog functionality. | Syslog configuration is not on-the-fly | Medium | All | n/a |

## 2.17 Previous Latest Release (LR) Versions

This section describes the previous LR versions of Release 7.4.

### 2.17.1 Version 7.40A.500.775

This version includes new features and resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**
  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**
  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.2.4 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.1.1 New Features

This section describes the new features introduced in this version.

#### 2.17.1.1.1 IPv6 Support for Deployments on Azure and AWS Cloud Platforms

The device now supports IPv6 addresses when deployed on Microsoft Azure or Amazon AWS cloud platforms.

**Applicable Application:** SBC

**Applicable Products:** Mediant CE; Mediant VE

#### 2.17.1.1.2 Support for Sending Syslog to Apache Kafka

The device's embedded syslog (Rsyslog) client can now send event logs (syslog messages) to Apache Kafka, an open-source platform for event streaming.

The device, as a Kafka *producer*, transmits syslog messages to the remote Kafka *broker*. The broker can be on a local server or hosted on the cloud.

The broker manages one or more *topics*, which act like categories for classifying syslog messages. For example, the device can be configured to send syslog messages to specific topics based on severity level. Multiple applications or services (Kafka *consumers*) can subscribe to these topics and receive the syslog messages.

The existing Syslog Servers table is used to configure this functionality. Kafka-specific configuration includes the following:

- 'Address' (existing) - defines the address (FQDN) of the Kafka broker.
- 'Kafka Topic' (new) - defines the Kafka topic (Event Hub name in Azure).
- 'Kafka Connection String' (new) - defines the authentication/encryption string (password) for connecting to the Kafka broker (topic).
- 'Transport Protocol' (existing) –set to the new optional value **KAFKA**.
- 'Port' (existing) – defines the listening port for Kafka (9093 for Azure Event Hub).

In addition to the above configuration, a TLS Context must be selected (using the global 'Syslog TLS Context' parameter).

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.3 New SNMP Alarms for Registration Failure and IP Group Connectivity

This release introduces the following new SNMP trap alarms:

- acIpGroupKeepAliveAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.163): This alarm is raised when there is no connection (based on keepalives) with an IP Group.

- acAccountRegistrationAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.164): This alarm is raised when a registration failure occurs for an Account.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.4Configurable Static ARP Mappings

The device now supports the configuration of static Address Resolution Protocol (ARP) entries for mapping MAC addresses to IP addresses. These ARP entries are configured in the newly added Static ARP table (accessible through Setup menu > IP Network tab > Core Entities folder > Static ARP).

Static ARP entries map the MAC addresses in a network to their rightful IP addresses. Therefore, this functionality can significantly reduce the device's risk of falling victim to ARP poisoning, by keeping network communication secure.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.5Using Initial SIP INVITE Information for re-INVITE Messages

The device can be configured to use the initial incoming SIP INVITE message to create a re-INVITE message. This can be used, for example, when the device receives (and locally terminates) a REFER message, and then creates and sends a re-INVITE to the peer side. This may be useful if the initial incoming SIP INVITE includes customized headers or bodies that the Customer wants to preserve for the outgoing INVITE.

This feature is enabled by the newly added IP Profile parameter called 'Use Initial Incoming INVITE for re-INVITE'.

**Note:** Enabling this feature may reduce the device's performance by up to 10%.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.6Test Calling through REST API

The device's REST API can now be used to run a test call, whereby the device initiates a call to a defined destination (and then ends the call). Previously, test calling was supported only by the Web and CLI (`debug test-call`) management platforms.

The test call is run using the new API URI endpoint */api/v1/sipTestCall*:

- Start test call: *POST /api/v1/sipTestCall/dial*
- Get test call results: *GET /api/v1/sipTestCall/getStatus?sessionId=<id>*
- Get test call configuration: *GET /api/v1/sipTestCall/show* or *GET /api/v1/sipTestCall/show?sessionId=<id>*
- End test call: *DELETE /api/v1/sipTestCall/drop?sessionId=<id>*

Like other supported management platforms, the REST API for test calls also provides attributes for configuring parameters such as called and calling number, destination IP Group, outgoing SIP Interface, and DTMF digits or tone to play.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.7 New SDR Field for Call Route Attempt Failure

The device supports a new optional Session Detail Records (SDRs) field called "Is Route Attempt". This field indicates if an attempt to route a call that includes alternative or forking routing rules (in the IP-to-IP Routing table) was successful ("yes") or unsuccessful ("no").

This new field can be included in SDRs by customizing the SDR structure using the existing SBC SDR Format table.

**Applicable Application:** SBC

**Applicable Products:** Median 90xx; Mediant Software

#### 2.17.1.1.8 Call Setup Rule in Routing Rule for Determining Destination Tag

The device can now be configured to run a Call Setup Rule (CSR) that is assigned to an IP-to-IP Routing rule to determine the destination tag. This feature is configured by the new IP-to-IP Routing table parameter called 'Pre Route Call Setup Rules Set ID'.

Previously, when the 'Destination Type' parameter of the IP-to-IP Routing rule was configured to **Destination Tag** and a CSR was assigned to it by the 'Call Setup Rules Set ID' parameter, the tag specified in the CSR was ignored. Instead, the tag was determined from a CSR assigned to other associated configuration entities such as the source SIP Interface, source IP Group, or Dial Plan.

One of the benefits of this feature is that a different tag and thus, a different destination IP Group can be used for each alternative route rule. This is done by assigning different CSRs per rule. Previously, such functionality wasn't supported because the CSR (if assigned to a source SIP Interface, source IP Group, or Dial Plan) ran only once for the initial incoming SIP dialog (during pre-routing stages such as classification and manipulation).

**Note:**

- The device first runs the CSR of the new 'Pre-Route Call Setup Rules Set ID' parameter before running the "regular" CSR of the 'Call Setup Rules Set ID' parameter (if assigned).
- The tag specified by the CSR of the 'Pre Route Call Setup Rules Set ID' parameter overrides all other previously determined tags.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.9 New "Abort" Action for "Exit" Call Setup Rules

Call Setup Rules (CSR) can now be configured to stop (abort) all attempts at routing the call, even if additional alternative routing rules exist. This feature is supported when the CSR's 'Action Type' parameter is configured to **Exit** and the 'Action Value' parameter to the new value called **Abort**.

Previously, the CSR that was assigned to the IP-to-IP Routing rule continued searching for alternative routes upon failure to match current rule. Now, if the CSR rule **Exits** with an **Abort**, the device stops its attempt at routing the call (even if additional alternative routing rules exist).

**Note:** This feature is applicable when the CSR is assigned to the IP-to-IP Routing table, using the 'Call Setup Rules Set ID' or the new 'Pre Route Call Setup Rules Set ID' parameter.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.10 DiffServ for Video Media

Differentiated services (DiffServ) for quality of service (QoS) can now be configured specifically for video media. Previously, DiffSev was configured together for audio and video media traffic, using the IP Profile parameter 'RTP IP DiffServ'. Now, the device can mark video traffic with a user-defined differentiated services code point (DSCP) value.

Video DiffServ is configured using the newly added IP Profile parameter 'RTP Video DiffServ'.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.11 Maximum Call Duration using Message Manipulation

Maximum call duration can now be configured using Message Manipulation rules (in the Message Manipulations table). This maximum call duration applies to calls belonging to the IP Group to which the Message Manipulation rule is associated.

This feature is supported by the new message manipulation call variables `Var.Call.Dst.MaxDuration` and `Var.Call.Src.MaxDuration` (depending on leg). The variable  is set in the 'Action Subject' field of the Message Manipulation rule, while the call duration (in minutes) is set in the 'Action Value' field. The value is set in single quotes (e.g., '30'). A value of '0' means unlimited duration.

**Note:** If this variable is defined, its maximum call duration value overrides both the global parameter [SBCMaxCallDuration] and the IP Profile parameter 'SBC Max Call Duration'.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.12 Maximum Characters Increased for LDAP Queries

The device can now send significantly longer search queries to the LDAP server for LDAP-based user authentication. Previously, the maximum length of a search query was limited to 255 characters. This limit has been more than doubled, allowing the device to send queries of up to 650 characters long. The search query is configured using the existing 'LDAP Authentication Filter' parameter.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.13 Maximum Characters Increased for SIP To/From Header 'tag'

The maximum number of characters supported by the device for the ‘tag‘ parameter in the SIP To and From headers has been increased from 99 to 150 for all devices. Previously, only Mediant 90xx and Mediant Software SBCs supported up to 150 characters.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.14 Enabling or Disabling MSRP

Message Session Relay Protocol (MSRP) functionality can now be enabled or disabled. This is configured using the newly added parameter 'Enable MSRP' / [EnableMSRP] / `configure voip > sbc settings > enable-msrp`.

This new control over MSRP ensures that the device allocates resources for MSRP, only when it's enabled.

**Note:**  By default, MSRP is disabled. Therefore, Customers using MSRP should make sure to implicitly enable MSRP after upgrading to this new software version.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.15 Keep-Alive for Keeping NAT Bindings Open of ICE Full Sessions

The device now sends keep-alive messages (per RFC) for media sessions using ICE Full. The purpose of these keep-alive messages is to keep NAT bindings open for the media session.

**Applicable Application:** SBC

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW

#### 2.17.1.1.16 Classification to IP Groups by Proxy Sets using SIP OPTIONS

Classification of incoming SIP dialog messages to IP Groups based on Proxy Sets can now be restricted to SIP OPTIONS. Previously, classification by Proxy Set applied to all SIP message types (e.g., INVITE, OPTIONS, and REGISTER).

This feature is enabled by configuring the existing IP Group parameter 'Classify By Proxy Set' to the newly added optional value **Enable For OPTIONS**.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.1.1.17 Alarm Update for Cloud Maintenance Events on SBC Virtual Machine

The HASystemFault SNMP alarm severity and description for HA switchovers during cloud platform maintenance events (Azure and GCP) has been updated.

When the device is deployed on a cloud platform and the virtual machine hosting it is undergoing a maintenance event, if a switchover occurs to the redundant device (triggered by a keepalive timeout), the HASystemFault SNMP alarm is now sent with minor severity level and its description indicates a switchover because of a maintenance event. Previously, the alarm was sent with major severity level and indicated a switchover because of a keep-alive error.

**Note:** This feature is applicable only to the following configuration setup:

- 'Maintenance Events Monitoring Enable' set to **Enable**.
- 'Maintenance Events Treatment Enable' set to **Disable**.

**Applicable Application:** SBC

**Applicable Products:** Mediant VE (HA)

#### 2.17.1.1.18 Updates to Existing Parameters

The following updates have been made to existing parameters:

- The 'Web Hostname' parameter (WebHostname) has been renamed 'Web Server Name'.
- The 'DNS Rebinding Protection' (DNSrebindingProtectionEnabled) parameter is now obsolete.
- The [HostHeaderProtection] parameter is now obsolete.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.1.1.19 Updates to CLI Commands

The optional values of the following CLI commands for the IP Profile table were changed to `enable` and `disable` to conform with CLI conventions:

- `sbc-generate-noop`
- `reliable-heldtone-source`
- `sbc-play-rbt-to-transferee`
- `sbc-renumber-mid`
- `sbc-rmt-can-play-ringback`

**Applicable Application:** All

**Applicable Products:** All

### 2.17.1.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-19: Resolved Constraints in Version 7.40A.500.775**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-47381 | Device runs out of resources for the Intrusion Detection System (IDS) feature, preventing malicious attackers (by IP and port) from being added to the IDS blocklist (even though empty). | Vulnerability as device fails to add attackers to IDS blocklist | Medium | All | n/a |
| SBC-47714 | When in HA mode, the Web Users table sometimes disappears (without any known reason). | No effect other than visually | Low | All | n/a |
| SBC-48177 | When uploading a CLI Script file using the REST API, it's incremental instead of full configuration. | No restart after uploading CLI Script file through REST API | Low | All | n/a |
| SBC-48339 | For a DTMF transcoding call, where one side uses DTMF RFC 2833 transport mode and the other uses DTMF transparent mode (in band), sometimes the device sends DTMF as RFC 2833 instead of transparent to the side using DTMF transparent mode. | Duplicated DTMFs | High | All | n/a |
| SBC-48548<br>SBC-49622 | When the Floating License is used, if the device restarts, the entries in the SBC User Information table are marked as invalid. | Invalid entries in SBC User Information table | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-48725 | The CLI command `rest-cdr-http-server` is missing from the CLI. (Its corresponding Web parameter is 'REST CDR HTTP Server'.) | Missing CLI command | Low | All | n/a |
| SBC-48797<br>SBC-49182 | When using the device's REST API to upload a CLI Script file containing a command with a filter (e.g., `show proxy-set display\|include proxy-name`), the output of the command isn't filtered. | Incorrect REST API output | Low | All | n/a |
| SBC-48805 | The device sends the SIP INVITE message to the SRS with an incorrect urn format ('urn:ietf:params:xml:ns:recording' instead of 'urn:ietf:params:xml:ns:recording:**1**'). | Partial support for RFC 7865 | Medium | All | n/a |
| SBC-48851 | The device restarts when importing a Dial Plan file, and at least one of the existing Dial Plans are deleted. | Device restart | Medium | All | n/a |
| SBC-48875 | The device supports only up to 15 characters for the ID in SIP Event headers (truncating any additional characters). | Event header's ID in SIP SUBSCRIBE messages is truncated to 15 characters. | Medium | All | n/a |
| SBC-48881 | The device restarts when installed with a License Key that exceeds users and session capacity according to the supported memory of the Azure instance type used for the device. | Device restart | Medium | Mediant-CE | Azure |
| SBC-48887 | The device's VMWare Tools version (12.1.5) may pose a security vulnerability (CVE-2023-20900). | Security vulnerability | Medium | All | n/a |
| SBC-48919<br>SBC-49255 | The device stops sending registration requests for users to the SIP server. | Device doesn't send SIP REGISTER requests to server | Medium | All | n/a |
| SBC-48920 | The device drops MSRP calls because of incorrect handling of the [NoRTPDetectionTimeout] parameter. | MSRP calls dropped | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-49096 | When the device is upgraded to 7.40A.500, the management interfaces don't show all the Ethernet ports (4 instead of 8 or 12, depending on hardware configuration). | Port degradation | Medium | Mediant 90xx | n/a |
| SBC-49117 | The device fails to latch to the correct RTP stream for a Teams call in which ICE negotiation with multiple incoming candidates (more than 6) occurs. | One-way voice | Medium | All | n/a |
| SBC-49130<br>SBC-49498 | The device fails to re-establish the MSRP connection with the UAC after connection failure. | MSRP connection failure | Medium | All | n/a |
| SBC-49133 | The device fails to handle duplicated incoming RTP streams, causing corrupted voice (with incorrect RTP sequence) on the peer side. | Device sends corrupted voice | Medium | All | n/a |
| SBC-49221 | When the device receives a SIP UPDATE message after call is established, and the other side doesn't support it, the device sends a re-INVITE, but with an SDP even though the UPDATE didn't have it. | | Medium | All | n/a |
| SBC-49236 | The device sends the SNMP traps PSTNSignalDSPUp and BoardConfigurationError upon a restart. | Unnecessary SNMP traps sent upon restart | Low | All | n/a |
| SBC-49400 | The device loses HA mode and moves to an active-active state (both devices active) after numerous switch overs. | Loss of HA | High | Mediant CE \ VE | Azure |
| SBC-49444 | The device can't be accessed through HTTPS redirection. | Device isn't accessible (reachable) | Medium | All | n/a |
| SBC-49453 | When the device is configured to fork a call to two destinations, if one of the forked destinations fail, the device routes the call to an alternative route (instead of waiting for the second forked destination to also fail). | Incorrect alternative routing logic | Medium | All | n/a |
| SBC-49514<br>SBC-50006 | Saving debug recording to the device's local storage [DebugRecordingLocalStorage] doesn't function. | Debug recording on local storage doesn't function | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-49520 | When the device is in HA mode and deployed on Azure, it sends a false alarm that indicates a virtual machine maintenance event was detected ("Event type = Redeploy"). | False alarm raised | Medium | Mediant CE/VE | Azure |
| SBC-49532 | When an incremental ini file is uploaded to the device, the device fails to apply the changes of the Authentication table (uses previous credentials for registration). | Incorrect credentials used | Medium | All | n/a |
| SBC-49556 | The device doesn't update the SIPREC SRS (by a SIP re-INVITE) when the DTMF payload type of the call changes. | Device doesn't send re-INVITE to SRS | Medium | Mediant-CE | n/a |
| SBC-49610 | The device generates a metering reporting with null values. | Corrupted metering report | Medium | All | n/a |
| SBC-49623 | The device adds an attribute without a reason ('a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid) to the SDP in the outgoing SIP INVITE. | Call failure | Medium | All | n/a |
| SBC-49636 | The device's feature for playing background tones to call parties fails after more than five concurrent SBC calls. | Playing background tones doesn't function as expected | Medium | All | n/a |
| SBC-49665 | Hitless software upgrade for HA devices fails because the redundant device doesn't acknowledge the receipt of the ini file from the active device. | Hitless upgrade failure | Medium | HA | n/a |
| SBC-49685 | The device uses alternative routing for non-dialog initiating SIP requests (e.g., BYE). | Incorrect alternative routing logic | Medium | All | n/a |
| SBC-49790 | The device restarts when running a SIP Message Manipulation rule on a URL’s 'pn-provider' parameter in a specific SIP header when it doesn’t exist. | Device restart | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-49820 | The device doesn't forward all supported crypto keys ('a=crypto') in the SDP offer. | Device sends partial SDP offer | Medium | All | n/a |
| SBC-49872 | No voice experienced for an attended call transfer attempt (SIP REFER with Replaces is sent at the same time when there is an ongoing UPDATE for a re-INVITE transaction in the other call). | No voice | Medium | All | n/a |
| SBC-49882 | The number of Contacts in the device's registration table increases because of a resource leak, causing no available free ID messages. | Lack of resources | Medium | All | n/a |
| SBC-49934 | The device repeatedly sends the syslog warning message "IsTimerOwnerIdValid". | No impact (repeated syslog warning message) | Low | All | n/a |
| SBC-49943 | The device restarts without any error message information (exception). | SBC restart | Medium | All | n/a |
| SBC-49997 | The device fails to connect to the LDAP server over TLS v1.3. | LDAP connection failure | Medium | All | n/a |
| SBC-50312<br>SBC-50523 | The device doesn't F the ICE candidates in the outgoing SIP 200 OK response that it sends to Teams. | Call failure | Medium | All | n/a |
| SBC-49679<br>SBC-50966 | The device displays the incorrect number of registered users after an HA switchover due to a resource leak in the registration process. | Device displays more than the allowed registered users | Medium | HA | n/a |
| SBC-49804 | The device's RADIUS login password is limited to 40 characters. | Short password for RADIUS- or LDAP-based device login. | Low | All | n/a |
| SBC-50085 | The device fails to add the STR XSRF-TOKEN when HTTP GET request returns a cookie that's too long to be added to the subsequent HTTP request. | Device fails to send subsequent HTTP requests | Medium | All | n/a |
| SBC-50390 | The IP Group table's 'Validate Source IP' parameter doesn't function correctly with an FQDN. | Classification failure | Medium | All | n/a |

### 2.17.2 Version 7.40A.500.357

This version includes new features and resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.1.1 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.2.1 New Features

This section describes the new features introduced in this version.

#### 2.17.2.1.1 Support for ICE-Full

The device now supports Interactive Connectivity Establishment (ICE) Full (RFC 8445). Up until now, it supported only ICE-Lite.

Full ICE is used to implement local media optimization for Unified Communication (UC), provided the UC vendor supports it. For example, in a SIP Gateway environment.

For Full-ICE, the device can play the role as ICE-controlled or ICE-controlling. The device initiates STUN negotiations for all candidate pairs. It sends the candidates with its local IP address, and a public IP address if configured in the device's NAT Translation table.

To support ICE-Full, the existing IP Profile parameter 'ICE Mode' has a new optional value called **Full**.

**Applicable Application:** SBC

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software

#### 2.17.2.1.2 Dynamic Selective Coder Transcoding during Calls of Unregistered Users

The device can now dynamically switch voice coders to improve voice quality during a call for the unregistered user side. If it detects poor voice quality (based on MOS), it switches the coder from G.711 to Opus (by using an alternative IP Profile). If it subsequently detects an improvement in the network (based on packet loss), it switches back to G.711. Up until now, this feature was supported only for registered users.

This functionality can be used for WebRTC click-to-call scenarios to reduce the number of transcoding resources on the device, by using transcoding only when voice quality is poor.

The feature is enabled by the following new IP Profile parameter:

- Web: 'Switch Coder Upon Voice Quality'
- CLI: `configure voip > coders-and-profiles ip-profile > switch-coder-upon-voice-quality`
- INI: [SwitchCoderUponVoiceQuality]

This feature also requires configuration of QoE profiles with severity-color thresholds for MOS (Quality of Experience Profile table), and configuration of Quality of Service rule with 'Rule Metric' set to **Poor Invoice Quality**, and 'Rule Action' to **Alternate IP Profile**.

**Note:** This feature doesn't support HA switchover. For example, if the coder changed to Opus before the switchover, after the switchover the call remains with Opus until it ends, even if voice quality improves.

**Applicable Applications:** SBC

**Applicable Products:** All

#### 2.17.2.1.3Load Balancing of SIPREC Servers (SRS)

SIPREC Servers (SRSs) can now be defined by the existing IP Group Set functionality, which is a group of IP Groups used for load balancing calls. Each time the device sends a SIPREC session, it chooses the IP Group based on the IP Group Set's load-balancing policy (i.e., round-robin, homing, or random weight).

This feature is configured by the new parameter in the SIP Recording Rules table called 'Recording Server (SRS) IP Group Set'. The parameter is a row pointer to the IP Group Set table.

**Note:** If the 'Recording Server (SRS) IP Group Set' parameter is used, the existing 'Recording Server (SRS) IP Group' and 'Redundant Recording Server (SRS) IP Group' parameters can't be used.

**Applicable Applications:** SBC

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software

#### 2.17.2.1.4Alternative Routing for MSRP Calls upon Broken Connection

The device's Broken Connection feature now also applies to Message Session Relay Protocol (MSRP) calls. Up until now, it was applicable only to RTP (voice) calls.

Configuration of this feature is the same as for RTP-based Broken Connection, by configuring the existing 'Broken Connection Mode' parameter to **Reroute** or **Reroute with Original SIP Headers**.

If the MSRP endpoints don't establish an MSRP connection within a user-defined timeout (configured by the existing 'Timeout to Establish MSRP Connection' global parameter), or if the MSRP socket is closed after the call was established, the device ends the session and searches the IP-to-IP Routing table for an alternative route. Explicit alternative routing rules for broken connection can be configured by setting the existing 'Call Trigger' parameter to **Broken Connection**.

**Applicable Application:** All

**Applicable Products:** All

#### 2.17.2.1.5Increase in Maximum Concurrent TLS Connections

The maximum number of concurrent TLS connections has been increased from 1,000 to 2,500.

**Applicable Applications:** SBC

**Applicable Products:** Mediant 2600; Mediant 4000/B.

#### 2.17.2.1.6Capacity of Accounts Table Increased

The maximum number of Accounts that can be configured in the Accounts table has been increased to 5,000.

**Applicable Applications:** SBC

**Applicable Products:** Mediant 90xx; Mediant Software (64 GB or greater)

#### 2.17.2.1.7Consultative Call Transfer for NG9-1-1 Calls

The device now supports consultative call transfers that are initiated by the PSAP operator for emergency (NG9-1-1) calls, per NENA i3 Standard for Next Generation 9-1-1 (NENA-STA-010.2-2016).

This feature functions as follows:

1. When the device receives a SIP INVITE request that is a 911 call, it sends it to the PSAP operator through its FXO port interface.
2. The PSAP operator places the 911 caller on hold, and then establishes a new call with another party (e.g., emergency provider).
3. The PSAP operator transfers the 911 caller to the new call party. The device uses a SIP REFER message to bridge the 911 caller with the new call party when the PSAP operator goes on hook.

This feature is enabled (disabled by default) by the following new parameters:

- **Global:**
  - CLI: `configure voip > gateway analog fxo-setting > fxo-consult-call-transfer`
  - ini: [FXOConsultCallTransfer]
- **Tel Profiles table:**
  - Web: 'FXO Consultative Call Transfer'
  - CLI: `configure voip > coders-and-profiles tel-profile > fxo-consult-call-transfer`
  - ini: [FXOConsultCallTransfer]

**Applicable Application:** FXO Gateways

**Applicable Products:** Mediant 500L; Mediant 800B/C; Mediant 1000B

#### 2.17.2.1.8 Optimized Handling of SIP SUBSCRIBE Dialogs

The device's handling of SIP SUBSCRIBE dialogs for registered User Agents (UAs) has been optimized. The optimization frees up the device's resources that are otherwise utilized by stored SUBSCRIBE dialogs.

This feature is supported by the following new parameters:

- **Backing up SUBSCRIBE Dialogs (Applicable to HA Only):**

  By default, when the device operates in HA mode, it backs up SUBSCRIBE dialogs of registered UAs. This allows the redundant (now active) device to maintain their subscriptions and send relevant NOTIFY messages to the SIP UAs after an HA switchover. However, for SUBSCRIBE dialogs over TLS or TCP connections, a new connection is usually established by the remote UA after a switchover and therefore, backing up SUBSCRIBE dialogs is unnecessary and wasteful to resources.

  The following new parameter configures this feature:

  - CLI: `config voip > sbc settings > backup-subscriptions`
  - INI: [BackupSubscriptions]

  The parameter provides the following optional behavior:

  - Disables backup of all SUBSCRIBEs.
  - Enables backup of only SUBSCRIBEs using the UDP transport protocol.
  - Enables backup of all SUBSCRIBES, regardless of transport protocol (default).
- **Clearing SUBSCRIBE Dialogs from Storage:**

  By default (and like in previous versions), the device stores SUBSCRIBE dialogs of registered UAs until they expire. Now, the device can be configured to delete from storage (disconnect) SUBSCRIBE dialogs upon the following: an unregister, a register expiry, or a refresh register from a different source IP address / port (e.g., when transport protocol is TCP or TLS).

  The following new parameter configures this feature:

- CLI: `config voip > sbc settings > disconnect-subscriptions`
- INI: [DisconnectSubscriptionsMode]

**Applicable Applications:** SBC

**Applicable Products:** All

#### 2.17.2.1.9 Certificate Expiry SNMP Alarm Includes Common Name

The text description of the Certificate Expiry SNMP alarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.128) now also includes the Common Name (CN) of the TLS certificate, for example: "The certificate of TLS context 0 (**CN=SBC.audiocodesaas.com**) will expire in 30 days"

**Note:** If the certificate doesn't contain a CN, the first subject alternative name (SAN) is included in the description. If a SAN also doesn't exist, "" is included in the description.

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.2.1.10 Multiple SIPREC Servers (SRS) Triggered by SIP INFO Messages

SIP INFO messages can now be used to trigger the device to record calls using multiple SIPREC servers (SRSs). Up until now, only a single SRS (IP Group) could be triggered by an INFO message.

This feature also allows the SIP INFO message to specify the SRS as an IP Group Set(s) instead of an IP Group(s). Using an IP Group Set may be useful, for example, if load balancing between IP Groups is required.

AudioCodes' proprietary 'X-AC-Action' header is also used to trigger multiple SRS IP Groups:

- **Individual IP Groups:**

  ```
  X-AC-Action: <action>;recording-ip-group="x,y,z"
  ```

- **IP Group Set(s):**

  ```
  X-AC-Action: <action>;recording-ip-group-set="x,y,z"
  ```

Where:

- <action> starts (*start-siprec*), stops (*stop-siprec*), pauses (*pause-siprec*), or resumes (*resume-siprec*) the SIPREC session.
- *x*, *y* and *z* represent the SRS IP Groups / IP Group Sets.

**Note:** Different IP Groups can be specified for each action. For example, the SIP REC session can be started (*start-siprec*) on SRS IP Groups x, y and z, and then later paused (*pause-siprec*) only on SRS IP Group y.

**Applicable Applications:** All

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software

#### 2.17.2.1.11 Performance Monitoring Parameters for Active TLS Connections

The device now provides new performance monitoring parameters (gauges) for indicating the number of active TLS connections for SIP sessions (total, maximum, and average):

- activeSipTlsConnTotal: Total number of currently active TLS connections.
- activeSipTlsConnMax: Historical maximum number of active TLS connections.

- activeSipTlsConnAvg: Historical average number of active TLS connections.

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.2.1.12 SFTP Folder Access Permission Based on Management User Level

The device now permits access to its folders through SFTP, based on the SFTP client's management user level:

- Security Administrator and Master user levels can access all folders, for example, those containing CDRs, SDRs, and debug capture.
- Administrator user levels can access only folders containing CDRs and SDRs (i.e., */cdr*, */cdr-gw*, and */sdr*).
- Monitor users can't access any folder.

