Release Notes

AudioCodes SBC and Media Gateway Series

Session Border Controllers Analog & Digital Media Gateways

Long Term Support (LTS) Releases

Version 7.2

audiocodes

Table of Contents

List of Tables

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: June-09-2024

Security Vulnerabilities

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

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

Related Documentation

Document Name
Mediant 500L Gateway and E-SBC Hardware Installation Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 500 E-SBC Hardware Installation Manual
Mediant 500 E-SBC User's Manual
Mediant 800 Gateway and E-SBC Hardware Installation Manual
Mediant 800 Gateway and E-SBC User's Manual
Mediant 1000B Gateway and E-SBC Hardware Installation Manual
Mediant 1000B Gateway and E-SBC User's Manual
MP-1288 Hardware Installation Manual
MP-1288 High-Density Analog Media Gateway User's 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 9000 SBC Hardware Installation Manual
Mediant SE SBC Installation Manual
Mediant Virtual Edition SBC Installation Manual
Mediant Virtual Edition SBC for Microsoft Azure Installation Manual
Mediant Virtual Edition SBC for Amazon AWS Installation Manual
Mediant VE SBC for Amazon Chime Voice Connector Installation Manual
Mediant CE SBC Installation Manual
Stack Manager for Mediant CE SBC User's Manual
Mediant Software SBC User's Manual

Document Revision Record

LTRT	Description
27726	Ver. 7.20A.259.392
27716	SRTP capacity update for Mediant 800C
27713	Ver. 7.20A.259.39
27709	MSRP capacity
27698	Ver. 7.20A.259.382
27693	Ver. 7.20A.259.366
27677	Ver. 7.20A.259.352
27668	Ver. 7.20A.259.339
27655	Ver. 7.20A.259.327
27650	Capacity of Proxy Sets table updated
27645	Ver. 7.20A.259.306; constraint SBC-25588 added to Ver. 7.20A.258.354
27640	Ver. 7.20A.259.280
27631	Ver. 7.20A.259.249; Access List table capacity; USA address and trademark
27624	Ver. 7.20A.259.221
27623	Ver. 7.20A.259.183
27597	Ver. 7.20A.259.134
27583	Ver. 7.20A.258.920
27580	Ver. 7.20A.258.919

LTRT	Description
27577	Ver. 7.20A.258.882
27569	Ver. 7.20A.258.826 (instead of 7.20A.258.825)
27558	Ver. 7.20A.258.750
27551	Ver. 7.20A.258.661
27545	Ver. 7.20A.258.559; Malicious Signature table capacity increased
27540	Typo (Mediant 800A removed); CRMX module feature added to 7.20A.258.354.
27535	Ver. 7.20A.258.459
27533	NGINX Ver. Added.
27532	Ver. 7.20A.258.457.
27527	Ver. 7.20A.258.367; update to feature re X-MS-SBC header support; SBC-21292 constraint added
27523	Ver. 7.20A.258.363.
27520	Typo; resolved constraint SBC-25559 added.
27519	Ver. 7.20A.258.354; capacity updated for Mediant 800C hybrid; typo (DS1_v1)
27506	On-Demand SIP-based Recording removed; MCProfile parameter added to Section Mediant CE SBC for VMware
27499	Updated with Ver. 7.20A.258.271
27494	Resolved constraints SBC-23125 and SBC-23148 added; Capacity per Feature updated
27493	Updated with Ver. 7.20A.258.246
27488	Note added re 7.20A.258.xxx vs 7.20A.256.725; max. SIPREC capacity for Mediant 500; WebRTC max. registered users for Mediant VE.
27484	Document becomes LTS for 7.2.0A.258.xxx (LR document created for 7.20A.260.xxx).
27483	Updated with Ver. 7.20A.258.119.
27478	Updated with Ver. 7.20A.258.010 and Ver. 7.20A.260.007; description updated for CDR Customization for Adding SIP Header Information; Mediant 800C Gateway capacity updated; OVOC and WebSocket note
27476	Updated with Ver. 7.20A.260.005.
27473	Updated with Ver. 7.20A.258.007; On-Demand SIP-Based Media Recording added to 7.20A.258.006; Mediant 4000 added to Feature Capacity table
27472	Typo fixed for SBC-19284.
27471	Updated with Ver. 7.20A.258.006.
27470	Updated with Ver. 7.20A.256.725.
27466	Capacity updated in Table 3-49 (Mediant SE based on DL360 Gen10).
27464	Updated with Ver. 7.20A.256.721; SSLv3 note added and 4096 DH key size removed for Ver. 7.20A.256.713.
27461	Updated with Ver. 7.20A.256.715 (applicable only to Mediant 2600, Mediant 4000/B, Mediant 90xx, and Mediant Software).
27460	Updated with Ver. 7.20A.256.713.

LTRT	Description
27459	OVOC note re WebSocket support; IP Group Set table capacity updated.
27455	Updated with Ver. 7.20A.256.511.
27452	Updated with Ver. 7.20A.256.399; Flex License feature description updated.
27450	Updated with Ver. 7.20A.256.366.
27448	Updated with Ver. 7.20A.256.024.
27444	Updated with Ver. 7.20A.254.565; SIP MESSAGE method added to supported SIP methods table.
27441	Updated with Ver. 7.20A.254.475.
27397	Updated with Ver. 7.20A.254.376; SBC-12847 added to Ver. 7.20A.252.011 as resolved constraint; SBC-15627 added to Ver. 7.20A.250.003 as known constraint; trademarks updated.
27396	Initial dedicated document for Latest Release (LR) versions for 7.2.

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 of Release 7.2 for AudioCodes' session border controllers (SBC) and media gateways.

Note:

- As the last decimal group ("*" – representing the minor build) of software version *7.20A.256.** has almost reached maximum capacity, from Version 7.20A.256.725, the software version numbering has been changed to *7.20A.**258.***. Version 7.20A.258.* is a minor version based on Version 7.20A.256.725. Version 7.20A.258.* includes the same content and functionality as 7.20A.256.725 (with the bug fixes listed in this document).
- For previous LTS versions (Version **7.20A.204.***), refer to *LTRT-27482 SBC-Gateway Series Release Notes for Long Term Support Versions 7.2*, which can be obtained from AudioCodes Support.
- 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 version on AudioCodes website at https://www.audiocodes.com/library/technical-documents.

1.1 Software Revision Record

The following table lists the LTS versions of Release 7.2.

Note: The latest software versions can be downloaded from AudioCodes' Services Portal (registered Customers only) at https://services.audiocodes.com.

Table 1-1: Software Revision Record of LTS Versions

LTS Software Version	Release Date
7.20A.259.392 (7.2.258-23)	June 9, 2024
7.20A.259.390 (7.2.258-22)	March 13, 2024
7.20A.259.382 (7.2.258-21)	December 3, 2023
7.20A.259.366 (7.2.258-20)	October 16, 2023
7.20A.259.352 (7.2.258-19)	July 9, 2023
7.20A.259.339 (7.2.258-18)	May 23, 2023
7.20A.259.327 (7.2.258-17)	March 16, 2023

LTS Software Version	Release Date
7.20A.259.306 (7.2.258-16)	January 17, 2023
7.20A.259.249 (7.2.258-15)	November 22, 2022
7.20A.259.280 (7.2.258-14)	September 28, 2022
7.20A.259.221 (7.2.258-13)	July 6, 2022
7.20A.259.183 (7.2.258-12)	May 25, 2022
7.20A.259.134 (7.2.258-11)	April 12, 2022
7.20A.258.920 (7.2.258-10.1)	January 30, 2022
7.20A.258.919 (7.2.258-10)	January 25, 2022
7.20A.258.882 (7.2.258-9)	December 15, 2021
7.20A.258.826 (7.2.258-8)	October 28, 2021
7.20A.258.750 (7.2.258-7)	August 15, 2021
7.20A.258.661 (7.2.258-6)	June 15, 2021
7.20A.258.559 (7.2.258-5)	April 20, 2021
7.20A.258.459 (7.2.258-4-1)	March 2, 2021
7.20A.258.457 (7.2.258-4)	February 17, 2021
7.20A.258.367 (7.2.258-3.2)	January 11, 2021
7.20A.258.363 (7.2.258-3.1)	December 28, 2020
7.20A.258.354 (7.2.258-3)	December 17, 2020
7.20A.258.271 (7.2.258-2.2)	November 5, 2020
7.20A.258.246	October 25, 2020
7.20A.258.119 (initial LTS version)	August 3, 2020
Previous LR Versions	
7.20A.258.010	July 20, 2020
7.20A.258.006	June 9, 2020
7.20A.256.725	May 14, 2020
7.20A.256.721	April 5, 2020
7.20A.256.715[1]	March 31, 2020
7.20A.256.713	March 30, 2020
7.20A.256.511	February 25, 2020
7.20A.256.399	February 17, 2020
7.20A.256.366	February 3, 2020
7.20A.256.024	January 8, 2020
7.20A.254.565	November 27, 2019
7.20A.254.475	November 4, 2019
7.20A.254.376	October 7, 2019

[1] Applicable only to Mediant 2600, Mediant 4000/B, Mediant 90xx, and Mediant Software.

LTS Software Version	Release Date
7.20A.254.375	September 16, 2019
7.20A.254.202	August 6, 2019
7.20A.252.269	June 30, 2019
7.20A.252.261	June 3, 2019
7.20A.252.023	May 20, 2019
7.20A.250.413	May 16, 2019
7.20A.252.011	April 17, 2019
7.20A.250.273	March 25, 2019
7.20A.250.256	February 18, 2019
7.20A.250.003	January 8, 2019

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 7.2

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 Gateways & E-SBC	288/0	-	-	2 GE	1	-
Mediant 2600 E-SBC	-	-	-	8 GE	-	-
Mediant 4000 SBC	-	-	-	8 GE	-	-
Mediant 4000B SBC	-	-	-	8 GE	-	√
Mediant 9030 SBC	-	-	-	12 GE	-	-

Product	Telephony Interfaces			Ethernet Interfaces	USB	OSN
	FXS/FXO	BRI	E1/T1			
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. B and C) ▪ Mediant 1000B 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 7.2.

2.1 Version 7.20A.259.392

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version OVOC 8.2.1382, and OVOC 8.2.3122 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.1.1 Resolved Constraints

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

Table 2-1: Resolved Constraints in Version 7.20A.259.392

Incident	Description
SBC-51977	The device sends a SIP INVITE to the outgoing leg with the incorrect Content-Length header, causing the far side to reject the SDP offer and the call. **Applicable Products:** All

2.2 Version 7.20A.259.390

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version OVOC 8.2.1382, and OVOC 8.2.3112 or later.

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

Note: Mediant 90xx and Mediant VE/CE/SE: To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.2.1 Resolved Constraints

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

Table 2-2: Resolved Constraints in Version 7.20A.259.390

Incident	Description
SBC-50937	The device erroneously sends an alarm from the media cluster with bandwidth miscalculation ("Cluster Bandwidth is above 90% utilization"). **Applicable Products:** Mediant VE

2.3 Version 7.20A.259.390

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version OVOC 8.2.1382, and OVOC 8.2.3112 or later.

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

Note: Mediant 90xx and Mediant VE/CE/SE: To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.3.1 Resolved Constraints

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

Table 2-3: Resolved Constraints in Version 7.20A.259.390

Incident	Description
SBC-50937	The device erroneously sends an alarm from the media cluster with bandwidth miscalculation ("Cluster Bandwidth is above 90% utilization"). **Applicable Products:** Mediant VE
SBC-50961	When the device terminates an SDP answer, it fails to match the outgoing SDP offer's security, replying with SRTP instead of RTP and resulting in call failure. **Applicable Products:** All

2.4 Version 7.20A.259.382

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.1382 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.4.1 Resolved Constraints

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

Table 2-4: Resolved Constraints in Version 7.20A.259.382

Incident	Description
SBC-48339	For a DTMF transcoding call of RFC 2833 to Transparent, the device sends DTMFs as RFC 2833 and transparent, creating duplicated DTMFs. **Applicable Products:** All
SBC-49192	Upon an SDP answer termination, the device fails to match the offer's security, and replies with SRTP instead of RTP. As a result, call failure occurs. **Applicable Products:** All
SBC-49221	When a delayed offer SIP UPDATE message is received, the device sends a re-INVITE message with incorrect SDP to the outgoing side that doesn't support UPDATE messages. **Applicable Products:** All

2.5 Version 7.20A.259.366

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.1368 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.5.1 Resolved Constraints

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

Table 2-5: Resolved Constraints in Version 7.20A.259.366

Incident	Description
SBC-47603	One-way voice occurs after a SIP re-INVITE for session expiry because of incorrect device handling of received RTCP packets with an invalid SSRC. **Applicable Products:** All
SBC-48450	The device restarts due to an internal buffer overrun. **Applicable Products:** All
SBC-48926	Call failure occurs due to lack of resources. **Applicable Products:** All
SBC-48964	The device rejects a new SIP INVITE request with the error message “CSeq inconsistency. Expected > 1; Received 1”. **Applicable Products:** All
SBC-49009	After an HA switchover, the device’s configuration is lost. **Applicable Products:** All

2.6 Version 7.20A.259.352

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.280 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.6.1 Resolved Constraints

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

Table 2-6: Resolved Constraints in Version 7.20A.259.352

Incident	Description
SBC-45975	The device resets upon a call flow of two MLPP priority calls to the same endpoint (first call makes the endpoint rings, then second call to the same endpoint while it's still ringing). **Applicable Products:** Gateway
SBC-46097	The device replies with a SIP 488 (Not Acceptable) to a re-INVITE where the SDP's label attribute has flipped (first re-INVITE has 'a=label:x', second re-INVITE has 'a=label:y', and third problematic re-INVITE has 'a= label:x'). As a result, the call disconnects. **Applicable Products:** SBC
SBC-46131	The device restarts in bootup and during HA synchronization when the active device tries to send a large ini. file to the redundant device. **Applicable Products:** HA
SBC-46530	The device's Accounts table setting of 'Registrar Search Mode' to **Avoid Previous Registrar Until Expiry** and the [AccountRegistrarAvoidanceTime] parameter don't function (reregistration is done only for the first rule). As a result, the device reregisters to the incorrect IP address. **Applicable Products:** SBC
SBC-46574	The device loses its TLS certificate after an HA switchover, causing the Web interface to be inaccessible and calls to fail. **Applicable Products:** HA

2.7 Version 7.20A.259.339

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.280 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.7.1 Resolved Constraints

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

Table 2-7: Resolved Constraints in Version 7.20A.259.339

Incident	Description
SBC-43750	The device fails to match an incoming SIP CANCEL request for an SBC-Gateway hybrid call when configured with the [GWDirectRoutePrefix] parameter. As a result, the call fails. **Applicable Products:** Hybrid SBC-Gateway
SBC-44315	The device limits the LDAP search string to 100 characters (instead of 255), discarding everything beyond 100 characters, causing a faulty LDAP query. **Applicable Products:** All
SBC-44395	The device provides incorrect CDR values (duration not equal to 'Release Time' minus 'Connect Time') on long calls (greater than 10 minutes). **Applicable Products:** All
SBC-45451	The device opens a new voice channel (instead of using current channel) upon a SIP re-INVITE containing the label attribute, causing no voice. **Applicable Products:** All

2.8 Version 7.20A.259.327

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.280 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.8.1 Resolved Constraints

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

Table 2-8: Resolved Constraints in Version 7.20A.259.327

Incident	Description
SBC-41628	The device sends the incorrect RTP stream at the start of an AMR-G.711 transcoding call, which results in crosstalk. **Applicable Products:** All
SBC-42165	The device loses connectivity to OVOC (for sending QoE reports) after the server's port changed. **Applicable Products:** All
SBC-43059	The device restarts (error message "Signal 6, Task LIBT"). **Applicable Products:** All
SBC-43141	The device rejects a call due to UDP mediation error, caused by receiving an SDP offer with two application media lines ('m=application'), one with RTP/AVP and the other with UDP/UDT/IX. **Applicable Products:** All
SBC-43666	The device loses connectivity to the routing server (ARM) due to session ID mismatch between the getRoute request and response. **Applicable Products:** All
SBC-43792	The device rejects a call when receiving a SIP UPDATE message containing SDP from the calling side, before receiving ACK from the calling side. **Applicable Products:** All
SBC-43823 SBC-43964	The device repeatedly resets when OVOC (for QoE reporting) is configured with an FQDN address and the DNS fails to resolve it. **Applicable Products:** All

Incident	Description
SBC-44280	The device requires DSP resources when the SDP answer contains the 'a=label:' attribute. Call failure occurs if the device has no DSP resources. **Applicable Products:** All

2.9 Version 7.20A.259.306

This version includes known and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.280 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.9.1 Known Constraints

This section lists known constraints.

Table 2-9: Known Constraints in Version 7.20A.259.306

Incident	Description

SBC-42036	The default value of the 'Use Specific Interface' parameter in the Firewall table was changed from **Disable** to **Enable**. As a result, Customers using CLI scripts for configuring this table must modify the script to explicitly specify the value for this parameter:
	`configure network`
	`  access-list <index>`
	`  use-specific-interface disable`

2.9.2 Resolved Constraints

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

Table 2-10: Resolved Constraints in Version 7.20A.259.306

Incident	Description
SBC-42104	The device fails to send a DNS query after running out of cache memory, causing the proxy server to be considered as offline. **Applicable Products:** All
SBC-42239	The 'User Security Mode' parameters (SRD_BlockUnRegUsers or SIPInterface_BlockUnRegUsers) also affects IP Groups of type "Gateway" (should only affect IP Groups of type 'User'). **Applicable Products:** All
SBC-42287	The device deletes the timer capabilities (for session refreshes) when initiating a SIP re-INVITE or UPDATE request for media sync, causing call disconnection. **Applicable Products:** All
SBC-42294	The device fails to send the snmpEngineID and MAC address to OVOC when configured with SNMPv3. **Applicable Products:** All
SBC-42552	The device replaces its crypto keys between the outgoing SIP 18x and outgoing 200 OK, even though it's configured not to. As a result, call failure occurs (no audio). **Applicable Products:** All

2.10 Version 7.20A.259.280

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.2.280 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.10.1 Resolved Constraints

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

Table 2-11: Resolved Constraints in Version 7.20A.259.280

Incident	Description
SBC-39600	The output of the CLI command `show network physical-port` displays the status of the active/redundant instead of active/active for the Ethernet Group configured with 2RX/2TX. **Applicable Products:** MP-1288
SBC-39610	The device fails to perform a call transfer to a busy endpoint, causing one-way voice, because reopening a channel from a state of no DSP to with DSP fails if no RTP is sent in between. **Applicable Products:** All
SBC-39886	The device has sporadic cross talk noises in some calls that use DSP because of an internal bug regarding DSPs. **Applicable Products:** All
SBC-40430 SBC-41672	The device resets after failing to recover from a wrong resource allocation and deletion of a TLS connection with OVOC. **Applicable Products:** All
SBC-40501	A few seconds of voice issues (sporadic poor voice quality) are observed at the beginning of a conference call, caused by the replay of SRTP packets when the channel is reopened. **Applicable Products:** MP-1288
SBC-41392	The device receives an SDP offer with 'm=audio' (SRTP) and 'm=x-data' (SRTP) from the incoming leg, causing it to send an SDP offer with 'm=audio' (RTP) and wrong 'm=x-data' (no RTP or SRTP - only space between port and coders). **Applicable Products:** All
SBC-41433	The 'Account Registration Status' table on the Web interface's Registration Status page doesn't display information in the 'Group Name' field. **Applicable Products:** All
SBC-41574	The device fails to reconnect to ARM (if, for example, connection to ARM is lost) due to wrong internal state machine and gets stacked in re-connecting state. **Applicable Products:** All

2.11 Version 7.20A.259.249

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3180 and EMS/SEM Version 7.2.3113 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.11.1 Resolved Constraints

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

Table 2-12: Resolved Constraints in Version 7.20A.259.249

Incident	Description
SBC-36025	The device fails to perform message manipulation that adds a new (unknown) SIP header, generating the syslog error "!! [ERROR] Failed to allocate new Unknown Header". **Applicable Products:** All
SBC-37554	Onboard three-way conferencing has no voice for one of the parties. **Applicable Products:** MP-1288
SBC-38434	The device experiencing an overload for task "SPLB" when handling many SIP SUBSCIBE messages over TLS for registration, resulting in registration failure. **Applicable Products:** All
SBC-38661	The device resets with task "MDI1" due to media optimization failure. **Applicable Products:** All
SBC-38778	The device doesn't include Progress Indication and Location in the Disconnect message to the PSTN. **Applicable Products:** Gateway
SBC-38846 SBC-39178 SBC-39256 SBC-39556 SBC-40071	LDAP-based login authentication fails after the device is upgraded to 7.20A.259.221. **Applicable Products:** All
SBC-39120	After a reset, the device sends a SIP SUBSCRIBE message before trunk registration process is complete. **Applicable Products:** All

Incident	Description
SBC-39128	The device doesn't clear the Proxy Set offline alarm when using REGISTER messages for Proxy Set keep-alive. **Applicable Products:** All
SBC-39285	The device fails to handle SIP INVITE messages with Replaces after receiving a 491 for a re-INVITE, resulting in call transfer failure. **Applicable Products:** All
SBC-39366	The device resets upon receipt of an LDAP response after a 10s delay. **Applicable Products:** All
SBC-39491	The device's CSR, when containing more than one SAN, has the wrong format (missing comma separation), resulting in certificate signing failure. **Applicable Products:** All
SBC-39772	Upon the receipt of a SIP 408 from the main proxy for REGISTER, the device doesn't send a REGISTER to the second proxy, resulting in alternative routing failure. **Applicable Products:** All
SBC-40088 SBC-40447 SBC-40514 SBC-40631	The device loses connectivity with OVOC (CLM) a few minutes after reset (and therefore, Floating License is no longer functional). **Applicable Products:** All
SBC-40181	When configured with Sticky Primary, the device fails to route calls to the second ARM router. **Applicable Products:** All
SBC-40183	The device resets when trying to configure a new control LDAP server (in addition to the existing one) **Applicable Products:** All

2.12 Version 7.20A.259.221

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3180 and EMS/SEM Version 7.2.3113 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.12.1 Resolved Constraints

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

Table 2-13: Resolved Constraints in Version 7.20A.259.221

Incident	Description
SBC-38257	The Web interface users with Administrator level can't edit the Caller Display Information table. **Applicable Products:** All
SBC-38175	Security vulnerability in the device's NGINX proxy (displays server's name and version in 404 responses). **Applicable Products:** All
SBC-37961	The device fails to downgrade from 7.2.258 to 7.2.256 because of a hardware mismatch (CRMX module). **Applicable Products:** All
SBC-37795	The device fails to mark a user as located behind NAT upon registration when the user appears in the User Information table. This causes the call routing to failure. **Applicable Products:** All
SBC-37729	The device resets when forking calls and the routing is based on destination tags (forked call have no destination tags). **Applicable Products:** All
SBC-37710	The device fails to perform a Call Setup Rule through an HTTP server because the server is erroneously marked as offline. As a result, calls fail. **Applicable Products:** All
SBC-37632	LDAP-based Web user authentication sometimes fails. **Applicable Products:** All
SBC-37490	The CLI command `copy <File> from` fails with a timeout. **Applicable Products:** All
SBC-37488	The device's Least Cost Routing feature (LCR) fails when configuring a Sunday time band that does not start on "SUN:00:00". **Applicable Products:** All
SBC-37353	The device sends a SIP 200 OK for a fax re-INVITE without the connection line 'c=' in the SDP for a specific call scenario. **Applicable Products:** All
SBC-37349	The device's ELIN callback number is not translated back to the caller's number when the user part of the SIP Request-URI contains 'phone-context=’. **Applicable Products:** All
SBC-37299	The device sends calls to ARM even though it's in Locked state (calls fail). **Applicable Products:** All
SBC-37043	The device stops sending call reports to OVOC (for Call History) because of a resource leak. **Applicable Products:** All

Incident	Description
SBC-35868	The device reports a false alarm for high temperature (acBoardTemperatureAlarm) and even if the alarm is manually cleared it appears again after some time. **Applicable Products:** Mediant 4000

2.13 Version 7.20A.259.183

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3180 and EMS/SEM Version 7.2.3113 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.13.1 Resolved Constraints

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

Table 2-14: Resolved Constraints in Version 7.20A.259.183

Incident	Description
SBC-34889	The device fails to save DNS results in its cache and therefore, needs to repeat DNS queries. **Applicable Products:** All
SBC-35542	The device's Media Realm ports resources are not properly released during a specific call flow scenario. **Applicable Products:** All
SBC-35969	The SIP Subject header is limited to 49 characters and the device truncates all characters exceeding this number. **Applicable Products:** All
SBC-36227	The device doesn't send SIP SUBSCRIBE messages to the MWI server and requires a reset for applying the EnableMWISubscription parameter. **Applicable Products:** Gateway
SBC-36324	The device sometimes fails to connect over TLS to the OVOC Floating License pool after upgrading to Version 7.2.258.920. **Applicable Products:** All
SBC-36407	The device sends a SIP SUBSCRIBE message to the MWI server before sending it a SIP REGISTER (should send REGISTER before SUBSCRIBE). **Applicable Products:** Gateway
SBC-36416	The device fails to activate the DND (do not disturb) feature if the activation code (KeyCFDoNotDisturb parameter) contains an asterisk (*). **Applicable Products:** Gateway

Incident	Description
SBC-36524	The device performs an HA switchover with the error message "Signal 901, Task LIBT" (and then resets) in case of active-redundant resource mismatches. **Applicable Products:** HA
SBC-36553	The IP Profile parameter IpProfile_EnableSymmetricMKI doesn't affect SIP re-INVITE sessions, sometimes adding the MKI size when the far side sends an SDP offer without MKI, causing one-way voice. **Applicable Products:** All
SBC-36674	Message Manipulation on re-INVITE responses doesn't function when interworking between re-INVITE and UPDATE SIP messages. **Applicable Products:** All
SBC-36677	The device rejects an incoming call because of a Session ID mismatch from ARM. **Applicable Products:** All
SBC-36685	The device rejects registration requests because of a resource overflow (SIPSBCRegisterLegMembers). **Applicable Products:** All
SBC-36848	The device accepts calls after performing an HA switchover in Locked state (instead of rejecting calls in this state). **Applicable Products:** HA
SBC-36875	The device issues a warning message that it can't receive RFC-2198 with payload type 63 because its range is 96 to 128. As a result, the WebRTC call fails. **Applicable Products:** All
SBC-37066	The device fails to do Message Manipulation on SIP 100 (Trying) messages when configured with ARM. **Applicable Products:** All
SBC-37087 SBC-37091 SBC-37092	The device receives an SDP video offer with 'a=recvonly' and replies with an SDP video answer with 'a=inactive', causing a failure in the video call. **Applicable Products:** All
SBC-37147	The device fails to add a new rule to the Accounts table for an index number that is higher than the maximum allowed IP Groups. **Applicable Products:** All
SBC-37215	The device experiences no voice when receiving a SIP re-INVITE message after an HA switchover. **Applicable Products:** Mediant Software HA (on Azure)
SBC-37244	The device fails to update the Local Users table when uploading a CLI script file. **Applicable Products:** All

2.14 Version 7.20A.259.134

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3137 and EMS/SEM Version 7.2.3113 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.14.1 Resolved Constraints

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

Table 2-15: Resolved Constraints in Version 7.20A.259.134

Incident	Description
SBC-30700 SBC-31594 SBC-33797	One-way voice on calls occurs where channels are opened without DSP and there are different multiple coders on both sides. **Applicable Products:** All
SBC-33833	The device fails to recover connectivity with the REST server, when the REST server disconnects and when SBC is configured with a non-zero [KeepAliveTimeout] value and without persistent connection. As a result, call failure occurs. **Applicable Products:** All
SBC-33925	The Intrusion Detection System (IDS) mechanism doesn't block the user's IP address for all ports and all transport types. **Applicable Products:** All
SBC-33963	Uploading a CLI Script file that contains both Dial Plan rules and non-Dial Plan rules is successful, but the newly added Dial Plan rules are not matched. As a workaround, load a separate CLI Script file for the Dial Plan only and a separate CLI Script file for the non-Dial Plan configuration.
SBC-34106	The device sends a SIP 200 OK with SDP answer containing a corrupted IPv6 in the candidate attributes (' a=candidate:'), causing call failure. **Applicable Products:** All

Incident	Description
SBC-34416	One-way voice on a specific Teams transfer scenario is experienced: user A calls user B, who blind transfers the call to user C who declines the call, and user B accepts call again, but user A doesn't hear B for a few seconds. The problem is that the call starts with SRTP-to-SRTP RTP mediation, but the device fails to set the call back to SRTP-to-SRTP RTP mediation. **Applicable Products:** All
SBC-34698	The device starts sending DTMF as SIP INFO (instead of RFC 2833) after a re-INVITE adds video to the call. As a result, DTMF failure occurs. **Applicable Products:** All
SBC-34725	The device fails to do transcoding for the EVS coder with "cmr=1", causing poor voice quality. **Applicable Products:** All
SBC-34754	The device's CLI parameter `password-4-auth` is not obscured in the downloaded CLI script, causing a security risk. The parameter has been renamed AuthPassword, in CLI auth-password. (Old parameter [Password] / password-4-auth are obsolete but are backward compatible. **Applicable Products:** All
SBC-35387	The device performs an HA switchover and then resets, generating the error "Signal 901, Task CEMT" due to an internal error committed by an internal process called "ErroHandler". **Applicable Products:** HA
SBC-35480	The device enters a reset loop when configured to operate with DHCP, and generates the error message "Signal 901, Task ROOT" **Applicable Products:** Mediant 1000
SBC-35536 SBC-35754	The device sends an invalid SDP answer (no coders in RTP media line) causing fax failure upon a specific scenario. **Applicable Products:** All
SBC-35739	Logging Filters configured for Debug Recording with User filter type cannot find a match in an ARM environment when ARM performs its own user number manipulation. **Applicable Products:** All
SBC-35870	The device increases its SDP version ('o=') when sending a SIP re-INVITE\UPDATE for session timer, even though SDP was unchanged. **Applicable Products:** All
SBC-35948	The device fails to recover from a crossed network-threshold on the MTC system, where the Signaling Component (SC) is the Mediant Software SBC and the Media Component (MC) is the Mediant 4000 SBC, causing media disconnections (no voice). **Applicable Products:** MTC (Mediant Software with Mediant 4000)
SBC-36031	The device resets upon a Tel-to-IP call with ARM, upon multiple alternative routing failures due to ARM failure. **Applicable Products:** All

2.15 Version 7.20A.258.920

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3106 and EMS/SEM Version 7.2.3113 or later.

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

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

2.15.1 Resolved Constraints

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

Table 2-16: Resolved Constraints in Version 7.20A.258.920

Incident	Description
SBC-34482	Hitless software upgrade from this 7.2 version to a 7.4 version is currently not supported. **Applicable Products:** Mediant Software; Mediant 90xx

2.16 Version 7.20A.258.919

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: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.3106 and EMS/SEM Version 7.2.3113.

Note: **Mediant 90xx and Mediant VE/CE/SE:** To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.

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

2.16.1 New Features

This section describes the new features introduced in this version.

2.16.1.1 Digitally Signed Software Files (.cmp)

The 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 digitally 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.

2.16.2 Known Constraints

This section lists known constraints.

Table 2-17: Known Constraints in Version 7.20A.258.919

Incident	Description
SBC-34482	Hitless software upgrade from this 7.2 version to a 7.4 version is currently not supported. To upgrade to a 7.4 version, refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note. **Applicable Products:** Mediant Software; Mediant 90xx

2.16.3 Resolved Constraints

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

Table 2-18: Resolved Constraints in Version 7.20A.258.919

Incident	Description
SBC-30692	The device's hyper-threading status (enabled / disabled) in the ini file doesn't reflect the actual host's hyper-threading status. **Applicable Products:** Mediant Software
SBC-32700 / SBC-33882	The output of the CLI command `show system utilization` displays high memory utilization. **Applicable Products:** Mediant 2600; Mediant 4000
SBC-32709	The device doesn't send SIP INFO messages upon the detection of the MRD CAS signal from the PSTN side. As a result, the call fails. **Applicable Products:** Gateway
SBC-32937	The device has a security vulnerability allowing it to be loaded with a script when loading a .cmp file using the software upgrade process. **Applicable Products:** All
SBC-33260	The device generates unrelated messages such as "</sbin/tail: '/var/log/messages" through the SMDI serial cable interface, causing SMDI calls to fail. **Applicable Products:** Gateway
SBC-33414	The device fails to upload a License Key to the redundant unit, generating the error message "ComapreTempFKDB: Active and redundant FK are not identical (OptionId=142)" even though they are identical. **Applicable Products:** HA
SBC-34008	The device is disconnected from OVOC (License Pool) after 10 retransmissions failures. **Applicable Products:** All
SBC-34157	The device ignores the Retry-After header when keep-alive is done using SIP REGISTER messages and keeps sending endless REGISTER messages to the proxy. **Applicable Products:** All

Incident	Description
SBC-34173	The device rejects calls, generating the message "[ERROR] ARMSession::ParseGetRouteResult - Session ID mismatch!" after receiving GetRoute replies from ARM. **Applicable Products:** All
SBC-34184	When the Web interface's CDR History table is set to display 50 records, none of the pages under the Core Entity folder are visible. **Applicable Products:** All
SBC-34250	The device generates two false error messages for keep-alive failure: "SIPServer::SendKeepAlive() KeepAlive not set because Previous Keep Alive in progress" and "[ERROR] SIPServer::DispatchQueueEvent - Fail to Resend KeepAlive due to Configuration Error". These messages are generated when one of the hosts in the Proxy Set is resolved into a new IP address and therefore, keep-alive for all the servers in the Proxy Set stops and then restarts. One of the servers whose resolved IP didn't change had an in-progress OPTIONS dialog at the time. Due to not resetting some flag in the object representing this server, the error was printed. **Applicable Products:** All
SBC-34431	The device fails to handle a User-To-User (UUI) header with a value longer than 512B (header is truncated). **Applicable Products:** All

2.17 Version 7.20A.258.882

This version includes only resolved constraints.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.2546 and EMS/SEM Version 7.2.3113.

