Release Notes

AudioCodes SBC and Media Gateway Series

Session Border Controllers Analog & Digital Media Gateways

Long Term Support (LTS) Releases

Version 7.40A.251 / 7.40A.250

The 7.40A.250/251 stream will continue to be supported until May 2024. After this date, no further scheduled maintenance releases or fixes will be provided for this stream. For the latest LTS versions, refer to the SBC-Gateway Release Notes for Long Term Support (LTS) Versions 7.40A.500.

SBC

audiocodes

Table of Contents

List of Tables

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: May-12-2024

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 Hardware Installation Manual
MP-1288 High-Density Analog Media Gateway User's Manual
Mediant 3100 Gateway & E-SBC User's Manual
Mediant 3100 Gateway & E-SBC Hardware Installation Manual

Document Name
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 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
27721	Registered users capacity updated for Mediant VE Hyper-V 4 vCPU; Mediant 800C non-hybrid SBC capacity updated
27718	Ver. 7.40A.251.524; Mediant 800C SRTP capacity updated (250)
27711	Ver. 7.40A.251.461
27708	MSRP capacity; enabling transcoding capability statement
27699	Ver. 7.40A.251.364; capacity typo for Mediant CE on AWS EC2 (m5.large capacity)
27697	Ver. 7.40A.251.287
27696	Ver. 7.40A.251.284
27695	Ver. 7.40A.251.283
27692	Ver. 7.40A.251.149 (returned)
27688	Ver. 7.40A.251.150 (replaced 7.40A.251.149)
27687	Ver. 7.40A.251.149
27685	Ver. 7.40A.251.147
27682	Ver. 7.40A.251.041
27681	Note for AWS instance support for Mediant VE/CE
27679	Ver. 7.40A.251.035
27675	Mediant 3100 gateway capacity updated
27674	Ver. 7.40A.251.026
27669	Ver. 7.40A.250.931
27664	Ver. 7.40A.250.926
27660	Ver. 7.40A.250.908 and 7.40A.250.851
27654	Ver. 7.40A.250.836
27651	Proxy Sets capacity updated; note updated for 7.2-to-7.4 upgrade

LTRT	Description
27646	Ver. 7.40A.250.754; Mediant VE AWS / EC2 capacity; Mediant CE registered agents capacity
27642	Ver. 7.40A.250.611
27638	Ver. 7.40A.250.609
27633	Ver. 7.40A.250.364 and 7.40A.250.366
27632	Ver. 7.40A.250.541
27629	Ver. 7.40A.250.528; Access List table and Proxy Sets table capacity
27625	Ver. 7.40A.250.440; IP Interfaces table capacity update
27622	Ver. 7.40A.250.363
27599	Ver. 7.40A.250.270; Mediant 3100 transcoding capacity table updated; Proxy Sets table capacity updated
27596	Ver. 7.40A.250.265
27595	Known constraints added to Ver. 7.40A.250.262; SBC User Information table capacity added; SBC-36042 added to resolved constraints.
27594	Ver. 7.40A.250.262
27592	Ver. 7.40A.250.255 (initial LTS version); new feature added to Ver. 7.40A.002.007 - SC Local Users Table Synchronized with MT.
27591	Ver. 7.40A.005.619; SBC-35373 added to Ver. 7.40A.250.010
27590	Typo (7.40A.250.010 instead of 7.40A.250.008); SBC-35748 fixe bug added
27589	Ver. 7.40A.250.008
27587	Web URL fixes; capacity for Azure DS3_v2 / D8s_v3/v4
27584	Ver. 7.40A.250.004
27581	Ver. 7.40A.250.001
27576	Ver. 7.40A.200.018
27575	Ver. 7.40A.100.338
27573	Ver. 7.40A.100.336
27572	Ver. 7.40A.200.015 (replaced Ver. 7.40A.200.05 - typo)
27570	Ver. 7.40A.200.05
27566	Ver. 7.40A.100.239; known constraint added to Ver. 7.40A.100.238
27564	Ver. 7.40A.100.238
27562	Ver. 7.40A.100.233
27554	Ver. 7.40A.005.613; configuration table capacity updates
27552	Ver. 7.40A.100.114
27546	Ver. 7.40A.100.011 and Ver. 7.40A.100.021
27542	Ver. 7.40A.005.509; new CRMX module feature (added to 7.40A.002.007)
27538	Typo (version number); updates to Ver. 7.40A.005.314 – feature Syslog Messages to Serial Console and constraint SBC-27180

LTRT	Description
27537	Typo (version number)
27534	Telnet-SNMP feature added to Ver. 7.40A.005.313
27530	Ver. 7.40A.005.313; Mediant 2600/4000 removed from persistent logging feature.
27518	Mediant 800A removed
27517	Mediant 800C hybrid capacity table updated
27513	Typo (cross-reference).
27509	Typo (Proxy Sets table capacity).
27503	DoS and DDoS protection and Wireshark plugins features added to Ver. 7.4; note updated for Mediant CE VMware re MCProfile.
27496	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. You can check for an updated document 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.251.524 (7.4.250-14)	April 2, 2024
7.40A.251.461 (7.4.250-13)	February 21, 2024
7.40A.251.364 (7.4.250-12)	December 13, 2023
7.40A.251.287 (7.4.250-11-02)	November 27, 2023
7.40A.251.284 (7.4.250-11-01)	November 13, 2023
7.40A.251.283 (7.4.250-11)	October 26, 2023
7.40A.251.150 (7.4.250-10-02)	September 11, 2023
7.40A.251.149 (7.4.250-10-01)	August 29, 2023
7.40A.251.147 (7.4.250-10)	August 23, 2023
7.40A.251.041 (7.4.250-9.02)	August 8, 2023
7.40A.251.035 (7.4.250-9.01)	July 17, 2023
7.40A.251.026 (7.4.250-9)	June 27, 2023
7.40A.250.931 (7.4.250-8.02)	June 4, 2023
7.40A.250.926 (7.4.250-8.01)	May 10, 2023

LTS Version	Released Date
7.40A.250.908 (7.4.250-8)	April 24, 2023
7.40A.250.851 (7.4.250-7.01)	March 28, 2023
7.40A.250.836 (7.4.250-7)	March 8, 2023
7.40A.250.754 (7.4.250-6)	January 31, 2023
7.40A.250.611 (7.4.250-5.01)	December 1, 2022
7.40A.250.609 (7.4.250-5)	November 17, 2022
7.40A.250.541 (7.4.250-4.01)	September 22, 2022
7.40A.250.366 (7.4.250-2.01)	September 18, 2022
7.40A.250.528 (7.4.250-4)	September 13, 2022
7.40A.250.440 (7.4.250-3)	July 21, 2022
7.40A.250.364 (7.4.250-2.01)	June 8, 2022
7.40A.250.363 (7.4.250-2)	May 25, 2022
7.40A.250.270 (7.4.250-1.04)	May 3, 2022
7.40A.250.265 (7.4.250-1.02)	April 6, 2022
7.40A.250.262 (7.4.250-1.01)	March 29, 2022
7.40A.250.255 (7.4.250-1) * Initial LTS version	March 23, 2022
Previous LR Software Versions	
7.40A.005.619 (7.4_R2-5)	March 15, 2022
7.40A.250.010 (7.4.250-02)	March 10, 2022
7.40A.250.004 (7.4.250-01)	January 31, 2022
7.40A.250.001 (7.4.250)	January 25, 2022
7.40A.200.018 (7.4.200-02)	December 12, 2021
7.40A.100.338 (7.4.100-3.1)	November 29, 2021
z7.40A.100.336 (7.4.100-3)	November 17, 2021
7.40A.200.015 (7.4.200-01)	November 8, 2021
7.40A.100.239 (7.4.100-2.2)	September 29, 2021
7.40A.100.238 (7.4.100-2.1)	September 9, 2021
7.40A.100.233 (7.4.100-2)	September 1, 2021
7.40A.100.114 (7.4.100-1)	July 1, 2021
7.40A.100.021 (7.4.100-01)	May 19, 2021
7.40A.100.011 (7.4.100)	May 3, 2021
7.40A.005.613 (7.4_R2-4)	August 1, 2021
7.40A.005.509 (7.4_R2-1)	April 6, 2021
7.40A.005.314 (7.4_R2)	February 16, 2021
7.40A.002.007	October 29, 2020

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			
Mediant 500 Gateway & E-SBC	-	-	1/1	4 GE	2	-
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	-
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): ▪ MP-1288 ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800 Gateway & E-SBC (Rev. B and C) ▪ Mediant 1000B Gateway & E-SBC
Device	All products
Digital	Products with digital PSTN interfaces (ISDN BRI or PRI): ▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800 Gateway & E-SBC (Rev. ▪ Mediant 1000B Gateway & E-SBC B and C) ▪ Mediant 3100 Gateway & E-SBC
Mediant 90xx	▪ Mediant 9000 ▪ Mediant 9000 Rev. B ▪ Mediant 9030 ▪ Mediant 9080
Mediant Software	Software-based products: ▪ Mediant SE SBC ▪ Mediant VE SBC ▪ Mediant CE SBC

2 Long Term Support (LTS) Versions

This chapter describes the LTS versions of Release 7.4.

2.1 Version 7.40A.251.524

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.3112 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.1.1 New Features

This section describes the new features introduced in this version.

2.1.1.1 CLI Commands for Customizing Web Logo and Browser Tab

Customizing the device's Web interface logo (replacing with text), and the tab title (name) of the web browser used to access the device's Web interface can now be configured through CLI. Previously, this functionality could only be done through ini file.

To support this feature, the following CLI commands were added under `configure system > web`:

- `web-logo-enable` (corresponding ini file parameter [UseWebLogo])
- `web-logo-text` (corresponding ini file parameter [WebLogoText])

Applicable Applications: All

Applicable Products: All.

2.1.1.2 Floating and Metering Licenses Included in Debug File

The downloaded Debug file now includes debug information of the Floating and Metering licenses. This information appears in the FloatLicense.lzma and MeterLicense.lzma files, respectively, under the *system_logs* folder.

Applicable Applications: All

Applicable Products: All.

2.1.2 Resolved Constraints

This section lists resolved constraints.

Table 2-1: Resolved Constraints in Version 7.40A.251.524

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-50762	No corresponding CLI commands for the ini file parameters [UseWebLogo] and [WebLogoText].	Missing CLI parameters	Low	All	n/a
SBC-50934	The device fails to authenticate a user upon a SIP re-INVITE from the user, because there is no User Info file and the device doesn't take the credentials from the correct place.	Call failure upon re-INVITE	Medium	All	n/a
SBC-51073	The device runs out of resources ("DirectMediaData"), resulting in users not being able to join a multi-users (more than 100) conference call.	Users unable to join conference call	Medium	All	n/a
SBC-51104	The device doesn't free up resources for HTTP Get requests that failed, causing the resources to run out.	HTTP buffer overrun	Medium	All	n/a
SBC-51187	The device fails to download the Debug Recording file from local storage through OpenSSH, sending the syslog error "rcvd big packet 32781, maxpack 32768".	Device fails to download a file from local storage	Low	All	n/a
SBC-51357	The device fails to detect digits pressed on the Tel side when an alarm is played onsite (background noise from alarm prevents device from detecting all dialed digits).	Call failure	Medium	All	n/a
SBC-51378	The device restarts when trying to access the local storage through SFTP.	Device restart	High	All	n/a
SBC-51412	The device's Web interface is missing the AGC parameters.	Web interfaces display issue	Low	Mediant 3100	n/a
SBC-51474	When operating in HA mode, the device restarts during a Hitless Upgrade (due to a race condition of two internal tasks).	Device restarts	Medium	HA	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-51570	The device sends incorrect content in the SIP User-to-User header on the outgoing leg when the header contains 'encoding=hex' and the first character is a hex digit greater than 7.	Call failure	Medium	All	n/a
SBC-51624	The device restarts with exception info "Signal 11, Task SPMR" because of a failure in resource allocation ("SipMessage").	Device restart	Medium	All	n/a
SBC-51720	The device selects the first common coder instead of the fist coder, even though configured for forced transcoding.	No voice	Medium	All	n/a

2.2 Version 7.40A.251.461

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.3112 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.2.1 New Features

This section describes the new features introduced in this version.

2.2.1.1 New CLI Command for Including Global Session ID in SIP Messages

The device's CLI can now be used to enable the inclusion of the global session ID in outgoing SIP messages (AC-Session-ID header). This is configured by the new CLI command `configure voip > sip-definition settings > send-acsessionid`. Previously, this could only be done through the ini file (SendAcSessionIDHeader).

Applicable Applications: All

Applicable Products: All.

2.2.2 Resolved Constraints

This section lists resolved constraints.

Table 2-2: Resolved Constraints in Version 7.40A.251.461

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-49648	The device fails to allocate virtual CID resources, causing call failure (SIP 488 response).	Call failure	High	All	n/a
SBC-49679 SBC-50966	The device displays the incorrect number of registered users after an HA switchover because of 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-49961	The device fails to load a TLS certificate (incomplete client certificate).	Security	Medium	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-50139	The device sends a SIP INVITE message with a corrupted P-Called-Party-ID header (name part), causing the INVITE to be rejected by the recipient.	Call failure	Medium	All	n/a
SBC-50150	The device resets the connection to OVOC because of a miscalculation of the network interface for the listening sockets in the nginx config file.	OVOC connection resets	Medium	All	n/a
SBC-50195	The device's Web interface displays “Unable to Apply Changes” when accessing the Registration Status page.	Web interface display issue	Low	All	n/a
SBC-50196	An IP Group remains online even though all associated proxy servers are down, when the Proxy Set configuration includes 'Proxy Keep-Alive' as **Using OPTIONS on Active Server** and 'Redundancy Mode' as **Parking**.	Incorrect device behavior	Low	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

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-50434	The device can't be accessed through HTTPS redirection.	Device is inaccessible	Medium	All	n/a
SBC-50615	The device's SNMP trap destination stops functioning when the OAMP IP address is changed.	Device stops sending SNMP traps	Medium	All	n/a
SBC-50620	Typo in the Message Manipulation editor ("suggestion").	Typo in Web interface	Low	All	n/a
SBC-50698 SBC-51346	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
SBC-50706	Video freezes in a WebRTC-to-WebRTC call because of incorrect 'ssrc-group' handling (SDP has two sets of 'ssrc-group' attributes).	Video freezes	Medium	All	n/a
SBC-50721	The device fails to re-open the channel when moving from SRTP tunneling with RTP forwarding, to mediation, causing a loss of audio.	No audio after a SIP re-NVITE	Medium	All	n/a
SBC-50758	The device fails to recover from a restart and remains inaccessible (no ping, Telnet, SSH, or Web) because it fails to upload the Configuration Package file from SNMP/OVOC.	Device inaccessible after restart	Medium	Mediant 800C	n/a
SBC-51100 SBC-51278	The device restarts with the error message "Board Was Crashed: Signal 11, Task SPMR" because of an internal buffer overrun.	Device restart	Medium	All	n/a

2.3 Version 7.40A.251.364

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.3.1 Resolved Constraints

This section lists resolved constraints.

Table 2-3: Resolved Constraints in Version 7.40A.251.364

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47381	Despite the IDS table being empty, the device doesn't add malicious attackers (address and port) to the IDS blocklist due to lack of IDS resources.	Vulnerability due to device failing to add new malicious attackers to IDS blocklist	Medium	All	n/a
SBC-47714	All entries in the Local Users table of the Web interface are hidden (even though the users still exist).	No impact other than visually in Web interface.	Low	All	n/a
SBC-48339	For a DTMF transcoding call of RFC 2833 to Transparent, the device sends DTMFs both as RFC 2833 and Transparent, creating duplicated DTMFs			All	n/a
SBC-48797 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-48851	The device restarts when importing a Dial Plan file, and at least one of the existing Dial Plans are deleted.	Device restarts	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.	SBC resets	Medium	Mediant-CE (14 GB)	Azure
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

Incident	Description	Impact	Severity	Affected Products	Affected Environment
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 a delayed offer SIP UPDATE message is received, the device sends a re-INVITE message with an incorrect SDP to the outgoing side that doesn't support UPDATE messages.			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	When operating in HA mode, after several switch overs, the device loses HA and both devices in the HA system become active.	Loss of HA mode	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 fails, 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-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	Gateway	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-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 restarts	Medium	All	n/a
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

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-49872	No voice observed 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-49934	The device repeatedly sends the "IsTimerOwnerIdValid" syslog warning message.	No impact (repeated syslog warning message)	Low	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

2.4 Version 7.40A.251.287

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.4.1 Resolved Constraints

This section lists resolved constraints.

Table 2-4: Resolved Constraints in Version 7.40A.251.287

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-49400	When operating in HA mode and deployed on Azure, HA disconnects and both devices become active (standalone) after numerous HA switchovers.	HA disconnects	High	Mediant-CE SBC; Mediant VE SBC	Azure

2.5 Version 7.40A.251.284

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.5.1 Resolved Constraints

This section lists resolved constraints.

Table 2-5: Resolved Constraints in Version 7.40A.251.284

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-49573	The device experiences a high CPU overload when the LDAP service is enabled.	CPU overload and possible switchover in HA systems.	Urgent	All	All

2.6 Version 7.40A.251.283

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 3.1.5 or later.

2.6.1 New Features

This section describes the new features introduced in this version.

2.6.1.1 "New" Users Prompted to Change Password Upon Initial CLI Login

Users configured in the Local Users table whose 'Status' is "New" are now prompted to change their password upon initial login to the device's CLI. Up until now, login to CLI was blocked for these users. (This functionality is already supported by the Web interface.)

In addition, if a user is currently logged into a CLI session and the administrator modifies the user's settings in the Local Users table through CLI, the user's CLI session is automatically terminated, and the user needs to log in again. (This functionality is already supported by the Web interface.)

Applicable Applications: All

Applicable Products: All.

2.6.1.2 CLI Command for RetryAfterMode INI File Parameter

The ini file parameter RetryAfterMode now has a corresponding CLI command -- `configure voip > sip-definition settings > retry-after-mode`.

This existing functionality determines the device's behavior upon receiving a SIP 503 that contains a Retry-After header in response to a SIP message (e.g., REGISTER) sent to a proxy server.

Applicable Applications: All

Applicable Products: All.

2.6.2 Resolved Constraints

This section lists resolved constraints.

Table 2-6: Resolved Constraints in Version 7.40A.251.283

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-46933	The password for logging into the device via LDAP or RADIUS is limited to 40 characters.	Short password for login via LDAP or RADIUS	Low	All	n/a
SBC-47054	When importing a Dial Plan file, existing rules (indices) are overwritten by the new rules specified in the file.	Dial plan rule is overwritten	Low	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47351	Debug recording (DR) displays the incorrect DiffServ value (DSCP) for outgoing SIP packets (as configured by the IP Profile parameter 'Signaling DiffServ').	Incorrect DSCP values in DR	Low	All	n/a
SBC-47537	The device displays incorrect values ("0") for CDR fields OutPackets and InPackets.	Incorrect CDR values	Low	All	n/a
SBC-47603	One-way voice occurs after a SIP re-INVITE for session expiry due to incorrect device handling of received RTCP packets that have an invalid SSRC.	One-way voice	Medium	All	n/a
SBC-47616	One-way voice occurs on an SRTP-to-SRTP call, which upon a SIP re-INVITE, changes from SRTP tunneling to SRTP forwarding (and ROC is initialized).	One-way voice after a re-INVITE.	Medium	All	n/a
SBC-47821	The device doesn't include all the required headers in the second getRoute (after a SIP REFER) sent to ARM.	Device sends partial getRoute to ARM	Medium	All	n/a
SBC-47834	When operating in HA mode, the device, on rare occasions, fails to recover from a switchover and remains in standalone mode, because the active device fails to send large files (such as .cmp) to redundant device.	No HA	Medium	HA	Cloud
SBC-48155	The device sends a syslog warning message ("AutoCompletionResult::SetType - No match for subject type 17") when trying to normalize a SIP message.	Syslog warning message	Low	All	n/a
SBC-48183	The device restarts when trying to upload a Dial Plan file (.csv) through the Auto-Update mechanism.	Device restart	Medium	All	n/a
SBC-48282	The device erroneously reports to OVOC of high RTP delay for calls, due to incoming RTCP packets with correct Last SR timestamp value, but with incorrect delay since last SR timestamp value.	Incorrect reporting to OVOC of high RTP delay	Medium	All	n/a
SBC-48323	The device fails to add a new IP Interface that has the same local IP address as another IP Interface.	IP Interface configuration failure	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-48375	The device chooses the incorrect routing server when multiple Server Groups contain multiple hosts, and routing policy within the groups is round robin.	Routing Server selection failure	Low	All	n/a
SBC-48517	The device uses the incorrect directive "ssl_verify" for NGINX configuration for the 'OVOC Interface Verify Certificate' parameter.	Incorrect device configuration	Low	All	n/a
SBC-48518	The device sends syslog error messages regarding licensing for the Media Component.	Media Component error events	Medium	Mediant CE	n/a
SBC-48614 SBC-48615	The 'Calls per Sec' and 'Transactions per Sec' statistics icons on the device's Monitor page in the Web interface display "0".	Incorrect Web interface display	Medium	All	n/a
SBC-48779	The device's Web interface pages Activity Log, Active Alarms, and Alarms History display different date formats.	Incorrect Web interface display	Low	All	n/a
SBC-48872 SBC-48965	Importing a Dial Plan file (.csv) to the device fails.	Import Dial Plan file failure	Medium	All	n/a
SBC-48906	The parameter 'Trap Manager Host Name' which configures SNMP trap hostname requires a device restart (instead of on-the-fly).	Parameter not affecting until restart	Medium	All	n/a
SBC-48946	The following alarm is erroneously generated: "Cluster HA. At least one of the MCs is inactive, cluster will now provide only partial HA' alarm".	False alarm	Medium	Mediant CE	n/a
SBC-48964	The device rejects a new SIP INVITE request, generating the error message "CSeq inconsistency. Expected > 1; Received 1".	Call failure	Medium	All	n/a

2.7 Version 7.40A.251.150

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.7.1 Resolved Constraints

This section lists resolved constraints.

Table 2-7: Resolved Constraints in Version 7.40A.251.150

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-48092	The device restarts because of SSH connection failure during SFTP download of files from the device.	Device restarts	Medium	All	n/a

2.8 Version 7.40A.251.149

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.8.1 Resolved Constraints

This section lists resolved constraints.

Table 2-8: Resolved Constraints in Version 7.40A.251.149

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47989	The device's DSP restarts upon the receipt of an RTCP packet during a DTMF transcoding session.	DSP restarts and no audio for a few seconds on all related channels	High	All	n/a

2.9 Version 7.40A.251.147

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.9.1 New Features

This section describes the new features introduced in this version.

2.9.1.1 Support for SIP Call-Info Headers with Multiple Values

The device now supports SIP Call-Info headers containing multiple values (per RFC 3261). To support this feature, a new parameter called [CallInfoListMode] was introduced. If the Call-Info header in the incoming SIP message contains multiple values (e.g., URIs), the device handles the header according to this parameter's setting:

- When configured to 1, the device sends the outgoing SIP message with a **single** Call-Info header containing all the values (comma-separated list).
- When configured to 0, the device sends the outgoing SIP message with a Call-Info header per value.

Applicable Applications: All

Applicable Products: All.

2.9.1.2 Miscellaneous Parameter Updates

The following changes have been made to existing parameters:

- The web parameter 'Reject Cancel after Connect' (RejectCancelAfterConnect) has been moved to the SIP Definitions General Settings page (because it's applicable to both Gateway and SBC applications).
- The CLI command `classification_fail_response_type` (in SIP Interfaces table) was renamed `classification-fail-response-type` (aligns with naming conventions).

Applicable Applications: All

Applicable Products: All.

2.9.2 Resolved Constraints

This section lists resolved constraints.

Table 2-9: Resolved Constraints in Version 7.40A.251.147

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-45878 SBC-46778	Backup of device's Configuration Package file on OVOC fails when OVOC's address is an FQDN.	File backup on OVOC fails	Medium	All	n/a
SBC-45988	Device clears the Performance Monitoring (KPI) table acKpiIntervalStats after 24 hours.	KPI information lost after 24 hours	Medium	All	n/a
SBC-46095 SBC-47511	A ground fault causes device to send the alarm acAnalogPortGroundFaultOutOfService, which can't be cleared.	Alarm not clearing	Medium	MP-1288	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-46508	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
SBC-46539	Proxy load balancing (hot swap with round robin) with Account registrar stickiness enabled doesn't function properly. If all proxies in the Proxy Set are offline and the user triggers an un-register/register (Un-Register and Register commands in Accounts table), the device always sends an unregister/register to the same IP address in the Proxy Set instead of to the next IP address in the list	Load balancing fails	Medium	All	n/a
SBC-46585	When operating in HA mode, certificates (TLS Contexts) are sometimes lost during synchronization between active and redundant devices	Device loses certificates	High	HA	HA
SBC-46708	The [EnableNonCallCdr] parameter returns to default upon a device restart.	Parameter value not applied	Low	All	n/a
SBC-46719	The device rejects a call with a SIP 488 response when the initial route to ARM fails and the alternative route is configured to a "Gateway" destination type.	Call failure	Medium	Hybrid SBC-Gateways	n/a
SBC-46856 SBC-44227	When SNMP is changed to disabled, the device sends a multitude of the same error message in syslog (CUdpSocket ..).	Repeated syslog messages	Low	All	n/a
SBC-46864	When the [UserInfo] parameter is enabled, the device allocates more registration instances than defined by its License Key.	Resource exceeds device's License Key	Low	Mediant 1000B	n/a
SBC-46875	The device doesn't support the SIP 608 response (forwards it as a corrupted SIP message).	Device sends corrupted SIP message	Medium	All	n/a
SBC-46897	The device restarts upon the receipt of a SIP INVITE message with a Replaces header to a leg that is currently disconnecting.	Device restarts	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-46928	The device fails to latch onto a new IP and port after a SIP re-INVITE message, when the [NAtMode] parameter is configured to 4 (NAT by Signaling Restricted IP).	One-way voice	Medium	All	n/a
SBC-47015	If the [SBCPerfromanceProfile] parameter is configured to 2, device upgrade to a specific version fails because of failed DSP resources.	Device upgrade failure	High	All	n/a
SBC-47056	SIP message manipulation on SIP Call-Info headers with multiple values separated by commas fails.	Message manipulation failure	Medium	All	n/a
SBC-47057	When the device operates in HA mode, if a Pre-parsing Manipulation rule is deleted, the device continues processing the rule until a switchover is done (or a restart).	Message manipulation failure	Medium	HA	HA
SBC-47095 SBC-47349	If the 'SIP Topology Hiding Mode' parameter is configured to Fallback to IP Addresses, the Contact header's value is the IP address instead of the hostname (from the IP Group's 'Local Host Name' parameter).	Partial SIP topology hiding	Medium	All	n/a
SBC-47117	The device ignores non-listed SIP headers with index of zero received from ARM (e.g., 'Header.Privacy.0').	Device ignores header from ARM	Medium	All	n/a
SBC-47229 SBC-47600	When operating in HA mode, the redundant device restarts because of two processes running simultaneously on the redundant device.	Redundant device restarts	Medium	HA	HA
SBC-47284	The device's DSP restarts because of an internal memory overrun.	Loss of audio for a few seconds	Medium	All	n/a
SBC-47289	The device loses connectivity with the Media Components for a few minutes after an HA switchover.	No voice for several minutes upon HA switchover	Urgent	Mediant CE	HA
SBC-47310	The device's REST API endpoint `api\vi\status` mixes the values between the subnetMask and defaultGateway fields.	Device sends incorrect REST API response	Low	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47413	The device's Web interface's parameter 'reject Cancel After Connect' appears in the Gateway section even though it's an SBC parameter.	Web interface parameter in incorrect location	Low	All	n/a
SBC-47536	The device sends the incorrect SDP version in the outgoing SIP re-INVITE message for session refresh.	Device sends incorrect SDP version	Medium	All	n/a
SBC-47540	The device fails to use DSP resources for calls changed from RTP forwarding to RTP transcoding.	Call failure	Medium	All	n/a
SBC-47585	The device repeatedly sends the syslog message "Task TIML: mu_lock while in AcLockStart".	Repeated syslog messages	Low	All	n/a
SBC-47670	The device's Web interface displays Hyper-Threading as disabled even though it's active on the device (cpuOverrideHT parameter) and on the VMware host.	Hyper-Threading appears disabled	Low	Mediant Software	VMware

2.10 Version 7.40A.251.041

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 2.9.8 or later.

2.10.1 Resolved Constraints

This section lists resolved constraints.

Table 2-10: Resolved Constraints in Version 7.40A.251.041

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47347 SBC-47491	When in HA mode and a switchover occurs, the Media Components disconnect, and reconnect only after about 20 min.	No voice for several minutes upon HA switchover	Urgent	Mediant CE	Cloud (HA)

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-47540	Device fails to use DSP resources for calls that changed from RTP forwarding to RTP transcoding.	Call failure	High	All	All

2.11 Version 7.40A.251.035

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 2.9.8 or later.

2.11.1 Resolved Constraints

This section lists resolved constraints.