**Applicable Applications:** SBC

**Applicable Products:** Mediant 90xx; Mediant Software

#### 2.17.2.1.13 Signaling Source in SIP Call Flow for OVOC

When the device is configured to send SIP call flows (ladder) to AudioCodes OVOC, it now includes the signaling source (IP address and port) of the SIP Interface that is associated with the call.

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.2.1.14 Additional Device Information Sent over SNMP to OVOC

The device can now provide additional information (if requested) to OVOC through SNMP, using the following new SNMP parameters:

- acTrunkGlobalConfiguredE1Trunks: Number of configured E1 trunks.
- acTrunkGlobalConfiguredTrunks: Number of configured trunks (regardless of trunk protocol type).
- acSysLicenseKeySipRecSessions: Number of licensed SIPREC sessions.
- acSysLicenseKeySBCSignalingSessions: Number of licensed SBC signaling sessions.

**Applicable Applications:** All

**Applicable Products:** All

### 2.17.2.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-20: Resolved Constraints in Version 7.40A.500.357**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-45082<br>SBC-45620 | When the device operates in HA mode and deployed in Azure, the redundant device "freezes" upon the receipt of | HA switchover | Medium | HA | Azure |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | an Azure maintenance event, which causes a switchover. | | | | |
| SBC-45305 | The device restarts when an trying to download the locally stored debug recoding files through FileZilla. | Device restart | Medium | All | n/a |
| SBC-45420 | The device's WebSocket tunnel connection with OVOC is shown in the debug recording (DR) file with the wrong IP interface. | Incorrect device IP interface in DR file | Medium | All | n/a |
| SBC-45799 | When the device is in HA mode, a switchover occurs due to a software watchdog, and the redundant device takes over without certificates. | Switch over causes redundant device to take over without certificates | High | HA | n/a |
| SBC-46069 | The device uses IP address 0.0.0.1 in the HTTP PUT URL request for the host (for OVOC's feature of Host Header Validation), causing a failure of Host header verification for backing up device configuration on OVOC. | Failure of device configuration backup on OVOC | Medium | All | n/a |
| SBC-46214 | Adding a new row to the Interface table through Stack Manager invalidates a row in the Ethernet Group table and disables the physical port corresponding to the new interface. | Switch over causes invalid network configuration | Medium | All | Cloud |
| SBC-46404 | If the last row in the device's Access List table is to deny all access, the Web interface becomes inaccessible after upgrading the device to Version 7.4.500. | Web interface isn't accessible | Medium | All | n/a |
| SBC-46980 | The device displays only up to 12 digits for the Caller ID (more than that is truncated). | Caller ID longer than 12 digits is truncated | Medium | MP-1288 | n/a |
| SBC-47470 | When the device is deployed in a cloud environment and operating in HA mode, the redundant device issues syslog warning messages ("cloudAPI: failed to export InterfaceTable CSV"). | Repeated syslog warning messages | Medium | HA | Cloud |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-47946 | When the device receives a SIP 408 in response to a forked 18x, it clears the entire SDP offer-answer process. As a result, when a new forked 183 is received, it fails to fork the call (and issues syslog message). | Forking failure, causing call termination | Medium | All | n/a |
| SBC-48271<br>SBC-48873 | The device restarts because of a race condition, where it receives a SIP 4xx rejection of a call from the outgoing leg and a SIP CANCEL from the incoming leg, The device then sends an ARM request, receives an ARM response, but fails to allocate resources, and then restarts. | Device restart | Medium | All | n/a |
| SBC-48283 | The device's VMWare Tools version may pose a security vulnerability (should be at least 12.0.5). | Vulnerability | Medium | All | n/a |
| SBC-48879 | On-the-fly replacement of a TLS certificate for a TLS Context fails, causing SSL handshake failure. | On-the-fly certificate replacement fails, requiring device restart | Medium | All | n/a |

### 2.17.3 Version 7.40A.500.019

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 3.0.6 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

#### 2.17.3.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-21: Resolved Constraints in Version 7.40A.500.019**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-47672 | When the device is in HA mode, uploading an incremental CLI script file through REST API causes configuration errors on the redundant device. | HA mode terminated | Medium | HA products | HA |

### 2.17.4 Version 7.40A.500.017

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.9.5 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

#### 2.17.4.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-22: Resolved Constraints in Version 7.40A.500.017**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-45095<br>SBC-45426<br>SBC-45689 | Sometimes after modifying the device's configuration by uploading a new ini file or using the device's REST API, the standby (redundant) device of a High-Availability pair may lose some of its configuration. | After a switchover, the redundant device may not operate as expected and in some cases, may lead to loss of service. | Urgent | High Availability | High Availability |
| SBC-45544 | HA mode fails when the device's management interface is configured to use HTTP and the port is configured to a value other than the default (80). | No HA | High | High Availability | High Availability |

### 2.17.5 Version 7.40A.500.010

This version includes new features and resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1368 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.9.3 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.5.1 New Features

This section describes the new features introduced in this version.

#### 2.17.5.1.1 High-Availability in AWS Across Multiple Availability Zones

Mediant VE and CE in High-Availability (HA) mode can now be deployed in an AWS environment across multiple availability zones.

**Applicable Application:** SBC

**Applicable Products:** Mediant VE/CE

#### 2.17.5.1.2 Background Tones for SBC Calls

The device can now play background tones to the call parties in an SBC call. The tone can be played to one or both call parties (caller and/or callee). If played to both parties, the tone is played simultaneously. This feature can be useful, for example, to indicate that a call is being recorded.

This feature is supported by configuring a Message Manipulation rule with the following new options:

- 'Action Subject' field: Var.Call.Dst|Src.**PlayBackgroundTone** enables background tone on configured side (Dst) or peer side (Src)
- 'Action Value' field: **<side>,<tone ID>,<time between play>**, where:
  - *side*: Defines the call party to which the device plays the tone – 'both' (both sides) or 'single' (only configured side).
  - *time between play:* Defines the duration of no tone play between each play of tone (i.e., periodic play). If not configured, the device plays the tone continuously.
  - *tone ID:* Defines the tone to play by index in the PRT file (acUserDefineTone<ID>).

  *For example:* 'both,5,3000'

The background tone can be played after call establishment or during early media.

This feature is support for HA, allowing the resumption of tone play after a switchover.

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.5.1.3 Operating System using Rocky Linux 8

Starting with this version, the device uses a custom Linux OS version that is derived from Rocky Linux 8 (instead CentOS stream 8).

Rocky Linux 8 is based on the same codebase as CentOS, which has a long history of being a dependable and secure platform. One of the main reasons to move to Rocky Linux 8 is that it offers longer support than most other Linux distributions. With an end date of May 31, 2029, it provides security updates for the next 6 years.

Applicable Application: SBC

Applicable Products: Mediant VE/CE; Mediant 90xx

### 2.17.5.1.4Component Replacement for FXS Blades

Due to global supply chain shortages, a component replacement has been done for the FXS analog blades that are installed in MediaPack 1288 (MP-1288).

As a result of this component replacement, the software version of MP-1288 was updated and the hardware revision incremented. For more information, please refer to the Product Notice.

**Applicable Application:** Gateway.

**Applicable Products:** MP-1288.

### 2.17.5.1.5Notifying Change in Remote Party (Called / Calling) after Call Transfer

The device now notifies a change in the remote party (calling or called) after a call transfer (locally handled by the device).

The updated information is provided by adding a Remote-Party-ID header to the outgoing message (INVITE, UPDATE, or 200 OK). As the From header in the SIP dialogs throughout the call transfer process contains the URI of the initial call, the inclusion of the Remote-Party-ID header resolves the problem for identifying the new party.

The device also sets the fields in the Remote-Party-ID header to 'party=calling;privacy=off;screen=yes'. However, if a Remote-Party-ID header with 'party=calling' is already present in the incoming request or response, the device only updates the URI. If a Remote-Party-ID header is present in the incoming request or response, but with a different value of the 'party' parameter (e.g. 'party=called'), the device adds an additional Remote-Party-ID header as described above.

This feature is configured by the new IP Profile parameter, 'Send Header for Transfer', which must be set to **Remote-Party-ID**. The device adds the Remote-Party-ID header to the message sent to the call party that is associated with the IP Profile.

**Applicable Application:** SBC.

**Applicable Products:** All.

### 2.17.5.1.6SIPREC Enhancements

#### 2.17.5.1.6.1 Sending DTMF Notifications to Session Recording Servers (SRS)

The device can now be configured to send DTMF notifications to SRS servers. These notifications are sent using SIP INFO messages. On the incoming leg (caller), all DTMF formats (e.g., RFC 2833, INFO, or in-band) are supported; on the outgoing leg (callee), only DTMF digits from SIP INFO messages are supported.

For example (assuming "A" is the caller):

- "A" sends DTMF (any format): The device sends an INFO message to the SRS and to "B" (which must support sending and receiving INFO messages).
- "B" sends DTMF in INFO message: The device forwards the INFO message to the SRS and sends the DTMF to "A" in the required format (such as RFC 2833, INFO, or in-band).

The device also adds the Remote-Party-ID header to the SIP INFO message that is sent to the SRS. The header's value is the URI of the sender of the DTMFs.

This feature is enabled using the new global parameter [FwdSignalingToSIPRec].

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.5.1.6.2 SIPREC Recording of Real-Time Text (RTT)

The device can now record real-time text (RTT) in SBC sessions and send the RTT to the Session Recording Server (SRS) for SIPREC call recording.

RTT is carried in RTP and allows text to be sent immediately as it's created through wireless handsets that use IP-based technology on networks that support RTT. With RTT, there is no need to press a "send" key as there generally is for SMS, chat, or other types of texting.

For recording audio with RTT calls (i.e., two media streams), additional SBC media channel resources are required. For example, recording 100 SBC sessions of which 30 contain RTT, the following licenses are required: "SIPREC Streams" = 100, "SBC Sessions" = 100, and "SBC Media" = 60 (30 for RTT sessions plus 30 for RTT SIPREC sessions).

**Applicable Application:** SBC

**Applicable Products:** All

#### 2.17.5.1.7 Gateway CDR Customization for Adding SIP Header Information

The device can retrieve any SIP header's data from dialog-initiating (e.g., INVITE) or non-dialog initiating (e.g., SIP 200 OK) SIP messages and use it as the value for a CDR field in the generated Gateway CDR. Up until now, this was supported only by SBC CDRs.

The feature is supported by using call variable *Var.Call.Dst.UserDefined<1-5>* in Message Manipulation rules and by customizing the CDR in the Gateway CDR Format table. The Message Manipulation rule retrieves and stores the specified SIP header's value in the variable, and the CDR is customized to use the stored value for a CDR field. (The Message Manipulation rule is applied to the incoming or outgoing message, using the existing [GWInboundManipulationSet] or [GWOutboundManipulationSet] parameters, respectively.)

The 'Field Type' parameter in the Gateway CDR Format table provides new optional values that represent the CDR fields that retrieve stored information from the variables: **Var Call User Defined 1**, **Var Call User Defined 2**, **Var Call User Defined 3**, **Var Call User Defined 4**, and **Var Call User Defined 5**. (The title of these "variable" CDR fields can be modified.)

If a variable is not added or modified in the Message Manipulation rule and the CDR is customized to include its stored value, the CDR displays an empty string value.

**Applicable Application:** Gateway.

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 1000B; Mediant 3100.

#### 2.17.5.1.8 RTP Streams Forwarding

The device can now be configured to support RTP stream forwarding without requiring SIP configuration.

By default, the device prohibits any RTP stream forwarding, and only specifically allowed sources can establish RTP-to-RTP sessions.

The feature is configured in the new RTP-Only table, by the CLI command `configure voip > rtp-only sessions` or ini file parameter table [RtpOnly]. Configuration specifies the number of sessions, local interface:port, remote IP address:port, and port spacing.

Monitoring RTP streams forwarding sessions is done using the new SNMP alarm acRtpOnlyBrokenRtpConnectionAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.160). The alarm is raised when one of the streams is "broken".

This feature supports up to 9,000 RTP streams forwarding sessions.

**Note:** The feature doesn't support DTLS, coder transcoding, or SRTP.

**Applicable Application:** SBC

**Applicable Products:** Mediant Software

### 2.17.5.1.9Call Rerouting with Original SIP Headers upon RTP Timeout

When rerouting a call because of no voice (RTP) for a user-defined timeout (*Broken RTP Connection* feature), the device can now route the call to the new destination using the original headers and non-SDP bodies (XML only of multipart bodies) in the new SIP INVITE message. The SDP body is not copied but re-generated by the device.

This feature is configured using the new optional value **Reroute with Original SIP Headers** for the existing IP Profile parameter 'Broken Connection Mode'.

This feature is applicable for routing rules in the IP-to-IP Routing table whose 'Call Trigger' parameter is configured to **Broken Connection**.

**Applicable Application:** SBC.

**Applicable Products:** All.

### 2.17.5.1.10 Passwords Hidden in Activity Log

The device now automatically hides all passwords in the Activity Log. Passwords are hidden by asterisks (*). Up until now, some passwords were visible in the Activity Log (depending on configuration parameter or command).

**Applicable Application:** All

**Applicable Products:** All

### 2.17.5.1.11 Passwords Hidden in CLI Command History Buffer

The device can now be configured to show or hide (default) passwords in the CLI command history buffer. The device hides the passwords by replacing them with asterisks (*).

Therefore, when using the up and down arrow keys on the CLI prompt to recall previously typed commands from the history buffer, or using the existing `history` command to view the history buffer, passwords are hidden.

This feature is configured using the following new CLI command:

```
conf system > cli-settings > password-history-visible {off|on}
```

**Applicable Application:** All

**Applicable Products:** All

### 2.17.5.1.12 Configuration Package File Enhancements

The following enhancements have been introduced for the Configuration Package file:

- The 7-Zip file format (.7z) is now used (instead of .tar.gz) for the Configuration Package file. Support for 7-Zip allows the file to be compressed (LZMA2) and optionally, encrypted with a password and the AES-256 algorithm.

  The Configuration File also supports the inclusion of TLS private keys, trusted root certificates, and TLS certificates (when file encryption is used).

- The CLI command for copying the Configuration Package file supports a new option for encrypting the file and optionally, for including the certificates (only `to`):

  ```
  copy configuration-pkg to|from <URL> encrypted <password>
  certificates
  ```

- The Auto-Update mechanism can now provision the device with the Configuration Package file, using the following new CLI command:

  ```
  (config-system)# automatic-update
  (auto-update)# configuration-pkg <URL>
  ```

If the file is password-protected, the password can be specified in the CLI, using the following new command:

```
(config-system)# automatic-update
(auto-update)# default-configuration-package-password
<password>
```

This feature is also applicable when downloading the Configuration Package file through SFTP.

**Note:** For backward compatibility, the device supports the upload of the Configuration Package file in TAR (.tar.gz) format.

**Applicable Application:** All

**Applicable Products:** All

### 2.17.5.1.13 Clearing of CLI Command History

The device's CLI command history buffer, which stores previously typed commands during the current CLI session, can now be cleared using the following new commands:

- To clear all history records:

```
clear history
```

- To clear a specific history record (by index):

```
clear history <index>
```

The CLI history of commands (and their indices) is displayed using the existing `history` command. Recalling previously typed commands from the history buffer is done using the up and down arrow keys, as previously supported.

**Applicable Application:** All

**Applicable Products:** All

### 2.17.5.1.14 IP Interfaces and Ethernet Devices Tables Read-Only for Azure

When the device is deployed on the Azure cloud platform, network configuration tables (i.e., IP Interfaces table and Ethernet Devices table) are now read-only (already supported for AWS deployments). This is because the Ethernet devices are automatically configured by the management interface of the cloud platform.

**Applicable Application:** SBC

**Applicable Products:** Mediant Software

### 2.17.5.1.15 Customizing DNS Servers and MTU Size for Azure and AWS

By default, when the device is deployed in Azure or AWS, the DNS servers and maximum transmission unit (MTU) size for each interface are automatically configured based on the public cloud network settings.

These settings are displayed in the IP Interface table's 'Primary DNS' and 'Secondary DNS' fields, as well as the Ethernet Devices table's 'MTU' field, which are all non-editable.

However, in the current version, users can now customize the DNS servers and MTU through the device's Web interface. This can be done using the newly added Custom DNS Servers table and Custom MTU table, enabling users to override the automatically obtained values with their own configurations.

**Applicable Application:** SBC

**Applicable Products:** Mediant Software

#### 2.17.5.1.16 Registration Synchronization for SBC User Info Entities

Registration synchronization is now also supported for users configured in the SBC User Information table. Up until now, only SIP Accounts supported registration synchronization. Registration synchronization affects both Accounts and SBC User Information users that register to the same proxy server.

If an Account or user receives a timeout (configured by SipT1Rtx, SipT2Rtx, or SIPMaxRtx parameters) or response failure (e.g., SIP 403) for a sent SIP REGISTER request, the device stops sending REGISTER messages for all Accounts and users associated with the same serving IP Group (proxy server). The Account or user that first detected the no response (or failure) from the server is considered the *lead* Account or user. Only this Account or user continues to attempt registering to the proxy server.

When the lead Account or user receives a successful response from the proxy server, the device resumes the registration process for all the other Accounts and users associated with the same serving IP Group.

This feature is enabled by the ini file parameter [RegistrationSyncMode] and CLI command configure voip > sip-definition proxy-and-registration > reg-sync-mode.

Note: The Serving IP Group for an Account is configured in the 'Serving IP Group' field of the Account table. The Serving IP Group for a user is configured in the 'Destination IP Group' field of the IP-to-IP Routing table, matching the source 'IP Group' field in the SBC User Information table.

**Applicable Application:** SBC.

**Applicable Products:** All.

#### 2.17.5.1.17 Debug Capturing of Network Traffic on Device Interfaces

The device can now be configured to debug capture (record) network packets on device interfaces such as eth0, eth1, lo, or tun0. Previously, the device only supported debug capture through VLAN. With this new feature, users can now capture packets on the interface used for WebSocket tunneling, among other use cases.

This feature is supported by the following new CLI command option `kernel-dev`:

```
# debug capture voip interface kernel-dev <Name>|vlan <VLAN ID>
```

Debug capturing can also be done on all interfaces, using the 'any' value.

**Applicable Application:** All

**Applicable Products:** All

### 2.17.5.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-23: Resolved Constraints in Version 7.40A.500.010**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-42999 | When uploading a private key and certificate to a TLS Context, if the certificate file contains a chain (multiple certificates), the upload process deletes the trusted roots of the TLS Context. | Trusted root certificates are deleted. | Medium | All | - |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-43942 | The 'SDR File Name' parameter doesn't accept certain symbols in the hostname (e.g., '<' and '>'). | CDR file name failure | Low | All | All |
| SBC-44308 | The SNMP trap event acRedundantBoardAlarm is not required as all alarms indicate if trap raised by active or redundant device (in source varbind). | None | Low | HA | - |
| SBC-44308 | On HA systems, the redundant device sends trap events to the active device as alarms instead of as events, causing the user to receive alarms instead of events. | Incorrect SNMP reporting | Low | All | All |

## 2.17.6 Version 7.40A.400.067

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**
  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1342 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.8.5 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.6.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-24: Resolved Constraints in Version 7.40A.400.067**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-44799 | The device restarts, generating error message "Board Was Crashed: Signal 11, Task SPLB". | Device restart | Medium | All | All |
| SBC-45123 | No voice after an HA switchover when sending a SIP re-INVITE with different crypto keys. | No voice after HA switchover | Medium | All HA-supporting | HA |
| SBC-45461 | The device sends an SDP answer to Teams with incorrect crypto and port upon a delayed offer call. | No voice | Medium | All | All |
| SBC-45578 | The device fails to play a tone upon connect when trying to open the channel with DSP after it was already opened with DSP. | Failure to play upon connect | Medium | All | All |

### 2.17.7 Version 7.40A.400.063

This version includes new features and resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1342 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.8.5 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.7.1 New Features

This section describes the new features introduced in this version.

#### 2.17.7.1.1 Number of FXS Ports in Outgoing HTTP User-Agent Header

The device can now be configured to include the number of FXS ports in the HTTP User-Agent header when sending HTTP Get requests to the provisioning server for the Automatic Update mechanism.

This is supported by the new optional "<FXS>" placeholder (variable tag) for the existing [AupdHttpUserAgent] parameter. The device replaces this placeholder with the total number of FXS ports (and IDs of the FXS blades if the parameter's default is used).

**Applicable Application:** Gateway

**Applicable Products:** MP-1288

### 2.17.7.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-25: Resolved Constraints in Version 7.40A.400.063**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-43822 | The Configuration wizard no longer provides the option to define an HTTP proxy. | Missing parameters in Configuration wizard | Low | All | All |
| SBC-44154 | The device sends a SIP re-INVITE after an HA switchover with incorrect ICE parameters. | No voice after an HA switchover | High | All | HA |

## 2.17.8 Version 7.40A.400.042

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1223 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.8.5 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.8.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-26: Resolved Constraints in Version 7.40A.400.042**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-43274 | Device requires DSP resources for SDP termination if offering side uses the 'a=label' attribute and termination side doesn't. | Calls now need DSPs and if no DSPs, call fails. | Medium | All | n/a |
| SBC-43999<br>SBC-44007 | Connectivity with device's Web interface is lost after using the SBC Configuration wizard when "Agent Status is not Ready" appears in virtual machine. | Loss of connectivity with Web interface. | High | All | Azure |
| SBC-44047 | Device fails to copy files (e.g., Auxiliary files) from Active to Redundant unit on HA systems when using the SBC Configuration wizard. | HA is not operational. | High | High Availability (HA) | Azure |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-44188 | Device resets when uploading a Configuration file through ARM (or any routing server). | Device resets. | High | All | n/a |

### 2.17.9 Version 7.40A.400.023

This version includes new features, known constraints, and resolved constraints.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1223 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.6.7 or later. It's recommended to use Version 2.8.0 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.9.1 New Features

This section describes the new features introduced in this version.

#### 2.17.9.1.1 Mediant VE/CE Support for Ddsv5-series Virtual Machines

Mediant VE/CE SBCs deployed on Microsoft Azure cloud platform now support the Ddsv5-series virtual machines. These SBCs now also support Azure's accelerated networking feature. This support provides enhanced networking performance and increased session SIP call / session capacity. For capacity, see SIP Signaling and Media Capacity.

**Applicable Application:** SBC

**Applicable Products:** Mediant VE; Mediant CE

#### 2.17.9.1.2 Message Session Relay Protocol (MSRP) Enhancements

This version introduces the following MSRP enhancements:

- Support for Message Session Relay Protocol (MSRP) is now also offered on the Mediant CE SBC.
- The method for configuring MSRP ports has changed. Instead of configuring an MSRP port range in the Media Realms table ('TCP Port Range Start' and 'TCP Port Range End'), a single TCP and/or TLS port is configured in the SIP Interfaces table. This is done using the new SIP Interface parameters -- 'MSRP TCP Port' (non-secured MSRP) and 'MSRP TLS Port' (MSRPS, i.e., secured MSRP). The IP Interface and TLS Context that are associated with the specific SIP Interface are used for the MSRP session.

  **Note:**

  - This new port configuration is not backward compatible, and users need to reconfigure the MSRP ports accordingly after upgrading their device to this new software version.
  - MSRP is currently supported only for IPv4 networks.
  - Due to this feature, the 'TCP Port Range Start' and 'TCP Port Range End' parameters in the Media Realms table are now obsolete.
- A timeout for establishing an MSRP connection can now be configured. The timeout starts countdown from when the device opens an MSRP media socket (port) for the MSRP session. This is configured by a new parameter, 'Timeout to Establish MSRP Connection' (MSRPConnectionEstablishTimeout).

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.9.1.3Time Synchronization by PTP

When the device is deployed on Microsoft Azure or Hyper-V, the time of the SBC virtual machine can now be synchronized by the host's virtual PTP (Precision Time Protocol) device. PTP provides an alternative to external time synchronization services such as an NTP server or the Date header in SIP messages.

This feature is supported by a new configuration parameter called 'PTP Time Sync' (EnablePTP / `configure system > clock > ptp-time-sync`).

**Note:** The device places the highest preference for time synchronization on NTP, then SIP Date header, and lastly PTP. For example, if an NTP server is configured, the device ignores SIP Date header and PTP settings. If multiple synchronization methods are enabled, the device sends the existing SNMP alarm acClockConfigurationAlarm to notify of this configuration scenario.

**Applicable Applications:** SBC

**Applicable Products:** Mediant VE/CE

#### 2.17.9.1.4Max. Value Increase for Fields in Message Policies Table

The maximum value that can be configured for the following fields in the Message Policies table has been increased:

- 'Max Message Length': 65000
- 'Max Header Length': 4096
- 'Max Body Length': 61440
- 'Max Num Headers': 64
- 'Max Num Bodies': 64

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.9.1.5SIP Recording Rules Table Capacity (Rows) Increase

The maximum number of SIP-based media recording (SIPREC) rules (rows) that can be configured in the SIP Recording Rules table has been increased from 30 to 50.

**Applicable Applications:** SBC

**Applicable Products:** Mediant 9000; Mediant Software

#### 2.17.9.1.6 SIPREC Session Recording Server (SRS) Increased to Six

The maximum number of SRS's to where the device sends recorded SIP call sessions (SIPREC) has been increased from three to six. In other words, the device can now send SIPREC sessions to up to six standalone SRS's, up to six active-standby SRS pairs, or a combination of standalone and active-standby SRS's.

**Applicable Products:** All.

#### 2.17.9.1.7 IP-to-Tel Routing Table Capacity (Rows) Increase

The maximum number of IP-to-Tel routing rules (rows) that can be configured in the IP-to-Tel Routing table has been increased from 120 to 288.

**Applicable Applications:** Gateway

**Applicable Products:** MP-1288

#### 2.17.9.1.8 Accounts Table Capacity (Rows) Increase

The maximum number of SIP account rules (rows) that can be configured in the Accounts table has been increased from 102 to 288.

**Applicable Applications:** Gateway

**Applicable Products:** MP-1288

#### 2.17.9.1.9 Configurable Analog and Digital Port Description through CLI

A short description can now be configured per analog (FXO and FXS) and digital (PRI and BRI) ports through CLI. This is supported by the new `port-info` command, which is located under the relevant interface (BRI, FXS, or E1-T1). For example, for BRI interfaces:

```
(config-voip)# interface bri 1/1
(bri 1/1)# port-info MyDescription
```

In addition, this port description is now displayed in the output of the `display` command under the relevant interface, and also in the output of the `show run` and `show voip interface` commands.

**Applicable Applications:** Gateway

**Applicable Products:** Analog; Digital

#### 2.17.9.1.10 Interworking SIP UPDATE and re-INVITE According to Allow Header

When the existing 'SIP UPDATE Support' parameter is configured to **According Remote Allow**, the device now prefers UPDATE messages and converts received re-INVITEs as follows:

- If the Allow header from the remote contained UPDATE and the received re-INVITE contains an SDP, the device sends an UPDATE.
- If the incoming INVITE is without an SDP, the device forwards the INVITE.
- If the Allow header didn't contain an UPDATE, the device forwards it as an INVITE.

**Applicable Applications:** SBC

**Applicable Products:** All

#### 2.17.9.1.11 Service Preservation in Case of Public Cloud Maintenance Events

The device can now be enabled to monitor and detect scheduled virtual machine maintenance events performed by the cloud platform (Microsoft Azure or Google Cloud Platform / GCP) on which the device is deployed and hosted. A maintenance event can be, for example, a security patch update or a reboot.

Up until now, the device was not aware of cloud-initiated maintenance events on virtual machines. During such events, the device could become non-functional or performed an HA switchover.

When enabled (default), the device periodically queries the cloud platform's metadata service through REST API for scheduled maintenance events. The device logs the events (syslog) and sends the new SNMP alarm acVMMaintenaceAlarm, which indicates event type and estimated scheduled time. The alarm is automatically cleared when the event completes. Maintenance events monitoring is enabled by the new parameter, 'Maintenance Events Monitoring Enable'.

In addition, a new parameter 'Maintenance Events Treatment Enable' (enabled by default) was added to perform certain operations before the maintenance event occurs:

- For High-Availability (HA) systems, if the maintenance event is scheduled for the virtual machine of the active device, a switchover to the redundant device is triggered just before the event. If the maintenance event is scheduled for the virtual machine of the redundant device, a restart of the redundant device is triggered just before the event.
- For Mediant CE (Elastic Media Cluster mode), if the maintenance event is scheduled for a Media Component's virtual machine, the Signaling Component attempts to move all current sessions on the Media Component to a different Media Component (running on a different virtual machine).

Therefore, this feature allows the device to prepare itself for maintenance events and minimize traffic disruption.

These new parameters are located on a new page, Cloud Settings in the Web interface (Setup menu > IP Network tab > Advanced folder > Cloud Settings) and CLI (`configure network > cloud-settings`).