2.17.1 Resolved Constraints

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

Table 2-19: Resolved Constraints in Version 7.20A.258.882

Incident	Description
SBC-31183	The device replies with a SIP 200 OK response that includes the wrong 'crypto' tag for the Teams re-INVITE message, causing the call to disconnect. **Applicable Products:** All
SBC-31903	The device replies with a SIP 200 OK response that includes the wrong 'crypto' tag for the Teams re-INVITE message, causing one-way voice. **Applicable Products:** All

Incident	Description
SBC-31995	The device fails to apply message manipulation on an outgoing challenged SIP REGISTER request, causing registration to fail. (Resolved by the new parameter, AuthenticatedMessageHandling.) **Applicable Products:** All
SBC-32111	The device's Web interface displays the value of the SNMP community string in plain text, exposing it to security vulnerabilities. **Applicable Products:** All
SBC-32267	The device's REST API `show` command that includes a pipe (e.g., `show run voip | grep "ip-group"`) does not function. **Applicable Products:** All
SBC-32424	Crosstalk occurs due to a DSP bug on transcoding calls (WB to G.711). **Applicable Products:** All
SBC-32425	LDAP server search error occurs due to "acLDAPService Problem ('Cannot allocate request' + '[ERROR] gwLDAPMngr::PerformLDAPQuery query failed due to acLdapService problem')", causing call failure. **Applicable Products:** All
SBC-32507	The device fails to find a match in its registered users database to a SIP REGISTER when the parameter [SBCGRUUMODE] is configured to 0 and the REGISTER's Contact header contains the 'sip.instance' parameter, causing a re-register to be a new REGISTER. This results in registration failure. **Applicable Products:** All
SBC-32619	No audio occurs on calls with the next port allocation and the following error messages were generated: "Failed to allocated port" and "Failed allocating audio rtp port inside audio entity". **Applicable Products:** All
SBC-32713	The device fails to send the hook-flash signal towards the TDM side for 911 FXO calls, causing a transfer failure for the 911 call. **Applicable Products:** All
SBC-32724	The device's Dial Plan tags cannot include a "+" prefix (or any special character, for example, "."). **Applicable Products:** All
SBC-32888	The device sends the first RTP packet with the wrong sequence number for WebRTC calls when the [EnableDtlsOnMediaPorts] parameter is configured to 1. **Applicable Products:** All
SBC-32983	An Administrator level user can change the [MgmntLDAPGroups_Level] parameter to Security Admin, giving the Administrator user rights like a Security Administrator. **Applicable Products:** All
SBC-33244	IP trace rules that are done by running the device's CmdShell DR command "AddIPTrafficTrace" are deleted after an HA switchover. **Applicable Products:** HA
SBC-33308	When the device uses the Floating License, it ignores OVR capacity licenses in the local License Key, but erroneously issues a warning message indicating that the OVR FK reached the limit of -1 instead of FEU=0. **Applicable Products:** All

2.18 Version 7.20A.258.826

This version includes only new features and resolved constraints.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.2546 and EMS/SEM Version 7.2.3113.

2.18.1 New Features

This section describes the new features introduced in this version.

2.18.1.1 RTP Media Restricted to Single Negotiated Coder

The device can now be configured to allow only media (RTP) packets from a specific SIP UA (according to IP Profile) with the SDP negotiated voice coder / payload type (single coder). All other packets from the UA with any other coder will be dropped. This feature is configured using the *new IP Profile parameter, IpProfile_SBCAllowOnlyNegotiatedPT.*

Applicable Application: SBC.

Applicable Products: All.

2.18.2 Resolved Constraints

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

Table 2-20: Resolved Constraints in Version 7.20A.258.826

Incident	Description
SBC-28690	When trying to upload, through REST API, an incremental CLI Script file containing the `do reload now` command, the device doesn't respond to the REST request before restarting (commands are applied correctly, but no reply sent back to REST API). **Applicable Products:** Gateway / HA
SBC-29354	The device crashes (resets) when a user attempts to access its Web interface over HTTPS while the device is undergoing a reset. **Applicable Products:** All
SBC-30603	When the device is configured to route SIP REGISTER messages from a UA to a server by destination IP address ('Destination Type' is set to Dest Address in the IP-to-IP Routing table), even when the expiry time of the user in the device's registration database has not yet expired, the device sends re-registrations (refreshes) to the destination (instead of terminating them locally). **Applicable Products:** All
SBC-30634	Fax transcoding fails when the far side sends Comfort Noise (CN) packets (due to a DSP bug, whereby it does not ignore CN packets in fax session). **Applicable Products:** All
SBC-30811	The TDM2SBC license miscalculates SBC resources (less than expected). This is because it calculates the resources before TDM is used up. **Applicable Products:** Mediant 5xx; Mediant 800; Mediant 1000

Incident	Description
SBC-31007	Data in the device's ELIN table is cleared upon an HA switchover and as a result, ELIN functionality fails. (A workaround prior to performing an upgrade to this version is to configure E911Gateway to 1.) **Applicable Products:** HA
SBC-31071	Deletion of some Dial Plans causes functionality failure of other (not deleted) Dial Plans. **Applicable Products:** All
SBC-31079	The device fails to handle SIP REFER requests containing the Refer-To header that has the 'tel:' attribute (and not 'sip:'). As a result, call transfer fails. (A workaround is to use SIP message manipulation to replace 'tel:' with 'sip:'.) **Applicable Products:** All
SBC-31113	The device's Telnet port 927 requires a device reset for it to be opened\closed (instead of on the fly). **Applicable Products:** All
SBC-31247	WebRTC calls with Firefox browser fails during the DTLS stage because the device does not respond to the Client Hello message with a Server Hello message. **Applicable Products:** All
SBC-31325 / SBC-31505	The 'Trunk Status Reporting Mode' parameter does not function correctly (device still sends SIP OPTIONS keep-alive messages when trunk is down). **Applicable Products:** Gateway
SBC-31338	The device crashes (resets), printing the exception "Watchdog: Run task TIMB" (internal task running for more than 10 seconds and getting device stuck). **Applicable Products:** All
SBC-31446	The device crashes (resets), printing the exception "Signal 11, Task SPMR" because it tried to resolve a DNS when setting a route to destination IP address 0.0.0.0. **Applicable Products:** All
SBC-31521	The device's NGINX (HTTP reverse proxy server) disconnects HTTPs connections when many (greater than 200) concurrent HTTPS sessions occurs. **Applicable Products:** All
SBC-31593	The device doesn't change the host part of the serving IP Group in the Accounts table (host part of Call-ID header) on the fly (instead, a device reset or un-register-register is required). As a result, user is unregistered. **Applicable Products:** All
SBC-31724	The device doesn't drop G.722 RTP packets when the channel is opened with G.711, because both coders have the same packet size. As a result, no voice is experienced. (Bug resolved by a new IP Profile parameter, IPProfile_*SBCAllowOnlyNegotiatedPT*). **Applicable Products:** All
SBC-31748	The device crashes (resets) when channels are opened with DSP and the device receives RTP with a different packetization time than negotiated (e.g., 10ms or 30ms, instead of 20ms). **Applicable Products:** All

Incident	Description
SBC-31759	The device's Web interface is exposed to security vulnerability Storage XSS (displays confidential information in the pop-up window). **Applicable Products:** All
SBC-31877	The device doesn't maintain the SIP Interface's 'Additional UDP Ports Mode' settings upon an HA switchover, causing call failures. **Applicable Products:** HA
SBC-31912	The Mediant1000DualPowerSupplySupported parameter doesn't report an alarm. **Applicable Products:** Mediant 1000
SBC-31991	The LDAP connection over TLS disconnects when the LDAP server resets and remains "not connected" even though the server is up again. (As a workaround, edit and apply the LDAP settings without changing any values.) **Applicable Products:** All
SBC-32128	The device sends UUIE (User-To-User information element) in the wrong format (decimal even though configured to hex – UserToUserHeaderFormat = 2). As a result, the call fails. **Applicable Products:** All

2.19 Version 7.20A.258.750

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.1122 and EMS/SEM Version 7.2.3113.

Note: **For Mediant 2600/4000/4000B SBC:** CDR local storage is erased when upgrading to this software version or when downgrading from this version to an earlier version. Therefore, it is recommended that you back up (download) the CDR local storage prior to upgrading or downgrading the device.

2.19.1 New Features

This section describes the new features introduced in this version.

2.19.1.1 Synchronization of Multiple SIP Accounts per IMS Specification

Per the IMS specification, the device can now synchronize multiple Accounts that are configured in the Accounts table whose 'Registrar Search Mode' is set to **By IMS Specification**. This feature is enabled by the new global parameter [SyncIMSAccounts].

The first Account (lowest index number) that is configured with 'Registrar Search Mode' to **By IMS Specification** is considered the "primary" Account. All other Accounts with this same setting are considered "secondary" Accounts.

Synchronization between Accounts mainly concerns the registrar server used by the Accounts. All Accounts send all their associated requests (REGISTERS for the Accounts themselves, and calls matched to the Accounts) to the same server. The primary Account is the only one that decides which server to use.

For more information, refer to the *User's Manual*.

Applicable Application: All.

Applicable Products: All.

2.19.2 Resolved Constraints

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

Table 2-21: Resolved Constraints in Version 7.20A.258.750

Incident	Description
SBC-22563	The device performs an HA switchover upon a REST API command that deletes Network Interface and Ethernet Device. **Applicable Products:** HA
SBC-27861	The device sends RTP packets to destination IP address of 0.0.0.0 after an HA switchover. As a result, no voice occurs. **Applicable Products:** All
SBC-28447 / SBC-30003	The device rejects the SDP answer with the "No MetaData index for media" error message. As a result, the call fails. **Applicable Products:** All
SBC-28666	The device uses a random port for the LDAP server connection (instead of a static port) when the LDAP server is configured as a domain name. **Applicable Products:** All
SBC-28962	The device marks the call as "Failed" when receiving a SIP BYE with cause 31 (incorrect CDR). **Applicable Products:** Gateway
SBC-29254	When configured with an SNMPv3 user, the device also allows SNMPv1 and v2 to operate. **Applicable Products:** All
SBC-29334	The device loses account registration when opening the Trunk Group table page and then selecting **13-24** from the 'Trunk Group Index' drop-down list. **Applicable Products:** Mediant 1000
SBC-29336	The Account table Search Mode is configured as IMS Registrar affects the routing only for the specific Account and not for all other Accounts. **Applicable Products:** All
SBC-29438	The device crashes (resets) upon the receipt of a SIP 200 OK in response to an UPDATE message in an early media scenario that includes hold. **Applicable Products:** All
SBC-29470	Calls fail due to a DTLS handshake failure (device sends a fingerprint and setup parameters on media level but receives a reply with fingerprint and setup on session level). **Applicable Products:** All
SBC-29747 / SBC-29892	The device sends a SIP BYE message without a user part as a result of terminating an UPDATE message with a 422 response. **Applicable Products:** All
SBC-29778	The device stops writing CDR files to local storage due to memory overrun that fills all device memory. **Applicable Products:** Mediant 2600/4000
SBC-29820	The device sends a SIP 200 OK in response to a re-INVITE without a refresher (Session-Expiry header). **Applicable Products:** All

Incident	Description
SBC-29856	For the Auto-Update mechanism, the device fails to load the incremental INI file when the IniFileURL parameter is configured with an FQDN. **Applicable Products:** MP-1288
SBC-29870	The device calculates wrong delay (reported to OVOC) for SILK-codec calls. **Applicable Products:** All
SBC-29874	The device does not forward RTCP after SSRC changes, causing call termination from Microsoft Teams. **Applicable Products:** All
SBC-29916	The device resets when configured to remove the SIP Diversion header and add the History-Info header, and then receives an INVITE with two Diversion headers. **Applicable Products:** All
SBC-29944	The device marks all proxies that have the same IP address as offline when receiving ICMP unreachable from one of them. **Applicable Products:** All
SBC-29970	The PSTNAlertTimeout parameter doesn't function when a trunk is configured as Network Side. **Applicable Products:** Gateway
SBC-29972	The device fails to resolve 500 proxies with domain name due to insufficient DNS resolver resources. **Applicable Products:** All
SBC-30030	The device fails to send HTTP REST messages over Call Setup Rules. **Applicable Products:** All
SBC-30061	The device receives an INVITE with an SDP offer that includes TCP and replies with an SDP answer that does not include TCP (instead of rejecting offer). As a result, SDP negotiation fails. **Applicable Products:** All
SBC-30139	The device sends a false minor alarm about not all proxies being online when proxy keep-alive is configured to use SIP OPTIONS on active proxy. **Applicable Products:** All
SBC-30152	The device reports poor call quality to OVOC when one leg is opened transparently, and the other leg is opened with Generate Always or Generate Only If RTP Active (IPProfile_SBCRTCPMode). **Applicable Products:** All
SBC-30154	A Logging Filter rule cannot be added when the user filter contains dashes in the host part. **Applicable Products:** All
SBC-30180	The HA system has CPU Overload alarms from redundant units with spikes of 1's. **Applicable Products:** HA
SBC-30181	The device sends a SIP 404 in response to an OPTIONS message when trunk is down or trunk is all busy (instead of sending a SIP 486 when trunk is full). **Applicable Products:** Gateway
SBC-30193	Pentest vulnerability - DOS on the admin interface causes the device to reset. **Applicable Products:** All

Incident	Description
SBC-30194	Pentest vulnerability - user with Administrator privileges can grant privileges to Security Admin. **Applicable Products:** All
SBC-30299 / SBC-30338	The device uses the same payload type for coder and DTMF, causing no voice. **Applicable Products:** All
SBC-30317	The device sends a CPU Overload alarm caused by NGINX when the server responds with a 401 and the used service line is not configured with user/password (device keeps sending requests). **Applicable Products:** All
SBC-30425	The device resets because of a resource leak caused by a Pre-Recorded Tone (PRT) being stopped during play. **Applicable Products:** All
SBC-30520 / SBC-30740	The device fails to play a RBT to the transferee for a Microsoft LMO transfer scenario, causing the transfer to fail. **Applicable Products:** All
SBC-30632	The device resets upon a Message Manipulation rule for an INVITE on asynchronous Call Flow (source IP Group uses a CSR rule which sends an HTTP request). **Applicable Products:** All
SBC-30633	The device stops sending SIP OPTIONS keep-alive messages to proxy and temporary blocks the IP Group. As a result, calls fail. **Applicable Products:** All
SBC-30691	Tel-to-IP calls fail after upgrade to 7.2.25x when routing a call to IP Group 0 which does not use Proxy Set 0. **Applicable Products:** Gateway
SBC-30699	The device undergoes a reset loop caused by a bug in the SD card. **Applicable Products:** Mediant 2600/4000
SBC-30801	The device fails to latch to its NAT IP address, causing one way voice. **Applicable Products:** All
SBC-30909	The device resets upon an SSH connection. **Applicable Products:** All
SBC-30912	The device sends a SIP BYE over UDP (instead of over TCP) when using a domain name type NAPTR (ProxyDNSQueryMode) with port upon an SSH connection. As a result, the call fails. **Applicable Products:** All
SBC-31019	For Dial Plans, the wildcard "n" matches any character (instead of only 2 to 9). **Applicable Products:** All
SBC-31074	The device's Message Manipulation on re-INVITE does not apply to re-INVITE in response to 491 responses. **Applicable Products:** All

2.20 Version 7.20A.258.661

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.1122 and EMS/SEM Version 7.2.3113.

2.20.1 New Features

This section describes the new features introduced in this version.

2.20.1.1 OpenSSL Updated to Version 1.1.1k

OpenSSL implemented in AudioCodes devices for secure communication using TLS has been upgraded to OpenSSL Version 1.1.1k.

Applicable Application: All.

Applicable Products: All.

2.20.1.2 Termination of SIP OPTIONS Messages

The device can be configured to terminate incoming in-dialog SIP OPTIONS messages (default) or forward them to the outbound leg. This feature is configured by the new global parameter 'Terminate Inbound OPTIONS' (SBCTerminateOPTIONS).

Applicable Application: SBC.

Applicable Products: All.

2.20.1.3 Body Header Manipulation on SIP Messages with Multipart Bodies

The device can now be configured to manipulate (add, modify, or remove) any header preceding a body part in a multipart body of a SIP message. Up to three headers can be added, removed, or modified per body part.

This feature is supported by the following new message manipulation syntax:

```
body.<body part name from Content-Type header>.header.<header to manipulate>
```

Up until now, only the Content-Type and Content-Disposition headers preceding a body part could be manipulated.

Applicable Application: All.

Applicable Products: All.

2.20.1.4 Mediant VE and CE Support for Gen3 Xeon-SP (Code-named "Ice Lake-SP")

The virtual SBCs (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 the Mediant VE or CE SBCs.

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

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.20.1.5 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 LTS software version (7.20A.258.661) or later. Earlier software versions are not compatible with the new hardware revision. Support for the new hardware revision will also be added to the 7.2 LR and 7.4 software version streams.

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

2.20.2 Resolved Constraints

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

Table 2-22: Resolved Constraints in Version 7.20A.258.661

Incident	Description
SBC-26365	The device doesn't include SNMP V3 login attempts in the syslog in cases of authentication failure. **Applicable Products:** All
SBC-27022	The device loses the Floating License Pool connection with OVOC upon a reset. **Applicable Products:** All
SBC-27145	The device fails to handle a race condition between a SIP REFER and a re-INVITE message that has a domain name in the Record-Route header, and replies with a 200 OK without an SDP response to the re-INVITE. As a result, call transfer fails. **Applicable Products:** All
SBC-27177	The Welcome message (configured by WelcomeMessage) doesn't function properly (order of login and welcome banner) for SSH sessions. **Applicable Products:** All
SBC-27531	The device's Message Manipulation feature fails to add the SIP Content-Disposition and Content-ID headers to the XML body. **Applicable Products:** All
SBC-27856	The device's AWS PAYG drop-down list box for the 'Metering Interface Name' parameter is empty even though the Interface table in the ini file contains the name for eth0. As a result, metering fails. **Applicable Products:** Mediant Software (AWS)
SBC-27858	When the device receives a SIP REFER with Replaces before it receives an ACK in a call transfer scenario, it fails to send an ACK for the 200 OK response. As a result, the transfer fails. **Applicable Products:** All
SBC-27900	The device erroneously prints “VQMON_DIVIDE” errors in the Syslog for long duration calls. **Applicable Products:** All
SBC-28021	The device deployed on Azure remains with the old tag after updating the Dial Plan rule through CLI. **Applicable Products:** Mediant Software (Azure)
SBC-28055	The device fails to handle SIP 3xx messages on forking calls and as a result, call forking fails. **Applicable Products:** All
SBC-28061	The device's Classification process fails due to a resolved IP address that belongs to a secondary domain name and not a primary domain name. **Applicable Products:** All
SBC-28083	The device disconnects calls upon an HA switchover when receiving a request with the same CSeq as the previous CSeq before the switchover. **Applicable Products:** HA

Incident	Description
SBC-28101	WebRTC calls with a specific agent fails due to the device sending RTCP packets with the wrong payload type. **Applicable Products:** All
SBC-28112	The device routes SIP NOTIFY requests to the wrong destination when the SIP dialog was not initiated by the SIP INVITE. **Applicable Products:** All
SBC-28146	The device resets due to a memory override caused by connection attempts between it and OVOC. **Applicable Products:** All
SBC-28181	The device erroneously marks Static Route rules and Firewall rules as invalid after they are loaded from the ini file. **Applicable Products:** All
SBC-28191	If the device receives a SIP INVITE with a user-to-user header containing a bad UTF-8 format, it sends a GetRoute to ARM with the corrupted user-to-user data. **Applicable Products:** All
SBC-28299	The device erroneously sends a minor alarm when one of the SIP proxies is down because of a keep-alive mode that is Using OPTIONS on Active Server. **Applicable Products:** All
SBC-28440	The device sends silence RTP packets to Teams on attended call transfer. As a result, the transfer fails. **Applicable Products:** All
SBC-28453	The device's Debug Recording for file target fails to function and gets stacked when using Debug Recording from two different sources. **Applicable Products:** All
SBC-28472	The device doesn't add the SIP Record-Route header from 200 OK to INVITE when the dialog was challenged with a 401/407. **Applicable Products:** All
SBC-28509	The device sends a SIP INFO in-dialog message to the wrong destination due to a forked 200 OK with the Record-Route header in the initial call setup. **Applicable Products:** All
SBC-28520	The device fails to load PSTN trunks upon startup, printing “PSTN configuration failed - Board loaded without PSTN”. **Applicable Products:** Gateway
SBC-28531	The Dial Plan fails to find a match when the extension is 4 digits long. **Applicable Products:** All
SBC-28538	The device sends a SIP INVITE message with an SDP offer that includes two identical DTMF payload types. **Applicable Products:** All
SBC-28542	The device allows transcoding even though it's not enabled by the License Key. This has been resolved by a change in the behavior when the [TranscodingMode] parameter is configured to **Forced Transcoding**. Up until now, the device always chose the first coder listed in the SDP offer instead of using a common coder offered by both the SIP UAs. Now, the device always chooses the common coder negotiated by the SIP UA peers, thereby avoiding coder transcoding. **Applicable Products:** All

Incident	Description
SBC-28682	The device changes the "#"" character to "%23" in the SIP INVITE message that is sent as a result of terminating a SIP REFER\3xx. **Applicable Products:** All
SBC-28684	The device replies to an HTTP to get a health check received on a non-OAMP interface with SIP 501 instead of 400. **Applicable Products:** All
SBC-28685 / SBC-28961	The device goes into a CPU overload for task VQM as a result of losing connection with OVOC. **Applicable Products:** All
SBC-28715	The device reports a Proxy Set as available to ARM even before it gets a SIP 200 OK reply to a SIP OPTIONS keep-alive. **Applicable Products:** All
SBC-28732	The device fails to update the redundant unit with new Web users that were added through the Web interface (Auxiliary Files) on the active unit. **Applicable Products:** HA
SBC-28749	The device raises a false alarm "Service for Transcoding sessions license parameter is stopped" even though the device or OVOC has no transcoding license. **Applicable Products:** All
SBC-28838	The device sends the wrong 'RemoteID' value in SIP PUBLISH messages for RTCP-XR. **Applicable Products:** All
SBC-28955	The device crashes (resets) when the SIP Interface's signaling port is modified. **Applicable Products:** All
SBC-28977	The device crashes (resets) when receiving a SIP 3xx with a destination to forward that is larger than 50 characters. **Applicable Products:** Gateway
SBC-29358	The device doesn't update the Contact details in its registration database upon a SIP re-Register for 401/407 challenge. **Applicable Products:** All
SBC-29427	The device's retransmission of SIP 18x is incorrect. **Applicable Products:** All
SBC-29468	The device crashes (resets) due to a networking task ("signal 904, task NWST"). **Applicable Products:** Mediant 1000
SBC-29525	The device crashes (resets) upon a call transfer scenario where it receives a SIP BYE message before being able to resolve the DNS to send the new INVITE. **Applicable Products:** All
SBC-29526	The device shows different RAM size values between the ini file and Web interface (Device Information page). **Applicable Products:** Mediant Software
SBC-29611	The device disconnects a call from Teams with SIPREC enabled after a transfer, with the error message "!![ERROR] Board command failed - Internal error". **Applicable Products:** All

Incident	Description
SBC-29687	The device crashes (resets) with a task "DSP" as a result of running a debug recording. **Applicable Products:** All
SBC-29779	The device crashes (resets) with a task "SPTM" because of a memory overrun. **Applicable Products:** All

2.21 Version 7.20A.258.559

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 8.0.114 and EMS/SEM Version 7.2.3113.

2.21.1 Resolved Constraints

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

Table 2-23: Resolved Constraints in Version 7.20A.258.559

Incident	Description
SBC-22563	The device performs an HA switchover upon a REST API command that deletes Network Interface and Ethernet Device. **Applicable Products:** HA
SBC-23324	The device fails to load the Dial Plan file through the CLI script when using Chrome Secure Shell extension. **Applicable Products:** All
SBC-24715	The ini file parameter [TransparentPayloadType] is missing from the CLI. **Applicable Products:** Gateway
SBC-25516	The device sends many syslog warning messages, causing a CPU overload. **Applicable Products:** All
SBC-25549	The device fails to perform a DNS lookup due to a buffer overflow. **Applicable Products:** All
SBC-26251 / SBC-27286 / SBC-27779	The device performs an HA switchover and loses connectivity when the Maintenance interface is over FE ports. **Applicable Products:** Mediant 800
SBC-26319	The device fails to allocate DSP resources, printing syslog messages "Lack of Resources: DSP resource isn't available". As a result, call failure occurs. **Applicable Products:** All
SBC-26413	The device generates DTMF because of false DSP detection. **Applicable Products:** Mediant Software

Incident	Description
SBC-26461	The device fails to allocate DSP resources, printing syslog messages "Not enough utilization for resource". As a result, call failure occurs. **Applicable Products:** All
SBC-26791	The ini file parameter IgnoreAuthorizationStale is missing from the CLI. **Applicable Products:** All
SBC-26820	The device sends a SIP UPDATE without an SRTP offer (even though configured for SRTP). As a result, the call fails. **Applicable Products:** All
SBC-26893	The device performs SIP header manipulation on invalid RTP packets instead of dropping them, causing one-way voice. **Applicable Products:** All
SBC-26961 / SBC-27115	The device's lockdown doesn't function when using the graceful option. **Applicable Products:** All
SBC-27023	The device fails to allocate an HTTP buffer for Remote Monitoring Web Service, printing "HTTPDataPool RestPool is full". As a result, CSR fails. **Applicable Products:** All
SBC-27033	The device's default Malicious Signature table doesn't contain 'pplsip' and 'PortSIP VoIP SDK'. **Applicable Products:** All
SBC-27202	The ENUMAllowNonDigits parameter's value isn't saved after a switch over. **Applicable Products:** HA
SBC-27210	The device's PM acPMChannelsPerCoderCoders doesn't support the EVS coder. **Applicable Products:** All
SBC-27253	The device fails to find a match for incoming SIP CANCEL message after the original INVITE's Request-URI user part changes through CSR. As a result, call disconnection failure occurs. **Applicable Products:** All
SBC-27254	The device fails to create long headers using message manipulation because message manipulation variables are limited to 700 characters. (To resolve this issue, max. characters have been increased to 1,500.) **Applicable Products:** All
SBC-27312	The device crashes (resets) upon connection of LAN_0_3 Ethernet port. **Applicable Products:** Mediant 1000
SBC-27387	The device sends T.38 packets to the wrong port because of incorrect T.38 NAT resolve error. As a result, the fax fails. **Applicable Products:** All
SBC-27399	The device doesn't increase the SDP version when it sends a different SDP. As a result, one-way voice occurs. **Applicable Products:** All
SBC-27470	The Media Component (MC) crashes (resets) when the offline parameter DTMFDetectorSensitivity is configured to "571473920", while the offline parameter CallerIDTransportType has a non-zero value. **Applicable Products:** Mediant CE

Incident	Description
SBC-27595	The device sends a syslog message in the outgoing SIP message's headers. **Applicable Products:** Gateway
SBC-27666	The device sends a SIP re-INVITE message for the session timer with a different SDP, but the same SDP version. **Applicable Products:** Gateway
SBC-27737	The device's CLI command `show voip register db sbc user *` shows only partial information because of character limitation (308). **Applicable Products:** All
SBC-27842	The device crashes (resets) with "Board Was Crashed: Signal 0, Task" because of a buffer overrun. **Applicable Products:** All
SBC-27845	The device adds its IP address as the host to the outgoing message's URL which are not sip: or sips:. **Applicable Products:** All
SBC-27877	The device rejects calls after an HA switchover because of incorrect HTTP buffers calculation. **Applicable Products:** HA
SBC-27882	The device rejects a new SIP INVITE message for an outgoing SIP 422 response upon asynchronous CMR when the outgoing leg has the IP Profile parameter 'SBC Session Expires Mode' set to **Transparent**. **Applicable Products:** All
SBC-27931	The device sends a GetRoute message without an SID. As a result, ARM-based routing fails. **Applicable Products:** Gateway
SBC-27933	The device's NGINX DNS query uses an incomplete FQDN when the upstream host contains a dash in its name. As a result, DNS fails. **Applicable Products:** All
SBC-28000	The device fails to authenticate (by User Info file) SIP REGISTER requests from an IP address that is not configured for the Proxy Set, if the ClassifyByProxySet parameter is disabled. **Applicable Products:** All
SBC-28059	The device ignores the 'Media Security Behaviour' parameter of IP Profile 0 (default). **Applicable Products:** Gateway
SBC-28088	The device crashes (resets) because of a wrong direct access to LDAP tables. **Applicable Products:** All
SBC-28130	The device crashes (resets) upon a SIPREC call that is established with both ways as 'a=inactive'. **Applicable Products:** All

2.22 Version 7.20A.258.459

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.2265 and EMS/SEM Version 7.2.3113.

2.22.1 Known Constraints

This section lists known constraints.

Table 2-24: Known Constraints in Version 7.20A.258.459

Incident	Description
SBC-26251 / SBC-27779	When the device performs a switchover (resets), it loses connectivity if the OAMP and Maintenance (HA) interfaces are configured on the FE ports. **Applicable Products:** Mediant 800 HA

2.22.2 Resolved Constraints

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

Table 2-25: Resolved Constraints in Version 7.20A.258.459

Incident	Description
SBC-27306	The device immediately disconnects the SBC call if it doesn't receive a SIP PRACK message on the incoming leg (instead of waiting for the PRACK and then connecting call). As a result, call failure occurs. **Applicable Products:** All

2.23 Version 7.20A.258.457

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.2265 and EMS/SEM Version 7.2.3113.

2.23.1 New Features

This section describes the new features introduced in this version.

2.23.1.1 OpenSSL Updated to Version 1.1.1i

OpenSSL implemented in AudioCodes devices for secure communication using TLS has been upgraded to OpenSSL Version 1.1.1i.

Applicable Application: All.

Applicable Products: All.

2.23.1.2 Increase in Table Capacity for NGINX HTTP-based Proxy Services

The capacity (maximum rows) of the following tables that are related to NGINX HTTP-based proxy services has been increased:

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

Applicable Application: SBC.

Applicable Products: Mediant SW (≥ 8GB).

2.23.1.3 NGINX Version Update

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

Applicable Application: All

Applicable Products: All.

2.23.2 Resolved Constraints

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

Table 2-26: Resolved Constraints in Version 7.20A.258.457

Incident	Description
SBC-21433	The device doesn't update the ROC of the outgoing SRTP stream, causing the video to freeze after about 5-10 minutes on WebRTC RTP-to-SRTP calls. **Applicable Products:** All
SBC-23558 / SBC-23969 / SBC-24283 / SBC-24349 / SBC-25603	The device crashes (resets) with cause of "CMX kernel panic" because TPNCP logger is running by default. **Applicable Products:** All
SBC-23826	The device's reset history is increased with the same date and time. **Applicable Products:** All
SBC-23933	The InputGain and VoiceVolume parameters fail to work on G.722. **Applicable Products:** All
SBC-23973	The device crashes (resets) with syslog messages "AuditRxPoolDepletion - buffer level below 6.25 percent" and task TIMB. **Applicable Products:** All
SBC-25099	The device cannot add another user with Master privileges, after creating the first Master user. **Applicable Products:** All
SBC-25217 / SBC-26258 / SBC-26370	When the License Key includes the license "FEU=0", the device can only register up to 160 endpoints. **Applicable Products:** MP-1288
SBC-25272 / SBC-25687 / SBC-27055	The device does not increase the SDP version even though it sends different SDPs. As a result, one-way voice occurs. **Applicable Products:** All
SBC-25273	The redundant unit in the HA system fails to upgrade, and crashes (resets) with the task "FLTT". **Applicable Products:** HA
SBC-25397	The device terminates in-dialog SIP OPTIONS messages and returns a 200 OK response instead of sending it to the other leg. This has been resolved by a new parameter SBCTerminateOptions, which when configured to disabled, forwards in-dialog SIP OPTIONS to the outbound peer. **Applicable Products:** All
SBC-25587	For security, the device needs to upgrade OpenSSL to Version 1.1.1i. **Applicable Products:** All
SBC-25615 / SBC-26062 / SBC-26255 / SBC-26322 / SBC-26468 / SBC-26755 / SBC-26941	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

Incident	Description
SBC-25675	The SIP To header's host part doesn't include the destination IP Group's "SIP Group Name" for Tel-to-IP calls when routing is by ARM. **Applicable Products:** Gateway
SBC-25679	The device does not consider 5xx responses from remote HTTP (Web) services (hosts) as a disconnect (and remains connected). **Applicable Products:** All
SBC-25724	The device offers SDP with corrupted crypto when the AMR rate is undefined (because the mode-set field isn't present in the 'a=fmtp' attribute). As a result, the call fails. **Applicable Products:** All
SBC-25918	The device sends a SIP REGISTER message with the wrong Request-Uri ("sip:sip:") upon the receipt of a SIP 301 with FQDN for the first REGISTER. As a result, registration fails. **Applicable Products:** All
SBC-26065	Call transfer fails because the device tries sending a SIP INVITE message instead of detecting its own IP address and performing RLT. **Applicable Products:** Gateway
SBC-26079	The device fails to send a SIP re-INVITE message for media sync in Microsoft's Local Media Optimization environment. As a result, the SBC call fails. **Applicable Products:** All
SBC-26194	The device crashes (resets) when both the AlwaysSendToProxy parameter and the IP Group's 'Always Use Source Addr' parameter are enabled. **Applicable Products:** Gateway
SBC-26331	The device fails to accept an FQDN for an HTTP Remote Host when any of the first three characters is a digit. As a result, an HTTP failure occurs. **Applicable Products:** All
SBC-26374	When the device receives a SIP INVITE message with a User-to-User header, it removes ';encoding=ascii' in the outgoing INVITE. **Applicable Products:** All
SBC-26477 / SBC-26754	The device crashes (resets) when running message manipulation on a header that doesn't exist. **Applicable Products:** All
SBC-26555	The device saves "device uptime" and "Time&Date" in the ini file, causing OVOC to upload the ini file even if it wasn't modifed. **Applicable Products:** All
SBC-26565	The device crashes (resets) with Task "HMGT" as a result of a failed connection with ARM. **Applicable Products:** All
SBC-26570	The device's message manipulation fails when trying to use the Param.IPG.Dst. syntax. The following Syslog message is displayed: "Param.IPG.Dst syntax isn't accessible in current context". **Applicable Products:** All
SBC-26662	The device fails to send Syslog messages. **Applicable Products:** All

Incident	Description
SBC-26767	The device crashes (resets) because it fails to handle the authentication challenge (401 code) with the provisioning server for HTTPS-based Automatic Provisioning. **Applicable Products:** All
SBC-26812	The device changes its SRTP stream, causing one-way voice, because of detecting invalid RTP packets on the other (RTP) leg. **Applicable Products:** All
SBC-26922	The device prints RADIUS credentials in the Syslog message when connecting to the RADIUS server (for RADIUS-based Web login), exposing possible security breach. **Applicable Products:** All

2.24 Version 7.20A.258.367

This version includes known and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.24.1 Known Constraints

This section lists known constraints.