Table 2-11: Resolved Constraints in Version 7.40A.251.035

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-46808	Sometimes the device's DSP restarts because of a DSP internal memory issue.	Loss of audio for about 3 seconds because of DSP restart	High	All	n/a
SBC-47140 SBC-47190 SBC-47247	When operating in HA mode, the device sometimes loses certificates (TLS Contexts) during synchronization between active and redundant devices.	The device has no certificates	High	High Availability	n/a
SBC-47190	Proxy load balancing (hot swap with round robin) with Account registrar stickiness enabled doesn't function properly. If all proxies in the Proxy Set are offline and the user triggers an un-register/register (**Un-Register** and **Register** commands in Accounts table), the device always sends an unregister/register to the same IP address in the Proxy Set instead of to the next IP address in the list.	Load balancing isn't functioning	Medium	All	n/a

2.12 Version 7.40A.251.026

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1368 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 2.9.8 or later.

2.12.1 New Features

This section describes the new features introduced in this version.

2.12.1.1 Optimized Handling of SIP SUBSCRIBE Dialogs

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

This feature is supported by the following new parameters:

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

  This parameter is applicable only for devices operating in High-Availability (HA) mode. By default, the device backs up SUBSCRIBE dialogs of registered UAs. This allows the redundant (now active) device to maintain their subscription 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 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).

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

  When enabled, the device disconnects (deletes from storage) a registered SIP UA's SUBSCRIBE dialogs upon an unregister, upon register expiration, or upon a refresh register done from a different source IP address / port (like when the transport protocol is TCP or TLS). If disabled (like in previous versions), the device stores the UA's SUBSCRIBEs until their expiration times are reached.

Applicable Applications: SBC

Applicable Products: All.

2.12.1.2 Disabling Incoming ICMP Echo Requests Limit

Up until now, the device's DDoS mechanism limited incoming ICMP echo requests to 100 packets per second, protecting it from possible ping flooding. This functionality was non-configurable.

Now, users can disable this limit to allow the device to accept unlimited incoming ICMP echo requests. This feature is supported by the following new configuration parameter:

- Web: 'Enable ICMP Echo Requests Rate Limiting'
- CLI: `configure network > network-settings > limit-incoming-icmp-echo-requests`
- ini file: [LimitIncomingIcmpEchoRequests]

Applicable Applications: SBC

Applicable Products: Mediant 90xx; Mediant Software.

2.12.2 Resolved Constraints

This section lists resolved constraints.

Table 2-12: Resolved Constraints in Version 7.40A.251.026

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-43826 SBC-45456 SBC-46573	The Media Transcoder restarts, sending the trap message "AuditRxPoolDepletion - buffer level below 6.25 percent for:Xms - restarting system!!!".	Media Transcoder restarts	Medium	All	n/a
SBC-44196	The device sends the error message "Incoming SUBSCRIBE dialog rejected due to exceeded allowed resource allocation" and fails to handle incoming SIP SUBSCRIBE messages upon a failure (Ethernet alarm or switchover), causing all users to re-subscribe/re-register due to broken TCP\TLS connection.	Device experiences CPU overload and fails to handle re-SUBSCRIBE requests	Medium	Gateways	n/a
SBC-44392	An alarm notifying license pool about to expire is sent for the Redundant device.	False alarm	Low	HA	n/a
SBC-44458 SBC-45086	The device is exposed to security vulnerabilities "Strict transport header" and "Header "Expect-CT, Permissions-Policy, Cross-Origin-Embedder-Policy, Cross-Origin-Resource-Policy, Cross-Origin-Opener-Policy"".	Device security	Medium	All	n/a
SBC-44541 SBC-45053	When in HA mode, loading an incremental CLI script file through REST API causes configuration errors on the Redundant device.	HA mode terminated	Medium	HA	n/a
SBC-44987	The device fails to handle a SIP INVITE with replaces during an INVITE/re-INVITE session (and 200 OK or ACK hasn't been received yet), sending the error message ""!! [ERROR]SBCOfferAnswerMngr(#729)::HandleSDPReinviteFromCore - Can't handle new Re-INVITE. Re-INVITE is in progress"".	Call transfer failure	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-45065	The device doesn't add the ';+sip.src' suffix to the Contact header in the SIP INVITE that's sent to the SRS when the [SIPRecMetadataFormat] parameter is set to 1.	Device doesn't fully comply to SIPREC	Medium	All	n/a
SBC-45225	The device's SIP topology hiding feature doesn't work on outgoing SIP OPTIONS messages.	Device fails to apply SIP topology hiding	Low	All	n/a
SBC-45286	WebRTC call fails upon a re-INVITE because of a DTLS handshake failure when the device sends a re-INVITE for media sync, even though the peer side sent an SDP answer with a single coder.	WebRTC call failure	Medium	SBC	n/a
SBC-45306	The device fails to send debug captures via FTP, sending the error message "ftpput put failed".	FTP failure	Medium	Mediant Software; Mediant 90xx	n/a
SBC-45357	The device uses incorrect resources (e.g., Media Realm) for a registered user, causing call failure in a specific call scenario where a registered UA changes its IP address (but same user part).	Device fails to update registered user contacts details, causing transaction failure	Medium	All	AWS
SBC-45358	The device uses incorrect crypto suite upon a re-INVITE session with Zoom, causing call failure.	Call failure with Zoom	Medium	All	n/a
SBC-45399	Upon a session refresh and when the device is the refresher, it sends an SDP with the incorrect version.	Device sends incorrect SDP version	Medium	All	n/a
SBC-45498	The device sends multiple SIP INFO messages for multiple DTMFs even though only one DTMF rtp event is received.	Device sends multiple SIP INFO messages instead of one	Medium	All	n/a
SBC-45506	When in HA mode, the device fails to find a matching registered user for an incoming INVITE (replies with a 404 Not Found), resulting in call failure.	Call failure	High	HA	n/a
SBC-45575	The device fails to parse a Contact header with a URI containing more than 300 characters.	Registration failure	Medium	All	n/a
SBC-45690	When in HA mode, a switchover occurs due to a bug in the SSH mechanism between active and redundant devices.	Switchover occurs	Medium	HA	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-45780	The device erroneously adds 'transport=tls' to a SIP 200 OK Contact header sent over UDP.	Device sends incorrect transport type.	Medium	All	n/a
SBC-45882	The device sends invalid SIP messages (corrupted multiple Via headers) in a specific call scenario that involves the receipt of multiple NOTIFY messages for the same dialog transaction.	Device sends corrupted SIP messages	Medium	All	n/a
SBC-45939	The device shows a discrepancy in license values when license changed from Flex to Floating licensing pools, and vice versa.	Device shows incorrect license values	Medium	All	n/a
SBC-46096	The sliding window CAC algorithm feature appears in the Web interface of devices that don't support it.	Device shows irrelevant parameters in Web interface	Low	All	n/a
SBC-46120	The sliding window CAC algorithm mistakenly counts alternative routes as affecting rate, resulting in incorrect CAC values.	Incorrect CAC values	Medium	All	n/a
SBC-46126	The Media Transcoder disconnects from the Signaling Component due to a collision between two GARPS (from active and redundant) when a switchover occurs.	Media Transcoder disconnects	Medium	HA	n/a
SBC-46132	The device's DDOS mechanism limits ICMP echo requests to 100 packets per second, without any possibility to disable it and allow unlimited receipt.	Device limits pings	Medium	All	n/a
SBC-46223	The Accounts table setting of 'Registrar Search Mode' to **Avoid Previous Registrar Until Expiry** and the [AccountRegistrarAvoidanceTime] parameter don't function - re-registration is done only for the first rule in the table.	Device re-registers to incorrect IP address	Medium	All	n/a
SBC-46286	When in HA mode, the redundant device experiences a restart loop.	Redundant device in restart loop	Medium	HA	n/a
SBC-46314	The output of the device's CLI command `show-running config` doesn't display the `interface e1-t1` settings.	Missing information in output of `show-running config`	Medium	Mediant 3100	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-46542	When a rule in the IP-to-IP Routing table is deleted, other rules may be affected, causing them not to work.	Incorrect routing	Medium	All	n/a
SBC-46578	The device restarts because of an internal buffer overrun ('Board Was Crashed: Signal 11, Task SPMR, FaultAddr: (nil)' + '_ZN17RTPStreamResou ')".	Device restarts	High	All	n/a

2.13 Version 7.40A.250.931

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1342 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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 2.9.5 or later.

2.13.1 Resolved Constraints

This section lists resolved constraints.

Table 2-13: Resolved Constraints in Version 7.40A.250.931

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-45819	The device sends the incorrect SDP session version on a specific LMO call flow (outgoing ACK with SDP answer after the re-INVITE delayed offer contains the same rejected SDP as the incoming ACK), causing call failure.	Call failure after a re-INVITE session.	Medium	All	All

2.14 Version 7.40A.250.926

This version includes resolved constraints only.

IMPORTANT NOTICE for HIGH AVAILABILITY DEVICES

This version has fixed a bug whereby the device sometimes loses configuration upon an HA switchover (see resolved constraints for details). Prior to upgrading to this version, Customers using High Availability SBCs should restart the standby (redundant) SBC (this action is not service affecting).

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1342 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.14.1 Resolved Constraints

This section lists resolved constraints.

Table 2-14: Resolved Constraints in Version 7.40A.250.926

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-45095 SBC-45426 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, this may lead to loss of service.	Urgent	High Availability	-

Note: Prior to upgrading to this version, Customers using High-Availability devices should restart the standby (redundant) device (not service affecting):

- Web interface: Click the **Reset** button (**Setup** > **Administration** > **Maintenance** > **High-Availability Maintenance**)
- CLI: Login as a privileged user, and then run the command `ha reset-redundant-unit`

Wait until the restart process completes and verify that the Web interface's Monitor page displays "Operational" in the 'HA Status' field.

2.15 Version 7.40A.250.908

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.1342 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.15.1 New Features

This section describes the new features introduced in this version.

2.15.1.1 Increase 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.

2.15.1.2 SIP re-INVITE Handling upon Location or Media Path Change for LMO

When the device is deployed in a Microsoft Teams environment using Local Media Optimization (LMO) for Direct Routing, the device can now be configured for handling changes in the location or media path (Teams headers X-MS-UserLocation or X-MS-MediaPath, respectively).

This feature is configured using the new IP Group parameter 'Teams Local Media Optimization Sync':

- Disabled (default and like in previous versions): The device sends a SIP re-INVITE to Teams.
- Enabled: The device doesn't send a re-INVITE but instead waits for a re-INVITE from the Teams client. Only when it receives a re-INVITE does the device either change the Media Realm (port) according to the new location or change the media path (direct media or non-direct media).

Applicable Applications: SBC

Applicable Products: All.

2.15.2 Resolved Constraints

This section lists resolved constraints.

Table 2-15: Resolved Constraints in Version 7.40A.250.908

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-42861	Failure to log in to the device's Web interface with local users (configured in Local Users table) when the RADIUS sever is down.	Can't log into Web interface	Medium	All	n/a
SBC-43744	Activity Log doesn't provide enough information regarding import of TLS certificates, private keys, trusted roots (and remove).	Activity Log doesn't show detailed information	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-43747	The device's Command Shell displays passwords in plaintext (instead of hidden).	Security	High	All	n/a
SBC-43753	When the 'Channel Select Mode' parameter in the Trunk Group Settings table is configured to **Select Trunk by Supp-Serv Table**, for registrations the device obtains the host part of the SIP To and From headers from the global parameter [SIPGatewayName] instead of the 'Gateway Name' parameter in the Trunk Group Settings table.	Incorrect host part in SIP headers.	Low	Gateway	n/a
SBC-43956 SBC-44017	The device marks the SIP Interface's 'Additional UDP Port Range' as gray in embedded DDOS mechanism, causing it to discard packets from these known ports upon CPU overload.	Device rejects packets from known sources (whitelisted) upon CPU overload.	High	All	n/a
SBC-44075	The device in HA performs a switchover when the redundant unit freezes for a certain duration (e.g., due to Azure maintenance), causing the entire HA system to restart and loss of service.	Active and redundant units are down, causing loss of service	High	High Availability	Azure
SBC-44076	Due to an error in DTMF transcoding, the device fails to remove unsupported crypto suites from the SIP re-INVITE offer, causing call failure.	Call failure upon re-INVITE for media sync	Medium	All	n/a
SBC-44083	The device doesn't display the correct RTP delay (only displays average round-trip delay time of the entire RTP stream) in the media CDR ("RTPdelay" field).	Incorrect CDR report	Low	All	n/a
SBC-44102	The device discards BFCP packets behind NAT because they are mistakenly considered as DTLS packets.	BFCP fails to traverse the device	Medium	All	n/a
SBC-44138	The device restarts after failing to handle a SIP SUBSCRIBE message (internal task in the code regarding object handling).	Device restarts	Medium	All	n/a
SBC-44146	The device uses a new TLS connection when sending a SIP BYE message when the Via header contains an FQDN and not an IP address.	Device opens extra TLS connection	Low	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-44158	The 'CDR File Name' parameter doesn't accept certain symbols in the hostname (e.g., '<' and '>').	CDR file name failure	Low	Mediant Software; Mediant 9000	n/a
SBC-44248	The device restarts when handling many raising\clearing alarms in a multithread environment.	Device restarts	Medium	Mediant Software	AWS
SBC-44382	The device doesn't remove unknown (and unsupported) crypto suites on the incoming leg, causing the device to attempt transcoding and if no transcoding capabilities, the call fails.	Devices attempts transcoding when it isn't required	Medium	All	n/a
SBC-44546	The device sends a SIP ACK message with an incorrect SDP (port = 0 and no media) upon a race condition between re-INVITE from Teams and a re-INVITE sent to Teams for LMO.	Call disconnection	Medium	All	n/a
SBC-44636	The device restarts when receiving or sending silence packets on non-G.711 channels.	Device restarts	Medium	All	n/a
SBC-44638	The device fails to connect to OVOC for sending QoE reports.	Devices doesn't send reports to OVOC	Medium	All	n/a
SBC-44908 SBC-44926	The device doesn't reply to incoming SIP OPTIONS messages that contain the 'Max-Forward: 0' header.	Device doesn't reply to incoming SIP messages.	Medium	All	n/a
SBC-45227	The device performs number manipulation only on the first outgoing INVITE message in a forked call (ARM environment).	Device fails to perform manipulation	Medium	All	ARM
SBC-45244	The device stops sending SIP REGISTER requests if it receives a SIP 4xx response with an 'Expires: 0' header (considers it as an un-subscribe).	Device stops sending REGISTER requests	Medium	All	n/a
SBC-45292	When the IP Profile parameter 'Generate SRTP Keys Mode' is configured to **Always**, the device sends a SIP re-INVITE with new crypto, but switches from SRTP to SRTP forwarding, causing one-way voice.	One-way voice	High	All	n/a

2.16 Version 7.40A.250.851

This version includes new features and resolved constraints only.

Note: This version is applicable only to Mediant 800C and MP-1288.

Note: Upgrade to Version 7.4 can only be done from the following 7.2 versions:

- 7.20A.260.*
- 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.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC versions 8.0 (8.0.3180 or later) and 8.2 (8.2.280 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.16.1 New Features

This section describes the new features introduced in this version.

2.16.1.1 Component 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.

2.16.2 Resolved Constraints

This section lists resolved constraints.

Table 2-16: Resolved Constraints in Version 7.40A.250.851

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-41948 SBC-42058 SBC-43181 SBC-43820 SBC-44506	The device restarts with the error message "CMX Kernel Panic" because of memory issue.	Device restarts	High	Mediant 800C; MP-1288	n/a

2.17 Version 7.40A.250.836

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.280 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.17.1 New Features

This section describes the new features introduced in this version.

2.17.1.1 Support for SIP 'precondition' per RFC 3312

The device can now be enabled to handle calls for SIP session preconditions according to RFC 3312.

To enable compliance, a new parameter called 'SBC Precondition' has been added to the IP Profiles table.

If enabled for a specific IP Profile, the device always adds the value ‘precondition’ to the Supported header in the outgoing SIP message and creates an SDP answer precondition if the incoming message contained an SDP offer precondition. If an incoming message includes this value in the Require header and the feature is disabled, the device rejects the message.

Applicable Application: SBC.

Applicable Products: All.

2.17.1.2 TLS Certificate Verification by Per Proxy Set

The device can now verify TLS certificates per Proxy Set.

If the received certificate's Subject Alternative Name (SAN) matches the Proxy Set's address (IP address or FQDN), the device establishes a TLS connection (and allows the call).

If there is no match and the SAN isn't marked as "critical", the device compares the Proxy Set's user-defined TLS subject name with the certificate's Common Name (CN). If they match, the device establishes a TLS connection and (allows the call).

This feature is configured by the following new parameters in the Proxy Sets table:

- 'Peer Host Name Verification Mode' – enables TLS certificate verification per Proxy Set
- 'TLS Remote Subject Name' – defines the Proxy Set's Subject Name

Applicable Application: All.

Applicable Products: All.

2.17.1.3 Classification by TLS Certificate's Subject Name

The device can now also use the TLS certificate's Subject Name as a matching characteristic for classifying incoming SIP dialog messages in the Classification table.

If the Subject Name (Common Name / CN or Subject Alternative Name / SAN) is the same as that of the certificate used for the TLS connection upon which the message was received (and the other configured classification matching characteristics are met), the device classifies it to the corresponding row in the Classification table.

This feature is configured by the new 'TLS Remote Subject Name' parameter in the Classification table.

Applicable Application: SBC.

Applicable Products: All.

2.17.2 Resolved Constraints

This section lists resolved constraints.

Table 2-17: Resolved Constraints in Version 7.40A.250.836

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-40939	Registration failures occur (with error 500 Server Internal Error) followed by "no more free id's" error messages for resource type SBCDialogs.	Registration fails	Medium	All	n/a
SBC-42399	The device fails to synchronize with the NTP server over a WebSocket connection with OVOC.	NTP failure over WebSocket	Medium	All	n/a
SBC-42421	The device periodically restarts due to Linux Signal (HCTL Task) caused by a corrupted pointer.	Device restarts	High	All	n/a
SBC-43009	The device rejects incoming ping requests due to an embedded DDOS mechanism.	Device sometimes rejects incoming ping requests	Low	All	n/a
SBC-43049	The device limits KPI monitoring to 56 IP Groups.	KPI monitoring is limited to 56 IP Groups	Low	All	n/a
SBC-43053	The device sends clear trap alarms to OVOC with incorrect severity, causing OVOC to send incorrect email notifications.	Device sends incorrect alarm severity to OVOC	Low	All	n/a
SBC-43163	The device restarts due to a DSP restart.	Device restarts	Medium	Mediant 800	n/a
SBC-43272	The device generates many syslog warning messages ("miGetInterfaceIndexByRowInMatrix(): Invalid rowInMatrix -1 [Code:0x20002]").	No impact	Low	All	n/a
SBC-43391	The device's Web interface doesn't display the **Tunnel** optional value for the [IpTracePhysicalPort] parameter after an HA switchover.	Tunnel option not displayed after a switchover	Medium	HA	HA
SBC-43519	The device's output for the REST API `upload incremental cli script` has changed between versions 7.2 and 7.4, breaking backward compatibility.	Backward compatibility not maintained	Low	All	n/a
SBC-43579	The device marks a SIP Interface as invalid when upgrading the device and the maximum UDP port range exceeds the maximum FEU in the License Key.	Users connected to the invalid SIP Interface are unregistered.	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-43752	The Message Manipulation feature can't manipulate the SIP Priority header to have any other value other than "normal".	SIP Header can't be modified.	Low	All	n/a
SBC-43856	The device's ISDN trunks aren't synchronized when the framing method is **DDF**.	Trunks are not synchronized.	High	Gateway	n/a
SBC-43896	The device does an HA switchover with "Software Watchdog: Run task WEBS, Wait task DSPD" due to failure of internal processes between active and redundant units.	Device does an HA switchover	High	HA	HA
SBC-43972	The device restarts when handling both a blind call transfer and receiving another call.	Device restarts	High	All	n/a
SBC-43978 SBC-44084 SBC-44241	The device changes the RFC 2833 timestamps when forwarding DTMFs, resulting in incorrect DTMFs.	DTMF failure	High	All	n/a
SBC-43984 SBC-44011 SBC-44285	The device restarts due to SDP negotiation of crypto keys and label attribute.	Device restarts	High	All	n/a
SBC-44003	In the SNMP Trap Destinations table, the device changes 'Trap User' to **v2cParams** (SNMPv2) and 'Trap Enable' to **Disable** without any warning to user.	SNMP trap destination changed	Medium	All	n/a
SBC-44012	The device requires transcoding resources when using DTLS and ICE.	Transcoding is required even for calls that shouldn't need it.	Medium	All	n/a
SBC-44078	The device sends unrecognized crypto suites toward a non-secure leg, causing call failure.	Call failure	Medium	All	n/a
SBC-44137	The device replies with ACK from the wrong UDP port (default SIP Interface port instead of dedicated UDP port) upon forked call.	No impact	Medium	All	n/a

2.18 Version 7.40A.250.754

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.280 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.18.1 New Features

This section describes the new features introduced in this version.

2.18.1.1 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 Application: All.

Applicable Products: All.

2.18.1.2 Increased SIP Header Length for Message Manipulation

When configuring a Message Manipulation rule that relates to a SIP header, the maximum length (characters) of the header's value in the incoming SIP message that can be manipulated has been increased from 1,500 to 4,096. (Previously, the result of a manipulated header would have been truncated to 1,500 characters.)

Applicable Application: All.

Applicable Products: All.

2.18.2 Known Constraints

This section lists known constraints.

Table 2-18: Known Constraints in Version 7.40A.250.754

Incident	Description	Impact	Severity	Affected Products	Affected Environments

SBC-42078	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:
	`configure network`
	`access-list <index>`
	`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

2.18.3 Resolved Constraints

This section lists resolved constraints.

Table 2-19: Resolved Constraints in Version 7.40A.250.754

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-40260	The device crashes (restarts), generating error type "TASK: WEBS" because of an internal task (SWWD) which runs every 15 minutes (when device connected to OVOC and periodically sends Performance Monitoring history queries).	Device restart	Medium	All	n/a
SBC-40776	The device has no serial connection when RADIUS is enabled without configuring a RADIUS server.	Device loses serial connectivity	Medium	All	n/a
SBC-41089	The device disconnects a call due to a media mismatch, in a specific call transfer scenario.	Call failure	Medium	All	n/a
SBC-41135	The device sometimes fails to upload a CLI Script file when it contains a download \ import command for an external file such as a Dial Plan file.	Device fails to upload the CLI Script file and only a restart resolves it	Medium	All	n/a
SBC-41208	The [SDRRemoteServers_Username] parameter is limited to 29 characters (instead of 30).	Limited CDR parameter name's lenght	Low	All	n/a
SBC-41514 SBC-42001 SBC-42516 SBC-42637 SBC-42823 SBC-42997	The device crashes (restarts) due to a CPU overload caused by an internal task process ("NWST").	Device restart	High	All	n/a
SBC-41541	The device can't recover from a DSP reset, causing device failure.	Device restart	Medium	Mediant 3100	n/a
SBC-41792	The device can't perform message manipulation on more than three SIP Call-Info headers ("unknown" header). (Now, it's considered a "known" header and the device can handle up to 10 occurrences of this header in a single SIP message.)	Message manipulation failure (limitation)	Low	All	n/a
SBC-41805	The device supports up to 600 characters for the SIP User-To-User header when the [UserToUserHeaderFormat] parameter is configured to 3.	Header length limitation	Low	All	n/a
SBC-41864	The device limits URL parameters in SIP headers (e.g., Contact) to 20 characters.	URL length limitation in SIP headers	Low	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-41889	The device is exposed to security vulnerability Cross-Frame Scripting (XFS).	Vulnerability	High	All	n/a
SBC-41924	The device is exposed to security vulnerability denial of service (DoS).	Vulnerability	High	All	n/a
SBC-42113	The device fails to handle the DSP label attribute if its value has a non-digit prefix (e.g., "a=label:vrsp-0").	SBC bad SDP	Low	All	n/a
SBC-42153	The device raises a false alarm of "GW locked" on the Media Transcoder.	False alarm	Low	Media Transcoder	n/a
SBC-42164	The device displays negative counter values on Performance Monitoring parameters when the CLI command `clear voip statistics` is run (command now obsolete).	Wrong Performance Monitoring values	Low	All	n/a
SBC-42166	For Local Media Optimization (LMO), the device sends an SDP answer with a false connection line "c=1.1.1.1" in a specific scenario when SDP contains only one rejected media which was created locally, and the IP is on the session level. (In this case, it should be updated with the correct IP.)	Call failure due to wrong media negotiation (false IP)	Medium	All	n/a
SBC-42300	When uploading an incremental CLI Script through REST API, the device erroneously generates a message indicating a restart (Activity Log: Device Reset. Session: WEB) in syslog, activity log and alarm.	False alarm about restart	Low	All	n/a
SBC-42317	The device lost its configuration after an HA switchover and returned to Standalone mode.	HA failure	High	Mediant CE	Azure
SBC-42375	The device extends DTMF payload type even if the payload type is already used by another coder, causing it to send an SDP offer with two similar payload types, one for coder and one for DTMF.	Device sends wrong SDP offer (in meaning of DTMF payload type)	Medium	All	n/a
SBC-42598	The device doesn't add ARM X-headers to new INVITE messages (as a result of REFER termination) when DNS results are received after the ARM response.	Device sends INVITE to Teams with missing headers	Medium	All	n/a
SBC-42645	The device infinitely plays hold tone when configured to play the hold tone and the CPT\PRT file doesn't contain the hold tone or has the wrong hold tone coder.	Devices plays hold tone infinitely	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-42728	The device restarts upon a race condition that involves alternative ARM call routing with forking, and when call is answered before synchronization with the ARM ends.	Device restart	Medium	All	n/a
SBC-42729 SBC-42862 SBC-42864 SBC-43097	If a Media Transcoder gets stacked in an upgrade from version 7.2 to 7.4R2, the cluster can't continue upgrading the remaining Media Transcoders.	Upgrade failure	Medium	Media Transcoder	n/a
SBC-42800	The device restarts due to a CPU overload caused by internal processing tasks "WEBS" and "VEEV".	Device restart	High	All	n/a
SBC-42839	The device traverses RTP packets between two call legs without checking and recalculating header normalization timestamp delta.	Poor voice due to timestamp gap	Low	All	n/a
SBC-42843	Upon SDP answer termination, the device fails to match the offer's security and replies with SRTP (instead of RTP).	Call failure due to SDP mismatch	Medium	All	n/a
SBC-42938	The device fails to clear the error message "SYS_HA: HA Remote address and Maintenance IF address are not on the same subnet" even though configuration was subsequently fixed and valid.	False alarm	Medium	HA	n/a

2.19 Version 7.40A.250.611

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.280 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.19.1 Resolved Constraints

This section lists resolved constraints.

Table 2-20: Resolved Constraints in Version 7.40A.250.611

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-41517	MT and MTC are not supported.	No MT\MTC functionality	High	Mediant CE (Elastic Media Cluster); Mediant VE (Media Transcoding Cluster)	All

2.20 Version 7.40A.250.609

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 versions 8.0 (8.0.3180 or later) and 8.2 (8.2.280or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.20.1 New Features

This section describes the new features introduced in this version.

2.20.1.1 SIP Account Synchronization upon No Response from Registrar

If an Account (configured in the SIP Accounts table) receives a timeout (as defined by SipT1Rtx, SipT2Rtx, or SIPMaxRtx) or response failure (e.g., SIP 403) for a sent SIP REGISTER request, the device stops sending REGISTER messages for all other Accounts using the same Serving IP Group (proxy server), until the proxy responds. The Account that detected the no response (or failure) from the server is considered the *lead Account*. Only this Account continues to attempt registration with the server.

When the lead Account receives a successful response from the server, the device resumes the registration process for all the other Accounts associated with the same Serving IP Group.

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

Applicable Application: All.

Applicable Products: All.

2.20.1.2 Freeing Up TLS Connection Resources

The device now attempts to close unused TLS connections and those that are kept open only because they are persistent, when the number of currently allocated incoming TLS connections exceeds 80% of the maximum number of allowed TLS connections. In this way, the device tries to prevent TLS connections from accumulating and reaching the device's maximum number of supported TLS connections.

The device also supports a new SNMP alarm called acTLSSocketsLimitAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.159), which it sends (Major severity) when the number of incoming TLS connections is over 95% of maximum. The alarm is cleared when the number of TLS connections returns to below 90% of maximum. Maximum TLS connections per device is shown in Table 3-2: Maximum Capacity per Feature.

Applicable Application: All.

Applicable Products: All.

2.20.2 Known Constraints

This section lists known constraints.

Table 2-21: Known Constraints in Version 7.40A.250.609

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-41517	MT and MTC are not supported.	No MT\MTC functionality	High	Mediant CE (Elastic Media Cluster); Mediant VE (Media Transcoding Cluster)	All

2.20.3 Resolved Constraints

This section lists resolved constraints.