**Applicable Applications:** SBC

**Applicable Products:** Mediant VE/CE on Azure/GCP

#### 2.17.9.1.12 Display of Active Port in Ethernet Port Group

The Ethernet Groups table now displays the currently active Ethernet port in the new 'Active Port' field. This is applicable to Ethernet Groups that contain two ports for active-standby or active-active redundancy schemes (1Rx-1Tx, 2Rx-1Tx, or 2Rx-2Tx modes).

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.9.1.13 Ethernet Port Redundancy based on Remote Host Connectivity

For Ethernet port redundancy, the device now also supports port switchover to the standby port in the Ethernet Group, based on the reachability (connectivity) to user-defined network entities (destinations). If this feature is disabled, port switchover occurs only upon physical port failure (as already supported).

The device monitors the reachability of the destinations (IP addresses or FQDNs), by pinging them through the active port in the Ethernet Group. If there is no reachability (and according to various configuration settings), a switchover from active to redundant port is triggered.

The destinations to monitor are configured in the new Ethernet Port Group Network Monitor table (Setup menu > IP Network tab > Core Entities folder). Multiple "monitored" rows can be configured per Ethernet Group, where each row can include multiple destinations. A port switchover occurs only if a user-defined number of monitored rows are not reachable (i.e., all destinations of all the rows are not reachable). The monitored row threshold is configured by the new parameter 'Monitor Threshold' in the Ethernet Groups table (if configured to 0, the monitoring feature is disabled for the specific Ethernet Group).

The Ethernet Port Group Network Monitor table provides a child table, Ethernet Port Group Network Monitor Peers Status table, which displays the reachability status of all the destinations that were configured for a specific monitored row.

**Note:** This feature is applicable only to Ethernet Groups whose 'Mode' parameter is configured to **REDUN_1RX_1TX** and whose 'Monitor Threshold' parameter is configured to a non-zero value.

**Applicable Applications:** All

**Applicable Products:** MP-1288; Mediant 3100

### 2.17.9.1.14 Shortened CLI Commands using Aliases

The device now allows management users to create command aliases for its CLI. An alias is a shortened version (shortcut) of a command. Aliases may be useful for commands that are frequently used.

Aliases are configured in the new table, CLI Aliases (Setup > Administration > Web & CLI > CLI Aliases) - `configure system > cli-settings > cli-alias`.

An alias can be configured for a specific command (e.g., `copy`) or for a command sequence (e.g., `copy cli-script`). For example, if the alias of the `copy cli-script` command is "copyC", then instead of running the following command:

```
# copy cli-script from …
```

the following alias command can be used:

```
# copyC from
```

A list of all configured aliases can be viewed in the CLI, using the new command `show aliases`.

**Applicable Applications:** All

**Applicable Products:** All.

### 2.17.9.1.15 Support for Non-Interactive SSH Sessions

The device now supports non-interactive SSH sessions that may be used for running multiple SSH commands via automated connections. Multiple commands must be entered on the single command line using semicolons to separate each command. For example:

- `show running-config network; show system utilization`
- `configure troubleshoot; syslog; syslog-ip 10.4.2.11; exit; exit`
- `configure voip; sip-definition settings; 100-to-18x-timeout 100; exit; exit`

You may use standard SSH clients to execute commands via non-interactive sessions. The exact syntax differs depending on the specific SSH client. For example, for plink (PuTTY Link) the syntax is as follows:

```
plink.exe -no-antispoof -ssh 10.4.30.11 -l Admin -pwd Admin "show
running-config network; show system utilization"
```

Non-interactive SSH sessions are logged in the device's Activity Log as follows: "Activity Log: Executing multiple CLI commands".

**Note:**

- This feature is not supported for async commands (e.g., ping).
- Up to 8,000 characters can be entered on the command line (input).
- During non-interactive SSH session execution, new SSH connections (sessions) cannot be established.

**Applicable Applications:** All

**Applicable Products:** All.

### 2.17.9.1.16 Syslog Indication of Wrong Login Password or Username

The device can now be configured to indicate (in syslog) if the login username or password entered by the management user is wrong. Up until now, syslog only indicated that wrong credentials were entered, without specifying whether it was the username or password that was incorrect. This feature is configured by the existing parameter 'Invalid Login Report'.

**Applicable Applications:** All

**Applicable Products:** All

### 2.17.9.1.17 Firewall Defaults Changed

The default values of the following parameters in the Firewall table have changed:

- 'Prefix Length': from 0 to 32.
- 'Use Specific Interface': from Disable to Enable.

**Note:** Customers using CLI scripts for configuring this table must modify the script to explicitly specify the value of the 'Use Specific Interface' parameter.

**Applicable Products:** All.

### 2.17.9.1.18 Disconnecting Calls by Dial Plan Tag

Calls matching a specified Dial Plan tag (name=value or name only) can now be forcibly disconnected.

This is done using the new optional CLI command `tag` for the existing command `clear voip calls`. For example, below disconnects all calls whose tag is "region=usa":

```
clear voip calls tag region=usa
```

**Applicable Applications:** All

**Applicable Products:** All

#### 2.17.9.2 Known Constraints

This section lists known constraints.

**Table 2-27: Known Constraints in Version 7.40A.400.023**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-37942 | If syslog is associated with a dynamic IPv6 interface, syslog messages are not sent until interface receives IP address from DHCP (can be retrieved using debug file). | Some syslog messages are not sent to syslog server. | Low | All | All |
| SBC-42036 | The default value of the 'Use Specific Interface' parameter in the Firewall table was changed from **Disable** to **Enable**. As a result, Customers using CLI scripts for configuring this table must modify the script to explicitly specify the value for this parameter:<br>`configure network`<br>`access-list <index>`<br>`use-specific-interface disable` | Configuration is preserved for the device when upgraded from earlier to later versions. This change only impacts Customers using a CLI script created for an earlier version and used to configure the device for this version or later. | Low | All | All |

#### 2.17.9.3 Resolved Constraints

This section lists resolved constraints.

**Table 2-28: Resolved Constraints in Version 7.40A.400.023**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-37724 | The CLI script is missing trunk configuration (`configure voip > interface e1-t1 x`) in the output of `show running config`. | Downloaded CLI script missing important E1\T1 trunk configuration section. | Medium | Mediant 3100 | n/a |
| SBC-40710 | Configuring TLS expiry for a single TLS Context affects all other TLS Contexts. | All TLS Contexts are affected when one of the TLS Contexts is modified. | High | All | n/a |
| SBC-40761 | The SIP Header Value Encryption feature occasionally produces a "0d" or "0a" as its last character. These characters may be interpreted as the CRLF or end of line, causing parser issues for network stack level devices. | Outgoing messages (e.g., INVITEs) can be rejected with 4xx from remote side with "Bad SIP message structure". | Medium | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-41226 | The device's NTP offset is ignored following an upgrade to Version 7.4.300. (The offset doesn't affect the device's time and reapplying the offset after the upgrade resolves the issue.) | Report of wrong device time. | Medium | Mediant 9000; Mediant Software | n/a |
| SBC-41265<br>SBC-41307 | Device upgrade to Version 7.4.300 disables an IP Interface if the DNS fields (primary and secondary) were empty (not even 0.0.0.0) before the upgrade. | Device may be inaccessible (if it was the OAMP IP Interface). | High | All | n/a |
| SBC-41569 | The device sends a SIP re-INVITE repeatedly when the Play Tone Upon Connect feature is enabled. | Network may become congested if the device keeps sending re-INVITEs. | Medium | All | n/a |

### 2.17.10 Version 7.40A.300.021

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.1223 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to this compatible OVOC version prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.6.7 or later. It's recommended to use Version 2.8.2 or later.

**Note:** The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

### 2.17.10.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-29: Resolved Constraints in Version 7.40A.300.021**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-42536 | The device replies to the wrong proxy server when AlwaysSendToProxy is enabled, and the Proxy Set includes 8 IP addresses with different priorities and weights in Homing mode. | Call failure due to device replying to wrong proxy server | Medium | Gateway | n/a |
| SBC-42974 | The device fails to use its cache of DNS-resolved IP addresses, causing repeated DNS queries and overloading of the device. | Device overloads with repeated DNS requests | High | All | n/a |
| SBC-43180 | The device restarts after a manual HA switch over because of wrong buffer read\write allocation and deallocation. | Device restarts | Medium | All | HA |

### 2.17.11 Version 7.40A.300.013

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**
  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.280 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (see above) prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**
  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.6.7 or later. It's recommended to use Version 2.7.4 or later.

#### 2.17.11.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-30: Resolved Constraints in Version 7.40A.300.013**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-40890 | P-Access-Network-Info header decryption using the device's Message Manipulation *func.decrypt* feature sometimes fails. | Device doesn't properly encrypt the key at the terminating end, causing call failure | High | All | n/a |

### 2.17.12 Version 7.40A.300.012

This version includes new features, resolved constraints and known constraints.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.2.265 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (see above) prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to a compatible version (see above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.6.7 or later. It's recommended to use Version 2.7.1 or later.

### 2.17.12.1 New Features

This section describes the new features introduced in this version.

#### 2.17.12.1.1 HA Support for Mediant VE SBC Deployed on Microsoft Azure

Mediant VE SBC now supports High-Availability (HA) mode when deployed on the Azure cloud platform.

To support this feature:

- A new parameter called 'Source IP Address' has been added to the NAT Translation table, which allows the device to perform NAT translations based on the local IP address (source) of the active and redundant devices. This is instead of using the IP Interface name, which is the same between devices.
- A new standalone parameter called [ReInviteAfterHA] has been added, which maintains active calls when an HA switchover occurs. The redundant (now active) device does this by sending a SIP re-INVITE message with its local IP address.
- For installation instructions, click here.

**Note:** This feature requires that the remote endpoints support symmetric response routing according to RFC 3581.

**Applicable Application:** SBC.

**Applicable Products:** Mediant VE (Azure).

#### 2.17.12.1.2 Preloaded Trusted Root Certificate Authorities

The device now provides a preloaded list of popular trusted root certificate authorities (CA). These CAs can be used only for TLS Context IDs 0 through 4. Up until now (and still for TLS Context IDs 5 and above), the CA(s) had to be uploaded to the device per TLS Context.

To support this feature:

- A new parameter called 'Use default CA Bundle' has been added to the TLS Contexts table, which enables (disabled by default) the use of the default CAs for a TLS Context.
- A new page called Default CA Bundle (Setup > IP Network > Security folder > Default CA Bundle) has been added, which displays a list of the default CAs.

**Applicable Application:** All

**Applicable Products:** MP-1288; Mediant 800C; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.

### 2.17.12.1.3 IPv6 Networking Support

The device now supports IPv6 networking, as described in the following subsections.

#### 2.17.12.1.3.1 Autoconfiguration of IPv6 Interfaces

The device now supports autoconfiguration of IPv6 interfaces, configured in the IP Interfaces table. Dynamic IPv6 addressing allows the device to automatically obtain an IPV6 address and prefix length (and optionally, the DNS and Default Gateway addresses) through DHCP for the specific IP Interface.

To support this feature, the following new optional values have been added to the existing 'Interface Mode' parameter in the IP Interfaces table:

- **IPv6 Stateless:** Known as IPv6 Stateless Address Autoconfiguration (SLAAC), this method allows the device to automatically acquire IPv6 addresses without managing a DHCP server. The device generates addresses using local and non-local information. The non-local information is the prefix advertised by routers, which forms the first 64-bit segment (*network part*) of the 128-bit address. The local information is generated by the device using an algorithm based on the device’s MAC address, which forms the second 64-bit segment (*client ID*). The device generates a unique address per IP Interface. This method can also be used to obtain the DNS addresses through DHCP and the Default Gateway through Router Advertisement (RA) messages.
- **IPv6 DHCP:** Known as Stateful (DHCPv6) Autoconfiguration, this method allows the device to act as a DHCP client to acquire IPv6 addresses from an external DHCP server. The device sends a DHCP request once configured and upon every device restart. The DHCP server can provide not only the IP address and prefix, but also the DNS server address and Default Gateway address. Based on the DHCP lease time, the device renews its lease over the IP address with the DHCP server.

For dynamic IPv6 addressing, the existing SNMP alarm acIPv6ErrorAlarm is raised (major) when an IPv6 address for an IP Interface is not received within 10 seconds from the server.

IP Interfaces configured for dynamic IPv6 addressing are supported by all the device's applications. This includes, for example, SIP signaling, media (RTP), RADIUS, LDAP, CDRs, HTTP services, debug recording, and syslog.

**Note:**

- Dynamic IPv6 addressing is not supported when the device operates in High-Availability (HA) mode.
- The SBC Configuration Wizard is not supported (and not available in Web interface) if the IP Interfaces table contains an IPv6 address.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.2 Dynamic Assignment of IPv6 DNS Server Address

The DNS server addresses (primary and secondary) configured per IP Interface in the IP Interfaces table can now be overwritten by IPv6 addresses obtained from a DHCP server when implementing dynamic IPv6 addressing (see description of previous feature).

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.3 Two OAMP Interfaces (IPv4 and IPv6) in IP Interfaces Table

Up until now, the IP Interfaces table supported only one IP Interface configured with an "OAMP" Application Type, which had an IPv4 address. Now, an additional IP Interface with an "OAMP" Application Type can be configured that has an IPv6 address.

Therefore, this feature is about the support for configuring up to two OAMP IP Interfaces in the IP Interfaces table, where each has a different IP version (IPv4 or IPv6).

**Note:**

- The device is still shipped with a single default IP Interface, which has an "OAMP" Application Type and an IPv4 address.
- The IP Interfaces table must have at least one IP Interface (IPv4 or IPv6) that is configured with an "OAMP" Application Type. For example, if an IPv6 OAMP interface is configured, the default IPv4 OAMP interface can be deleted.
- The IPv4 OAMP interface is used by default by the device’s management interfaces (e.g., Web interface and CLI) and applications (e.g., syslog, RADIUS, and CDRs). Therefore, before deleting the IPv4 OAMP interface, a different IP Interface (which from this release no longer needs to be an OAMP interface) must be assigned to each of the management interfaces and required applications. If an IP Interface is not assigned, the IPv6 OAMP interface is used by default.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.4 SNMP over IPv6

The device now supports SNMP over IPv6.

To support this feature:

- A new parameter called 'IPv6 Interface Name' has been added, which assigns an IPv6 Interface for SNMP over IPv6.
- A new parameter called 'IPv4 Interface Name' has been added, which assigns an IPv4 Interface for SNMP over IPv4.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.5 IPv6 Hostname for SNMP Trap Manager

The address of the SNMP Trap Manager can now be configured with an FQDN (hostname) that resolves into an IPv6 address. Up until now, only a hostname that resolved into an IPv4 address was supported.

To support this feature, a new parameter called 'Trap Manager Host Name for IPv6' has been added.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.6 NTP over IPv6

The device can now automatically update its date and time through Simple Network Time Protocol (SNTP) from an NTP server over IPv6.

To support this feature:

- A new parameter called 'NTP Interface' has been added, which allows the user to select an IP Interface (IPv4 or IPv6).
- The existing 'Primary NTP Server Address' and 'Secondary NTP Server Address' parameters can now be configured with an IPv6 address.

In addition to this feature, a new parameter called 'Enable NTP' has been added, which enables or disables NTP.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.7 Auto-Provisioning over IPv6

Auto provisioning (Auto-Update mechanism) of the device can now be done over IPv6.

To support this feature:

- A new parameter called [AUPDInterface] has been added, which assigns an IP Interface from the IP Interfaces table to the Auto-Update mechanism. By default, the device uses the IPv4 OAMP interface.
- The URLs that define the location of the various files that can be uploaded by the Auto-Update mechanism (e.g., CmpFileURL) can now be configured with an IPv6 address.

**Note:** The IP version (IPv4 or IPv6) of the chosen IP Interface and the configured URLs must be the same.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.8 Remote HTTP Services over IPv6

The device now supports Remote Web Services (configured in the Remote Web Services > HTTP Remote Hosts table) over IPv6. Each Remote Web Service can be configured with multiple HTTP hosts with different IP address versions (IPv4 or IPv6).

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.9 HTTP Proxy over IPv6

The device now supports HTTP Proxy over IPv6.

To support this feature, IPv6 interfaces can be used in the HTTP Proxy Server and HTTP Locations tables.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.10 LDAP over IPv6

The device now supports LDAP over IPv6.

To support this feature:

- The existing 'LDAP Network Interface' parameter in the LDAP Servers table can be assigned an IPv6 interface.
- The existing 'LDAP Server IP' parameter in the LDAP Servers table can be configured with an IPv6 address.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.11 RADIUS over IPv6

The device now supports RADIUS over IPv6.

To support this feature:

- The existing 'IP Address' parameter in the RADIUS Servers table can now be configured with an IPv6 address.
- A new parameter called 'Interface Name' has been added to the RADIUS Servers table, which assigns an IP Interface (IPv4 or IPv6) for RADIUS communication.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.12 SDRs over IPv6

The device now supports sending Session Detail Records (SDRs) to a remote server over IPv6.

To support this feature:

- A new parameter called 'Interface Name' has been added to the SBC SDR Remote Servers table, which assigns an IP Interface (IPv4 or IPv6) for communication with the server.
- The existing 'Address' parameter in the SBC SDR Remote Servers table, which configures the server's address can now be configured with an IPv6 address.

**Applicable Application:** SBC.

**Applicable Products:** Mediant 9000; Mediant Software.

#### 2.17.12.1.3.13 SBC CDRs over IPv6

The device now supports sending CDRs of SBC calls to a remote server over IPv6.

To support this feature:

- A new parameter called 'Interface Name' has been added to the SBC CDR Remote Servers table, which assigns an IP Interface (IPv4 or IPv6) for communication with the server.
- The existing 'Address' parameter in the SBC CDR Remote Servers table, which configures the server's address can now be configured with an IPv6 address.

**Applicable Application:** SBC.

**Applicable Products:** Mediant 9000; Mediant Software.

#### 2.17.12.1.3.14 CDRs and SDRs over IPv6 through REST API

The device now supports sending CDRs and SDRs through REST API to remote HTTP/S-based REST servers (Remote Web Service) over IPv6.

To support this feature, the existing 'Address' parameter in the HTTP Remote Hosts table can now be configured with an IPv6 address and the ‘Interface’ parameter can be associated with an IPv6 interface.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.3.15 Syslog over IPv6

The syslog server can now be configured with an IPv6 address.

To support this feature:

- The existing global 'Syslog Server IP' parameter and the 'Address' field in the Syslog Servers table can now be configured with IPv6 addresses.
- A new global parameter called 'Syslog Interface' has been added, which assigns an IP Interface (IPv4 or IPv6) to the primary syslog server.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.3.16 Packet Capturing using RPCAP over IPv6

Packet capturing using the device’s embedded Remote Capture Protocol (rpcap) server now can be done over IPv6.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.3.17 Debug Recording over IPv6

The device now supports sending debug recording packets to a remote server over IPv6.

To support this feature:

- The existing 'Destination IP Address' (DebugRecordingDestIP) parameter can now be configured with an IPv6 address.
- The existing 'Interface Name' (DebugRecordingIpInterfaceName) parameter can now be assigned an IPv6 interface.
- The following debug recording operations through CLI now support IPv6:
  - `debug capture voip interface ... tftp-server <IPv4 / IPv6 Address>`
  - `debug capture voip physical stop <IPv4 / IPv6 Address>`
  - `debug capture voip physical get_last_capture <IPv4 / IPv6 Address>`

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.3.18 Online Certificate Status Protocol (OCSP) over IPv6

The OCSP server can now be configured with an IPv6 address. Up until now, it could only be configured with an IPv4 address.

To support this feature:

- The existing ‘OCSP Server’ parameter in the TLS Contexts table can be configured with an IPv6 address.

- The existing 'OCSP Interface' parameter in the TLS Contexts table can be assigned an IPv6 interface.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.19 QoE Reporting to OVOC over IPv6

The device now supports the sending of Quality of Experience (QoE) voice metric reports to OVOC over IPv6.

To support this feature:

- The existing 'Primary OVOC Address' and ‘Secondary OVOC Address’ parameters in the Quality of Experience Settings table can be configured with IPv6 addresses.
- The existing 'QoE Network Interface' parameter in the Quality of Experience Settings table can be assigned an IPv6 interface.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.20 File Transfer over IPv6 through CLI

The device's CLI can now be used to copy files to/from a remote server over IPv6.

To support this feature, the existing `copy` CLI command can now include URLs with IPv6 addresses and provides a new option called `network-source` to choose the IP Interface:

```
copy <File Type> from|to <URL> network-source <IP Interface Name>
```

By default, the device uses the IPv4 OAMP or IPv6 OAMP interface for the copy process for IPv4 or IPv6 servers, respectively. If there is no IP Interface with the same IP version (IPv4 or IPv6) as the remote server, the copy process fails.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.3.21 Network Traces of Both Source and Destination IPv6 Packets

The device can now be configured to include IP network traces of all IPv6 packets (source and destination) in syslog and debug recording messages. Up until now, the trace could either be configured for source or destination IPv6 address.

To support this feature, a new value called "ipv6" can now be configured in the 'Value' parameter of the Logging Filters table (applicable when the 'Filter Type' parameter is **IP Trace**).

**Applicable Application:** All

**Applicable Products:** All.

### 2.17.12.1.4 Maintenance Script

The device can now be loaded with a digitally signed maintenance script provided by AudioCodes. The script may be used, for example, to:

- Provide immediate mitigation for urgent security vulnerabilities.
- Apply minor software patches.

To upload the script, the Web interface's Auxiliary Files page now provides an additional file load area called "Maintenance Script file" which includes the buttons for selecting the file and loading it.

Only users with Security Administrator or Master level privileges can upload the Maintenance script file.

**Applicable Application:** SBC.

**Applicable Products:** Mediant 9000; Mediant Software.

#### 2.17.12.1.5 Multiple Management Interfaces

Up until now, the device’s management interfaces (e.g., Web, Telnet and SSH) only used the single (default) OAMP IP Interface in the IP Interfaces table. Now, any type of IP Interface (OAMP, Media or Control) can be used for management interfaces, and multiple management interfaces can now also be configured.

##### 2.17.12.1.5.1 Multiple Web and REST Interfaces

The device can now be configured with multiple management interfaces for accessing its Web and REST interfaces.

To support this feature, a new table called Web Interfaces (Setup menu > Administration tab > Web & CLI folder > Web Interfaces) has been added. Access to the Web and REST management interfaces can only be done through these configured Web Interfaces.

The Web Interfaces table provides a default Web Interface, which is associated with the default IPv4 OAMP interface.

**Notes:**

- The [EnableWebAccessFromAllInterfaces] parameter, which allowed access to the Web interface from all IP Interfaces in the IP Interfaces table is now obsolete. If this parameter was enabled in a previous version and the device is updated to 7.40A.300, the device automatically configures Web Interfaces for all the IP Interfaces, thereby maintaining required functionality.
- The Additional Management Interfaces table is now obsolete.

**Applicable Application:** All.

**Applicable Products:** All.

##### 2.17.12.1.5.2 Multiple Telnet Interfaces

The device can now be configured with multiple IP interfaces for accessing its embedded CLI server using Telnet.

To support this feature, a new table called Telnet Interfaces (Setup > Administration > Web & CLI > Telnet Interfaces) has been added. Each Telnet interface can be assigned any IP Interface type from the IP Interfaces table (IPv4 or IPv6) and configured with a port number.

**Note:** As a result of this feature, the [TelnetServerPort] parameter is now obsolete.

**Applicable Application:** All.

**Applicable Products:** All.

##### 2.17.12.1.5.3 Multiple SSH and SFTP Interfaces

The device can now be configured with multiple IP interfaces for accessing its embedded CLI server using SSH.

To support this feature, a new table called SSH Interfaces (Setup > Administration > Web & CLI > SSH Interfaces) has been added. Each SSH interface can be assigned any IP Interface type from the IP Interfaces table (IPv4 or IPv6) and configured with a port number.

**Note:** As a result of this feature, the [SSHServerPort] parameter is now obsolete.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.6 SIPREC Triggered upon Early Media

The device can now start recording calls (SIPREC) as soon as media starts. SIPREC can start even before the call is answered in case of early media (i.e., 18x response prior to 200 OK, for example, playing ring tone) or media after call connect.

To support this feature, a new optional value called **Media Start** has been added to the existing 'Trigger' parameter in the SIP Recording Rules table.

**Applicable Application:** All.

**Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.

#### 2.17.12.1.7 New VM Types for Mediant VE/CE Deployed on AWS

Mediant VE and Mediant CE SBCs now support the c5n and m5n instance types on AWS. These instance types provide improved networking performance and stability compared to the previously (and still) supported c5 and m5 instance types. Therefore, the c5n and m5n instance types are more recommended.

**Applicable Application:** SBC.

**Applicable Products:** Mediant VE; Mediant CE

#### 2.17.12.1.8 Automatic Configuration of Network Interfaces on Public Clouds

The Mediant VE and Mediant CE SBCs now automatically detect network interfaces attached/detached to/from the underlying virtual machine through cloud management interfaces and updates the IP Interfaces and Ethernet Devices tables accordingly. Configuration update is done online and without service disruption.

The feature is currently limited to public cloud environments (AWS, Azure, and Google) and requires that Ethernet port redundancy be disabled through a new parameter called [EnablePortRedundancy]. (This parameter is also applicable to Mediant 90xx and Mediant SE.)

**Applicable Application:** SBC.

**Applicable Products:** Mediant Software.

#### 2.17.12.1.9 Elliptic Curve Digital Signature Algorithm (ECDSA) Support for TLS

The device can now generate Elliptic Curve Digital Signature Algorithm (ECDSA) public-private keys. This means that the device can generate certificate signing requests (CSRs) and self-signed certificates that are digitally signed with ECDSA keys.

This feature also provides support for using ECDSA keys for accessing the device's CLI through an SSH connection. Instead of logging in with username and password, only username is required, and authentication is automatically done using the public key. (Up until now, only RSA was supported for SSH.)

To support this feature, a new parameter called 'Private Key Format' has been added to the Change Certificates page (TLS Context table > Change Certificates). The parameter defines the required key algorithm (ECDSA or RSA). When ECDSA is selected, the existing 'Private Key Size' parameter defines the required ECDSA key size (256-bit, 384-bit, or 521-bit).

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.10 Product Documentation Accessible from Web Interface

The device's documentation (e.g., User's Manual, Installation Manual, Security Guidelines, and Release Notes) can now be accessed from the Web interface. The Web interface's toolbar provides a new icon ? that when clicked, displays a drop-down list of documents that can be referenced. The documents' names are hyperlinked to their respective location on AudioCodes website, allowing users quick-and-easy access to these resources.

**Note:** For private labeling when the Web interface's logo is non-default, this new icon is not displayed. A workaround is to add a forward "/" slash at the end of the URL of a new parameter called [ExternalDocumentsBaseURL]:

```
ExternalDocumentsBaseURL =
'https://acredirect.azurewebsites.net/api/'
```

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.11 FQDN for Server Address

An FQDN can now be configured for certain servers, as described in the following subsections.

#### 2.17.12.1.11.1 FQDN for CDR and SDR Syslog Servers

The address of the CDR and SDR syslog servers for collecting CDRs and SDRs respectively, can now be configured as an FQDN. The device sends a DNS resolution query to a DNS server for the server's IP address (IPv4 or IPv6).

To support this feature, the existing 'CDR Syslog Server IP Address' [CDRSyslogServerIP] and 'SDR Server Address' [SDRServerIPAddress] parameters can now be configured with FQDNs.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.11.2 FQDN for OCSP Server Address

The OCSP server can now be configured with an FQDN. When configured with an FQDN, the device sends a DNS resolution query to a DNS server for the server's IP address (IPv4 or IPv6).

To support this feature, the existing 'OCSP Server' parameter in the TLS Contexts table can be configured with an FQDN.

**Note:** FQDN support for OCSP is applicable only to TLS Contexts that are dedicated for SIP traffic. If an FQDN is configured for a TLS Context that is used for non-SIP connections, the certificate is not checked by the OCSP server.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.11.3 FQDN for Syslog Server Address

The syslog server can now be configured with an FQDN. When configured as an FQDN, the device sends a DNS resolution query to a DNS server for the server's IP address (IPv4 or IPv6).

To support this feature, the existing global 'Syslog Server IP' parameter and the 'Address' field in the Syslog Servers table can now be configured with an FQDN.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.12 User-Friendly Coders Groups Table

The Coders Groups table, which configures groups of coders, now has a more user-friendly design. The new design provides two tables with parent-child relationship, where the parent table defines the name of the group while the child table defines the coders in the group.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.13 Registration Stickiness and Change in Proxy Set's IP Addresses

If an Account (configured in the Accounts table) is registered with a registrar server that the device no longer "knows" (e.g., removed from the DNS-resolved IP addresses of the associated Proxy Set) and the Registrar Stickiness feature is enabled, the device immediately initiates a new registration for the Account (with a different server belonging to the Proxy Set).