Table 2-27: Known Constraints in Version 7.20A.258.367

Incident	Description
SBC-25615 / SBC-26062 / SBC-26255 / SBC-26322 / SBC-26468 / SBC-26755 / SBC-26941	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

2.24.2 Resolved Constraints

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

Table 2-28: Resolved Constraints in Version 7.20A.258.367

Incident	Description
SBC-25831 / SBC-26025	The device crashes (resets) when syslog is enabled (EnablerSyslog = 1 and GWDebugLevel>0). A workaround is to disable Syslog and GWDebugLevel=0. **Applicable Products:** MP-1288, Mediant 5xx, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000

2.25 Version 7.20A.258.363

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.25.1 Known Constraints

This section lists known constraints.

Table 2-29: Known Constraints in Version 7.20A.258.363

Incident	Description
SBC-25615 / SBC-26062 / SBC-26255 / SBC-26322 / SBC-26468 / SBC-26755 / SBC-26941	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-26251 / SBC-27779	When the device performs a switchover (resets), it loses connectivity if the OAMP and Maintenance (HA) interfaces are configured on the FE ports. **Applicable Products:** Mediant 800 HA

2.25.2 Resolved Constraints

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

Table 2-30: Resolved Constraints in Version 7.20A.258.363

Incident	Description
SBC-25398	The device's PAYG (pay-as-you-go) SBC on AWS shows no FEU licenses, causing registration failure **Applicable Products:** Mediant VE
SBC-25545	The device on Azure crashes (resets) with the exception reason "CHashMap CIterator". **Applicable Products:** Mediant CE
SBC-25642	The device on Azure has no audio for SRTP calls during software upgrade (until MCs are also upgraded). **Applicable Products:** Mediant CE
SBC-25664	The device has no audio and video for WebRTC calls in a Genesis environment. **Applicable Products:** All
SBC-25709	WebRTC call failure upon a SIP re-INVITE from the calling side in a Genesis environment **Applicable Products:** All

2.26 Version 7.20A.258.354

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.26.1 New Features

This section describes the new features introduced in this version.

2.26.1.1 ARM Management of SBCs in Teams Environment

Device(s) deployed in a Microsoft Teams environment can now be managed by AudioCodes Routing Manager (ARM). To support this feature, a new parameter has been added to the Media Realm table 'Used By Routing Server', which needs to be configured to **Used**. This enables ARM to get information on the Media Realm (used by ARM for Teams call routing).

Applicable Application: SBC.

Applicable Products: All.

2.26.1.2 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 now 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.

2.26.1.3 X-MS-SBC Header Support for Microsoft Teams Direct Routing

The device now supports sending the Microsoft's proprietary X-MS-SBC header in outgoing SIP OPTIONS and INVITE messages to the Teams server for Direct Routing. This header is used by Microsoft Teams to identify vendor equipment (e.g., AudioCodes SBC). The device includes the following values in this header: *Audiocodes/<model>/<firmware>*, where:

- *model* is the AudioCodes device name (valid values are listed by Microsoft at https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers)
- *firmware* is the software version running on the device

The feature is configured by the new IP Group table parameter, 'Teams Direct Routing Mode' (**Enable** or **Disable**). (Note that this header cannot be modified or removed using the device's Message Manipulation functionality.)

Applicable Application: SBC.

Applicable Products: All.

2.26.1.4 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 7.20A.258.354 and later.

Applicable Application: All.

Applicable Products: Mediant 1000.

2.26.2 Known Constraints

This section lists known constraints.

Table 2-31: Known Constraints in Version 7.20A.258.354

Incident	Description
SBC-25588	The device's Web interface's Configuration Wizard doesn't function properly (tiny font size and impossible to configure). **Applicable Products:** All.
SBC-25559	Backward compatibility for CLI no longer functions. If a load attempt for a CLI script of a very earlier software version is loaded to the device running a later version, the CLI script is not applied. **Applicable Products:** All

Incident	Description
SBC-25615 / SBC-26062 / SBC-26255 / SBC-26322 / SBC-26468 / SBC-26755 / SBC-26941	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

2.26.3 Resolved Constraints

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

Table 2-32: Resolved Constraints in Version 7.20A.258.354

Incident	Description
SBC-20913	Fax calls fail because the device fails to open the channel with fax detectors in the Media-Sync stage. **Applicable Products:** All
SBC-22593	The device fails to open voice towards its own NAT IP address in a loopback delayed offer call. As a result, one-way voice occurs. **Applicable Products:** All
SBC-22925	The device's Dial Plan ranges (prefix-suffix) don't match the number of digits in the target string. **Applicable Products:** All
SBC-22970	The device's LDAP search fails with "CyclicId already in use" error message. **Applicable Products:** All
SBC-23151	The CLI commands `show voip calls active gw` and `show voip calls history gw` have different syntax. **Applicable Products:** Gateway
SBC-23576	The device loses connection to OVOC because of a socket error event. **Applicable Products:** All
SBC-23616	The device doesn't send all CDRs over RADIUS when operating with two RADIUS servers. **Applicable Products:** All
SBC-23659	The device's TDM-to-SBC license doesn't function as expected. **Applicable Products:** Gateway
SBC-23781	When the device operates in HA mode, the Web interface's Active LED's color doesn’t display correctly. **Applicable Products:** Mediant 2600; Mediant 4000
SBC-23824	For SBC calls, the device changes the 'Type' and 'Boundary' values in the Content-Type header of SIP messages containing multipart bodies. (This constraint has been resolved by a new parameter PreserveMultipartContentType, which enables the device to preserve the value of the Content-Type header in the outgoing message. **Applicable Products:** All

Incident	Description
SBC-23840	The device generates DTMF after a DSP false detection. **Applicable Products:** All
SBC-23854	The parameters 'Call Success Internal Reasons' and 'Call Failure Internal Reasons' can't be configured with the following internal response codes: ▪ "814" (RELEASE_BECAUSE_FORWARD_SUPPLEMENTARY) ▪ "816" (RELEASE_BECAUSE_LDAP_FAILURE) ▪ "817" (RELEASE_BECAUSE_CALLSETUPRULES_FAILURE) **Applicable Products:** All
SBC-23862	The device sends the SDP answer with 'c= 0.0.0.0' and 'a=recvonly', causing call failure. **Applicable Products:** All
SBC-23983	The device doesn't forward the "Content-Type: application/X-NECSIPEXT2MLv1" body in SIP REGISTER requests. As a result, registration fails. **Applicable Products:** All
SBC-24300	The device changes the expires and q-value in SIP REGISTER messages from 'q=1.1' to 'q=1.001', causing a registration failure. **Applicable Products:** All
SBC-24393	The device crashes (resets) after receiving 'application/dialog-info+xml' in the SIP Content-Type header with a participant that is longer than 100 characters. **Applicable Products:** All
SBC-24646	The device changes the RTP sequence number, causing one-way voice. **Applicable Products:** All
SBC-24653	The device adds T.38 to the SDP offer even though the far side is not configured for T.38, causing call failure. **Applicable Products:** All
SBC-24674	The device is not accessible over SSH. **Applicable Products:** All
SBC-24730	The maximum number of supported characters for the SIP Call-ID header is insufficient. (Now, it has been increased to 231 characters.). **Applicable Products:** All
SBC-24759	The device sends to the network duplicated RTCP packets. **Applicable Products:** Mediant 1000
SBC-24772	The Accounts table cannot be removed through CLI using the `where` attribute. **Applicable Products:** All
SBC-24835	When the device operates in HA mode, a false FAN alarm on the redundant device is raised. **Applicable Products:** HA
SBC-24924	The device's Message Manipulation functionality copies the Header.Via.Host into the Header.From.Url.Host and issues an "Illegal IPv4Address" parsing error. **Applicable Products:** All
SBC-24946	The 'Connectivity Status' field of the Tel-to-IP Routing table always displays "N\A". **Applicable Products:** Gateway

Incident	Description
SBC-25009	The device doesn't send a SIP ACK message for transferred calls, causing the transfer to fail. **Applicable Products:** All
SBC-25014	The device is inconsistent regarding naming of BRI interfaces between CLI command outputs of `sh voip calls active` and `sh voip calls history gw`, displaying wrong port starting from the second module. **Applicable Products:** Gateway
SBC-25063	The device's Message Manipulation condition check of 'm=video' line fails. **Applicable Products:** All
SBC-25096	The device crashes (resets) after changing the Proxy Set's 'Proxy Keep-Alive' parameter to **Using OPTIONS on Active Server**. **Applicable Products:** All
SBC-25199	The device sends multiple warnings (spam) to the syslog. **Applicable Products:** All
SBC-25208	The device's CLI Script default value of the 'Tagging' parameter for Index #0 in the Ethernet Device table is inconsistent. **Applicable Products:** All
SBC-25212	The Call-ID SIP header's value is limited to 192 characters. (This constraint has been resolved by increasing it to 231 characters.) **Applicable Products:** Mediant 9000; Mediant Software
SBC-25219	The device doesn’t replace the originating (source) number with the ELIN number for E911 calls, causing call failure. **Applicable Products:** Gateway
SBC-25313	The device sends RTP packets with inconsistent sequence numbers after a SIP re-INVITE. **Applicable Products:** All
SBC-25342	The device rejects the SDP answer with a SIP 488 response with a "Security Feature can’t handle media" reason, because the wrong crypto suite was chosen. As a result, the call fails. **Applicable Products:** All
SBC-25364	The Command Shell command "AnalogLineTest" doesn't function on FXO channels. **Applicable Products:** Mediant 1000

2.27 Version 7.20A.258.271

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.27.1 New Features

This section describes the new features introduced in this version.

2.27.1.1 Minimum Interval between DTLS Packet Transmissions

The minimum interval that the device waits between transmission of DTLS packets for the same DTLS handshake can now be configured. The configured value is applied in a "best-effort" manner (i.e., time between transmitted DTLS packets in the same handshake may differ due to constraints on the network layer and load on the device).
This feature is configured using a new parameter, DTLSTimeBetweenTransmissions.

Applicable Application: SBC.

Applicable Products: All.

2.27.2 Resolved Constraints

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

Table 2-33: Resolved Constraints in Version 7.20A.258.271

Incident	Description
SBC-17606	The device experiences one-way voice after the DTMF key is pressed for a WebRTC call. **Applicable Products:** All
SBC-18645 / SBC-19072	The device runs Message Manipulation and Call Setup Rules simultaneously, causing faulty results (for example, empty headers or wrong ports). **Applicable Products:** All
SBC-23459	Modification of the device's username and password through SNMP fails. **Applicable Products:** All
SBC-23633	The device crashes (resets) upon the receipt of a SIP 18x for an alternative call where the originator doesn't support multiple 18x responses. **Applicable Products:** All
SBC-23697	The device doesn’t remove the 'a=msid' attribute in the SDP body for WebRTC-to-non WebRTC calls, causing no voice. **Applicable Products:** All
SBC-23735	The device's registration database erroneously increased with registered users (full) because it fails to send un-registers to expired users. **Applicable Products:** All
SBC-23984	The device fails to detect DTMF digits (RFC 2833) when the digit’s payload type is changed during the digit detection process. **Applicable Products:** All

Incident	Description
SBC-24307	When a WebRTC call begins, no voice occurs. Voice occurs only after the user presses any DTMF key on the phone keypad. This constraint was resolved by a new IP Profile parameter, SBCRenumberMID, which when enabled and the outgoing SDP offer contains the 'a=mid:n' (where *n* is a unique value), the device changes the value to start from 0. **Applicable Products:** All

2.28 Version 7.20A.258.246

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.28.1 New Features

This section describes the new features introduced in this version.

2.28.1.1 Board ID (BID) SID Changed for Mediant 90xx/Software

The Board ID (BID) and Session ID (SID), which are included in generated Syslog messages, are now based on the device's serial number (last 6 characters of the hex number). This provides improved accuracy for identifying the device that generated the Syslog. (Up until now, their values were based on MAC address.)

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.28.1.2 Fax Transmission over IP

For Tel-to-IP fax transmissions, the existing IsFaxUsed parameter now has a new optional value, G.711 reject T.38 (4). This setting is similar to the optional value G.711 Transport (2), but if the incoming media is of type image ('m=image'), the device rejects the re-INVITE message for T.38.
Applicable Products: Gateway.

2.28.2 Resolved Constraints

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

Table 2-34: Resolved Constraints in Version 7.20A.258.246

Incident	Description
SBC-17364	When the device runs WebRTC over the Safari browser, it experiences video breakdowns after a SIP re-INVITE. **Applicable Products:** All
SBC-18310	The device stops sending SIP ladder messages (SIP call flows) to OVOC and experiences a QoE connection lost. **Applicable Products:** All
SBC-18808	The device sends bad audio quality because it activates the channel in receive-only mode with a combination of both play-silence and generate-no-op enabled. **Applicable Products:** All
SBC-19887 / SBC-23785	The device disconnects and deletes the socket connection to OVOC when OVOC replies with a 5xx to the device's request. **Applicable Products:** All
SBC-20334	The device's web interface displays "maximum log messages reached" messages when refreshing the message log page too many times. **Applicable Products:** All
SBC-20953	The device tries allocating DSP for transcoding even though the device was configured for forwarding (MC has no DSP). As a result, calls fail. **Applicable Products:** Mediant CE
SBC-20970 / SBC-22874	The device fails to perform transcoding to SILK coders (no voice towards SILK side). **Applicable Products:** Mediant CE
SBC-21280 / SBC-22789	The device's BRI LED does not turn red when a busy-out condition occurs and BRI is configured with NT. **Applicable Products:** Gateway
SBC-21619	The device erroneously changes the RFC 2833 DTMF duration from 800 to 400 on Opus to G.711 calls. **Applicable Products:** All
SBC-21759 / SBC-21978	The device stops sending messages to the web interface's Message Log page. **Applicable Products:** Mediant Software
SBC-21832	The device changes the outgoing SDP answer, but doesn't increase the SDP version (in the 'o=' line). **Applicable Products:** All
SBC-21867	The device experiences memory leak issues when running debug recording with Media & PCM on transcoding calls. **Applicable Products:** All
SBC-21920	The device resets upon an SSH connection when TLS Context #0 contains pkey and cert that are not RSA. **Applicable Products:** All

Incident	Description
SBC-21975	The device doesn't support LDAP queries containing white spaces in the LDAPNumericAttribute parameter. A workaround is to replace white spaces with "\20". **Applicable Products:** All
SBC-21979	When accessing the device's web interface, it doesn't display properly, and the following Syslog message is generated: "chank alloc failed …". **Applicable Products:** All
SBC-22072	The device incorrectly calculates SBC session resources upon a failed INVITE with Replaces, causing a mismatch between actual active calls and license key of the fixed license pool. **Applicable Products:** All
SBC-22100	When Remote Monitoring is set (HTTPRemoteServices with HTTP Type set to Remote Monitoring) with Active Alarms and Performance Indicators enabled, the device continuously raises and clears the acSWUpgradeAlarm alarm. **Applicable Products:** All
SBC-22133	The device doesn’t support a User-Info file containing the LF character for end of line (and not CRFL). **Applicable Products:** All
SBC-22143	The device crashes (resets) upon sending a request to the next IP address in the destination IP list, which is empty. **Applicable Products:** All
SBC-22173	The device generates the "Comment:RTCPSrvValidateRTCPPacket() failed" message in the Syslog on an SBC RTP-Forwarding call with header normalization, and where an invalid incoming RTCP packet with wrong CumLost value is received by the device. **Applicable Products:** All
SBC-22255	The device disconnects the call after an HA switchover when the SC (device) and MC are on the same server. **Applicable Products:** Mediant CE
SBC-22259 / SBC-22983	The device crashes (resets) when using ARM for routing and using DNS to resolve more than four IP addresses. **Applicable Products:** All
SBC-22298	The device sends a SIP 404 instead of the exact 4xx received by ARM. **Applicable Products:** All
SBC-22310	The device crashes (resets) when running high traffic and displaying the web interface's Message Log page. **Applicable Products:** All
SBC-22349	The device activates Call Setup Rules on a SIP Interface (before classification), but fails to find a match to the user in its registration database. As a result, the CSR fails. **Applicable Products:** All
SBC-22395	There is no corresponding CLI command for the ini file parameter GwSdpConnectionMode. **Applicable Products:** Gateway

Incident	Description
SBC-22399	The device has a bad echo from the TDM (FXO) side. **Applicable Products:** Mediant 1000
SBC-22456	Even though the device is configured for G.711 Fax (IsFaxUSed=2), it still accepts SDP offers with T.38. As a result, fax fails. To resolve bug, a new value was added to IsFaxUsed - 4 (G.711 reject T.38). **Applicable Products:** Gateway
SBC-22465	The device sends a re-INVITE for fax with image media only ('m=image') and with crypto (should send without crypto if fax only). As a result, the fax fails. **Applicable Products:** All
SBC-22540	The device crashes (resets) upon DNS resolve refresh for DNS of Call Setup Rules with persistent connection, because the order of resolved IP addresses change. **Applicable Products:** All
SBC-22541	Device upgrade to software version greater than 7.20A.254 fails if the license key contains "VoiceAI-GW". **Applicable Products:** All
SBC-22568	The device fails to establish a TLS connection when 'TLS Mutual Authentication' is configured to **Enable** and 'Strict Certificate Extension Validation' to **Enable** in Teams' TLS Context. **Applicable Products:** All
SBC-22591	The device fails to receive T.38 packets for fax. As a result, the fax call fails. **Applicable Products:** All
SBC-22598	The device crashes (resets) upon a race condition when a single call begins to disconnect and then the CLI command `show voip calls active sbc` is run. **Applicable Products:** All
SBC-22719	The device's Auto-Update parameter TLSRootFileUrl replaces existing root certificates instead of appending them, causing the device to crash (reset). (A new parameter has been added to resolve bug – TLSIncrRootFileUrl, which loads trusted root incrementally. **Applicable Products:** All
SBC-22772 / SBC-22773	The device crashes (resets) because of a race condition between T.38 fax QoE report and timer expiration. **Applicable Products:** All
SBC-22787 / SBC-22920	The device crashes (resets) when connecting (Telnet or SSH) with a long username containing spaces and special characters (ASCII value below 31) and then checking the Web interface's Activity Log page (Monitor > Summary > Activity Log). **Applicable Products:** All
SBC-22788	The parameter EnableSilenceCompression is hidden in the management interfaces. **Applicable Products:** All
SBC-22845	When DR is running, many warnings are generated in Syslog ("_drSyslogRecordRead() ERROR: trying to read up to page size"). **Applicable Products:** All

Incident	Description
SBC-22868	When the device adds a new header to outgoing INVITE messages using a Message Manipulation rule, the header's length is limited to 39 characters. (Now, header length has been increased to 49.) **Applicable Products:** All
SBC-22871	The device randomly reports abnormally high values for the PM acPMModuleRTPPacketLossRxVolume. **Applicable Products:** All
SBC-22958 / SBC-22999	The device (on AWS) fails to recover from an HA switchover if the Redundant device is configured with the wrong UTC time offset when UTC offset or DST is configured. **Applicable Products:** Mediant Software (AWS)
SBC-23013	The device crashes (resets) when receiving a SIP BYE in blind transfer scenario, where the device still collects digits. **Applicable Products:** Gateway
SBC-23024	Fax transcoding (T38-G.711) fails when the originator's fax offer is with both voice and fax, but the terminator's fax answer is with fax only. **Applicable Products:** All
SBC-23033	The device doesn't replace the FQDN of the incoming SDP origin field ('o=') with an IPv4 IP address. **Applicable Products:** All
SBC-23075	Parameters return to default when loading a License Key file using the Auto-Update IniFileUrl parameter. **Applicable Products:** All
SBC-23111	The device crashes (resets) when the CLI command `conf voip gateway trunk-group-settings 0` is run. **Applicable Products:** Gateway
SBC-23117	The device fails to latch to a new RTP stream when NatMode is configured to 2 (Force NAT), even though InboundMediaLatchMode is configured to 1 (Dynamic) and NewSRTPStreamPackets to 3. As a result, no voice occurs. **Applicable Products:** All
SBC-23125	The device crashes (resets) after an alternative routing scenario that caused a memory overrun **Applicable Products:** All
SBC-23148	The device's ENUM query should conditionally allow non-digits and support longer input strings **Applicable Products:** All
SBC-23247	The device's Web interface has cross-site scripting (XSS) security vulnerability discovered by pentest. **Applicable Products:** All
SBC-23377	The device blocks HTTP ports in OVOC\UDP\TCP Servers for non-OAM interfaces. As a result, connection fails with HTTP server. **Applicable Products:** All

Incident	Description
SBC-23395	The device resets the SRTP data when receiving SRTCP with wrong SSRC. As a result, no voice occurs. **Applicable Products:** All
SBC-23428	The device runs out of pool size and has no more free IDs for resource of "SIPAppEventResource"", causing forking to fail and calls to drop. **Applicable Products:** All
SBC-23434	The device displays credentials (username and password) in the Syslog when the user updates the INIFileURL and CMPFileURL parameters through the Admin Page. **Applicable Products:** All
SBC-23436	The device fails to perform a transcoding call when "TranscodingOnM500L = 1". **Applicable Products:** Gateway
SBC-23449	The device's disk becomes full because of an NGINX bug (sending error_log to syslog still also sends messages to a file on disk). **Applicable Products:** All
SBC-23521	The device performs an HA switchover because the parameter HeartbeatIntervalmsec returns to default (100ms instead of 300ms). **Applicable Products:** Mediant CE
SBC-23652	The device (SC) shows MC as disconnected after a software upgrade that includes a hard reset. **Applicable Products:** Mediant 9000
SBC-23726	The device crashes (resets) upon multiple SIP 18x for an alternative routing call when the originator doesn't support multiple 18x responses. **Applicable Products:** All
SBC-23740	The device's pipe operators such as "| grep" are not supported in the CLI `show voip calls` commands. **Applicable Products:** All

2.29 Version 7.20A.258.119

This version includes new features and resolved constraints only.

Note:

- This is the first LTS version for Release 7.2.
- This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1130 and EMS/SEM Version 7.2.3113.

2.29.1 New Features

This section describes the new features introduced in this version.

2.29.1.1 Built-in Firewall Rules to Allow HA Maintenance Traffic

The device now provides built-in firewall rules that allow High Availability (HA) traffic between Active and Redundant devices on the Maintenance network interface. Up until now, the user had to configure special firewall rules on the device to allow and ensure HA maintenance traffic on specific ports.

Applicable Application: SBC.

Applicable Products: Mediant 500; Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.29.2 Resolved Constraints

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

Table 2-35: Resolved Constraints in Version 7.20A.258.119

Incident	Description
SBC-18640	The device generates error messages in the Syslog ("gwSession failed to allocate handle"). **Applicable Products:** All
SBC-19431 / SBC-21778	The device sends distorted voice (bad voice quality) towards the G.711 side for G.722-to-G.711 transcoding SBC calls. **Applicable Products:** All
SBC-19517	The ini file parameter SBCRemoveSIPSFromNonSecuredTransport has no corresponding parameter/command in the web/CLI management interfaces. Now, it has been added to the web ('Remove SIPS from Non-Secured Transport') and CLI (configure voip > sbc settings > sbc-remove-sips-non-sec-transp). **Applicable Products:** All
SBC-19609	The device falls back to alternative SBC routing when CAC is crossed even if an alternative reason for CAC is not configured (in the Alternative Reasons Set table). **Applicable Products:** All

Incident	Description
SBC-19979	The device doesn't synchronize the last login information (of any user) between the active and redundant units in a High Availability (HA) system. As a result, login (to the redundant unit after a switchover) fails. **Applicable Products:** HA
SBC-20269 / SBC-21627	The device's message manipulation on the SDP removes (instead of copying) the ICE candidate from the outgoing SDP offer. **Applicable Products:** All
SBC-20726	The device doesn't report QoE media attributes (such as MOS) to OVOC. **Applicable Products:** All
SBC-20843	The device's Floating License connection to OVOC (using WebSocket) fails after an HA switchover. **Applicable Products:** Mediant CE (HA)
SBC-20661	The Automatic Update mechanism shows the username and password in the syslog message (when credentials are used in the IniFileUrl parameter), exposing the device to security risks. **Applicable Products:** All
SBC-20703	The device fails to play MOH using PRT, because it opens the channel with 'a=inactive' (instead of 'a=recvonly'). **Applicable Products:** All
SBC-20769	If the device receives a call from the PSTN (ISDN) with 'SrcPres=1', it still shows the calling number in the SIP From header (instead of "Anonymous"). **Applicable Products:** Gateway
SBC-20801	If the device receives a call from the PSTN with 'DstNT=-1 DstNP=-1', it sends a Route request to ARM with wrong values. As a result, the call fails. **Applicable Products:** Gateway
SBC-20897	The device replies with a SIP 500 (Server Internal Error) to an incoming SIP NOTIFY message. **Applicable Products:** All
SBC-20994	The device performs an HA switchover due to wrong Firewall (access list) rules. Now, special firewall rules are no longer required to allow Maintenance traffic. **Applicable Products:** HA
SBC-21010	The device retransmits CDR in RADIUS format (duplicated) upon receipt of accounting response message from server. **Applicable Products:** All
SBC-21092	The device terminates the SIP re-INVITE message after a transfer (REFER) failure, causing one-way voice. **Applicable Products:** All
SBC-21134 / SBC-21238	The device sends distorted voice (bad voice quality) towards the G.711\G.729 side on an Opus-to-G.711 transcoding SBC call using Managed Opus. **Applicable Products:** All
SBC-21313	The device crashes (resets) when a user attempts to deactivate call forwarding using the keypad feature. **Applicable Products:** Gateway

Incident	Description
SBC-21316 / SBC-21410 / SBC-21976	The device fails to open the voice towards itself (fails to detect its own NAT IP address) on a Local Media Optimization (Microsoft) SBC call. **Applicable Products:** All
SBC-21428	The device crashes (resets) upon a blind call transfer which requires DSPs (when the device is configured to operate with RTP forwarding). **Applicable Products:** Mediant CE
SBC-21474	The device crashes (resets) upon a Least Cost Routing failure (row in IP-to-IP Routing table is deleted when table sorted). **Applicable Products:** All
SBC-21560	An SBC conference call in a Microsoft Teams environment fails, because the device blocks STUN packets. This occurs as the device's robust mechanism blocks all traffic that is different than the latched stream. Now, STUN packets bypass this mechanism. **Applicable Products:** Mediant 1000
SBC-21631	The device doesn't support configuration of NGINX Resolver Mode (IPv4 and IPv6). **Applicable Products:** All
SBC-21731	The device marks an IP Group as temporary blocked because of SRV resolved failures (SRV query requires 3 result records in addition to the already allocated 3 server-info records to succeed, while customer had 61 simultaneous requests, which required 6 times more result records for the SRV DNS resolution). As a result, call routing failed. **Applicable Products:** All
SBC-21736	The device removes video coders from the outgoing SDP answer. **Applicable Products:** All
SBC-21760	The device fails to get the local ICE credential and sends a SIP INVITE message with an SDP offer (incorrect) that has 'IP=0.0.0.0' for ICE candidates. **Applicable Products:** All
SBC-21763	When the device receives an SDP offer with two identical media lines (for whatever reason) it fails to send SDP answer with the correct order (should accept the first media and reject the second media). **Applicable Products:** All
SBC-21843	The device fails to send the Server Name Identity (SNI) field in the Client Hello message when redirected to different server during the Auto Update process. **Applicable Products:** MP-1288

2.30 Previous LR Versions

This section describes the new features, constraints and resolved constraints of previous LR versions for Release 7.2.

2.30.1 Version 7.20A.258.010

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1119 and EMS/SEM Version 7.2.3113.

2.30.1.1 Resolved Constraints

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

Table 2-36: Resolved Constraints in Version 7.20A.258.010

Incident	Description
SBC-20676 \ SBC-21116 \ SBC-21130 \ SBC-21171 \ SBC-21211 \ SBC-21393 \ SBC-21419 \ SBC-21682	The device crashes (resets) due to a memory overrun. This affects software versions 7.20A.256.721, 7.20A.256.725, 7.20A.258.006, and 7.20A.258.007. **Applicable Products:** Mediant 4000
SBC-21331 \ SBC-21400 \ SBC-21541	The device resets with exception information of a kernel panic because of a memory overrun (incorrect calculation of buffer's size - 2K instead of 4K). This affects software version 7.20A.258.006. **Applicable Products:** Mediant Software (Kernel-based Virtual Machine)

2.30.2 Version 7.20A.258.007

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1119 and EMS/SEM Version 7.2.3113.

2.30.2.1 Resolved Constraints

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

Table 2-37: Resolved Constraints in Version 7.20A.258.007

Incident	Description
SBC-20425	The device rejects an alternative routing call with a SIP 488 response when multiple answers are not allowed. **Applicable Products:** All
SBC-20759	No access to the device's web interface after an HA switchover because of a "stuck" internal task (SendTCP_TPNCPPacket(): Partial data sent). As a result, switchover fails. **Applicable Products:** Mediant CE (Azure)

2.30.3 Version 7.20A.258.006

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

Note:

- As the last decimal group ("xxx" – representing the minor build) of software version *7.20A.**256**.xxx* has almost reached maximum capacity, from Version 7.20A.256.725, the software version numbering has been changed to *7.20A.**258**.xxx*. Version 7.20A.258.xxx is a minor version based on Version 7.20A.256.725. Version 7.20A.258.xxx includes the same content and functionality as 7.20A.256.725 (with the bug fixes listed in this document).
- This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.1119 and EMS/SEM Version 7.2.3113.

2.30.3.1 New Features

This section describes the new features introduced in this version.

2.30.3.1.1 OpenSSL Updated to Version 1.1.1g

OpenSSL implemented in AudioCodes devices for secure communication using TLS, has been upgraded to OpenSSL Version 1.1.1g.

Applicable Application: All.

Applicable Products: All.

2.30.3.1.2 Specific Source Address for Static Routes

The source IP address of outgoing packets for a static route can now be configured, by assigning the static route a local source IP interface (from the IP Interfaces table). This feature can be used when the device sends packets to a specific destination that requires a specific source address, for example, when using multi-homing (multiple IP addresses configured on the same VLAN device). It also provides predictability and consistency of locally-generated traffic, which is useful (or even needed) for firewalls, monitoring or reporting, and various other use cases.

The feature is supported by the new parameter in the existing Static Routes table, called 'Preferred Source' (StaticRouteTable_PreferredSourceInterfaceName / preferred-source-interface-name). The parameter references (points) the IP Interfaces table. If not specified, the device sets the source address of the outgoing packet to the address of the IP Interface that is associated with the static route's VLAN ('Ethernet Output Device').

Applicable Application: All.

Applicable Products: All.

2.30.3.2 Known Constraints

This section lists known constraints.