Table 2-22: Resolved Constraints in Version 7.40A.250.609

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-38452	The device sends a wrong disconnect reason in the SIP NOTIFY message for failed call transfer scenarios when it terminates the original call with a SIP REFER.	Device sends wrong disconnect code (e.g., 408 instead of 480)	Medium	All	n/a
SBC-38513	When deployed on Azure, the device loses access to the Web interface and only a restart resolves the issue.	No access to the device	Medium	Mediant VE (HA)	Azure
SBC-39064	The device fails to run REST API commands using PowerShell.	Device fails to run REST API commands over PowerShell	Medium	All	n/a
SBC-39204 SBC-40262	The device disconnects from AudioCodes Syslog Viewer utility (over HTTP\S).	Device disconnects from Syslog Viewer	Medium	All	n/a
SBC-39291	The device loses connectivity to its Web interface when using a long cookie (greater than 800 characters).	Device loses connectivity to Web interface	Medium	All	n/a
SBC-40081	The device fails to keep the original crypto key in Local Media Optimization for Direct Routing SDP offer-answer session, causing the call to fail.	Device in LMO call fails due to no audio.	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-40083	The device restarts upon a "race" condition when two ARM 4xx responses for alternative routing are received.	Device restarts	Medium	All	n/a
SBC-40129	The device sends a SIP INVITE message without the user-part in the Request-URI header in an OVR environment.	Call failure	Medium	All	n/a
SBC-40246	HA Hitless Upgrade fails.	Device fails to perform Hitless upgrade	Medium	Mediant 800 HA	n/a
SBC-40261	The device is exposed to vulnerability CVE-2022-37434 (zlib buffer overflow on inflate).	Security	Medium	All	n/a
SBC-40387 SBC-40806	The device restarts when a Message Manipulation rule that has an index number that is out of the allowed range is added or deleted.	Device restarts	Medium	All	n/a
SBC-40525	The device restarts with error reason "Task WEBS" when downgraded from 7.4 CentOS6 ("interim" version) to 7.2 CentOS6.	Device restarts	Medium	All	n/a
SBC-40686	The device attempts to resolve domain names using the DNS server configured for the HTTP Proxy instead of the DNS server configured in the IP Interfaces table.	Device fails to resolve DNS	Medium	All	n/a
SBC-40758 SBC-40912	The device restarts with error "Task TIML, Wait task VEEV" due to an internal failure in its voice engine.	Device restart	Medium	All	n/a
SBC-40764	The device adds spaces to CDR and SDR file names, making them unreadable.	Device creates corrupted CDR / SDR file names.	High	All	n/a
SBC-40821	The device fails to fork a call to all users when the parameter [SBCKeepContactUserInRegister] is configured to 1.	Device sends call only to one user (instead of forking to all users)	Medium	All	n/a
SBC-40840 SBC-40766 SBC-40834	The device fails to reconnect to ARM (if, for example, connection to ARM was lost) due to incorrect internal state machine and gets stacked in state re-connecting.	Device can’t reconnect to ARM	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environment
SBC-40875 SBC-40932	The device doesn't send a warning and doesn't use the clear unused TLS resources mechanism when 80% of TLS resources are used.	Device runs out of TLS resources	High	All	n/a
SBC-40896	The device randomly loses the first 1-1.5 sec. of a WebRTC call during the call DTLS handshake.	Device skips the voice in the beginning of the call.	Medium	All	n/a
SBC-40955	The device fails to recover from losing a UDP port (on a dedicated connection using the Stickiness feature) and fallbacks to the SIP Interface's default UDP port.	Devices Stickiness feature doesn't function	Medium	All	n/a
SBC-40956	Some calls processed by the device are without audio due to an internal bug in the voice engine.	Some calls have no audio	High	All	n/a
SBC-40973	Configuration of the SBC SDR Format table is not affecting sent SDRs.	Incorrect SDR format	Medium	All	n/a
SBC-40975	The device limits the number of characters in the SDP's 'a=mid' attribute to 7.	SDP's mid attribute is cut after 7 characters	Low	All	n/a
SBC-41045	Call Setup Rules (CSR) become inactive after a restart if the 'Rand.Number' function was used.	Call Setup Rules are inactive after restart	Low	All	n/a
SBC-41059	The device fails to correctly parse the SIP Referred-By header when it has more than 500 characters	Long Referred-By headers are not handled correctly	Low	All	n/a
SBC-41091	The device restarts upon opening the RTP port because of a memory allocation error.	Device restart	Medium	All	n/a
SBC-41092	The device fails to terminate SIP OPTIONS messages because of a change in the SIP Interface.	Device fails to reply to keep-alive messages	Low	All	n/a
SBC-41434	The device generates an error message "Task PHDL: mu_lock while in AcLockStart" messages followed by a trace back when PSTN trace is enabled.	Syslog messages	Low	Mediant 3100	n/a

2.21 Version 7.40A.250.541

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 (8.0.3180 or later) and Version 8.2 (8.2.277 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.21.1 Resolved Constraints

This section lists resolved constraints.

Table 2-23: Resolved Constraints in Version 7.40A.250.541

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-40453	The device resets if during high HTTP traffic the HTTP server disconnects (for whatever some reason).	Device reset	High	All	n/a

2.22 Version 7.40A.250.528

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 (8.0.3180 or later) and Version 8.2 (8.2.277 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.22.1 New Features

This section describes the new features introduced in this version.

2.22.1.1 Client Defaults Included in Debug File

The Client Defaults file (default.ini) is now included in the Debug File (under the 'Device' folder).

Applicable Application: All.

Applicable Products: All.

2.22.1.2 Increased Character Support for 'tag' in SIP To/From Headers

The maximum number of characters that can be supported for the 'tag' parameter in the SIP To and From headers has been increased from 99 to 150.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.22.1.3 IP Interface for WebSocket Tunneling

An IP Interface can now be specified for the WebSocket tunnel. This is supported by the new 'Interface Name' parameter (WSTunInterfaceName / `configure network > ovoc-tunnel-settings > interface-name`) on the Web Service Settings page. If not specified, the default OAMP IP Interface is used.

Applicable Application: All.

Applicable Products: All.

2.22.1.4 Improved Activity Log

The device's Activity Log, which logs management user actions performed in the Web interface has been enhanced as follows:

- A log is now generated when an expired user tries to log in.
- When a user's level is changed, the log now also indicates the previous level, for example:

```
Activity Log: Local Users Table row 3 (myUser123) - 'User
Level' was changed from 'Administrator' to 'Security
Administrator'. User: Admin. Session: WEB (10.10.10.10)
[Time:07-09@16:39:22.736]
```

- When a user's password is changed, the log now also indicates the user (username).
- When a username is changed, the log now also indicates the previous username.
- When a parameter's value is changed, the log now also indicates the previous value, for example:

```
Activity Log: Media Realms row 3 - 'UDP Port Range Start' was
changed from 6300 to 6310. User: Admin. Session: WEB
(10.10.10.10) [Time:07-09@16:39:22.736]
```

Applicable Application: All.

Applicable Products: All.

2.22.2 Resolved Constraints

This section lists resolved constraints.

Table 2-24: Resolved Constraints in Version 7.40A.250.528

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-36330 SBC-37360	The device fails to resolve DNS when the Access List table is configured with a domain name.	DNS failure	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-37361 SBC-38451 SBC-38689 SBC-38742 SBC-39045 SBC-39320 SBC-39554 SBC-39768 SBC-40086	The device raises a CPU Overload alarm for task - NWST	CPU overload alarm may cause loss of service.	High	HA	n/a
SBC-37811	The device marks the acKpiMediaStatsCurrentIpGroupMediaQualityOut KPI as "0" even though there are no active calls.	Wrong KPI	Medium	All	n/a
SBC-38292	The device doesn't send a retransmission of SIP 200 OK over TCP.	No impact	Low	All	n/a
SBC-38695	The device indicates low fan speed if overheated when using the latest iLO.	Wrong fan speed presentation	Low	Mediant 9000	n/a
SBC-38738	The device runs out of resources – (SIPSockets) printing "[ERROR] ResourcePool<SIPSocket>:: GetNewObject Failed - GetId failed - no more free IDs available - m_NumberOfAllocatedObjects=200'"	Device fails to maintain connection with proxies	Medium	All	n/a
SBC-38775	The device runs out of TLS resources because it considers each new connection request without an alias as a non-reusable connection.	Device fails to maintain connection with proxies	Medium	All	n/a
SBC-38856	The device fails to handle a file (ini) upload request from OVOC with the error message "OBJECT POOL DEBUG: Pool(RfsReq) is full".	OVOC fails to upload file from device	Medium	All	n/a
SBC-38913	Uploading an ini file to the device with a different "DeviceTable" causes a disconnection with the device (requires a hardware reset to recover).	Device loses connectivity	Medium	All	n/a
SBC-39112	If the word "Any" appears in the IP Group's name, the	Wrong Web interface	Low	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
	device displays the IP Group as "Any" only.	presentation of IP Group name			
SBC-39118	The device's Automatic Update mechanism uses the definitions of the Proxy Set (even if the same), causing the device's endpoints to lose their registrations (until the next re-registration).	Device endpoints shown as not registered	Medium	Gateway	n/a
SBC-39219	Calls are disconnected after an HA switchover if SIP INVITEs are defined to be supported only with SDP.	Calls are disconnected after a switchover	High	Mediant CE	n/a
SBC-39337	The device undergoes a switchover when doing an SNMP walk.	Device switchover	Medium	HA	n/a
SBC-39340	NAT translation doesn't support IPv6.	IPv6 addresses are not NAT translated	Medium	All	n/a
SBC-39361	Device login using LDAP fails as the user is mistakenly considered as belonging to two different groups with overlapping names (e.g., "ABC" and "BC01").	Web access failure	Medium	All	n/a
SBC-39482	The device resets due to a hardware watchdog related to a memory leak ("Task SPLB").	Device reset	Medium	Mediant 800	n/a
SBC-39490	Alarm raised about time differences between Metering server and device.	No real impact – only a repeated alarm	Low	All	n/a
SBC-39497	Alarms in the Active Alarms and History Alarms tables are displayed in wrong order.	Web interface presentation changed	Low	All	n/a
SBC-39515	The Web interface's Save button is highlighted after a CLI Script file upload (even if there are no configuration changes).	Web interface's presentation	Low	All	n/a
SBC-39527	The device opens a channel with DTMF set to transparent instead of RFC 2833 for a specific fax scenario.	No DTMF's	Medium	All	n/a
SBC-39538	The device fails to remove the ARM header 'X-ARM-	Transfer failure	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
	DETAIL' and issues the syslog error "ArmRemoveHeader - header X-ARM-DETAIL-1 wasn't found".				
SBC-39546	The device fails to transfer CDRs (saved on local storage) over WinSCP.	CDR failure	Medium	All	n/a
SBC-39547	The device resets with "TASK: SPMR" because of an internal buffer overrun.	Device reset	Medium	All	n/a
SBC-39550	The device downloads the CDR files in wrong format (no ".gz/" suffix).	CDRs can't be extracted	Medium	All	n/a
SBC-39595	The device fails to resolve DNS on the redundant unit.	DNS failure	Medium	HA	n/a
SBC-39601	Dial Plan rules with a prefix containing characters fails to get re-applied because of incorrect case-sensitive mode.	Dial Plan rule can't be re-applied	Low	All	n/a
SBC-39620	The device generates the syslog error message "Num of Framers detected on board is zero (MaxTrunkNum=0)".	No impact – only unnecessary syslog messages	Low	Mediant 800	n/a
SBC-39678 SBC-39864	The device fails to clear the old cache of DNS resolved IP addresses, causing wrong DNS resolutions.	Wrong DNS resolutions when using cache	High	All	n/a
SBC-39767	HA Hitless Upgrade failure occurs from 7.40A.005.619 to 7.4.250.	Hitless upgrade failure	High	HA	n/a

2.23 Version 7.40A.250.440

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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 (8.0.3180 or later) and Version 8.2 (8.2.265 or later).
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to a compatible version (stated 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 (stated 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.

2.23.1 New Features

This section describes the new features introduced in this version.

2.23.1.1 Network Interface Status Check for Mediant VE/CE Deployed in Microsoft Azure Cloud

Mediant VE/CE SBC deployed in Azure cloud may experience intermittent problems in communication with virtual hosts that may cause the virtual network interface (NIC) to "freeze".

To overcome this issue, Mediant VE/CE periodically checks the status of all network interfaces to detect if this condition exists and mitigates it by performing a maintenance reboot.

The new parameter [NetworkInterfaceStatusCheck] enables this feature.

Applicable Application: SBC.

Applicable Products: Mediant VE/CE.

2.23.1.2 User Authentication by Local Users Table before LDAP/RADIUS

When authenticating users logging in to the device, the Local Users table can be used first for authentication and only if authentication fails, will the device use the LDAP or RADIUS authentication server (if configured).

This feature is supported by the new optional value **Always Before Auth Server** for the existing 'Use Local Users Database' parameter.

Applicable Application: All.

Applicable Products: All.

2.23.2 Resolved Constraints

This section lists resolved constraints.

Table 2-25: Resolved Constraints in Version 7.40A.250.440

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-32171	Device vulnerability of Dynamic Data Exchange (DDE) injection in Dial Plans.	A specific combination of characterS IN THE Dial Plan can activate some Windows OS commands.	Low	All	n/a
SBC-35116	The device's Web interface is not accessible over LDAP when using many REST calls with LDAP authentication enabled.	Web interface not accessible	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-35568	Columns of the Web interface's IP-to-IP Routing table can't be resized when using Google Chrome.	Web interface presentation is limited.	Low	All	n/a
SBC-37044 SBC-38171	When in HA mode, the WebSocket connection with OVOC can't be re-established after a switchover.	Device loses connection with OVOC after a switchover.	High	All HA	n/a
SBC-37048	When in HA mode, the device doesn't send alarms when one of its ports are down.	No impact	Low	Mediant 9000 HA	n/a
SBC-37199	When in HA mode and deployed on an AWS c5.9xlarge machine with transcoding profile, the device fails to upgrade to 7.40A.250 because of a DSP reset.	Device fails to upgrade	High	Mediant Software HA	AWS
SBC-37239	When the device interworks with Broadworks, it fails to display more than one alias in its user registration database.	Partial WEB interface presentation of the device's registration database	Medium	All	n/a
SBC-37261	The device's syslog server stops working.	No syslog messages are sent by the device	Low	All	n/a
SBC-37265	The device sends an SDP answer with SRTP (RTP\SAVP) without any crypto suites on calls to VoiceAI Connect.	Calls fail due to no voice	Medium	All	n/a
SBC-37301	The device's CmdShell command "Show DSP Perf" doesn't display any output.	CMDShell command doesn't work	Low	All	n/a
SBC-37700	The device's HTTP Server Groups using TLS Contexts are not valid after upgrading to 7.40A.250.	Invalid configuration	Medium	All	n/a
SBC-37763	The device doesn't show the DstSN (Destination Sub Number) when there is no destination number for Tel-to-IP calls.	Incomplete call numbers	Medium	Gateway	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-37765 SBC-38520 SBC-38549	The device fails to send a DNS query for SRV type records if DNS is not configured.	Calls failure because of no DNS resolution	High	All	n/a
SBC-37778	The device restarts when using ARM to handle an IP-to-Tel call with a non-existing alternative route.	Device restarts	Medium	Gateway	n/a
SBC-37892	When in HA mode and deployed on Azure, the device undergoes several consecutive switchovers, causing one of the Ethernet ports to "freeze".	Device non-functional	High	HA	Azure
SBC-37934	The device sends an ini file to OVOC (upon a backup request) containing some ini file headers, causing OVOC to reject the ini file.	OVOC backup fails	Medium	All	n/a
SBC-38105	The device's Active Alarm table displays flapping acDebugRecordingActivationAlarm (DR activate) alarm.	Flapping alarms	Medium	All	n/a
SBC-38133	The device doesn't send SIP REGISTER messages beyond the first 172 ports.	Failed user registrations	High	MP-1288	n/a
SBC-38193	The device loses connection with OVOC after an upgrade to 7.40A.250.	No connection to OVOC	High	All	n/a
SBC-38480	The device fails to issue an HTTP request and the syslog error "[ERROR] Failed get write buffer from pool" is generated.	Call failure	High	All	n/a
SBC-38839	The device switches from SRTP tunneling to SRTP forwarding without any reason, causing no voice on the call	Call failure	High	All	n/a

2.24 Version 7.40A.250.366

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

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

2.24.1 Resolved Constraints

This section lists resolved constraints.

Table 2-26: Resolved Constraints in Version 7.40A.250.366

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-39545 SBC-39742	Performance Monitoring values are not aligned towards OVOC, causing reports of value "0".	Incorrect Performance Monitoring	High	All (Media Transcoding \ Media Transcoding Cluster setup)	All

2.25 Version 7.40A.250.364

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

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

2.25.1 Resolved Constraints

This section lists resolved constraints.

Table 2-27: Resolved Constraints in Version 7.40A.250.364

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-37563	The device failed to add DSP resources on a call that changed from RTP forwarding to transcoding for the AMR coder.	Call failure	High	All (Media Transcoding \ Media Transcoding Cluster setup)	All

2.26 Version 7.40A.250.363

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

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

2.26.1 New Features

This section describes the new features introduced in this version.

2.26.1.1 Locally Stored SDRs Download through SFTP

SDR files stored locally on the device (*Local Storage*) can now be downloaded through SFTP.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.26.1.2 Password Complexity for SNMPv3 Users

Password complexity, configured by the existing [EnforcePasswordComplexity] parameter, now also applies to SNMPv3 users (configured in the SNMPv3 Users table). This is used for the 'Authentication Key' and 'Privacy Key' fields.

Applicable Application: All.

Applicable Products: All.

2.26.2 Resolved Constraints

This section lists resolved constraints.

Table 2-28: Resolved Constraints in Version 7.40A.250.363

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-33324	The device's BRI trunks don't establish a link after device reset when connected to NTT BRI circuits.	BRI trunks are not active after reset	Low	Gateway (BRI interfaces)	n/a
SBC-33534	Removing a BRI module in hot-swap mode fails to send an un-REGISTER message if the BRI trunk is configured as Network side.	Proxy does not receive any notification for re-REGISTER.	Low	Gateway (BRI interfaces)	n/a
SBC-34807	The device's TEL LED doesn't turn red when trunks are out-of-service.	Incorrect display in Web interface.	Low	Mediant 3100	n/a
SBC-35124 SBC-35865	The device doesn't send a SIPREC XML body to VoiceAI Connect.	SIPREC for VoiceAI Connect calls fail	High	All	All
SBC-35228	The device sends a SIP ACK request (in response to a 487 response) with the wrong URI in the To and Request-URI headers.	No impact	Low	All	All
SBC-35388	The device generates empty SDR reports upon a specific transfer scenario when the SDRRecordType parameter is set to default (STOP).	SDRs are not collected nor sent.	High	All	All
SBC-35456	The device reports Caller ID to an analog phone with invalid date and time, causing the Caller ID not to be displayed	No Caller ID	Medium	MP-1288	n/a
SBC-35597	The device fails to detect broken connection upon a call from A to B, where only B sends RTP.	Broken Connection mechanism failure	Medium	All	All

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-35598	The device doesn't consider crypto changes if the SDP version was not changed, causing one-way voice.	One-way voice	Medium	All	All
SBC-35612	The device fails to send a DNS request for resolving the FQDN of the QoE server (OVOC) on any interface that is not the OAMP interface.	QoE DNS-resolved failure	Medium	All	All
SBC-35640	The device's Web interface doesn't show the Coder Groups table properly for Monitor user levels.	Web interface display bug	Low	All	All
SBC-35641	The device runs out of "gwSession" resources, causing Message Manipulation rules to not being executed.	Message Manipulation rule failures	Medium	All	All
SBC-35889	The device sends an SDP answer based on a terminated SDP offer for transcoding calls, causing some changes in the SDP to be rejected by the far side.	SDP rejected because of incorrect fields	Medium	All	All
SBC-35890	When deployed in Azure, the device experiences no voice when receiving a SIP re-INVITE after an HA switchover.	No voice after HA switchover	High	High-Availability (HA) devices	Azure
SBC-35980	The Performance Monitoring parameter acKpiCoderStatsCurrentIpGroupCoderG711 is increased upon a specific scenario - G.711A-law call, where outgoing side is configured with ICE and rejects the call with SIP 486.	Incorrect Performance Monitoring report	Medium	All	All
SBC-36225	The device doesn't disconnect the call when receiving a SIP 481 (Transaction Does Not Exist) for a re-INVITE.	Call is not terminated normally	Medium	All	All
SBC-36331	The device adds trailing zeros to the SIP Contact header's 'q' parameter.	Invalid header's parameter	Low	All	All
SBC-36332	The device reports MOS over REST on scales of 1 to 50 instead of 1 to 5.	Incorrect scale for MOS reports	Low	All	All

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-36347	The device doesn't allow special characters (% and !) in the TLS private key.	The device doesn't accept the private key's passphrase	Medium	All	All
SBC-36360	When configured to operate with an external LDAP Authentication server, the device may reset after a specific sequence of unsuccessful CLI logins.	Device resets	Medium	All	All
SBC-36371	The device resets upon configuration of max. Proxy Sets, where all have a different domain name that are resolved into the same IP address.	Device resets	High	All	All
SBC-36503	The device doesn't change its crypto on a SIP re-INVITE when the far side changed its crypto on an SRTP forwarding call, causing one-way voice.	One-way voice after a re-INVITE	Medium	All	All
SBC-36553	The device doesn't behave according to the IP Profile parameter EnableSymmetricMKI on re-INVITE sessions, sometimes adding the MKI when the far side sends an SDP offer without MKI, causing one-way voice.	One-way voice after a re-INVITE	Medium	All	All
SBC-36667	Logging Filter rules don’t work after debug recording is stopped and applied, unless refreshed	Debug recording needs to be refreshed to function	Low	All	All
SBC-36692	When debug recording is activated, the redundant device raises alarms ("Board Fatal Error: Debug Recording is running").	False alarm from the redundant device	Low	HA devices	All
SBC-36884	When deployed in Azure, the device experiences OAuth request failures after several delays from the OAuth server.	Authentication failures after server’s timeout	Medium	Mediant Software	Azure
SBC-37231	The device resets after receiving a SIP 4xx response from one of the alternative routes in a complicated routing configuration that uses both internal routing and forking.	Device resets	High	All	All

2.27 Version 7.40A.250.270

This version includes resolved constraints only.

Note: This version is applicable only to Mediant 90xx and Mediant VE/CE/SE SBCs.

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: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

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

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

2.27.1 Resolved Constraints

This section lists resolved constraints.

Table 2-29: Resolved Constraints in Version 7.40A.250.270

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-36694 SBC-36757	Device upgrade sometimes fails due to a timeout when upgrading a device running a 7.2CO or a 7.4.x version.	Unable to complete a hitless upgrade	High	Mediant 9030/9080; Mediant VE/CE/SE	All

2.28 Version 7.40A.250.265

This version includes resolved constraints only.

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

Starting with Version 7.40A.250.001, the .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:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

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.
  - √ OVOC Version 8.0.3137 is compatible with both device versions 7.2 and 7.4.
  - √ 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.

2.28.1 Resolved Constraints

This section lists resolved constraints.

Table 2-30: Resolved Constraints in Version 7.40A.250.265

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-36154 SBC-36335 SBC-36439	When the SBC is connected to ARM, a device restart may occur when receiving a SIP CANCEL message and sending a GetRoute message to ARM as part of a specific signaling scenario.	Device restart	High	All	SBCs connected to ARM
SBC-36437	In Azure installations, device upgrade may fail in some cases when upgrading from an earlier version that is based on CentOS 8.	Unable to complete software upgrade and device needs to be restarted	High	Mediant CE/VE deployed in Azure	Azure

2.29 Version 7.40A.250.262

This version includes known constraints and resolved constraints.

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

Starting with Version 7.40A.250.001, the .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:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

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.
  - √ OVOC Version 8.0.3137 is compatible with both device versions 7.2 and 7.4.
  - √ 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.

2.29.1 Known Constraints

This section lists known constraints.

Table 2-31: Known Constraints in Version 7.40A.250.262

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-36154 SBC-36335 SBC-36439	When the SBC is connected to ARM, a device restart may occur when receiving a SIP CANCEL message and sending a GetRoute message to ARM as part of a specific signaling scenario.	Device restart	High	All	SBCs connected to ARM
SBC-36437	In Azure installations, device upgrade may fail in some cases when upgrading from an earlier version that is based on CentOS 8.	Unable to complete software upgrade and device needs to be restarted	High	Mediant CE/VE deployed in Azure	Azure

2.29.2 Resolved Constraints

This section lists resolved constraints.

Table 2-32: Resolved Constraints in Version 7.40A.250.262

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-34717 SBC-35937 SBC-35600	The device fails to connect to the RSyslog server over TLS when the certificate's CN/SAN contains dots in it.	RSyslog server doesn't receive syslog messages from the device	Medium	All	All
SBC-35759	In some cases, the device changes its crypto numbering ('a=crypto') in a SIP re-INVITE, creating an illegal SDP offer.	SIP re-INVITE session failure and call disconnection	High	All	All
SBC-35867	Device registration fails after the 10th attempt because of an error in the device's database of port usernames/passwords.	Random registration failures occur after 10 successful registrations	Medium	All	All
SBC-36183 SBC-36246 SBC-36308	Web login over LDAP sometimes fails, after the device was upgraded to 7.40A.250.255.	Unable to login to the device's Web interface	High	All	All
SBC-36042	CVE-2022-0778 (OpenSSL Denial of Service).	A flaw was reported in OpenSSL – it's possible to trigger an infinite loop in OpenSSL by crafting a specific certificate that has invalid explicit curve parameters. OpenSSL was updated to 1.1.1.n, which resolves this CVE.	High	All	All

2.30 Version 7.40A.250.255

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

Note: Version 7.40A.250.255 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, the .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:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

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.
  - √ OVOC Version 8.0.3137 is compatible with both device versions 7.2 and 7.4.
  - √ 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.

2.30.1 New Features

This section describes the new features introduced in this version.

2.30.1.1 Security Enhancements

The following security enhancements have been introduced:

- Password complexity, enabled by the existing [EnforcePasswordComplexity] parameter, now also applies to SNMPv2 Community Strings. Up until now, it applied only to user login passwords.
- The Activity Log ('Action Executed)' now also logs file downloads through Web interface.
- If a management user in the Local Users table is modified or deleted, and the user is currently logged into the device, the device immediately logs the user out of the management interface.
- The login password of users in the Local Users table can't be the same as any of the last (previous) four passwords. This is enabled using the new ini file parameter [CheckPasswordHistory].

Applicable Application: All.

Applicable Products: All.

2.30.1.2 Global Configuration of Syslog Severity Level

The syslog severity level can now be configured globally, using the [SyslogLogLevel] ini file parameter. In addition, for this parameter and for the existing 'Severity Level' parameter in the Syslog Servers table, the optional values **Debug** and **Info** have been renamed **Debug [not recommended]** and **Info [not recommended]** to indicate that setting the severity level to any of these values may cause excessive use of device resources.

Applicable Application: All.

Applicable Products: All.

2.30.1.3 Restore to Factory Defaults with TLS Files Deletion

To enhance security, when restoring the device to factory defaults (`write factory`), the administrator can also optionally delete TLS-related files (TLS certificates, root certificates and public keys). This feature is configured by the new option, `clear-keys-and-certs`:

```
# write factory clear-keys-and-certs
```

Applicable Application: All.

Applicable Products: All.

2.30.1.4 New SNMP Alarm for No DNS Reply

The new SNMP alarm acNoReplyFromDNSServerAlarm has been added, which is raised when the device sends a DNS query, and the DNS server doesn't reply. DNS queries are sent for Proxy Sets configured with FQDNs.

Applicable Application: All.

Applicable Products: All.

2.30.1.5 Temperature Alarm Update for Mediant 4000B

The conditions for raising and clearing the SNMP alarm acBoardTemperatureAlarm has been updated. The alarm is now raised when the critical temperature threshold minus 5 is reached. It's cleared when it falls below this threshold minus 5, for a duration of at least 60 seconds.

Applicable Application: SBC.

Applicable Products: Mediant 4000.

2.30.1.6 CPU and Memory Utilization in Syslog

The device can be configured to send CPU and memory utilization in syslog messages. This is configured through CLI, using the following new CLI command:

```
debug os-util memory|cpu [interval]
```

Applicable Application: All.

Applicable Products: All.

2.30.1.7 BID and UUID in Management Interfaces

Board ID (BID) and UUID (applicable only to Mediant 90xx and Mediant Software) are now available in the device's management interfaces (Web, CLI and ini file).

Up until now, BID and UUID were displayed only in syslog messages.

Applicable Application: All.

Applicable Products: All.

2.30.2 Known Constraints

This section lists known constraints.

Table 2-33: Known Constraints in Version 7.40A.250.255

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-35152	The 'SDR Type' parameter was added to the SBC SDR Format table in Version 7.4.250 and by default, the parameter is set to **Syslog SBC**. When upgrading from an earlier version to 7.4.250 or later, all existing rules are set to this default (syslog), even though in earlier versions all rules applied to both syslog and local storage. If you want to also apply rules for local storage, you need to manually add rules and set the 'SDR Type' parameter to **Local Storage SBC**.	SDRs not sent to local storage.	High	Mediant 90xx; Mediant Software	All
SBC-36042	CVE-2022-0778 (OpenSSL Denial of Service).	A flaw was reported in OpenSSL – it's possible to trigger an infinite loop in OpenSSL by crafting a specific certificate that has invalid explicit curve parameters.	High	All	All
SBC-36436	When using Media Transcoding Cluster (MTC), an MT hitless upgrade can't be stopped using OVOC.	MT hitless upgrade can't be stopped using OVOC (can be stopped using Web interface)	Medium	Mediant CE (Elastic Media Cluster); Mediant VE (Media Transcoding Cluster)	Elastic Media Cluster and MTC

2.30.3 Resolved Constraints

This section lists resolved constraints.