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.14 Proxy Keep-Alive using Fake Register Requests

Proxy keep-alive can now be done by sending fake REGISTER request messages (Contact header contains a fake name). The mode of operation is identical to the method using OPTIONS messages, but with REGISTER messages. This feature is supported by the new optional value **Using Fake REGISTER** for the 'Proxy Keep-Alive' parameter in the Proxy Sets table.

**Applicable Products:** All.

### 2.17.12.1.15 CLI Display of IP Interfaces per IP Version

The `show network interface description` CLI command, which displays IP Interfaces that were configured in the IP Interfaces table, now provides two new options called `ipv4` and `ipv6` that can be used to filter the output by IPv4 or IPv6 interfaces, respectively.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.16 "Reset" Button in Web Interface Renamed "Restart"

The "Reset" button in the device’s Web interface has been renamed "Restart".

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.17 Change in Rx Payload Type Behavior

The device's behavior for Rx payload type has changed. Up until now, certain media features (e.g., RFC 2833 DTMF, RTP redundancy, and fax bypass) were supported even if not negotiated in SDP, using configured payload types (see related parameters below). From this version, the device only supports media features that are negotiated in SDP and ignores the default / configured payload types.

For example, up until now, if the [RFC2833RxPayloadType] parameter was configured to "100", every packet whose payload type was 100 was processed as RFC 2833 packets. Now, even if the packets' payload type is 100, the device doesn't process the packets as RFC 2833 (unless SDP negotiation results in payload type 100).

To maintain backward compatibility, a new parameter called [BackwardPTBehavior] has been added, which must be enabled (disabled by default).

Affected parameters:

- [FaxBypassPayloadType]
- [ModemBypassPayloadType]
- [RxT38OverRTPPayloadType]
- [RTPNoOpPayloadType]
- [RFC2833RxPayloadType]
- [RFC2198PayloadType]

**Note:**

- For the SBC application, the "T38 over RTP" coder doesn't support transcoding (only forwarding).
- This feature affects only Rx behavior (Tx behavior remains without change).

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.18 Core Dump Configuration through CLI

The Core Dump feature can now also be configured through CLI:

- To configure the server address to where the Core Dump file is sent [CoreDumpDestIP]:
  ```
  configure troubleshoot > debug-file > core-dump-dest-ip
  ```
- To enable Core Dump file generation [EnableCoreDump]:
  ```
  configure troubleshoot > debug-file > enable-core-dump
  ```
- To include the Core Dump file with the Debug file:
  ```
  configure troubleshoot > debug-file > debug-file-mask
  ```

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.12.1.19 HTTP Host Header Validation for Web Access

The device can now be configured to validate the Host header of incoming HTTP requests for accessing the Web interface. When enabled, the device checks that the value of the Host header matches the device's OAMP IP address (or hostname, if configured). If there is no match, the device rejects the request with an HTTP 403 Forbidden response (redirected to a "403 Forbidden" page).

To support this feature, a new parameter called [HostHeaderProtection] has been added.

Enabling this feature (disabled by default) means that only direct access to the Web interface is allowed (i.e., access through a proxy or tunnel is blocked). This feature may also help to prevent malicious attacks on the device using Host header manipulation (injection).

**Applicable Application:** All.

**Applicable Products:** All.

##### 2.17.12.1.20 Capacity for Mediant VE/CE Deployed on Google Cloud Platform

Capacity for Mediant VE and Mediant CE SBCs deployed on Google Cloud Platform (GCP) has been added to the capacity table (see Table 3-1).

**Applicable Application:** SBC.

**Applicable Products:** Mediant VE; Mediant CE.

##### 2.17.12.1.21 Encryption of SIP Header Value

For enhanced security, the device can now encrypt the value of a SIP header. This feature is typically used between two deployed AudioCodes devices, where the device that sends the SIP message encrypts the header's value while the device receiving the SIP message decrypts it. Note that this feature is intended for SIP headers (e.g., proprietary headers) that are not used in the device's classification and routing logic.

To support this feature:

- A new parameter called 'AES-256 Encryption Key' has been added, which configures the AES-256 encryption key. Both devices must be configured with the same key.
- The specific SIP header to encrypt (and decrypt) is configured in the existing Message Manipulations table, using the new syntax option "Func.Encrypt" (and "Func.Decrypt") in the 'Action Value' parameter, for example:

```
Func.Encrypt(Header.P-Access-Network-Info)
```

**Applicable Application:** All.

**Applicable Products:** All.

##### 2.17.12.1.22 Multiple Sockets per HTTP Host

The device can now be configured to open multiple sockets per remote HTTP host. This is configured in the existing Remote Web Services table, using a new parameter called 'Number of Connections'.

Multiple sockets allow the device to send HTTP messages (e.g., POST) in parallel without waiting for a response from the host per sent message. Up until now, only a single socket was opened with the host.

**Applicable Application:** All.

**Applicable Products:** All.

##### 2.17.12.1.23 Support for Standard SNMP MIB ipNetToMediaTable

The device now supports the standard MIB (MIB-2) ipNetToMediaTable (OID 1.3.6.1.2.1.4.22), which maps IPv4 addresses to physical addresses (IP Address Translation table).

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.12.1.24 SIP Transactions Rate for Performance Monitoring

The device's Performance Monitoring feature now also provides SIP transaction rate statistics for Gateway calls. This includes current, average, and maximum SIP transactions per second.

Only SIP requests are considered in the SIP transaction count. For example, a single SIP transaction is from the initial SIP INVITE request to the final SIP 200 OK response.

This feature also adds SIP transaction statistics to the Web interface's Monitor page (GW tab > "Transactions per Sec.").

**Applicable Application:** Gateway.

**Applicable Products:** Gateway.

#### 2.17.12.1.25 Loss of Frame (LOF) Renaming for Performance Monitoring

The following Loss of Frame (LOF) Performance Monitoring parameters have been renamed:

- lofSecondsCurrent has been renamed lofEventsCurrent
- lofSeconds has been renamed lofEvents

**Applicable Application:** Gateway.

**Applicable Products:** Gateway.

### 2.17.12.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-31: Resolved Constraints in Version 7.40A.300.012**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-35891 | The device is impacted by CVE-2004-0230 (TCP Sequence Number Approximation Based Denial of Service). | Vulnerability | Low | Mediant 4000<br>Mediant 2600<br>Mediant 1000<br>Mediant 800<br>Mediant 500<br>MP-1288 | n/a |
| SBC-37695 | The device doesn't support certificate formats with multiple X509.3 Subject Alternative Name headers. | Certificate format | Medium | All | n/a |
| SBC-38603 | The device has TLS connections de-allocation wrong calculation, causing a memory leak Task SPLB | TLS resources leak | Medium | All | n/a |
| SBC-39057 | The device has DNS cache de-allocation wrong calculation, causing a memory leak Task SPMR | DNS resources leak | Medium | All | ha |

### 2.17.12.3 Known Constraints

This section lists known constraints.

**Table 2-32: Known Constraints in Version 7.40A.300.012**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| - | When the device is configured to use an IPv6 OAMP interface, the following functionality is not supported: | ▪ Connectivity with ARM isn't supported, as a result, the device can't use ARM.<br>▪ OVOC-managed session licenses aren't supported, as a result Fixed, Floating, and Flex licensing models are not supported.<br>▪ Connectivity to OVOC using WebSocket is isn't supported, resulting with no connection with OVOC over WebSocket.<br>▪ SNMP Trusted Managers isn't supported, as a result Trusted SNMP Managers can't be configured. | Medium | All | All |
| | | Mediant CE doesn't support an IPv6 OAMP interface, and the device cannot be managed through an IPv6 OAMP. | Medium | Mediant CE<br>Mediant VE | All |
| | | Media Transcoding Cluster (MTC) is not supported. | Medium | Mediant VE<br>Mediant 9000 | MTC |
| | | AWS PAYG (Pay-As-You-Go) deployments are not supported | Medium | Mediant VE | AWS |
| SBC-39368 | When the 'Interface Mode' parameter of an IP Interface in the IP Interfaces table is configured to **IPv6 Stateless** (i.e., autoconfiguration of IPv6 interfaces), obtaining DNS server addresses via DHCP doesn't function. | DNS servers not obtained via Stateless IPv6 (device can use the overwrite DNS servers option which configures them manually; otherwise the | Low | All | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | | default DNS at 8.8.8.8 is used). | | | |
| SBC-39368 | When the following are both configured, the device uses both for DNS servers:<br>▪ The 'Interface Mode' parameter of an IP Interface in the IP Interfaces table is configured for autoconfiguration of IPv6 interfaces (i.e., **IPv6 Stateless** or **IPv6 DHCP**) and used to obtain DNS addresses through DHCP.<br>▪ The dedicated parameters for the HTTP Proxy feature ('Primary DNS Server IP' and Secondary DNS Server IP') are configured. | A DNS server can't be specified for use. (The latest DNS-resolution response is used.) | Low | Mediant 500<br>Mediant 500L<br>Mediant 800<br>Mediant 1000<br>Mediant 2600<br>Mediant 4000<br>Mediant 3100<br>MP-1288 | n/a |
| SBC-38419 | When using IPv6, the SNMP trap destination is not removed on the device after it's deleted on OVOC. | Need to delete the SNMP trap destination through the device's Web or CLI. | Low | All | n/a |
| SBC-39506 | Performance degradation of the device is experienced. | Performance degradation with 1+x cores. | Medium | Mediant Software with 2 vCPU on KVM | KVM |
| SBC-38487 | Downloading files from OVOC to the device through SNMP is not supported when OVOC is configured with a hostname. | Files can't be downloaded to the device. | Medium | All | n/a |
| SBC-39265 | The device doesn't recognize the USB after removing it and then re-inserting it. | A device reset is required. | Low | Mediant 3100 | n/a |
| SBC-39112 | In some configuration tables (e.g., SIP Interfaces or IP Profiles), the name of the row entity can't be "Any". | Configuration entities can't be named "Any". | Low | All | n/a |
| SBC-40511 | For WebRTC-to-WebRTC calls (using G.711 forwarding with RTP header extension), some noise is experienced at the beginning of the call. | WebRTC-to-WebRTC calls voice issues | Medium | Mediant Software | n/a |
| SBC-41214 | For Hitless Upgrade from Version 7.4.300 or later to a version earlier than 7.4.300, the Web interface's Software Upgrade Wizard displays only the "stage 1/3" window and not | Web display issue. | Low | HA | n/a |

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| | the next "2/3 and "3/3" stage windows (even though the upgrade succeeds). | | | | |
| SBC-41265 | If the device is upgraded to Version 7.4.300 and the IP Interfaces table had a row whose DNS was not configured (empty; not even 0.0.0.0), the device deletes all the rows in the IP Interfaces table. | Connectivity to the device may be lost (if the OAMP network interface is deleted) | High | All | n/a |

## 2.17.13 Version 7.40A.260.313

This version includes resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**
  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.3180 or later, and 8.2.280 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to Version 8.0.3137 or later, prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.3137 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.3.2 or later. It's recommended to use Version 2.5.8 or later.

### 2.17.13.1 Resolved Constraints

This section lists resolved constraints.

**Table 2-33: Resolved Constraints in Version 7.40A.260.313**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-43148 | The SBC uses the incorrect Media Realm (associated with incorrect IP Interface index) on a single IP Voice-AI call (no background tone) where Media Realm on SIP side uses an IP Interface X and Voice.AI Connector table is configured with IP Interface Y. | No voice | Medium | All | AWS |
| SBC-43672 | The device's soft-DSP causes transcoding calls to have corrupted voice on WebRTC-to-VoiceAI Connect calls. | Corrupted voice. | Medium | All | n/a |
| SBC-44519 | For the sound moods feature, background music is played only for a few seconds. | Play of background music feature doesn't fully function | Medium | All | n/a |

### 2.17.14 Version 7.40A.260.152

This version includes new features and resolved constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.3180 or later, and 8.2.280 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to Version 8.0.3137 or later, prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.3137 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.3.2 or later. It's recommended to use Version 2.5.8 or later.

### 2.17.14.1 New Features

This section describes the new features introduced in this version.

#### 2.17.14.1.1 Increase in Maximum DNS-resolved IP Addresses for All Proxy Sets

The maximum number of supported DNS-resolved IP addresses for all Proxy Sets (combined) has been increased. For updated values, see the Proxy Sets table capacity in Section 'Configuration Table Capacity'.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.14.1.2 Capacity Increase for IP Profiles and Accounts Tables

The maximum number of rows that can be configured in the IP Profiles table and the Accounts table has been increased to 5,000.

**Note:** This capacity is applicable only when the device's License Key includes the VoiceAI Connect feature key.

**Applicable Application:** All.

**Applicable Products:** Mediant 9000; Mediant Software (64 GB).

#### 2.17.14.1.3 Destination IP Group in Call Setup Rules

Destination IP Groups can now be included in Call Setup Rules. This is only supported when the CSR is assigned to an IP-to-IP Routing rule (in the IP-to-IP Routing table).

Up until now, it was only possible to access information from the source IP Group. Now, it's also possible to access information from the determined destination IP Group. For example, a CSR can be used to set a specific SIP header to the value of a destination IP Group's tag value.

This can be configured using the syntax *param.ipg.dst* in the 'Action Value' or 'Condition' fields of the Call Setup Rules table.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.14.1.4 SDR Generation upon Call Connect for REST

The device can now generate Session Detail Reports (SDRs) upon call connect when sending SDRs to a REST server (over REST API). These SDRs are referred to as *START* SDRs and are generated as the call is connected.

To support this feature, the following new optional values have been added to the existing parameter 'REST SDR Record Type':

- **ATTEMPT, START and STOP**
- **ATTEMPT, START INTERMEDIATE and STOP**

**Applicable Application:** SBC.

**Applicable Products:** Mediant 9000; Mediant Software.

#### 2.17.14.1.5 New SDR Fields Indicating Device or Call Party Released Call

SDRs can now be customized to include two new optional fields—'Ingress Released From IP' and 'Egress Released From IP'. These fields indicate if the call was terminated by the device (i.e., internal reason, for example, "registered user not found") or by one of the call parties.

**Applicable Application:** SBC.

**Applicable Products:** Mediant 9000; Mediant Software.

### 2.17.14.2 Resolved Constraints

This section lists resolved constraints.

**Table 2-34: Resolved Constraints in Version 7.40A.260.152**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-40121 | After performing a specific network configuration change, Mediant CE may lose network connectivity. | After removing a secondary IP address from a network interface, Mediant CE deployed in AWS loses a network configuration entry and needs to be manually reconfigured. | Medium | Mediant CE | AWS |

## 2.17.15 Version 7.40A.260.007

This version includes new features and known constraints only.

**IMPORTANT NOTICE for MEDIANT 90xx/VE/CE/SE SBCs**

Starting with Version 7.40A.250.001,.cmp files are digitally signed. Prior to upgrading the device, please refer to the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

**Note:** Upgrading from Version 7.2 to a 7.4 version for all devices (hardware and software based):

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 7.20A.259.*
  - √ 7.20A.258.*
  - √ 7.20A.256.*
  - √ 7.20A.204.878
  - √ 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx and Mediant VE/CE/SE SBCs:**

  Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

**Note:**

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.3137 or later.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to the compatible OVOC version (above) prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to the compatible OVOC version (above) prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

  When using the Floating or Flex license pool for WebRTC and SIPREC sessions, OVOC version 8.0.3000 or later is required.

**Note:** This SBC version is compatible with Stack Manager Version 2.3.2 or later. It's recommended to use Version 2.5.8 or later.

### 2.17.15.1 New Features

This section describes the new features introduced in this version.

#### 2.17.15.1.1 Dedicated TCP Connection per User in SBC User Information Table

The device can now be configured to use a dedicated TCP/TLS connection per user listed in the SBC User Information table, with a SIP registrar server (Proxy Set). The dedicated connection is established when the device initially registers (SIP REGISTER) the user with the server. All SIP dialogs (e.g., INVITE) originating from the user are sent to the server over this dedicated connection.

Typically, this feature is not required. It should **only** be used if the registrar server (or firewall) blocks the connection upon SIP authentication failures / SIP transaction failures, wrongly assuming, for example, it's a DOS attack (i.e., receives many SIP messages from the same address).

This feature is enabled by the new IP Groups table parameter 'Dedicated Connection Mode'.

**Note:** When this feature is enabled, the maximum number of supported TLS connections is limited (see Configuration Table Capacity).

**Applicable Application:** SBC.

**Applicable Products:** All.

### 2.17.15.1.2 Local UDP Port Spacing of 2 for Media Channels

The device can now allocate its local UDP ports for RTP/T.38 (use same ports) and RTCP traffic per media channel (leg) in increments (spacing) of 2.

For example, if the UDP port range starts at 6000 and the port spacing is 2, the available ports are 6000 (port 6000 for RTP/T.38 and port 6001 for RTCP), 6002 (port 6002 for RTP/T.38 and port 6003 for RTCP), 6004 (port 6004 for RTP/T.38 and port 6005 for RTCP), and so on.

This feature is supported by configuring the existing [UdpPortSpacing] ini file parameter to the new optional value of "2".

**Note:** For UDP port spacing of 2, you must configure the device to use the same port for RTP and T.38, by configuring the ini file parameter [T38UseRTPPort] to 1.

**Applicable Application:** All.

**Applicable Products:** Mediant 500; Mediant 500L; Mediant 800; Mediant 3100; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

### 2.17.15.1.3 Improved Configuration for AWS and Azure Environments

This enhancement is applicable for Mediant VE and CE SBCs that are deployed in AWS and Azure public cloud environments.

Cloud Manager task for the AWS environment has been available since Version 7.2. However, it has been completely redesigned in this 7.40A.260 version. The new implementation is more robust, fully compatible with IMDSv2, provides improved handling for intermittent failures of AWS EC2 and metadata APIs, and generates clear alarms in case of any problem.

Cloud Manager task support for Azure environments has been added to Version 7.40A.260.

Cloud Manager task is responsible for updating SBC network configuration tables -- IP Interfaces table (InterfaceTable) and Ethernet Devices (DeviceTable) -- with network parameters of the specific virtual machine provisioned by the public cloud. For example, if you attach a new network interface to the virtual machine or add an additional secondary IP address to the existing network interface, Cloud Manager task discovers these changes and updates the InterfaceTable accordingly.

Cloud Manager task utilizes instance metadata service (available at http://169.254.169.254) to read current virtual machine configuration. It runs periodically and may take up to a minute to discover and apply the changes.

In an AWS environment, the SBC's network configuration tables are read-only and can only be provisioned by Cloud Manager task.

In an Azure environment, the SBC's network configuration tables are read-write and therefore, it's possible to configure and apply some changes manually, for example, DNS servers. However, most parameters in the InterfaceTable are configured by Cloud Manager task ('Name', 'Mode', 'IP Address', 'Prefix Length' and 'Gateway') and therefore, should NOT be configured manually.

Cloud Manager logs can be obtained using the following CLI commands:

- `tail cloud-manager-log <num of lines>`
- `show cloud-manager-log`

The logs are also included in the Debug file, which can be downloaded through the Web interface (Troubleshooting > Debug > Debug Files).

**Applicable Application:** SBC.

**Applicable Products:** Mediant CE/VE.

#### 2.17.15.1.4 Improved Traffic Flow using Custom EC2 Endpoint for Mediant VE and CE AWS Environments

High-Availability (HA) deployments of Mediant VE and CE SBCs in AWS environments use AWS EC2 API to implement IP failover. Prior to Version 7.40A.260, the SBC software automatically generated the AWS EC2 API endpoint based on the region in which it was deployed (e.g., ec2.eu-central-1.amazonaws.com). However, if two SBC instances were deployed in separate availability zones within the same region, the same AWS EC2 API endpoint was used for both availability zones. This resulted in all traffic towards AWS EC2 API endpoint to flow through the first availability zone, even for virtual machines deployed in the second availability zone.

Version 7.40A.260 introduces a new configuration parameter that can be used to configure a custom EC2 API Endpoint FQDN and/or IP address:

- Ini file: AwsEc2Endpoint
- CLI: `configure network > network-settings > aws-ec2-endpoint`

The parameter may contain one of the following values:

- Empty (default): The SBC CE automatically generates AWS EC2 API endpoint based on the region in which it is deployed (e.g., ec2.eu-central-1.amazonaws.com)
- Custom EC2 API endpoint FQDN (e.g., vpce-0123456789.ec2.eu-central-1.vpce.amazonaws.com)
- Custom EC2 API endpoint FQDN followed by its IP address (e.g., ec2.eu-central-1.amazonaws.com:10.1.2.3)

**Applicable Application:** SBC.

**Applicable Products:** Mediant CE/VE.

#### 2.17.15.1.5 Weak Password Detection

The device can now be configured to detect and alert if a user in the Local Users table has been configured with a weak password.

A password is considered weak if it is listed in the new Weak Passwords List table (Setup > Administration > Web & CLI > Weak Passwords List). This table can be configured with up to 150 weak passwords and provides 6 passwords by default.

This feature is enabled by the new 'Check Weak Passwords' parameter.

If the device detects a weak password, it raises the new SNMP alarm acWeakPasswordAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.156).

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.15.1.6 SBC User Information Capacity Increase

The maximum number of supported far-end users that can be registered with the device has been increased from 20,000 to 50,000. Users are configured in the existing SBC User Information table.

**Applicable Application:** SBC.

**Applicable Products:** Mediant Software (16-64 GB); Mediant 90xx.

### 2.17.15.1.7 Hitless License Upgrade for WebRTC and SIPREC

The Hitless License Key Upgrade feature for devices in High-Availability (HA) mode now also supports WebRTC and SIPREC licenses. Up until now, hitless license upgrade was only supported for far-end users (FEU), SBC sessions, transcoding sessions, and SBC signaling licenses.

**Applicable Application:** All.

**Applicable Products:** Mediant 500 HA; Mediant 800 HA; Mediant 2600 HA; Mediant 4000 HA; Mediant 90xx HA; Mediant Software HA.

### 2.17.15.1.8 Call Duration Limit when using Device Free Trial Evaluation

Starting from this version, the free trial of the device offered by AudioCodes for evaluation purposes (without installing a License Key), not only restricts the device to three concurrent calls, but now also limits each call to three minutes.

**Note:** Devices connected to licensing models (e.g., Floating License) are not affected by this feature.

**Applicable Application:** SBC.

**Applicable Products:** Mediant Software.

### 2.17.15.1.9 Removal of CSRC Identifiers from RTP Packets

The device can now remove CSRC identifiers from RTP packets without using transcoding capabilities. Removing CSRC may be useful in some scenarios where, for example, the call is sent to a third-party application such as voicemail and the presence of CSRC causes a reduction in voice quality.

This feature is supported by the new IP Profiles table parameter 'Remove CSRC' (removes CSRC from packets sent to the SIP User Agent associated with the IP Profile).

**Applicable Application:** SBC.

**Applicable Products:** All.

### 2.17.15.1.10 Alarm Customization Based on Alarm Source Entity

The existing Alarms Customization table (Setup menu > Administration tab > SNMP folder > Alarm Customization) can now customize alarms based on the specific entity (e.g., IP Group 3, Ethernet port 1, Trunk 5) for which the alarm was raised. The entity appears in the alarm source after the hash (#) sign -- for example, Board#1/IPGroup#**2,** indicating that the alarm was raised for IP Group index 2. This feature may be useful, for example, to suppress specific alarms raised by a specific IP Group.

To support this feature, the new field 'Entity ID' has been added to the Alarms Customization table.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.15.1.11 New CDR Field Indicating if Call Terminated by Device

The device supports a new CDR field called 'Released From IP' (IsReleasedFromIP), which indicates if the call was terminated by the device (i.e., because of an internal reason, for example, register user not found), or by the callee / called parties. The field is not included by default in the CDR, but it can be included by customizing the CDR using the SBC CDR Format table.

**Applicable Application:** SBC.

**Applicable Products:** All.

### 2.17.15.1.12 New SDR Field for Call Type

A new SDR field has been added called 'Call Type', which indicates the type of call (e.g., SIP-WebRTC call or SIP-bot call).

**Applicable Application:** SBC.

**Applicable Products:** Mediant Software; Mediant 90xx.

### 2.17.15.1.13 Tail CLI Command for Displaying Last Lines in Show Output

The CLI output of various log commands can now be configured to show the last lines (tail end) of the log output, using the new `tail` command. In addition, the number of lines to show can optionally be specified (if not, the last 100 lines are shown). This is especially useful for long outputs where the user needs to scroll all the way down to view the last lines.

The `tail` command can be used with the following commands:

- `tail cloud-init-log [<lines>]`: Shows cloud-init logs (Mediant Software SBC only)
- `tail aws-manager-log [<lines>]`: Shows aws-manager logs (Mediant Software SBC on AWS only)
- `tail system log [<lines>]`: Shows system logs
- `tail system log no-sip [<lines>]`: Shows system logs without SIP messages
- `tail system log persistent [<lines>]`: Shows persistent system logs

The tail command is available in privilege mode only (i.e., `> enable`).

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.15.1.14 SBC Configuration Wizard Templates for Orange and Alcatel-Lucent

The SBC Wizard provides new interoperability templates for Orange (OBS Business Talk & BTIP) and Alcatel-Lucent.

**Applicable Application:** SBC.

**Applicable Products:** All.

#### 2.17.15.1.15 Mediant 3100 Power Type Status on Web Monitor Page Update

On the Web interface's Monitor page, the 'Power Type' read-only field for the Power Supply module now displays "n/a" if no module is installed, or if a new module is installed but not yet connected to power (DC or AC).

**Applicable Application:** All.

**Applicable Products:** Mediant 3100.

#### 2.17.15.1.16 Update to Proxy Hot Swap Mode

For the existing Proxy Sets table parameter 'Proxy Hot Swap Mode' (ProxySet_IsProxyHotSwap), the textual description of value "0" was changed from **Disable** to **Enable Only Before Alternative Routing**, which now more accurately describes the device’s behavior. Customers who want the hot-swap mode fully disabled, should choose the new value **Disable** (2).

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.17.15.1.17 Gateway-Type IP Group Status Updated

The read-only fields 'GW Group Registered IP Address' and 'GW Group Registered Status' in the IP Groups table now display "NA" when the IP Group is a **User**-type or **Server**-type. These fields are applicable only to Gateway-type IP Groups.

**Applicable Application:** All.

**Applicable Products:** All.

### 2.17.15.2 Known Constraints

This section lists known constraints.

**Table 2-35: Known Constraints in Version 7.40A.260.007**

| Incident | Description | Impact | Severity | Affected Products | Affected Environments |
|---|---|---|---|---|---|
| SBC-42301 | Configuring a name (‘Name’ field) in the Ethernet Devices table and IP Interfaces table instead of using the default name causes a networking issue (and device freezes upon restarts). | Loss of device's network information on Azure | Major | Mediant VE / CE | Azure |

# 3 Session Capacity

This section provides capacity figures.

## 3.1 SIP Signaling and Media Capacity

The following table lists the maximum, concurrent SIP signaling sessions, concurrent media sessions, and registered users per product.