Table 2-38: Known Constraints in Version 7.20A.258.006

Incident	Description
SBC-19284	If the SBC is not configured to work with NTP, and the system administrator has manually changed the system time to a time in the past, the system might perform an unsuccessful reset cycle, resulting in a system restore to factory defaults (via factory image). To avoid this, it is recommended to use NTP or not to set a past system time. **Applicable Products:** Mediant SW

2.30.3.3 Resolved Constraints

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

Table 2-39: Resolved Constraints in Version 7.20A.258.006

Incident	Description
SBC-16828	The device resets due to a fatal exception error during a WebRTC call **Applicable Products:** Mediant SW
SBC-18426	The device ignores the ARM response 404, and sends a 500 reply instead. **Applicable Products:** All
SBC-18469	The device resets due to an LDAP error. **Applicable Products:** All
SBC-18479	The device's SRD Isolation feature has no effect with tag-based routing. **Applicable Products:** All
SBC-18552	Changes in the name of the IP Group are not synchronized with the active alarm when IP Group blocked (still shows the old IP Group name). **Applicable Products:** All
SBC-18553	The device uses the wrong source IP address for an HTTP packet. (This was resolved by the new feature described in Section 2.30.3.1.2.) **Applicable Products:** All
SBC-18615	The device disconnects a WebRTC video call because it attempted to allocate DSP resources to transrate the video (where there are no DSP resources available). **Applicable Products:** All
SBC-18822	The device fails to remove silence suppression on the outgoing leg (incorrect SDP) when using the G.722 coder, even though the IP Profile's 'Use Silence Suppression' is configured to **Remove**. **Applicable Products:** All
SBC-18874	The device reports the wrong value for packet loss (greater than 100%) to OVOC when the remote endpoint sends the wrong value for Cum Lost. **Applicable Products:** Gateway

Incident	Description
SBC-18989	When the device works with HTTP, POST (http.request.body) requests produce the error "HTTPDataPool RestPool is full", causing call failure. **Applicable Products:** All
SBC-19091	The device incorrectly replies to the REST API request */api/v1/status* with "N/A" for the default subnet (subnetMask) and default Gateway (defaultGateway) fields. **Applicable Products:** All
SBC-19112	The device's CLI `traceroute` command fails for some interfaces ("traceroute: x.x.x.x is not on interface eth3.52 ping was closed"). **Applicable Products:** All
SBC-19116	The device's IPv6 emergency calls fail to establish due to parser error, as the To header URL host does not accept square brackets (e.g., urn:service:sos@[2001:db8:aaaa:b::2] SIP/2.0). **Applicable Products:** All
SBC-19117	The device has one-way voice when the IP Profile's 'Media IP Version Preference' is configured to **Prefer IPv6**, because the device chooses the wrong remote crypto key (IPv4 instead of IPv6). **Applicable Products:** All
SBC-19144	The device resets when the Call Pickup feature is used with dial plan tagging. **Applicable Products:** Gateway
SBC-19179	The device failed temperature and humidity chamber test on 3 of the 4 FXS modules (causing FXS out-of-service). **Applicable Products:** MP-1288
SBC-19262	The device resets when processing a SIP REGISTER for registering a user from the User Info table. **Applicable Products:** Mediant CE
SBC-19276 / SBC-19779 / SBC-19887	The device experiences a CPU overload for task "HMGT", due to high traffic of NGINX which makes the buffers full. **Applicable Products:** All
SBC-19292	The device's Web interface is missing the parameter SbcRemoveSipsFromNonSecuredTransport. **Applicable Products:** All
SBC-19293	The device deployed on the AWS cloud loses connection to the DNS server, causing an outage **Applicable Products:** Mediant SW (AWS)
SBC-19294	The device deployed on the AWS cloud resets upon receiving a UDP packet that is greater than 1,500 bytes **Applicable Products:** Mediant SW (AWS)
SBC-19324	The device shows notations for the Internal Success/Failure Reasons (Call Detail Record Settings) **Applicable Products:** All
SBC-19434	The device deployed on Hyper-V experiences no voice after its vCPU is upgraded. **Applicable Products:** Mediant SW (Hyper-V)

Incident	Description
SBC-19438	The device resets when it receives a SIP INVITE\REGISTER with a malformed Authorization header. **Applicable Products:** All
SBC-19445	When the device is loaded with invalid configuration (Physical Ports table) it cannot be modified to fix the configuration. **Applicable Products:** All
SBC-19467 / SBC-20064	The device loses the certificate after a private key *.pfx file is loaded, therefore, exposing a security risk. **Applicable Products:** All
SBC-19493	The device incorrectly allows the same TCP and TLS port for a SIP Interface (in the SIP Interfaces table). **Applicable Products:** All
SBC-19630	The device doesn't support SIP INVITE with the Replaces header received on a different SIP Interface than the original call. As a result, the call fails. **Applicable Products:** All
SBC-19726	The device tries to allocate DSPs for transcoding when Teams replies with multiple coders that have G.722 with Silence Suppression. As a result, the call fails. **Applicable Products:** All
SBC-19797	The device answers to a SIP Re-INVITE session timer with an incorrect attribute ('a=inactive' instead of 'a=sendrecv'). As a result, no voice occurs. **Applicable Products:** All
SBC-19954	The device's Web interface doesn't show the CEDTransferMode ini file parameter. **Applicable Products:** All
SBC-20018	The device uses the wrong RTP port when receiving an ARM call with delayed offer. As a result, no voice occurs. **Applicable Products:** Gateway
SBC-20026	The device tries (and fails) to play a hold tone for a direct media call, although not supporting it. **Applicable Products:** All
SBC-20181	The device tries to allocate DSPs for transcoding even though there is no need for transcoding (fax scenario). As a result, the call fails. **Applicable Products:** All

2.30.4 Version 7.20A.256.725

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.4.1 Resolved Constraints

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

Table 2-40: Resolved Constraints in Version 7.20A.256.725

Incident	Description
SBC-18211	The device's HTTP Request Update IP to FQDN fails, resulting in a DNS failure. **Applicable Products:** All.
SBC-19433 / SBC-19626	The device fails to detect DTMF when the SILK coder is used. If the voice coder is wideband, but both offer and answer DTMF are narrowband, the correct DTMF payloads are not chosen. **Applicable Products:** All.
SBC-19625 / SBC-19754	The device resets upon receiving an illegal STUN request (incorrect integrity) **Applicable Products:** Mediant 1000.

2.30.5 Version 7.20A.256.721

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.5.1 Parameter Names Aligned with Microsoft Teams Optimization

The names of the following IP Group parameters have been modified to align with Microsoft's updated term for its media optimization feature - "*Media Optimization"* is now referred to as "*Local Media Optimization"*:

Previous Name	New Name
▪ Web: 'Teams Media Optimization Handling' ▪ CLI: `teams-media-optimization-handling` ▪ ini: IPGroup_TeamsMediaOptimization	▪ Web: 'Teams Local Media Optimization Handling' ▪ CLI: `teams-local-media-optimization-handling` ▪ ini: TeamsLocalMediaOptimization
▪ Web: 'Teams Media Optimization Initial Behavior' ▪ CLI: `teams-mo-initial-behavior` ▪ ini: IPGroup_TeamsMOInitialBehavior	▪ Web: 'Teams Local Media Optimization Initial Behavior' ▪ CLI: `teams-local-mo-initial-behavior` ▪ ini: TeamsLocalMOInitialBehavior

Note: This update does not support backward compatibility.

Applicable Application: SBC.

Applicable Products: All.

2.30.5.2 Resolved Constraints

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

Table 2-41: Resolved Constraints in Version 7.20A.256.721

Incident	Description
SBC-17606	The device fails to negotiate all DTMF RFC 2833 payload types in WebRTC calls. As a result, no audio is heard. **Applicable Products:** All.
SBC-18475	The device generates Syslog debug messages "ProcessRun failed process: '/acBin/Scripts/check_ipmi_service.sh'. status: 1 File:LinuxProcess.cpp Line:517". **Applicable Products:** Mediant Software.
SBC-18530	When the device is deployed on AWS and as an HA system, HA switchover fails when using UTC offset, because AWS doesn't support the timestamp argument for AWS API. **Applicable Products:** Mediant CE/VE (AWS).
SBC-18534	The device's Microsoft Teams Local Media Optimization support fails when STUN is behind NAT. As a result, no audio occurs. **Applicable Products:** All
SBC-18890	The device doesn't report MOS and delay for the outbound RTP direction. **Applicable Products:** All

2.30.6 Version 7.20A.256.715

This version includes resolved constraints only.

Note:

- This version is applicable only to Mediant 2600, Mediant 4000/B, Mediant 90xx, and Mediant Software.
- This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.6.1 Resolved Constraints

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

Table 2-42: Resolved Constraints in Version 7.20A.256.715

Incident	Description
SBC-19025	In a non-WebRTC to a WebRTC call, if the offer doesn't contain the 'mid' attribute and the WebRTC does contain it (e.g. 'a=mid:0'), and if the non-WebRTC side sends a new offer that contains 'mid', the offer towards the WebRTC contains a wrong value in the 'mid' attribute (not 0). **Applicable Products:** Mediant 2600, Mediant 4000/B, Mediant 90xx, and Mediant Software.

2.30.7 Version 7.20A.256.713

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.7.1 New Features

This section describes the new features introduced in this version.

2.30.7.1.1 TLS Version 1.3 Support

The device now supports TLS Version 1.3. As a result, the following configuration updates have been made to the existing TLS Contexts table:

- Additional optional values have been added to the 'TLS Version' parameter:
  - [8] TLSv1.3
  - [12] TLSv1.2 and TLSv1.3
  - [14] TLSv1.1 TLSv1.2 and TLSv1.3
  - [15] TLSv1.0 TLSv1.1 TLSv1.2 and TLSv1.3

  The existing value Any - Including SSLv3 (0) has been renamed "Any TLS 1.x", which now indicates support for only TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.

Note: SSLv3 is no longer supported as it's not sufficiently secure.

- New parameters for configuring a cipher list for TLSv1.3:
  - 'Cipher Server TLS1.3'
  - 'Cipher Client TLS1.3'
- New 'Key Exchange Groups' parameter for configuring groups that are supported for key exchange (applicable to all TLS versions):
  - X25519
  - P-521 (applicable only to Mediant 2600/4000/9000/Software)
  - P-256
  - P-384
  - X448
- Existing 'DH Key Size' parameter updates:
  - Default has changed to 2048.
  - New optional value 3072 (applicable only to Mediant 2600/4000/9000/Software)
  - Value 1024 is now displayed as "1024 – Not Recommended" (1024 is only available in the Web interface.)

  Above also affects the existing ‘Private Key Size’ parameter on the Change Certificates page.

Note: If the old (obsolete) Auto-Update related ini file parameter [AupdCipherString] was used for defining the TLS 1.0-1.2 cipher string and the device is upgraded to this software version, this parameter is ignored (i.e., no backward compatibility). Therefore, after upgrade, the TLS 1.0-1.2 cipher string must be configured in the TLS Contexts table ('Cipher Client' parameter).

Applicable Application: All.

Applicable Products: All.

2.30.7.1.2 Concealing Caller and Callee Fields in CDRs

The device can be configured to hide the values of the Caller and Callee fields in certain CDRs that are displayed by the device:

- SBC CDR History table (Web)
- Gateway CDR History table (Web)
- `show voip calls history` (CLI)
- `show voip calls active` (CLI)

An asterisk (*) is displayed instead of the actual value.

The feature is enabled by the new ini file parameter [CDRHistoryPrivacy] or CLI command `configure troubleshoot > cdr > cdr-history-privacy`.

Applicable Application: All.

Applicable Products: All.

2.30.7.1.3 Delay in Opening Voice Channel for Tel-to-IP Calls

The device can be configured to delay RTP (voice) with the FXO endpoint after it has received a SIP 200 OK response from the IP side. This delay may be useful in scenarios in which a 'click' noise is audible when the FXO interface (PBX) seizes the line. A delay in opening the voice channel eliminates this noise.

The feature is configured by the new ini file parameter [FXOVoiceDelayon200OK], which defines the time (in msec) to wait from receiving the 200 OK, before opening the voice channel with the FXO endpoint.

Applicable Application: Gateway (FXO).

Applicable Products: Mediant 5xx; Mediant 800; Mediant 1000.

2.30.7.2 Known Constraints

This section lists known constraints.

Table 2-43: Known Constraints in Version 7.20A.256.713

Incident	Description
SBC-17228	The device doesn't support deployment on the AWS cloud platform. **Applicable Products:** Mediant VE/CE.
SBC-18815	The CLI command `clear system-log` (which clears Syslog messages on the Web interface's Message Log page), deactivates the Message Log entirely and no further Syslog messages are displayed. **Applicable Products:** Mediant 9000.

Incident	Description
SBC-18933	When using Mozilla Firefox, the Web interface's Configuration Wizard doesn't display all templates (in the 'Template' field). A workaround is to exit and then re-access the wizard. **Applicable Products:** All.
SBC-19025	In a non-WebRTC to a WebRTC call, if the offer doesn't contain the 'mid' attribute and the WebRTC does contain it (e.g. 'a=MID:0'), and if the non-WebRTC side sends a new offer that contains 'mid', the offer towards the WebRTC contains a wrong value in the 'mid' attribute (not 0). **Applicable Products:** All.

2.30.7.3 Resolved Constraints

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

Table 2-44: Resolved Constraints in Version 7.20A.256.713

Incident	Description
SBC-13487	The device plays a harsh click noise when the FXO seizes the line. (This constraint has been resolved by new parameter FxoVoiceDelayOn200ok, as described in Section 2.30.7.1.3). **Applicable Products:** Gateway (FXO).
SBC-15627	The device crashes (resets) when running Hyper-V 2019 with Hyper-Threading. **Applicable Products:** Mediant VE/CE.
SBC-16277	The device erroneously reports many calls with bad MOS values, causing a Red color in OVOC (i.e., incorrect call quality reporting). **Applicable Products:** All.
SBC-16356 / SBC-17770	When the device is deployed on Azure, a noise (i.e., poor voice quality) in the RTP stream of SBC calls is heard when using DSP for transcoding. **Applicable Products:** All.
SBC-16922	Transcoding of SBC calls fails with "[ERROR] Board command failed - Internal error". **Applicable Products:** Mediant 800; Mediant 1000; Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.
SBC-16933	The device's maximum UDP port is limited to 11,219 for the Media Realm. (This constraint has been resolved by increasing maximum port range to 65,535, like all other products.) **Applicable Products:** Mediant 1000.
SBC-17016 / SBC-18386 / SBC-18654	SBC fax fails when the device receives a T.38 IP address of 0.0.0.0. **Applicable Products:** All.
SBC-17096	The device doesn't have the correct DSCP value in the outgoing SIP 100 Trying message. **Applicable Products:** All.

Incident	Description
SBC-17129	In the Local Users table, a user can be configured with User Level of "End User", which is only applicable to MSBR products. **Applicable Products:** All.
SBC-17137	The device fails to load (`copy dial-plan from`) the Dial Plan file through CLI with IPv6. **Applicable Products:** All.
SBC-17138	Some CLI commands are missing for supplementary services deactivation keys. **Applicable Products:** Gateway.
SBC-17240	The device doesn't support the IncrementalIniFileURL parameter in the SNMP interface. (This constraint has been resolved by the new MIB object, acSysHTTPClientIncrementalIniFileURL.) **Applicable Products:** All.
SBC-17248	When configuring a new Ethernet Group, its settings return to default after a device reset. **Applicable Products:** Mediant 9000.
SBC-17595 / SBC-17703	The device's Customize Access Level table cannot limit access to some Web pages (e.g., Web Service Settings page or Redundant Ethernet Port Information page). **Applicable Products:** All.
SBC-17684	The device sends the wrong SIP Request-URI domain in the ACK request message when message manipulation is done on the To header. **Applicable Products:** All.
SBC-17688	In the Upstream Groups table (for HTTP proxy and NGINX), the 'Name' field value cannot include dots (periods), and therefore, an FQDN cannot be configured for the name. **Applicable Products:** All.
SBC-17735	After a device reset, the device fails to perform DNS resolution for the Proxy Sets configured with FQDNs. **Applicable Products:** All.
SBC-17743	The device fails to add the SIP Record-Route header to the INVITE message after a REFER message. **Applicable Products:** All.
SBC-17745	A mismatch exists between the downloaded CLI script file and the uploaded CLI script file. In the downloaded CLI script, "Allowed Coder" appears after "IP Profile", which is why the script cannot be uploaded (should appear before). **Applicable Products:** All.
SBC-17758	The device doesn't increase the SDP version when SDP is changed, even if the far end doesn't change their SDP version. As a result, the call fails. **Applicable Products:** All.
SBC-17760	The device experiences a CPU overload because of the HTTP Proxy (NGINX) keep-alive mechanism. **Applicable Products:** All.
SBC-17781	The device doesn't change its destination MAC for Syslog/DR, even after the far end sends ARP\GARP. **Applicable Products:** All.

Incident	Description
SBC-17826	The device plays a held tone only for the first time that the call is put on hold (and not for subsequent on-hold scenarios). **Applicable Products:** All.
SBC-17838	The device doesn't reply to re-INVITE messages from the SIPREC SRS and as a result, the call fails. **Applicable Products:** Gateway.
SBC-17844	No CLI command exists for the device's Web interface's 'Forking Handling Mode' parameter (erroneously hidden). **Applicable Products:** Gateway.
SBC-17892	The device rejects the media offer with a SIP 488 response on a delayed offer call, even though media was established correctly. As a result, the call fails. **Applicable Products:** All.
SBC-17896	The device crashes (resets) upon a TLS negotiation timer issue. **Applicable Products:** All.
SBC-17925	The device's REST module init failed (allocation failure) error occurs. **Applicable Products:** Mediant CE.
SBC-18073	The device changes the RFC 2833 payload type in the re-INVITE response (i.e., incorrect DTMF). **Applicable Products:** All.
SBC-18089	Software upgrade fails due to insufficient disk space for writing the new .cmp file. **Applicable Products:** Mediant Software.
SBC-18132	The device generates Exception info when executing the DR command RT All in the CMDShell. **Applicable Products:** All.
SBC-18172	The User Defined Failure PM table (UserDefinedFailurePM) appears in the management interfaces of products that don't support this feature. (The feature is applicable only to Mediant 9000 and Mediant Software.) **Applicable Products:** Mediant 5xx; Mediant 800; Mediant 1000; Mediant 2600; Mediant 4000.
SBC-18185	The device handles STUN packets even though ICE-Lite is disabled. As a result, the call fails. **Applicable Products:** All.
SBC-18206	The device's User Registration Grace Time is limited to 2,000,000 sec. (This constraint has been resolved by increasing it to 15,500,000 sec.) **Applicable Products:** All.
SBC-18249	The device sends all RFC 2833 DTMF digits with the same timestamp. **Applicable Products:** All.
SBC-18258	When the device receives more than 17 forked SIP 183 responses in less than 120 msec, a lack of resources occurs. **Applicable Products:** All.
SBC-18310	The device stops sending SIP ladder messages (for OVOC SIP call flow diagrams) and QoE connection is lost. **Applicable Products:** All.

Incident	Description
SBC-18362	The device's NGINX Configuration file for OVOC Services is not valid. **Applicable Products:** All.
SBC-18414	The device sends the wrong crypto key in the SDP answer ('a=crypto'). As a result, media negotiation fails. **Applicable Products:** All.
SBC-18432 / SBC-18668 / SBC-18960	One-way voice occurs in WebRTC calls. **Applicable Products:** All.
SBC-18443	The device is missing the report of the latched IP address for calls behind NAT. **Applicable Products:** All.
SBC-18477	The new FXS Outdoor models (GTPM01046) port 2 and port 4 remain at 0 volts after a ground fault event. **Applicable Products:** Mediant 1000.
SBC-18504	The device increments the 'mid:0' value to 'mid:1' in the SDP offer in WebRTC calls, causing call failure. **Applicable Products:** All.
SBC-18526	Fax transcoding fails as the device cannot handle fax transcoding of two different G.711 coder types. **Applicable Products:** All.
SBC-18532	The active device in an HA system can ping the redundant device (Maintenance interface), even though a firewall rule should have blocked it. **Applicable Products:** HA.
SBC-18538	When the device uses the INIFILEURL parameter for provisioning, credentials are displayed in clear text in the Syslog (instead of being hidden). **Applicable Products:** All.
SBC-18582	The ENERGYDETECTORCMD parameter appears in the ini file. (Now, it has been removed as it's not applicable to the device.) **Note:** When upgrading the device to this version or later, the following Syslog message might be generated: "'ENERGYDETECTORCMD = 587202560', unknown parameter name". This message should be ignored. **Applicable Products:** All.
SBC-18814	WebRTC calls lose video after a re-INVITE for hold and then un-hold. **Applicable Products:** All.

2.30.8 Version 7.20A.256.511

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.8.1 Resolved Constraints

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

Table 2-45: Resolved Constraints in Version 7.20A.256.511

Incident	Description
SBC-17656	When recording Gateway calls, the device's SIPREC feature stops functioning when the SRS sends a SIP re-INVITE message. **Applicable Products:** Gateway.
SBC-18248	The device crashes (resets) when an SRTP SBC call is put on hold with RTP, and then un-hold with SRTP. **Applicable Products:** All.

2.30.9 Version 7.20A.256.399

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.9.1 Resolved Constraints

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

Table 2-46: Resolved Constraints in Version 7.20A.256.399

Incident	Description
SBC-17972	In the device's Web Interface Configuration Wizard, the 'Enabled' check box for OCT on the Remote Users wizard page cannot be cleared. **Applicable Products:** All

2.30.10 Version 7.20A.256.366

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.8.126 and EMS/SEM Version 7.2.3113.

2.30.10.1 New Features

This section describes the new features introduced in this version.

2.30.10.1.1 New Flex License Model for SBC Capacity Licenses

AudioCodes now offers a new licensing model for SBC capacity called *Flex License*. This model is similar to the existing Floating License model, but with the following differences:

- The Flex License is solely managed by OVOC; it doesn't employ a cloud-based license manager module like the Floating License. This reduces the exposure of OVOC to security risks from the public cloud.
- The Flex License enforces (gracefully) the purchased license pool capacity; the Floating License allows devices to exceed pool capacity and bills Customers at the end of the month for the extra license usages.

The Flex License model provides a central pool of purchased SBC licenses per license type—SBC sessions, transcoding sessions, and user registrations (far-end users)—which is managed solely by OVOC and shared among multiple devices. Each device can use as many licenses as it wants as long as the pool has available licenses. However, each device is obviously limited by its inherent maximum SBC capacity support, as well as an optional, additional user-defined capacity limitation (*Allocation Profiles*) per license type.

Devices periodically (typically, every 5 minutes) report their current license usage per license type to OVOC. Based on these reports, OVOC continuously calculates the remaining licenses in the pool per license type. As soon as pool capacity of a license type is reached (or temporarily exceeded), OVOC attempts to restore licenses to the pool by initially instructing a certain percentage of the devices (based on their *priority level* configured on OVOC) to reject new calls. This allows higher priority devices to continue providing call service. However, if license utilization is still at full capacity after a certain "graceful" period, OVOC also instructs the other devices to reject new calls. Only when the pool is replenished does OVOC allow the devices to accept new calls.

The Flex License feature also introduces the new SNMP alarm, acFlexLicenseManagerAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.144). This alarm is sent by the device when OVOC instructs it to reject new calls due to the Flex License pool capacity of a specific license type being reached ("over-license").

Device configuration for the Flex License is identical to the Floating License (enabling and Allocation Profiles). In addition, when the Flex License is used, the Web interface displays the following:

- The License Key page displays "Flex License" in the 'Mode' read-only field.
- The License Key page displays the Flex License pool's capacity per license type in the 'Flex' column under the SBC Capacity group.
- The Floating License page has a new group called Flex Pool, which displays the following:
  - Device's license utilization (%) of the pool per license type.
  - Status of license utilization of the pool per license type by all devices ("ok" if licenses remaining in pool or "overlicense" if no more licenses in pool).

The Flex License status can also be viewed in the CLI, using the existing command `show system floating-license`.

Applicable Application: SBC.

Applicable Products: All.

2.30.10.1.2 New AWS Metered License Model for SBC Capacity

When deployed on the Amazon Web Services (AWS) cloud computing platform, AudioCodes provides a new optional, licensing model for the device, called *Metered License*. This license model is based on the device's monthly consumption or usage (call duration). It offers a pay-as-you-go SBC service without any upfront fees, allowing Customers to easily adapt and improve responsiveness to changing business needs without overcommitting budgets. The Metered License model is similar to Amazon's On-Demand pricing model, where Customers are billed monthly based on service consumption.

Subscription to this licensing model and Customer billing is done through the Customer's AWS Marketplace account. Communication between the device and the AWS Marketplace is through HTTPS-based REST APIs.

The device sends periodic reports (every hour) to the AWS billing system, detailing its SBC service consumption in the last hour. The report includes usages, for example, total minutes of all calls, total minutes of transcoding calls, and total minutes of SIPREC calls. Usage is calculated monthly by AWS Marketplace, which it bills to the Customer's AWS account.

If the device fails to communicate with the AWS Marketplace API (where it sends its usage reports), the device begins rejecting new calls if connectivity is not restored after a graceful period. When this communication failure occurs, the device sends the new SNMP alarm acMeteringAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.146).

For setting up the Metered License model, refer to the *Mediant Virtual Edition SBC for Amazon AWS Installation Manual*.

Note: When the Metered License feature is used, the device's other OVOC-managed licensing models (i.e., Fixed License Pool and Floating License) cannot be used.

Applicable Application: SBC.

Applicable Products: Mediant VE.

2.30.10.1.3 OVOC Management of Devices behind NAT through WebSocket Tunnel

Note:

- This feature will be supported by OVOC in the next applicable OVOC release. For feature availability, please refer to the OVOC Release Notes.
- This feature is currently supported only for OVOC deployed on AWS. To check if supported on other cloud platforms, please refer to OVOC documentation.

Devices located behind NAT can now be managed by OVOC when it's deployed in a public cloud, by implementing WebSocket tunneling (over HTTP/S). In this tunneling application, the device is a WebSocket client and OVOC is the WebSocket server.

WebSocket tunneling has many advantages over the alternative method used up until now for connecting OVOC to the device when located behind NAT. The main advantage is that it easily resolves NAT traversal problems and requires less configuration (no need for port forwarding and no need for firewall settings to allow certain traffic).

The WebSocket tunnel connection is secure (HTTPS). When the device initiates a WebSocket tunnel connection, it verifies that the TLS certificate presented by OVOC is

signed by one of the CAs in the trusted root store of its default TLS Context (ID #0). The device authenticates itself with OVOC using username-password credentials, which must be the same as configured on OVOC.

This feature is configured on the device in the existing Web Service Settings page, using the following new parameters:

- 'OVOC WebSocket Tunnel Server Address' / WSTunServer / configure network > ovoc-tunnel-settings > address: Defines the OVOC WebSocket tunnel server's IP address or hostname.
- 'Path' / WSTunServerPath / configure network > ovoc-tunnel-settings > path: Defines the OVOC WebSocket tunnel server's path.
- 'Username' / WSTunUsername / configure network > ovoc-tunnel-settings > username: Defines the username for connecting to the OVOC WebSocket tunnel server.
- 'Password' / WSTunPassword / configure network > ovoc-tunnel-settings > password: Defines the password for connecting to the OVOC WebSocket tunnel server.
- 'Secured (HTTPS)' / WSTunSecured / configure network > ovoc-tunnel-settings > secured: Enables (default) secure (HTTPS) WebSocket connection.
- 'Verify Certificate' / WSTunVerifyPeer / configure network > ovoc-tunnel-settings > verify-server: Enables (default) certificate verification from WebSocket tunnel server.

Applicable Application: All.

Applicable Products: All.

2.30.10.1.4 Increased Capacity for Mediant VE on VMware

Mediant VE SBC installed on the VMware hypervisor provides increased capacity, by introducing new profiles and by using Hyper-Threading.

Guests (i.e., Mediant VE SBC) on VMware hypervisor do not inherit the Hyper-Threading capability of the host server. However, the new ini file parameter—CPUOverrideHT—has been introduced in this release to override this by enabling or disabling Hyper-Threading for Mediant VE on the host's server. The new recommended profiles for Mediant VE installed on VMware (listed in the table in Section 3.1 on page 165) require that Hyper-Threading is enabled on the server. Therefore, for these profiles, this parameter must be configured to 1 to enforce Hyper-Threading on the Mediant VE guest.

The recommended profiles improve capacity (including transcoding), by utilizing the Hyper-Threading capabilities of the host server. It also utilizes the enhanced performance capabilities of the Intel Xeon Scalable Processors (or later). For detailed capacity, see Section 3.3.14.1 on page 199.

Applicable Application: SBC.

Applicable Products: Mediant VE.

2.30.10.1.5 Interworking SIP 183 Cause Code and NTT ISDN Disconnect

For trunks configured for the Japanese NTT ISDN PRI (T1) variant, the device can be configured to send an ISDN Disconnect message if it receives a SIP 183 response with SDP containing a specific cause value (SIP status code) in the Reason header, in response to the device's sent INVITE message. The device maps (translates) the SIP cause code to an ISDN cause code in the Release Cause field of the outgoing Disconnect message. This feature is applicable to Tel-to-IP calls.

After the device sends the Disconnect message, it can send early media (e.g., an announcement) received from the IP side to the ISDN. If after sending the Disconnect message the device receives a SIP failure response (e.g., 4xx) or a 200 OK from the IP side, it sends a Release message to the ISDN. However, the device can be configured to send the Release only after a user-defined timeout (activated from when the Disconnect is sent) if no

SIP message is received. This timeout is configured using the new ISDNJapanNttTimerT305 parameter. If the device receives a SIP failure response or 200 OK before the timeout expires, it sends the Release instead of waiting for the timeout to expire.

The above behavior is configured using SIP Message Manipulation rules. For more information, refer to the device's *User's Manual*.

Applicable Application: Gateway (T1).

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

2.30.10.1.6 Call Destination Type in Routing Server Response

AudioCodes REST API-based routing by a third-party routing server or AudioCodes Routing Manager (ARM) can now be configured to indicate the SBC call destination type in its response to the device's getRoute request.

This is supported by the new "destType" attribute, which can be set to one of the following:

- "RequestUri" (SBC calls only): This value is typically used when the routing server receives a SIP REFER message, which should be handled by the device (i.e., for blind transfer). Upon receiving such a response, the device routes a new INVITE message according to the Request-URI header (such as the 'maddr' parameter). This URI is the same as in the SIP Refer-To header in the REFER request. Note that the SIP Interface and IP Profile are determined by the specified IP Group (see "DestGroup" attribute below).
- "DestGroup": This value instructs the device to send the call to an IP Group or Trunk Group, as indicated by the new "dstGroup" attribute. (This attribute is added by default.)
- "DestAddress": This value instructs the device to send the call to the destination URI as specified in the SIP message.

For more information, refer to the *REST API* document.

Applicable Application: SBC.

Applicable Products: All.

2.30.10.2 Known Constraints

This section lists known constraints.

Table 2-47: Known Constraints in Version 7.20A.256.366

Incident	Description
SBC-17565	Message Session Relay Protocol (MSRP) is not supported (and is not planned for future support). **Applicable Products:** Mediant CE.

2.30.10.3 Resolved Constraints

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

Table 2-48: Resolved Constraints in Version 7.20A.256.366

Incident	Description
SBC-16846	The device's jitter calculation is incorrect (and differs to that shown in Wireshark) when the device receives long DTMF digits for RFC 2833. (Therefore, the device sends incorrect jitter report to OVOC.) **Applicable Products:** All
SBC-17364	The device adds multiple attributes to the SDP due to Message Manipulation rules and loses all SDP resources. As a result, call failure occurs. **Applicable Products:** All
SBC-17551	The device uses wrong ports for media when video is added upon a SIP re-INVITE message. As a result, call failure occurs. **Applicable Products:** All
SBC-15824	When an IP Interface that is associated with a rule in the Firewall table is deleted, access to the device is lost and the device resets. **Applicable Products:** All
SBC-15855	No audio for three-way conference when the initiator of the conference receives an MLPP call. **Applicable Products:** Gateway
SBC-16356 / SBC-17770	The device adds noise to an SRTP-to-RTP transcoding SBC call when it receives a Contributing Source header in the SRTP packets. **Applicable Products:** All
SBC-16457	The device experiences high CPU utilization in Ver. 7.2.254 due to one of the tasks (TPNCP) running twice. **Applicable Products:** All
SBC-17067	The device crashes (resets) when it's accessed through SFTP using the latest Filezilla program. **Applicable Products:** All
SBC-17104 / SBC-17590 / SBC-17783	For some calls whose SIP endpoints are located behind NAT, the device opens the voice (RTP) channel to the wrong IP address. As a result, no audio occurs. **Applicable Products:** All
SBC-17114	The device adds an empty 'received=' parameter to the SIP Via header in the outgoing SIP message. **Applicable Products:** All
SBC-17164	The device crashes (resets) when it rejects a request, for example, because of remote authentication failure. **Applicable Products:** All
SBC-17717	The device's Signaling Component (SC) fails to start due to a full disk (bug in NGINX task). As a result, the device crashes (resets). **Applicable Products:** Mediant CE (Azure)

2.30.11 Version 7.20A.256.024

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.2144 and EMS/SEM Version 7.2.3113.

2.30.11.1 New Features

This section describes the new features introduced in this version.

2.30.11.1.1 ICE Lite for Teams Direct Routing (Mediant 1000B)

The device now supports Interactive Connectivity Establishment (ICE) Lite, which is required when operating in a Microsoft Teams Direct Routing (media bypass mode) environment.

The only required configuration for this feature is enabling ICE (STUN message handling) for the configuration entity representing Microsoft Teams. This is done using the new IP Profile parameter, 'ICE Mode' parameter (set to **Lite**).

Note: ICE Lite is already supported by the following products: Mediant 800, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant SW.

Applicable Application: SBC.

Applicable Products: Mediant 1000B.

2.30.11.1.2 Mediant VE Deployable on Google Cloud Platform

Mediant Virtual Edition (VE) SBC can now be deployed on the Google Cloud platform.

Applicable Application: SBC.

Applicable Products: Mediant VE.

2.30.11.1.3 Transcoding Capacity Updates for Mediant 9000 Rev. B / 9030 / 9080

Transcoding capacity has been increased for Mediant 9000 Rev. B / 9030 / 9080 SBCs. For updated capacity, see Section 3.3.10 on page 190 for Mediant 9000 Rev. B / 9080, and Section 3.3.12 on page 193 for Mediant 9030.

Applicable Application: SBC.

Applicable Products: Mediant 9000 Rev. B; Mediant 9030; Mediant 9080.

2.30.11.1.4 Push Notification Service

The device supports call handling of users registered to a Push Notification Service (PNS), per IETF draft "Push Notification with the Session Initiation Protocol (SIP)". This service is used to "wake" devices (typically, mobile phones) and operating systems that have gone to "sleep" (to save resources such as battery life), so that they can receive traffic.