Table 2-34: Resolved Constraints in Version 7.40A.250.255

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-32169	The device's SNMPv2 community string is shown in the Activity Log when configured.	Security breach, as the community string is exposed	Medium	All	All
SBC-32172	A CLI command output was able to show device passwords.	Possible security breach, as passwords may be exposed to authenticated device users that have access the CLI.	Medium	All	All
SBC-33351	The device disconnects from OVOC when the value of the parameter [WSTunUsername] contains special characters (invalid).	Connection to OVOC is lost	Medium	All	All
SBC-34003	The device sends a SIP Date header in an invalid format for the seconds (255 instead of 00).	Call failure due to inability of far side to obtain the Date header.	Medium	GW	n/a
SBC-34021	The device's Web interface fails to display all information about the TLS Context's SAN.	SAN information can't be obtained from Web interface.	Low	All	n/a
SBC-34053	The device rejects a new SIP INVITE with old random Contact - [UseRandomUser] parameter configured to 2 (per register) - after a failure of a new registration attempt (with new random Contact user part).	Call failure.	Low	All	n/a
SBC-34118	The device replies with a 404 (instead of 204) to a REST API query for /api/v1/alarms/active.	Incorrect REST API response from device.	Low	All	n/a
SBC-34293	The device fails to handle a transfer request when the transferor and the transferee are on a different SIP Interface.	Transfer failure.	Medium	All	n/a

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-34330 SBC-34417	The device runs out of Call-ID resources on high traffic.	Call failure on high traffic volume.	Medium	All	n/a
SBC-34431	The device receives a SIP INVITE with a User-To-User header that has UUI data longer than 512 bytes and truncates it incorrectly.	Incorrect UUI data.	Low	All	n/a
SBC-34436	The device's Web interface shows XML body leftovers when browsing through a long IP-to-IP Routing Table.	Incorrect Web interface display.	Low	All	n/a
SBC-34679	The device fails to complete a DTLS handshake on SIP-to-WebRTC calls when [NATMode] parameter is configured to 4, sending packets to port 0.	No voice on SIP-WebRTC calls located behind NAT.	Medium	All	n/a
SBC-34727	The device doesn't save the value of the IP TOS after an HA switchover.	Incorrect DSCP on RTP packets.	Medium	HA	HA
SBC-34773	The device's Tel-to-IP Routing table gives incorrect matching results based on the destination prefix pattern.	Incorrect routing.	Medium	Gateway	-
SBC-34804	The [RFC2833RxPayloadType] and [RFC2833TxPayloadType] parameters are hidden in CLI (under configure voip/media rtp-rtcp).	n/a	Low	Gateway	-
SBC-34809	The device raises a false alarm for missing certificate when TLS Context is not the default one and both private key and certificate are not defined.	False certificate alarm.	Medium	All	All
SBC-34945	The device's Web interface displays incorrect Network Topology display.	Incorrect Web interface display.	Low	All	All
SBC-34946	The device resets upon querying a domain name received on a call transfer.	Device reset.	High	All	All
SBC-35145	SIP OPTIONS keep-alive messages that the device sends, fails due to a false ICMP unreachable report from the OS. As a result, calls fail. This issue has been resolved by the new parameter AbortRetriesOnICMPError (CLI - abort-retries-on-icmp-error).	Call failure.	High	All	All

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-35155	The device restores all parameters to default upon the receipt of an ARM HTTP PUT for an update, instead of updating the relevant parameters only.	Unnecessary parameter changes.	Low	All	All
SBC-35220	The device ignores a DTLS handshake successfully ended event in the middle of opening the channel while changing from transcoding to RTP forwarding.	No voice on WebRTC-to-WebRTC calls.	High	All	All
SBC-35266	The device handles HTTP response headers as case-sensitive and fails to handle "content-length" if the "C" of content and "L" of length are not in upper case.	Device ignores legal HTTP responses causing call failure.	Medium	All	All
SBC-35412	The device stops sending Activity Logs messages to syslog.	n/a	Low	All	All
SBC-35421 SBC-35461	The device's WebSocket connection to OVOC doesn't function in 7.4.250.	Floating License failure when using WebSocket.	High	All	All
SBC-35453	The device resets with the next exception (Signal 904, Task SPMR) due to a software watchdog caused by maintaining the call preemption list.	Device reset.	High	All	All
SBC-35535	The device resets with the next exception (Signal 6, Task SPMR) due to executing a Call Setup Rule with an ENUM query, where the destination target is internal.	Device reset.	High	All	All
SBC-35569	The device's Web interface stops responding when a new IP-to-IP Routing rule is added in HA systems.	n/a	Medium	HA	HA

2.31 Previous Latest Release (LR) Versions

This section describes the previous LR versions of Release 7.4.

2.31.1 Version 7.40A.250.010

This version includes resolved constraints only.

Note: This version is applicable only to Mediant VE/CE SBCs on Azure.

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

Starting with Version 7.40A.250.001, the .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:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

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.
  - √ OVOC Version 8.0.3137 is compatible with both device versions 7.2 and 7.4.
  - √ 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 version is compatible with Stack Manager Version 2.5.2 or later.

2.31.1.1 Resolved Constraints

This section lists resolved constraints.

Table 2-35: Resolved Constraints in Version 7.40A.250.010

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-35094 SBC-35151 SBC-35119 SBC-35636 SBC-35704	Following a recent update of the Microsoft Azure Linux Agent, the Agent functionality was found to be incompatible with the 7.4 software versions of AudioCodes SBC when deployed on Azure.	Major service disruption may occur in various scenarios, including loss of connectivity, loss of access to the device and/or call failures.	Critical	Mediant Software on Azure	Azure
SBC-34914 SBC-34691 SBC-35216 SBC-35748 SBC-35373	SBC hitless upgrade sometimes fails when upgrading from 7.2.258CO.xxx\7.40A.005.xxx to any 7.40A.xxx.xxx version.	Unable to complete a hitless upgrade.	High	Mediant Software on Azure	Azure

2.31.2 Version 7.40A.250.004

This version includes resolved constraints only.

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

Starting with Version 7.40A.250.001, the .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:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2555 or later.
  - √ OVOC Version 8.0.2555 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to Version 8.0.2555 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 8.0.2555 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 version is compatible with Stack Manager Version 2.5.2 or later.

2.31.2.1 Resolved Constraints

This section lists resolved constraints.

Table 2-36: Resolved Constraints in Version 7.40A.250.004

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-33985	WebRTC-to-WebRTC calls fail due to a DTLS handshake error upon a SIP re-INVITE message before initial DTLS negotiation ends.	Agent-to-agent WebRTC calls fail.	High	All	All
SBC-34308	A device reset may occur when retrieving a file through SFTP.	Device reset.	High	All	All

2.31.3 Version 7.40A.250.001

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

IMPORTANT NOTICE for MEDIANT CE SBC

For upgrading Mediant CE SBC to this version, you **must** follow the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

Note:

- Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to a 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, and Mediant 4000:**

  Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2555 or later.
  - √ OVOC Version 8.0.2555 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to Version 8.0.2555 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 8.0.2555 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.

Note: This version is compatible with Stack Manager Ver. 2.5.2 or later.

2.31.3.1 New Features

This section describes the new features introduced in this version.

2.31.3.1.1 Digitally Signed Software Files (.cmp)

Software update files (.cmp) are now digitally signed, preventing the loading of tampered or corrupted .cmp files to the device.

Note: Once the device has been upgraded to a signed .cmp file, it can only be downgraded or upgraded to a signed .cmp file. For upgrade instructions using signed .cmp files, refer to the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.3.1.2 Floating and Flex Licensing for WebRTC and SIPRec Sessions

WebRTC and SIPRec session capacity can now be licensed through the Floating and Flex licensing models, which are managed by OVOC. This is supported from OVOC Version 8.0.3000 or later.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.3 SIPRec Recording Triggered by REST

The device can now be triggered through REST API to stop and start recording (SIPRec sessions) of calls with a Session Recording Server (SRS). Call recording is triggered upon the receipt of a REST message (HTTP POST request) containing specific fields, and the matching of a rule in the existing SIP Recording Rules table that specifies SIPRec triggered by REST.

The following configuration updates have been done to support this feature:

- SIP Recording Rules table:
  - The 'Trigger' parameter has a new optional value called **REST**.
  - The new 'Recording Server Role' parameter can be optionally used as a matching condition for using the SIP Recording rule. If configured (string), the same value must be present in the incoming REST message ("role" field) for the rule to be chosen.
- REST message and Message Manipulation:

  As REST messages are sent out of call context (i.e., not in SIP messages), the device needs a way to determine which call to record. This is done using a "call key". If the call key value in the incoming REST message is the same as the call key value of the INVITE message, the device identifies the call as the one to record.

The call key value of the INVITE message is obtained using a Message Manipulation rule with the newly supported syntax variables *Param.Call.HashKey* or *Param.Peer-Call.HashKey*. For example, the rule can be configured to obtain the call key value from a specific SIP header. (The rule is used internally only and doesn't modify the outgoing INVITE message.)

The REST message can also specify additional SIP headers (and their values) to add to the outgoing INVITE message sent to the SRS. It can also specify the user part of the SIP Request-URI in this INVITE message.

Below shows an example of a REST message (with mandatory and optional fields) used for triggering SIPRec:

```
{
  "command": "start",
  "callKey": "aa_bbaa",
  "role": "AgentAssist",
  "callRecordingDestUsername": "AgentAssistBot",
  "headers": [
    {
      "name": "X-MyCallId",
      "value": "dddd-eeee"
    },
    {
      "vame": "X-MyAccount",
      "value": "4567876565"
    }
  ]
}
```

Applicable Application: All.

Applicable Products: All.

2.31.3.1.4 SDR Reporting to REST Server using REST API

The device can now send SDRs to a remote HTTP-based REST server, using the device's REST API. The SDRs are sent in JSON format.

This feature is supported by the following new parameters:

- 'SDR REST': Enables SDR reporting (disabled by default).
- 'REST SDR Record Type': Defines the type of SDR records to send (e.g., for failed call attempts).
- 'REST SDR HTTP Server Name': Defines the REST server (configured in the Remote Web Services table) to where the SDRs are sent.
- 'SDR Type' in the SBC SDR Format table: Defines the SDR type and one of the options is JSON SBC for customizing SDRs sent to REST server.

Applicable Application: SBC.

Applicable Products: Mediant Software; Mediant 90xx.

2.31.3.1.5 Mediant 3100 Support for 64 T1/E1

The Mediant 3100 SBC and Media Gateway now supports up to 64 E1/T1 PSTN digitalized trunks.

Applicable Application: Gateway.

Applicable Products: Mediant 3100.

2.31.3.1.6 Enhanced PII Masking in CDRs Sent to OVOC and External Servers

The following new parameters have been added for masking of PII in CDRs:

- 'Mask PII in CDRs for OVOC' (PIIMaskPrivateInfoForOVOC): Masks (with asterisks) phone numbers, URI user part, and display names that appear in CDRs sent to OVOC.
- 'Mask URI Host Part in CDRs' (PIIMaskHost): Masks (with asterisks) the host part of URIs (including IP addresses) in CDRs sent to Web, CLI, Syslog, REST, RADIUS, and Local Storage (depending on PIIMaskPrivateInfoInCDRs), or to OVOC if PIIMaskPrivateInfoForOVOC is enabled.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.7 SBC Cloud-Init Enhancements

Cloud-init configuration scripts can now be loaded to the SBC virtual machine through Azure user data. User data can also be used after initial setup. Up until now, only Azure custom data was supported (used only for initial setup).

In addition, the device now supports Version 2 of AWS EC2 Instance Metadata service (IMDSv2), which is used to load cloud-init to the SBC virtual machine and used for HA functionality. Up until now, only IMDSv1 was supported.

Applicable Application: SBC.

Applicable Products: Mediant VE/CE.

2.31.3.1.8 Registration Status of SIP Accounts in Web Interface

The Accounts table now displays the status per Account in the new 'Account Registration Status' field.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.9 IP Group Classification based on Source IP Address and SIP Attributes

When the Classification table is used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to IP Groups, the device can now also be configured to verify that the request was sent from one of the IP addresses (including DNS-resolved IP addresses) in the Proxy Set associated with the IP Group.

This feature is applicable to classification both by Proxy Set (IP Group's 'Classify By Proxy Set' parameter) and by Classification table rules. However, this feature is typically implemented when classification is according to Classification rules when you need to classify SIP dialogs originating from the same Proxy Set into multiple IP Groups and where Classification rules are necessary to produce the desired mapping (classification) to the different IP Groups.

This feature is configured using the new 'Validate Source IP' parameter in the IP Groups table.

Note:

- Validation is done after Classification, but before Manipulation and Routing.
- Validation is done for the IP address only (not port, transport, or SIP Interface).
- Upon validation failure, the device rejects the incoming SIP dialog with a 500 SIP

response (Reason header value is "Source IP does not match Proxy Set").

- This feature is typically used for Server-type IP Groups. However, it can also be used for User-type IP Groups.
- This feature should not be enabled if 'Classify By Proxy Set Mode' is configured to **Contact Header** or **Both**, as in most cases, the source IP address of the SIP message will not be a member of the Proxy Set.

Applicable Application: SBC.

Applicable Products: All.

2.31.3.1.10 Pause and Resume SIPRec Triggered by SIP INFO Messages

The device can now be triggered through SIP INFO messages to pause and resume SIPRec recordings. Up until now, only start and stop recording was supported.

Pause and resume recording are triggered by the following new parameters in AudioCodes proprietary X-AC-Action header in SIP INFO messages:

```
X-AC-Action: pause-siprec;recording-ip-group=<ID>
X-AC-Action: resume-siprec;recording-ip-group=<ID>
```

Applicable Application: SBC.

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

2.31.3.1.11 UUID Generation for Session ID by Message Manipulation

The device can now be configured to generate a random Universally Unique Identifier (UUID) value. This can be used, for example, to associate a unique identifier to specific calls.

UUID generation is done using the new keyword "Func.UUID-Generate" in the Message Manipulations table or Call Setup Rules table ('Action Value' field). For example, a Call Setup Rule can be configured to add to the SIP message a header called "My-Identifier" with a unique UUID for each new call.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.12 Retrieval of Call Trigger by Call Setup Rules

Call Setup Rules can now be used to obtain the trigger (e.g., due to a SIP 3xx or call transfer) for re-routing calls to alternative destinations. This applies to call re-routing that is handled locally by the device (e.g., 'Remote REFER Mode' configured to **Handle Locally** for call transfer).

This feature is supported by the new optional value "Param.Routing.Trigger" for the 'Action Value' parameter in the Call Setup Rules table. For example, you can configure a rule to add the call trigger to a new header in the outgoing SIP re-INVITE message.

(The IP-to-IP Routing table's parameter 'Call Trigger' defines the trigger type required for re-routing the call using the specific routing rule.)

Applicable Application: SBC.

Applicable Products: All.

2.31.3.1.13 Referred By Tags in Call Setup Rules

Dial Plan tags of call parties that initiate (i.e., transferor) call transfer (REFER message) can be used in the Call Setup Rules table as conditions ('Condition' field) or values ('Action Value'). This is supported by the new optional field value, "ReferredByTags".

For example, a Call Setup Rule can be configured to add a specific prefix to the destination number of calls that are transferred by an IP Group whose tag is "PBX".

Applicable Application: SBC.

Applicable Products: All.

2.31.3.1.14 Retrieval of Global Session ID by CSR or Message Manipulation

Call Setup Rules and Message Manipulation rules can now be used to obtain the global session ID of the call. This is supported by the new optional value "Param.Session.GID" in the 'Action Value' parameter of these tables. For example, you can configure a rule to add the global session ID to a new header in the outgoing SIP message.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.15 New SDR Fields

The following new SDR fields have been introduced in this version:

- 'Ingress Call Orig' and 'Egress Call Orig': Displays the direction of the call (incoming or outgoing).
- 'Is Success': Displays if the call succeeded.
- 'Ingress SIP Term Description' and 'Egress SIP Term Description': Displays the description of the SIP call termination reason for the incoming and outgoing legs.
- 'IsRecorded': Displays if the call leg was recorded (SIPRec).
- 'Global Session ID': Displays the global session ID.
- 'ReferredBy Tags': Displays the tags of the call leg that initiated the call transfer.

Applicable Application: SBC.

Applicable Products: Mediant Software; Mediant 90xx.

2.31.3.1.16 Direct Media Calls using Proprietary X-AC-Action SIP Header

The device can now identify incoming SIP dialog-initiating requests (e.g., INVITE messages) as direct media calls (i.e., media doesn't traverse device), based on AudioCodes' proprietary 'X-AC-Action' SIP header. If the header contains the newly supported value 'direct-media' (i.e., 'X-AC-Action: direct-media'), the device handles the call as direct media. The device doesn't allocate any resources to these calls, and they remain as direct media calls until they end.

Note that parameters that enable and disable direct media, for example, the global [SBCDirectMedia] parameter are ignored for these calls.

Applicable Application: SBC.

Applicable Products: All.

2.31.3.1.17 SNI-to-TLS Context Mapping

The device can now be configured to use a specific TLS Context according to the name of the server (Server Name Indication or SNI).

TLS does not provide a mechanism for a client to tell a server (i.e., the device) the name of the server it is contacting. It may be desirable for clients to provide this information to facilitate secure connections, for example, to servers that host multiple virtual servers at a single underlying IP network address. To provide any of the server names, clients may include the extension type "server_name" in the (extended) "client hello" message. According to the "server_name", the device can now select the appropriate TLS Context (certificate) to use.

This feature is supported by the new SNI To TLS Mapping table (Setup > IP Network > Security > SNI To TLS Mapping), which maps the "server_name" (SNI) to a TLS Context in the TLS Contexts table.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.18 Cached DNS Resolution for Proxy Sets

For Proxy Sets configured with FQDNs, the device queries the DNS server to resolve FQDNs every user-defined interval (ProxyIPListRefreshTime), which refreshes the Proxy Set's list of DNS-resolved IP addresses. However, up until now, if the DNS server went offline, the device took the Proxy Set offline.

This feature now enables the device to cache (store) the last successful DNS resolution and if the DNS server doesn't respond (for whatever reason) to the device's DNS query refresh, instead of taking the Proxy Set offline, the device reuses the cached DNS-resolved addresses. The device continues querying the DNS server every 10 seconds. The device only clears the cache 30 minutes after the time-to-live (TTL) of each entry expires. If the DNS server still doesn't respond after the device has cleared the cache, the device takes the Proxy Set offline.

This feature is configured by the new parameter [DNSCache], which is enabled by default.

Applicable Application: All.

Applicable Products: All.

2.31.3.1.19 IP Group Authentication as Both Client and Server

The device can now be configured on the IP Group level to authenticate SIP requests from an IP Group, both as a client and as a server, with different credentials. This is supported by the new optional value, **SBC as Both Client and Server** for the existing 'Authentication Mode' parameter in the IP Groups table.

When acting as a client and the device receives a challenge (SIP 401/407 response) from an authentication server (proxy) for the outgoing request, it retries the request with the credentials. The credentials are obtained from the Accounts table, if configured; otherwise, from the new 'Username As Client' and 'Password As Client' parameters in the IP Groups table.

When acting as an authentication server, the device challenges incoming SIP requests from the IP Group. It authenticates them based on the credentials configured in the new 'Username As Server' and 'Password As Server' parameters in the IP Groups table. (If the user is configured in the User Information table with a username and password, then it authenticates them based on the User Information table.)

Note: Due to this feature, the 'Username' and 'Password' parameters in the IP Groups table are now obsolete and it's recommended not to configure them in CLI scripts from this version. However, if these parameters are configured in CLI, the value configured for the obsolete parameter `username` is assigned to the new parameter `username-as-client`, and the value configured for the obsolete parameter `password` is assigned to new parameter `password-as-client`.

Applicable Application: SBC.

Applicable Products: All.

2.31.3.1.20 Upgrade Enhancement for New Media Components

When adding a new virtual Media Component (vMC) to an existing Signaling Component (SC) and there is no vMC image (software version .cmp file) in the SC's repository, the device can now be configured by the new [ScUsingLocalCmpAsRepository] parameter to load the vMC with the same software version as used by the SC.

If this feature is disabled (default), the vMC continues using its currently installed software version. However, this may cause compatibility issues between the new vMC and the SC if the vMC is using a software version that is later (received, for example, from Marketplace) than that used by the SC.

Applicable Application: SBC.

Applicable Products: Mediant CE.

2.31.3.1.21 Web GUI Parameter Name Changes

The following Web parameters have been renamed:

- 'Mask Private Information in CDRs' > 'Mask PII in CDRs'
- 'Mask Digits Information' > 'Mask Digits'
- 'Number of unmasked characters' > 'Number of Unmasked Characters in PII'
- 'Location of unmasked characters' > 'Location in PII of Unmasked Characters'

Applicable Application: All.

Applicable Products: All.

2.31.3.2 Known Constraints

This section lists known constraints.

Table 2-37: Known Constraints in Version 7.40A.250.001

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-33406	After preforming an upgrade to this version, the device can't be downgraded using a .cmp file of an earlier version. If you want to keep the option to downgrade the device in the future, follow the downgrade procedure described in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.	Device can't be downgraded using a .cmp file of an earlier version.	High	Mediant 90xx; Mediant Software	All
SBC-34198	When using the Web interface's Software Upgrade wizard, after selecting and loading the .cmp file (**Load File** button), if the user then clicks **Next** (providing options to load other files) and then clicks **Back** to return to the wizard page where the .cmp file was loaded, the wizard fails (freezes).	Device can't be upgraded using the Software Upgrade wizard when the **Next** and then **Back** buttons are clicked. To unfreeze the wizard, close the device's web interface by clicking the window's "x" button, re-login and then restart the device.	Low	All	All

2.31.3.3 Resolved Constraints

This section lists resolved constraints.

Table 2-38: Resolved Constraints in Version 7.40A.250.001

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-30961	Media performance monitoring statistics (e.g., mediaKBytesInTotal) for calls established prior to an HA switchover and then terminated after the switchover are not calculated on the new active device.			HA	
SBC-32426	The device's hitless software upgrade feature fails when the web session timeout expires (resulting in redirection to login page) and a reset is required to complete process.	Hitless software upgrade requires a reset.	Medium	HA	All

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-32517	The device's message waiting indication (MWI) for voicemail fails when a SIP NOTIFY message is routed according to the IP-to-Tel Routing table (PSTNPrefix) with the 'Source SIP Interface' is set to the device's SIP Interface.	MWI failure.	Medium	Mediant 500/500L/800/ 1000	Gateway
SBC-32979	The device allocates a resource (RecordingStreamsConnector) upon the receipt of a SIP INFO message to start SIPREC but doesn't deallocate this resource upon SIP INFO to stop SIPREC, causing calls to fail with 488 due to no more resources.	Device runs out of resources and rejects new calls.	Medium	All	All
SBC-33258	The device doesn’t attempt to resolve the FQDN of the Route header host part when the 'Destination URI Input' parameter in the IP Groups table is configured to **Route**.	Device uses incorrect route.	Medium	All	All
SBC-33334	The device rejects calls from Microsoft if License Key doesn't include the MSFT/TEAMS feature keys.	Device rejects Microsoft calls.	Medium	All	All
SBC-33370	The device sometimes fails to export SDR over SFTP, generating the error "SDRHandler has no more free IDs".	Device fails to export SDRs.	Medium	All	All
SBC-33454	Two different devices installed on Hyper-V have the same BID in the Syslog message.	Managed Services cannot differ between different virtual machines.	Medium	Mediant Software on Hyper-V	All
SBC-33510 SBC-33641 SBC-34162	The device resets when forking calls and routing based on destination tags (dst tags), while the forked call has no dst tags.	Device resets.	Medium	All	All
SBC-33532 SBC-33795	The device doesn't work with SNMP Trusted Managers table after upgrade to 7.4.200.	OVOC fails to connect to device.	Medium	All	All
SBC-33572 SBC-33641	The Additional Management Interfaces table doesn’t function after upgrade to 7.4.200.	Device has no access to Web interface.	Medium	All	All
SBC-33573	The device reports the same values in the alarm source and description.	OVOC fails to remove the device's cleared alarms.	Medium	All	All

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-33655	The Accounts table fails to send SIP REGISTER in this scenario: 1 Proxy is down and IP Group goes offline. 2 Device sends an un-register. 3 Proxy is up and IP Group goes online before device receives 200 OK for un-register. 4 Device receives 200 OK for the un-register.	Device loses Accounts table registration.	Medium	All	All
SBC-33707	The device can't be configured with subnet 31 (prefix length).	Configuration limitation.	Medium	Mediant 3100	n/a
SBC-33748	The device experiences keep-alive failures between active and redundant units.	HA switch overs.	Medium	Mediant Software HA	All
SBC-33817	The device resets in this scenario: 1 Call established between X and Y. 2 X sends BYE and device forwards it to Y. 3 Before receiving a response for the BYE, the device receives a new INVITE from Z with the Replaces header, while the Replaces header matches the leg between the device and Y. 4 The device sends a getRoute to ARM and receives and handles a 200 OK for the BYE before receiving the getRoute response from ARM.	Device resets.	Medium	All	All
SBC-33916	The device enters a busy-out state and fails to recover in this scenario: 1 Load-balancing is enabled for a Proxy Set with multiple DNS hosts configured. 2 All resolved servers are offline and busy-out is set. 3 Due to periodic DNS resolution, the IP of one of the hosts changes. 4 Immediately after (before/without failure of keep-alive with the new server), a keep-alive with one of the servers succeeds.	PSTN connectivity breaks.	Medium	Gateway	All
SBC-33960	WebRTC video calls fail (no video) because RTP tunneling was only supported for streams that are in RTP forwarding state.	No video.	Medium	All	All

2.31.4 Version 7.40A.200.018

This version includes only known and resolved constraints.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2546 or later.
  - √ OVOC Version 8.0.2546 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.2546 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 8.0.2546 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.

2.31.4.1 Known Constraints

This section lists known constraints.

Table 2-39: Known Constraints in Version 7.40A.200.018

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-33532	The SNMP Trusted Manager table (SNMPTrustedMgr) is not functional in this release.	As the SNMP Trusted Managers table is not functional, trusted managers cannot be configured and therefore, the device will accept SNMP Get/Set requests from any IP address as long as the community string is correct.	Medium	All	All

2.31.4.2 Resolved Constraints

This section lists resolved constraints.

Table 2-40: Resolved Constraints in Version 7.40A.200.018

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-32607	The Media Transcoding Cluster (MTC) mode is not supported in this version.	MTC feature is not supported (does not work) in this version.	High	MTC	All

2.31.5 Version 7.40A.200.015

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

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2546 or later.
  - √ OVOC Version 8.0.2546 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.2546 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 8.0.2546 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.

Note: The [SyslogLogLevel] parameter is for internal use only (by AudioCodes).

2.31.5.1 New Features

This section describes the new features introduced in this version.

2.31.5.1.1 Masking Personally Identifiable Information for GDPR Compliance

In line with AudioCodes' commitment to support the European Union's (EU) General Data Protection Regulation (GDPR) on data protection and privacy, the device can now be configured to mask (hide) personally identifiable information (PII) in its generated log files (Syslog, CDRs and SDRs). This is supported by the following:

- **Masking PII in CDRs:**
  - New parameter 'Mask Private Information in CDRs' – enables the masking (using the asterisk sign) of PII (e.g., telephone numbers, URI user and host parts, and display names) in CDRs and SDRs that are sent to remote servers, stored locally, or displayed in the device's Web interface and CLI.

    Note: This parameter replaces the previously supported CdrHistoryPrivacy parameter (backward compatible).
  - New parameters 'Number of unmasked characters' and 'Location of unmasked characters' – define which characters in the PII to show; masking all the rest. For example, in the following masked PII, the last four characters are shown while the rest are masked: "*****6789"
- **Masking in-call dialed digits (DTMF) in log file:** New parameter 'Mask Digits Information- enables the masking (using the asterisk sign) of digits, typically in-band DTMFs that are detected by the device and sent as events in Syslog (including logged SIP messages INFO / NOTIFY).
- **Script for removing of PII from external log files:** AudioCodes offers an easy-to-use Python-based script tool that can be used to automatically remove all PII from a specified log file. The script can be run on any computer that has Python 3 installed (https://www.python.org/downloads). The tool can be downloaded from AudioCodes website at https://tools.audiocodes.com/install

Applicable Application: All.

Applicable Products: All.

2.31.5.1.2 OAuth 2.0 Authentication of Users using Azure AD

The device can now use Microsoft's Azure Active Directory (Azure AD) to authenticate (credentials) and authorize (access level) users attempting to log in to its management interfaces (Web interface, CLI, and REST API). Authentication is done using the OAuth 2.0 protocol. (Up until now, the device supported LDAP, RADIUS, and local user-login authentication.)