**Table 3-1: SIP Signaling and Media Capacity per Product**

| Product | | Signaling Capacity | | Media Sessions | | | |
|---|---|---|---|---|---|---|---|
| | | SIP Sessions | Registered Users | Session Type | RTP | SRTP | Detailed Media Capabilities |
| Mediant 500 | | 250 | 1,500 | Hybrid | 250 | 200 | Transcoding: n/a<br>GW: Table 3-4 |
| | | | | GW-Only | 30 | 30 | |
| Mediant 500L | | 60 | 200 | Hybrid | 60 | 60 | Transcoding: n/a<br>GW: Table 3-6 |
| | | | | GW-Only | 8 | 8 | |
| Mediant 800B | | 250 | 1,500 | Hybrid | 250 | 250 | GW & Transcoding: Table 3-8<br>SBC Only: Table 3-7 |
| | | | | GW-Only | 64 | 64 | |
| Mediant 800C | | 400 | 2,000 | Hybrid | 400 | 250 | GW & Transcoding: Table 3-10 |
| | | | | GW-Only | 124 | 124 | |
| Mediant 1000B | | 150 | 600 | Hybrid | 150 | 120 | Transcoding: Table 3-14<br>GW: Tables Table 3-11, Table 3-12, Table 3-13 |
| | | | | GW-Only | 192 | 140 | |
| Mediant 3100 | | 5,000 | 20,000 | Hybrid | 5,000 | 5,000 | Transcoding: Table 3-16<br>GW: Table 3-15 |
| | | 960 | 20,000 | GW-Only | 960 | 960 | Table 3-15 |
| MP-1288 | | 588 | 350 | Hybrid | 588 | 438 | Transcoding: n/a<br>GW: Table 3-17 |
| | | | | SBC-Only | 300 | 300 | |
| | | | | GW-Only | 288 | 288 | |
| Mediant 2600 | | 600 | 8,000 | SBC-Only | 600 | 600 | Transcoding: Table 3-18 |
| Mediant 4000 | | 5,000 | 20,000 | SBC-Only | 5,000 | 3,000 | Transcoding: Table 3-19 |
| Mediant 4000B | | 5,000 | 20,000 | SBC-Only | 5,000 | 5,000 | Transcoding: Table 3-21 |
| Mediant 9000 | SIP Performance Profile (HT Enabled) | 30,000 | 300,000 | SBC-Only | 30,000 | 16,000 | Transcoding: n/a |
| | | 55,000 | 0 | SBC-Only | 55,000 | 18,000 | Transcoding: n/a |
| | DSP Performance Profile (HT Enabled) | 50,000 | 0 | SBC-Only | 50,000 | 18,000 | Transcoding: Table 3-23 |
| | SRTP Performance Profile (HT Enabled) | 50,000 | 0 | SBC-Only | 50,000 | 40,000 | Transcoding: n/a |
| Mediant 9000 Rev. B | SIP Performance Profile | 50,000 | 500,000 | SBC-Only | 50,000 | 30,000 | Transcoding: n/a |
| | | 70,000 | 0 | SBC-Only | 70,000 | 30,000 | Transcoding: n/a |
| | DSP Performance Profile | 50,000 | 0 | SBC-Only | 50,000 | 28,000 | Transcoding: Table 3-25 |
| | SRTP Performance Profile | 70,000 | 0 | SBC-Only | 70,000 | 40,000 | Transcoding: n/a |

| Product | | | Signaling Capacity | | Media Sessions | | | |
|---|---|---|---|---|---|---|---|---|
| | | | SIP Sessions | Registered Users | Session Type | RTP | SRTP | Detailed Media Capabilities |
| Mediant 9030 | SIP Performance Profile | | 30,000 | 200,000 | SBC-Only | 30,000 | 30,000 | Transcoding: n/a |
| | DSP Performance Profile | | 30,000 | 200,000 | SBC-Only | 30,000 | 15,000 | Transcoding: Table 3-28 |
| Mediant 9080 | SIP Performance Profile | | 50,000 | 500,000 | SBC-Only | 50,000 | 30,000 | Transcoding: n/a |
| | | | 70,000 | 0 | SBC-Only | 70,000 | 30,000 | Transcoding: n/a |
| | DSP Performance Profile | | 50,000 | 0 | SBC-Only | 50,000 | 28,000 | Transcoding: Table 3-25 |
| | SRTP Performance Profile | | 70,000 | 0 | SBC-Only | 70,000 | 40,000 | Transcoding: n/a |
| Mediant 9000 with Media Transcoders (MT-type) | | | 24,000 | 180,000 | SBC-Only | 24,000 | 16,000 | Transcoding: Table 3-27 |
| Mediant 9000 Rev. B with Media Transcoders (MT-type) | | | 60,000 | 200,000 | SBC-Only | 60,000 | 40,000 | Transcoding: Table 3-27 |
| Mediant 9080 with Media Transcoders (MT-type) | | | 60,000 | 200,000 | SBC-Only | 60,000 | 40,000 | Transcoding: Table 3-27 |
| Mediant CE | AWS / EC2 | | 50,000 | 100,000 | SBC-Only | 50,000 | 50,000 | Forwarding: Table 3-30<br>Transcoding: Table 3-31 |
| | Azure | | 50,000 | 100,000 | SBC-Only | 50,000 | 50,000 | Forwarding: Table 3-32<br>Transcoding: Table 3-33 |
| | VMware | | 12,000 | 100,000 | SBC-Only | 12,000 | 12,000 | Forwarding: Table 3-34<br>Transcoding: Table 3-35 |
| | GCP | | 50,000 | 100,000 | SBC-Only | 50,000 | 40,000 | Forwarding: Table 3-36<br>Transcoding: Table 3-38 |
| Mediant VE | VMware | 1 vCPU<br>2-GB RAM (HT) | 250 | 1,000 | SBC-Only | 250 | 250 | Transcoding: n/a |
| | | 1 vCPU<br>8-GB RAM (HT) | 4000 | 15,000 | SBC-Only | 4,000 | 2,600 | Transcoding: n/a |
| | | 4 vCPU<br>16-GB RAM (HT) | 10,000 | 75,000 | SBC-Only | 10,000 | 8,000 | Transcoding: n/a |
| | | 2 vCPUs<br>8-GB RAM (HT) | 4,000 | 15,000 | SBC-Only | 2,200 | 1,900 | Transcoding: Table 3-39 |
| | | 4 vCPU<br>8-GB RAM (HT) | 4,000 | 15,000 | SBC-Only | 1,800 | 1,600 | Transcoding: Table 3-39 |
| | | 8 vCPU<br>16-GB RAM (HT) | 9,000 | 75,000 | SBC-Only | 6,000 | 5,000 | Transcoding: Table 3-39 |
| | | 16 vCPU<br>16-GB RAM (HT) | 9,000 | 75,000 | SBC-Only | 6,500 | 5,000 | Transcoding: Table 3-39 |
| | KVM / OpenStack | 1 vCPU<br>2-GB RAM (HT) | 250 | 1,000 | SBC-Only | 250 | 250 | Transcoding: n/a |
| | | 1 vCPU<br>8-GB RAM (HT) | 2,500 | 15,000 | SBC-Only | 2,500 | 1,700 | Transcoding: n/a |
| | | 4 vCPU<br>16-GB RAM (HT) | 4,500 | 75,000 | SBC-Only | 4,500 | 3,500 | Transcoding: n/a |
| | | 2 vCPUs<br>8-GB RAM (HT) | 1,900 | 15,000 | SBC-Only | 1,900 | 1,400 | Transcoding: Table 3-39 |
| | | 8 vCPU<br>16-GB RAM (HT) | 5,800 | 75,000 | SBC-Only | 5,800 | 4,800 | Transcoding: Table 3-39 |
| | | 16 vCPU<br>16-GB RAM (HT) | 3,800 | 75,000 | SBC-Only | 3,800 | 2,800 | Transcoding: Table 3-39 |

| Product | | | Signaling Capacity | | Media Sessions | | | |
|---|---|---|---|---|---|---|---|---|
| | | | SIP Sessions | Registered Users | Session Type | RTP | SRTP | Detailed Media Capabilities |
| | | 8 vCPU<br>32-GB RAM<br>SR-IOV Intel NICs<br>(non-HT) | 24,000 | 75,000 | SBC-Only | 24,000 | 10,000 | Transcoding: n/a |
| | Hyper-V | 1 vCPU<br>2-GB RAM (HT) | 250 | 1,000 | SBC-Only | 250 | 250 | Transcoding: n/a |
| | | 1 vCPU<br>8-GB RAM (HT) | 1,500 | 15,000 | SBC-Only | 1,500 | 1,200 | Transcoding: n/a |
| | | 4 vCPU<br>8-GB RAM (HT) | 2,500 | 15,000 | SBC-Only | 2,500 | 2,300 | Transcoding: n/a |
| | | 2 vCPUs<br>8-GB RAM (HT) | 1,900 | 15,000 | SBC-Only | 1,900 | 1,400 | Transcoding: Table 3-39 |
| | | 8 vCPU<br>16-GB RAM (HT) | 2,500 | 75,000 | SBC-Only | 2,500 | 2,300 | Transcoding: Table 3-39 |
| | AWS / EC2 | m5n.large | 3,200 | 30,000 | SBC-Only | 3,200 | 3,200 | Transcoding: n/a |
| | | | 2,500 | 20,000 | SBC-Only | 2,500 | 1,500 | Transcoding: Table 3-40 |
| | | c5n.2xlarge | 5,500 | 75,000 | SBC-Only | 5,500 | 5,000 | Transcoding: n/a |
| | | | 4,500 | 75,000 | SBC-Only | 4,500 | 2,400 | Transcoding: Table 3-41 |
| | | c5n.9xlarge | 7,000 | 75,000 | SBC-Only | 7,000 | 6,000 | Transcoding: n/a |
| | | | 7,000 | 75,000 | SBC-Only | 7,000 | 4,500 | Transcoding: Table 3-42 |
| | Azure | DS1_v2 | 600 | 1,000 | SBC-Only | 600 | 500 | Transcoding: n/a |
| | | | 300 | 1,000 | SBC-Only | 300 | 300 | Transcoding: Table 3-44 |
| | | D2ds_v5 | 3,200 | 15,000 | SBC-Only | 3,200 | 2,700 | Transcoding: n/a |
| | | | 2,500 | 15,000 | SBC-Only | 2,500 | 1,600 | Transcoding: Table 3-44 |
| | | D4ds_v5 | 7,000 | 50,000 | SBC-Only | 7,000 | 6,000 | Transcoding: n/a |
| | | | 4,800 | 50,000 | SBC-Only | 4,800 | 3,200 | Transcoding: Table 3-44 |
| | | D8ds_v5 | 12,000 | 75,000 | SBC-Only | 12,000 | 9,000 | Transcoding: n/a |
| | | | 4,600 | 75,000 | SBC-Only | 4,600 | 3,000 | Transcoding: Table 3-44 |
| | GCP | n2-standard-2 | 3,500 | 15,000 | SBC-Only | 3,500 | 2,400 | Transcoding: n/a |
| | | | 1,500 | 15,000 | SBC-Only | 1,500 | 1,100 | Transcoding: Table 3-45 |
| | | n2-standard-4 | 4,000 | 75,000 | SBC-Only | 4,000 | 3,000 | Transcoding: n/a |
| | | | 2,400 | 75,000 | SBC-Only | 2,400 | 1,800 | Transcoding: Table 3-45 |
| | | n2-standard-8 | 2,400 | 75,000 | SBC-Only | 2,400 | 1,800 | Transcoding: Table 3-45 |
| | | n2-highcpu-32 | 3,600 | 75,000 | SBC-Only | 3,600 | 3,400 | Transcoding: Table 3-45 |
| Mediant SE | DL360p Gen8 or DL360 Gen9 | | 24,000 | 120,000 | SBC-Only | 16,000 | 14,000 | Transcoding: n/a |
| | | | 24,000 | 0 | SBC-Only | 24,000 | 14,000 | Transcoding: n/a |
| | DL360 Gen10 | SIP Performance Profile | 50,000 | 500,000 | SBC-Only | 50,000 | 30,000 | Transcoding: n/a |
| | | | 70,000 | 0 | SBC-Only | 70,000 | 30,000 | Transcoding: n/a |
| | | DSP Performance Profile | 50,000 | 0 | SBC-Only | 50,000 | 28,000 | Transcoding: Table 3-46 |
| | | SRTP Performance Profile | 70,000 | 0 | SBC-Only | 70,000 | 40,000 | Transcoding: n/a |

**Note:**

- The listed capacities are accurate at the time of publication of this document. However, they may change due to a later software update. For the latest capacities, please contact your AudioCodes sales representative.
- ***GW*** refers to Gateway functionality.
- ***SIP Sessions*** refers to the maximum concurrent signaling sessions for both SBC and Gateway (when applicable). Whenever signaling sessions is greater than the maximum media sessions, the remaining signaling sessions can be used for Direct Media.
- ***Session Type*** refers to Gateway-only sessions, SBC-only sessions, or Hybrid sessions which is any mixture of SBC and Gateway sessions under the limitations of Gateway-only or SBC-only maximum values.
- ***RTP Sessions*** refers to the maximum concurrent RTP sessions when all sessions are RTP-RTP (SBC sessions) or TDM-RTP (Gateway sessions).
- ***SRTP Sessions*** refers to the maximum concurrent SRTP sessions when all sessions are RTP-SRTP (for SBC sessions) or TDM-SRTP (for Gateway sessions).
- ***Registered Users*** refers to the maximum number of users that can be registered with the device. This applies to the supported application (SBC or CRP).
- Regarding signaling, media, and transcoding session resources:
  - √ A signaling session is a SIP dialog session between two SIP entities, traversing the device and using one signaling session resource.
  - √ A media session is an audio (RTP or SRTP), fax (T.38), or video session between two SIP entities, traversing the device and using one media session resource.
  - √ A gateway session (TDM-RTP or TDM-SRTP) is considered as a media session for the calculation of media sessions. In other words, the maximum media sessions shown in the table refer to the sum of Gateway and SBC sessions.
  - √ For direct media (i.e., anti-tromboning or non-media anchoring) where only SIP signaling traverses the device and media flows directly between the SIP entities, only a signaling session resource is used. Thus, for products with a greater signaling session capacity than media, even when media session resources have been exhausted, additional signaling sessions can still be handled for direct-media calls.
  - √ For call sessions requiring transcoding, one transcoding session resource is also used. For example, for a non-direct media call in which one leg uses G.711 and the other G.729, one signaling, one media, and one transcoding session resources are used.
- Cloud Resilience Package (CRP) application capacity appears under ***Registered Users***.
- Lync Analog Device (LAD) application capacity appears under ***Media Sessions***.

**Note for MP-1288:**

- The maximum number of media and signaling sessions is the sum of the maximum 300 RTP-to-RTP (SBC) sessions and the maximum 288 TDM-RTP (Gateway) sessions.
- The maximum number of SRTP sessions is the sum of the maximum 150 RTP-to-SRTP (SBC) sessions and the maximum 288 TDM-SRTP (Gateway) sessions.

**Note for Mediant 90xx SBC:**

- Mediant 90xx SBC with Media Transcoders limitations:
  - √ To allow DSP capabilities (such as transcoding), the ‘Performance Profile’ parameter must be configured to the DSP profile.
    Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP figure specified in the table. As a result, if all sessions involve transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding specified in the table.
  - √ The maximum number of SRTP-RTP sessions is also affected by the above limitations. For example, if sessions involve transcoding, the maximum number of SRTP-RTP sessions is also limited by half of the maximum SRTP-RTP sessions without transcoding.
- The Media Transcoding Cluster (MTC) feature is supported only on Mediant 9080 SBC.

**Note for Mediant VE SBC:**

- **Mediant VE SBC on VMware:** Capacity was measured with ESXi Version 7.0.3 and a host of CPU Xeon 6226R with Hyper-Threading enabled. For example, a 4-vCPU virtual machine allocates only 2 physical cores. For minimum requirements, see Section 3.3.15.1 on page 210.
- **Mediant VE SBC on KVM:** Capacity for virtual machine instance with SR-IOV was done with Intel 82599 NIC.
- **Mediant VE SBC on Azure:**
  - √ DS_v2 virtual machine series in general and DS1_v2 virtual machine size in particular are scheduled for retirement in May 2028. Therefore, it’s recommended **not** to use them for new deployments, and to migrate existing deployments to the Dds_v5 (D2ds_v5, D4ds_v5, or D8ds_v5) virtual machine series.
  - √ Capacity for virtual machine instances D2ds_v5, D4ds_v5, D8ds_v5 is with Accelerated Networking enabled.
  - √ When operating in HA mode, it's not recommended to exceed 5,000 sessions because of the duration required for processing a failover.
- **Mediant VE SBC on AWS:**
  - √ Network performance on AWS cloud is subject to network conditions, which may depend on time and region.
  - √ Capacity shown in the table are based on lowest capacities found during performance testing.
  - √ It’s recommended to use the m5n and c5n instance types as they provide more stable network characteristics. However, the m5 and c5 instance types are still supported.

**Note for Mediant CE SBC:**

Mediant CE SBC is based on the following instances:

- **AWS:**
  - √ Signaling Components (SC): m5.2xlarge
  - √ Media Components (MC) - forwarding only: m5n.large
  - √ MC - forwarding and transcoding: c5.4xlarge
- **Azure:**
  - √ SC: D4ds_v5 (up to 10,000 sessions and 50,000 users) or D8ds_v5 (up to 50,000 sessions and 100,000 users)
  - √ MC - forwarding only: D2ds_v5, D4ds_v5, and D8ds_v5
  - √ MC - forwarding and transcoding: D2ds_v5, D4ds_v5, and D8ds_v5

  It's not recommended to exceed 5,000 sessions per MC because of the duration required for processing an MC failover.
- **VMware:**
  - √ SC: 8 vCPU (Hyper-Threading), 16-GB RAM
  - √ MC - forwarding only: 2 vCPU (Hyper-Threading), 8-GB RAM
  - √ MC - forwarding and transcoding: 8 vCPU (Hyper-Threading), 8-GB RAM
- **GCP:**
  - √ SC: n2-standard-8 (8 vCPU, 32-GB RAM)
  - √ MC - forwarding only: n2-standard-2 (2 vCPU, 8-GB RAM)
  - √ MC - forwarding and transcoding: n2-standard-2 (2 vCPU, 8-GB RAM), n2_highcpu-8 (8 vCPU, 8-GB RAM)

**Note for Mediant SE SBC:** For new deployments, it's highly recommended to use the DL360 G10 server. For exact specifications and BIOS settings, please contact your AudioCodes sales representative.

## 3.2 Capacity per Feature

The table below lists maximum capacity per feature.

**Table 3-2: Maximum Capacity per Feature**

| Product | Concurrent WebRTC Sessions | | One-Voice Resiliency (OVR) Users | Concurrent SIPREC Sessions | Concurrent TLS Connections | Concurrent MSRP Sessions |
|---|---|---|---|---|---|---|
| | Click-to-Call | Registered Agents | | | | |
| MP-1288 | - | - | - | 150 | 350 | 100 |
| Mediant 500 | - | - | - | 125 | 300 | 100 |
| Mediant 500L | - | - | - | 30 | 100 | 100 |
| Mediant 800B | 100 | 100 | 100 | 200 | 300 | 100 |
| Mediant 800C | 100 | 100 | 150 | 200 | 450 | 100 |
| Mediant 1000B | - | - | 50 | - | 300 | 100 |
| Mediant 3100 | 1,000 | 1,000 | - | 2,500 | 6,000 | 100 |
| Mediant 2600 | 600 | 600 | - | 300 | 2,500 | 100 |
| Mediant 4000/B | 1,000 | 1,000 | - | 2,500 | 2,500 | 100 |
| Mediant 9000 | 5,000 | 16,000 | - | ▪ Hyper-Threading: 20,000<br>▪ No Hyper-Threading: 12,000 | 25,000 | 100 |
| Mediant 9030 | 5,000 | 16,000 | - | 15,000 | 16,000 | 100 |
| Mediant 9080 | 8,000 | 25,000 | - | 20,000 | 25,000 | 100 |
| Mediant SE (see note #1) | 5,000 | 25,000 | - | 12,000 | 25,000 | 100 |
| Mediant VE (see note #2) | 5,000 | 5,000 | 2,000 | 12,000 | ▪ 2 GB: 100<br>▪ 3 GB: 500<br>▪ 4 GB: 5,000<br>▪ 8-16 GB: 6,000<br>▪ 32 GB: 16,000<br>▪ 64 GB: 25,000 | 100 |
| Mediant CE (see note #2) | 5,000 | ▪ SC with 8 vCPUs: 16,000<br>▪ SC with 4 vCPUs: 5,000 | - | 20,000 | ▪ 2 GB: 100<br>▪ 3 GB: 500<br>▪ 4 GB: 5,000<br>▪ 8-16 GB: 6,000<br>▪ 32 GB: 16,000<br>▪ 64 GB: 25,000 | 100 |

**Note:**

- WebRTC sessions:
  - √ The maximum number of concurrent WebRTC sessions can't be more than the maximum number of concurrent SRTP sessions (specified in Table 3-1). Therefore, the actual maximum number of concurrent WebRTC sessions per deployment environment is less than the numbers shown in the table below.
  - √ The maximum number of concurrent WebRTC sessions can't be greater than the maximum number of concurrent TLS connections.
- Capacity assumes that a TLS key size of 2048-bit is used for WebSocket and DTLS negotiations.
- SIPREC capacity assumes that there are no other concurrent, regular (non-SIPREC) voice sessions. SIPREC sessions are counted as part of the SBC session capacity. The maximum number of SIPREC sessions can't be more than the number of RTP sessions, as indicated in Table 3-1. Therefore, the actual maximum number of SIPREC sessions per deployment environment is less than the numbers shown in the table below.
- For TLS capacity, each registered user is assigned a TLS connection even if there are no ongoing SIP dialogs or transactions using the same connection.
- Capacity is when using the approved Mediant SE server specifications with an Intel Xeon Gold 6126 processor. For specifications, please contact AudioCodes.

## 3.3 Detailed Capacity

This section provides detailed capacity figures.

### 3.3.1 Mediant 500 E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500 E-SBC are shown in the tables below.

#### 3.3.1.1 Non-Hybrid (SBC) Capacity

**Table 3-3: Mediant 500 E-SBC (Non-Hybrid) - SBC Capacity**

| H/W Configuration | TDM-RTP Sessions | | | | Max. SBC Sessions (RTP-RTP) |
|---|---|---|---|---|---|
| | DSP Channels Allocated for PSTN | Wideband Coders | | | |
| | | G.722 | AMR-WB (G.722.2) | SILK-WB | |
| SBC | n/a | n/a | n/a | n/a | 250 |

#### 3.3.1.2 Hybrid (with Gateway) Capacity

**Table 3-4: Mediant 500 Hybrid E-SBC (with Gateway) - Media & SBC Capacity**

| H/W Configuration | TDM-RTP Sessions | | | | Max. SBC Sessions (RTP-RTP) |
|---|---|---|---|---|---|
| | DSP Channels Allocated for PSTN | Wideband Coders | | | |
| | | G.722 | AMR-WB (G.722.2) | SILK-WB | |
| 1 x E1/T1 | 30 (full E1) | √ | - | - | 220 |
| | 24 (full T1) | | | | 226 |
| | 26 (partial E1) | √ | √ | - | 224 |
| | 24 (full T1) | √ | √ | - | 226 |
| | 26 (partial E1) | √ | √ | √ | 224 |
| | 24 (full T1) | √ | √ | √ | 226 |

## 3.3.2 Mediant 500L Gateway and E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500L Gateway and E-SBC is shown in the tables below.

### 3.3.2.1 Non-Hybrid (SBC) Capacity

**Table 3-5: Mediant 500L E-SBC (Non-Hybrid) - SBC Capacity**

| H/W Configuration | TDM-RTP Sessions | | | Max. SBC Sessions (RTP-RTP) |
|---|---|---|---|---|
| | DSP Channels Allocated for PSTN | Wideband Coders | | |
| | | G.722 | AMR-WB (G.722.2) | |
| SBC | n/a | n/a | n/a | 60 |

### 3.3.2.2 Hybrid (with Gateway) Capacity

**Table 3-6: Mediant 500L Hybrid E-SBC (with Gateway) - Media & SBC Capacity**

| H/W Configuration | DSP Channels Allocated for PSTN | Additional Coders | | | | Max. SBC Sessions |
|---|---|---|---|---|---|---|
| | | Narrowband | Wideband | | | |
| | | Opus-NB | G.722 | AMR-WB (G.722.2) | Opus-WB | |
| 2 x BRI /<br>4 x BRI | 4/8 | - | - | - | - | 56/52 |
| | 4/8 | - | √ | - | - | 56/52 |
| | 4/6 | √ | - | √ | - | 56/54 |
| | 4 | - | - | - | √ | 56 |

### 3.3.3 Mediant 800 Gateway & E-SBC

This section describes capacity for Mediant 800 Gateway & E-SBC.

#### 3.3.3.1 Mediant 800B Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800B Gateway & E-SBC are shown in the tables below.

##### 3.3.3.1.1 Non-Hybrid (SBC) Capacity

**Table 3-7: Mediant 800B Gateway & E-SBC - SBC Session Capacity per Capabilities (SBC Only)**

| H/W Configuration | DSP Channels for PSTN | SBC Transcoding Sessions | | | | | | | | Max. SBC Sessions |
|---|---|---|---|---|---|---|---|---|---|---|
| | | From Profile 2 with Additional Advanced DSP Capabilities | | | | | | To Profile 1 | To Profile 2 | |
| | | AMR-NB / G.722 | AMR-WB (G.722.2) | SILK-NB / iLBC | SILK-WB | Opus-NB | Opus-WB | | | |
| SBC | n/a | - | - | - | - | - | - | 57 | 48 | 250 |
| | n/a | √ | - | - | - | - | - | 51 | 42 | 250 |
| | n/a | - | - | √ | - | - | - | 39 | 33 | 250 |
| | n/a | - | √ | - | - | - | - | 36 | 30 | 250 |
| | n/a | - | - | - | √ | - | - | 27 | 24 | 250 |
| | n/a | - | - | - | - | √ | - | 27 | 24 | 250 |
| | n/a | - | - | - | - | - | √ | 21 | 21 | 250 |

**Note:** "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).

### 3.3.3.1.2 Hybrid (with Gateway) Capacity

**Table 3-8: Mediant 800B Gateway & E-SBC - Channel Capacity per Capabilities (with Gateway)**

| Telephony Interface Assembly | DSP Channels Allocated for PSTN | SBC Transcoding Sessions | | | | | | | | Conf. Participants | Max. SBC Sessions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | From Profile 2 with Additional Advanced DSP Capabilities | | | | | | To Profile 1 | To Profile 2 | | |
| | | AMR-NB / G.722 | AMR-WB (G.722.2) | SILK-NB | SILK-WB | Opus-NB | Opus-WB | | | | |
| 2 x E1/T1 | 60/48 | - | - | - | - | - | - | 3/15 | 2/13 | - | 190/202 |
| 2 x T1 | 48 | - | - | - | - | - | - | 11 | 9 | - | 202 |
| 1 x E1/T1<br>8 x FXS/FXO | 38/32 | - | - | - | - | - | - | 22/28 | 18/22 | - | 212/218 |
| | 38/32 | - | - | √ | - | - | - | 8/12 | 7/11 | - | 212/218 |
| 1 x E1/T1 | 30/24 | - | - | √ | - | - | - | 14/18 | 12/16 | - | 220/226 |
| 1 x E1<br>4 x BRI | 38 | - | - | - | - | - | - | 22 | 18 | - | 212 |
| 1 x E1<br>4 x FXS | 34 | - | - | - | - | - | - | 26 | 21 | - | 216 |
| 2 x E1<br>4 x FXS | 64 | - | - | - | - | - | - | 0 | 0 | - | 186 |
| 4 x BRI<br>4 x FXS<br>4 x FXO | 16 | - | - | - | - | - | - | 5 | 4 | - | 234 |
| 8 x BRI<br>4 x FXS | 20 | - | - | - | - | - | - | 1 | 1 | - | 230 |
| 8 x BRI | 16 | - | - | - | - | - | - | 5 | 4 | - | 234 |
| 12 x FXS | 12 | - | - | √ | - | - | - | 3 | 3 | - | 238 |
| 4 x FXS<br>8 x FXO | 12 | - | - | √ | - | - | - | 3 | 3 | - | 238 |
| 8 x FXS<br>4 x FXO | 12 | - | - | √ | - | - | - | 3 | 3 | - | 238 |
| 4 x BRI<br>4 x FXS | 12 | - | - | √ | - | - | - | 3 | 3 | - | 238 |
| 4 x FXS<br>4 x FXO | 8 | - | - | - | - | - | - | 7 | 5 | 6 | 242 |
| | 8 | - | - | √ | - | - | - | 6 | 6 | - | 242 |
| 4 x BRI | 8 | - | - | - | - | - | - | 7 | 5 | 6 | 242 |
| | 8 | - | - | √ | - | - | - | 6 | 6 | - | 242 |
| 1/2/3 x BRI | 2/4/6 | - | - | - | - | - | - | 17/15 /14 | 14/13 /11 | - | 248/246/ 244 |

| Telephony Interface Assembly | DSP Channels Allocated for PSTN | SBC Transcoding Sessions | | | | | | | | Conf. Participants | Max. SBC Sessions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | From Profile 2 with Additional Advanced DSP Capabilities | | | | | | To Profile 1 | To Profile 2 | | |
| | | AMR-NB / G.722 | AMR-WB (G.722.2) | SILK-NB | SILK-WB | Opus-NB | Opus-WB | | | | |
| | 2/4/6 | - | - | √ | - | - | - | 11/10/8 | 10/8/7 | - | 248/246/244 |
| 4 x FXS<br>or<br>4 x FXO | 4 | - | - | √ | - | - | - | 10 | 8 | - | 246 |
| | 4 | √ | - | - | - | - | - | 12 | 10 | 4 | 246 |
| | 4 | - | - | √ | - | - | - | 6 | 6 | 4 | 246 |
| | 4 | - | √ | √ | - | - | - | 4 | 4 | 4 | 246 |
| | 4 | - | √ | √ | √ | - | - | 3 | 3 | 4 | 246 |
| | 4 | - | - | - | - | √ | - | 1 | 0 | 4 | 246 |
| | 4 | - | - | - | - | - | √ | 0 | 0 | 3 | 246 |
| FXS, FXO, and/or BRI, but not in use | 0 | - | - | - | - | - | - | 19 | 16 | - | 250 |

**Notes:**

- "Max. SBC Sessions" for Mediant 800B applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g., Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

### 3.3.3.2 Mediant 800C Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800C Gateway & E-SBC are shown in the tables below.