Typically, each operating system uses a dedicated PNS. For example, Apple iOS devices use the Apple Push Notification service (APNs) while Android devices use the Firebase Cloud Messaging (FCM) service. Without using a PNS to "wake" SIP User Agents (UAs), the UAs wouldn't be able to send binding refresh SIP REGISTER requests, receive SIP requests (e.g., INVITE), or send periodic keep-alive messages for maintaining connectivity with SIP servers.

The device interfaces with a third-party RESTful server that serves as a proxy to the various Push Notification Servers deployed in the customer's network. The RESTful server is configured on the device as a Remote Web Service (HTTP host).

The device supports the Push Notification Service parameters that are used to indicate this service over SIP. These parameters are sent by the user in the Contact header of REGISTER requests (and saved with the user's contact details in the device's registration database):

- 'pn-provider': Specifies the type of PNS service
- 'pn-prid': Specifies the unique identifier used by the PNS to identify the user
- 'pns-param': (Optional) Specifies additional implementation-specific data required by the PNS

Below is an example of a REGISTER message containing these parameters (**bolded**):

```
REGISTER sip:alice@example.com SIP/2.0
Via: SIP/2.0/TCP
alicemobile.example.com:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: Alice <sip:alice@example.com>
From: Alice <sip:alice@example.com>;tag=456248
Call-ID: 8438176376842309@998sdasdh09
CSeq: 1826 REGISTER
Contact: <sip:alice@alicemobile.example.com;
  pn-provider=acme;
  pn-param=acme-param;
  pn-prid=ZTY4ZDJlMzODE1NmUgKi0K>
Expires: 7200
Content-Length: 0
```

This feature is configured by the following new parameters:

- Push Notification Servers table (PushNotificationServers / `configure voip > sip-definition push-notification-servers`): Defines the type of Push Notification Service ('pn-provider' value), the Push Notification Server's address (configured as a Remote Web Service), and the protocol for communication with the Push Notification Server (currently, JSON format).
- PNSReminderPeriod (`configure voip > sbc settings > pns-reminder-period`): Defines the time (in seconds) before user registration expires at which the device sends a push notification request (through the Push Notification Sever) to remind the user to send a refresh REGISTER.
- PNSRegisterTimeout (`configure voip > sbc settings > pns-register-timeout`): Defines how long (in seconds) the device waits for a refresh REGISTER from the user after it has sent a push notification request due to an incoming SIP dialog-initiating request (e.g., INVITE) for the user.

For more information, refer to the device's *User's Manual*.

Applicable Application: SBC.

Applicable Products: All.

2.30.11.1.5 Remote Monitoring of Device behind NAT

When the device is located behind NAT, it can now send periodic reports to a third-party monitoring server (configured on the device as a Remote Web Service / HTTP host). The reports can include device status (e.g., software version, configuration entities such as IP Groups, and serial number), active alarms, key performance indicators (e.g., number of active SBC sessions and average call duration), and user registration status. The reports are sent over HTTP/S using RESTful API (in JSON format), where the device acts as the client.

The feature is configured by the following:

- The existing Web Service Settings page provides a new group called Remote Monitoring, which provides the following new parameters:
  - 'Remote Monitoring': Enables the feature
  - 'Reporting Period': Defines the interval between sent reports
  - 'Device Status': Enables inclusion of device status in reports
  - 'Active Alarms': Enables inclusion of active alarms in reports
  - 'Performance Indicators': Enables inclusion of performance indicators in reports
  - 'Registration Status': Enables inclusion of user registration status in reports
- The 'Type' parameter in the Remote Web Services table now provides an additional optional value--Remote Monitoring [10]—which if selected, indicates that the monitoring reports must be sent to this Remote Web Service (HTTP host). This option can be configured for only one Remote Web Service.
- A new SNMP alarm, acRemoteMonitoringAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.145) is sent (with Warning severity) when the device receives an HTTP failure (4xx/5xx/6xx) response from the Remote Web Service, and cleared when it receives a successful (2xx).

Applicable Application: All.

Applicable Products: All.

2.30.11.1.6 Proxy Keep-Alive for Active Proxy Server Only

Up until now, when the device was enabled to send keep-alive SIP OPTIONS messages to proxy servers belonging to a Proxy Set, it sent them to all the proxies regardless of the configured redundancy mode (parking or homing), configured by the 'Redundancy Mode' parameter. Now, the device can be configured to regard the redundancy mode, using the new optional value **Using OPTIONS on Active Server** for the existing 'Proxy Keep-Alive' parameter in the Proxy Sets table:

- Parking mode: The device sends keep-alive OPTIONS messages only to the currently active proxy server.
- Homing mode: The device sends keep-alive OPTIONS messages to the currently active proxy server as well as to all servers (offline) with higher priority than the active server. Once a higher priority server comes online, the device stops sending OPTIONS to the previously active server and connects to this higher priority server. The device now sends keep-alive messages to it and all servers (offline) with higher priority.
- If the 'Redundancy Mode' parameter is not specified and the 'Proxy Load Balancing Method' parameter is configured to any value other than **Disable**, the device sends keep-alive OPTIONS messages to all active proxy servers (same behavior as if the Proxy Keep-Alive parameter was configured to **Using OPTIONS**).

Applicable Application: All.

Applicable Products: All.

2.30.11.1.7 Automatic Topology Hiding in SIP Messages

Topology hiding in SIP messages has been enhanced to consider SIP headers concerned with the source (e.g., From) and destination (e.g., To) of the message. This feature replaces the host part of URIs in specific headers with a user-defined hostname or an IP address. In this way, the real hostname or IP address of the communicating SIP User Agents (UAs) are hidden from one another.

The IP Group parameter, 'SIP Topology Hiding Headers List' (IPGroup_TopologyHidingHeaderList) that was added in a previous release for SIP topology hiding is now obsolete and has been replaced by the following new parameters:

- 'SIP Source Host Name' IP Group parameter (IPGroup_SIPSourceHostName / `sip-source-host-name`): Defines a hostname that overwrites the hostname of the source URI in specific SIP headers.
- 'SIP Topology Hiding Mode' (SIPTopologyHidingMode / `configure voip > sbc settings > sip-topology-hiding-mode`): Enables the device to overwrite the host part in SIP headers with IP addresses, unless the relevant IP Group's hostname parameters ('SIP Group Name' and 'SIP Source Host Name') are configured.

For more information, refer to the device's *User's Manual*.

Applicable Application: SBC.

Applicable Products: All.

2.30.11.1.8 SNMP Alarm for Faulty MPM Module on Mediant 4000

A new SNMP alarm, AcDSPFarmsMismatchAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.143) has been added, which indicates if an MPM module is faulty, not installed correctly, or missing from the chassis.

The device sends the alarm if the number of MPM modules that is configured by the new ini file parameter, DspFarmsInstalledNum (default is 0) is greater than the actual number of physical MPM modules installed in the chassis. The alarm and the parameter are typically used to check that all required MPMs are present and correctly installed in the device's chassis.

Applicable Application: SBC.

Applicable Products: Mediant 2600; Mediant 4000.

2.30.11.1.9 SNMP Performance Monitoring for G.711 A-law and G.711 U-law

The existing SNMP Performance Monitoring MIB acPMChannelsPerCoderTable doesn't distinguish between G.711 A-law and G.711 µ-law (U-law) coders, but combines these two G.711 flavors into its count. This new feature provides a new Performance Monitoring MIB, acPMChannelsPerCoderG711Table (OID 1.3.6.1.4.1.5003.10.7.2.26), which distinguishes between these two coders, showing separate counts per coder.

Applicable Application: All.

Applicable Products: All.

2.30.11.1.10 Web Login 'Remember Me' Renamed

The 'Remember Me' check box on the Web Login page (displayed when accessing the device's web interface) has been renamed to 'Remember Username'. This was done to reflect the check box's functionality, which is to remember the username (and not password) for future login attempts ('Username' field is automatically populated).

Applicable Application: All.

Applicable Products: All.

2.30.11.1.11 No Reply Time is Saved when Call Forward Rule Deactivated

When an active call forwarding rule is deactivated in the Call Forward table (i.e., 'Type' field changed to **Deactivate**), the value that was configured in the 'No Reply Time' field is now maintained. Up until now, the 'No Reply Time' value reverted to default (30) when the rule was deactivated.

Applicable Application: Gateway.

Applicable Products: Analog Gateways.

2.30.11.1.12 Max. Characters Increased for Prefix and Tag in Dial Plan Rules

The maximum number of characters that can be configured in the 'Prefix' and 'Tag' fields in the Dial Plan Rule table has been increased to 120.

Applicable Application: All.

Applicable Products: Mediant 9000; Mediant SW.

2.30.11.1.13 Media-related CDR Fields in CALL_END (Signaling) CDRs

Media-related CDR fields can now be added to CALL_END CDRs (sent at the end of calls), which, by default, contain only signaling-related CDR fields. These fields are added by customizing the CDR, using the existing SBC CDR Format table. The media-related CDR fields are selected from the table's 'Field Type' parameter, which now also lists media-related CDR fields (e.g., Local MOS CQ and Local Packet Loss).

This CDR customization is applicable only when the 'CDR Type' parameter is configured to Syslog SBC, Local Storage SBC, or RADIUS SBC.

Note: When the SBC session includes multiple media streams, the added media fields represent only the first audio media.

Applicable Application: SBC.

Applicable Products: All.

2.30.11.1.14 Allocation of DSPs on SDP Answer

The device can now be configured to allocate DSPs (if available and required) at the SDP Answer stage (instead of at the SDP Offer stage), which is the stage that determines if the call requires DSPs (for example, for transcoding).

Up until now (and by default), the device's allocation of DSP resources for calls was done at the SDP Offer stage. If DSP resources were available at this stage, the device reserved DSPs for the call just in case call setup succeeded with the SDP Answer and DSPs were required. If there were no free DSP resources at the SDP Offer stage, no DSP resources were allocated for the call at any stage of the SDP Offer-Answer exchange.

However, this default behavior may cause call failure when DSPs are required, even if DSP resources are available. For example, assume the device is licensed for 10 concurrent transcoding calls and is currently handling the setup of 10 calls where only 5 require transcoding (DSPs). For all these calls, the device allocates DSPs during the SDP Offer stage. If during this time the device starts processing an 11th call that requires transcoding, since it has already allocated all its DSP resources, it has no free DSPs to allocate this call and as a result, the device rejects the call.

To avoid such scenarios, the device can be configured to allocate DSPs only at the SDP Answer stage (SIP 200 OK or 180), when it can determine if DSPs are required or not for the call. If DSPs are required and DSP resources are available, the device allocates the call DSPs; if there are no available DSPs, the device rejects the call.

This feature is configured by setting the new parameter, 'Reserve DSP on SDP Offer' (ReserveDSPOnSDPOffer / `configure voip > sbc settings > reserve-dsp-on-sdp-offer`) to **Disable**.

Applicable Application: SBC.

Applicable Products: All.

2.30.11.1.15 Free WebRTC Sessions in Evaluation License Key

The device's free evaluation License Key (which includes up to three concurrent SBC sessions) now also offers up to three concurrent WebRTC sessions for evaluation purposes.

Note: For post-evaluation deployment, this evaluation License Key cannot be used. Instead, a new License Key must be purchased with the required WebRTC sessions and any other features that may be required.

Applicable Application: SBC.

Applicable Products: Mediant VE/SE/CE.

2.30.11.1.16 Additional Supported SIP Responses

The device now recognizes (and acknowledges them in generated Syslog messages) the receipt of the following additional SIP response codes:

- 204 (No Notification)
- 424 (Bad Location Information)
- 428 (Use Identity Header)
- 429 (Provide Referrer Identity)
- 436 (Bad Identity Info)
- 437 (Unsupported Credential)
- 438 (Invalid Identity Header)
- 439 (First Hop Lacks Outbound Support)
- 440 (Max-Breadth Exceeded)
- 470 (Consent Needed)

Applicable Application: All.

Applicable Products: All.

2.30.11.1.17 Delay Time for Resending Failed SIP OPTIONS Keep-Alive Messages

The device can now wait a user-defined duration (in seconds) before re-sending a SIP OPTIONS keep-alive message to the SIP proxy server after receiving a failed SIP response from the previously sent keep-alive message. The feature is configured by the new ini file parameter, FailedOptionsRetryTime.

Applicable Application: All.

Applicable Products: All.

2.30.11.1.18 Configuration of Active Device during HA Synchronization

During High-Availability (HA) synchronization between Active and Redundant devices, configuration operations can now be performed on the Active device. HA Synchronization occurs, for example, during Hitless Software Upgrade and after an HA switchover. Up until now, configuration was blocked during HA synchronization.

Applicable Application: All.

Applicable Products: Mediant 500; Mediant 800; Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.

2.30.11.1.19 Microsoft Teams Optimization Update

This feature provides a configuration update when the device is deployed in a Microsoft Teams environment for Media Optimization. How the device (i.e., central SBC in the proxy SBC scenario) initially sends the INVITE message with the SDP Offer from the remote SBC to Teams can now be configured. The SDP Offer can be sent as is, or with the "internal" or "external" (regular) Media Realm. If sent as is, the device indicates that the call is intended as a direct media call. If sent with the "internal" or "external" Media Realm, the device indicates that the call is intended as a non-direct media call.

The feature is configured by a new IP Groups table parameter, 'Teams Media Optimization Initial Behavior' (IPGroup_TeamsMOInitialBehavior).

Applicable Application: SBC.

Applicable Products: All.

2.30.11.1.20 Third-party Routing Server Fallback to SBC IP-to-IP Routing Table

When using a third-party routing server, the device can now be triggered by the server to use its IP-to-IP Routing table to route the call. This behavior is triggered if the routing server's response to the device's HTTP Get Route request includes the REST API command 'action' set to the newly supported 'continue' value.

To route the call, the device uses the routing rule whose 'Alternative Route Options' parameter is configured to **Route Row** and which is located below the original routing rule ('Destination Type' set to **Routing Server**) used to initially query the routing server. This routing can be used at any stage of the call (e.g., after alternative routing failure by the Routing server or after receiving a REFER/3xx).

Applicable Application: All.

Applicable Products: All.

2.30.11.2 Known Constraints

This section lists known constraints.

Table 2-49: Known Constraints in Version 7.20A.256.024

Incident	Description
SBC-16988	When the device is accessed from OVOC (Single Sign On) over WebSocket tunneling, software upgrade doesn't function if the WebSocket session timeout is not configured to 30 minutes. **Applicable Products:** All
SBC-17056	When the device is accessed from OVOC (Single Sign On) over WebSocket tunneling, the SBC Configuration Wizard is not supported. **Applicable Products:** All
SBC-21292	When remote monitoring is enabled, the device sends only the first 100 (Mediant 2600, Mediant 4000, Mediant 9000, Mediant Software) or 40 (Mediant 5xx, Mediant 800, Mediant 1000, MP-1288) IP Groups and only the first 100 Network Interfaces, to the HTTP endpoint (all other IP Groups are ignored). **Applicable Products:** All

2.30.11.3 Resolved Constraints

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

Table 2-50: Resolved Constraints in Version 7.20A.256.024

Incident	Description
SBC-12969	The device's firewall (Access List) doesn't function when changing the IP Interface or the Ethernet Device table ('Underlying Interface' field) of a related firewall rule. **Applicable Products:** All
SBC-13964 / SBC-15612	When the device has FXS and FXO interfaces and the License Key has "FXS=0", FXO registration fails. **Applicable Products:** Gateway
SBC-14416	A user with Administrator level privileges can upload files (through REST) to the device even though this action is allowed only by users with Security Administrator level or higher. **Applicable Products:** All
SBC-14419	A user with Administrator privileges can use the File Upload function even though it is hidden from the Web interface. Therefore, any user with access to the device can access certain Web application resources without having to provide credentials. In other words, Cross Site Request Forgery (CSRF) is not functioning correctly. **Applicable Products:** All
SBC-14539	An attacker without logging in may be able to cause Denial of Service (DoS) because the option to initiate SSL renegotiation as a client can be used for DoS attacks. **Applicable Products:** All
SBC-15646	When the device is configured to classify calls by Proxy Set, it fails to modify the proxy IP addresses resolved from DNS. Therefore, classification of the call fails. **Applicable Products:** All

Incident	Description
SBC-15709	The device allows SSH access to the device by a Security Administrator user that was deleted. **Applicable Products:** All
SBC-15750	The device doesn't close the TCP socket after a TLS call is disconnected. **Applicable Products:** All
SBC-15753	For SIPREC, the device includes only one Participant ID in the XML body of the SIP INVITE that it sends to the SRS. **Applicable Products:** All
SBC-15846	The device's Web interface's Customize Access Level table is missing the Call Admission Control Profile table. **Applicable Products:** All
SBC-15870	The device sends a SIP UPDATE message to the outgoing leg after a PRACK message for Media Sync. As a result, the call fails. **Applicable Products:** All
SBC-15878	The device sometimes doesn't display the correct duration in the CDR for long calls. **Applicable Products:** All
SBC-15894	SSH access with an RSA Public Key for the Monitor user doesn't function. **Applicable Products:** All
SBC-15903	SSH access with key authentication doesn't function. **Applicable Products:** All
SBC-15960	The device can import a corrupted dial plan (i.e., device doesn't validate the .csv file beforehand). **Applicable Products:** All
SBC-15987	The device's Message Manipulation rule for the SIP User-To-User header fails (duplicates content). **Applicable Products:** All
SBC-16058	The device's Customize Access Level table doesn't function for Active Alarms and Alarms History. **Applicable Products:** All
SBC-16298	The redundant Signaling Component device crashes (resets) when it receives control packets during scale-in process. **Applicable Products:** Mediant CE
SBC-16344	The device removes RFC 2833 from the SDP answer. **Applicable Products:** All
SBC-16382	The device crashes (resets) because of "no more release descriptors". **Applicable Products:** All
SBC-16454	The device's ICE candidates are not changed when the local address is changed (i.e., ICE negotiation fails). **Applicable Products:** All
SBC-16476	The device crashes (resets) due to lack of resources. **Applicable Products:** All

Incident	Description
SBC-16503	The device issues a parsing error when performing normalization Message Manipulation rules on an outgoing SIP INVITE message. As a result, the call failures. **Applicable Products:** All
SBC-16510	The device fails to open the voice on a loopback call with ICE Lite. As a result, no audio occurs. **Applicable Products:** All
SBC-16596	The device rejects registrations on high rate when the "SBC" license key is small, even though the "FEU" license key is ok. **Applicable Products:** All
SBC-16600	The device's firewall rules (Firewall table) doesn't function for domain names after the device resets. **Applicable Products:** All
SBC-16636	The Mediant CE in Azure fails to upgrade due to insufficient space for the new .cmp file. **Applicable Products:** Mediant CE
SBC-16691	The device crashes (resets) when attempting an SSH connection with the device using FileZilla (which inundates it with commands). **Applicable Products:** All
SBC-16775	The device generates CPU overload messages for task SPLB after the TLS certificate is replaced. (Resolved by parameter FailedOptionsRetryTime.) **Applicable Products:** All
SBC-16777	Mediant CE in Azure sends QoE disconnect alarms every 15 minutes. **Applicable Products:** Mediant CE
SBC-16787	Mediant CE in Azure doesn't traverse DTMF on early media when there is no prior RTP. As a result, DTMF transcoding fails. **Applicable Products:** Mediant CE
SBC-16840	The device rejects a SIP 200 OK for a re-INVITE on fax transcoding (T.38 to G.711). As a result, the fax fails. **Applicable Products:** All
SBC-16853	The device adds a timestamp on the last line of syslog CDRs (should be removed). **Applicable Products:** All
SBC-16855	The device disconnects Tel-to-IP calls with "Purge connected call" messages (calls fail). **Applicable Products:** All
SBC-16860	The device changes the 'a=crypto' tag on a SIP re-INVITE offer even though the SDP Offer from the other side was not changed. As a result, the call fails. **Applicable Products:** All
SBC-17010	The device doesn't send a re-INVITE session-refresh when configured to not support call hold (IPProfile_SBCRemoteHoldFormat = 6). As a result, the SBC call fails. **Applicable Products:** All
SBC-17125	The device crashes (resets) when TCP\TLS connection to OVOC terminates. **Applicable Products:** All

Incident	Description
SBC-8825 (VI-154358)	The device's Web interface (Monitor page) doesn't display the redundant power supply unit. **Applicable Products:** Mediant 9000

2.30.12 Version 7.20A.254.565

This version includes known constraints and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.2144 and EMS/SEM Version 7.2.3113.

2.30.12.1 Known Constraints

This section lists known constraints.

Table 2-51: Known Constraints in Version 7.20A.254.565

Incident	Description
SBC-16112	In some Google Cloud locations (e.g. us-central-1), it may take up to 10 sec. for Load Balancer to discover and fully process changes in the backend servers state. When deploying Mediant VE in HA configuration, this may translate into outages in the media path during a switchover. As a workaround, consider deploying Mediant VE in a different location. This does not affect Mediant CE deployments where the media path doesn't pass through the Load Balancer. **Applicable Products:** Mediant CE

2.30.12.2 Resolved Constraints

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

Table 2-52: Resolved Constraints in Version 7.20A.254.565

Incident	Description
SBC-14417	Logging into the device's CLI (USB, SSH, Telnet, Web) triggers a buffer overflow, which causes a reset (i.e. denial of service attack) and potentially allows a break-in into the underlying operating system and a full takeover of the CPU. **Applicable Products:** All
SBC-15404	The device crashes (resets) upon receiving a SIP INVITE message in a "race" condition for forked calls. **Applicable Products:** All
SBC-15789	The device crashes (resets) upon receiving long SIP messages with ARM and when the Logging Filters feature is enabled. **Applicable Products:** All

Incident	Description
SBC-16094	The device crashes (resets) on "TASK: VQM upon resetting the socket between the SBC and the OVOC". **Applicable Products:** All
SBC-16219 / SBC-16384 / SBC-16498	The device's Web GUI doesn't display the trusted root certificate. **Applicable Products:** All
SBC-16230	The device crashes (resets) when the Floating License Key is enabled and the user logs into the device through SSH with a long login password. **Applicable Products:** All
SBC-16346	When the device is installed on Azure and the LDAP Server Group configured for 'Type' Control (in the LDAP Server Groups table) is removed through the Web interface, the device crashes (resets). **Applicable Products:** Mediant CE (Azure)
SBC-16422	The device (installed on Azure) crashes (resets) due to keep-alive (TASK: CEMT). **Applicable Products:** Mediant CE (Azure)
SBC-16520	When using a non-default logo for the Web interface, it's not displayed when using Internet Explorer browser. **Applicable Products:** All

2.30.13 Version 7.20A.254.475

This version includes new features and resolved constraints.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.2125 and EMS/SEM Version 7.2.3113.

2.30.13.1 New Features

This section describes the new features introduced in this version.

2.30.13.1.1 Multiple Client-Initiated TLS Renegotiations Blocked

The device can now be configured to block client-initiated TLS renegotiations (handshakes). This is useful for preventing Denial-of-Service (DoS) attacks on the device caused by multiple TLS renegotiations per second of the encrypted key initiated by the attacker.

The feature is supported by the new TLS Contexts table parameter, 'TLS Renegotiation' (TLSContexts_TlsRenegotiation / tls-renegotiation). For backward compatibility, TLS renegotiations is enabled by default.

Applicable Application: All.

Applicable Products: All.

2.30.13.1.2 Minimum Length of Complex Login Passwords

For complex login passwords for device management users (enabled by the existing EnforcePasswordComplexity parameter), the minimum number of required characters in the password can be configured. This is done using the new parameter, MinWebPasswordLen (configure system > web >min-web-password-len).

Applicable Application: All.

Applicable Products: All.

2.30.13.1.3 Compatibility with Microsoft's Emergency E9-1-1 Call ELIN Update

The device supports Microsoft's latest emergency call (E9-1-1) handling using their new <ELIN> XML tag for indicating the Emergency Location Identification Number (ELIN) number (911 caller) in the PIDF-LO body of the SIP message. This tag has replaced the former <NAM> tag (which is still supported by the device for backward compatibility). This change applies to both Skype for Business and Teams environments.

Applicable Application: All.

Applicable Products: All.

2.30.13.1.4 Microsoft Teams with Media Path Optimization Support

This feature is intended for complex environments consisting of a single core SBC device integrated in a Microsoft Teams environment and consisting of multiple branch SBCs (or Gateways). In this environment, the core SBC determines the optimal path for Teams calls, based on connectivity (and then voice quality). The device determines the media path from Microsoft proprietary headers (X-MS-UserLocation and X-MS-MediaPath) received in the incoming SIP message. Based on these headers, the device selects the appropriate Media Realm (regular or "internal) for the IP Group to which the incoming call belongs.

To support the feature, the following new parameters have been added to the IP Groups table:

- 'Teams Media Optimization Handling' / IPGroup_TeamsMediaOptimization / configure voip > ip-group > teams-media-optimization-handling: Defines if the device uses the Teams headers to determine the media path (Media Realm), and if so, which headers to uses. By default, the device ignores the headers.
- 'Internal Media Realm' / IPGroup_InternalMediaRealm / configure voip > ip-group > internal-media-realm-name: Assigns an "internal" Media Realm, which is used for the call if the X-MS-UserLocation header value is "Internal".

Applicable Application: SBC.

Applicable Products: All.

2.30.13.1.5 SBC Configuration Wizard for Alcatel-Lucent Remote Users

The device's SBC Configuration Wizard has been enhanced to include configuration for the Alcatel-Lucent Remote Users application. When this application is selected, the wizard provides an additional IP-PBX configuration page ("IP-PBX3") as well as a new group ("OTC IP PHONE (KAMAILIO)" of parameters for IP phone configuration on the existing Remote Users wizard page.

Applicable Application: SBC.

Applicable Products: All.

2.30.13.2 Resolved Constraints

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

Table 2-53: Resolved Constraints in Version 7.20A.254.475

Incident	Description
SBC-16084	Topology hiding using the IP Group parameter 'SIP Topology Hiding Headers List' (IPGroup_TopologyHidingHeaderList) has limitations. Therefore, the parameter has been removed and will be replaced by an enhanced topology hiding feature in Version 7.20A.256. **Applicable Products:** All
SBC-14403	When uploading a new certificate to the device's Trusted Root Certificates of the default TLS Context, the device crashes (resets). **Applicable Products:** All
SBC-14413	The device is exposed to a security vulnerability whereby some cookies containing session-relevant or confidential information are not protected by security-relevant flags. This can facilitate an attacker’s access to the content of these cookies. **Applicable Products:** All
SBC-14415	The device is exposed to a security vulnerability due to short password lengths. If the EnforcePasswordComplexity parameter is enabled, the password length is limited to 8 characters. (Now, the constraint has been resolved by the new parameter MinWebPasswordLen, which defines the minimum number of characters in the password.) **Applicable Products:** All
SBC-14418	The device is exposed to a security vulnerability as some of its configuration resources can be accessed by simply using the correct URL to the configuration resource page and credentials to access them are not required. **Applicable Products:** All
SBC-14539	An attacker without logging in might be able to cause a Denial-of-Service (DoS) attack, using multiple client-initiated TLS renegotiations (handshakes). (Now, this has been resolved by the new parameter TlsRenegotiation in the TLS Context table, which can be configured to disable TLS renegotiation.) **Applicable Products:** All
SBC-14670 / SBC-15515 / SBC-15824	When the device loses TLS connection with OVOC, it experiences a CPU overload caused by new TLS connection attempts from OVOC (due to the VQMM task). **Applicable Products:** All
SBC-14710	The device's Allowed Audio Coders table doesn’t list the T.38 and Transparent coders. **Applicable Products:** All
SBC-15035	The device experiences video delay upon call establishment. **Applicable Products:** All
SBC-15110	The device doesn't support direct media (bypass) for a new INVITE message due to a terminating REFER message (call transfer). As a result, one-way voice occurs. **Applicable Products:** All
SBC-15346	The device doesn't show in the Syslog an SDP that contains a binary ISUP body that is added by Message Manipulation. **Applicable Products:** All

Incident	Description
SBC-15367 / SBC-15755 / SBC-15864	If the peer side doesn't support re-INVITE/UPDATE messages and the device receives an INVITE message containing a Replaces header, it generates the error "HandleCoreMediaNegotiateEv Media Negotiation isn't supported". As a result, the call fails. **Applicable Products:** All
SBC-15369	The device stops sending SIP ladder messages to OVOC during high traffic when all buffers are full and doesn't recover from it. **Applicable Products:** All
SBC-15414	When installing the device on Azure, the device receives the "Unsupported API version" error because of the unsupported un-escape &, < and > characters in Azure's username/password. As a result, installation on Azure fails. **Applicable Products:** Mediant Software SBC (Azure)
SBC-15435 / SBC-15636	When an SBC call has multiple coders in the SDP Answer and DSP is required due to DTMF transcoding, the device sends a re-INVITE message to both sides with fax coders instead of RTP with a single coder. As a result, no voice occurs. **Applicable Products:** All
SBC-15445	The device adds static noise when it opens a channel with DSP and CN is received, causing poor voice quality. **Applicable Products:** All
SBC-15507	When the 'Primary DNS' or 'Secondary DNS' parameters are configured through the SBC Configuration Wizard, their settings are not applied to the device configuration. **Applicable Products:** All
SBC-15517	The 'SIP Group Name' parameter in the IP Groups table can't be configured (i.e., invalid IP Group) with an IP address and port combination (e.g., 194.90.179.0:5083). **Applicable Products:** All
SBC-15521	The device sends CALL_CONNECT CDRs after SIP 200 OK responses (instead of after ACK responses). **Applicable Products:** All
SBC-15527	The device crashes (resets) after the CLI command `show voip calls history gw` is run. **Applicable Products:** Gateway
SBC-15541	For Call Setup Rules (CSR) to HTTP (asynchronous rule), if the CSR exits with a "false", the device doesn't go to the next rule, but runs the same rule again and again (loop). As a result, the call fails. **Applicable Products:** Gateway
SBC-15542	The device considers an incoming STUN packet as an RTP voice packet, and then stops playing RTP. As a result, no voice occurs. **Applicable Products:** All
SBC-15543	The device incorrectly detects a fax tone when an iPhone that is close to the handset of the call party issues a default notification sound. **Applicable Products:** Gateway
SBC-15555	The device crashes (resets) when a user runs multiple Python scripts through SSH (consuming all the device's CLI resources). **Applicable Products:** All

Incident	Description
SBC-15580	The device cannot process dial plans configured with a prefix/suffix number containing more than 9 digits, for example, [1234567890]. (Now, a dial plan can be configured with up to 19 digits, for example, [1234567891234567890-1234567891234567899]. **Applicable Products:** All
SBC-15614	The device sends RTP instead of SRTP (as configured) to the SIPREC SRS server for RTP-RTP calls. As a result, SIPREC fails. **Applicable Products:** All
SBC-15633	The device is exposed to a security vulnerability as users with Monitor level can run the CLI command `show running config` and therefore, obtain login information of the valid Administrator user. (Now, the Local Users table is only included in the output of the command if run when in Privileged User command mode.) **Applicable Products:** All
SBC-15645	The device crashes (resets) when processing a Message Manipulation rule to normalize a SIP message where the user part is long, causing corruption in memory. **Applicable Products:** All
SBC-15702	The device sends a SIP 200 OK without SDP in response to an INVITE message with delayed Offer for a specific call flow scenario: 1) A sends a delayed Offer and the device sends B an Offer with SDP, 2) B answers with 18x with SDP and the device sends it to A as an Offer, 3) when B sends a 200 OK with the same SDP, it is removed because it is the same. As a result, the call fails. **Applicable Products:** All
SBC-15721	For a SIPREC call, the device sends an INVITE message to the SRS without the 'a=label:1' and 'a=label:2' media labels. Instead, it sends "a=label:main-audio" in each media. As a result, SIPREC fails. **Applicable Products:** All
SBC-15823	When the device is installed on Hyper-V, no voice occurs when using VLAN tagging. **Applicable Products:** Mediant Software
SBC-15825	The device duplicates an SDP attribute ("a=rtcp-fb:* ccm fir") during high traffic. **Applicable Products:** All
SBC-15871	Static Route validation failure is generated upon an HA switchover. **Applicable Products:** HA
SBC-15938	An HTTP proxy configuration error is generated by wrong validation. **Applicable Products:** All

2.30.14 Version 7.20A.254.376

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.2125 and EMS/SEM Version 7.2.3113.

2.30.14.1 Resolved Constraints

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

Table 2-54: Resolved Constraints in Version 7.20A.254.376

Incident	Description
SBC-14298 / SBC-15077 / SBC-15618 / SBC-15644 / SBC-15686	The device offers the same crypto in SIP re-INVITE messages for SBC call session refreshes in a Microsoft Teams environment. As a result, there is no audio. **Applicable Products:** All.

2.30.15 Version 7.20A.254.375

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.2125 and EMS/SEM Version 7.2.3113.

2.30.15.1 New Features

This section describes the new features introduced in this version.

2.30.15.1.1 Mediant CE Deployable on Google Cloud Platform

Mediant Cloud Edition (CE) SBC can now be deployed on the Google Cloud platform.

Applicable Application: SBC.

Applicable Products: Mediant CE.

2.30.15.1.2 Microsoft Teams License Included in Evaluation License Key

The device's evaluation License Key (three free SBC sessions) now also includes the license for Microsoft Teams Direct Routing ("TEAMS").

Note: For post-evaluation deployment, this evaluation License Key cannot be used. Instead, a new License Key must be purchased with the required SBC sessions and features, including the "TEAMS" license for proper operation with Teams Direct Routing.

Applicable Application: SBC.

Applicable Products: Mediant Software.

2.30.15.1.3 License Keys for Microsoft Teams

When operating in a Microsoft Teams environment (for example, Phone System Direct Routing), both the Teams license ("TEAMS") and the general Microsoft license ("MSFT") must be present in the installed License Key. Up until now, only the "TEAMS" license was required.

Note: For all products not listed below under Applicable Products, the "MSFT" license is provided by default in the License Key.

Applicable Application: SBC.