When the user browsers to the device's Web login page and then selects to log in using Azure AD, the user is redirected to Microsoft login page. If login fails (authentication failure of credentials), the app redirects the user to the Web login page and a failure message is displayed. If the login process succeeds, the user is redirected back to the Web interface and is logged into the Web interface with appropriate user level (i.e., Monitor, Administrator, or Security Administrator).

To support this feature, the following configuration updates have been introduced:

- New table - OAuth Servers (Setup > IP Network > AAA Servers > OAuth Servers): Configures the OAuth 2.0 server (Azure AD).
- New table - Login OAuth Servers (Setup > Administration > Web & CLI > Login OAuth Servers): Enables and configures OAuth 2.0 login authentication.

- New parameter - 'Use OAuth for Web Login': Enables OAuth 2.0 login authentication (with or without local authentication using the Local Users table).
- New optional value **HTTPS Redirect** for existing 'Secured Web Connection (HTTPS)' parameter: Allows access to the device's Web interface only from HTTPS (secured) redirect URLs (i.e., Azure AD redirects user to this URI – device's address - upon successful authentication and authorization).
- New parameter - 'Web Hostname': Configures an FQDN for the device, allowing users to use it to access the device instead of the OAMP IP address. (If not configured, the hostname configured by the existing 'Host Name' parameter is used).
- New parameter - 'Local Users Table can be Empty': Allows Security Administrator to delete all users (including itself) in Local Users table. This feature may be required to increase security, enforcing log in only through external services (e.g., RADIUS, LDAP, or OAuth 2.0).

Note: The "RADIUS & LDAP" folder (Setup menu > IP Network tab > RADIUS & LDAP folder) has been renamed "AAA Servers".

Applicable Application: All.

Applicable Products: All

2.31.5.1.3 OAuth 2.0 Authentication of SIP Requests using Azure AD

Customers can now use Microsoft Azure Active Directory (Azure AD) Authentication to authenticate WebRTC-based or SIP-based agents.

The device can now use Azure AD to authenticate incoming SIP messages, based on the OAuth 2.0 protocol. Azure AD is Microsoft's cloud-based identity and access management service, designed for Internet-based applications.

As Azure AD doesn't support OAuth Token Introspection, the device validates the received token using its embedded NGINX server, which simulates an OAuth 2.0 Introspection endpoint.

The SIP UA obtains its token from Azure AD in JSON Web Token (JWT) format, which is a secure signed and encrypted JSON document identifying the user. For the device to validate the JWT, it needs the public keys from Azure AD, which it downloads using the NGINX server (HTTP GET). These keys are rotated daily (device periodically refreshes the keys from Azure AD).

When the device receives a SIP request that needs validation, it extracts the token from the 'Authorization: Bearer <token>' header of the SIP message and sends it the NGINX server. NGINX then decrypts the token using the public keys and validates them.

Applicable Application: All.

Applicable Products: All

2.31.5.1.4 Multiple Syslog Servers and Syslog over TLS

The device's Syslog support has been enhanced as follows:

- The device can now be configured to send Syslog messages to up to five remote Syslog servers. In addition to the existing parameters to configure the single Syslog server as in previous releases, the additional Syslog servers are configured in the new Syslog Severs table (Troubleshoot menu > Troubleshoot tab > Logging folder > Syslog Servers).
- The transport layer protocol (UDP, TCP or TLS) for communicating with the Rsyslog server can now be configured. Up until now, the device used UDP only. This feature is supported by the following new configuration entities:

- 'Protocol' field in the new (see above) Syslog Servers table configures the transport protocol of the additional Syslog servers.
- New parameter 'Syslog Protocol' (SyslogProtocol) configures the transport protocol of the single Syslog server (applies also to CDR and SDR servers).
- New parameter 'Syslog TLS Context' assigns a TLS Context when TLS is used (applies also to CDR and SDR servers).

Note: The CLI command `syslog-tlscontext` has been renamed `syslog-tls-context-name`.

Applicable Application: All.

Applicable Products: All.

2.31.5.1.5 Real-time Selective Coder Transcoding Based on MOS

The device can now monitor MOS levels during a call (every 30 seconds) and dynamically change the coder between G.711 and Opus during the call, based on MOS. When MOS becomes low (i.e., poor voice quality), the device immediately switches the coder to Opus; when MOS increases (i.e., improved packet loss), the device switches back (after a small delay) to the G.711 coder. Up until now, the coder was changed only for subsequent calls, based on the MOS of the previous call. This functionality requires the Voice Quality license key (orderable).

Applicable Application: All.

Applicable Products: All.

2.31.5.1.6 New Hybrid SBC and Media Gateway - Mediant 3100

The Mediant 3100 is a 2U chassis, supporting up to 64 E1/T1 spans, scaling up to 5,000 concurrent SBC sessions. Mediant 3100 provides redundant, load-sharing AC or DC power supplies.

Applicable Application: All.

Applicable Products: Mediant 3100.

2.31.5.1.7 Virtual SBC Suport for VMware vSphere ESXi 7.0

The device can now be installed on a host server that is running hypervisor VMware ESXi Version 7.0.

Applicable Application: SBC.

Applicable Products: Mediant VE/CE

2.31.5.1.8 Selective Quality of Experience (QoE) Reporting to OVOC

Quality of Experience (QoE) reporting to OVOC can now be filtered using any filter type (e.g., by IP Group). Up until now, QoE reports included all calls. To enable this feature:

- The new parameter 'Filter Reports' has been added to the Quality of Experience Settings table, which must be enabled. (If disabled, all CDRs are sent to OVOC.)
- The Logging Filters rule must be configured as follows: Log Destination' configured to **OVOC** and 'Log Type' configured to **CDR**.

Applicable Application: All.

Applicable Products: All

2.31.5.1.9 Web Interface Support for Microsoft Edge

The device's Web interface has been successfully tested for compatibility with the Microsoft Edge web browser.

Applicable Application: All.

Applicable Products: All.

2.31.5.1.10 Automatic Update Mechanism for TLS-Related File Provisioning

Up until now, the device's Automatic Update mechanism only uploaded TLS-related files (certificate, private key, and trusted root) for TLS Context #0. Now, the Automatic Update mechanism has been enhanced to allow upload of files for any TLS Context. This relates to the existing file provisioning parameters, TLSCertFileUrl, TLSPkeyFileUrl, and TLSRootFileUrl.

- TLS-related files can be downloaded for **all** TLS Contexts in the TLS Contexts table. This is done by including the "<ID>" meta-variable in the URLs (e,g., http://10.1.1.12/certs/<ID>/cert.pem). The meta-variable is replaced by a number, which is consecutively incremented from 0, according to the number of configured TLS Contexts (e.g., http://10.1.1.12/certs/0/cert.pem, http://10.1.1.12/certs/1/cert.pem, and http://10.1.1.12/certs/2/cert.pem).
- TLS-related files can be downloaded for a **specific** TLS Context. This is done by including the "#<TLS Context index row>" placeholder in the URLs. For example, http://10.1.1.12/certs.pem#2 downloads the file for TLS Context #2 in the TLS Contexts table.

Applicable Application: All.

Applicable Products: All.

2.31.5.1.11 File Rotation by Age for Persistent Logging

The persistent logging feature has been enhanced and now allows configuration of file age (in minutes) for log rotation (closing current file and creating a new file). This is configured by the new parameter, SystemPersistentLogPeriod. Thus, log rotation now occurs when either the maximum file size or file age has been reached (whichever occurs first).

Applicable Application: SBC.

Applicable Products: Mediant 9000; Mediant Software.

2.31.5.1.12 Table Capacity Increase for NGINX HTTP-based Proxy Services

The capacity (maximum rows) of the following tables for configuring NGINX HTTP-based proxy services has been increased:

- HTTP Proxy Server table - increased from 10 to 40
- HTTP Locations table - increased from 40 to 120

Applicable Application: SBC.

Applicable Products: Mediant SW (≥ 8GB)

2.31.5.1.13 Configuration Package File Backup through SNMP MIB

A new file type called Configuration-Package has been added to the device's SNMP MIB. This MIB allows OVOC to perform a full backup of the device (all files including Auxiliary files), by uploading the Configuration Package file. OVOC uploads the file only if it was modified (compared to current file in OVOC, using checksum - acSysConfigurationPackageChecksum).

Applicable Application: All.

Applicable Products: All

2.31.5.1.14 Software Update Status through REST API

Software update status indication has been added to the device's REST API. The software status is displayed by the following new fields under the API request `http://<IP Address>/api/v1/status`:

- `upgradeStatus` ("None", "In Progress", "Hitless-beforeSwitchOver", "Hitless-beforeSwitchBack", or "Hitless-WaitRdnReconnect")
- `mcUpgradeStatus` ("None" or "In Progress") - Applicable only to Mediant CE for upgrade of its Media Components

Applicable Application: All.

Applicable Products: All

2.31.5.1.15 Debug File Creation and Download through REST API

The Debug file (optionally with Core Dump file) can be created and downloaded through the device's REST API. The following new URL paths are used for this feature:

- Creating (POST HTTP/S method) Debug file:
  - `/api/v1/files/create/debugFile` – creates the Debug file (if HA, from Active device)
  - `/api/v1/files/create/debugFileRedundant` – creates the Debug file from the redundant unit for HA
- Downloading (GET HTTP/S method) Debug file:
  - `/api/v1/files/debugFile` – downloads the Debug file (if HA, from active unit)
  - `/api/v1/files/debugFile/redundant` – downloads the Debug file from the redundant device for HA systems

Applicable Application: All

Applicable Products: All

2.31.5.1.16 License Information for Redundant Device through REST API

The REST API URL `http://<Ip Address>/api/v1/license` now also includes the following information on the Redundant device:

- Serial number ("serialNumberRedundant")
- License Key ("keyRedundant")
- License Key description ("keyDescriptionRedundant")
- MAC address ("macAddressRedundant")

The Redundant device's serial number and MAC address is now also displayed on the Web interface's Device Information page.

Applicable Application: All

Applicable Products: Mediant 500; Mediant 800; Mediant 90xx; Mediant Software

2.31.5.1.17 Enhanced SSH Security

The following security enhancements have been added to the device's Secure SHell (SSH):

- The key exchange method (configured by the 'Kex Algorithms String' parameter) can now also be configured with the following new value:
  - diffie-hellman-group14-sha1
- The cipher string (configured by the 'Ciphers String' parameter) can now also be configured with the following new values:
  - aes256-ctr
  - aes256-cbc

Applicable Application: All.

Applicable Products: All

2.31.5.1.18 Display of Active Users Logged into Device

The device's Web interface now displays all active users that are currently logged into the device's Web interface, CLI, or REST API. This is displayed in the new Active Users table (Setup menu > Administration tab > Web & CLI folder > Active Users). The table displays the username, client's IP address, user's privilege level, login method (e.g., local login, OAuth server, or OVOC), and remaining idle session timeout.

Applicable Application: All.

Applicable Products: All

2.31.5.1.19 New Call Release Reason for Lack of Media Resources

The device supports a new call-release reason due to insufficient media resources. The reason description is "RELEASE_BECAUSE_LACK_OF_MEDIA_RESOURCES" (334), which is added to the Reason header in SIP BYE messages (and to the CDR field 'Termination Reason').

Applicable Application: All.

Applicable Products: All

2.31.5.1.20 Registrar Address Displayed for Account Registration Status

For registration status of Accounts, the IP address and port of the registrar server (Proxy Set of Serving IP Group) are now also displayed. This is supported by the new 'Server Address' field in the Account Registration Status table on the Web interface's Registration Status page. This is also supported by CLI (`show voip register account gw|sbc`).

Applicable Application: All.

Applicable Products: All

2.31.5.1.21 Privacy Protocol Enhancement for SNMPv3 Users

The privacy protocol of SNMPv3 users, configured by the 'Privacy Protocol' parameter in the SNMPv3 Users table can now be configured for 192-bit and 256-bit AES encryptions.

Applicable Application: All.

Applicable Products: All

2.31.5.1.22 File Transfer using SCP

The device can now transfer files using Secure Copy Protocol (SCP). This is done using the `copy <File Type> to|from` command. The authentication username and password are included in the URL, using the following syntax:

```
copy <File Type> from|to scp://<Username>:<Password>@<IP>/<Path>
```

For example:

```
copy firmware from scp://sue:1234@10.4.10.0/firmware.cmp
```

Applicable Application: All.

Applicable Products: All

2.31.5.1.23 Status Indication of OVOC WebSocket Tunnel

The status of the WebSocket tunnel between the device and OVOC is now available. The status is displayed by the new read-only 'Status' and 'IP Address' fields on the existing Web Service Settings page, and by the new CLI command `show network ovoc-tunnel`.

Applicable Application: All.

Applicable Products: All

2.31.5.1.24 Optimizing SIP Registration Failovers Between Multiple Registrars

This feature is designed to prevent the device from sending registration requests to a SIP registrar server to which it previously registered if it subsequently registered to a different server. This may occur in scenarios where the initial registrar server went briefly offline.

The device avoids registering to this initial server for a duration that is based on the cumulative value of the Proxy Server's last 'Expires' time and a new configurable grace time.

To support this feature, the following configuration updates have been done:

- The existing 'Registrar Search Mode' field in the Accounts table has a new optional value, **Avoid Previous Registrar Until Expiry** (2) which enables this feature.
- A new global parameter [AccountRegistrarAvoidanceTime] defines the grace time.

Applicable Application: All.

Applicable Products: All.

2.31.5.1.25 Enhanced Logging Filters Feature

The device's Logging Filters feature has been enhanced as follows:

- Logs can now be filtered by an IP Group tag. This is configured by the new optional value, **IP Group Tag** for the 'Filter Type' parameter.
- The optional values of the following parameters in the Logging Filters table have been renamed:
  - 'Log Destination' parameter: **Call Flow Server** renamed **OVOC** (used for reporting **to OVOC**, as described in Selective Quality of Experience (QoE) Reporting to OVOC**)**
  - 'Log Type' parameter:

- **Call Flow** renamed **SIP Ladder**
- **CDR Only** renamed **CDR**

Applicable Application: All.

Applicable Products: All

2.31.5.1.26 New Gateway Statistics on Web Monitor Page

The following new performance monitoring statistics for Gateway calls have been added to the Web interface's Monitor page:

- "Tel-to-IP Call Attempts per Sec" (attemptedCallsRateTel2Ip)
- "IP-to-Tel Call Attempts per Sec" (attemptedCallsRateIp2Tel)

Applicable Application: Gateway.

Applicable Products: MP-1288; Mediant 5xx; Mediant 800; Mediant 1000B; Mediant 3100

2.31.5.1.27 Maximum Tags Increased per Entity

The maximum number of tags that can be configured in the 'Source Tags' or 'Destination Tags' for IP-to-IP Routing rules and Outbound Manipulation rules has been increased from 5 to 8.

Applicable Application: All.

Applicable Products: All

2.31.5.1.28 Mediant 3100 Support for License Pool Models

The Mediant 3100 now supports all licensing pool models – Floating, Flex, and Fixed.

Applicable Application: All.

Applicable Products: Mediant 3100.

2.31.5.1.29 No Answer Timeout Value from ARM / Routing Server

ARM or third-party routing servers can provide the "no-answer timeout" for each GetRoute request received from the device. If the called IP party does not answer the call within this timeout, the device disconnects the session or forks the call (delayed call forking). If provided, this value overrides the [SBCAlertTimeout) parameter for SBC calls and [PSTNAlertTimeout] parameter for Gateway calls.

Applicable Application: All.

Applicable Products: All.

2.31.5.2 Known Constraints

This section lists known constraints.

Table 2-41: Known Constraints in Version 7.40A.200.015

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-32327	To process WebRTC calls, the device's EnableMediaSecurity parameter must be enabled.	When the device is used for WebRTC calls, and the EnableMediaSecurity parameter is not set to enabled, a device reset may occur during an HA switchover or a Hitless upgrade.	High	All	All
SBC-32545	If CDR/SDR local storage is enabled, the device's System Snapshot functionality cannot be used.	System Snapshots will not be created. Existing device snapshots can still be used. To create a new snapshot, first disable CDR/SDR local storage.	Medium	All	All
SBC-32597	The device crashes (resets) when the CLI command `show storage-history services` is run.	If the CLI command `show storage-history services` is run, the device will crash (resets).	High	All	All
SBC-32607	The Media Transcoding Cluster (MTC) mode is not supported in this version.	MTC feature is not supported (does not work) in this version.	High	MTC	All

2.31.5.3 Resolved Constraints

This section lists resolved constraints.

Table 2-42: Resolved Constraints in Version 7.40A.200.015

Incident	Description	Impact	Severity	Affected Products	Affected Environments
SBC-29927	The device's Firewall table (Access List) resolves only the first IP address from an FQDN when the DNS Query Type is configured to CNAME A.	No IP redundancy	Medium	All	All
SBC-31324	The device replies to both SNMPv1 and SNMPv2 requests even though it's configured to SNMPv3 only.	Security	Medium	All	All
SBC-32117	The device crashes due to an internal memory overrun.	Service down	Medium	All Gateways	n/a

2.31.6 Version 7.40A.100.338

This version includes resolved constraints only.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2546 or later.
  - √ OVOC Version 8.0.2546 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.2546 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 8.0.2546 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.

2.31.6.1 Resolved Constraints

This section lists resolved constraints.

Table 2-43: Resolved Constraints in Version 7.40A.100.338

Incident	Description
SBC-32987	The device in HA mode and installed on AWS crashes, resulting in an HA switchover. Applicable Products: Mediant VE SBC

2.31.7 Version 7.40A.100.336

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

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.2546 or later.
  - √ OVOC Version 8.0.2546 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.2546 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 8.0.2546 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.

2.31.7.1 New Features

This section describes the new features introduced in this version.

2.31.7.1.1 Telnet Disabled by Default

Access to the device through Telnet is now disabled by default (TelnetServerEnable) for all device types. Up until now, it was disabled by default only for Mediant 90xx and Mediant Software.

Applicable Application: All.

Applicable Products: All.

2.31.7.1.2 Increased Defense Against CSRF Vulnerability

The device's mechanism against the Cross-Site Request Forgery (CSFR) vulnerability has been improved.

Applicable Application: All.

Applicable Products: All.

2.31.7.1.3 Secured Access to Show Configuration in CLI

The `show ini-file` command, which displays the device's configuration, can now only be executed in the CLI's Privileged User mode (`> enable`). As access to this mode requires a password, viewing device configuration using this command is therefore more secured.

Applicable Application: All.

Applicable Products: All.

2.31.7.1.4 Password Complexity for CLI Privileged User Mode

Password complexity can now also be enabled for the password to access the device's CLI Privielged User mode (`> enable`). This is configured by the existing parameter, EnforcePasswordComplexity (used up until now only for Web interface login).

Two additional password complexity rules have been added for CLI logins (regular and privileged modes): The username and password can't be the same and can't be the opposite of each other.

Applicable Application: All.

Applicable Products: All.

2.31.7.1.5 Algorithms for SIP Digest Authentication

When the device authenticates incoming SIP requests as an authentication server, the cryptographic hash algorithm used when it sends the authentication challenge in the SIP 401 or 407 response can now be configured. This is done using the new SIPServerDigestAlgorithm parameter (sip-server-digest-algorithm, md5/0,sha256/1), which can be set to MD5 (default) or SHA-256 (no Web param). Up until now, the device used only MD5.

Applicable Application: SBC.

Applicable Products: All.

2.31.7.2 Resolved Constraints

This section lists resolved constraints.

Table 2-44: Resolved Constraints in Version 7.40A.100.336

Incident	Description
SBC-31118	The device fails to activate channels with the SILK coder because of a bug in its DSPs, causing no voice on Microsoft Teams calls. Applicable Products: All
SBC-31178 / SBC-32224	WebRTC calls fail (no voice) because of a DTLS handshake failure, after a SIP re-INVITE message (for call transfer) changes from transcoding to RTP forwarding. Applicable Products: All
SBC-31484 / SBC-32485	The device reports (to OVOC) of low MOS values for the remote side of the call (even though MOS is actually higher) because of incorrect RTCP/RTCP-XR parameters for SRTP tunneling without authentication. Applicable Products: All
SBC-31564	The device experiences high CPU utilization because of an internal process (PIDS) using up most of its CPU resources. This affects service. Applicable Products: All
SBC-31788	The device is exposed to a security vulnerability of HTTP Host header attacks. Applicable Products: All
SBC-31895	In response to a SIP re-INVITE message, the device sends a SIP 200 OK that contains incorrect crypto suite, causing no voice. Applicable Products: All
SBC-32004	The device sends the wrong calling (display) name to OVOC - dots (…) instead of Cyrillic characters (which, for example, are used in the Russian alphabet). Applicable Products: All
SBC-32065	The device's Web interface's Web Service Settings page displays the configured password in plain text (instead of masking it). Applicable Products: All
SBC-32066	The device's Web interface displays the SNMP community strings in plain text (instead of masking it). Applicable Products: All
SBC-32067	The device's Web interface's initial login page doesn't have an active exit feature. Applicable Products: All
SBC-32068	The device's Cross Site Request Forgery (CSRF) defense mechanism is missing in cases where the first login password is changed for a new user account. Applicable Products: All
SBC-32069	The device's CSRF token length is 32 bytes after hexadecimal encoding, and 16 bytes after conversion, which does not meet security requirements of 24 bytes. Applicable Products: All
SBC-32070	The device's Activity Log table doesn't report the import of the ini file when the device restarts after uploading the .ini file. Applicable Products: All
SBC-32105	The device resets with the exception message "Signal 11, Task MDI1" (i.e., memory overrun). Applicable Products: All

Incident	Description
SBC-32133	The device rejects incoming SIP INVITE messages from a user whose re-registration is in progress (device waits for 200 OK to re-REGISTER) when the parameter [UseRandomUser] is set to 2. As a result, these calls fail. Applicable Products: All
SBC-32199	The device doesn't generate the acKpiThresholdCrossing SNMP trap for performance monitoring, even though thresholds were crossed. Applicable Products: All
SBC-32227	Device information is exposed after an SSH login is done in the background, while product-key verification is not valid (malicious code can be entered to cause storage TYPE XSS to be generated). Applicable Products: All
SBC-32248	Loading a new certificate on the Signaling Component (SC) causes DTLS errors on the Media Components (MCs). As a result, calls fail. Applicable Products: Mediant CE
SBC-32292	The device has no mechanism against brute-force cracking for background SSH logins. Applicable Products: All
SBC-32368	The device resets with the exception message "Signal 11, Task MDI1" when performing a System Snapshot. Applicable Products: Mediant Software
SBC-32468	The device resets (or does a switchover if in HA) because of high CPU utilization caused by miscalculation of internal timers. Applicable Products: All
SBC-32470	The device fails to transcode DTMF digits (RFC 2833 to transparent) in the early media stage, sending only the first DTMF digit. Applicable Products: All
SBC-32472	The device fails to send a SIP BYE message when retransmissions of SIP 200 OK responses are not ended, but the far side sends a BYE. As a result, calls are not disconnected ("ghost" calls). Applicable Products: All
SBC-32487	The device attempts alternative routing when the last forked IP Group is offline even though not all forked calls failed. (Should do alternative routing only if all forked calls fail.) Applicable Products: All
SBC-32708	When the device is hosted on AWS, NAT translation fails because the NAT Translation table is hidden in the device's Web interface (should be shown) for the Media Components (MCs), and the Public IP address is only in automatic mode (instead of using address in NAT Translation table). Applicable Products: Mediant Software (AWS)
SBC-32717	The device resets upon a hardware watchdog with the error message "Recursion detected for CSocket::_DebugHandler". Applicable Products: All

2.31.8 Version 7.40A.100.239

This version includes resolved constraints only.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.1139 or later.
  - √ OVOC Version 8.0.1139 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1139 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 8.0.1139 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.

2.31.8.1 Resolved Constraints

This section lists resolved constraints.

Table 2-45: Resolved Constraints in Version 7.40A.100.239

Incident	Description
SBC-32001 \ SBC-32084 \ SBC-32103 \ SBC-32124	The device loses connection to the OVOC Floating License pool. Applicable Products: All

2.31.9 Version 7.40A.100.238

This version includes new features and resolved constraints only.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.1139 or later.
  - √ OVOC Version 8.0.1139 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1139 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 8.0.1139 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.

2.31.9.1 New Features

This section describes the new features introduced in this version.

2.31.9.1.1 Improved Performance for Connections to HTTP/S Upstream Servers

A new parameter 'Max Connections' has been added to the existing Upstream Groups table to allow configuration of the maximum number of simultaneous active connections towards the proxied upstream server (activating connection re-use). If not configured (i.e., 0), a new upstream connection is opened for every incoming HTTP or HTTPS request.

Applicable Application: All.

Applicable Products: All.

2.31.9.2 Known Constraints

This section lists known constraints.

Table 2-46: Known Constraints in Version 7.40A.100.238

Incident	Description
SBC-32001 \ SBC-32084 \ SBC-32103 \ SBC-32124	The device loses connection to the OVOC Floating License pool. Applicable Products: All

2.31.9.3 Resolved Constraints

This section lists resolved constraints.

Table 2-47: Resolved Constraints in Version 7.40A.100.238

Incident	Description
SBC-31806	After rebooting, the device doesn't reconnect to ARM. Applicable Products: All

2.31.10 Version 7.40A.100.233

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

Note: Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.1139 or later.
  - √ OVOC Version 8.0.1139 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1139 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 8.0.1139 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.

2.31.10.1 New Features

This section describes the new features introduced in this version.

2.31.10.1.1 Random String in Contact User Part for Re-Registrations

A new value (2) has been added to the existing [UseRandomUser] parameter, which enables the device to generate a randomized string for the user part of the Contact header for every sent SIP REGISTER message, including initial registrations as well as registration refreshes.

Applicable Application: All.

Applicable Products: All.

2.31.10.1.2 Session Expiry Observer Mode per RFC 4028

The device now complies strictly with RFC 4028 regarding SIP session expiration.

This feature is supported by the new [SipSessionExpiresObserverMode] global parameter, which determines if the observer mode (when IP Profile parameter 'Session Expires Mode' is configured to **Observer**) is strictly according to RFC 4028 or according to AudioCodes method of adding a "graceful" session expiration time.

Applicable Application: SBC.

Applicable Products: All.

2.31.10.1.3 New "Tenant ID" CDR Field

The CDR can now be customized in the SBC CDR Format table to include the Tenant ID, using a new CDR field called "Tenant ID". The Tenant ID value is obtained from any SIP header, using the new call variable *var.call.dst|src.TenantId* in Message Manipulation rules. This feature can be used to allow OVOC to know which Tenant ID the call belongs to.

Applicable Application: SBC.

Applicable Products: All.

2.31.10.2 Known Constraints

This section lists known constraints.

Table 2-48: Known Constraints in Version 7.40A.100.233

Incident	Description
SBC-31806	After rebooting, the device doesn't reconnect to ARM. Applicable Products: All
-	FIPS Mode is not supported in this version. Applicable Products: All

2.31.10.3 Resolved Constraints

This section lists resolved constraints.

Table 2-49: Resolved Constraints in Version 7.40A.100.233

Incident	Description
SBC-29859	The device crashes (resets) when loading an incremental ini file that contains only NGINX configuration. Applicable Products: All
SBC-29860	The device fails to complete DTLS negotiation due to fragmented DTLS packets and as a result, the call fails. Applicable Products: All
SBC-30243	The device does not print the source\destination sub-addresses (if exist) in the "pstn recv <-- INCOMING_CALL" syslog message. Applicable Products: Gateway
SBC-30289	The device fails to add the Content-Disposition header to a SIP INFO request, as configured by the Message Manipulation. Applicable Products: All
SBC-30368	The device rejects the SDP offer when it contains an "@" in the origin field ('o='), with a SIP 415 response and parsing error. As a result, the call fails. Applicable Products: All
SBC-30433	The device's web parameter 'Classify By Proxy Set Mode' should be under SIP Definitions General Settings > SBC Settings (instead of SIP Definitions General Settings > General). Applicable Products: All
SBC-30987	The device crashes (resets) with the exception reason "TPAPP no sched for the last 16000 ticks". Applicable Products: All
SBC-31143	The device fails to perform alternative routing when forking to two User-type IP Groups. As a result, the call fails. Applicable Products: All
SBC-31148	The device generates new user part for the Contact header in outgoing SIP 18x requests when the UseRandomUser parameter is configured to 2 (should only be generated for REGISTER messages). As a result, the call fails. Applicable Products: All
SBC-31177	The device sends RTP to the wrong port on simultaneous ring call flow, causing a one-way voice. Applicable Products: All
SBC-31236	The device tries to add the crypto suits group before removing the unsupported crypto suits, causing the call to fail. Applicable Products: All
SBC-31246	The device sends an alarm without indicating the severity level in REST API, for running an active DR rule. Applicable Products: All

2.31.11 Version 7.40A.100.114

This version includes new features and resolved constraints.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.1122 or later.
  - √ OVOC Version 8.0.1122 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1122 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 8.0.1122 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.

2.31.11.1 New Features

This section describes the new features introduced in this version.

2.31.11.1.1 NGINX Version Update

The device's embedded NGINX engine has been updated to Version 1.20.1.

Applicable Application: SBC

Applicable Products: All.