#### 3.3.3.2.1 Non-Hybrid (SBC) Capacity

**Table 3-9: Mediant 800C Gateway & E-SBC - SBC Session Capacity per Capabilities (SBC Only)**

| H/W Configuration | SBC Transcoding Sessions | | | | | | | | Max. SBC Sessions |
|---|---|---|---|---|---|---|---|---|---|
| | From Profile 2 with Additional Advanced DSP Capabilities | | | | | | To Profile 1 | To Profile 2 | |
| | AMR-NB / G.722 | AMR-WB (G.722.2) | SILK-NB / iLBC | SILK-WB | Opus-NB | Opus-WB | | | |
| SBC | - | - | - | - | - | - | 120 | 96 | 400 |
| | √ | - | - | - | - | - | 108 | 84 | 400 |
| | - | - | √ | - | - | - | 78 | 66 | 400 |
| | - | √ | - | - | - | - | 72 | 60 | 400 |
| | - | - | - | √ | - | - | 54 | 48 | 400 |
| | - | - | - | - | √ | - | 54 | 48 | 400 |
| | - | - | - | - | - | √ | 42 | 42 | 400 |
| | **From Profile 1** | | | | | | 156 | 120 | 400 |

**Note:**

- "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).
- The maximum SBC sessions with DTMF transcoding (Profile 1 in-band DTMF to Profile 1 RFC 2833) is 156 sessions (RTP-RTP or RTP-SRTP).

#### 3.3.3.2.2 Hybrid (with Gateway) Capacity

**Table 3-10: Mediant 800C Gateway & E-SBC - SBC Session Capacity per Capabilities with Gateway**

| Telephony Interface Assembly | DSP Channels Allocated for PSTN | SBC Transcoding Sessions | | | | | | | Max SBC Sessions |
|---|---|---|---|---|---|---|---|---|---|
| | | From Profile 2 | From Profile 2 with SILK-NB / iLBC | From Profile 2 with SILK-WB | From Profile 2 with OPUS-NB | From Profile 2 with OPUS-WB | To Profile 1 | To Profile 2 | |
| 4 x E1/T1<br>4 x FXS | 124/100 | √ | - | - | - | - | 2/23 | 2/18 | 276/300 |
| | 102/100 | - | √ | - | - | - | 0 | 0 | 298/300 |
| | 78 | - | - | √ | - | - | 0 | 0 | 322 |
| | 72 | - | - | - | √ | - | 0 | 0 | 328 |
| | 54 | - | - | - | - | √ | 0 | 0 | 346 |
| 1 x E1/T1<br>4 x FXS | 35/29 | √ | - | - | - | - | 25/30 | 2025 | 365/371 |
| | 35/29 | - | √ | - | - | - | 10/15 | 9/13 | 365/371 |
| | 35/29 | - | - | √ | - | - | 1/5 | 1/5 | 365/371 |
| | 35/29 | - | - | - | √ | - | 0/4 | 0/3 | 365/371 |
| | 27 | - | - | - | - | √ | 0 | 0 | 373 |
| 8 x BRI<br>4 x FXS | 20 | √ | - | - | - | - | 38 | 31 | 380 |
| | 20 | - | √ | - | - | - | 22 | 19 | 380 |
| | 20 | - | - | √ | - | - | 12 | 11 | 380 |
| | 20 | - | - | - | √ | - | 11 | 9 | 380 |
| | 20 | - | - | - | - | √ | 4 | 3 | 380 |
| Not in use | - | √ | - | - | - | - | 114 | 96 | 400 |
| | - | - | √ | - | - | - | 78 | 66 | 400 |
| | - | - | - | √ | - | - | 54 | 48 | 400 |
| | - | - | - | - | √ | - | 54 | 48 | 400 |
| | - | - | - | - | - | √ | 42 | 42 | 400 |

**Notes:**

- "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g., Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

### 3.3.4 Mediant 1000B Gateway & E-SBC

This section lists the channel capacity and DSP templates for Mediant 1000B Gateway & E-SBC DSP.

**Notes:**

- The maximum number of channels on any form of analog, digital, and MPM module assembly is 192. When the device handles both SBC and Gateway call sessions, the maximum number of total sessions is 150. When the device handles SRTP, the maximum capacity is reduced to 120.
- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes sales representative.

#### 3.3.4.1 Analog (FXS/FXO) Interfaces

The channel capacity per DSP firmware template for analog interfaces is shown in the table below.

**Table 3-11: Mediant 1000B Analog Series - Channel Capacity per DSP Firmware Template**

|  | **DSP Template** |  |
|---|---|---|
|  | 0, 1, 2, 4, 5, 6 | 10, 11, 12, 14, 15, 16 |
|  | **Number of Channels** |  |
|  | 4 | 3 |
| Voice Coder |  |  |
| G.711 A/Mu-law PCM | √ | √ |
| G.726 ADPCM | √ | √ |
| G.723.1 | √ | √ |
| G.729 (A / AB) | √ | √ |
| G.722 | - | √ |

### 3.3.4.2 BRI Interfaces

The channel capacity per DSP firmware template for BRI interfaces is shown in the table below.

**Table 3-12: Mediant 1000B BRI Series - Channel Capacity per DSP Firmware Template**

| | DSP Template | | | | | |
|---|---|---|---|---|---|---|
| | 0, 1, 2, 4, 5, 6 | | | 10, 11, 12, 14, 15, 16 | | |
| | Number of BRI Spans | | | | | |
| | 4 | 8 | 20 | 4 | 8 | 20 |
| | Number of Channels | | | | | |
| | 8 | 16 | 40 | 6 | 12 | 30 |
| Voice Coder | | | | | | |
| G.711 A/Mu-law PCM | √ | | | √ | | |
| G.726 ADPCM | √ | | | √ | | |
| G.723.1 | √ | | | √ | | |
| G.729 (A / AB) | √ | | | √ | | |
| G.722 | - | | | √ | | |

### 3.3.4.3 E1/T1 Interfaces

The channel capacity per DSP firmware template for E1/T1 interfaces is shown in the table below.

**Table 3-13: Mediant 1000B E1/T1 Series - Channel Capacity per DSP Firmware Templates**

| | DSP Template | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 or 10 | | | | | 1 or 11 | | | | | 2 or 12 | | | | | 5 or 15 | | | | | 6 or 16 | | | | |
| | Number of Spans | | | | | | | | | | | | | | | | | | | | | | | | |
| | 1 | 2 | 4 | 6 | 8 | 1 | 2 | 4 | 6 | 8 | 1 | 2 | 4 | 6 | 8 | 1 | 2 | 4 | 6 | 8 | 1 | 2 | 4 | 6 | 8 |
| | Number of Channels | | | | | | | | | | | | | | | | | | | | | | | | |
| Default Settings | 31 | 62 | 120 | 182 | 192 | 31 | 48 | 80 | 128 | 160 | 24 | 36 | 60 | 96 | 120 | 24 | 36 | 60 | 96 | 120 | 31 | 60 | 100 | 160 | 192 |
| With 128-ms Echo Cancellation | 31 | 60 | 100 | 160 | 192 | 31 | 48 | 80 | 128 | 160 | 24 | 36 | 60 | 96 | 120 | 24 | 36 | 60 | 96 | 120 | 31 | 60 | 100 | 160 | 192 |
| With IPM Features | 31 | 60 | 100 | 160 | 192 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 31 | 60 | 100 | 160 | 192 |
| Voice Coder | | | | | | | | | | | | | | | | | | | | | | | | | |
| G.711 A-Law/M-Law PCM | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | |
| G.726 ADPCM | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | | - | | | | |
| G.723.1 | ✓ | | | | | - | | | | | - | | | | | - | | | | | - | | | | |
| G.729 (A / AB) | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | |
| GSM FR | ✓ | | | | | ✓ | | | | | - | | | | | - | | | | | - | | | | |
| MS GSM | ✓ | | | | | ✓ | | | | | - | | | | | - | | | | | - | | | | |
| iLBC | - | | | | | - | | | | | - | | | | | ✓ | | | | | - | | | | |
| EVRC | - | | | | | - | | | | | ✓ | | | | | - | | | | | - | | | | |
| QCELP | - | | | | | - | | | | | ✓ | | | | | - | | | | | - | | | | |
| AMR | - | | | | | ✓ | | | | | - | | | | | - | | | | | - | | | | |
| GSM EFR | - | | | | | ✓ | | | | | - | | | | | - | | | | | - | | | | |
| G.722 | - | | | | | - | | | | | - | | | | | - | | | | | ✓ | | | | |
| Transparent | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | | ✓ | | | | |

**Note:** "IPM Features" refers to Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD).

### 3.3.4.4 Media Processing Interfaces

The transcoding session capacity according to DSP firmware template (per MPM module) is shown in the table below.

**Notes:**

- The device can be housed with up to four MPM modules.
- The MPM modules can only be housed in slots 1 through 5.

**Table 3-14: Transcoding Sessions Capacity per MPM According to DSP Firmware Template for Mediant 1000B**

| | **DSP Template** | | | | |
|---|---|---|---|---|---|
| | 0 or 10 | 1 or 11 | 2 or 12 | 5 or 15 | 6 or 16 |
| IPM Detectors Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD) | **Number of Transcoding Sessions per MPM Module** | | | | |
| - | 24 | 16 | 12 | 12 | 20 |
| ✓ | 20 | - | - | - | 20 |
| **Voice Coder** | | | | | |
| G.711 A-law / Mμ-law PCM | ✓ | ✓ | ✓ | ✓ | ✓ |
| G.726 ADPCM | ✓ | ✓ | ✓ | ✓ | - |
| G.723.1 | ✓ | - | - | - | - |
| G.729 (A / AB) | ✓ | ✓ | ✓ | ✓ | ✓ |
| GSM FR | ✓ | ✓ | - | - | - |
| MS GSM | ✓ | ✓ | - | - | - |
| iLBC | - | - | - | ✓ | - |
| EVRC | - | - | ✓ | - | - |
| QCELP | - | - | ✓ | - | - |
| AMR | - | ✓ | - | - | - |
| GSM EFR | - | ✓ | - | - | - |
| G.722 | - | - | - | - | ✓ |
| Transparent | ✓ | ✓ | ✓ | ✓ | ✓ |

### 3.3.5 Mediant 3100 Gateway & E-SBC

This section describes the capacity of Mediant 3100 Gateway & E-SBC.

#### 3.3.5.1 Gateway Capacity

The following table shows the maximum number of Gateway sessions when there are no SBC transcoding sessions.

**Table 3-15: Mediant 3100 - Gateway Channel Capacity per Capability Profile**

| Profile | Hardware Assembly | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | E1 | | | | T1 | | | |
| | 8 x E1 | 16 x E1 | 32 x E1 | 64 x E1 | 8 x T1 | 16 x T1 | 32 x T1 | 64 x T1 |
| Profile 1 | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 + G.722 / AMR-NB | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 + AMR-WB | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 + SILK-NB | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 + SILK-WB | 208 | 416 | 832 | 1664 | 192 | 384 | 768 | 1536 |
| Profile 2 + Opus-NB | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |
| Profile 2 + Opus-WB | 240 | 480 | 960 | 1920 | 192 | 384 | 768 | 1536 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.

#### 3.3.5.2 Non-Hybrid (SBC) Transcoding Capacity

The following table shows the maximum number of SBC transcoding sessions when there are no Gateway sessions.

**Table 3-16: Mediant 3100 - SBC Transcoding Capacity per Coder Capability Profile**

| Transcoding Session Coders | | 8 x E1/T1 | 16 x E1/T1 | 32 x E1/T1 | 64 x E1/T1 |
|---|---|---|---|---|---|
| **From Coder** | **To Coder** | | | | |
| Profile 1 | Profile 1 | 460 | 925 | 1,855 | 3,700 |
| Profile 1 | Profile 2 | 400 | 800 | 1,600 | 3,200 |
| Profile 2 | Profile 2 | 350 | 700 | 1,405 | 2,800 |
| Profile 1 | Profile 2 + G.722 / AMR-NB | 400 | 800 | 1,600 | 3,200 |
| Profile 2 | Profile 2 + G.722 / AMR-NB | 350 | 700 | 1,405 | 2,800 |
| Profile 1 | Profile 2 + AMR-WB | 255 | 510 | 1,020 | 2,025 |
| Profile 2 | Profile 2 + AMR-WB | 240 | 480 | 960 | 1,900 |
| Profile 1 | Profile 2 + SILK-NB | 260 | 525 | 1,055 | 2,100 |
| Profile 2 | Profile 2 + SILK-NB | 245 | 495 | 990 | 1,975 |
| Profile 1 | Profile 2 + SILK-WB | 180 | 365 | 735 | 1,450 |
| Profile 2 | Profile 2 + SILK-WB | 175 | 350 | 700 | 1,400 |
| Profile 1 | Profile 2 + Opus-NB | 220 | 445 | 895 | 1,775 |
| Profile 2 | Profile 2 + Opus-NB | 205 | 415 | 830 | 1,650 |
| Profile 1 | Profile 2 + Opus-WB | 205 | 415 | 830 | 1,650 |
| Profile 2 | Profile 2 + Opus-WB | 190 | 380 | 765 | 1,525 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.

### 3.3.6 MP-1288 Analog Gateway & E-SBC

Session capacity includes Gateway sessions as well as SBC sessions without transcoding capabilities. The maximum capacity of Gateway sessions for MP-1288 Gateway & E-SBC is shown in the table below.

**Table 3-17: MP-1288 Gateway - Session Capacity**

| Coder | Gateway Sessions Capacity | |
|---|---|---|
| | Single FXS Blade | Fully Populated (4 x FXS Blades) |
| Basic: G.711, G.729 (A / AB), G.723.1, G.726 / G.727 ADPCM | 72 | 288 |
| G.722 | 72 | 288 |
| AMR-NB | 72 | 288 |
| Opus-NB | 60 | 240 |

**Note:**

- Quality Monitoring and Noise Reduction are not supported.
- SRTP is supported on all configurations.

### 3.3.7 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below:

**Table 3-18: Mediant 2600 E-SBC - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Without MPM4** | **With MPM4** |
| Profile 1 | Profile 1 | 400 | 600 |
| Profile 2 | Profile 1 | 300 | 600 |
| Profile 2 | Profile 2 | 250 | 600 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 275 | 600 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 225 | 600 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 200 | 600 |
| Profile 2 | Profile 2 + AMR-WB (G.722.2) | 175 | 525 |
| Profile 1 | Profile 2 + iLBC | 175 | 575 |
| Profile 2 | Profile 2 + iLBC | 150 | 500 |
| Profile 1 | Profile 2 + SILK-NB | 200 | 600 |
| Profile 2 | Profile 2 + SILK-NB | 175 | 525 |
| Profile 1 | Profile 2 + SILK-WB | 100 | 350 |
| Profile 2 | Profile 2 + SILK-WB | 100 | 350 |
| Profile 1 | Profile 2 + Opus-NB | 125 | 425 |
| Profile 2 | Profile 2 + Opus-NB | 125 | 375 |
| Profile 1 | Profile 2 + Opus-WB | 100 | 300 |
| Profile 2 | Profile 2 + Opus-WB | 75 | 275 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

### 3.3.8 Mediant 4000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-19: Mediant 4000 SBC - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Without MPM8** | **With MPM8** |
| Profile 1 | Profile 1 | 800 | 2,400 |
| Profile 2 | Profile 1 | 600 | 1,850 |
| Profile 2 | Profile 2 | 500 | 1,550 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 550 | 1,650 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 450 | 1,350 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 400 | 1,200 |
| Profile 2 | Profile 2 + AMR-WB (G.722.2) | 350 | 1,050 |
| Profile 1 | Profile 2 + iLBC | 350 | 1,150 |
| Profile 2 | Profile 2 + iLBC | 300 | 1,000 |
| Profile 1 | Profile 2 + SILK-NB | 400 | 1,200 |
| Profile 2 | Profile 2 + SILK-NB | 350 | 1,050 |
| Profile 1 | Profile 2 + SILK-WB | 200 | 700 |
| Profile 2 | Profile 2 + SILK-WB | 200 | 700 |
| Profile 1 | Profile 2 + Opus-NB | 250 | 850 |
| Profile 2 | Profile 2 + Opus-NB | 250 | 750 |
| Profile 1 | Profile 2 + Opus-WB | 200 | 600 |
| Profile 2 | Profile 2 + Opus-WB | 150 | 550 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

#### 3.3.8.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-20: Mediant 4000 SBC - Forwarding Capacity per Feature**

| Feature | Max. Sessions |
|---|---|
| Fax Detection | 5,000 |
| AD/AMD/Beep Detection | 5,000 |
| CP Detection | 5,000 |
| Jitter Buffer | 5,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

### 3.3.9 Mediant 4000B SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-21: Mediant 4000B SBC - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | | | | |
|---|---|---|---|---|---|---|
| From Coder Profile | To Coder Profile | Without MPM | 1 x MPM8B | 1 x MPM12B | 2 x MPM12B | 3 x MPM12B |
| Profile 1 | Profile 1 | 800 | 2,400 | 3,250 | 5,000 | 5,000 |
| Profile 2 | Profile 1 | 600 | 1,850 | 2,450 | 4,350 | 5,000 |
| Profile 2 | Profile 2 | 500 | 1,550 | 2,100 | 3,650 | 5,000 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 550 | 1,650 | 2,200 | 3,850 | 5,000 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 450 | 1,350 | 1,800 | 3,150 | 4,550 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 400 | 1,200 | 1,600 | 2,850 | 4,050 |
| Profile 2 | Profile 2 + AMR-WB (G.722.2) | 350 | 1,050 | 1,400 | 2,500 | 3,600 |
| Profile 1 | Profile 2 + iLBC | 400 | 1,200 | 1,600 | 2,850 | 4,050 |
| Profile 2 | Profile 2 + iLBC | 350 | 1,050 | 1,400 | 2,500 | 3,600 |
| Profile 1 | Profile 2 + SILK-NB | 400 | 1,200 | 1,600 | 2,850 | 4,050 |
| Profile 2 | Profile 2 + SILK-NB | 350 | 1,050 | 1,400 | 2,500 | 3,600 |

| Session Coders | | Max. Sessions | | | | |
|---|---|---|---|---|---|---|
| From Coder Profile | To Coder Profile | Without MPM | 1 x MPM8B | 1 x MPM12B | 2 x MPM12B | 3 x MPM12B |
| Profile 1 | Profile 2 + SILK-WB | 200 | 700 | 950 | 1,650 | 2,400 |
| Profile 2 | Profile 2 + SILK-WB | 200 | 700 | 950 | 1,650 | 2,400 |
| Profile 1 | Profile 2 + Opus-NB | 250 | 850 | 1,150 | 2,000 | 2,850 |
| Profile 2 | Profile 2 + Opus-NB | 250 | 750 | 1,050 | 1,800 | 2,600 |
| Profile 1 | Profile 2 + Opus-WB | 200 | 600 | 850 | 1,500 | 2,150 |
| Profile 2 | Profile 2 + Opus-WB | 150 | 550 | 750 | 1,300 | 1,900 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPMB is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

### 3.3.9.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-22: Mediant 4000B SBC - Forwarding Capacity per Feature**

| Feature | Max. Sessions |
|---|---|
| Fax Detection | 5,000 |
| AD/AMD/Beep Detection | 5,000 |
| CP Detection | 5,000 |
| Jitter Buffer | 5,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

### 3.3.10 Mediant 9000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-23: Mediant 9000 SBC - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | | | |
|---|---|---|---|---|---|
| From Coder Profile | To Coder Profile | Without Hyper-Threading | | With Hyper-Threading | |
| | | Basic | Extended | Basic | Extended |
| Profile 1 | Profile 1 | 3,025 | 2,525 | 6,575 | 3,875 |
| Profile 2 | Profile 1 | 1,500 | 1,325 | 2,125 | 1,700 |
| Profile 2 | Profile 2 | 1,000 | 900 | 1,275 | 1,100 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 1,500 | 1,300 | 2,075 | 1,625 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 1,000 | 900 | 1,225 | 1,050 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 500 | 475 | 600 | 575 |
| Profile 2 | Profile 2 + AMR-WB | 425 | 400 | 500 | 475 |
| Profile 1 | Profile 2 + SILK-NB | 1,300 | 1,175 | 1,700 | 1,450 |
| Profile 2 | Profile 2 + SILK-NB | 900 | 825 | 1,100 | 975 |
| Profile 1 | Profile 2 + SILK-WB | 775 | 750 | 1,000 | 950 |
| Profile 2 | Profile 2 + SILK-WB | 625 | 600 | 750 | 725 |
| Profile 1 | Profile 2 + Opus-NB | 825 | 750 | 1,050 | 900 |
| Profile 2 | Profile 2 + Opus-NB | 650 | 600 | 775 | 700 |
| Profile 1 | Profile 2 + Opus-WB | 625 | 575 | 800 | 700 |
| Profile 2 | Profile 2 + Opus-WB | 525 | 475 | 625 | 575 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

#### 3.3.10.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-24: Mediant 9000 SBC - Forwarding Capacity per Feature**

| Feature | Max. Sessions | |
|---|---|---|
| | Without Hyper-Threading | With Hyper-Threading |
| Fax Detection | 24,000 | 40,000 |
| AD/AMD/Beep Detection | 24,000 | 39,000 |
| CP Detection | 24,000 | 44,000 |
| Jitter Buffer | 2,225 | 5,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

### 3.3.11 Mediant 9000 Rev. B / 9080 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-25: Mediant 9000 Rev. B / 9080 - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| From Coder Profile | To Coder Profile | Basic | Extended |
| Profile 1 | Profile 1 | 9,600 | 6,625 |
| Profile 2 | Profile 1 | 4,400 | 3,625 |
| Profile 2 | Profile 2 | 2,875 | 2,500 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 2,925 | 2,600 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 2,150 | 1,950 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 950 | 925 |
| Profile 2 | Profile 2 + AMR-WB | 850 | 825 |
| Profile 1 | Profile 2 + SILK-NB | 2,750 | 2,500 |
| Profile 2 | Profile 2 + SILK-NB | 2,050 | 1,900 |
| Profile 1 | Profile 2 + SILK-WB | 1,575 | 1,475 |
| Profile 2 | Profile 2 + SILK-WB | 1,300 | 1,250 |
| Profile 1 | Profile 2 + Opus-NB | 1,700 | 1,450 |
| Profile 2 | Profile 2 + Opus-NB | 1,375 | 1,200 |
| Profile 1 | Profile 2 + Opus-WB | 1,375 | 1,200 |
| Profile 2 | Profile 2 + Opus-WB | 1,175 | 1,025 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

#### 3.3.11.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-26: Mediant 9000 Rev. B / 9080 SBC - Forwarding Capacity per Feature**

| Feature | Max. Sessions |
|---|---|
| Fax Detection | 45,000 |
| AD, AMD, and Beep Detection | 45,000 |
| CP Detection | 45,000 |
| Jitter Buffer | 6,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

### 3.3.12 Mediant 9000 / 9000 Rev. B / 9080 SBC with Media Transcoders

Mediant 9000, Mediant 9000 Rev. B, or Mediant 9080 SBC with Media Transcoders allows increasing the number of transcoding sessions by using Media Transcoders. The maximum number of transcoding sessions depends on the following:

- Number of Media Transcoders in the media transcoding cluster. (The cluster can have up to eight Media Transcoders.)
- Cluster operation mode (Best-Effort or Full-HA mode).
- Maximum transcoding sessions. Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP value specified in the table. As a result, if all sessions are with transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding as specified in Table 3-1.

The following table lists maximum transcoding sessions capacity of a single Media Transcoder.

**Table 3-27: Single Media Transcoder (MT) - Transcoding Capacity per Profile**

| Session Coders | | Max. Sessions | | |
|---|---|---|---|---|
| From Coder Profile | To Coder Profile | 1 x MPM12B | 2 x MPM12B | 3 x MPM12B |
| Profile 1 | Profile 1 | 2,875 | 5,000 | 5,000 |
| Profile 2 | Profile 1 | 2,300 | 4,025 | 5,000 |

| Session Coders | | Max. Sessions | | |
|---|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **1 x MPM12B** | **2 x MPM12B** | **3 x MPM12B** |
| Profile 2 | Profile 2 | 1,800 | 3,175 | 4,550 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 2,000 | 3,525 | 5,000 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 1,625 | 2,850 | 4,075 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 1,425 | 2,500 | 3,600 |
| Profile 2 | Profile 2 + AMR-WB (G.722.2) | 1,225 | 2,175 | 3,100 |
| Profile 1 | Profile 2 + SILK-NB | 1,425 | 2,500 | 3,600 |
| Profile 2 | Profile 2 + SILK-NB | 1,225 | 2,175 | 3,100 |
| Profile 1 | Profile 2 + SILK-WB | 850 | 1,500 | 2,150 |
| Profile 2 | Profile 2 + SILK-WB | 850 | 1,500 | 2,150 |
| Profile 1 | Profile 2 + Opus-NB | 1,050 | 1,825 | 2,625 |
| Profile 2 | Profile 2 + Opus-NB | 950 | 1,675 | 2,400 |
| Profile 1 | Profile 2 + Opus-WB | 750 | 1,325 | 1,900 |
| Profile 2 | Profile 2 + Opus-WB | 650 | 1,175 | 1,675 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM12B is a Media Processing Module in the Media Transcoder that provides additional DSPs, allowing higher capacity.
- For best cluster efficiency, all Media Transcoders in the Cluster should populate the same number of MPM12Bs.
- The SBC employs load balancing of transcoding sessions among all Media Transcoders in the Cluster. Each Media Transcoder can handle up to 200 calls (transcoded sessions) per second (CPS).

### 3.3.13 Mediant 9030 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-28: Mediant 9030 SBC - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 4,025 | 2,775 |
| Profile 2 | Profile 1 | 1,825 | 1,525 |
| Profile 2 | Profile 2 | 1,200 | 1,050 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 1,200 | 1,075 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 875 | 825 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 400 | 375 |
| Profile 2 | Profile 2 + AMR-WB | 350 | 350 |
| Profile 1 | Profile 2 + SILK-NB | 1,150 | 1,050 |
| Profile 2 | Profile 2 + SILK-NB | 850 | 775 |
| Profile 1 | Profile 2 + SILK-WB | 650 | 625 |
| Profile 2 | Profile 2 + SILK-WB | 525 | 525 |
| Profile 1 | Profile 2 + Opus-NB | 700 | 600 |
| Profile 2 | Profile 2 + Opus-NB | 575 | 500 |
| Profile 1 | Profile 2 + Opus-WB | 575 | 500 |
| Profile 2 | Profile 2 + Opus-WB | 475 | 425 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

#### 3.3.13.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-29: Mediant 9030 SBC - Forwarding Capacity per Feature**

| Feature | Max. Sessions |
|---|---|
| Fax Detection | 23,000 |
| AD/AMD/Beep Detection | 23,000 |
| CP Detection | 23,000 |
| Jitter Buffer | 3,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

## 3.3.14 Mediant Cloud Edition (CE) SBC

The Media Components (MC) in the media cluster of the Mediant CE must all be of the same instance type: either forwarding-only, or forwarding and transcoding. A maximum of 21 MCs can be used.

### 3.3.14.1 Mediant CE SBC for AWS EC2

#### 3.3.14.1.1 Forwarding Sessions

The number of concurrent forwarding sessions per MC is shown in the following table.

**Table 3-30: Forwarding Capacity per MC Instance Type**

| MC Instance Type | Max. Forwarding Sessions |
|---|---|
| m5n.large | 3,200 |
| c5.4xlarge | 4,000 |

**Note:** Forwarding performance was tested in AWS Ireland Region.

#### 3.3.14.1.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be of the AWS instance type c5.4xlarge. The number of supported transcoding sessions per MC is shown in the following table.

**Table 3-31: Transcoding Capacity per c5.4xlarge MC**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| From Coder Profile | To Coder Profile | Basic | Extended |
| Profile 1 | Profile 1 | 3,500 | 2,825 |
| Profile 2 | Profile 1 | 2,375 | 1,900 |
| Profile 2 | Profile 2 | 1,625 | 1,425 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 1,500 | 1,300 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 1,150 | 1,050 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 475 | 475 |
| Profile 2 | Profile 2 + AMR-WB | 425 | 425 |
| Profile 1 | Profile 2 + SILK-NB | 1,400 | 1,250 |
| Profile 2 | Profile 2 + SILK-NB | 1,100 | 1,025 |
| Profile 1 | Profile 2 + SILK-WB | 775 | 750 |
| Profile 2 | Profile 2 + SILK-WB | 675 | 675 |
| Profile 1 | Profile 2 + Opus-NB | 850 | 725 |

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 2 | Profile 2 + Opus-NB | 725 | 650 |
| Profile 1 | Profile 2 + Opus-WB | 700 | 600 |
| Profile 2 | Profile 2 + Opus-WB | 625 | 550 |

⚠

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

### 3.3.14.2 Mediant CE SBC for Azure

#### 3.3.14.2.1 Forwarding Sessions

The number of concurrent forwarding sessions per Media Component (MC) is shown in the following table.