Applicable Products: Mediant 500L; Mediant 500.

2.30.15.1.4 Registration Status Updates with ARM and Third-party Routing Server

The device can notify AudioCodes ARM or third-party Routing servers of all the SIP user agents (endpoints) that are registered with the device. It does this by periodically synchronizing its registration database with the Routing server to keep it up to date, enabling the Routing server to use this information to perform correct and optimal routing decisions based on user registration.

The feature is enabled by the new parameter 'Routing Server Registration Status'. AudioCodes REST API also supports GET, PUT and POST actions for this parameter from a REST client, using the following new REST URL path: /api/v1/rmConfig/globals/routingServerRegistrationStatus

In addition to enabling the feature, the 'Type' parameter of the Remote Web Service (i.e., Routing server) in the Remote Web Services table must be configured to the new optional value **Registration Status**.

Applicable Application: All.

Applicable Products: All.

2.30.15.2 Known Constraints

This section lists known constraints.

Table 2-55: Known Constraints in Version 7.20A.254.375

Incident	Description
SBC-15254	For Mediant CE on Google Cloud, use of the Internal Network Load Balancer is not supported. **Applicable Products:** Mediant CE
SBC-15397	For devices in HA mode, log messages from the redundant device that are longer than 254 bytes, which are sent by the active device to syslog, are truncated to 254 bytes. **Applicable Products:** HA
SBC-15526	For recording (SIPREC) audio-video calls, the order of the 'm=' lines in the SDP body that the device sends to the SRS might be incorrect for specific call scenarios (m=video, m=audio, m=audio, and then m=video). As a result, some third-party SRS's may reject the SIPREC INVITE message. A workaround is to use the device's Message Manipulation feature to reorder the lines in the SDP. **Applicable Products:** All

2.30.15.3 Resolved Constraints

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

Table 2-56: Resolved Constraints in Version 7.20A.254.375

Incident	Description
SBC-15496	The device resets upon a call attempt to a full Trunk\Trunk Group when operating with ARM. **Applicable Products:** All (Gateway)
SBC-15401	The CLI command `hotline-dia-ltone-duration` has a typo (should be `hotline-dial-tone-duration`). **Applicable Products:** All UpdatedCLI-UM
SBC-15361	The device runs out of MDML resources on high SBC traffic when call duration is long (more than 30s). As a result, calls fail. **Applicable Products:** All
SBC-15351	The device resets upon connecting to the Web interface. **Applicable Products:** All
SBC-15251	The device fails to ping its own IP address. **Applicable Products:** Mediant 5xx; Mediant 8xx; Mediant 1000B; MP-1288
SBC-15250	The device's ELIN number is limited to 12 digits. (Now, it has been increased to 16.) **Applicable Products:** All
SBC-15244	The device is exposed to the CSFR (Cross-Site Request Forgery) security vulnerability. **Applicable Products:** All
SBC-15240	The device fails to play the hold tone from the PRT file during an on-hold scenario. As a result, the call disconnects. **Applicable Products:** All
SBC-15227	The device replies with a SIP 488 to a 200 OK of a forked call if the original INVITE contains a Record-Route header. As a result, the call fails. **Applicable Products:** All
SBC-15226	The device's CDR displays the wrong IP address of the remote side. **Applicable Products:** All
SBC-15225	The device resets when the Web interface session opens, because of a memory issue. **Applicable Products:** All
SBC-15198	When the device does a second HA switchover, the call that was established before the first switchover, disconnects upon hold/unhold scenario. **Applicable Products:** HA
SBC-15131	The device doesn't increase the SDP's session ID upon a re-INVITE after switching from a direct-media call to non-direct media call. As a result, no voice occurs. **Applicable Products:** All

Incident	Description
SBC-14902	The device removes the SIP header, P-Asserted-Identity after the call is rerouted by ARM. **Applicable Products:** All
SBC-14707	The device fails to authenticate re-INVITE requests of a rerouted call (alternative routing or REFER). **Applicable Products:** All
SBC-14683	The device resets upon configuring debug syslog messages using the HTTPProxySyslogDebugLevel parameter. **Applicable Products:** All
SBC-14682	The performance monitoring counter UnAvailable Seconds (UAS) displays (show voip interface e1-t1) incorrect values. **Applicable Products:** Gateway
SBC-14647	Changing the Web interface's Admin user password fails, and it can be changed only 24 hours after the previous password change. (Now, the default of the WebPassChangeInterval has been changed to 0.) **Applicable Products:** All
SBC-14626	Upon an HA switchover, the device's STWR task gets stuck in the read Linux file, causing a CPU overload. **Applicable Products:** HA
SBC-14561	Direct media (media bypass) calls disconnect when the SBC remains without any active Media Components (MCs). (Now, such calls don't get disconnected upon this scenario, as long as they don’t change to non-direct media calls.) **Applicable Products:** Mediant CE

2.30.16 Version 7.20A.254.202

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1133 and EMS/SEM Version 7.2.3113.

2.30.16.1 New Features

This section describes the new features introduced in this version.

2.30.16.1.1 SIPREC for Audio-Video Calls

The device's SIPREC feature now also supports the recording of video streams for audio-video calls. Up until now, the SIPREC feature recorded only audio streams. This feature can be used when the device (Session Recording Client or SRC) interacts with third-party Session Recording Servers (SRS) that support video streams recording.

The new parameter 'Video Recording Sync Timeout' (VideoRecordingSyncTimeout) has been introduced for video recording synchronization (media port negotiation). If the SRS doesn't send the SIP 200 OK within this timeout period, the device connects the video stream between the UAs, and then starts sending recorded video and audio streams to the SRS.

Note: For audio-video calls, video recording requires additional SBC media channel resources and therefore, the purchased License Key needs to accommodate for this.

Applicable Application: SBC.

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

2.30.16.1.2 SIP Signaling over SCTP Transport

The device now supports the Stream Control Transmission Protocol (RFC 4960 "Stream Control Transmission Protocol") transport protocol, which provides multi-homing capabilities, preventing single points of failure. This is used for SIP signaling (SIP over SCTP) in accordance with RFC 4168 (The Stream Control Transfer Protocol (SCTP) as a Transport for SIP).

SCTP multi-homing provides redundancy capabilities which maintains all SIP sessions in case of network failure between the device and the remote SIP proxy. The device can support up to two local IP addresses (IP Interfaces) per SIP Interface and multiple IP addresses on the remote proxy. Each SIP Interface creates its own SCTP association, which can include multiple paths between the device and proxy.

For this feature, the following new configuration parameters and optional values have been added:

- SIP Interfaces table:
  - 'SCTP Port' parameter (currently, Web only) - defines the port on which the device listens for inbound SCTP connections.
  - SCTP Secondary Network Interface' parameter (currently, Web only) - assigns an additional local address or IP Interface (from the IP Interfaces table) for multi-homing. The primary IP Interface for multi-homing is configured for the SIP Interface by the existing 'Network Interface' parameter.
- Proxy Address table (child of Proxy Sets table):

- **SCTP** optional value for the 'Transport Type' parameter.
- For multi-homing support, multiple remote proxy IP addresses can be configured for the same Proxy Set. When at least one IP address in a Proxy Set is configured to use the SCTP transport type, the device assumes that all the IP addresses in the same Proxy Set are a set of multi-homing remote addresses for a single proxy. In this case, all the IP addresses in the Proxy Set must be configured with the SCTP transport type and with the same remote SCTP port number.

- SCTP has been added as an optional value for the following parameters:
  - Classification table: 'Source Transport Type' (Classification_SrcTransportType)
  - IP-to-IP Routing table: 'Destination Transport Type' (IP2IPRouting_DestTransportType)
  - Test Call Rules table: 'Destination Transport Type' (Test_Call_DestTransportType)
- SCTP parameters (Web and CLI) according to the SCTP RFC:
  - sctpHeartbeatInterval (heartbeat-interval): Defines the SCTP heartbeat interval
  - sctpInitialRTO (initial-rto): Defines the Initial retransmission timeout (RTO)
  - sctpMinimumRTO (minimum-rto): Defines the Minimum Retransmission Timeout (RTO)
  - sctpMaximumRTO (maximum-rto): Defines the maximum retransmission timeout (RTO)
  - sctpMaxPathRetransmit (max-path-retransmit): Defines the maximum path retransmissions per address
  - sctpMaxAssociationRetransmit (max-association-retransmit): Defines the maximum association retransmit
  - sctpMaxDataTxBurst (max-data-tx-burst): Defines Maximum number of DATA chunks that can be transmitted at one time – default 4 packets
  - sctpMaxDataChunksBeforeSACK (max-data-chunks-before-sack): Defines SACK sent after number of received packets
  - sctpTimeoutBeforeSACK (timeout-before-sack): Defines SACK sent after timeout since the received packet
- (CLI) show sctp connections – displays local SCTP endpoint and SCTP associations
- (CLI) show sctp statistics – displays statistics of all SCTP associations

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.30.16.1.3 Message Session Relay Protocol Support (MSRP)

The device now supports Message Session Relay Protocol (MSRP), which is a text-based protocol for exchanging a series of related instant messages (IM) across an IP network (TCP/TLS only) in the context of a session. The protocol can also be used to transfer large files or images or sharing remote desktops or whiteboards. MSRP is typically used for Next Generation 911 (NG911) services, allowing 911 callers to not only access 911 services through voice calls, but also through text messages with Public Safety Answering Points (PSAPs). MSRP support is in accordance with RFC 4975 (The Message Session Relay Protocol (MSRP)) and RFC 6135 (An Alternative Connection Model for the Message Session Relay Protocol (MSRP)).

The device establishes MSRP sessions using the SDP offer/answer negotiation model over SIP. The MSRP session starts with a SIP INVITE and ends with a SIP BYE message. As a B2BUA, the device interoperates between the MSRP endpoints, terminating the incoming MSRP message on the inbound leg and then generating a new MSRP message on the outbound leg. Before sending the INVITE, the device manipulates the SDP body (e.g., 'a=path', 'c=', 'm=', 'a=setup' and 'a=fingerprint' lines). The device can perform optional

message manipulation and other translations such as resolving NAT traversal issues when the endpoints or device are located behind NAT. The device also supports secure MSRP sessions (MSRPS), using TLS certificates (TLS Context).

Below shows an example of an MSRP message (*SEND* request):

```
MSRP a786hjs2 SEND
To-Path: msrp://biloxi.example.com:12763/kjhd37s2s20w2a;tcp
From-Path: msrp://atlanta.example.com:7654/jshA7weztas;tcp
Message-ID: 87652491
Byte-Range: 1-25/25
Content-Type: text/plain

Hey Bob, are you there?
-------a786hjs2$
```

This feature provides the following configuration updates:

- IP Profiles table:
  - 'MSRP Offer Setup Role' parameter (new): Configures the device's MSRP role mode in SDP negotiations ('a=setup' line).
  - 'Data DiffServ' parameter (new): Configures DiffServ marking of MSRP traffic and media of TCP traffic in the IP header's DSCP field.
  - 'MSRP re-INVITE/UPDATE' parameter (new): Configures if the destination UA participating in the MSRP session supports the receipt of re-INVITE requests and UPDATE messages.
  - 'SBC Media Security Mode' parameter (existing): Configures the transport protocol for the outgoing leg (**Secured** and **Both** for MSRPS; **Not Secured** for MSRP). The optional values of the parameter have been renamed -- **SRTP** to **Secured**; **RTP** to **Not Secured** -- to reflect that it's also for MSRP (not only SRTP).
  - 'MSRP Empty Message Format' parameter (new): Configures if the device adds a Content-Type header to the first empty (no body) MSRP message that is used in the connection.
- IP address and port of the 'path' attribute is determined by the Media Realm associated with the IP Group. The port is configured by the new Media Realm parameters 'TCP Port Range Start' (CpMediaRealm_TCPPortRangeStart) and 'TCP Port Range End' (CpMediaRealm_TCPPortRangeEnd), which enables a single Media Realm to serve both RTP and MSRP. As a result of these new parameters, the existing Media Realm parameters 'Port Range Start' and 'Port Range End' have been renamed ('UDP Port Range Start' and 'UDP Port Range End').
- For NAT traversal, the existing NAT Translation table is used (and the new IP address:port is used in the 'a=path' field).
- The IP Group's existing 'DTLS Context' parameter has been renamed (Web only) to 'Media TLS Context' to reflect that the parameter can also be used for MSRP sessions (not only DTLS).

CDRs generated by the device for MSRP calls include the value "msrp" for the CDR field, Media List (existing).

Applicable Application: SBC.

Applicable Products: All.

2.30.16.1.4 Automatic Topology Hiding of URI Host Part by IP Group's SIP Group Name

The device now provides an easy-to-configure method to replace the host part of the URI in outgoing SIP messages with the destination IP Group's 'SIP Group Name' parameter value. This feature enhances the device's capability for hiding the incoming network topology (i.e., URI) from the outbound IP Group. Up until now, Message Manipulation rules for each header were required to implement such topology hiding.

The SIP headers to which this feature can be applied is specified by the new IP Groups table parameter 'SIP Topology Hiding Headers List' (IPGroup_TopologyHidingHeaderList).

Note:

- If the 'SIP Group Name' field is not configured and the 'SIP Topology Hiding Headers List' parameter is configured, the device replaces the host part of the URI with the local IP address (IP Interface) associated with the IP Group.
- If Outbound Message Manipulation is also configured for the IP Group, it's applied only after this topology hiding feature is applied.
- The 'SIP Topology Hiding Headers List' parameter doesn't change the default behavior of the 'SIP Group Name' (i.e., replaces the host part of the Request-URI and To headers in outbound messages and replaces the host part in the From header in inbound messages).

Applicable Application: SBC.

Applicable Products: All.

2.30.16.1.5 Enhanced SIP PRACK Handling

The device's SIP PRACK handling, which is configured by the existing IP Profile parameter 'PRACK Mode' (IpProfile_SbcPrackMode) has been enhanced with the following additional optional values:

- [0] **Disabled**: Depending on scenario, the device either disables PRACK with the SIP User Agent (UA) or rejects the call.
- [4] **Optional With Adaptations**: Optimized PRACK handling, which is based on the presence of PRACK-related SIP headers and parameters ('Require:100rel' or 'Supported: 100rel') as well as the presence of SIP message bodies (e.g., SDP) in 18x responses. This option may be useful, for example, to avoid PRACK congestion due to the device being flooded with 18x messages without a body.

For a detailed description, refer to the device's *User's Manual*.

Applicable Application: SBC.

Applicable Products: All.

2.30.16.1.6 Customizing CDR Call Success Indication Based on Responses

Call success indication in CDRs (using the optional 'Call Success' field - "yes" or "no"), which is based on call release (termination) reason (i.e., SIP response code or internal response generated by device) can be changed from default (customized). For example, by default, calls released with SIP 486 (Busy Here) responses are indicated in CDRs as call failure. By employing this feature, these SIP responses can be reported in CDRs as call success.

To support this feature, the following new parameters have been added (under Troubleshoot-> Call Detail Record -> Call Detail Record Settings) to override the device's default behavior for determining call success:

- SIP response codes:
  - 'Call Success SIP Reasons' [CallSuccessSIPReasons] - defines SIP responses for call success

- 'Call Failure SIP Reasons' [CallFailureSIPReasons] - defines SIP responses for call failure

- Internal response codes:
  - 'Call Success Internal Reasons' [CallSuccessInternalReasons] - defines internal responses for call success
  - 'Call Failure Internal Reasons' [CallFailureInternalReasons] - defines internal responses for call failure

This feature also allows customization of call status (success or failure) for the following special internal responses before or after call connect (SIP 200 OK):

- "GWAPP_NO_USER_RESPONDING" (18):
  - 'No User Response before Connect' [NoUserResponseBeforeConnectSuccess] - defines call status when the response is received before call connect
  - 'No User Response after Connect' [NoUserResponseAfterConnectSuccess]- defines call status when the response is received after call connect
- "RELEASE_BECAUSE_CALL_TRANSFERRED" (807):
  - 'Call Transferred before Connect' [CallTransferredBeforeConnectSuccess] - defines call status when the response is received before call connect
  - 'Call Transferred after Connect' [CallTransferredAfterConnectSuccess] - defines call status when the response is received after call connect

The valid value of these parameters is the SIP response code number (e.g., 486). Multiple responses can be configured, whereby each code is separated by a comma (e.g., 486,408,406). A range of responses can also be configured using the "xx" wildcard (e.g., 4xx).

Applicable Application: All.

Applicable Products: All.

2.30.16.1.7 Alternative Routing Based on SIP Responses per IP Group

Alternative call routing based on SIP response codes can now be configured per IP Group. Up until now, this was configured globally (for all calls), using the Alternative Routing Reasons table. Now, multiple SIP response codes for alternative routing can be configured and grouped under an Alternative Reasons Set and then assigned to a specific IP Group.

To support the feature, configuration has been updated as follows:

- The Alternative Routing Reasons table has been replaced with the following parent-child table:
  - Alternative Reasons Set (parent) – defines a name for the group of SIP response codes
  - Alternative Reasons Rules (child) – defines the SIP response codes for the Alternative Reasons Set to trigger alternative routing
- The new parameter 'SBC Alternative Routing Reasons Set' has been added to the IP Groups table to assign the Alternative Reasons Set to an IP Group.

Applicable Application: SBC.

Applicable Products: All.

2.30.16.1.8 Enhanced IPMI Indication for Fan and CPU Temperature Alarms

The device's Intelligent Platform Management (IPMI or iLO) chassis indicators for fan status and CPU temperature has been enhanced as follows:

- Fan status: Up until now, the SNMP alarm acFanTrayAlarm indicated a failure for the entire Fan Tray module (Major severity). Now, it's also sent to indicate failures per fan

(removed or faulty). For example, if a failure occurs in fan 3, the alarm is sent ("Fan-Tray Alarm. Fan 3 is faulty"). If a failure then occurs in fan 4 as well, the first alarm is cleared and a new alarm is sent indicating failures in fans 3 and 4 ("Fan-Tray Alarm. Fans 3,4 are faulty"). If fans 3 and 4 return to normal operation, the alarm is cleared.

- Temperature status: Up until now, the SNMP alarm acBoardTemperatureAlarm was sent only when the overall temperature of the CPU exceeded a specific threshold (configured by the HighTemperatureThreshold parameter). Now, it's sent per temperature sensor. For example, if the temperature threshold exceeds at sensor 1, the alarm is sent ("Board Temperature Alarm: Sensor #1 is 88 degrees celsius. Exceeded threshold of 70"). If the temperature threshold at sensor 2 then exceeds as well, the first alarm is cleared and a new alarm is sent indicating exceeded temperature thresholds at both sensors ("Board Temperature Alarm: Sensors #1,#2 are 88,90 degrees celsius. Exceeded threshold of 70").

Applicable Application: SBC.

Applicable Products: Mediant 9000 Rev. B; Mediant 9030; Mediant 9080.

2.30.16.1.9 VMware Tools Version Update

VMware Tools is deployed as part of the SBC image for the VMware virtualization platform. VMware Tools has been updated from Version 9.4.10 to Version 10.3.5.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.30.16.1.10 Enhanced System Snapshot Features

The device's System Snapshot feature has been enhanced as follows:

- For HA systems, renaming a System Snapshot on the active device synchronizes with the redundant device and renames the corresponding System Snapshot on the redundant device. (Note that if the new name is not unique on the active and redundant devices, the renaming operation fails).
- The device generates a Syslog error message when the user tries to create a System Snapshot and there is insufficient memory on the device to store it ("SSM: CreateSystemSnapshot(): Failed to create snapshot (name=<Snapshot Name>, rc=<ERR_CODE>)"). Up until now, the System Snapshot was created even though it was corrupted.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.30.16.1.11 Additional User Activity Details in Activity Log and Syslog

Additional details regarding management user activity through the device's management interfaces have been added to the Activity Log and Syslog. These additional details improve security and tracing capabilities regarding the actions taken by users. Note that the format of these messages in the Activity Log and Syslog were changed accordingly. These additional activities that are reported include the following:

- User attempts to log in with incorrect username or password.
- Blocked or inactive (new or inactive user) user attempts to log in.
- Session limit exists when user attempts to log in.
- User's access level is changed (e.g., Monitor to Administrator).
- Added or deleted user (in the Local Users table).

Applicable Application: All.

Applicable Products: All.

2.30.16.1.12 DNS Rebinding Protection

The device now provides protection against DNS rebinding attacks. This may occur when management users access the device using its hostname (configured by the existing parameter HostName) instead of the IP address. The feature is enabled by the new parameter 'DNS Rebinding Protection Enabled'.

Applicable Application: All.

Applicable Products: All.

2.30.16.1.13 IPv6 Addresses for IP Traces in Logging Filters Table

Logging filter configuration for IP traces now supports IPv6 source and destination addresses. Up until now, only IPv4 addresses were supported.

The IPv6 addresses are configured by the existing 'Value' parameter in the Logging Filters table, when the 'Filter Type' parameter is configured to **IP Trace**. The addresses are configured using the new keywords "ipv6.src", "ipv6.dst" and "ipv6.addr". Examples are shown below:

- "ipv6.addr==2001:0db8:85a3:0000:0000:8a2e:0370:7334"
- "ipv6.src==2001:db8:abcd:0012::0/64" (where /64 is the prefix length)

For IPv4, the existing keywords are used ("ip.src", "ip.dst" and "ip.addr").

Applicable Application: All.

Applicable Products: All.

2.30.16.1.14 Hidden Password when Configuring Users through CLI

When configuring a management user for the device in the Local Users table through CLI, the user's password can be concealed (hidden) when typing it in. The feature is supported by pressing the Enter key intermediately after typing the existing `password` command:

```
(config-system)# user john
Configure new user john
(user-john)# password
Please enter hidden password (press CTRL+C to exit):
```

Applicable Application: All.

Applicable Products: All.

2.30.16.1.15 Direct Media Calls Automatically Disabled for SIPREC

When the device needs to record calls that are configured for direct media or media bypass (i.e., media stream doesn't traverse the device), it automatically disables direct media for these calls (during their setup). This ensures that the media passes through the device so that it can be recorded and sent to the SRS.

Note: This feature doesn't apply if direct media is enabled using the global parameter SBCDirectMedia (i.e., for all calls). In this scenario, direct media is maintained and SIP recording is not done on these calls. The feature is applicable only if direct media is enabled per specific calls using, for example, IP Profiles ('Direct Media Tag' parameter) or SIP Interfaces ('Direct Media' parameter).

Applicable Application: SBC.

Applicable Products: Mediant 500; Mediant 500L; Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.30.16.1.16 Max. RADIUS-Accounting Attributes for CDR Customization

The maximum number of RADIUS Accounting attributes that can be customized (and sent) in the CDR generated by the device has been increased from 70 to 128.

Applicable Application: SBC.

Applicable Products: Mediant 2600; Mediant 4000.

2.30.16.1.17 Configured Hostname Exposed to Hypervisor

If the device is configured with a hostname (using the existing 'Host Name' parameter), the hostname is now also "exposed" to the VMware vSphere hypervisor on which the SBC is deployed.

Applicable Application: SBC.

Applicable Products: Mediant 9xx; Mediant Software.

2.30.16.2 Known Constraints

This section lists known constraints.

Table 2-57: Known Constraints in Version 7.20A.254.202

Incident	Description
SBC-15055	On the Mediant CE, only one snapshot can be added (in addition to the default). New files can be uploaded only with one snapshot, in addition to the default. **Applicable Products:** All Mediant CE
-	SCTP is currently not supported by the products listed below. Please contact your AudioCodes' representative for more information. **Applicable Products:** MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 1000; Mediant 2600; Mediant 4000
-	Even though the products listed below don't support SCTP, the **SCTP** optional value appears for the following parameters: Classification_SrcTransportType; IP2IPRouting_DestTransportType; Test_Call_DestTransportType. **Applicable Products:** All (except Mediant 90xx; Mediant Software)
-	Even though the products listed below don't support SCTP, the **SCTP** optional value appears for the 'Transport Type' parameter in the Proxy Address table. **Applicable Products:** All (except Mediant 90xx; Mediant Software)
-	Even though the products listed below don't support SCTP, the CLI `sctp-port` ('SCTP Port') parameter appears in the SIP Interfaces table. **Applicable Products:** All (except Mediant 90xx; Mediant Software)
-	Even though the products listed below don't support SCTP, the CLI `sctp-second-network-interface` ('Secondary Network Interface') parameter appears in the SIP Interfaces table. **Applicable Products:** All (except Mediant 90xx; Mediant Software)

2.30.16.3 Resolved Constraints

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

Table 2-58: Resolved Constraints in Version 7.20A.254.202

Incident	Description
SBC-14689	Prefix length 120 is not supported for IPv6 network interfaces. **Applicable Products:** All
SBC-14664	SIP parsing errors occur due to record route. **Applicable Products:** All
SBC-14650	The device's WebRTC drops the video stream from calls due to different SSRCs. **Applicable Products:** All
SBC-14552	The device's Call Forward activation and deactivation fails for calls, as the device doesn't release the Gateway call towards the IP. **Applicable Products:** Gateway
SBC-14499	The device disconnects from ARM upon the receipt of a 504 reply from OVOC. **Applicable Products:** All
SBC-14426	The Gateway CDR Format table doesn't appear in the Web interface (appears as Test Call CDR Format table). **Applicable Products:** Gateway
SBC-14401	The device tries to extend coders even though it has no transcoding capabilities. As result, the call fails. **Applicable Products:** All
SBC-14323	The device forwards a second identical 183 with the wrong SDP. **Applicable Products:** All
SBC-14313	The device rejects STUN with high priority after a re-INVITE, generating the error message "STUN_ATTRIBUTE_USERNAME failed". As a result, no voice occurs. **Applicable Products:** All
SBC-14234	A TLSSocket issue causes the device to be in a state of "connection not established", stopping the device from reporting the Floating License Pool to OVOC. **Applicable Products:** All
SBC-14223	The device doesn't show the Caller ID name, when Caller ID is enabled for IP-to-Tel calls. **Applicable Products:** MP-1288
SBC-14112	One-way voice occurs due to a specific call transfer scenario **Applicable Products:** All
SBC-14057	The device resets with the exception info of TASK PMON, which is caused by a dereference of a null pointer. **Applicable Products:** All
SBC-14024	The device experiences no voice when the IP address of the IP Interface is changed. **Applicable Products:** All

Incident	Description
SBC-13991	The device's Web interface displays the wrong number of active calls, due to incorrect calculation of alternative routing. **Applicable Products:** Gateway.
SBC-13982	The device shows Syslog messages in debug recording (DR) even though it is configured to include SIP only (Logging Filters table 'Log Type' parameter configured to SIP Only). **Applicable Products:** All.
SBC-13951	The device sends CDR reports (Media_End) to the CDR server even if it's configured to 0.0.0.0. **Applicable Products:** All.
SBC-13899	The device provides only 100 resources for RTCP-XR PUBLISH messages, which is insufficient for high traffic loads. **Applicable Products:** All.
SBC-13812	The device limits CDR types that are for RADIUS SBC to 70 (instead of 128). **Applicable Products:** Mediant 2600.
SBC-13776	The device is exposed to a security vulnerability (X-Content-Type-Options is not specified), as the X-Content-Type-Options is missing. **Applicable Products:** All.
SBC-13774	The device is exposed to a security vulnerability (form validation has been turned off), as its missing HTML5. **Applicable Products:** All.
SBC-13773	The device is exposed to a security vulnerability (Page after login has been cached locally), as its Web interface can be accessed after login without authentication. **Applicable Products:** All.
SBC-13771	The device is exposed to security vulnerability (unrestricted file upload), as it loads any type of file from the Auxiliary Files page. **Applicable Products:** All.
SBC-13770	The device is exposed to security vulnerability (XML Entity Expansion Injection), as it accepts document type definition from untrusted sources. **Applicable Products:** All.
SBC-13757	The device sends invalid SRTP packets after upgrade to Ver. 7.2.252. **Applicable Products:** All.
SBC-13642	When using DTLS without STUN, the device sends DTLS Client Hello packets with the destination MAC containing only zeros, causing a DTLS delay. **Applicable Products:** All
SBC-13638	The device's Syslog warning message "invalid payload type" doesn't include the source IP address. **Applicable Products:** All
SBC-13622	The HA system experiences a mismatch in Proxy IP addresses between active and redundant devices after an HA switchover. **Applicable Products:** HA
SBC-13437	The device is not able to configure the virtual machine host name (default is localhost.localdomain). **Applicable Products:** Mediant VE (VMware Sphere)

Incident	Description
SBC-13384	The ini file that is extracted from the configuration_package.tar.gz file through SFTP is corrupt. **Applicable Products:** All
SBC-13043	The device sends a DNS query as an A-Record instead of an SRV. **Applicable Products:** All
SBC-12758	For SBC calls, the device offers an "extended" coder with the same dynamic payload type as the existing coder, resulting in a faulty SDP offer. **Applicable Products:** All
SBC-12526	The device's TLS Contexts don't offer the chain of trust in Server Hello responses. **Applicable Products:** All
SBC-11727	A warning message on the virtual host occurs. The configured guest OS (Red Hat Enterprise Linux 6 (64-bit)) for this virtual machine does not match the guest that is currently running (CentOS 4/5/6/7 (64-bit)). **Applicable Products:** Mediant Software
SBC-10026	The Message Conditions table configuration is lost after a device reset (or HA switchover) because of the comma (,) symbol in its name. **Applicable Products:** All
SBC-13967 / SBC-14221 / SBC-14541	When the Proxy Set is modified, the device resets, which is caused by a memory overrun. **Applicable Products:** All.
SBC-13942 / SBC-14546	If the device receives an SDP offer with ICE and the IP Profile parameter SBCIceMode is disabled, it doesn't update the remote IP address, causing no voice. **Applicable Products:** All.
SBC-14142 / SBC-14478	The device resets when receiving a SIP 200 OK with 'a=inactive' for WebRTC and SIPREC calls. **Applicable Products:** All
SBC-14300 / SBC-14501	If the device receives an SDP answer with ICE lite or no ICE, the channel mode isn't updated and thus, remains in ICE mode. According to RFC, in such a scenario it should be in no-ICE mode. As a result, no voice occurs. **Applicable Products:** All

2.30.17 Version 7.20A.252.269

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1133 and EMS/SEM Version 7.2.3113.

2.30.17.1 Resolved Constraints

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

Table 2-59: Resolved Constraints in Version 7.20A.252.269

Incident	Description
SBC-14262	The device resets due to memory overrun in the following scenario: when a high SIP call traffic load occurs, and the GWDebugLevel parameter is configured to 5, and DR captures all Syslog packets. **Applicable Products:** All.
SBC-13616	In a WebRTC-to-WebRTC SBC call, after a re-INVITE the following Syslog is generated "DTLSContext(#242)::StartHandshake" and voice is lost. **Applicable Products:** All.
SBC-13139	For an outgoing call that has an established connection, when a re-NVITE is sent with a different DTLS key, the connection results in one-way voice and cannot be restored. **Applicable Products:** All.
SBC-13125	During an SBC SIP session with voice and video, after repeatedly turning the video off and on, the video is transmitted with a delay of about 2-3 seconds. **Applicable Products:** All.

2.30.18 Version 7.20A.252.261

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1132 and EMS/SEM Version 7.2.3113.

2.30.18.1 Resolved Constraints

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

Table 2-60: Resolved Constraints in Version 7.20A.252.261

Incident	Description
SBC-13775	The device allows the loading of any file type through the Auxiliary Files page (Setup > Administration > Maintenance > Auxiliary Files), exposing it to security vulnerability. **Applicable Products:** All.
SBC-13772	Some passwords configured on the device are not masked (displayed in plain text) in the Web interface, exposing it to security vulnerability. **Applicable Products:** All.
SBC-13756	The CPU Overload (in SPLB) alarm isn't cleared when the device's CPU utilization returns to normal. **Applicable Products:** All.
SBC-13734	WebRTC client forking fails when ARM replies (to the device's GetRoute request) with a User-type IP Group – the call is not forked to all the users (Client Forking Mode configured to Parallel). **Applicable Products:** All.
SBC-13621	DNS resolution for the HA Network Monitor feature is incorrect when the destination is configured as a hostname. **Applicable Products:** HA.
SBC-13617	For IP-to-Tel calls, the device doesn’t send the redirect number received in the SIP History-Info header to the PSTN. **Applicable Products:** Gateway.
SBC-13534	The LoginNeeded parameter restores to default after the device resets or a failover occurs. **Applicable Products:** All.
SBC-13478	When using Call Setup Rules (CSR) with ENUM queries and the query target is defined, the device doesn't cache the resulting information and CSR fails. **Applicable Products:** All.
SBC-13420	Call forwarding fails for FXS interfaces (in Ver. 7.20.250). **Applicable Products:** Gateway.
SBC-13385	Tel-to-IP routing fails when configuring IP Group Index 0 and Proxy Set Index 0. **Applicable Products:** Gateway.

Incident	Description
SBC-13268	Modifying any row in the Ethernet Devices table (such as the 'Tagging' field) in an HA system causes an error ("SYS_HA: Offline Parameter PhysicalPortsTable was changed, in case HA is lost, HA reestablishment must be after system reboot"). As a result, HA mode fails. **Applicable Products:** HA.
SBC-13267	An SBC call for Microsoft Teams Direct Routing with media bypass results in no media (no voice). **Applicable Products:** All.
SBC-13251	Access to the device's Web Interface from another subnet is not possible. **Applicable Products:** All.
SBC-13168	For WebRTC-to-WebRTC calls, the device handles the SDP's 'ssrc' attributes incorrectly (should send all 'ssrc' attributes between sides, while SIP-to-WebRTC calls should remove all 'ssrc' attributes). **Applicable Products:** All.
SBC-13150	The device resets upon receipt of a SIP INVITE message containing the Replaces header in specific scenarios: 1) device sends call to A, 2) A sends a REFER to connect with B, 3) after connection, C sends INVITE with Replaces to replace B. **Applicable Products:** All.
SBC-12989	When RTP Transparent and DTMF RFC 2833 use the same payload type, the device doesn't transfer the RTP packets. **Applicable Products:** Gateway.
SBC-11142	The device's Linux kernel is vulnerable to security attacks (CVE-2018-5391). **Applicable Products:** All.
SBC-13511 / SBC-13783	The EnableSingleDspTranscoding parameter is applicable only to Mediant 3000, however, it also appears in the Web interface of other products. **Applicable Products:** All.
SBC-13754 / SBC-14030	Graceful Lock doesn't function in Ver. 7.2.252. **Applicable Products:** All.
SBC-13623 / SBC-13678	The device's NGINX HTTP Proxy doesn't start after the device resets. **Applicable Products:** All.
SBC-13372 / SBC-13421	When the device handles QoE over T.38 (T.38 fax session while VQMON is enabled), in certain scenarios the device resets. **Applicable Products:** All.