2.31.11.1.2 Mediant VE and CE Support for Gen3 Xeon-SP ("Ice Lake-SP")

The virtual SBCs (Mediant VE and CE) now support 3rd Gen Intel® Xeon® Scalable processors (code-named "Ice Lake-SP") based host servers. This allows the use of Intel's latest CPU server architecture with these SBCs.

Currently, there is no change in the supported SBC capacity when using these servers.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.31.11.1.3 Secured Media Cluster Connectivity

Up until now, connectivity in the media cluster between the Signaling Component and the Media Components for the management of the Media Components was non-secured (TCP). Now, when upgrading to Version 7.40A.100.114, this connectivity changes to secured (TLS), by default. The connectivity mode can be configured (secured or non-secured), using the new [TpncpEncryptionEnable] parameter. For more information, refer to the *User's Manual*.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.31.11.1.4 New SNMP Alarms

The following new SNMP alarms have been introduced in this version:

- acFaultyDSPAlarm - sent when one or more of the device's DSP cores are faulty.
- acTLSCertificateMismatchAlarm - sent when a mismatch occurs between the private key and the TLS certificate (public key).
- acMCNotSecuredAlarm – (Mediant VE/CE Only) sent when the connection between the Signaling Component (SC) and at least one of the Media Components (MC) remains unsecured after a specific partially completed upgrade scenario.

Applicable Application: All.

Applicable Products: All.

2.31.11.1.5 Mediant 9080 SBC Hardware Revision Update

Later this year, Mediant 9080 SBCs will be shipped with a new hardware revision that includes an updated CPU module.

There is no change in the Mediant 9080 supported capacity, device configuration or supported features following this update.

The updated hardware revision is supported by this 7.4 software version (7.40A.100.114) or later. Earlier 7.4 software versions are not compatible with the new hardware revision.

Support for the new hardware revision was also added to the 7.2 LTS software version stream (7.20A.258.661 or later).

For upgrading 7.2 software to 7.4, an intermediate version which supports the new hardware revision should be used (7.40A.005.569 or later). For the upgrade procedure, refer to *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

Note: For Mediant 9080 HA system deployments: The HA pair (active-redundant) can have different hardware revisions, only if they are both running a supported software version (see above). Therefore, Customers are recommended to consider upgrading their HA pair to a software version supporting the new hardware revision. Doing so will ensure that a Mediant 9080 with the new hardware revision can be used in the HA system in case of a need for device replacement.

The updated hardware revision can be identified using one of the following methods:

- Yellow label on the left side of the device's chassis:
  - **Previous HW revision:** "Version P01"
  - **Updated HW revision:** "Version P02"
- Silver label on the upper cover of the device's chassis:
  - **Previous HW revision:** "FPRZ00157" (AC power supply) or "FPRZ00168" (DC power supply)
  - **Updated HW revision:** "FPRZ00191" (AC power supply) or "FPRZ00192" (DC power supply)
- Using the CLI command `show system hardware`:
  - **Previous HW revision:** `CPU: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz, total 48 cores, avx supported`
  - **Updated HW revision:** `CPU: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz, total 64 cores, avx supported`

Note: Mediant 9030 SBCs and the old Mediant 9000 (Gen 8) SBCs are not affected by this update.

Applicable Application: SBC.

Applicable Products: Mediant 9080

2.31.11.1.6 Classify by Proxy Set using IP Address in SIP Contact Header

Up until now, the IP Group table's 'Classify By Proxy Set' parameter enabled the classification of incoming calls as belonging to a specific IP Group, by searching the associated Proxy Set for an IP address that matched the source IP address (ISO Layer 3) of the incoming packet.

Classification by Proxy Set can now be done using the IP address of the Contact header of the incoming SIP message. If the header contains a SIP URI that has an IP address in the host part that matches an IP address in the Proxy Set, the call is classified to the IP Group. This mode is useful, for example, when the source IP address is an internal address (like when the Mediant CE SBC is deployed in Azure).

To support this feature, a new global parameter—'Classify By Proxy Set Mode' (ClassifyByProxySetMode)—has been introduced, which determines the IP address used for this classification process - source IP address (default), IP address of Contact header, or both. When configured for both, the device first checks the associated Proxy Set for an IP address that matches the source IP address. If there is no match, it checks the Proxy Set for an IP address that matches the IP address of the Contact header.

Note:

- Classification using the Contact header is supported only when the header has an IP address (not a DNS hostname).
- For IDS, only the source IP address is used.
- For TLS Contexts, only the source IP address is used. (If a Proxy Set is not found, the TLS Context configured for the SIP Interface is used.)

Applicable Application: SBC.

Applicable Products: All.

2.31.11.1.7 SDR Fields for MOS

The device can now generate Session Detail Records (SDR) with Mean Opinion Score (MOS) fields, if customized to do so. These fields are generated at the end of the call (STOP SDRs) and indicate MOS values for incoming (local and remote peer) and outgoing (local and remote peer) calls:

- IngressLocalMosCQ
- IngressRemoteMosCQ
- EgressLocalMosCQ
- EgressRemoteMosCQ

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.11.2 Resolved Constraints

This section lists resolved constraints.

Table 2-50: Resolved Constraints in Version 7.40A.100.114

Incident	Description
SBC-28750	The device crashes (resets) upon a flash-hook in the middle of dialing a secondary call. Applicable Products: Gateway
SBC-28955	The device crashes (resets) upon ARM sending a discover remote hosts for service that has an illegal HOST line for ARMTopology. Applicable Products: All
SBC-29025	When the device is deployed on Microsoft Azure and undergoes an HA switchover, it loses connection with ARM. Applicable Products: Mediant CE
SBC-29358	The device doesn't update Contact details during registration in its registration database. Applicable Products: All
SBC-29386	The device ignores a SIP ACK for a SIP 302 response when it terminates an incoming INVITE using the internal and 302 response. As a result, call failure occurs. Applicable Products: All
SBC-29596 / SBC-29625	The device drops all pending retransmissions when receiving an ICMP error. Applicable Products: All
SBC-29604	The device sends a TLSCertificateMismatchAlarm alarm for the Media Component (MC). Applicable Products: Mediant CE
SBC-29607 / SBC-30005	The device fails to load a TLS certificate, printing "RsaKeyMatch failed". Applicable Products: All
SBC-29614 / SBC-29822	The device's Web interface does not allow the user to change the index number of a row for a configuration table. Applicable Products: All
SBC-30080	The device's performance monitoring polling from OVOC fails when using a negative UTC offset (-1 or less). Applicable Products: All

2.31.12 Version 7.40A.100.021

This version includes only resolved constraints.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, 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*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.114 or later.
  - √ OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 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 8.0.114 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.

2.31.12.1 Resolved Constraints

This section lists resolved constraints.

Table 2-51: Resolved Constraints in Version 7.40A.100.021

Incident	Description
-	The device doesn't support AWS. (Now supports AWS.) **Applicable Products:** Mediant Software
SBC-28951	When running on AWS, HA fails to initialize due to the wrong time zone in initial startup on the redundant unit. **Applicable Products:** Mediant Software
SBC-29207	When running on AWS, the device crashes (resets) on task "WEBS" because of wrong pointers to the HTTP Remote Host (ARM). **Applicable Products:** SBC
SBC-29365	When running on Hyper-V, the device loses voice when using VLAN tagging. **Applicable Products:** Mediant Software

2.31.13 Version 7.40A.100.011

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

Note:

- Mediant VE/CE SBC on AWS or Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to Version 7.40A.100.011:

- **For Mediant 90xx, Mediant VE/CE/SE SBCs:** For upgrade instructions, please refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.
- **For MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** These devices can be directly upgraded only from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.114 or later.
  - √ OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 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 8.0.114 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.

2.31.13.1 New Features

This section describes the new features introduced in this version.

2.31.13.1.1 MOS Measurement, Reporting and Storing per Registered User

The device can be configured to measure and report MOS (value and color) for users that are registered with the device:

- The SBC Registered Users table (and output of the CLI command `show voip register db sbc`) now displays MOS per registered user (stores MOS).
- The device can be configured to switch to a different voice coder (e.g., from G.7.11 to Opus) for new calls if the MOS of a registered user falls under a specific level.
- The device reports MOS to registered users, by sending an out-of-dialog SIP NOTIFY message containing the proprietary x-VoiceQuality header, at the end of the call.

To support this feature, the following configuration updates were made:

- New web page called Registered User Voice Quality (Setup menu > Signaling & Media tab > Media folder > Quality of Experience > Registered User Voice Quality), which provides the following new parameters:
  - 'Registered User MOS Observation Window': Defines the length (1 or 2 hours) of each interval in the "observation window" (12 intervals) for calculating average MOS.
  - 'MOS Stored Timeout For No Calls': Defines the period of no calls after which the MOS measurement is reset (0 with color gray).
- New IP Group table parameter 'User Voice Quality Report': Enables this feature for registered users belonging to the IP Group (User-type).
- New optional value **Registered User Voice Quality** for the 'Rule Metric' parameter in the Quality of Service Rules table: Defines the rule for this feature (reject calls or use an alternative IP Profile if MOS is low).

Note: For HA systems, upon an HA switchover, MOS measurements restart on the new active device.

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.2 MOS Measurement Based on RTCP

The device can calculate MOS based on RTCP without the need for RTCP-XR packets. This is useful for WebRTC calls since, up until now, MOS calculation wasn't available as WebRTC clients typically don't send RTCP-XR reports.

Applicable Application: All.

Applicable Products: Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.31.13.1.3 Test Call Duration Specified in SIP INVITE

The duration of test calls can now be determined by the caller SIP user agent (UA). This is specified using the 'duration=<length in msec>' URI parameter of the Request-URI in the incoming SIP INVITE message. Up until now, caller-based test calls lasted until the caller ended the call (i.e., sent SIP BYE message).

This feature is in accordance with RFC 4240 (Basic Network Services with SIP).

This feature is also used for the MOS reporting of WebRTC click-to-call platforms feature, described in MOS Reporting for WebRTC Click-to-Call.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.4 MOS Reporting for WebRTC Click-to-Call

The device can be configured to test voice quality (MOS) with WebRTC clients.

The test is typically triggered when a client accesses the web page on which the WebRTC click-to-call widget button is displayed. If the device reports a low MOS, Customers can, for example, have the button deactivated (grayed out) so that the client can't use it to call.

Implementation of this feature requires configuration on the device, and configuration by the Web Developer using AudioCodes WebRTC web browser client SDK API:

- AudioCodes WebRTC Web Browser Client SDK API:

  When the client opens the web page, the web browser needs to send the device a SIP INVITE message containing AudioCodes proprietary SIP header, 'X-AC-Action: test-voice-quality' and the 'duration=' parameter in the Request-URI. The device identifies this feature by the receipt of the 'X-AC-Action: test-voice-quality' header. The 'duration=' parameter specifies the duration of the test call (see Test Call Duration Specified in SIP INVITE). For more information on AudioCodes web browser client SDK API, click here.

- SBC Device:

  The device routes the incoming SIP INVITE from WebRTC client to its embedded Test Call endpoint and establishes the call. During the call, the device plays a pre-recorded tone (PRT) to the client. When the duration, specified in the Request-URI (see above) expires, the device terminates the call and sends a SIP BYE message containing AudioCodes proprietary SIP header, 'X-VoiceQuality'. This header indicates the measured MOS (value and color), for example, 'X-VoiceQuality: 42 green'.

Applicable Application: SBC.

Applicable Products: Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.31.13.1.5 Enhanced Display of SBC Registered Users

The SBC Registered Users table, which displays users registered with the device, has been re-designed to provide the following enhancements:

- Capability to search for AORs (by user part)
- Display of number of registered AORs
- Display of a detailed information pane per contact of an AOR
- Improved readability

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.6 Capacity Increase of Configuration Tables

Capacity related to the following tables has been increased:

- Call Setup Rules table:
  - Max. rows:
    - Mediant 500/500L/800: 100
    - Mediant 1000/MP-1288: 64
    - Mediant 2600/4000: 400
    - Mediant 90xx/SE: 1,000
    - Mediant VE/CE: 500 for 2-8 GB and 1,000 for 16-64 GB
  - Max 'Rules Set ID's:
    - Mediant 500/500L/800/1000/MP-1288: 32
    - Mediant 2600/4000: 50
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB and 100 for 16-64 GB
  - Max. rules per 'Rules Set ID':
    - Mediant 500/500L/800/2600/4000/90xx/Software: 25
    - Mediant 1000/MP-1288: 10
- Accounts table:
  - Max Accounts per 'Served IP Group':
    - Mediant 500/500L/800: 30
    - Mediant 1000/MP-1288: 10
    - Mediant 2600/4000: 75
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB and 100 for 16-64 GB
- Message Manipulations table:
  - Max. 'Manipulation Set ID's:
    - Mediant 500/500L/800: 30
    - Mediant 1000/MP-1288: 20
    - Mediant 2600/4000: 50
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB; 100 for 16-64 GB
  - Max. rules per 'Manipulation Set ID':
    - Mediant 500/500L/800: 200
    - Mediant 1000/MP-1288: 100
    - Mediant 2600/4000: 500
    - Mediant 90xx/SE: 1,000
    - Mediant VE/CE: 750 for 2-8 GB; 1,000 for 16-64 GB

Applicable Application: All.

Applicable Products: All.

2.31.13.1.7 SHA-2 Authentication Protocol for SNMPv3 Users

SNMPv3 users can now be configured with SHA-2 authentication (SHA-2 224-bit, SHA-2 256-bit, SHA-2 384-bit, and SHA-2 512-bit). Up until now, only MD5 and SHA-1 were supported. This feature is configured by the existing 'Authentication Protocol' parameter in the SNMPv3 Users table.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.8 SNMP Enabled and Disabled On-The-Fly

A device reset is no longer required after changing the value of the 'Disable SNMP' parameter for enabling or disabling SNMP.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.9 New Default TLS Version

For enhanced security, the default value of the 'TLS Version' parameter in the TLS Contexts table has been changed from **Any TLS1.x** (0), which includes the relatively weak TLS versions 1.0 and 1.1, to **TLSv1.2 and TLSv1.3** (12).

Applicable Application: All.

Applicable Products: All.

2.31.13.1.10 SRTCP per IP Profile

Up until now, Secure RTCP (SRTCP) packet encryption could only be configured globally (all calls), using the 'Encryption on Transmitted RTCP Packets' [RTCPEncryptionDisableTx] parameter. In other words, both legs of the call could only be enabled or disabled for SRTCP. Now, SRTCP can be configured per specific calls using the new IP Profile parameter 'Encryption on RTCP Packets', allowing different settings for the incoming and outgoing legs (e.g., enabled for the incoming leg and disabled for the outgoing leg).

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.11 SRTP Crypto Suites per IP Profile

Supported offered crypto suites for SRTP can now be configured per IP Profile. Up until now, crypto suites (all or only one) could only be configured globally (for all calls), using the 'Offered SRTP Cipher Suites' parameter (which is still the default if not configured by this new feature).

This feature is configured by the following:

- New table - SBC Crypto Suite Groups (Setup menu > Signaling & Media tab > Media folder > SBC Crypto Suite Groups), which defines groups of crypto suites (AES-CM-128-HMAC-SHA1-80, AES-CM-128-HMAC-SHA1-32, AES-256-CM-HMAC-SHA1-80, and/or AES-256-CM-HMAC-SHA1-32)
- New IP Profile parameter 'Crypto Suites Group', which assigns an SBC Crypto Suite Group to the IP Profile

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.12 Additional SSH Settings for Secure CLI

Secure access to the device's CLI through SSH has been enhanced by the following new SSH configuration parameters:

- [SSHKexAlgorithmsString]: Key Exchange Method (Diffie-Hellman-Group-Exchange-SHA256 or Diffie-Hellman-Group1-SHA1)
- [SSHCiphersString]: Cipher string (AES128-CTR or AES128-CBC)
- [SSHMACsString]: HMAC (HMAC-SHA2-256 or HMAC-SHA1)

Applicable Application: All.

Applicable Products: All.

2.31.13.1.13 Prefer Secured Media on Outgoing SDP Answer

The device can now be configured to prefer secured media on the outgoing SDP answer sent by the device. When configured and a peer SIP user agent offers both secured and unsecured media, the device chooses to use secured media (SRTP).

This feature is supported by configuring the existing IP Profile parameter 'SBC Media Security Mode' to the new optional value, **Offer Both - Answer Prefer Secured** (4).

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.14 LDAP Authentication for NGINX HTTP Reverse Proxy

The device's HTTP Reverse Proxy can now be configured to authenticate HTTP requests with an LDAP server.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.15 Enhanced NGINX Support for TLS Context Parameters

The device's integrated NGINX server supports the following additional parameters in the TLS Contexts table: 'Cipher Server TLS1.3', 'Cipher Client TLS1.3', 'Key Exchange Groups', 'Strict Certificate Extension Validation', and 'DH key Size'.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.16 HTTP Proxy Interface Binding to Device Network Interface

The device's embedded NGINX can be enabled to bind the HTTP Proxy interface to a specific device network interface. This feature is configured by the new 'Bind To Device' parameter (enable/disable) in the HTTP Proxy Servers table.

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.17 Case-Sensitivity for Dial Plan Matching

Matching Dial Plan patterns can now be configured to take into account case-sensitivity (upper- or lower-case letters). This feature is configured by the new parameter, 'Prefix Case Sensitivity' in the Dial Plan table.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.18 Conference Call Support with Microsoft Local Media Optimization

The device can now handle conference calls with Local Media Optimization for Microsoft Teams Direct Routing. If a call is established with a Teams user who wants to add a third-participant, Teams sends a SIP re-INVITE message to connect the new media. The device can handle this even if the initial user location is internal, by offering its public IP address (instead of its private IP address). The device does this by its additional support for handling X-MS headers received from the Teams client in re-INVITE messages. Using the re-INVITE, a non-direct media internal call (using the internal Media Realm) or a direct media call can be changed to non-direct media external call (using the regular Media Realm for the IP Group).

Applicable Application: SBC.

Applicable Products: All.

2.31.13.1.19 IPv6 for Debug Recording Server

The remote debug recording server (to where the device sends debug recording packets), can now be configured (by the existing DebugRecordingDestIP parameter) to an IPv6 address.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.20 Enhanced Debug File Contents

The device's debug file now provides additional information of the device's configuration and status (e.g., date and memory). This information is located in the new *status.tar.gz* file.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.13.1.21 Embedded RPCAP Server for Packet Capturing

The device now provides an embedded Remote Capture Protocol (rpcap) server that allows Wireshark to connect to it remotely. Once connected, Wireshark controls the packet capturing process (i.e., starting/stopping network capture of selected network interfaces, collecting the captured data, and filtering it). For more information on rpcap functionality, refer to Wireshark documentation.

The device's rpcap server is enabled by the new CLI command, `debug capture rpcap-server {start|stop} [<port number>]`. By default, the device use port 2002 for the remote packet capture sessions.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.22 Persistent Storage of History Alarms

SNMP alarms in the Alarms History table can now be stored on the device's flash memory and maintained (persistent) even after a device reset. Up until now (and when the feature is disabled), these alarms are deleted from the table upon a device reset.

This feature is configured by the following new parameters:

- [AlarmsPersistentHistory]: Enables the feature. When enabled, the Alarms History page displays an additional column called "Note", which indicates if the alarm occurred (raised or cleared) before or after the last device restart.

- [SavePersistentHistoryInterval]: Defines how often the device saves the alarms of the Alarms History table to flash (overwriting previously stored file).

Note: Currently, the device cannot be connected to OVOC when this feature is enabled.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.23 SDR Enhancements

The Session Detail Record (SDR) feature has been enhanced:

- The device can now generate a new SDR type called "INTERMEDIATE". These SDRs are generated during the call. The time when the first Intermediate SDR is generated is configurable, by the new parameter 'First Intermediate Interval'. The interval between every generated SDR during the call is also configurable, by the new parameter 'Periodic Intermediate Interval'.
- Additional fields (optional) have been added to the SDR (media-related and tag fields)

Applicable Application: All.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.13.1.24 New Performance Monitoring Parameters

The device's Performance Monitoring module has been enhanced with additional performance monitoring parameters, providing statistical information for the following:

- WebRTC sessions and license key usage
- DS-1 (T1) calls
- Analog calls
- Storage utilization
- CPU utilization
- Call sessions
- Transcoding sessions
- Various SIP (SUBSCRIBE and REGISTER)
- DDOS

Applicable Application: All.

Applicable Products: All.

2.31.13.1.25 IP Profile Used by Third-Party Routing Server or ARM

IP Profiles can now be configured to be used by third-party routing servers or AudioCodes ARM. This feature is configured by the new IP Profile parameter, 'Used By Routing Server'.

Applicable Application: All.

Applicable Products: All.

2.31.13.1.26 Change in 'Caller ID Transport Type' Parameter Behavior

The 'Caller ID Transport Type' parameter [CallerIDTransportType] has been modified. The optional value **Relay** (1) is no longer supported and a new optional value **Set By Software** (4) has been added (which is now the new default value).

When the parameter is configured to **Set By Software**, Gateway calls will use the caller ID behavior as though the parameter is configured to **Mute** (3), and SBC calls will use the caller ID behavior as though the parameter is configured to **Disable** (0).

Applicable Application: All.

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

2.31.13.1.27 Missing Commands and Web Parameters Added

The following CLI commands and Web parameters (fields) that were missing in previous versions have now been added.

- New CLI commands:
  - `digest-auth-uri-mode` [SipDigestAuthorizationUriMode]
  - `unreg-on-startup` [UnRegisterOnStartup]
  - `max-sdp-sess-ver-id` [MaxSdpSessionVersionId]
  - `regions-connectivity-dial-plan` [RegionsConnectivityDialPlan]
  - `deny-access-on-fail-count` [DenyAccessOnFailCount]
  - `deny-auth-timer` [DenyAuthenticationTimer]
  - `use-rand-user` [UseRandomUser]
- New Web fields (TLS Contexts > Change Certificates table):
  - 'Subject Key Identifier' (`set-subject-key-identifier`)
  - 'Key Usage' (`set-key-usage`)
  - 'Extended Key Usage' (`set-extended-key-usage`)

Applicable Application: All.

Applicable Products: All.

2.31.13.2 Known Constraints

This section lists known constraints.

Table 2-52: Known Constraints in Version 7.40A.100.011

Incident	Description
SBC-28846	If an Ethernet Device associated with an IPv6 network interface is modified, the associated Static Route is deleted. Applicable Products: All

2.31.13.3 Resolved Constraints

This section lists resolved constraints.

Table 2-53: Resolved Constraints in Version 7.40A.100.011

Incident	Description
SBC-28575	Loading certificate errors appear in the Syslog. Applicable Products: All
SBC-27683	The device crashes (resets) on networking task (signal 904, task NWST). Applicable Products: Mediant 1000
SBC-27283	Removing Calling Name towards PSTN also removes Facility IE [03], causing the ISDN side to not recognize the reason of Anonymous call. As a result the call fails. Applicable Products: Gateway
SBC-27189	The device sends connection line 'c=0.0.0.0' in the SDP if it receives an SDP offer with a 'c=' line in the session section and an SDP answer with a 'c=' line in the media section. As a result, one-way voice occurs. Applicable Products: All
SBC-25947	SSH weakness discovered by the pentest tool. Applicable Products: All
SBC-25560	No corresponding CLI command for the ini file parameter [UseRandomUser]. Applicable Products: All
SBC-25064	The device fails to activate GenerateRTP (no voce) after call transfer Applicable Products: All
SBC-18309	The device saves only the first 20 coders in the SDP offer, causing a DTMF miss-match. Applicable Products: All
SBC-27859 / SBC-27894 / SBC-28131	A CPU overload of 100% is caused by a failed networking task. Applicable Products: All
25546 / 25157	When the Dial Plan is configured with the "n" wildcard, it doesn't only match digits 2 to 9. Applicable Products: All
22858	NGINX doesn't support the following TLS Context parameters - Cipher Server TLS13, Cipher Client TLS13, Key Exchange Groups Applicable Products: All

2.31.14 Version 7.40A.005.619

This version includes resolved constraints only.

Note: This version is applicable only to Mediant VE/CE/SE and Mediant 90xx SBCs.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- For FIPS support, please contact AudioCodes for details.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. Hitless upgrade requires the use of the "intermediate" 7.40A.005.509 version. 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 8.0.1122 or later.
  - √ OVOC Version 8.0.1122 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1122 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 8.0.1122 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.

2.31.14.1 Resolved Constraints

This section lists resolved constraints.

Table 2-54: Resolved Constraints in Version 7.40A.005.619

Incident	Description
SBC-34755	Hitless software upgrade from 7.20A.258 to this 7.40A.005.619 interim version fails (upgrade is successful, but all active calls are disconnected) due to call database mismatch between 7.2 and 7.4 versions. Applicable Products: Mediant Software; Mediant 90xx.

2.31.15 Version 7.40A.005.613

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

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- For FIPS support, please contact AudioCodes for details.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - √ 7.20A.260.*
  - √ 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, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. Hitless upgrade requires the use of the "intermediate" 7.40A.005.509 version. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.1122 or later.
  - √ OVOC Version 8.0.1122 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1122 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 8.0.1122 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.

2.31.15.1 New Features

This section describes the new features introduced in this version.

2.31.15.1.1 Mediant VE and CE Support for Gen3 Xeon-SP ("Ice Lake-SP")

The virtual SBCs (Mediant VE and CE) now support 3rd Gen Intel® Xeon® Scalable processors (code-named "Ice Lake-SP") based host servers. This allows the use of Intel's latest CPU server architecture with these SBCs.

Currently, there is no change in the supported SBC capacity when using these servers.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.31.15.1.2 Mediant 9080 SBC Hardware Revision Update

Later this year, Mediant 9080 SBCs will be shipped with a new hardware revision that includes an updated CPU module.

There is no change in the Mediant 9080 supported capacity, device configuration or supported features following this update.

The updated hardware revision is supported by this 7.4 software version (7.40A.100.114) or later. Earlier 7.4 software versions are not compatible with the new hardware revision.

Support for the new hardware revision was also added to the 7.2 LTS software version stream (7.20A.258.661 or later).

For upgrading 7.2 software to 7.4, an intermediate version which supports the new hardware revision should be used (7.40A.005.569 or later). For the upgrade procedure, refer to *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

Note: For Mediant 9080 HA system deployments: The HA pair (active-redundant) can have different hardware revisions, only if they are both running a supported software version (see above). Therefore, Customers are recommended to consider upgrading their HA pair to a software version supporting the new hardware revision. Doing so will ensure that a Mediant 9080 with the new hardware revision can be used in the HA system in case of a need for device replacement.

The updated hardware revision can be identified using one of the following methods:

- Yellow label on the left side of the device's chassis:
  - **Previous HW revision:** "Version P01"
  - **Updated HW revision:** "Version P02"
- Silver label on the upper cover of the device's chassis:
  - **Previous HW revision:** "FPRZ00157" (AC power supply) or "FPRZ00168" (DC power supply)
  - **Updated HW revision:** "FPRZ00191" (AC power supply) or "FPRZ00192" (DC power supply)
- Using the CLI command `show system hardware`:
  - **Previous HW revision:** `CPU: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz, total 48 cores, avx supported`
  - **Updated HW revision:** `CPU: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz, total 64 cores, avx supported`

Note: Mediant 9030 SBCs and the old Mediant 9000 (Gen 8) SBCs are not affected by this update.

Applicable Application: SBC.

Applicable Products: Mediant 9080.

2.31.15.2 Known Constraints

This section lists known constraints.

Table 2-55: Known Constraints in Version 7.40A.005.613

Incident	Description
SBC-30961	Media performance monitoring statistics (e.g., mediaKBytesInTotal) for calls that were established prior to an HA switchover and then closed after the switchover are not calculated in the new active device. Applicable Products: All

2.31.15.3 Resolved Constraints

This section lists resolved constraints.

Table 2-56: Resolved Constraints in Version 7.40A.005.613

Incident	Description
SBC-17014	A mismatch exists between the Performance Monitoring parameter and the CDR for attempted calls count. Applicable Products: All
SBC-18552	When the IP Group name is modified, the active alarm is not updated to reflect this name change. Applicable Products: All
SBC-19449	The device crashes (resets) when a search is performed in the Web interface that has a result of more than 3,000 characters. Applicable Products: All
SBC-19692	The device fails to perform a Telnet connection from the active to redundant unit. Applicable Products: HA
SBC-29907	Performance Monitoring polling from OVOC fails upon an NTP refresh. Applicable Products: All
SBC-29951	Performance Monitoring polling from OVOC fails upon negative UTC offsets other than -1. Applicable Products: All
SBC-30187	The device crashes (resets) with the error "TASK SPMR" due to race condition. Applicable Products: All
SBC-30383	The device crashes (resets) with the exception reason "TPAPP no sched for the last 16000 ticks". Applicable Products: All
SBC-31090	A CPU overload of 100% is caused by a failed networking task. Applicable Products: All

2.31.16 Version 7.40A.005.509

This version includes new features and resolved constraints.

Note: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

Note:

- **This version supports device upgrade from the following 7.2 versions**:
  - √ 7.20A.260.*
  - √ 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 you are using one of the supported versions listed above.
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 8.0.114 or later.
  - √ OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 or later prior to upgrading your device to this SBC version.
  - √ For Mediant VE/CE on Azure or AWS, the device serial number changes during the upgrade from Version 7.2 to 7.4 and therefore, a new entity for the device is created on OVOC. This limitation will be resolved in OVOC Version 8.0.
- **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 8.0.114 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.