**Table 3-32: Session Capacity per MC**

| MC VM Size | Max. Forwarding-Only Sessions | Max. Forwarding & Transcoding Sessions |
|---|---|---|
| D2ds_v5 | 3,000 | 3,000 |
| D4ds_v5 | 6,500 | 5,500 |
| D8ds_v5 | 12,000 | 6,000 |

**Note:** It's not recommended to exceed 5,000 sessions per MC because of the duration required for processing an MC failover.

#### 3.3.14.2.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be Azure virtual machine size D2ds_v5, D4ds_v5, or D8ds_v5. The number of supported transcoding sessions per MC is shown in the following table.

**Table 3-33: Transcoding Capacity per MC**

| Session Coders | | D2ds_v5 | | D4ds_v5 | | D8ds_v5 | |
|---|---|---|---|---|---|---|---|
| From Coder Profile | To Coder Profile | Basic | Extended | Basic | Extended | Basic | Extended |
| Profile 1 | Profile 1 | 275 | 175 | 575 | 350 | 1,725 | 1,100 |
| Profile 2 | Profile 1 | 150 | 125 | 300 | 250 | 925 | 750 |
| Profile 2 | Profile 2 | 100 | 75 | 200 | 175 | 625 | 550 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 75 | 75 | 175 | 150 | 575 | 500 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 75 | 50 | 150 | 125 | 450 | 400 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 25 | 25 | 50 | 50 | 175 | 175 |
| Profile 2 | Profile 2 + AMR-WB | 25 | 25 | 50 | 50 | 175 | 175 |
| Profile 1 | Profile 2 + SILK-NB | 75 | 75 | 175 | 150 | 550 | 500 |
| Profile 2 | Profile 2 + SILK-NB | 50 | 50 | 125 | 125 | 425 | 400 |
| Profile 1 | Profile 2 + SILK-WB | 50 | 50 | 100 | 100 | 300 | 300 |
| Profile 2 | Profile 2 + SILK-WB | 25 | 25 | 75 | 75 | 275 | 250 |
| Profile 1 | Profile 2 + Opus-NB | 50 | 25 | 100 | 75 | 325 | 275 |

| Session Coders | | D2ds_v5 | | D4ds_v5 | | D8ds_v5 | |
|---|---|---|---|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** | **Basic** | **Extended** | **Basic** | **Extended** |
| Profile 2 | Profile 2 + Opus-NB | 25 | 25 | 75 | 75 | 275 | 250 |
| Profile 1 | Profile 2 + Opus-WB | 25 | 25 | 75 | 75 | 275 | 225 |
| Profile 2 | Profile 2 + Opus-WB | 25 | 25 | 75 | 50 | 250 | 200 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

### 3.3.14.3 Mediant CE SBC for VMware

The following tables list maximum forwarding and transcoding capacities for Mediant CE SBC running on VMware hypervisor with Hyper-Threading.

Each vCPU refers to a single thread of a physical core. For example, a 4-vCPU virtual machine is allocated by only two physical cores.

**Note:**

- The profiles below require the following minimum requirements:
  - √ Intel Xeon Scalable Processors or later. The capacity listed in the following table refers to 3.3 GHz all-core Turbo speed. When using different all-core Turbo speed, capacity is increased or decreased accordingly.
  - √ Hyper-Threading is enabled on host.
  - √ VMware ESXi 6.7 or later.
  - √ CPUOverrideHT ini file parameter is configured to 1.
- CPU Affinity is recommended. For more information, refer to the *Installation Manual*.
- For Server Failure redundancy, the maximum active media sessions (before failure) on each server must not exceed 4,000 media sessions.

#### 3.3.14.3.1 Forwarding Sessions

The number of concurrent forwarding sessions per Media Component (MC) is shown in the following table.

**Table 3-34: Forwarding Capacity per MC Instance Type**

| MC Instance Type | Max. Sessions |
|---|---|
| 2 vCPUs, 8GB | 4,000 (Forwarding Only) |
| 8 vCPUs, 8GB | 4,000 (Forwarding and Transcoding) |

#### 3.3.14.3.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be a virtual machine of 8 vCPUs and 8 GB. The number of supported transcoding sessions per MC is shown in the following table.

**Note:** For transcoding capabilities, the 'Media Component Profile' parameter on all Media Components must be configured to **Transcoding Enabled** (MCProfile = 1).

**Table 3-35: Mediant CE SBC on VMware with Hyper-Threading - Transcoding Capacity**

| Session Coders | | Max. Sessions<br>8 vCPU 8-GB RAM | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 1,800 | 1,175 |
| Profile 1 | Profile 2 | 975 | 775 |
| Profile 2 | Profile 2 | 675 | 575 |
| Profile 1 | Profile 2 + G.722 / AMR-NB | 600 | 525 |
| Profile 2 | Profile 2 + G.722 / AMR-NB | 475 | 425 |
| Profile 1 | Profile 2 + AMR-WB | 200 | 175 |
| Profile 2 | Profile 2 + AMR-WB | 175 | 175 |
| Profile 1 | Profile 2 + SILK-NB | 575 | 525 |
| Profile 2 | Profile 2 + SILK-NB | 450 | 425 |
| Profile 1 | Profile 2 + SILK-WB | 325 | 300 |
| Profile 2 | Profile 2 + SILK-WB | 275 | 275 |
| Profile 1 | Profile 2 + Opus-NB | 350 | 300 |
| Profile 2 | Profile 2 + Opus-NB | 300 | 275 |
| Profile 1 | Profile 2 + Opus-WB | 300 | 250 |
| Profile 2 | Profile 2 + Opus-WB | 250 | 225 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

### 3.3.14.4 Mediant CE SBC for GCP

#### 3.3.14.4.1 Forwarding Sessions

The number of concurrent forwarding sessions (RTP-RTP) per Media Component (MC) is shown in the following table.

**Table 3-36: Session Capacity per MC**

| MC VM Size | Max. Forwarding-Only Sessions |
|---|---|
| n2-standard-2 | 3,500 |

#### 3.3.14.4.2 Transcoding Sessions

For transcoding capabilities, the MC should be of the n2-standard-2 or n2_highcpu-8 instance types.

When the transcoding session is at maximum, the total sessions is reduced as shown in the following table.

**Table 3-37: Transcoding Sessions per MC**

| MC VM Size | Max. Forwarding and Transcoding Sessions |
|---|---|
| n2-standard-2 | 1,500 (up to 300 transcoding sessions) |
| n2-highcpu-8 | 1,600 (up to 1,500 transcoding sessions) |

The number of supported transcoding sessions per MC is shown in the following table.

**Table 3-38: Transcoding Capacity per MC**

| Session Coders | | n2-standard-2 | | n2-highcpu-8 | |
|---|---|---|---|---|---|
| From Coder Profile | To Coder Profile | Basic | Extended | Basic | Extended |
| Profile 1 | Profile 1 | 300 | 175 | 1,500 | 1,175 |
| Profile 2 | Profile 1 | 150 | 125 | 975 | 775 |
| Profile 2 | Profile 2 | 100 | 75 | 675 | 575 |

| Session Coders | | n2-standard-2 | | n2-highcpu-8 | |
|---|---|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** | **Basic** | **Extended** |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 100 | 75 | 625 | 525 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 75 | 50 | 475 | 425 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 25 | 25 | 200 | 175 |
| Profile 2 | Profile 2 + AMR-WB | 25 | 25 | 175 | 175 |
| Profile 1 | Profile 2 + SILK-NB | 75 | 75 | 575 | 525 |
| Profile 2 | Profile 2 + SILK-NB | 75 | 50 | 450 | 425 |
| Profile 1 | Profile 2 + SILK-WB | 50 | 50 | 325 | 300 |
| Profile 2 | Profile 2 + SILK-WB | 25 | 25 | 275 | 275 |
| Profile 1 | Profile 2 + Opus-NB | 50 | 50 | 350 | 300 |
| Profile 2 | Profile 2 + Opus-NB | 50 | 25 | 300 | 275 |
| Profile 1 | Profile 2 + Opus-WB | 50 | 25 | 300 | 250 |
| Profile 2 | Profile 2 + Opus-WB | 25 | 25 | 250 | 225 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

## 3.3.15 Mediant Virtual Edition (VE) SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required (DSP Performance Profile), the number of sessions that can use DSP capabilities is reduced, as shown in the tables in this section.

### 3.3.15.1 Mediant VE SBC for Hypervisors with Hyper-Threading

The following tables list maximum transcoding capacity for Mediant VE SBC running on the following hypervisors with Hyper-Threading: VMware, KVM/OpenStack, and Hyper-V.

Each vCPU refers to a Hyper-Threaded core (logical). For example, a 4-vCPU virtual machine allocates only 2 physical cores.

**Note:**

- The transcoding profiles below require the following minimum requirements:
  - √ Intel Xeon Scalable Processors or later. The capacity listed in the table below refer to 3.3 GHz all-core Turbo speed. When using different all-core Turbo speed, the capacity is increased or decreased accordingly.
  - √ Hyper-Threading enabled on host.
  - √ VMware Hypervisor:
    - o VMware ESXi 6.7 or later. Capacities in table Table 3-1 were achieved using ESXi Version 7.0.3.
    - o CPUOverrideHT ini file parameter is configured to 1.
  - √ KVM Hypervisor/OpenStack: Host-Passthrough mode must be used. For more information, refer to the *Installation Manual*.
- CPU Affinity is recommended. For more information, refer to the *Installation Manual*.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to Optimized for Transcoding (2).

**Table 3-39: Mediant VE SBC on Hypervisors with Hyper-Threading - Transcoding Capacity**

| Session Coders | | Max. Sessions | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 2 vCPU 8-GB RAM | | 4 vCPU 8-GB RAM (VMware Only) | | 8 vCPU 16-GB RAM | | 16 vCPU 16-GB RAM (Not Hyper-V) | |
| From Coder Profile | To Coder Profile | Basic | Extended | Basic | Extended | Basic | Extended | Basic | Extended |
| Profile 1 | Profile 1 | 300 | 200 | 800 | 600 | 1,200 | 825 | 2,400 | 2,400 |
| Profile 1 | Profile 2 | 150 | 125 | 500 | 400 | 675 | 550 | 2,075 | 1,650 |
| Profile 2 | Profile 2 | 100 | 100 | 350 | 300 | 475 | 400 | 1,425 | 1,250 |
| Profile 1 | Profile 2 + G.722 / AMR-NB | 100 | 75 | 325 | 275 | 425 | 375 | 1,300 | 1,150 |
| Profile 2 | Profile 2 + G.722 / AMR-NB | 75 | 75 | 250 | 225 | 325 | 300 | 1,000 | 925 |
| Profile 1 | Profile 2 + AMR-WB | 25 | 25 | 100 | 100 | 125 | 125 | 425 | 400 |

| Session Coders | | Max. Sessions | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 2 vCPU 8-GB RAM | | 4 vCPU 8-GB RAM (VMware Only) | | 8 vCPU 16-GB RAM | | 16 vCPU 16-GB RAM (Not Hyper-V) | |
| From Coder Profile | To Coder Profile | Basic | Extended | Basic | Extended | Basic | Extended | Basic | Extended |
| Profile 2 | Profile 2 + AMR-WB | 25 | 25 | 75 | 75 | 125 | 125 | 375 | 375 |
| Profile 1 | Profile 2 + SILK-NB | 100 | 75 | 300 | 275 | 400 | 350 | 1,225 | 1,100 |
| Profile 2 | Profile 2 + SILK-NB | 75 | 75 | 225 | 225 | 325 | 300 | 975 | 900 |
| Profile 1 | Profile 2 + SILK-WB | 50 | 50 | 175 | 150 | 225 | 200 | 700 | 650 |
| Profile 2 | Profile 2 + SILK-WB | 50 | 50 | 150 | 150 | 200 | 200 | 600 | 600 |
| Profile 1 | Profile 2 + Opus-NB | 50 | 50 | 175 | 150 | 250 | 200 | 750 | 650 |
| Profile 2 | Profile 2 + Opus-NB | 50 | 25 | 150 | 125 | 200 | 175 | 650 | 575 |
| Profile 1 | Profile 2 + Opus-WB | 50 | 25 | 150 | 125 | 200 | 175 | 625 | 525 |
| Profile 2 | Profile 2 + Opus-WB | 25 | 25 | 125 | 100 | 175 | 150 | 550 | 475 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

### 3.3.15.2 Mediant VE SBC for Amazon AWS EC2

The following tables list maximum channel capacity for Mediant VE SBC on the Amazon EC2 platform.

#### 3.3.15.2.1 Transcoding Sessions

**Note:** For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

##### 3.3.15.2.1.1 m5n.large

**Table 3-40: Mediant VE SBC on m5n.large - Transcoding Capacity**

| **Session Coders** | | **Max. Sessions** | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 250 | 150 |
| Profile 2 | Profile 1 | 125 | 100 |
| Profile 2 | Profile 2 | 75 | 75 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 75 | 75 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 50 | 50 |
| Profile 1 | Profile 2 + AMR-WB | 25 | 25 |
| Profile 2 | Profile 2 + AMR-WB | 25 | 25 |
| Profile 1 | Profile 2 + SILK-NB | 75 | 50 |
| Profile 2 | Profile 2 + SILK-NB | 50 | 50 |
| Profile 1 | Profile 2 + SILK-WB | 25 | 25 |
| Profile 2 | Profile 2 + SILK-WB | 25 | 25 |
| Profile 1 | Profile 2 + Opus-NB | 50 | 25 |
| Profile 2 | Profile 2 + Opus-NB | 25 | 25 |
| Profile 1 | Profile 2 + Opus-WB | 25 | 25 |
| Profile 2 | Profile 2 + Opus-WB | 25 | 25 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

###### 3.3.15.2.1.2 c5n.2xlarge

**Table 3-41: Mediant VE SBC on c5n.2xlarge - Transcoding Capacity**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 1,950 | 1,275 |
| Profile 2 | Profile 1 | 1,050 | 850 |
| Profile 2 | Profile 2 | 725 | 625 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 675 | 575 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 500 | 475 |
| Profile 1 | Profile 2 + AMR-WB | 200 | 200 |
| Profile 2 | Profile 2 + AMR-WB | 175 | 175 |
| Profile 1 | Profile 2 + SILK-NB | 625 | 550 |
| Profile 2 | Profile 2 + SILK-NB | 500 | 450 |
| Profile 1 | Profile 2 + SILK-WB | 350 | 325 |
| Profile 2 | Profile 2 + SILK-WB | 300 | 300 |
| Profile 1 | Profile 2 + Opus-NB | 375 | 325 |
| Profile 2 | Profile 2 + Opus-NB | 325 | 300 |
| Profile 1 | Profile 2 + Opus-WB | 300 | 275 |
| Profile 2 | Profile 2 + Opus-WB | 275 | 250 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

#### 3.3.15.2.1.3 c5n.9xlarge

**Table 3-42: Mediant VE SBC on c5n.9xlarge - Transcoding Capacity**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 7,000 | 6,800 |
| Profile 2 | Profile 1 | 5,725 | 4,575 |
| Profile 2 | Profile 2 | 3,925 | 3,450 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 3,600 | 3,125 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 2,775 | 2,550 |
| Profile 1 | Profile 2 + AMR-WB | 1,175 | 1,150 |
| Profile 2 | Profile 2 + AMR-WB | 1,050 | 1,000 |
| Profile 1 | Profile 2 + SILK-NB | 3,400 | 3,025 |
| Profile 2 | Profile 2 + SILK-NB | 2,675 | 2,475 |
| Profile 1 | Profile 2 + SILK-WB | 1,900 | 1,800 |
| Profile 2 | Profile 2 + SILK-WB | 1,650 | 1,625 |
| Profile 1 | Profile 2 + Opus-NB | 2,075 | 1,775 |
| Profile 2 | Profile 2 + Opus-NB | 1,775 | 1,600 |
| Profile 1 | Profile 2 + Opus-WB | 1,725 | 1,450 |
| Profile 2 | Profile 2 + Opus-WB | 1,500 | 1,325 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

#### 3.3.15.2.2Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-43: Mediant VE SBC on Amazon EC2 - Forwarding Capacity per Feature**

| Feature | Max. Sessions | |
|---|---|---|
| | c5.2xlarge | c5.9xlarge |
| Fax Detection | 5,500 | 7,000 |
| AD/AMD/Beep Detection | 5,500 | 7,000 |
| CP Detection | 5,500 | 7,000 |
| Jitter Buffer | 1,800 | 7,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

### 3.3.15.3 Mediant VE SBC for Azure

The following tables list maximum channel capacity for Mediant VE SBC on the Azure platform.

**Table 3-44: Mediant VE SBC on DS1_v2, D2ds_v5, D4ds_v5, D8ds_v5 - Transcoding Capacity**

| Session Coders | | Max. Sessions | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | DS1_v2 | | D2ds_v5 | | D4ds_v5 | | D8ds_v5 | |
| From Coder Profile | To Coder Profile | Basic | Extended | Basic | Extended | Basic | Extended | Basic | Extended |
| Profile 1 | Profile 1 | 200 | 200 | 300 | 175 | 600 | 375 | 1,800 | 1,175 |
| Profile 2 | Profile 1 | 100 | 100 | 150 | 125 | 325 | 250 | 975 | 775 |
| Profile 2 | Profile 2 | 75 | 50 | 100 | 75 | 225 | 175 | 675 | 575 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 100 | 100 | 100 | 75 | 200 | 175 | 600 | 525 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 75 | 50 | 75 | 50 | 150 | 125 | 475 | 425 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 25 | 25 | 25 | 25 | 50 | 50 | 200 | 175 |
| Profile 2 | Profile 2 + AMR-WB | 25 | 25 | 25 | 25 | 50 | 50 | 175 | 175 |
| Profile 1 | Profile 2 + SILK-NB | 100 | 75 | 75 | 75 | 175 | 175 | 575 | 525 |
| Profile 2 | Profile 2 + SILK-NB | 50 | 50 | 75 | 50 | 150 | 125 | 450 | 425 |
| Profile 1 | Profile 2 + SILK-WB | 50 | 50 | 50 | 50 | 100 | 100 | 325 | 300 |
| Profile 2 | Profile 2 + SILK-WB | 50 | 25 | 25 | 25 | 75 | 75 | 275 | 275 |
| Profile 1 | Profile 2 + Opus-NB | 50 | 50 | 50 | 50 | 100 | 100 | 350 | 300 |
| Profile 2 | Profile 2 + Opus-NB | 50 | 50 | 50 | 25 | 100 | 75 | 300 | 275 |
| Profile 1 | Profile 2 + Opus-WB | 50 | 25 | 50 | 25 | 100 | 75 | 300 | 250 |
| Profile 2 | Profile 2 + Opus-WB | 25 | 25 | 25 | 25 | 75 | 75 | 250 | 225 |

**Notes:**

- Azure DS_v2 virtual machine series in general and DS1_v2 virtual machine size in particular are scheduled for retirement in May 2028. Therefore, it’s recommended not to use them for new deployments, and to migrate existing deployments to the Dds_v5 (D2ds_v5, D4ds_v5, or D8ds_v5) virtual machine series.
- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

### 3.3.15.4 Mediant VE SBC for GCP

The following tables list maximum channel capacity for Mediant VE SBC on the GCP platform.

**Table 3-45: Mediant VE SBC on GCP - Transcoding Capacity**

| Session Coders | | n2-standard-2 | | n2-standard-4 | | n2-standard-8 | | n2-highcpu-32 | |
|---|---|---|---|---|---|---|---|---|---|
| From Coder Profile | To Coder | Basic | Extended | Basic | Extended | Basic | Extended | Basic | Extended |
| 1 | Profile 1 | 300 | 200 | 625 | 400 | 1900 | 1225 | 3600 | 3600 |
| 2 | Profile 1 | 150 | 125 | 325 | 275 | 1025 | 825 | 3600 | 3600 |
| 2 | Profile 2 | 100 | 100 | 225 | 200 | 700 | 625 | 3350 | 2925 |
| 1 | Profile 2 + AMR-NB / G.722 | 100 | 75 | 200 | 175 | 650 | 575 | 3075 | 2675 |
| 2 | Profile 2 + AMR-NB / G.722 | 75 | 75 | 150 | 150 | 500 | 450 | 2375 | 2175 |
| 1 | Profile 2 + AMR-WB | 25 | 25 | 50 | 50 | 200 | 200 | 1000 | 975 |
| 2 | Profile 2 + AMR-WB | 25 | 25 | 50 | 50 | 175 | 175 | 900 | 875 |
| 1 | Profile 2 + SILK-NB | 100 | 75 | 200 | 175 | 600 | 550 | 2900 | 2600 |
| 2 | Profile 2 + SILK-NB | 75 | 75 | 150 | 150 | 475 | 450 | 2275 | 2125 |
| 1 | Profile 2 + SILK-WB | 50 | 50 | 100 | 100 | 350 | 325 | 1650 | 1550 |

| Session Coders | | n2-standard-2 | | n2-standard-4 | | n2-standard-8 | | n2-highcpu-32 | |
|---|---|---|---|---|---|---|---|---|---|
| **From Coder Profile** | **To Coder** | **Basic** | **Extended** | **Basic** | **Extended** | **Basic** | **Extended** | **Basic** | **Extended** |
| 2 | Profile 2 + SILK-WB | 50 | 50 | 100 | 100 | 300 | 300 | 1425 | 1400 |
| 1 | Profile 2 + Opus-NB | 50 | 50 | 125 | 100 | 375 | 325 | 1775 | 1525 |
| 2 | Profile 2 + Opus-NB | 50 | 25 | 100 | 75 | 325 | 275 | 1525 | 1350 |
| 1 | Profile 2 + Opus-WB | 50 | 25 | 100 | 75 | 300 | 250 | 1475 | 1250 |
| 2 | Profile 2 + Opus-WB | 25 | 25 | 75 | 75 | 275 | 225 | 1275 | 1125 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

### 3.3.16 Mediant Server Edition (SE) SBC

**Note:** Digital signal processing (DSP) is supported only on Mediant SE SBC based on DL360 G10.

The maximum number of supported SBC sessions is listed in Section 3.1 on page 169. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

**Table 3-46: Mediant SE SBC (DL360 G10) - Transcoding Capacity per Coder Capability Profile**

| Session Coders | | Max. Sessions | |
|---|---|---|---|
| **From Coder Profile** | **To Coder Profile** | **Basic** | **Extended** |
| Profile 1 | Profile 1 | 9,600 | 6,625 |
| Profile 2 | Profile 1 | 4,400 | 3,625 |
| Profile 2 | Profile 2 | 2,875 | 2,500 |
| Profile 1 | Profile 2 + AMR-NB / G.722 | 2,925 | 2,600 |
| Profile 2 | Profile 2 + AMR-NB / G.722 | 2,150 | 1,950 |
| Profile 1 | Profile 2 + AMR-WB (G.722.2) | 950 | 925 |
| Profile 2 | Profile 2 + AMR-WB | 850 | 825 |
| Profile 1 | Profile 2 + SILK-NB | 2,750 | 2,500 |
| Profile 2 | Profile 2 + SILK-NB | 2,050 | 1,900 |
| Profile 1 | Profile 2 + SILK-WB | 1,575 | 1,475 |
| Profile 2 | Profile 2 + SILK-WB | 1,300 | 1,250 |
| Profile 1 | Profile 2 + Opus-NB | 1,700 | 1,450 |
| Profile 2 | Profile 2 + Opus-NB | 1,375 | 1,200 |
| Profile 1 | Profile 2 + Opus-WB | 1,375 | 1,200 |
| Profile 2 | Profile 2 + Opus-WB | 1,175 | 1,025 |

**Notes:**

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

### 3.3.16.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

**Table 3-47: Mediant SE SBC (DL360 G10) - Forwarding Capacity per Feature**

| Feature | Max. Sessions |
|---|---|
| Fax Detection | 45,000 |
| AD/AMD/Beep Detection | 45,000 |
| CP Detection | 45,000 |
| Jitter Buffer | 6,000 |

**Notes:**

- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

# 4 Configuration Table Capacity

The maximum rows (indices) that can be configured per configuration table is listed in the table below.

**Table 4-1: Capacity per Configuration Table**

| Configuration Table | Mediant<br>500 / 500L / 800 / 1000B / 3100<br>MP-1288 | Mediant<br>2600 / 4000B | Mediant<br>90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **Accounts** | ▪ MP-1288: 288<br>▪ Mediant 500 / 500L / 800 / 1000: 102<br>▪ Mediant 3100: 1,500 | 625 | 5,000 | ▪ 2-32 GB: 1,500<br>▪ 64 GB: 5,000 |
| **Allowed Audio Coders Groups** | 10<br>(20 for Mediant 3100) | 20 | 20 | 20 |
| **Allowed Video Coders Groups** | 5 | 5 | 5 | 5 |
| **Alternative Routing Reasons** | 20 | 20 | 20 | 20 |
| **Bandwidth Profile** | 486<br>(1,724 for Mediant 3100) | 1,009 | 1,884 | 1,884 |
| **Call Admission Control Profile** | 102 | 1,500 | 1,500 | 1,500 |
| **Call Admission Control Rule (per Profile)** | 8 | 8 | 8 | 8 |
| **Call Setup Rules** | ▪ MP-1288 / Mediant 1000/3100: 64<br>▪ Mediant 500/500L/800: 100 | 400 | 1,000 | ▪ 2-8 GB: 500<br>▪ 16-64 GB: 1,000 |
| **Calling Name Manipulation for IP-to-Tel Calls** | 120 | n/a<br>(Gateway only) | n/a<br>(Gateway only) | n/a<br>(Gateway only) |
| **Calling Name Manipulation for Tel-to-IP Calls** | 120 | n/a<br>(Gateway only) | n/a<br>(Gateway only) | n/a<br>(Gateway only) |
| **Char Conversion** | 40 | n/a<br>(Gateway only) | n/a<br>(Gateway only) | n/a<br>(Gateway only) |
| **Charge Codes** | 25 | n/a<br>(Gateway only) | n/a<br>(Gateway only) | n/a<br>(Gateway only) |
| **Classification** | 102<br>(1,500 for Mediant 3100) | 1,500 | 1,500 | ▪ 2 GB: 750<br>▪ 3.5-64 GB: 1,500 |
| **Coders Groups** | 11<br>(21 for Mediant 3100) | 21 | 21 | 21 |
| **Coders Groups > Coders** | 10<br>(per Coders Group) | 10<br>(per Coders Group) | 10<br>(per Coders Group) | 10<br>(per Coders Group) |

| Configuration Table | Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288 | Mediant 2600 / 4000B | Mediant 90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **Cost Groups** | 10 | 10 | 10 | 10 |
| **Custom DNS Servers** | n/a | n/a | 32 (Mediant SE) | 32 |
| **Custom MTU** | n/a | n/a | 16 (Mediant SE) | 16 |
| **Destination Phone Number Manipulation for IP-to-Tel Calls** | 120 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Destination Phone Number Manipulation for Tel-to-IP Calls** | 120 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **DHCP Servers** | 1 | 1 | 1 | 1 |
| **Dial Plan** | 10<br>Except:<br>25 for Mediant 3100 | 25 | 50 | 50 |
| **Dial Plan Rule** | 2,000<br>Except:<br>Mediant 3100: 10,000 | 10,000 | 100,000 | ▪ < 16 GB: 2,000<br>▪ ≥ 16 GB: 100,000 |
| **Ethernet Devices** | 16<br>Except:<br>▪ Mediant 3100: 1,024<br>▪ Mediant 500/800: 14 | 1,024 | 1,024 | 1,024 |
| **External Media Source** | 1 | 1 | 1 | 1 |
| **Firewall** | 50<br>Except:<br>Mediant 3100: 500 | 500 | 500 | 500 |
| **Forward On Busy Trunk Destination** | ▪ MP-1288: 288<br>▪ Mediant 500/500L/800: 100<br>▪ Mediant 1000: 240<br>▪ Mediant 3100: 512 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Gateway CDR Format** | 128 Syslog; 40 RADIUS (128 for Mediant 3100); 64 Locally Stored & JSON | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **HA Network Monitor** | 10 | 10 | 10 | 10 |
| **HTTP Directive Sets** | 30 | 30 | 30 | 30 |
| **HTTP Directives** | 500 | 500 | 500 | 500 |
| **HTTP Locations** | 40 | 40 | 120 | ▪ < 8 GB: 40<br>▪ ≥ 8 GB: 120 |
| **HTTP Proxy Servers** | 10 | 10 | 40 | ▪ < 8 GB: 10<br>▪ ≥ 8 GB: 40 |