2.30.19 Version 7.20A.252.023

This version includes new features only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1116.

2.30.19.1 New Features

This section describes the new features introduced in this version.

2.30.19.1.1 HA Support for Mediant CE for Microsoft Azure Deployments

Mediant Cloud Edition (CE) can now be deployed as a High Availability (HA) system on the Microsoft Azure cloud platform.

Applicable Application: SBC.

Applicable Products: Mediant CE.

2.30.20 Version 7.20A.252.011

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1116 and EMS/SEM Version 7.2.3113.

2.30.20.1 New Features

This section describes the new features introduced in this version.

2.30.20.1.1 Call Setup Rules for HTTP POST Requests

Call Setup rules can be configured for HTTP POST methods (in addition to the already supported HTTP GET method). Such Call Setup rules allows the device to send HTTP POST requests to an HTTP server. This is configured in the Call Setup Rules table by the following new optional values of the 'Request Type' parameter:

- **HTTP POST Notification:** This option is used to send an HTTP POST request that is for notification purposes only (i.e., device does not expect a response from the server). For example, a Call Setup Rule can be configured to send an HTTP POST request whenever the device receives a 911 (emergency) call.
- **HTTP POST Query:** This option is used to send an HTTP POST request that requires a response from the server (Http.Result keyword).

In addition, a new optional value—**None**—has been added to the 'Action Type' parameter. This is used when no action is needed by the device, for example, when sending an HTTP POST request to notify the HTTP server.

Unlike HTTP GET requests which include all required data in the URL, HTTP POST requests include a URL and a message body. Call Setup Rules can now be used to customize

(manipulate) the HTTP Content-Type header (e.g., Content-Type: application/x-www-form-urlencoded) and message body of POST requests, using the following new keywords:

- Http.Request.Body: Customizes the message body and is used in the 'Action Subject' parameter to add or modify the value of the body.
- Http.Request.Content-Type: Customizes the Content-Type header and is used in the 'Action Subject' parameter to add or modify the value. For POST requests, the header is omitted by default; for GET requests, it is set to "html/text".

Due to this feature, the parameters in the Call Setup Rules table have been renamed:

- 'Query Type' has been renamed 'Request Type'
- 'Query Target' has been renamed 'Request Target'
- 'Search Key' has been renamed 'Request Key'

Applicable Application: All.

Applicable Products: All.

2.30.20.1.2 Customization of SNMP Alarm Severity Levels

SNMP trap alarms (not events) can now be customized. This includes the following:

- Changing an alarm's severity level (e.g., from Minor to Major)
- Suppressing an alarm's severity level
- Suppressing an alarm

This feature is configured in the following new table:

- Web: Alarms Customization (Setup menu > Administration tab > SNMP folder > Alarms Customization)
- CLI: configure system > snmp alarm-customization
- ini: AlarmSeverity

Applicable Application: All.

Applicable Products: All.

2.30.20.1.3 Customization of User Access Privileges per Web Page

Read-write and read-only access privileges of user levels (Monitor, Administrator, or Security Administrator) per Web page in the device's Web interface can be customized (overriding default access privileges).

This feature is configured in the following new table:

- Web Interface: Customize Access Level table (Setup > Administration > Web & CLI > Customize Access Level)
- ini File: WebPagesAccessLevel

Applicable Application: All.

Applicable Products: All.

2.30.20.1.4 User-Defined Performance Monitoring SNMP MIBs

Up to 26 user-defined Performance Monitoring (PM) MIB groups can be configured to count specified SIP failure responses (e.g., SIP 408) or responses generated internally by the device (e.g., CAC limit reached or NER threshold crossed). The PMs can be configured to count the responses due to sent SIP INVITE or REGISTER messages.

Each user-defined PM group includes the following PM MIBs:

- acPMSBCInUserDefinedFailures<1-26>Table: Counts the total incoming responses
- acPMSBCOutUserDefinedFailures<1-26>Table: Counts the total outgoing responses

- acPMSBCSRDInUserDefinedFailures<1-26>Table: Counts the total incoming responses per SRD
- acPMSBCSRDOutUserDefinedFailures<1-26>Table: Counts the total outgoing responses per SRD
- acPMSBCIPGroupInUserDefinedFailures<1-26>Table: Counts the total incoming responses per IP Group
- acPMSBCIPGroupOutUserDefinedFailures<1-26>Table: Counts the total outgoing responses per IP Group

The feature is configured in the new table, User Defined Failure PM (Monitor menu > Monitor tab > Performance Monitoring folder > User Defined Failure PM).

Applicable Application: SBC.

Applicable Products: All.

2.30.20.1.5 New SBC Performance Monitoring SNMP MIBs

The following new Performance Monitoring (PM) SNMP MIBs (counters) have been added for the SBC application:

- Attempted calls:
  - acPMSBCInAttemptedCallsTable
  - acPMSBCSRDInAttemptedCallsTable
  - acPMSBCOutAttemptedCallsTable
  - acPMSBCSRDOutAttemptedCallsTable
- Established calls:
  - acPMSBCInEstablishedCallsTable
  - acPMSBCSRDInEstablishedCallsTable
  - acPMSBCOutEstablishedCallsTable
  - acPMSBCSRDOutEstablishedCallsTable
- Broken connection:
  - acPMSBCMediaBrokenConnectionCallsTable
  - acPMSBCSRDMediaBrokenConnectionCallsTable
  - acPMSBCIPGroupMediaBrokenConnectionCallsTable
- Short call duration: Calls whose duration are less than a configurable duration in seconds, using the new ini file parameter, ShortCallSeconds.
  - acPMSBCInShortCallsTable
  - acPMSBCOutShortCallsTable
  - acPMSBCSRDInShortCallsTable
  - acPMSBCSRDOutShortCallsTable
  - acPMSBCIPGroupInShortCallsTable
  - acPMSBCIPGroupOutShortCallsTable
- Attempted registrations:
  - acPMSBCInAttemptedRegistrationsTable
  - acPMSBCOutAttemptedRegistrationsTable
  - acPMSBCSRDInAttemptedRegistrationsTable
  - acPMSBCSRDOutAttemptedRegistrationsTable
  - acPMSBCIPGroupInAttemptedRegistrationsTable
  - acPMSBCIPGroupOutAttemptedRegistrationsTable

- Successful registrations:
  - acPMSBCInSuccessfulRegistrationsTable
  - acPMSBCOutSuccessfulRegistrationsTable
  - acPMSBCSRDInSuccessfulRegistrationsTable
  - acPMSBCSRDOutSuccessfulRegistrationsTable
  - acPMSBCIPGroupInSuccessfulRegistrationsTable
  - acPMSBCIPGroupOutSuccessfulRegistrationsTable
- Calls per second (CPS):
  - acPMSBCInCapsTable
  - acPMSBCOutCapsTable
  - acPMSBCSrdInCapsTable
  - acPMSBCSrdOutCapsTable
  - acPMSBCIPGroupInCapsTable
  - acPMSBCIPGroupOutCapsTable

Note: To free up memory for these new PM MIBs, the maximum number of SRDs, IP Groups and Routing Policies that can be configured has been reduced. For configuration table capacity, see Section Mediant Server Edition (SE) SBC on page 213.

Applicable Application: SBC.

Applicable Products: All.

2.30.20.1.6 FXS Phone Number Configuration via Phone Keypad

Phone numbers of analog phones connected to the device's FXS ports can now be configured using the phones' keypad. The feature is configured by the new parameter, KeyPortConfigure (configure voip > gateway analog keypad-features key-port-configure). The parameter configures the key sequence that needs to be dialed on the phone's keypad to access this configuration mode. Once accessed, the phone number can be configured using the keypad. The number sign key (#) indicates the end of the number. For example, if the parameter is configured to "*81", the key sequence to configure the phone number is "*81<phone number>#". To delete the phone number, the key sequence is dialed without the phone number (e.g., "*81#").

The FXS port must be assigned to a Trunk Group ID (in the Trunk Group table) that is dedicated only to this port. It can be configured with or without a phone number, which can be changed or deleted by pressing the special key sequence.

Applicable Application: Gateway (FXS).

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

2.30.20.1.7 IDS Count for WebSocket Connection Failures

The device's Intrusion Detection System (IDS) feature now also counts WebSocket connection (establishment) failures.

In addition, IDS for TLS handshake failures is counted only for incoming connections (instead of both incoming and outgoing).

Applicable Application: All.

Applicable Products: All.

2.30.20.1.8 IP Subnet Conditions for Message Manipulation Rules

Message Manipulation rules can now be configured with conditions that check if an IP address (IPv4 or IPv6) in a SIP header (e.g., From and To) belongs to a specific subnet. The feature is configured using the new operand, "insubnet" (or "!insubnet" for not in subnet) in

the 'Condition' field. The subnet is expressed in CIDR (Classless Inter-Domain Routing) notation. A few examples are shown below:

```
Header.From.URL.Host insubnet '10.8.0.0/8'
Header.To.URL.Host !insubnet ' 172.0.0.0/10'
Header.From.URL.Host insubnet 'ffff:a08:705:0:0::/32'
```

Applicable Application: All.

Applicable Products: All.

2.30.20.1.9 Enhanced Test Call Feature

The Test Call feature, configured in the Test Call Rules table, has been enhanced with the following new features:

- Test Calls can now be configured to play a specific tone from the installed PRT file to the called party when the call is answered. This feature is configured by the new parameter, 'Play Tone Index' (Test_Call_PlayToneIndex), which specifies the index of the tone as defined in the file. Up until now, a default tone (Index 22) was played from the PRT file.
- Test Calls can now be configured with the Stream Control Transmission Protocol (SCTP) transport type. This is configured by the new optional value, **SCTP** for the 'Destination Transport Type' parameter.
- The 'Route By' parameter's optional value **Tel-to-IP** is now obsolete (the remote endpoint is now defined as an IP Group or IP address).
- The following parameters concerned with SDP Offer-Answer negotiations and which are typically configured in the IP Profiles table have been added to the Test Call Rules table:
  - 'Offered Coders Group': Assigns a Coders Group, whose coders are added to the SDP Offer
  - 'Allowed Coders Group': Assigns an Allowed Audio Coders Group, which lists permitted coders
  - 'Allowed Coders Mode': Configures the mode of operation for Allowed Coders - only allowed coders (restriction) or according to listed priority (preference)
  - 'Media Security Mode': Configures media security (SRTP and/or RTP)
  - 'Play DTMF Method': Configures the method for sending DTMF digits (RFC 2833 or In-band)

  The values of these parameters override the values of the corresponding parameters in the IP Profile of the IP Group that is associated with the Test Call.
- Support for basic NetAnn parameters in the Request-URI of incoming INVITE messages to play specific tones from the installed PRT file:
  - *early=yes*: The device sends a SIP 183 with SDP instead of connecting the call (no 200 OK).
  - *play=<Tone Index in PRT File>*: Defines the tone (prompt) to play from the PRT file
  - *repeat=<Integer>*: Defines how many times the prompt is played before disconnecting the call
  - *delay=<Time in msec>*: Defines the delay between each played prompt

  For example: INVITE sip:200@1.1.1.1;early=yes;play=15;repeat=3

Note: Some of these new features are not backward compatible. For more information, see the known constraint SBC-10191 in this document.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.10 Increase in Number Ranges for Dial Plan Rules

The maximum set of numbers (consisting of single numbers and/or range of numbers) that can be configured for prefixes and suffixes of dial plan rules (in the Dial Plan Rule table) has been increased significantly. Up until now, each dial plan rule could only include up to two sets of numbers (on average) for the prefix/suffix, for example, [101-103,911].

The following dial plan rule example represents number prefixes and is configured with six sets of numbers (each separated by a comma) consisting of ranges and single numbers: [120-125,150,160-164,170,200,210-215]

The maximum set of numbers can be calculated by multiplying the maximum number of supported dial plan rules by six. For example, if the maximum number of supported dial plan rules is 100,000, then the maximum set of numbers is 600,000 (6*100,000).

Applicable Application: All.

Applicable Products: All.

2.30.20.1.11 Modification and Deletion of IDS Default Policies

The default IDS policies in the IDS Policies table can now be modified and deleted (previously, they were read-only). In addition, if the table is empty (i.e., all policies have been deleted), the default policies can be returned by disabling IDS, and then enabling it again.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.12 Dedicated TCP Socket for FXS Channel Signaling

The device can be configured to use a dedicated TCP socket for SIP traffic (REGISTER, re-REGISTER, SUBSCRIBE, and INVITE messages) for each FXS analog channel (endpoint). The dedicated TCP socket is the socket from which the endpoint successfully registered to the registrar server.

Up until now, multiple endpoints used the same TCP socket. If SIP authentication failed for one endpoint with the server and the server "blacklisted" the TCP socket, it meant that the server blocked traffic from all the other endpoints that used this same socket.

The dedicated socket is used **only** for SIP requests from the Trunk Group (to which the endpoints belong) whose destination is the same as the destination where the endpoint registered (i.e., same Proxy Set and "Serving" IP Group). If the endpoint is not registered to the Serving IP Group over a TCP connection, calls from the endpoint to the Serving IP Group are rejected (and trigger an immediate registration attempt).

The feature is configured by the new parameter—'Dedicated Connection Mode' (**Reuse Connection**/0 and **Connection per Endpoint**/1)—in the Trunk Group Settings table. When enabled, the table's 'Serving IP Group' must be configured and the 'Registration Mode' parameter must be configured to **Per Endpoint**.

Applicable Application: Gateway (FXS).

Applicable Products: MP-1288.

2.30.20.1.13 Call Forking by Third-Party Routing Server

The device supports call forking that is handled by a third-party Routing server. When an IP-to-IP Routing rule is matched and its 'Destination Type' parameter is configured to **Routing Server**, the device sends an HTTP getRoute request to the Routing server. When it receives a successful response from the server, the device sends an INVITE message to a destination based on the response. If the routingMethod from the server is "fork", the device sends another getRoute request and upon a successful response, sends another INVITE to another destination based on the response, and so on. This call forking process continues until no routingMethod is received or it is set to “seq”, or there is a failed response from the server. If

all the contacts fail (4xx), the device falls back to an alternative route, if exists, from the server. If 3xx is received for any of the forked destinations, the device handles it after all the forked INVITEs have been terminated.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.14 Standalone OVOC QoE Parameters in Table Format

The standalone OVOC parameters for QoE have been replaced by a table to facilitate configuration (especially, the option to select an IP Interface). As such, the OVOC page (Setup > Signaling & Media > Media > Quality of Experience > OVOC) has been replaced by the following new table:

- Web: Quality of Experience Settings (Setup > Signaling & Media > Media > Quality of Experience > Quality of Experience Settings)
- ini File: QOESettings
- CLI: configure voip > qoe qoe-settings

Note: Due to this feature, the following standalone parameters are now obsolete: QOEServerIP, QOESecondaryServerIp, QOEInterfaceName, QOEEnableTLS, QoETLSContextName, and QoeReportMode.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.15 Configurable Keep-Alive Time with OVOC

The keep-alive interval (in seconds) between every keep-alive message sent by the device to OVOC is now configurable. Increasing the rate of keep-alive messages can be useful in keeping the communication link between the device and OVOC open when there is no traffic flow between them.

The feature is configured by the new 'Keep Alive Time Interval' parameter in the Quality of Experience Settings table (Setup > Signaling & Media > Media > Quality of Experience > Quality of Experience Settings).

Applicable Application: All.

Applicable Products: All.

2.30.20.1.16 32-bit Prefix Length for IPv4 Network Interfaces

IPv4 network interfaces in the IP Interfaces table can now be configured with 32-bit prefix length. In addition, the interface's Default Gateway no longer needs to be in the same subnet as the interface.

Applicable Application: SBC.

Applicable Products: Mediant 9000; Mediant Software.

2.30.20.1.17 DiffServ for HA Maintenance Traffic

Differentiated Services (DiffServ) can now be configured for HA Maintenance traffic. This is traffic that flows on the HA Maintenance interface between the two devices participating in a High-Availability (HA) system. Therefore, if needed, higher priority can be given to this traffic type. This feature is configured by the new ini file parameter, HAMaintenanceIFDiffServValue (device reset required).

Applicable Application: All.

Applicable Products: Mediant 500; Mediant 800; Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.

2.30.20.1.18 Delayed Transition to HA Operational State

HA systems can now be configured to delay (in seconds) their transition from HA non-operational state, which occurs during HA synchronization between active and redundant devices, to HA operational state. This feature may be useful, for example, to delay HA switchover when using switches with spanning tree protocol (STP) that take a long time until their ports (to which the redundant device is connected) is ready. In such scenarios, if this feature were not enabled, after synchronization there would be no connectivity between the redundant device's network interface and the switch.

The feature is configured by the following new parameter:

- CLI: configure network > high-availability settings > operational-state-delay
- ini file: HAOperationalStateDelayInSec

Applicable Application: All.

Applicable Products: HA.

2.30.20.1.19 Idle Timeout for CLI Sessions through RS-232 Serial Interface

The device now automatically activates a session timeout counter when a CLI session becomes idle. If the session is idle for up to five minutes (not configurable), the user is automatically logged out of the CLI. This applies only to CLI sessions that are established (successfully logged in) through an RS-232 serial connection (i.e., not Telnet or SSH).

Applicable Application: All.

Applicable Products: All.

2.30.20.1.20 Reset Confirmation Message for File Loads via Web

When loading files (ini file, CLI Startup Script file, and Configuration Package file) using the Web interface's Configuration File page, a confirmation message box informs the user that the device will reset after the file is loaded. The user can accept or cancel the operation.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.21 Configurable Hostname for SBCs and Gateways

The device can now be configured with a hostname (FQDN) in addition to the already supported IP address. This is configured by the following new parameter:

- Web interface: 'Host Name' (Setup > IP Network > Advanced > Network Settings)
- Cli: configure network > network-settings > hostname
- ini File: Hostname

When configured, the hostname affects the following:

- The device's Web interface and CLI (remotely via Telnet/SSH) can be accessed using its' IP address or hostname.
- The CLI prompt displays the hostname instead of the device type.
- The Web interface displays the hostname (first 16 characters only) on the toolbar instead of the device type.
- The SNMP interface's SysName object (under MIB-2) is set to this hostname.
- For certificate signing requests (CSR) to a Certification Authority (CA), the hostname can be used as the Common Name (CN or Subject Name) and Subject Alternative

Name (SAN)

- For CDR local storage (supported only by Mediant Software and Mediant 9000 SBCs), the name of the CDR file can include the device's hostname, by using the newly supported format specifier (placeholder) "%<hostname>" when configuring the name with the 'CDR File Name' (CDRLocalFileName) parameter.
- In HA systems, the device-pair share the same hostname

Applicable Application: All.

Applicable Products: All.

2.30.20.1.22 FQDN Address for OVOC Server for QoE Reporting

The address of the OVOC server (primary and redundant) to where the device sends QoE reports can now be configured as an FQDN (in the Quality of Experience Settings table). If only the primary server is configured with an FQDN, the device accepts up to two DNS-resolved IP addresses, which are used as primary and redundant IP addresses. If both the primary and redundant server are configured with an FQDN, only the first DNS-resolved IP address from each FQDN is used.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.23 TLS Certificate Verification and FQDN

The device now can verify certificates based on hostname:

- TLS certificates used by the device for HTTPS-based communication with OVOC now supports a hostname (FQDN). Up until now, certificates were issued only for IP addresses.
- The following new certificate-related parameters have been added to the Quality of Experience Settings table:
  - 'Verify Certificate': validates the server's certificate
  - 'Verify Certificate Subject Name': validates the server's certificate subject name (CN/SAN), which contains the hostname or IP address of the server
- The 'Verify Certificate Subject Name' has been added to the Remote Web Services table, which validates the certificate's subject name, which contains the hostname or IP address of the server.
- Auto-Update mechanism: verify-ssl-subject-name has been renamed to verify-cert-subject-name. If the server's URL contains a hostname, the device validates the server's certificate subject name (CN/SAN) against this hostname (and not IP address); otherwise, the device validates the server's certificate subject name against the server's IP address.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.24 Default Cipher Suite Changed for TLS Context

The default cipher suite for TLS clients and servers (configured in the TLS Contexts table) has changed to "DEFAULT". This is an OpenSSL keyword for the recommended configuration for the default cipher list, which is determined at compile time and is normally ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.25 Automatic Re-Generation of Default Self-Signed TLS Certificate

If the device's default self-signed certificate (Index 0) is about to expire (less than a day), the device automatically re-generates a new self-signed certificate.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.26 Password Display Obscured (Encrypted) in CLI

The existing CLI command, **password-obscurity** (configure system > cli-settings), which enables the display of passwords in the CLI as encrypted (obscured), now applies to all parameters –standalone and tables—that configure passwords.

Below shows two examples of a password for a Remote Web Service that is displayed in obscured and plain text format in the output of the **show running-config** command:

- Password displayed as encrypted:

```
rest-password 8ZybmJHExMTM obscured
```

- Password displayed in plain text:

```
rest-password john1234
```

Note: Due to this feature, the names of the following parameters have been modified to reflect that they configure passwords:

- SNMPReadOnlyCommunityString has been renamed SNMPReadOnlyCommunityStringsPassword
- SNMPReadWriteCommunityString has been renamed SNMPReadWriteCommunityStringsPassword
- SNMPTrapCommunityString has been renamed SNMPTrapCommunityStringPassword
- ntpAuthMd5Key has been renamed ntpAuthMd5KeyPassword
- CLIPrivPass has been renamed CLIEnableModePassword

Applicable Application: All.

Applicable Products: All.

2.30.20.1.27 SNMP Alarm for Off-hooked Phone

The device can be configured to send the new SNMP alarm, acAnalogLineLeftOffhookAlarm, to indicate that an FXS phone connected to one of the device's FXS ports has been in off-hook state for more than a user-defined time (in seconds). The tImeout is configured by the new parameter, FXSOffhookTimeoutAlarm (configure voip > gateway analog fxs-setting fxs-offhook-timeout-alarm). The timer starts once the reorder tone begins playing when the phone goes off hook. The alarm is cleared when the hook-flash button is pressed or the phone returns to on-hook state.

Applicable Application: Gateway (FXS).

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

2.30.20.1.28 Test Call CDR Customization and Display Changes

CDR customization and historical display of Test Calls has been updated as follows:

- Test Call CDRs are now customized in the existing SBC CDR Format table instead of in the Test Call CDR Format table (Troubleshoot menu > Troubleshoot tab > Call Detail Record folder > Test CDR Format), which is now obsolete.
- Historical Test Call CDRs are now displayed in the existing SBC CDR History table instead of in the Test Call CDR History table (Monitor menu > Monitor tab > VoIP Status folder > Test Call CDR History), which is now obsolete. To differentiate between

SBC and Test calls, the 'Endpoint Type' parameter has been added to the table.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.29 New Customizable CDR Field for Call Success

CDRs generated and sent by the device can be customized to include a new optional field, "Call Success" [447], which indicates whether the call succeeded ("yes") or failed ("no"). Customization is done in the existing SBC CDR Format table or Gateway CDR Format table.

Applicable Application: All.

Applicable Products: All.

2.30.20.1.30 New Customizable CDR Field for Multiple Media Types

CDRs generated and sent by the device can be customized to include a new optional field, "Media List" [819], which lists all the media types (e.g., "audio", "video" and "text") that were used during the call. This applies only to SBC signaling CDRs and for "CALL_END" Report Types (sent after a SIP BYE).

Applicable Application: SBC.

Applicable Products: All.

2.30.20.1.31 Call-End CDR Features

The following new features have been introduced for CDRs that are sent at the end of a call (SIP BYE):

- The device can be enabled to not send Call-End CDRs for calls of zero (0) duration:
  - Web interface: Call-End CDR Zero Duration Filter
  - ini: CallEndCDRZeroDurationFilter
  - CLI: call-end-cdr-zero-duration-filter
- The device can be configured to not send Call-End CDRs if a specific SIP release cause(s) is received (comma-separated list from 300 through to 699; supports "xx" to denote decimal range such as 3xx):
  - Web interface: Call-End CDR SIP Release Reasons Filter
  - ini: CallEndCDRSIPReasonsFilter
  - CLI: call-end-cdr-sip-reasons-filter

Applicable Application: All.

Applicable Products: All.

2.30.20.1.32 Minimum Severity Level in Syslog Messages

Syslog messages generated by the device can now be configured to include only messages from a specific severity level (minimum) and higher. Severity levels include (from highest to lowest severity): Fatal, Alert, Critical, Error, Warning, Notice, Informational, and Debug. The feature is configured by the following new parameter:

- Web: 'Log level' (Logging Settings page)
- CLI: log-level
- ini File: SyslogLogLevel

Applicable Application: All.

Applicable Products: All.

2.30.20.1.33 Enhanced CPU Overload Details in Syslog Messages

Syslog messages sent when the device detects a CPU overload now includes more detailed information (processes and tasks), which can help identify the cause of the overload. When the device detects a CPU overload, it sends a Syslog message every 10 seconds until the device returns to normal state.

Applicable Application: SBC.

Applicable Products: All.

2.30.20.1.34 Consolidation of Log-Related Parameters

The Syslog Settings page (Troubleshoot menu > Troubleshoot tab > Logging folder > Syslog Settings) has been removed and all the parameters that were on this page have been moved to the Logging Settings page (Troubleshoot menu > Troubleshoot tab > Logging folder > Logging Settings).

Applicable Application: All.

Applicable Products: All.

2.30.20.2 Known Constraints

This section lists known constraints.

Table 2-61: Known Constraints in Version 7.20A.252.011

Incident	Description

-	Upgrading to Version 7.20A.252 from any version earlier than 7.20A.202 fails. This is due to the increased software version file (.cmp) size of Ver. 7.20A.252 due to various new features.
	To upgrade from a version earlier than 7.20A.252, the device must be loaded with an ini file (through the Auxiliary Files page) containing the following, which enables the device to handle the large .cmp file size:
	`BSPMAXCMPFILESIZE = 180`
	`initialshellcommand = 'HideAndNotBurn; RunOnTheFly; ForceRunAll; */ResetWebServer RESET'`
	Applicable Products: Mediant 90xx; Mediant Software.

-	The Media Transcoding Cluster (MTC) feature is not supported in this release. **Applicable Products:** Mediant 90xx; Mediant Software.
SBC-13319	If the redundant device in an HA system fails (e.g., due to invalid configuration) and you load an ini file to it containing the original HA settings to configure it as the redundant device, it may result in an active-active scenario without network communication between the devices. A workaround to this issue: prior to loading the ini file, access the redundant device (Web interface or CLI) and configure the 'HA Remote Address' parameter to the Maintenance IP address of the active device. **Applicable Products:** HA.
SBC-13306	For the Media Transcoding Cluster (MTC) feature, despite HA synchronization because of a switchover, operations on the MTC can still be performed through the Web interface (instead of being blocked). For example, software upgrade (.cmp) can still be initiated during this phase (although the system may fail). **Applicable Products:** Mediant 90xx; Mediant Software.

Incident	Description
SBC-13226	When many SRDs are configured, the colors of the SRDs (as well as the #IDs in the SRD names) are no longer displayed in the Web interface. **Applicable Products:** All.
SBC-12469	If the device sends an INVITE without an SDP body, it cannot handle the receipt of multiple SIP 18x responses for call forking. **Applicable Products:** All.
SBC-11649	SCTP transport type is not supported in this version. **Applicable Products:** All.
SBC-10191	For the Test Call feature, there is backward incompatibility when upgrading to Version 7.20A.252: ▪ Routing of test calls according to the Tel-to-IP Routing table is no longer a configurable option (**Tel-to-IP** value has been removed from the 'Route By' parameter). After upgrading the device, this field needs to be re-configured to one of the remaining options (**IP Group** or **Dest Address**). ▪ Coder choice, played DTMF method (RFC 2833 or In Band), and SRTP are now configurable for Test Calls. After upgrading the device, these need to be configured. **Applicable Products:** All.
SBC-9958	Due to improved adaptive memory configuration (SPD), the device performs a double reset when the device is software upgraded for the first time. **Applicable Products:** Mediant 500C; Mediant 800C.

2.30.20.3 Resolved Constraints

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

Table 2-62: Resolved Constraints in Version 7.20A.252.011

Incident	Description
SBC-152338	The Intelligent Platform Management (IPMI) chassis indicators (i.e., status of fans, chassis temperature and power supply) are currently unavailable from the device's management interfaces. However, these indicators can be viewed directly from the Integrated Lights Out (iLO 5) interface (Web, SNMP or REST). **Applicable Products:** Mediant 9000 Rev. B; Mediant 9030; Mediant 9080.
SBC-13229	When the Admin user creates a Call Admission Control Profile, the same Admin user cannot edit this profile after a device reset. **Applicable Products:** All.
SBC-13190	When running both Debug Recording and 30,000 concurrent calls, the device runs out of memory buffers and as a result, an HA switchover occurs. **Applicable Products:** Mediant 9000 HA.
SBC-13021	Modifying the name of the Maintenance network interface in the IP Interfaces table causes HA to fail. **Applicable Products:** HA.
SBC-12847 / SBC-15788	The device generates a TLS certificate expiry alarm that cannot be cleared even though the associated TLS Context row was deleted. **Applicable Products:** All.

Incident	Description
SBC-12745	Fax transcoding fails (T.38 negotiation) for SBC calls. **Applicable Products:** All.
SBC-12591	When the device applies a configured Message Manipulation rule that removes the Request-URI header to a call, it resets. **Applicable Products:** All.
SBC-12572	The device stops sending SIP REGISTER messages to the IP side when registration is by Trunk Group and the Trunk Group Settings is modified. As a result, registration fails. **Applicable Products:** Gateway.
SBC-12448	The device doesn't trigger the session timer on specific call flows (refresher sends re-INVITE \ UPDATE without Session-Expires header). As a result, the call is disconnected. **Applicable Products:** All.
SBC-12415	Debug Recording causes some syslog error messages "drPollIpFilterSocket: Socket recv failed with error". **Applicable Products:** All.
SBC-12283	The output of the CLI command **show voip cpu-stats** always displays 0%. **Applicable Products:** All.
SBC-12265	The device's Web interface doesn't display the User Information table when the License Key is obtained from the Floating License. **Applicable Products:** All.
SBC-12109	The device's Pre-Parsing Message Manipulation causes a corrupted header (race condition that creates memory overrun). **Applicable Products:** All.
SBC-12011	The Web interface erroneously displays the error message "Error getting peer address" for the HA Network Monitor feature **Applicable Products:** All.
SBC-11933	The device tries allocating DSPs for call transfer (which it shouldn't) and the transfer fails. **Applicable Products:** All.
SBC-11744	The device's TCP port 2424 is opened by default, creating a security breach. **Applicable Products:** All.
SBC-11317	Downloading the device's Configuration Package file through SFTP (with keys) fails. **Applicable Products:** All.
SBC-10882	The HTTP proxy settings in the downloaded CLI script is listed in the wrong order and therefore, the file cannot be loaded to the device. **Applicable Products:** All.
SBC-10861	The device sends an alarm indicating ARM connection failure if it reconnects successfully to ARM. **Applicable Products:** All.
SBC-10719	In response to PRACK, the device sends a SIP 200 OK with a Contact header (but according to RFC 3262, it should not add the Contact header). **Applicable Products:** All.

Incident	Description
SBC-10676	The device sends alarms relating to a high CPU overload after upgrading to Version 7.20A.204 **Applicable Products:** All.
SBC-10459	The device reports incorrect packet loss (PL) statistics to OVOC in a specific scenario (upon receiving incorrect report or RTCP from remote side). **Applicable Products:** All.
SBC-9925	The device's management interfaces display the wrong speed for the Ethernet ports when the NIC is 20 Gbps. **Applicable Products:** All.
SBC-11610 / SBC-12135	When the device experiences a CPU overload, it resets. **Applicable Products:** All.
SBC-8631 (VI#154056)	Loading a CLI Script file through the Web interface automatically resets the device. (Now it can be done with or without a reset.) **Applicable Products:** All.
SBC-9329 (VI#155107)	If the device receives early media (18x + SDP) for an SBC call that doesn't support video (port in the 'm=video' line is '0'), then upon a 200 OK, the device erroneously sends a 200 OK with the same port for media and video. **Applicable Products:** All.
SBC-9696 (VI#155708)	The Web interface's SBC Configuration Wizard doesn’t save the WAN NAT IP address. **Applicable Products:** All.

2.30.21 Version 7.20A.250.413

This version includes new features and known constraints.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.1116 and EMS/SEM Version 7.2.3113.

2.30.21.1 New Features

This section describes the new features introduced in this version.