2.31.16.1 New Features

This section describes the new features introduced in this version.

2.31.16.1.1 Disk Resize for Mediant VE

By default, Mediant VE images in Version 7.4 use 20-GB disk size. If additional disk space is needed, the virtual machine's disk size can be changed through the virtual environment / public cloud configuration. For example, in Azure it's done via the Azure portal by navigating to **Disks** > disk name > **Size + performance**, and then choosing **Resize**. Mediant VE software adjusts itself to the new disk size upon the next reboot.

Applicable Application: SBC

Applicable Products: Mediant VE.

2.31.16.1.2 Mediant VE SBC on Hyper-V and KVM

Mediant VE can now deployed on Hyper-V and KVM platforms.

Applicable Application: SBC

Applicable Products: Mediant VE.

2.31.16.2 Resolved Constraints

This section lists resolved constraints.

Table 2-57: Resolved Constraints in Version 7.40A.005.509

Incident	Description
SBC-19202	The device's Web interface is exposed to HTML code injection vulnerability. Applicable Products: All
SBC-22878	The device's NGINX configuration fails when IPv6 interfaces are used. Applicable Products: All
SBC-26515 / SBC-27917	The device responds to the REST `GET /api/v1/status` with the wrong time format in "localTimeStamp", causing loss of synchronization with OVOC. Applicable Products: All
SBC-27171	The device's hostname is missing in the textual description of the No-HA alarm and Manual Switch over alarm. Applicable Products: HA
SBC-27533	After upgrading Media Components to Version 7.4, the number of CPU cores is reduced from 8 to 7. Applicable Products: Mediant Software

2.31.17 Version 7.40A.005.314

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

Note: The following products are **not** supported in this version and will be supported in the next applicable release:

- Mediant VE SBC on Hyper-V and KVM
- Mediant VE/CE SBC on Google Cloud

Note:

- **Version 7.4 supports device upgrade from the following 7.2 versions**:
  - √ 7.20A.260.*
  - √ 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 you are using one of the supported versions listed above.
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 7.8.2265 or later.
  - √ OVOC Version 7.8.2265 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 7.8.2265 or later prior to upgrading your device to this SBC version.
  - √ For Mediant VE/CE on Azure or AWS, the device serial number changes during the upgrade from Version 7.2 to 7.4 and therefore, a new entity for the device is created on OVOC. This limitation will be resolved in OVOC Version 8.0.
- **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 7.8.2265 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.

2.31.17.1 New Features

This section describes the new features introduced in this version.

2.31.17.1.1 CentOS Stream 8

Version 7.4 uses custom Linux distribution based on CentOS Stream 8.

For upgrading your SBC from the 7.20A stream (based on CentOS 6), refer to the document SBC Upgrade Procedure from Ver. 7.2 to 7.4 Configuration Note. For upgrading your SBC from the 7.20CO stream (based on CentOS 8), use the Web-based interface's Software Upgrade Wizard.

Note: For hitless upgrade from 7.20A steam versions, AudioCodes provides a CMP file for an intermediate 7.4 version based on CentOS 6. This intermediate version is intended **only** for temporary use during the upgrade process. For more information, refer to the document, *SBC Upgrade Procedure from Ver. 7.2 to 7.4 Configuration Note*.

Applicable Application: SBC

Applicable Products: Mediant VE; Mediant CE; Mediant SE; Mediant 9000.

2.31.17.1.2 SNMP and Telnet Protocols Disabled by Default

SNMP and Telnet protocols are disabled by default for improved device security.

If you want to use one of these protocols, enable them using the following configuration parameters:

- **SNMP:** Setup > Administration > SNMP > SNMP Community Settings > 'Disable SNMP'
- **Telnet:** Setup > Administration > Web & CLI > CLI Settings > 'Embedded Telnet Server'

Note: The SNMP protocol must be enabled for devices that are managed by AudioCodes One Voice Operations Center (OVOC).

Applicable Application: SBC

Applicable Products: Mediant VE; Mediant CE; Mediant SE; Mediant 90xx.

2.31.17.1.3 Performance Monitoring Graph Configuration through CLI

The performance monitoring graphs and KPI layouts can now also be configured through the device's CLI, using the new `configure system > kpi` command.

Applicable Application: SBC

Applicable Products: All.

2.31.17.1.4 Performance Monitoring for Dropped Packets due to Firewall

A new performance monitoring parameter (aclDroppedTotal) has been added, which counts the number of IP packets dropped due to the device's Firewall table (access list).

Applicable Application: All

Applicable Products: All.

2.31.17.1.5 Syslog Messages to Serial Console

The device can now be configured to send syslog messages to the serial console (physically connected to the serial interface). This feature is enabled by the new parameter EnableConsoleLog (requires a device reset). The syslog messages are also sent to the remote Syslog server. While enabled, the CLI cannot be used for anything else.

Applicable Application: All

Applicable Products: All.

2.31.17.1.6 NGINX Version Update

The device's embedded NGINX engine has been updated to Version 1.19.1.

Applicable Application: SBC

Applicable Products: All.

2.31.17.2 Known Constraints

This section lists known constraints.

Table 2-58: Known Constraints in Version 7.40A.005.314

Incident	Description
SBC-27005 / SBC-23971	When terminating the ping through CLI, using the key sequence ^C, error messages appear in the Syslog and this action may crash (reset) the device. Applicable Products: Mediant 4000
SBC-27180	Software Upgrade from 7.20.CO.258.* versions is supported only via the Web Interface. Upgrade via REST API / CLI interface / Stack Manager is not working. Applicable Products: Mediant 90xx; Mediant VE; Mediant CE

2.31.17.3 Resolved Constraints

This section lists resolved constraints.

Table 2-59: Resolved Constraints in Version 7.40A.005.314

Incident	Description
SBC-24681	The device sends the debug file to the TFTP server from the wrong network interface. Applicable Products: All
SBC-24807	The device doesn't update the redundant unit after the license pool parameter is changed, causing an alarm. Applicable Products: HA
SBC-25108	The device resets with Task SPMT because of a memory overrun. Applicable Products: All
SBC-25197	The device's REST API has a syntax error for KPI (missing ";"). Applicable Products: All
SBC-25548	The 'Condition' field in the Message Conditions table is limited to 200 characters. This bug has been resolved (increased to 299). Applicable Products: All
SBC-26699	The device loses its certificate after an HA switch over because of a disproportion of TLS Contexts between active and redundant units. Applicable Products: HA

2.31.18 Version 7.40A.002.007

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

Note: The following products are not supported in this version and will be supported in the next applicable release:

- Mediant 9000 SBC
- Mediant 9030 SBC
- Mediant 9080 SBC
- Mediant SE SBC
- Mediant VE SBC
- Mediant CE SBC

Note:

- **Version 7.4 supports device upgrade from the following 7.2 versions**:
  - √ 7.20A.204.xxx software stream: 7.20A.204.540 and later
  - √ 7.20A.258.xxx software stream: 7.20A.258.119 and later
  - √ 7.20A.260.xxx software stream: 7.20A.260.005 and later

  Therefore, prior to upgrading to Version 7.4, make sure that you are using one of the supported versions listed above.
- **Using Version 7.4 with AudioCodes One Voice Operations Center (OVOC):**
  - √ This version is compatible only with OVOC Version 7.8.2000 or later.
  - √ OVOC Version 7.8.2000 is compatible with both device versions 7.2 and 7.4.
  - √ If you plan on using OVOC with SBC Version 7.4, first upgrade your OVOC to version 7.8.2000 or later prior to upgrading your device to Version 7.4.
- **Using Version 7.4 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 7.8.2000 or later, prior to upgrading the devices in the pool to Version 7.4. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.31.18.1 New Features

This section describes the new features introduced in this version.

2.31.18.1.1 FIPS Support

The device can operate in "FIPS Mode" to fully comply with Federal Information Processing Standards (FIPS) 140-2 Level 1, which is a security standard specified by the United States Government that is used to validate cryptographic modules (i.e., the device). The FIPS standards specify best practices and security requirements for implementing crypto algorithms, encryption schemes, handling important data, and working with various operating systems and hardware, whenever cryptographic-based security systems must be used to protect sensitive, valuable data. FIPS also defines specific methods for encryption and specific methods for generating encryption keys. For more information on AudioCodes' FIPS certification, go to https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3708.

The following new CLI commands were added for enabling and configuring FIPS on the device:

- `fips on|off`: Enables and disables FIPS mode.
- `clear security-files`: Triggers zeroization (automatically done when enabling FIPS mode). Zeroization wipes out all sensitive content residing on the device, including security secrets such as private keys for SSH and TLS, the core dump file, and System Snapshot files.
- `show system security status`: Indicates if the device is operating in FIPS mode.

Applicable Application: SBC

Applicable Products: Mediant 9080; Mediant 4000B.

2.31.18.1.2 Enhanced DoS and DDoS Protection

The device provides improved protection from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:

- Enhanced prevention of DoS/DDoS SIP flood attacks
- Improved defense against TCP\IP vulnerabilities
- Optimal handling of SIP user registration avalanche
- Designed to prevent over-the-top traffic from unknown sources

Applicable Application: SBC

Applicable Products: Mediant 90xx; Mediant Software.

2.31.18.1.3 Lawful Interception Support

Note:

- The Lawful Interception feature is not part of the standard Software Version 7.4 build. It is delivered as a separate, dedicated 7.4 version build, available only to Customers that have ordered and licensed this feature.
- For further information on the Lawful Interception feature, contact your AudioCodes sales representative.

Under the terms stated in the note above, the device now supports lawful interception for intercepting signaling and media traffic of specific (targeted) subscribers towards mediation devices in Law Enforcement Agency (LEA) networks. This functionality is known as Lawful Interception and refers to the facilities in telecommunications and telephone networks that allow LEAs (with court orders or other legal authorization) to selectively wiretap individual subscribers.

Applicable Application: SBC

Applicable Products: Mediant 9080; Mediant VE/SE.

2.31.18.1.4 New Performance Measurement Infrastructure

The device provides a new infrastructure for performance monitoring.

2.31.18.1.4.1 New Performance Measurement System

The device provides a new performance monitoring (PM) infrastructure, offering the following enhancements:

- Five-fold increase in the number of key-performance metrics (KPI), measuring almost every aspect of the SBC including additional areas such as license usage, DDOS,

CPU utilization, and memory usage.

- Capability to configure a fully customized threshold-crossing SNMP trap event (acKpiThresholdCrossing / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.148) per performance monitoring parameter and entity (e.g., per IP Group):
  - Threshold value to raise and clear the trap event
  - Trap severity level
  - Trap message
- Delivery of PMs to multiple interfaces, including REST API, SNMP, CLI, Web and OVOC. REST and CLI interfaces also enable the user to perform flexible queries of PMs (for example, for a specific measured interval), including the ability to query multiple concurrent PMs in a single request.
- Web interface provides a sophisticated tool for plotting graphs of performance monitoring parameters (real-time or historical). The graphs can be customized (labels, line color, and legend) and can be sent to a printer or downloaded in different file formats (e.g., PDF or PNG).
- Number of stored 15-minute collection intervals has been increased from 2 to 4 for historical PM measurements (some PMs have even been increased to a 100 – reflecting 25 hours).

Note: Due to this new performance monitoring system, the following previously supported features are now obsolete:

- Success/Failure Ratio page (Monitor menu > Monitor tab > Performance Monitoring folder > Success / Failure Ratio)
- Average Call Duration page (Monitor menu > Monitor tab > Performance Monitoring folder > Average Call Duration)
- Trunk Utilization page (Monitor menu > Monitor tab > Performance Monitoring folder > Trunk Utilization)
- Performance Profile table (Monitor menu > Monitor tab > Performance Monitoring folder > Performance Profile)
- User Defined Failure PM table (Monitor menu > Monitor tab > Performance Monitoring folder > User Defined Failure PM)

Applicable Application: All.

Applicable Products: All.

2.31.18.1.4.2 Plotting Graphs for Performance Monitoring Parameters

Performance monitoring parameters (real-time or historical) can now be displayed in the Web interface in graph format:

- Graphs can be displayed in different grid layouts per page (1x1, 1x2, 2x1, or 2x2).
- Graph title, x-axis title, and y-axis title can be customized.
- Each graph can include multiple, plotted performance monitoring parameters.
- Each plotted performance monitoring parameter can be assigned a line color, allowing the user to easily distinguish between the performance monitoring parameters on the graph.
- A powerful, but easy-to-use tool is provided for drilling down and selecting each performance monitoring parameter from the device's hierarchical structure of REST-based performance monitoring parameters.
- A tooltip can be enabled which displays the value where the user hovers over the plotted performance monitoring line.
- Each graph provides a legend, showing the performance monitoring parameter's name and its color. The legend can also be used to filter the graph, by hiding or showing the

plotted performance monitoring parameter.

- The graph can be easily zoomed in or out, allowing the user to view values of different resolutions.
- Graphs can be printed or downloaded in file format (PNG, JPEG, SVG, PDF or CSV).

The feature is configured by the following parent-child Web page, located under the new Monitor menu > Monitor tab > Performance Monitoring folder:

- Parent table (page) - KPI Layouts table: This table configures the layout's name and grid layout.
- Children pages: These are the pages of each configured KPI Layout, on which the actual graphs are created and plotted.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.4.3 Alarm Thresholds for Performance Monitoring

Alarm thresholds (acKpiThresholdCrossing / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.148) can now be configured for any performance monitoring parameter. An alarm can be configured to be raised or cleared when the parameter crosses a user-defined upper or lower threshold value. The alarm text of the raised or cleared alarm can also be customized as well as the severity level of the raised alarm.

The feature is supported by the new Alarm Thresholds table, located under Setup menu > Administration tab > Performance Monitoring folder.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.5 Session Detail Records (SDR) Support

The device can now generate Session Detail Records (SDRs). Unlike CDRs, which are generated per SBC leg (ingress or egress leg of the call), SDRs are generated for both legs. In other words, an SDR is a call detail record of the entire call session. SDRs also contain more information on the call that is relevant for billing applications and thus, are especially useful in billing applications.

SDRs can be stored locally on the device in CSV format or periodically sent to a remote third-party SFTP server. The SDR can be generated for successfully established and terminated calls (STOP SDRs), or for failed call attempts (ATTEMPT SDRs).

The device supports a default SDR structure. However, the structure can be customized, by selecting only the fields to include in the SDR and by defining the field names (titles).

For SDR configuration, the Web interface's navigation pane provides a new "Session Detail Record" folder, which contains menu items that open the following new pages:

- SDR Settings page:
  - General:
    - 'Record Type'
  - Syslog SDR Reports:
    - 'SDR Syslog': Defines a dedicated Syslog server to where SDRs can be sent
    - 'SDR Server IP Address': Defines the address of the Syslog server (if not configured, sends to CDR Syslog server address)
  - SDR Local Storage:
    - 'Local Storage': Enables local storage of SDRs.

- 'File Size': Defines the maximum size (in kilobytes) of the SDR file.
- 'Number of files': Defines the maximum number of SDR files in local storage.
- 'File name': Defines the filename format of the stored SDR file.
- 'Rotation period': Defines how often an SDR file is created.
- 'Compression format': Defines the file compression type (none, .zip, or .gzip).

- SDR Servers:
  - 'SDR Servers Send Period': Defines the interval between each SDR files transaction to the server.
  - 'SDR Servers Bulk Size': Defines the number of files sent to the server at each file transfer transaction.
  - 'Pending SDR Files': Displays the number of files yet to be transferred.

  If the device fails to send the locally stored SDRs to the remote servers, the device sends a new SNMP alarm, acSDRServerAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.147).

- SBC SDR Format table: This new table customizes the SDR fields (remove, add, or change the name of fields, change order of fields)
- SBC SDR Remote Servers table: Defines up to two remote SDR servers, which can provide active-standby redundancy.

For HA, SDR configuration is synchronized. For local storage, active and redundant devices maintain their own stored SDR files. Upon switchover, the stored files are not copied over. Stored files on the redundant device can be viewed and managed from the active device through SSH or SFTP.

Applicable Application: SBC.

Applicable Products: Mediant Software; Mediant 90xx.

2.31.18.1.6 Media Path Optimization in Media Bypass Mode for Direct Routing

The device now supports Microsoft's proprietary SIP header X-MS-UserSite, which is used for Local Media Optimization in Microsoft's Teams environments. This header, which is present in the SIP message received from the Teams client, indicates the Teams site (name) within which the Teams client is located. Based on this header, the device can now determine if the path (connectivity) between the Teams clients is good for voice quality and thus, intended for direct media calls.

The following configuration has been updated due to this support:

- The device's handling of Teams calls to determine direct media has been updated regarding the existing IP Group's 'Teams Local Media Optimization Handling' parameter. For more information, refer to the *User's Manual*.
- For determining if the path is good for voice quality and thus, intended for direct media, the device uses the following mechanism:
  - A new parameter 'Teams Local Media Optimization Site' has been added to the IP Groups table to define the name of the Teams site (e.g., "Singapore"). For each IP Group representing specific Teams clients, this parameter is configured accordingly with the site's name.
  - A Dial Plan is used to determine if the path between the Teams clients is intended for direct media. The Dial Plan is specified by the new parameter 'Region Connectivity Dial Plan'. Each Dial Plan rule in the Dial Plan is configured with a Teams site name in the 'Prefix' parameter (e.g., "Singapore") and with logical group(s) to which the Teams site belongs in the 'Tag' parameter (e.g., "Group=2,7"). When the device receives the SIP dialog from a Teams client, it checks the Dial Plan to see if the Teams sites of the source and destination Teams clients share a common group number. If they do, the device considers the call as direct media.

Applicable Application: SBC.

Applicable Products: All.

2.31.18.1.7 Bulk Software Upgrade of Media Cluster Via OVOC

OVOC can now be used to upgrade a media cluster (multiple Media Components or also referred to as MTs) for the Media Transcoding Cluster (MTC) feature or Elastic Media Cluster feature (Mediant CE). During the upgrade, the Signaling Component (SC) sends status updates of the upgrade process to OVOC.

Applicable Application: SBC.

Applicable Products: Mediant 90xx (with MTs); Mediant CE; Mediant VE.

2.31.18.1.8 TLS Context (Certificate) Enhancements

TLS Context (certificate) configuration includes the following enhancements:

- A device reset is no longer required when adding or modifying TLS Context parameters, including their related files (self-signed certificates, private keys or root certificates).
- Private key size of 1024 is no longer an optional value.
- SHA-1 has been removed as an optional value for the signature algorithm.
- CLI commands have been restructured.
- The Change Certificates page (child of the TLS Contexts page) in the Web interface has been updated with regards to design.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.9 CNAME and SRV DNS Queries for Firewall

The device's firewall (access list), which is configured in the Firewall table, now supports CNAME and SRV DNS queries when the 'Source IP' parameter is configured with an FQDN.

A CNAME query for an FQDN replies with the canonical name of the requested FQDN. This hostname is used to resolve the IP address. An SRV query for an FQDN replies with a service list of one or more SRV records, each containing multiple fields, including the canonical hostname of the machine providing the service. This hostname is used to resolve the IP address. Up until now, if an FQDN was configured, the device performed an A-record DNS query to resolve the domain name into an IPv4 IP address.

The feature is supported by a new parameter in the Firewall table, 'DNS Query Type' (DnsQueryType) which allows the user to choose the DNS query type:

- [1] A (default and for IPv4 queries)
- [2] AAAA (IPv6 queries)
- [3] CNAME A (cname query, resolved into IPv4 address)
- [4] CNAME AAAA (cname query, resolved into an IPv6 address)
- [5] SRV A (SRV query, resolved into an IPv4 address)
- [6] SRV AAAA (SRV query, resolved into an IPv6 address)

The device performs DNS resolution periodically (i.e., resolved addresses are not persistent).

For the CLI command `nslookup`, support for SRV/CNAME resolution types has also been added:

```
nslookup <hostname> [source voip interface vlan] type
<A/AAAA/SRV/CNAME>
```

A total of 500 IP addresses can be added to the Firewall (defined as IP addresses or resolved by DNS).

Applicable Application: All.

Applicable Products: All.

2.31.18.1.10 Persistent Logging

The device now automatically saves logged event messages on its local storage memory, which remain (persistent) even after the device resets or powers off. This functionality is by default and can't be disabled.

- The device can store up to 10 persistent log files. The maximum size (in KB) of each file (default is 1,024 KB) can be configured by the new parameter SystemPersistentLogSize (`configure troubleshoot > syslog > system-persistent-log-size`).
- Persistent log file contents can be viewed using the new CLI command `show system log persistent`

  (The `show system persistent-log` and `debug persistent-log` commands are now obsolete.)
- Persistent log files can be downloaded or sent to a remote server, using the new CLI command `copy system-log-persistent to`.

Note: This feature replaces the persistent logging feature supported by Mediant 90xx and Mediant Software in Version 7.2.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.18.1.11 Enhanced Logging Features

The following enhancements have been made to the logging feature:

- Viewing logs through the CLI can be filtered to include only non-SIP logged messages, using the new CLI command `show system log no-sip`.
- Downloading logged files (compressed in tar.gz format):
  - `copy system-log to`: downloads system log file
  - `copy system-log-no-sip to`: downloads system log file without SIP-related information
- The debug file (`show debug-file`) now also includes persistent logs, no-sip logs, and syslog of kernel
- A new SNMP trap event is sent when debug recording is activated (acDebugRecordingActivationAlarm / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.150)

Applicable Application: All.

Applicable Products: All.

2.31.18.1.12 AudioCodes Plugins No Longer Required for Wireshark

Installing AudioCodes Wireshark packet-dissector plugins are no longer required from Wireshark Version 3.4.0 and later. The plugins have now been integrated into the Wireshark open-source application, providing built-in support for AudioCodes Debug Recording (ACDR).

Applicable Application: All.

Applicable Products: All.

2.31.18.1.13 CAC Algorithm Based on Sliding Window Counter

The device's Call Admission Control (CAC) now supports an additional, more accurate rate-limiting algorithm for SIP dialogs based on a *sliding window counter*, than the already supported token bucket algorithm.

The Sliding Window counter algorithm sets a rate for the window, where the window is the previous (last) second to when the incoming SIP dialog-initiating request (e.g., INVITE) is received. When the device receives a new SIP dialog request, it checks how many dialog requests were received in the window (previous second). If the number (counter) is below the configured rate, the device accepts the SIP dialog. If the number is at the configured rate, the device rejects the call.

For example, assume the rate is configured to 5. If the device receives a new incoming SIP-dialog request at 18:00:01 (hh:mm:ss) and only 4 dialog requests were received in the previous window (i.e., 18:00:00-18:00:01), it accepts the new dialog request. However, if 5 dialog requests were received in the window when the new dialog arrived, the new dialog is rejected.

This new CAC algorithm is enabled (disabled by default) by the new parameter 'Sliding Window Counter Rate Limiting Algorithm For CAC'.

In addition to this feature, the following existing parameters now have a valid value range (0-65535): 'Rate', 'Rate Per User', 'Maximum Burst', 'Maximum Burst Per User'. Note that if configured out of this range in a previous version when upgrading to Version 7.4, if the value is less than 0 the value is set to 0 and if the value is greater than 65,535 it is set to 65,535.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.18.1.14 Debug Recording Enhancements

The device's debug recording feature has been enhanced:

- Logging Filters table:
  - (Only Mediant 90xx and Mediant Software) Up until now, local storage ('Log Destination' set to **Local Storage**) was supported only for CDRs ('Log Type' set to **CDR Only**). Now, local storage is also supported for the following log types:
    - Signaling
    - Signaling & Media
    - Signaling & Media & PCM
    - SIP Only
  - New 'Filter Type' value called **System Trace**, which includes logs that don't relate to calls (e.g., CPU or disconnected LDAP server; HA traffic between active and redundant). When selected, the 'Value' parameter can be configured to one of the following values:
    - "syslog": INFO packets
    - "tpncp": device event and command packets as shown when using "tpncp" Wireshark filter
    - "ha": communication between active and redundant
- A new page titled "Debug Recording" has been added (Troubleshoot menu > Troubleshoot tab > Logging folder > Debug Recording), which contains the following groups of parameters:

- **IP Trace:** This group provides new parameters for filtering IP traces when the Logging Filters table has a rule whose 'Filter Type' parameter is set to **IP Trace**. The traces can be filtered by a specific physical entity -- Ethernet port, VLAN, or Ethernet Group (Mediant 90xx and Mediant Software only). If not specified (default), the IP trace records traffic received from and transmitted to all ports.
- **Debug Recording Server:** The debug recording parameters under this group were moved from the Debug Recording group on the existing Logging Settings page ('Debug Recording Destination IP', 'Debug Recording Destination Port' and 'Debug Recording Interface Name'). In addition, "Debug Recording" has been removed from their parameter names.
- **Local Files Storage:** (Only Mediant 90xx and Mediant Software) Local storage of debug recording files are now supported. This is relevant for Logging Filter rules whose 'Log Destination' parameter is configured to **Local Storage** and 'Log Types' configured to any value except **CDR Only** or **Call Flow**. New parameters have been added to support the feature - 'Local Storage', 'Recording', 'File Size', 'Number of Files', 'File Mode' and 'Rotation Period'

- SFTP can be used to download locally stored debug files.
- Up until now, after an HA switchover, only data was recorded (not media/RTP) for IP traces. Now, the IP trace also includes media after a switchover.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.15 Maximum Characters Increased for Dial Plan Tags

The maximum number of characters that can be configured for Dial Plan tags in the Dial Plan Rule table ('Tag' parameter) has been increased from 120 to 255.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.31.18.1.16 Maximum IP Profiles Increased

The maximum number of IP Profiles that can be configured (in the IP Profiles table) has been increased to 1,500 for devices supporting 64 GB storage.

Applicable Application: SBC.

Applicable Products: Mediant VE/CE.

2.31.18.1.17 Interworking between ISDN CUG and SIP

The device now supports interworking between the ISDN Closed User Group (CUG) supplementary service and SIP, for Tel-to-IP calls. The CUG supplementary service enables users to form groups, where members of a specific closed user group can communicate among themselves but not, in general, with users outside the group.