| Configuration Table | Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288 | Mediant 2600 / 4000B | Mediant 90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **HTTP Remote Hosts** | 10 (per Remote Web Service) | 10 (per Remote Web Service) | 10 (per Remote Web Service) | 10 (per Remote Web Service) |
| **IDS Matches** | 20 | 20 | 20 | 20 |
| **IDS Policies** | 20 | 20 | 20 | 20 |
| **IDS Rule** | 100 (20 per Policy) | 100 (20 per Policy) | 100 (20 per Policy) | 100 (20 per Policy) |
| **Inbound Manipulations** | 205<br>Except:<br>Mediant 3100: 3,000 | 3,000 | 3,000 | 3,000 |
| **Internal DNS** | 20 | 20 | 20 | 20 |
| **Internal SRV** | 10 | 10 | 10 | 10 |
| **IP Group Set** | 51<br>Except:<br>Mediant 3100: 350 | 350 | 2,500 | ▪ 2 GB: 40<br>▪ 3.5 GB: 500<br>▪ 4-16 GB: 750<br>▪ 32-64 GB: 2,500 |
| **IP Groups** | 80<br>Except:<br>Mediant 3100: 700 | 700 | 5,000 | ▪ 2 GB: 80<br>▪ 3.5 GB: 1,000<br>▪ 4-16 GB: 1,500<br>▪ 32-64 GB: 5,000 |
| **IP Interfaces** | 16<br>Except:<br>Mediant 3100: 1,024 | 1,024 | 1,024 | 1,024 |
| **IP Profiles** | ▪ MP-1288/Mediant 500/500L/800: 20<br>▪ Mediant 1000: 40<br>▪ Mediant 3100: 300 | 300 | ▪ Mediant 9030: 300<br>▪ Mediant 9000/9080 /SE: 1,500 | ▪ 2 GB: 150<br>▪ 5-32 GB: 300<br>▪ 64 GB: 1,500 (5,000 if License Key includes VoiceAI Connect) |
| **IP-to-IP Routing** | 615<br>Except:<br>Mediant 3100: 9,000 | 9,000 | 9,000 | ▪ 2 GB: 4,500<br>▪ 3.5-64 GB: 9,000 |
| **IP-to-Tel Routing** | 120<br>Except:<br>MP-1288: 288 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **LDAP Server Groups** | 41<br>Except:<br>Mediant 3100: 600 | 600 | 600 | 600 |
| **LDAP Servers** | 82<br>Except:<br>Mediant 3100: 1,200 | 1,200 | 1,200 | 1,200 |
| **Local Users** | 20 | 20 | 20 | 20 |

| Configuration Table | Mediant<br>500 / 500L / 800 / 1000B / 3100<br>MP-1288 | Mediant<br>2600 / 4000B | Mediant<br>90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **Logging Filters** | 60 | 60 | 60 | 60 |
| **Login OAuth Servers** | 1 | 1 | 1 | 1 |
| **Malicious Signature** | 20 | 20 | 20 | 20 |
| **Management Access List** | 50 | 50 | 50 | 50 |
| **Media Realm Extension** | ▪ MP-1288 / Mediant 500/500L/800: 2 x Max. Media Realms<br>▪ Mediant 3100: 5 x Max. Media Realms | ▪ Mediant 2600: 2 x max. Media Realms<br>▪ Mediant 4000B: 5 x max. Media Realms | 5 x Max. Media Realms | 5 x Max. Media Realms |
| **Media Realms** | 12<br>Except:<br>Mediant 3100: 1,024 | 1,024 | 1,024 | 1,024 |
| **Message Conditions** | 82<br>Except:<br>Mediant 3100: 1,200 | 1,200 | 1,200 | 1,200 |
| **Message Manipulations** | ▪ MP-1288 / Mediant 500/500L/800: 100<br>▪ Mediant 1000: 200<br>▪ Mediant 3100: 500 | 500 | 500 | 500 |
| **Message Policies** | 20 | 20 | 20 | 20 |
| **NAT Translation** | 32 | 32 | 32 | 32 |
| **OAuth Servers** | 1 | 1 | 1 | 1 |
| **Outbound Manipulations** | 205<br>Except:<br>Mediant 3100: 3,000 | 3,000 | 3,000 | 3,000 |
| **OVOC Services** | 1 | 1 | 1 | 1 |
| **Phone Contexts** | 20 | n/a<br>(Gateway only) | n/a<br>(Gateway only) | n/a<br>(Gateway only) |
| **Pre-Parsing Manipulation Rules** | 30 | 30 | 30 | 30 |
| **Pre-Parsing Manipulation Sets** | 10 | 10 | 10 | 10 |
| **Proxy Sets** | 80<br>Except:<br>Mediant 3100: 700 | 700 | 5,000 | ▪ 2 GB: 80<br>▪ 3.5 GB: 1,000<br>▪ 4-16 GB: 1,500<br>▪ 32-64 GB: 5,000 |
| **Proxy Sets > Proxy Address** (per Proxy Set) | 10 | 10 | 50 | ▪ 2 GB: 10<br>▪ 3.5 GB: 10 |

| Configuration Table | Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288 | Mediant 2600 / 4000B | Mediant 90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| | | | | ▪ 8-16 GB: 10<br>▪ 32-64 GB: 50 |
| **Proxy Sets** > **Proxy Address** (DNS-resolved IP addresses per Proxy Set) | 15 | 15 | 50 | ▪ 2 GB: 15<br>▪ 3.5 GB: 15<br>▪ 8-16 GB: 50<br>▪ 32-64 GB: 50 |
| **Proxy Sets** > **Proxy Address** (DNS-resolved IP addresses for all Proxy Sets combined) | 500 | 2,100 | 20,000 | ▪ 2 GB: 500<br>▪ 3.5 GB: 3,000<br>▪ 4 GB: 4,500<br>▪ 8-16 GB: 6,000 (20,000 for VAIC feature)<br>▪ 32-64 GB: 20,000 |
| **QoS Mapping** | 64 | 64 | 64 | 64 |
| **Quality of Experience Color Rules** | 256 | 256 | 256 | 256 |
| **Quality of Experience Profile** | 256 | 256 | 256 | 256 |
| **Quality Of Service Rules** | 510<br>Except:<br>Mediant 3100: 3,500 | 3,500 | 7,500 | 7,500 |
| **RADIUS Servers** | 3 | 3 | 3 | 3 |
| **Reasons for IP-to-Tel Alternative Routing** | 10 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Reasons for Tel-to-IP Alternative Routing** | 10 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Redirect Number IP-to-Tel** | 20 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Redirect Number Tel-to-IP** | 20 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Release Cause ISDN->ISDN** | 10 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Release Cause Mapping from ISDN to SIP** | 12 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Release Cause Mapping from SIP to ISDN** | 12 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Remote Media Subnet** | 5 | 5 | 5 | 5 |

| Configuration Table | Mediant<br>500 / 500L / 800 / 1000B / 3100<br>MP-1288 | Mediant<br>2600 / 4000B | Mediant<br>90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **Remote Web Services** | 7 | 7 | 7 | 7 |
| **Routing Policies (SBC)** | 20<br>Except:<br>Mediant 3100: 600 | 600 | 600 | ▪ 2 GB: 20<br>▪ 3.5 GB: 70<br>▪ 4 GB: 100<br>▪ 8 GB: 200<br>▪ 16 GB: 400<br>▪ 32-64 GB: 600 |
| **Routing Policies (Gateway)** | 1 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **RTP-Only** | n/a | n/a | 3,000 (Mediant SE) | 3,000 |
| **SBC CDR Format** | 128 Syslog; 40 RADIUS (128 for Mediant 3100); 64 Locally Stored & JSON | 128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON) | 128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON) | 128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON) |
| **SBC User Information** | ▪ Mediant 500: 1,600<br>▪ Mediant 500L/800: 2,000<br>▪ Mediant 1000: 800<br>▪ Mediant 3100: 20,000<br>▪ MP-1288: 350 | 20,000 | 50,000 | ▪ 2 GB: 1,000<br>▪ 3-4 GB: 3,000<br>▪ 8 GB: 20,000<br>▪ 16-64 GB: 50,000 |
| | **Note:** The device limits the maximum number of users that can use a TLS connection: | | | |
| | ▪ Mediant 500: 300<br>▪ Mediant 500L: 100<br>▪ Mediant 800: 300<br>▪ Mediant 1000: 300<br>▪ Mediant 3100: 6,000<br>▪ MP-1288: 350 | 1,000 | 25,000 | ▪ 2 GB: 100<br>▪ 3 GB: 500<br>▪ 4 GB: 5,000<br>▪ 8-16 GB: 6,000<br>▪ 32 GB: 16,000<br>▪ 64 GB: 25,000 |
| **SIP Interfaces** | 80<br>Except:<br>Mediant 3100: 1,200 | 700 | 1,200 | ▪ 2 GB: 40<br>▪ 3 GB: 200<br>▪ 4 GB: 400<br>▪ 8 GB: 800<br>▪ 16 GB: 1,200<br>▪ 32-64 GB: 1,200 |
| **SIP Recording Rules** | 30 | 30 | 50 | 50 |
| **SNI-to-TLS Mapping** | 12<br>Except:<br>▪ Mediant 1000: 15<br>▪ Mediant 3100: 100 | 100 | 100 | 100 |
| **SNMP Trap Destinations** | 5 | 5 | 5 | 5 |
| **SNMP Trusted Managers** | 5 | 5 | 5 | 5 |
| **SNMPv3 Users** | 10 | 10 | 10 | 10 |

| Configuration Table | Mediant<br>500 / 500L / 800 / 1000B / 3100<br>MP-1288 | Mediant<br>2600 / 4000B | Mediant<br>90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
| **Source Phone Number Manipulation for IP-to-Tel Calls** | 120 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Source Phone Number Manipulation for Tel-to-IP Calls** | 120 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **SRDs** | 20<br>Except:<br>Mediant 3100: 600 | 600 | 600 | ▪ 2 GB: 20<br>▪ 3.5 GB: 70<br>▪ 4 GB: 100<br>▪ 8 GB: 200<br>▪ 16 GB: 400<br>▪ 32-64 GB: 600 |
| **SSH Interfaces** | 16 | 16 | 16 | 16 |
| **Static Routes** | 30 | 30 | 30 | 30 |
| **Supplementary Services** | 100 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Syslog Servers** | 4 | 4 | 4 | 4 |
| **TCP/UDP Proxy Servers** | 10 | 10 | 10 | 10 |
| **Tel Profiles** | 9<br>Except:<br>Mediant 3100: 40 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Tel-to-IP Routing** | 180 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Telnet Interfaces** | 16 | 16 | 16 | 16 |
| **Test Call Rules** | 5 (default) | 5 (default) | 5 (default) | 5 (default) |
| **Time Band** | 70 (21 per Cost Group) | 70 (21 per Cost Group) | 70 (21 per Cost Group) | 70 (21 per Cost Group) |
| **TLS Contexts** | ▪ MP-1288 / Mediant 500/500L/800: 12<br>▪ Mediant 1000: 15<br>▪ Mediant 3100: 100 | 100 | 100 | 100 |
| **Tone Index** | 50 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Trunk Group** | ▪ MP-1288: 288<br>▪ Mediant 500/500L/800: 24<br>▪ Mediant 1000: 240<br>▪ Mediant 3100: 512 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |
| **Trunk Group Settings** | ▪ MP-1288: 289<br>▪ Mediant 500/500L/800: 101 | n/a (Gateway only) | n/a (Gateway only) | n/a (Gateway only) |

| Configuration Table | Mediant<br>500 / 500L / 800 / 1000B / 3100<br>MP-1288 | Mediant<br>2600 / 4000B | Mediant<br>90xx / SE | Mediant VE / CE |
|---|---|---|---|---|
|  | ▪ Mediant 1000: 241<br>▪ Mediant 3100: 512 |  |  |  |
| **Upstream Groups** | 10 | 10 | 10 | 10 |
| **Upstream Hosts** | 50 (5 per Upstream Group) | 50 (5 per Upstream Group) | 50 (5 per Upstream Group) | 50 (5 per Upstream Group) |
| **Weak Passwords List** | 150 | 150 | 150 | 150 |
| **Web Interfaces** | 20 | 20 | 20 | 20 |

# 5 Supported SIP Standards

This section lists SIP RFCs and standards supported by the device.

## 5.1 Supported SIP RFCs

The table below lists the supported RFCs.

**Table 5-1: Supported RFCs**

| RFC | Description | Gateway | SBC |
|---|---|---|---|
| draft-choudhuri-sip-info-digit-00 | SIP INFO method for DTMF digit transport and collection | √ | √ |
| draft-ietf-bfcpbis-rfc4583bis-12 | Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams | × | √ (forwarded transparently) |
| draft-ietf-sip-connect-reuse-06 | Connection Reuse in SIP | √ | √ |
| draft-ietf-sipping-cc-transfer-05 | Call Transfer | √ | √ |
| draft-ietf-sipping-realtimefax-01 | SIP Support for Real-time Fax: Call Flow Examples | √ | √ (forwarded transparently) |
| draft-ietf-sip-privacy-04.txt | SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header | √ | √ |
| draft-johnston-sipping-cc-uui-04 | Transporting User to User Information for Call Centers using SIP | √ | √ (forwarded transparently) |
| draft-levy-sip-diversion-08 | Diversion Indication in SIP | √ | √ |
| draft-mahy-iptel-cpc-06 | The Calling Party's Category tel URI Parameter | √ | √ (forwarded transparently) |
| draft-mahy-sipping-signaled-digits-01 | Signaled Telephony Events in the Session Initiation Protocol | √ | √ |
| draft-sandbakken-dispatch-bfcp-udp-03 | Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport | × | √ (forwarded transparently) |
| ECMA-355, ISO/IEC 22535 | QSIG tunneling | √ | √ (forwarded transparently) |
| RFC 2327 | SDP | √ | √ |
| RFC 2617 | HTTP Authentication: Basic and Digest Access Authentication | √ | √ |
| RFC 2782 | A DNS RR for specifying the location of services | √ | √ |
| RFC 2833 | Telephone event | √ | √ |
| RFC 2976 | SIP INFO Method | √ | √ |
| RFC 3261 | SIP | √ | √ |

| RFC | Description | Gateway | SBC |
|---|---|---|---|
| RFC 3262 | Reliability of Provisional Responses | √ | √ |
| RFC 3263 | Locating SIP Servers | √ | √ |
| RFC 3264 | Offer/Answer Model | √ | √ |
| RFC 3265 | (SIP)-Specific Event Notification | √ | √ |
| RFC 3310 | Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) | √ | × |
| RFC 3311 | UPDATE Method | √ | √ |
| RFC 3323 | Privacy Mechanism | √ | √ |
| RFC 3325 | Private Extensions to the SIP for Asserted Identity within Trusted Networks | √ | √ |
| RFC 3326 | Reason header | √ | √ (forwarded transparently) |
| RFC 3327 | Extension Header Field for Registering Non-Adjacent Contacts | √ | × |
| RFC 3361 | DHCP Option for SIP Servers | √ | × |
| RFC 3362 | Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration | √ | √ |
| RFC 3372 | SIP-T | √ | √ (forwarded transparently) |
| RFC 3389 | RTP Payload for Comfort Noise | √ | √ (forwarded transparently) |
| RFC 3420 | Internet Media Type message/sipfrag | √ | √ |
| RFC 3455 | P-Associated-URI | √ | √ (using user info \ account) |
| RFC 3489 | STUN - Simple Traversal of UDP | √ | √ |
| RFC 3515 | Refer Method | √ | √ |
| RFC 3550 | RTP: A Transport Protocol for Real-Time Applications | √ | √ |
| RFC 3578 | Interworking of ISDN overlap signalling to SIP | √ | × |
| RFC 3581 | Symmetric Response Routing - rport | √ | √ |
| RFC 3605 | RTCP attribute in SDP | √ | √ (forwarded transparently) |
| RFC 3608 | SIP Extension Header Field for Service Route Discovery During Registration | √ | × |
| RFC 3611 | RTCP-XR | √ | √ |
| RFC 3665 | SIP Basic Call Flow Examples | √ | √ |
| RFC 3666 | SIP to PSTN Call Flows | √ | √ (forwarded transparently) |
| RFC 3680 | A SIP Event Package for Registration (IMS) | √ | × |

| RFC | Description | Gateway | SBC |
|---|---|---|---|
| RFC 3711 | The Secure Real-time Transport Protocol (SRTP) | √ | √ |
| RFC 3725 | Third Party Call Control | √ | √ |
| RFC 3824 | Using E.164 numbers with SIP (ENUM) | √ | √ |
| RFC 3842 | MWI | √ | √ |
| RFC 3891 | "Replaces" Header | √ | √ |
| RFC 3892 | The SIP Referred-By Mechanism | √ | √ |
| RFC 3903 | SIP Extension for Event State Publication | √ | √ |
| RFC 3911 | The SIP Join Header | Partial | × |
| RFC 3960 | Early Media and Ringing Tone Generation in SIP | Partial | √ |
| RFC 3966 | The tel URI for Telephone Numbers | √ | √ |
| RFC 4028 | Session Timers in the Session Initiation Protocol | √ | √ |
| RFC 4040 | RTP payload format for a 64 kbit/s transparent call - Clearmode | √ | √ (forwarded transparently) |
| RFC 4117 | Transcoding Services Invocation | √ | × |
| RFC 4168 | The Stream Control Transfer Protocol (SCTP) as a Transport for SIP | × | √ |
| RFC 4235 | Dialog Event Package | Partial | Partial |
| RFC 4240 | Basic Network Media Services with SIP - NetAnn | √ | √ (forwarded transparently) |
| RFC 4244 | An Extension to SIP for Request History Information | √ | √ |
| RFC 4320 | Actions Addressing Identified Issues with SIP Non-INVITE Transaction | √ | √ |
| RFC 4321 | Problems Identified Associated with SIP Non-INVITE Transaction | √ | √ |
| RFC 4411 | Extending SIP Reason Header for Preemption Events | √ | √ (forwarded transparently) |
| RFC 4412 | Communications Resource Priority for SIP | √ | √ (forwarded transparently) |
| RFC 4458 | SIP URIs for Applications such as Voicemail and Interactive Voice Response | √ | √ (forwarded transparently) |
| RFC 4475 | SIP Torture Test Messages | √ | √ |
| RFC 4497 or ISO/IEC 17343 | Interworking between SIP and QSIG | √ | √ (forwarded transparently) |
| RFC 4566 | Session Description Protocol | √ | √ |
| RFC 4568 | SDP Security Descriptions for Media Streams for SRTP | √ | √ |
| RFC 4582 | The Binary Floor Control Protocol (BFCP) | × | √ (forwarded transparently) |

| RFC | Description | Gateway | SBC |
|---|---|---|---|
| RFC 4715 | Interworking of ISDN Sub Address to sip isub parameter | √ | √ (forwarded transparently) |
| RFC 4730 | A SIP Event Package for Key Press Stimulus (KPML) | Partial | × |
| RFC 4733 | RTP Payload for DTMF Digits | √ | √ |
| RFC 4904 | Representing trunk groups in tel/sip URIs | √ | √ (forwarded transparently) |
| RFC 4960 | Stream Control Transmission Protocol | × | √ |
| RFC 4961 | Symmetric RTP and RTCP for NAT | √ | √ |
| RFC 4975 | The Message Session Relay Protocol (MSRP) | × | √ |
| RFC 5022 | Media Server Control Markup Language (MSCML) | √ | × |
| RFC 5079 | Rejecting Anonymous Requests in SIP | √ | √ |
| RFC 5627 | Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP | √ | √ (forwarded transparently) |
| RFC 5628 | Registration Event Package Extension for GRUU | √ | × |
| RFC 5806 | Diversion Header, same as draft-levy-sip-diversion-08 | √ | √ |
| RFC 5853 | Requirements from SIP / SBC Deployments | - | √ |
| RFC 6035 | SIP Package for Voice Quality Reporting Event, using sip PUBLISH | √ | √ |
| RFC 6135 | An Alternative Connection Model for the Message Session Relay Protocol (MSRP) | × | √ |
| RFC 6140 | Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP) | √ | √ |
| RFC 6337 | Session Initiation Protocol (SIP) Usage of the Offer/Answer Model | - | √ |
| RFC 6341 | Use Cases and Requirements for SIP-Based Media Recording<br>(Session Recording Protocol - draft-ietf-siprec-protocol-02, and Architecture - draft-ietf-siprec-architecture-03) | √ | √ |
| RFC 6442 | Location Conveyance for the Session Initiation Protocol | - | √ |
| RFC 7245 | An Architecture for Media Recording Using the Session Initiation Protocol | √ | √ |
| RFC 7261 | Offer/Answer Considerations for G723 Annex A and G729 Annex B | √ | √ |
| RFC 7865 | Session Initiation Protocol (SIP) Recording Metadata | √ | √ |
| RFC 7866 | Session Recording Protocol | √ | √ |
| RFC 8068 | Session Initiation Protocol (SIP) Recording Call Flows | √ | √ |

## 5.2 SIP Message Compliancy

The SIP device complies with RFC 3261, as shown in the following subsections.

### 5.2.1 SIP Functions

The device supports the following SIP Functions:

**Table 5-2: Supported SIP Functions**

| Function | Comments |
|---|---|
| User Agent Client (UAC) | - |
| User Agent Server (UAS) | - |
| Proxy Server | The device supports working with third-party Proxy Servers such as Nortel CS1K/CS2K, Avaya, Microsoft OCS, Alcatel, 3Com, BroadSoft, Snom, Cisco and many others |
| Redirect Server | The device supports working with third-party Redirection servers |
| Registrar Server | The device supports working with third-party Registration servers |

### 5.2.2 SIP Methods

The device supports the following SIP Methods:

**Table 5-3: Supported SIP Methods**

| Method | Comments |
|---|---|
| ACK | - |
| BYE | - |
| CANCEL | - |
| INFO | - |
| INVITE | - |
| MESSAGE | Supported only by the SBC application and send only |
| NOTIFY | - |
| OPTIONS | - |
| PRACK | - |
| PUBLISH | Send only |
| REFER | Inside and outside of a dialog |
| REGISTER | Send only for Gateway application; send and receive for SBC application |
| SUBSCRIBE | - |
| UPDATE | - |

### 5.2.3 SIP Headers

The device supports the following SIP headers:

**Table 5-4: Supported SIP Headers**

| SIP Header | SIP Header |
|---|---|
| Accept | Proxy- Authenticate |
| Accept–Encoding | Proxy- Authorization |
| Alert-Info | Proxy- Require |
| Allow | Prack |
| Also | Reason |
| Asserted-Identity | Record- Route |
| Authorization | Refer-To |
| Call-ID | Referred-By |
| Call-Info | Replaces |
| Contact | Require |
| Content-Disposition | Remote-Party-ID |
| Content-Encoding | Response- Key |
| Content-Length | Retry-After |
| Content-Type | Route |
| Cseq | Rseq |
| Date | Session-Expires |
| Diversion | Server |
| Expires | Service-Route |
| Fax | SIP-If-Match |
| From | Subject |
| History-Info | Supported |
| Join | Target-Dialog |
| Max-Forwards | Timestamp |
| Messages-Waiting | To |
| MIN-SE | Unsupported |
| P-Associated-URI | User- Agent |
| P-Asserted-Identity | Via |
| P-Charging-Vector | Voicemail |
| P-Preferred-Identity | Warning |
| Priority | WWW- Authenticate |
| Privacy | - |

**Note:** The following SIP headers are not supported:

- Encryption
- Organization

## 5.2.4 SDP Fields

The device supports the following SDP fields:

**Table 5-5: Supported SDP Fields**

| SDP Field | Name |
|---|---|
| v= | Protocol version number |
| o= | Owner/creator and session identifier |
| a= | Attribute information |
| c= | Connection information |
| d= | Digit |
| m= | Media name and transport address |
| s= | Session information |
| t= | Time alive header |
| b= | Bandwidth header |
| u= | URI description header |
| e= | Email address header |
| i= | Session info header |
| p= | Phone number header |
| y= | Year |

## 5.2.5 SIP Responses

The device supports the following SIP responses:

**Table 5-6: Supported SIP Responses**

| Response Type | | Comments |
|---|---|---|
| **1xx Response (Information Responses)** | | |
| 100 | Trying | The device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling. |
| 180 | Ringing | The device generates this response for an incoming INVITE message. Upon receiving this response, the device waits for a 200 OK response. |
| 181 | Call is Being Forwarded | The device doesn't generate these responses. However, the device does receive them. The device processes these responses the same way that it processes the 100 Trying response. |

| Response Type | | Comments |
|---|---|---|
| 182 | Queued | The device generates this response in Call Waiting service. When the SIP device receives a 182 response, it plays a special waiting Ringback tone to the telephone side. |
| 183 | Session Progress | The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP |
| **2xx Response (Successful Responses)** | | |
| 200 | OK | |
| 202 | Accepted | |
| 204 | No Notification | |
| **3xx Response (Redirection Responses)** | | |
| 300 | Multiple Choice | The device responds with an ACK, and then resends the request to the first new address in the contact list. |
| 301 | Moved Permanently | The device responds with an ACK, and then resends the request to the new address. |
| 302 | Moved Temporarily | The device generates this response when call forward is used to redirect the call to another destination. If such a response is received, the calling device initiates an INVITE message to the new destination. |
| 305 | Use Proxy | The device responds with an ACK, and then resends the request to a new address. |
| 380 | Alternate Service | The device responds with an ACK, and then resends the request to a new address. |
| **4xx Response (Client Failure Responses)** | | |
| 400 | Bad Request | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 401 | Unauthorized | Authentication support for Basic and Digest. Upon receipt of this message, the device issues a new request according to the scheme received on this response. |
| 402 | Payment Required | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 403 | Forbidden | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 404 | Not Found | The device generates this response if it is unable to locate the callee. Upon receiving this response, the device notifies the User with a Reorder Tone. |
| 405 | Method Not Allowed | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 406 | Not Acceptable | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |

| Response Type | | Comments |
|---|---|---|
| 407 | Proxy Authentication Required | Authentication support for Basic and Digest. Upon receipt of this message, the device issues a new request according to the scheme received on this response. |
| 408 | Request Timeout | The device generates this response if the no-answer timer expires. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 409 | Conflict | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 410 | Gone | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 411 | Length Required | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 413 | Request Entity Too Large | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 415 | Unsupported Media | If the device receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone.<br>The device generates this response in case of SDP mismatch. |
| 420 | Bad Extension | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 423 | Interval Too Brief | The device does not generate this response. Upon receipt of this message the device uses the value received in the Min-Expires header as the registration time. |
| 424 | Bad Location Information | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 428 | Use Identity Header | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 429 | Provide Referrer Identity | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 433 | Anonymity Disallowed | If the device receives a 433 Anonymity Disallowed, it sends a DISCONNECT message to the PSTN with a cause value of 21 (Call Rejected). In addition, the device can be configured, using the Release Reason Mapping, to generate a 433 response when any cause is received from the PSTN side. |
| 436 | Bad Identity Info | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 437 | Unsupported Credential | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |

| Response Type | | Comments |
|---|---|---|
| 438 | Invalid Identity Header | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 439 | First Hop Lacks Outbound Support | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 440 | Max-Breadth Exceeded | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 470 | Consent Needed | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 480 | Temporarily Unavailable | If the device receives this response, it notifies the User with a Reorder Tone. This response is issued if there is no response from remote. |
| 481 | Call Leg/Transaction Does Not Exist | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 482 | Loop Detected | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 483 | Too Many Hops | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 484 | Address Incomplete | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 485 | Ambiguous | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 486 | Busy Here | The SIP device generates this response if the called party is off-hook and the call cannot be presented as a call waiting call. Upon receipt of this response, the device notifies the User and generates a busy tone. |
| 487 | Request Canceled | This response indicates that the initial request is terminated with a BYE or CANCEL request. |
| 488 | Not Acceptable | The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call. |
| 491 | Request Pending | When acting as a UAS: the device sent a re-INVITE on an established session and is still in progress. If it receives a re-INVITE on the same dialog, it returns this response to the received INVITE.<br>When acting as a UAC: If the device receives this response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again. |

| Response Type | | Comments |
|---|---|---|
| **5xx Response (Server Failure Responses)** | | |
| 500 | Internal Server Error | Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side. The device generates a 5xx response according to the PSTN release cause coming from the PSTN. |
| 501 | Not Implemented | |
| 502 | Bad gateway | |
| 503 | Service Unavailable | |
| 504 | Gateway Timeout | |
| 505 | Version Not Supported | |
| **6xx Response (Global Responses)** | | |
| 600 | Busy Everywhere | Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side. |
| 603 | Decline | |
| 604 | Does Not Exist Anywhere | |
| 606 | Not Acceptable | |

**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

Document #: LTRT-27765