If this feature is enabled and the device receives an ISDN Setup message whose Facility IE indicates CUG (cUGCall invoke), it adds an XML body containing CUG information (CUG index and outgoing access) to the outgoing SIP INVITE message, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
elementFormDefault=" qualified"
attributeFormDefault="unqualified">
<xs:annotation>
```

```
<xs:documentation>XML Schema Definition for the closed user group
parameter</xs:documentation>
</xs:annotation>
<xs:include schemaLocation="xcap.xsd"/>
<!--Definition of simple types-->
<xs:simpleType name="twobitType">
<xs:restriction base="xs:string">
<xs:pattern value="[0-1][0-1]"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="networkIdentityType">
<xs:restriction base="xs.hexBinary">
<xs.length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="sixteenbitType">
<xs:restriction base="xs:hexBinary">
<xs:length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="cugIndexType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="0"/>
<xs:maxInclusive value="32767"/>
</xs:restriction>
</xs:simpleType>
<!--Definition of complex types-->
<xs:complexType name="cugRequestType">
<xs:sequence>
<xs:element name="outgoingAccessRequest" type="xs:boolean"/>
<xs:element name="cugIndex" type="cugIndexType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<!--Definition of document structure-->
<xs:element name="cug" substitutionGroup="ss:absService">
<xs:complexType>
<xs:complexContent>
<xs:extension base="ss:simservType">
<xs:sequence>
<xs:element name="cugCallOperation" type="cugRequestType"
minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="outgoingAccessRequest" type="xs:boolean"
value="True"/>
<xs:element name="cugIndex" type="xs:integer" value="32767"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="networkIndicator" type="networkIdentityType"
minOccurs="0"/>
```

```
<xs:element name="cugInterlockBinaryCode" type="sixteenbitType"
minOccurs="0"/>
<xs:element name="cugCommunicationIndicator" type="twobitType"
minOccurs="0"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
</xs:schema>
```

The feature is enabled by the new parameter, 'Cug Data Mode' (CugDataMode / cug-data-mode). By default (disabled), the device doesn't add the CUG body. If enabled, the device adds the CUG XML body.

Applicable Application: Gateway (ISDN).

Applicable Products: Mediant 500; Mediant 800; Mediant 1000.

2.31.18.1.18 Activity Log Includes Parameter Changes from Incremental ini File

The existing Activity Log, which sends logs of selected management user operations done in the device's management interfaces to Syslog, can now be enabled to include a log of parameter changes due to an uploaded incremental ini file. When loading an incremental ini file, only parameter settings included in the ini file are applied to the device; all other parameters remain at their current settings. This feature applies to incremental ini file load through the Web interface (Auxiliary Files page) or CLI (`copy incremental-ini-file from`).

The feature is enabled by a new checkbox located under the Activity Log group in the Web interface (`configure troubleshoot > activity-log > incremental-ini-log`). In addition, the maximum number of lines (not empty or comments) to log from the ini file can be configured using the new parameter MaxINIActivityLog (`configure troubleshoot > max-ini-activity-logs`).

Applicable Application: All.

Applicable Products: All.

2.31.18.1.19 NGINX Syntactic Errors Displayed in Syslog

Syntactic errors when adding NGINX directives (in the HTTP Directive Sets > HTTP Directives table) for the device's HTTP Proxy functionality are now reflected in Syslog messages. Up until now, they were displayed only in the device's CLI (`show network http-proxy conf errors`).

Applicable Application: SBC.

Applicable Products: All.

2.31.18.1.20 Incremental ini File Load through SNMP

SNMP can now be used to load an incremental ini file to the device from a remote HTTP-based server. This is done using the new MIB object, acSysHTTPClientIncrementalIniFileURL. The corresponding existing ini file parameter is IncrementalIniFileURL.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.21 SC Local Users Table Synchronized with MT

The Signaling Component's (SC) Local Users table, which configures the management users, is now synchronized with all the Media Components (MCs). Therefore, accessing the Media Components' management interfaces should be done using the same users (username and password) as for accessing the Signaling Component.

The SC transfers the Local Users table to the MTs upon the following conditions:

- When MT connects to the SC.
- When the table is modified on the SC (any change causes transfer of the entire table to the MTs)

If the MT admin modifies the MT's Local Users table, the new configuration on the MT remains until one of the conditions above occurs.

Applicable Application: SBC.

Applicable Products: Mediant CE (Elastic Media Cluster); Mediant 90xx (Media Transcoding Cluster).

2.31.18.1.22 B-Channel Negotiation Mode Configuration Update

As the CLI command `b-ch-negotiation` is a global parameter (i.e., affecting all trunks), it has been moved from `configure voip` > `interface e1-t1|bri` to `configure voip` > `gateway digital settings`. A new CLI command, `b-channel-nego-for-trunk` has been added to `configure voip` > `interface e1-t1|bri` for configuring B-channel negotiation mode per trunk.

Applicable Application: Gateway (Digital).

Applicable Products: Digital.

2.31.18.1.23 Maximum Stored Historical SBC CDRs Reduced

The maximum number of historical SBC CDRs that can be stored on the device (and displayed in the SBC CDR History table) has been reduced for some products, as follows:

- 2,048 (instead of 4,096): MP-1288, Mediant 500, Mediant 500L, Mediant 800 and Mediant 1000
- 4,096: Mediant 2600 and Mediant 4000

Applicable Application: SBC.

Applicable Products: MP-1288; Mediant 500; Mediant 500L, Mediant 800; Mediant 1000; Mediant 2600; Mediant 4000.

2.31.18.1.24 Management User Password Hidden in Activity Log

When password obscurity is enabled or enforced (`obscure-password-mode on` and `enforce-password-complexity`) and a password is configured for a new management user (successfully or not) or the password of an existing user is modified (Local Users table), if reporting of management user activities is enabled, the password is not shown in the Activity Log.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.25 Reduction in Excess SIP Interfaces

As the maximum number of SIP Interfaces was more than required for typical deployments, the maximum has been reduced to free-up memory for other functionality:

- MP-1288, Mediant 500/L, Mediant 800, Mediant 1000: 80 (was 82)
- Mediant 2600, Mediant 4000: 700 (was 1,200)
- Mediant 90xx: 1,200 (no change)
- Mediant Software:
  - 2 GB: 40 (was 600)
  - 3 GB: 200 (was 1,200)
  - 4 GB: 400 (was 1,200)
  - 8 GB: 800 (was 1,200)
  - 16 GB: 1,200 (no change)
  - 32-64 GB: 1,200 (no change)

Note: When upgrading to Version 7.4 from an earlier version when the device is configured with more SIP Interfaces than the new maximum number of allowed SIP Interfaces for Ver. 7.4, the excess configured SIP Interfaces (trimmed from the SIP Interface with the highest table row index) are deleted. For example, if there are 1,000 SIP Interfaces in Ver. 7.2, only the first 700 SIP Interfaces in the table remain after the upgrade to Ver. 7.4.

Applicable Application: All.

Applicable Products: All.

2.31.18.1.26 New Hardware Revision for CRMX Module

The CRMX module, which is housed in the Mediant 1000 E-SBC & Gateway, was updated due to one of its components reaching End-Of-Life (EOL) status. The new CRMX module no longer has a WAN port (which was not used and covered by a metal plate).

The new CRMX module is compatible with Software Version 7.40A.002.007 and later.

Applicable Application: All.

Applicable Products: Mediant 1000.

2.31.18.2 Known Constraints

This section lists known constraints.

Table 2-60: Known Constraints in Version 7.4

Incident	Description
-	The following products are not supported in this version: ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant SE SBC ▪ Mediant VE SBC ▪ Mediant CE SBC
SBC-24381	For the Lawful Interception feature, the target's XID can only be configured to a numerical value. If it's alphanumeric, it can't be deleted nor updated.

2.31.18.3 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 2-61: Resolved Constraints in Version 7.4

Incident	Description
SBC-15662	The device experiences no audio after an attempt to replace the TLS certificate on the fly (without a reset). **Applicable Products:** All
SBC-16401	The device generates the following messages to the CLI: "file truncated /sbin/tail: /var/log/messages:" and "/sbin/tail: /var/log/messages: file truncated". **Applicable Products:** All
SBC-16408	Customizing user-level access privileges for Web interface pages doesn't apply to the import and export commands of the Action button on Web pages that provide this button. For example, if the Malicious Signature table is customized to read-write for all users, it doesn't apply this to the import/export actions (and only Security Admin can import/export). **Applicable Products:** All
SBC-17014	The value of the performance monitoring parameter for attempted calls count doesn't match the CDR. **Applicable Products:** All
SBC-17618	Device's Web interface is using outdated libraries. These libraries have now been updated.
SBC-18658	The associated contact address (AOR) is not updated in the database after changes in the Dial Plan. **Applicable Products:** All
SBC-19202	The device is exposed to a security vulnerability, allowing HTML injection tags/scripts to search a term. **Applicable Products:** All
SBC-19603 / SBC-21622	Lines (rows) in the Classification table of the Web interface cannot be reordered. **Applicable Products:** All

Incident	Description
SBC-20216	The CLI `ping` command doesn't function for IPv4 addresses. **Applicable Products:** All
SBC-21716	Filtering the `show voip calls` command output using the grep filter (`| grep`) doesn't function. This has been resolved by replacing the grep switch with the new `match` switch, which provides a simple string match of the call detail record text. For example, to search the string "abc": `show voip calls active sbc match abc` **Applicable Products:** All
SBC-21801	Loading an ini file to the SBC through OVOC doesn't function properly when SetDefaultOnIniFileProcess parameter is configured to 0. **Applicable Products:** All

3 Session Capacity

This section provides capacity for the Gateway and SBC products.

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 GW: Table 3-4
				GW-Only	30	30	
Mediant 500L		60	200	Hybrid	60	60	Transcoding: n/a GW: Table 3-6
				GW-Only	8	8	
Mediant 800B		250	1,500	Hybrid	250	250	GW & Transcoding: Table 3-8 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 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 GW: Table 3-15
		960	20,000	GW-Only	960	960	Table 3-15
MP-1288		588	350	Hybrid	588	438	Transcoding: n/a 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 Transcoding: Table 3-31
	Azure		36,000	75,000	SBC-Only	36,000	32,000	Forwarding: Table 3-32
			32,000	75,000	SBC-Only	32,000	32,000	Forwarding: Table 3-32 Transcoding: Table 3-33
	VMware		12,000	100,000	SBC-Only	12,000	12,000	Forwarding: Table 3-34 Transcoding: Table 3-35
Mediant VE	VMware	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	4,000	15,000	SBC-Only	4,000	2,600	Transcoding: n/a
		4 vCPU 16-GB RAM (HT)	8,000	75,000	SBC-Only	8,000	6,000	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	4,000	15,000	SBC-Only	2,200	1,900	Transcoding: Table 3-36
		4 vCPU 8-GB RAM (HT)	4,000	15,000	SBC-Only	1,800	1,600	Transcoding: Table 3-36
		8 vCPU 16-GB RAM (HT)	9,000	75,000	SBC-Only	6,000	5,000	Transcoding: Table 3-36
		16 vCPU 16-GB RAM (HT)	9,000	75,000	SBC-Only	6,500	5,000	Transcoding: Table 3-36
	KVM / OpenStack	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	2,500	15,000	SBC-Only	2,500	1,700	Transcoding: n/a
		4 vCPU 16-GB RAM (HT)	4,500	75,000	SBC-Only	4,500	3,500	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	1,900	15,000	SBC-Only	1,900	1,400	Transcoding: Table 3-36
		8 vCPU 16-GB RAM (HT)	5,800	75,000	SBC-Only	5,800	4,800	Transcoding: Table 3-36
		16 vCPU 16-GB RAM (HT)	3,800	75,000	SBC-Only	3,800	2,800	Transcoding: Table 3-36

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
		8 vCPU 32-GB RAM SR-IOV Intel NICs (non-HT)	24,000	75,000	SBC-Only	24,000	10,000	Transcoding: n/a
	Hyper-V	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	1,500	15,000	SBC-Only	1,500	1,200	Transcoding: n/a
		4 vCPU 8-GB RAM (HT)	2,500	15,000	SBC-Only	2,500	2,300	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	1,900	15,000	SBC-Only	1,900	1,400	Transcoding: Table 3-36
		8 vCPU 16-GB RAM (HT)	2,500	75,000	SBC-Only	2,500	2,300	Transcoding: Table 3-36
	AWS / EC2	m5.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 3-37
		c5.2xlarge	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 3-38
		c5.9xlarge	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 3-39
	Azure	DS1_v2	600	1,000	SBC-Only	600	500	Transcoding: n/a
			300	1,000	SBC-Only	300	300	Transcoding: Table 3-41
		DS2_v2	1,200	15,000	SBC-Only	1,200	800	Transcoding: n/a
			900	15,000	SBC-Only	900	600	Transcoding: Table 3-41
		DS3_v2	1,700	50,000	SBC-Only	1,700	1,600	Transcoding: n/a
			1,100	50,000	SBC-Only	1,100	800	Transcoding: Table 3-41
		DS4_v2	1,800	75,000	SBC-Only	1,800	1,600	Transcoding: n/a
			1,600	75,000	SBC-Only	1,600	1,600	Transcoding: Table 3-41
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 3-42
		SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a

General:

- The figures listed in the table are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, 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 above the maximum media sessions, the rest of the 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 (for SBC sessions) or TDM-RTP (for 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 SBC 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 SBC and using one media session resource.
  - √ A gateway session (i.e., TDM-RTP or TDM-SRTP) is also considered as a media session for the calculation of media sessions. In other words, the maximum Media Sessions specified in the table refer to the sum of Gateway and SBC sessions.
  - √ In case of direct media (i.e., Anti-tromboning / Non-Media Anchoring), where only SIP signaling traverses the SBC 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 leg G.729, one signaling resource, one media session resource, and one transcoding session resource is used.
- Cloud Resilience Package (CRP) application capacity is listed under "Registered Users".
- Lync Analog Device (LAD) application capacity is listed under "Media Sessions".

MP-1288:

- The maximum number of media and signaling sessions is the summation 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 summation of the maximum 150 RTP-to-SRTP (SBC) sessions and the maximum 288 TDM-SRTP (Gateway) sessions.

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 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.

Mediant VE SBC:

- Mediant VE SBC for AWS: Versions prior to 7.40A.300 don't support AWS instance types m5n, c5n, and r5n. If these instance types are required, upgrade to Version 7.40A.300 or later.
- Mediant VE SBC for VMware: The profiles are applicable to when ESXi version is 6.7 or later, host's CPU is Intel Xeon Scalable Processors, and Hyper-Threading is enabled. For example, a 4-vCPU virtual machine allocates only 2 physical cores. For minimum requirements, see Section 3.3.15.1 on page 230.

Mediant CE SBC:

Mediant CE is based on the following instances:

- AWS:
  - √ Signaling Components (SC): m5.2xlarge
  - √ Media Components (MC) - forwarding only: m5.large
  - √ MC - forwarding and transcoding: c5.4xlarge

  Note that versions prior to 7.40A.300 **don't** support AWS instance types m5n, c5n, and r5n. If these instance types are required, upgrade to Version 7.40A.300 or later.
- Azure:
  - √ SC: DS3_v2 (up to 10,000 sessions and 50,000 users) or D8s_v3/v4 (up to 36,000 sessions and 75,000 users)
  - √ MC - forwarding only: DS2_v2, DS3_v2 or DS4_v2
  - √ MC - forwarding and transcoding: DS2_v2, DS3_v2, or DS4_v2
- VMware:
  - √ SC: 8-vCPU (Hyper-Threaded), 16-GB RAM
  - √ MC - forwarding only: 2-vCPU (Hyper-Threaded), 8-GB RAM
  - √ MC - forwarding and transcoding: 8-vCPU (Hyper-Threaded), 8-GB RAM

Mediant SE SBC:

For new deployments, it's strongly 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 capacity per feature.

Table 3-2: Maximum Capacity per Feature

Product	Concurrent WebRTC Sessions (see Note #3)		One-Voice Resiliency (OVR) Users	Concurrent SIPRec Sessions (see Note #4)	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 4000B / Mediant 4000	1,000	1,000	-	2,500	2,500	100
Mediant 9000	5,000	16,000	-	▪ With Hyper-Threading: 20,000 ▪ Without 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 ▪ 3 GB: 500 ▪ 4 GB: 5,000 ▪ 8-16 GB: 6,000 ▪ 32 GB: 16,000 ▪ 64 GB: 25,000	100

Product	Concurrent WebRTC Sessions (see Note #3)		One-Voice Resiliency (OVR) Users	Concurrent SIPRec Sessions (see Note #4)	Concurrent TLS Connections	Concurrent MSRP Sessions
	Click-to-Call	Registered Agents				
Mediant CE (see note #2)	5,000	▪ SC with 8 vCPUs: 16,000 ▪ SC with 4 vCPUs: 5,000	-	20,000	▪ 2 GB: 100 ▪ 3 GB: 500 ▪ 4 GB: 5,000 ▪ 8-16 GB: 6,000 ▪ 32 GB: 16,000 ▪ 64 GB: 25,000	100

Note:

- Using the approved Mediant SE server specifications with an Intel Xeon Gold 6126 processor. For the specifications, please contact AudioCodes.
- For WebRTC sessions:
  - √ The maximum number of concurrent WebRTC sessions can't be greater 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 will be the lower of these numbers.
  - √ The maximum number of concurrent WebRTC sessions can't be greater than the maximum number of concurrent TLS connections.
- Capacity figures assume that a TLS key size of 2048-bit is used for the WebSocket and DTLS negotiation,
- The capacity figures for SIPRec assume 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 cannot be higher than the number of RTP sessions, as indicated in Table 3-1. Therefore, the actual maximum number of SIPRec sessions per deployment environment will be the lower of these numbers.
- For TLS connections capacity, each registered user is assigned a TLS connection, even if there are no ongoing SIP dialogs or transactions using the same connection.

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

Hardware 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

Hardware 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

Hardware 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

Hardware 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 / 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	
		Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-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	V.150.1				
2 x E1/T1	60/48	-	-	-	-	-	-	-	3/15	2/13	-	190/202
2 x T1	48	-	-	-	-	-	-	√	11	9	-	202
1 x E1/T1 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 4 x BRI	38	-	-	-	-	-	-	-	22	18	-	212
1 x E1 4 x FXS	34	-	-	-	-	-	-	-	26	21	-	216
2 x E1 4 x FXS	64	-	-	-	-	-	-	-	0	0	-	186
4 x BRI 4 x FXS 4 x FXO	16	-	-	-	-	-	-	-	5	4	-	234
8 x BRI 4 x FXS	20	-	-	-	-	-	-	-	1	1	-	230
8 x BRI	16	-	-	-	-	-	-	-	5	4	-	234
12 x FXS	12	-	-	√	-	-	-	√	3	3	-	238
4 x FXS 8 x FXO	12	-	-	√	-	-	-	-	3	3	-	238
8 x FXS 4 x FXO	12	-	-	√	-	-	-	-	3	3	-	238
4 x BRI 4 x FXS	12	-	-	√	-	-	-	-	3	3	-	238
4 x FXS 4 x FXO	8	-	-	-	-	-	-	-	7	5	6	242
	8	-	-	√	-	-	-	-	6	6	-	242
4 x BRI	8	-	-	-	-	-	-	-	7	5	6	242
	8	-	-	√	-	-	-	-	6	6	-	242

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	V.150.1				
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	-	17/15 /14	14/13 /11	-	248/246/ 244
	2/4/6	-	-	√	-	-	-	-	11/10 /8	10/8/ 7	-	248/246/ 244
4 x FXS or 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.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *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	
	Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-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).
- *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.

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 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 4 x FXS	35/29	√	-	-	-	-	25/30	2,025	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 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.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *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		
	8 x E1	16 x E1	32 x E1
Profile 1	240	480	960
Profile 2	240	480	960
Profile 2 + SILK-NB	240	480	960
Profile 2 + AMR-WB	240	480	960
Profile 2 + G.722 / AMR-NB	240	480	960
Profile 2 + SILK-WB	208	416	832
Profile 2 + Opus-NB	240	480	960
Profile 2 + Opus-WB	240	480	960

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		8xE1	16xE1	32xE1	64xE1
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 + SILK-NB	260	525	1,055	2,100
Profile 2	Profile 2 + SILK-NB	245	495	990	1,975
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 + 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 + 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 191. 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 + iLBC	175	575
Profile 2	Profile 2 + iLBC	150	500
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 + SILK-NB	200	600

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Without MPM4**	**With MPM4**
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 191. 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 + iLBC	350	1,150
Profile 2	Profile 2 + iLBC	300	1,000
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 + 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 191. 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 + 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 + 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 + 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 191. 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 191. 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 191. 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
m5.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	4,000	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
DS2_v2	1,200	900
DS3_v2	1,700	1,100
DS4_v2	1,800	1,600

3.3.14.2.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be of the Azure DS2_v2 / DS3_v2 / DS4_v2 virtual machine size. The number of supported transcoding sessions per MC is shown in the following table.

Table 3-33: Transcoding Capacity per MC

Session Coders		DS2_v2		DS3_v2		DS4_v2	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	175	175	575	575	1,175	1,175
Profile 2	Profile 1	100	100	325	300	675	600
Profile 2	Profile 2	75	50	225	200	450	400
Profile 1	Profile 2 + AMR-NB / G.722	100	100	325	300	675	600
Profile 2	Profile 2 + AMR-NB / G.722	75	50	225	200	450	400
Profile 1	Profile 2 + AMR-WB (G.722.2)	25	25	100	100	225	200
Profile 2	Profile 2 + AMR-WB	25	25	75	75	175	175
Profile 1	Profile 2 + SILK-NB	100	75	300	250	600	525
Profile 2	Profile 2 + SILK-NB	50	50	200	175	400	375
Profile 1	Profile 2 + SILK-WB	50	50	175	150	350	325
Profile 2	Profile 2 + SILK-WB	25	25	125	125	275	275
Profile 1	Profile 2 + Opus-NB	50	50	175	175	375	350
Profile 2	Profile 2 + Opus-NB	25	25	125	125	275	275
Profile 1	Profile 2 + Opus-WB	25	25	125	125	275	250
Profile 2	Profile 2 + Opus-WB	25	25	100	100	225	225

3.3.14.3 Mediant CE SBC for VMware

The following tables list maximum transcoding capacity 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 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 + SILK-NB	575	525
Profile 2	Profile 2 + SILK-NB	450	425
Profile 1	Profile 2 + AMR-WB	200	175
Profile 2	Profile 2 + AMR-WB	175	175
Profile 1	Profile 2 + G.722 / AMR-NB	600	525
Profile 2	Profile 2 + G.722 / AMR-NB	475	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

3.3.15 Mediant Virtual Edition (VE) SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 191. 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:
    - VMware ESXi 6.7 or later.
    - 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 3-36: 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 + 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 + AMR-WB	25	25	100	100	125	125	425	400
Profile 2	Profile 2 + AMR-WB	25	25	75	75	125	125	375	375

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 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 + 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

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.

Table 3-37: 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

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
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

Table 3-38: Mediant VE SBC on c5.2xlarge – 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

Table 3-39: Mediant VE SBC on c5.9xlarge - 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

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
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.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to **Optimized for Transcoding** (2).

3.3.15.2.1.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-40: 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 3-41: Mediant VE SBC on DS1_v2, DS2_v2, DS3_ v2 & DS4_v2 - Transcoding Capacity

Session Coders		Max. Sessions					
		DS1_v2 and DS2_v2		DS3_v2		DS4_v2	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	200	200	625	600	1,025	1,025
Profile 2	Profile 1	100	100	350	325	600	525
Profile 2	Profile 2	75	50	225	200	400	350
Profile 1	Profile 2 + AMR-NB / G.722	100	100	350	300	600	525
Profile 2	Profile 2 + AMR-NB / G.722	75	50	225	200	400	350
Profile 1	Profile 2 + AMR-WB (G.722.2)	25	25	100	100	200	175
Profile 2	Profile 2 + AMR-WB	25	25	100	75	175	150
Profile 1	Profile 2 + SILK-NB	100	75	300	275	525	475
Profile 2	Profile 2 + SILK-NB	50	50	200	200	350	325
Profile 1	Profile 2 + SILK-WB	50	50	175	175	300	300
Profile 2	Profile 2 + SILK-WB	50	25	150	125	250	225
Profile 1	Profile 2 + Opus-NB	50	50	200	175	325	300
Profile 2	Profile 2 + Opus-NB	50	50	150	150	250	250
Profile 1	Profile 2 + Opus-WB	50	25	150	125	250	225
Profile 2	Profile 2 + Opus-WB	25	25	125	100	200	200

Note: 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 191. 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 3-42: 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.

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 3-43: 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 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Access List	50	50	50	50
Accounts	102 (1,500 for Mediant 3100)	625	1,500	1,500
Allowed Audio Coders Groups	10 (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 (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	▪ 64: MP-1288 / Mediant 1000/3100 ▪ 100: Mediant 500/500L/800	400	1,000	▪ 2-8 GB: 500 ▪ 16-64 GB: 1,000
Calling Name Manipulation for IP-to-Tel Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Calling Name Manipulation for Tel-to-IP Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Char Conversion	40	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Charge Codes	25	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Classification	102 (1,500 for Mediant 3100)	1,500	1,500	▪ 2 GB: 750 ▪ 3.5-64 GB: 1,500
Coder Groups	11 (21 for Mediant 3100)	21	21	21
Cost Groups	10	10	10	10
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)

Configuration Table	Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
DHCP Servers	1	1	1	1
Dial Plan	10 (25 for Mediant 3100)	25	50	50
Dial Plan Rule	2,000 (10,000 for Mediant 3100)	10,000	100,000	▪ < 16 GB: 2,000 ▪ > 16 GB: 100,000
Ethernet Devices	16 (1,024 for Mediant 3100)	1,024	1,024	1,024
External Media Source	1	1	1	1
Firewall	50 (500 for Mediant 3100)	500	500	500
Forward On Busy Trunk Destination	▪ 288: MP-1288 ▪ 100: Mediant 500/500L/800 ▪ 240: Mediant 1000 ▪ 512: Mediant 3100	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 ▪ ≥ 8 GB: 120
HTTP Proxy Servers	10	10	40	▪ < 8 GB: 10 ▪ ≥ 8 GB: 40
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 (3,000 for Mediant 3100)	3,000	3,000	3,000
Internal DNS	20	20	20	20
Internal SRV	10	10	10	10
IP Group Set	51 (350 for Mediant 3100)	350	2,500	▪ 2 GB: 40 ▪ 3.5 GB: 500 ▪ 4-16 GB: 750 ▪ 32-64 GB: 2,500
IP Groups	80 (700 for Mediant 3100)	700	5,000	▪ 2 GB: 80 ▪ 3.5 GB: 1,000

Configuration Table	Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
				▪ 4-16 GB: 1,500 ▪ 32-64 GB: 5,000
IP Interfaces	16 1,024 (Mediant 3100)	1,024	1,024	1,024
IP Profiles	▪ 20: MP-1288 / Mediant 500/500L/800 ▪ 40: Mediant 1000 ▪ 300: Mediant 3100	300	300 (Mediant 9030); 1,500 (Mediant 9000/9080/SE)	▪ 2 GB: 150 ▪ 5-32 GB: 300 ▪ 64 GB: 1,500
IP-to-IP Routing	615 (9,000 for Mediant 3100)	9,000	9,000	▪ 2 GB: 4,500 ▪ 3.5-64 GB: 9,000
IP-to-Tel Routing	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
LDAP Server Groups	41 (600 for Mediant 3100)	600	600	600
LDAP Servers	82 (1,200 for Mediant 3100)	1,200	1,200	1,200
Local Users	20	20	20	20
Logging Filters	60	60	60	60
Login OAuth Servers	1	1	1	1
Malicious Signature	20	20	20	20
Media Realm Extension	▪ 2 x Max. Media Realms: MP-1288 / Mediant 500/500L/800 ▪ 5 x Max. Media Realms: Mediant 3100	2 x Max. Media Realms (Mediant 2600) 5 x Max. Media Realms (Mediant 4000B)	5 x Max. Media Realms	5 x Max. Media Realms
Media Realms	12 (1,024 for Mediant 3100)	1,024	1,024	1,024
Message Conditions	82 (1,200 for Mediant 3100)	1,200	1,200	1,200
Message Manipulations	▪ 100: MP-1288 / Mediant 500/500L/800 ▪ 200: Mediant 1000 ▪ 500: Mediant 3100	500	500	500
Message Policies	20	20	20	20
NAT Translation	32	32	32	32
OAuth Servers	1	1	1	1
Outbound Manipulations	205 (3,000 for Mediant 3100)	3,000	3,000	3,000
OVOC Services	1	1	1	1

Configuration Table	Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Phone Contexts	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Pre-Parsing Manipulation Rules	30	30	30	30
Pre-Parsing Manipulation Sets	10	10	10	10
Proxy Sets	80 (700 for Mediant 3100)	700	5,000	▪ 2 GB: 80 ▪ 3.5 GB: 1,000 ▪ 4-16 GB: 1,500 ▪ 32-64 GB: 5,000
Proxy Sets > Proxy Address (Rows)	10	10	50	▪ 2 GB: 10 ▪ 3.5 GB: 10 ▪ 8-16 GB: 10 ▪ 32-64 GB: 50
Proxy Sets > Proxy Address (DNS-resolved IP addresses)	15	15	50	▪ 2 GB: 15 ▪ 3.5 GB: 15 ▪ 8-16 GB: 50 ▪ 32-64 GB: 50
Proxy Sets > Proxy Address (Total DNS-resolved IP addresses for all Proxy Sets combined)	160	1,400	10,000	▪ 2 GB: 160 ▪ 3.5 GB: 2,000 ▪ 4 GB: 3,000 ▪ 8-16 GB: 3,000 ▪ 32-64 GB: 10,000
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 (3,500 for Mediant 3100)	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)

Configuration Table	Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
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
Remote Web Services	7	7	7	7
Routing Policies (SBC)	20 (600 for Mediant 3100)	600	600	▪ 2 GB: 20 ▪ 3.5 GB: 70 ▪ 4 GB: 100 ▪ 8 GB: 200 ▪ 16 GB: 400 ▪ 32-64 GB: 600
Routing Policies (Gateway)	1	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
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 ▪ Mediant 500L/800: 2,000 ▪ Mediant 1000: 800 ▪ Mediant 3100: 20,000 ▪ MP-1288: 350	20,000	50,000	▪ 2 GB: 1,000 ▪ 3 GB: 3,000 ▪ 4 GB: 3,000 ▪ 8 GB: 20,000 ▪ 16-64 GB: 20,000
SIP Interfaces	80 (1,200 for Mediant 3100)	700	1,200	▪ 2 GB: 40 ▪ 3 GB: 200 ▪ 4 GB: 400 ▪ 8 GB: 800 ▪ 16 GB: 1,200 ▪ 32-64 GB: 1,200
SIP Recording Rules	30	30	30	30
SNI-to-TLS Mapping	12 (15 for Mediant 1000; 100 for Mediant 3100)	100	100	100
SNMP Trap Destinations	5	5	5	5
SNMP Trusted Managers	5	5	5	5
SNMPv3 Users	10	10	10	10
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)

Configuration Table	Mediant 500 / 500L / 800 / 1000B / 3100 MP-1288	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
SRDs	20 (600 for Mediant 3100)	600	600	▪ 2 GB: 20 ▪ 3.5 GB: 70 ▪ 4 GB: 100 ▪ 8 GB: 200 ▪ 16 GB: 400 ▪ 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 (40 for Mediant 3100)	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	▪ 12: MP-1288 / Mediant 500/500L/800 ▪ 15: Mediant 1000 ▪ 100: Mediant 3100	100	100	100
Tone Index	50	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Trunk Group	▪ 288: MP-1288 ▪ 24: Mediant 500/500L/800 ▪ 240: Mediant 1000 ▪ 512: Mediant 3100	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Trunk Group Settings	▪ 289: MP-1288 ▪ 101: Mediant 500/500L/800 ▪ 241: Mediant 1000 ▪ 512: Mediant 3100	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
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)
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 (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. 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. 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
Naimi Park
6 Ofra Haza Street
Or Yehuda, 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-27721