2.30.21.1.1 Periodic CDR Transfer to Remote SFTP Server

CDRs that are locally stored on the device can be transferred periodically to remote SFTP servers. The CDRs are sent in the same file format as stored on the device - compressed (GZIP), comma-separated value (CSV). The servers (currently, up to two) are configured in the new SBC CDR Remote Servers table (Troubleshoot menu > Troubleshoot tab > Call detail Record > SBC CDR Remote Servers). In addition, the following new standalone parameters have been added to the Call Detail Record Settings page:

- 'CDR Servers Send Period' - defines the periodic interval (in seconds) at which the device checks if a CDR file is available for sending to the remote server
- 'CDR Servers Bulk Size' – defines the maximum number of files that the device can send to the remote server per transfer operation (i.e., batch of files)
- 'Pending CDR Files' (read-only) - displays the number of CDR files that are waiting to be sent to the remote server

The CDR servers (including number of pending files) are also shown in the new CLI command, `show cdr-servers`.

If the device fails to send CDRs to **all** the configured servers, the new SNMP alarm, acCDRServerAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.142) is sent.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.30.21.1.2 New HA Network Monitor Status for Unresolved Hostnames

For the HA Network Monitor feature, if the destination host is configured with a hostname and it cannot be resolved into an IP address, the device displays a status message in the HA Network Monitor table indicating this ("Host not resolved").

Applicable Application: SBC.

Applicable Products: Mediant 500; Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.30.21.2 Known Constraints

This section lists known constraints.

Table 2-63: Resolved Constraints in Version 7.20A.250.413

Incident	Description
SBC-13833	When sending CDR files to a remote SFTP server during high traffic load (CPS), in rare cases the server may receive an unzipped file with the .zip filename extension, which is invalid (even though its contents are valid). **Applicable Products:** Mediant 90xx; Mediant Software.

2.30.22 Version 7.20A.250.273

This version includes resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.164 and EMS/SEM Version 7.2.3113.

2.30.22.1 Resolved Constraints

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

Table 2-64: Resolved Constraints in Version 7.20A.250.273

Incident	Description
SBC-12224	The device experiences a problem with stack creation in standalone mode (not HA), which produces a network interface error. **Applicable Products:** Mediant CE

2.30.23 Version 7.20A.250.256

This version includes new features and resolved constraints only.

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.164 and EMS/SEM Version 7.2.3113.

2.30.23.1 New Features

This section describes the new features introduced in this version.

2.30.23.1.1 Maximum DNS-Resolved IP Addresses per Proxy Set

The maximum number of DNS-resolved IP addresses per Proxy Set has been increased from 15 to 50 for Mediant Software 8-16GB memory.

Applicable Application: SBC.

Applicable Products: Mediant Software (8-16GB).

2.30.23.1.2 Call Forking with ICE in Microsoft Teams Environment

The device now supports working in a Microsoft Teams environment that implements call forking with Interactive Connectivity Establishment (ICE). The only required device configuration for this feature is enabling ICE (STUN message handling) for the IP Group representing Microsoft Teams (existing 'ICE Mode' parameter set to **Lite**).

Applicable Application: All.

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

2.30.23.2 Resolved Constraints

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

Table 2-65: Resolved Constraints in Version 7.20A.250.256

Incident	Description
SBC-9664 (VI-155567)	Modifications on the Web interface's Trunk Group page doesn't affect the registration\un-registration of the Trunk Group. As a result, registration fails. **Applicable Products:** Gateway.
SBC-12100	The device's optimized syslog contains “^^” prefix on each line (which should not appear). **Applicable Products:** SBC.
SBC-11913	In certain scenarios, the device fails to remove users (doesn't unregister them) from its users' database, resulting in a database overflow. **Applicable Products:** SBC.
SBC-11867	The device's CLI menu “voip > application” was removed (it should be hidden). As a result, CLI Script file fails when it includes an enable application setting associated with this command path. **Applicable Products:** SBC.

Incident	Description
SBC-11808	When the device is configured with 1+1 port redundancy and the cable is later disconnected from the active Ethernet port, a device reset is required. **Applicable Products:** SBC.
SBC-11747	The device fails to process SIP PRACK correctly for specific scenarios (received 18x while PRACK in process). As a result, the call fails. **Applicable Products:** SBC.
SBC-11589	The device crashes (resets) due to several DSP errors such as “Max number of failures (type=200) was reached for Dsp 52. Dsp is refreshed” and “Restart reason of DSP #52 is: Keep_Alive_Failure (RDC=1653)”. **Applicable Products:** SBC.
SBC-11572	The device sends a SIP CANCEL message with the wrong Reason header value. Instead of "Reason: SIP ;cause=200 ;text="Call completed elsewhere"" it sends "Reason: SIP ;cause=400 ;text="local"". **Applicable Products:** SBC.
SBC-11548	The device crashes (resets) with exception information of "TASK:SPMR" **Applicable Products:** SBC.
SBC-11496	When a SIP Connect user registers with the device on two different SIP Interfaces, the device fails to handle responses from the user. As a result, calls fail. **Applicable Products:** SBC.
SBC-11392	The device experiences DSP utilization errors ("not enough utilization for resource 14"). As a result, no voice is experienced. **Applicable Products:** SBC.
SBC-11269	When the device receives a SIP 200 OK with a large Allow header, it crashes (resets). **Applicable Products:** SBC.
SBC-11252	The RAI alarm is not functioning correctly (sometimes false alarms). **Applicable Products:** Gateway.
SBC-10939	When the Proxy Set is configured with a DNS, for every DNS-resolved IP address received, the device sends the trap message "TRAP: E_acProxyConnectionLost[2] CLEAR Proxy found" to OVOC (flooding OVOC with these messages). **Applicable Products:** SBC.
SBC-10871	For a direct media session, when the device receives an SDP offer with 'a=sendonly', it answers with 'a=sendonly' (instead of 'a=recvonly'). As a result, direct media ends. **Applicable Products:** SBC.
SBC-10459	The device sends incorrect packet loss report values to OVOC **Applicable Products:** SBC.
SBC-10424	When upgrading the License Key for an HA system using the Hitless method, after the upgrade, the active unit shows an alarm about a License Key mismatch. **Applicable Products:** HA.

Incident	Description
SBC-9886 / SBC-10049	When the device receives STUN responses, it doesn't latch the RTP to the correct STUN (should latch RTP according to the STUN with the highest priority). As a result, no voice is experienced. **Applicable Products:** SBC.
SBC-11568 / SBC-11603	The device crashes (resets) when the 'Destination Phone Pattern' parameter in the Tel-to-IP Manipulation Table is longer than 50 characters. **Applicable Products:** Gateway.

2.30.24 Version 7.20A.250.003

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

Note: This version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.6.164 and EMS/SEM Version 7.2.3113.

2.30.24.1 New Features

This section describes the new features introduced in this version.

2.30.24.1.1 24-FXS Ports Support

The device now supports up to 24 FXS ports (i.e., six FXS modules, each providing four ports). This applies to the indoor-outdoor FXS module (CPN M1KB-VM-4FXS-O). Up until now, up to 20 FXS ports were supported.

Note: When installed with 24 FXS ports, only up to 20 FXS ports can be active (process voice traffic) simultaneously.

Applicable Application: Gateway.

Applicable Products: Mediant 1000B.

2.30.24.1.2 WebRTC License Key Update

The License Key for WebRTC now defines the ordered maximum number of concurrent WebRTC sessions. Up until now, the License Key simply enabled WebRTC. The License Key that is displayed in the device's management interfaces (e.g., License Key page) indicates the number of WebRTC sessions.

Note: For Customers with an old License Key, the management interfaces will display the WebRTC support (enabled or disabled) as in previous releases (without any indication about sessions).

Applicable Application: All.

Applicable Products: All.

2.30.24.1.3 New License Key for Microsoft Teams Support

A new License Key has been introduced ("SW/TEAMS") that enables Microsoft Teams Direct Routing support on the device. The License Key enables the following:

- Connecting and pairing of the device with Microsoft Teams Hub for Direct Routing
- Connecting the device to any SIP trunk, PSTN line or customer-owned telephony

equipment such as third-party PBXs, analog devices, and Microsoft Phone System

The Microsoft License Key ("MSFT") must also be enabled on the device to activate the Microsoft Teams feature (most of AudioCodes devices are shipped by default with this license, except Mediant 500 Gateway & E-SBC, and Mediant 500L Gateway & E-SBC).

Note:

- An optional license to support HA-pair with Microsoft Teams can also be purchased ("SW/TEAMS/R").
- The "SW/TEAMS" license automatically enables the following voice coders:
  - SILK Narrowband
  - SILK Wideband
  - OPUS Narrowband
  - OPUS Wideband
- Number of required SBC sessions must be ordered separately.
- If media transcoding is required, the appropriate transcoding license sessions must be ordered separately.

Applicable Application: SBC.

Applicable Products: All.

2.30.24.1.4 Mediant CE in Microsoft Azure Environment

Mediant CE now supports deployment in a Microsoft Azure environment. Up until now, this type of deployment was available for evaluation purposes only.

Applicable Application: SBC.

Applicable Products: Mediant CE.

2.30.24.1.5 Unlimited Multiple Registrations per User with Same Contact

The device supports multiple user registrations containing identical SIP Contact headers. Up until now, the number of such multiple registrations (each identified by a unique AOR) per user was limited. It is now unlimited.

Applicable Application: SBC.

Applicable Products: All.

2.30.24.1.6 Enhanced Registrar Server Stickiness Feature

The Registrar Stickiness feature has been enhanced for handling refresh REGISTER messages. Up until now, when enabled ('Registrar Stickiness' parameter in the Accounts table configured to **Enable**), refresh REGISTER messages for the Account was always sent to the registrar server that accepted the previous REGISTER request. The 'Registrar Stickiness' parameter now provides an additional optional value—**Enable for Non-Register Requests**—which re-starts the registration process for refresh REGISTER messages, sending the message to one of the registrar servers according to the settings of the Proxy Set associated with the Account's Serving IP Group. For non-REGISTER messages, the behavior is the same as for the existing **Enable** option - once registered to the registrar, these messages are always sent to this registrar.

Applicable Application: Gateway & SBC.

Applicable Products: All.

2.30.24.1.7 SIP Account Re-registration upon INVITE Failure

The device can now be configured to re-register an Account upon the receipt of specific SIP response codes for a failed INVITE message. This is configured by the new 'Re-Register on Invite Failure' (**Enable** / **Disable**) parameter in the Accounts table. The response codes are configured by the new global parameter, AccountInviteFailureTriggerCodes.

Applicable Application: Gateway & SBC.

Applicable Products: All.

2.30.24.1.8 Resolution of DNS-A and SRV Queries per Proxy Set Address

When a Proxy Set includes an address that is configured with an FQDN, the maximum number of resolved domain names and IP addresses for SRV and DNS-A queries respectively, have been increased per proxy address:

- An SRV query sent by the device can return up to 50 hostnames (instead of 4 as in previous releases)
- A DNS-A (of a hostname) query sent by the device can resolve into up to 50 IP addresses (instead of 15 as in previous releases)

Applicable Application: All.

Applicable Products: All.

2.30.24.1.9 SIP 3xx Redirect Response Handling Enhancement

The device's handling of SIP 3xx responses (for INVITE requests) has been enhanced. The configuration of this handling is done by the existing parameter, 'Remote 3xx Mode' (SBCRemote3xxBehavior) in the IP Profile table. This parameter now provides two new optional values:

- IP Group Name: If the 'SIP Group Name' parameter of the dialog-initiating UA is configured with a non-empty value, the device changes the host part of the Contact header in the 3xx response to this value, before forwarding the 3xx response to the dialog-initiating UA.
- Local Host: The device changes the host part of the Contact header in the 3xx response before forwarding the 3xx response to the dialog-initiating UA. If the 'Local Host Name' parameter of the IP Group of the dialog-initiating UA is configured with a non-empty value, the device changes the host part of the Contact header to this value. If the 'Local Host Name' is empty, the device changes the host part to the device's IP address (the same IP address used in the SIP Via and Contact headers of messages sent to the IP Group).

Applicable Application: SBC.

Applicable Products: All.

2.30.24.1.10 Handling Advice of Charge Information in XML Format

The device can now handle SIP INFO messages containing advice-of-charge (AOC) information in XML format ('application/vnd.etsi.aoc+xml' body), for IP-to-Tel calls. Message Manipulation rules must be applied to the SIP INFO message to add a SIP AOC header with the AOC information from the XML body, and to remove the XML body.

Applicable Application: Gateway (Digital).

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

2.30.24.1.11 SIP Response Codes Exclusion from IDS

The device's Intrusion Detection System (IDS) feature can be configured to ignore specified SIP response codes as reasons for SIP-dialog establishment failures. If a specified SIP

response code is received, the IDS feature does not include them in its' count of establishment failures.

This is configured by the new parameter:

- INI: IDSExcludedResponseCodes
- Web: 'Excluded Response Codes' (Signaling & Media > Intrusion Detection > IDS General Settings)
- CLI: configure voip > ids global-parameters > excluded-responses

Note:

- The parameter applies only to rejected responses received from the upstream server; not rejected responses generated by the device (except for 404).
- The response codes 401 and 407 are considered authentication failures and thus, are not applicable to this parameter.

The new event type—"establish-cac-reject" (Syslog) and "CAC rejection" (SNMP)—has been added to indicate "Dialog Establishment Failure" due to Call Admission Control (CAC) rejections.

The existing IDSAlarmClearPeriod ini file parameter has been added to the other management platforms:

- CLI: configure voip > ids global-parameters > alarm-clear-period
- Web: 'Alarm Clear Period' (Signaling & Media > Intrusion Detection > IDS General Settings)

Applicable Application: All.

Applicable Products: All.

2.30.24.1.12 SIPREC of SRTP-to-SRTP Calls Decrypted to RTP for SRS

For SIP-based media recording (SIPREC) of SRTP calls, the device can now send the recorded packets to the Session Recording Server (SRS) as RTP packets (i.e., decrypted). This is useful for SRS's that don't support the handling of recorded SRTP media. The feature is supported by adding an IP Profile for the SRS and configuring its' 'SBC Media Security Mode' parameter to **RTP**.

Applicable Application: SBC & Gateway.

Applicable Products: Mediant 500; Mediant 500L; Mediant 800; Mediant 2600/4000; Mediant 9000; Mediant Software.

2.30.24.1.13 NAT Traversal for NGINX with OVOC

When the device is located behind NAT, OVOC can only communicate with the device's embedded NGINX HTTP-based proxy using the device's public static NAT address. However, by default, the device sends OVOC its private address (in the proprietary X-AC-Proxy-URL header). To send its public (global) address, the new parameter, HttpProxyGlobalAddress (http-proxy-global-address) has been added. This parameter defines the global address (dotted-decimal notation) that it uses in the X-AC-Proxy-URL header for HTTP requests that the device sends to OVOC.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.14 Default UDP Port Spacing

The default for UDP port spacing, configured by the UdpPortSpacing parameter, has been changed to 4 (instead of 5).

Applicable Application: All.

Applicable Products: Mediant 2600; Mediant 4000; Mediant 9000; Mediant Software.

2.30.24.1.15 24-Hour Support for UTC Offsets

The value range for configuring the Universal Time Coordinate (UTC) offset (in seconds) from the local time (configured by the NTPServerUTCOffset parameter) has been changed. The new range is from -86400 seconds (-24 hours) to +86400 seconds (+24 hours). Therefore, the offset is no longer limited to +/-12 hours, but now supports +/-24-hour offsets.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.16 Non-Operational HA Reduction for Switchovers and Upgrades

Hitless software upgrades and active-redundant switchovers for the device-pair in High-Availability (HA) mode has been optimized to reduce the duration that the HA system is non-operational during these operations.

Applicable Application: All.

Applicable Products: HA.

2.30.24.1.17 CLI Command Path and Name Changes

The following changes have been done to the CLI:

- CLI paths:
  - charge-code (Charge Codes table): configure voip > gateway dtmf-supp-service charge-code
  - inbound-map-set (GWInboundManipulationSet): configure voip > message > settings > inbound-map-set
  - outbound-map-set (GWOutboundManipulationSet): configure voip > message > settings > outbound-map-set
- CLI command names:
  - ssh-redundant-device-port (instead of ssh-redundant-proxy-port)

Applicable Application: All.

Applicable Products: All.

2.30.24.1.18 ISDN Progress Indicator and SDP Body for Tel-to-IP Calls

The device can now be configured to send SIP 180 messages without an SDP body depending on the value of the Progress Indicator (PI) information element (IE) in the received ISDN Progress message. This is configured by the new ini file parameter, NoSdpForIsdnPi (or CLI command, no-sdp-for-isdn-pi). The configuration value is a bit field, allowing you to specify more than one PI. The default is 0, meaning that SDP is included in the outgoing SIP 180 message, regardless of PI value.

Applicable Application: Gateway (PRI).

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

2.30.24.1.19 Name Field for Various Configuration Tables

The 'Name' field, which allows the administrator to configure a descriptive name for the configuration entity, has been added to the following configuration tables:

- Alternative Routing Reasons table
- Accounts table
- Call Setup Rules table

Applicable Application: All.

Applicable Products: All.

2.30.24.1.20 AES-256 SRTP Cipher Suites

The device now supports the following additional cipher encryption algorithms (crypto suites) according to RFC 6188 for SRTP:

- AES-CM encryption with a 256-bit key and HMAC-SHA1 message authentication with a 32-bit tag (AES_256_CM_HMAC_SHA1_32)
- AES-CM encryption with a 256-bit key and HMAC-SHA1 message authentication with an 80-bit tag (AES_256_CM_HMAC_SHA1_80)

The feature is supported by the existing parameter, SRTPofferedSuites, which now provides two additional optional values – AES-256-CM-HMAC-SHA1-32 and AES-256-CM-HMAC-SHA1-80.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.21 OAuth2 Token-based SIP Authentication

The device can authenticate any incoming SIP requests (e.g., REGISTER and INVITE) from client applications, based on access tokens with an OAuth2 Authorization Server (RFC 7662 and Internet Draft draft-ietf-sipcore-sip-authn-02 "Third-Party Authentication for Session Initiation Protocol (SIP)).

When the device receives a SIP request (with an OAuth access token) from a client application (e.g., WebRTC client), the device introspects the token with the OAuth Authorization server (HTTP server). Upon successful introspection, the device allows the client access to the device's resources (e.g., registration and calls) and continues to handle and process the SIP request as usual.

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

- New parameter added to the IP Groups table - 'SBC Server Authentication' (IPGroup_TypeSBCServerAuthType), which defines the authentication method:
  - [-1] According to Global Parameter (default, according to SBCServerAuthMode)
  - [0] Authentication is performed locally
  - [2] According to draft-sterman-aaa-sip-01
  - [3] Authenticate with OAuth authorization
- New parameter added to the IP Groups table - 'OAuth HTTP Service' (OAuthHTTPService_IPGroup), which assigns a Remote Web Service that is configured as the Authorization server when authenticating by OAuth.

- Existing IP Group table parameter, 'Authentication Method List' now supports the value "setup-invite" to support authenticating only setup INVITE requests and not re-INVITE requests

Applicable Application: SBC.

Applicable Products: All.

2.30.24.1.22 Message for Hidden Tables Removed from ini File

For configuration tables that are not displayed / "hidden" (due to security) in the ini file when they are modified, the message in the ini file indicating that the table has been modified will no longer be displayed.

Applicable Application: SBC and Gateway.

Applicable Products: All.

2.30.24.1.23 Device Uptime Display Format Changed

The format of the device uptime that is displayed in the 'Device Up Time' field on the Web interface's Device Information page (Monitor menu > Monitor tab > Summary folder > Device Information) has changed. The hundredth of a second is now displayed after a dot ("th" removed).

Applicable Application: All.

Applicable Products: All.

2.30.24.1.24 Temperature Indication for Media Components

For the Media Cluster feature, the 'Temperature' field has been added to the Media Components table. The field displays the Media Component's (i.e., Mediant 4000) CPU and DSP temperatures.

Applicable Application: SBC.

Applicable Products: Mediant 9000 (MC); Mediant Software (MC).

2.30.24.1.25 SIP Local and Remote Tags for CDRs

Gateway and SBC CDRs that are generated by the device can be customized to add the SIP 'tag' parameter values, which may be present in the From and To headers, for example:

```
To: Bob@company.com; tag = 1930394343437322
```

The tags are included in the CDR using the new CDR fields—SIP Local Tag (445) and SIP Remote Tag (446)—in the existing SBC CDR Format table and Gateway (Test) CDR Format table. The "local" tag is generated by the device in the outgoing SIP message while the "remote" tag is received in the incoming message. These fields are applicable to all types of CDRs, except Syslog SBC media. By default, these fields are not included in the CDR.

Note: The SIP tags are not always included in all CDR report types. For example, both tags are not included in Call-End CDR report types, while for Call-Connect CDR report types they are typically included.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.26 Hostname for HA Network Monitoring

Monitored network entities (destinations) for the device's HA Network Monitor feature can now be configured as hostnames or FQDNs (in addition to IP addresses in dotted-decimal notation, as supported previously). This is configured in the existing HA Network Monitor table (HaNetworkMonitor).

Applicable Application: SBC & Gateway.

Applicable Products: Mediant 500; Mediant 800; Mediant 2600/4000; Mediant 9000; Mediant Software.

2.30.24.1.27 Minor Severity for acProxyConnectionLost SNMP Alarm

The existing SNMP alarm, acProxyConnectionLost has been enhanced to indicate a Minor severity alarm. This severity is raised upon any one of the following scenarios:

- All proxy servers were online and now at least one proxy server in the Proxy Set is offline (and at least one proxy server is still online)
- All proxy servers were offline and now at least one proxy server in the Proxy Set is online (and at least one proxy server is still offline)

Applicable Application: SBC & Gateway.

Applicable Products: All.

2.30.24.1.28 Device Authentication for the Automatic Update Feature

Device authentication with an HTTP/S or FTP server for the Automatic Update feature has changed. If the username and password (for basic authentication) is not included in the existing parameter AutoCmpFileUrl (which is used to configure the URL to the .cmp file), as supported in earlier versions, the device uses the username and password configured by the new parameter, AUPDUserPassword (configure system > automatic-update > credentials). The syntax value is 'username:password'. This new parameter applies to basic and digest authentication (MD5).

The AUPDDigestUsername and AUPDDigestPassword parameters are now obsolete. If these parameters were configured and the device is subsequently upgraded to this version, the username and password configured for these parameters are automatically configured for the new AUPDUserPassword parameter.

Applicable Application: All.

Applicable Products: All. -

2.30.24.1.29 Debug Recording Packets Filtered by SIP Messages

Debug recording packets generated by the device can now be filtered to include only SIP messages (without Syslog messages). This is supported by configuring the 'Log Type' parameter in the Logging Filters table to the new optional value, **SIP Only**.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.30 Improved Log Filtering

The device's log filtering feature (configured in the Logging Filters table) has been improved. Up until now, the device sent unfiltered syslog messages in the early call processing stages (e.g., Classification) and only once the source and destination IP Groups were determined did it start sending filtered Syslog messages according to configuration. Now, the initial syslog messages are not sent; only the filtered syslog mesages.

Applicable Application: All.

Applicable Products: All.

2.30.24.1.31 CLI Command Update for PSTN Debug Recording and Trace Level

PSTN debugging through CLI has been updated as follows:

- The command **debug voip interface trace-level** is now obsolete. The trace level can now only be configured per interface, using the existing command, **configure voip** > **interface** > **trace-level**.
- The command **debug pstn** is now obsolete. To send PSTN traces to Syslog, the following command has been added: **configure troubleshoot > pstn-debug**.
- To start a PSTN trace:
  - Per trunk (trace level is configured by the **debug voip interface trace level** command – see above): **configure troubleshoot** > **logging logging-filters** (existing command)
  - All trunks (whose trace level have been configured by the **debug voip interface trace level** command - see above): **debug debug-recording <IP Address> pstn-trace** (existing command)

Applicable Application: Gateway.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B.

2.30.24.1.32 Ping and Traceroute CLI Enhancements

The following enhancements have been introduced to the ping and traceroute CLI commands:

- Ping: QoS (ToS or Class) of the pinged packets can now be configured:

```
ping … [tos|traffic-class <0-254>]
```

- Traceroute: Protocol type (UDP or ICMP) of the traceroute can now be configured:

```
traceroute … proto [udp|icmp]
```

Applicable Application: All.

Applicable Products: All.

2.30.24.2 Known Constraints

This section lists known constraints.

Table 2-66: Known Constraints in Version 7.20A.250.003

Incident	Description
SBC- 15627	Mediant VE installed on Microsoft Hyper-V is currently not supported on the Windows Server 2019 host. **Applicable Products:** Mediant VE (on Hyper-V).
SBC-11399	The Test Call feature cannot accept incoming calls. A workaround is to first configure a Test Call rule for an outgoing call ('Call Party' parameter configured to Caller) and activate it (by clicking Dial), and then edit the same rule by changing the 'Call Party' parameter to Called. **Applicable Products:** All.
SBC-11356	For Azure platform, when set to use instance type (size) "Standard_D4_v2", the device (Media Components - MCs) crash (reset). **Applicable Products:** Mediant CE.
SBC-11343	The WebRTC feature will not function with the new Google Chrome version that will be released in a few weeks. **Applicable Products:** All.

Incident	Description
SBC-11197	Call forking performed by the device does not function. **Applicable Products:** Mediant CE.
SBC-11172	After editing the description of a BRI port on the Web interface's Monitor page, the port's status, displayed on the Trunks & Channels Status page, is incorrect. **Applicable Products:** Mediant 500.
SBC-10527	For the Gateway application, when the SrtpOfferedSuites is configured to All, the device sends the SDP Offer with only four crypto lines, excluding AES 256. To offer AES 256, the parameter must be configured to the AES 256 option. **Applicable Products:** Gateway.
SBC-9523	Sometimes the Web browser doesn't display the 'IP Network', 'Signaling & Media' and 'Administration' tabs in the Web interface. Pressing the F5 key resolves this display problem. **Applicable Products:** All.
SBC-175	When downgrading the software version, Hitless Upgrade is not supported. **Applicable Products:** HA.
SBC-11568 / SBC-11603	If the manipulation tables of the Gateway application are configured with a pattern that exceeds 51 characters, the device crashes (resets). A workaround is to split the pattern into new patterns that are shorter than 51 characters). **Applicable Products:** Gateway.

2.30.24.3 Resolved Constraints

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

Table 2-67: Resolved Constraints in Version 7.20A.250.003

Incident	Description
SBC-9728 (VI-155751)	When the device sends an HTTP GET message, it uses an IP address in the Host instead of an FQDN, as required by the HTTP 1.1 RFC. **Applicable Products:** All.
SBC-9694 (VI-155701)	The device resets due to configuration of a Message Manipulation variable that exceeds its range (0-13). **Applicable Products:** All.
SBC-9691 (VI-155696)	When performing a debug recording, SIP packets are not marked with the correct DSCP QoS. **Applicable Products:** All.
SBC-9642 (VI-155619)	The device should use default of "4" for the UDP Port Spacing parameter (currently, the default is "5"). **Applicable Products:** Mediant 4000; Mediant Software.
SBC-9592 (VI-155532)	When trying to use the Rand.Number search key in the Call Setup Rule table, an error is generated: "CallSetupRules-CrossValidation: Rand.number.1.10 MATRIX CallSetupRules; Unable to Activate Line(29) since it is Invalid". **Applicable Products:** All.
SBC-10171 (VI-154923)	The parameter 'Digital Out Of Service Behavior Per Trunk' has a mismatch between the Web interface and CLI. **Applicable Products:** All.

Incident	Description
SBC-9535 (VI-155448)	Configuring the IP-to-IP Routing table with alternative routing rules based on a condition fails. **Applicable Products:** All.
SBC-9515 (VI-155407)	The CLI command TraceRoute doen't function. **Applicable Products:** All.
SBC-9509 (VI-155395)	If the ini file is downloaded from the device, attempting to upload it to the device fails if the parameter OSNInternalVLAN is configured to 1. **Applicable Products:** All.
SBC-9489 (VI-155352)	The device's firewall prevents the option to configure an access list rule with protocol 'SIP'. **Applicable Products:** All.
SBC-9428 (VI-155253)	When the Proxy Set is associated with two SIP Interfaces, it gives precedence to the GW SIP Interface, which may cause issues with unsupported transport types on this SIP Interface. As a result, connectivity fails. **Applicable Products:** All.
SBC-9386 (VI-155189)	The device resets upon the receipt of an invalid RTCP-XR packet. **Applicable Products:** All.
SBC-9369 (VI-155167)	The device resets with the exception information of TASK DSPD. **Applicable Products:** All.
SBC-9318 (VI-155081)	The device generates syslog messages with "SYS_HA: KA_MONITOR_POLL_TIMEOUT" **Applicable Products:** HA Devices.
SBC-9312 (VI-155074)	The device resets due to the HW Watchdog with exception Signal 904, Task IDLE **Applicable Products:** All.
SBC-9203 (VI-154921)	The device has the incorrect timer calculation in Session-Expires when operating in Transparent mode **Applicable Products:** All.
SBC-9168 (VI-154869)	The device displays CPU overload alarms for the NWST task. **Applicable Products:** All.
SBC-8857 (VI-154409)	The device repeatedly generates syslog messages with "VQMON_DIVIDE". **Applicable Products:** All.
SBC-8843 (VI-154386)	The device doesn't send calls that were not established (due to an ARM routing error, for example) to the SIP call flow ladder in OVOC. **Applicable Products:** All.
SBC-8720 (VI-154205)	When the device contains the DATA feature key, it resets when running the SNMP walk command. **Applicable Products:** All.
SBC-8541 (VI-153895)	The device doesn't send the SIP Privacy header to ARM, which may result in the display of the Calling Party Number, which is not allowed. **Applicable Products:** All.

Incident	Description
VI-155352	The "sip" special string value for the 'Protocol' field in the Firewall table generates an error. This bug has been resolved and the string is now no longer required for specifying SIP ports. Instead, specific udp/tcp rules must be configured for SIP traffic according to the SIP Interfaces table. Therefore, before upgrading to this version, replace the rules containing the "sip" string. **Applicable Products:** All.
SBC-109050	The performance monitoring SNMP MIB, acPMSIPIPGroupInDialogs has incorrect counter calculation. **Applicable Products:** All.
SBC-10846	The device doesn't save the CLI Privilege password in the backed-up ini file. **Applicable Products:** All.
SBC-10812	The **show voip subscribe list** CLI command resets the device. **Applicable Products:** All.
SBC-10717	When the **set-default snapshot** CLI command is run from its old, hidden (but supported) directory, the device resets. **Applicable Products:** Mediant 9000; Mediant Software.
SBC-10597	If the user's password expires (configured by the Password Age parameter), upon a login attempt the user is prompted to change the password. However, after the user changes the password and logs in to the Web interface with the new password, no indication occurs that the user must click the Save button (i.e., not encircled by red). If it is not clicked, the user will be prompted again on the next login attempt (or for HA systems, when a switchover occurs) to change the expired password. **Applicable Products:** All.
SBC-10587	The device's SIPREC metadata format doesn't comply with RFC 7865 - UUID for each metadata should be 128 bits (16 bytes) and not 64 bits (8 bytes). **Applicable Products:** All.
SBC-10576	The IpProfile_SBCRemoveCryptoLifetimeInSDP parameter in the IP Profiles table doesn't remove the crypto lifetime from SIP 18x. **Applicable Products:** All.
SBC-10556	The performance monitoring SNMP MIB, acPMSBCMediaLegsVal shows incorrect number of active media channels when some calls fail upon a switchover. **Applicable Products:** All.
SBC-10538	The **default-window-height** CLI command (window resize) doesn't function. **Applicable Products:** All.
SBC-10320	The **show dsp status** CLI command displays incorrect units ('sessions' instead of 'DSP resources'). **Applicable Products:** All.
SBC-10320	The number of channels displayed in the 'Num DSP Channels' field in the ini file is incorrect. As the number of channels depends on many factors (features and coders), this field has been removed from the ini file. **Applicable Products:** All.
SBC-9972	The device truncates the HTTP GET path and limits it to 125 characters, causing an incorrect HTTP GET query. **Applicable Products:** All.

Incident	Description
SBC-9942	When the Web interface's session timeout expires, it is not possible to reconnect to the device (only by refreshing the browser page). **Applicable Products:** All.
SBC-9893	The CDR sorting in the Web interface doesn't function. **Applicable Products:** All.
SBC-9792	The UTC offset is limited to +/-12 hours and therefore, it's impossible to set it to +13 (for example, for New Zealand). **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	
MP-1288		588	350	Hybrid	588	438	Transcoding: n/a GW: Table 3-15
				SBC-Only	300	300	
				GW-Only	288	288	
Mediant 2600		600	8,000	SBC-Only	600	600	Transcoding: Table 3-16
Mediant 4000		5,000	20,000	SBC-Only	5,000	3,000	Transcoding: Table 3-17
Mediant 4000B		5,000	20,000	SBC-Only	5,000	5,000	Transcoding: Table 3-19
Mediant 9000	Hyper-Threading (HT) Disabled	24,000	180,000	SBC-Only	16,000	16,000	Transcoding: Table 3-21
		24,000	0	SBC-Only	24,000	16,000	Transcoding: Table 3-21
	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 3-21
	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 3-23
	SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a
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 3-26
Mediant 9080	SIP Performance Profile	50,000	500,000	SBC-Only	50,000	30,000	Transcoding: n/a

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
			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 3-23
	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 3-25
Mediant 9000 Rev. B with Media Transcoders (MT-type)			60,000	200,000	SBC-Only	60,000	40,000	Transcoding: Table 3-25
Mediant 9080 with Media Transcoders (MT-type)			60,000	200,000	SBC-Only	60,000	40,000	Transcoding: Table 3-25
Mediant CE	AWS / EC2		40,000	0	SBC-Only	40,000	40,000	Forwarding: Table 3-28 Transcoding: Table 3-29
			20,000	100,000	SBC-Only	20,000	20,000	
	Azure		10,000	50,000	SBC-Only	10,000	10,000	Transcoding: Table 3-31
	VMware		1,000	10,000	SBC-Only	1,000	1,000	Transcoding: Table 3-32
Mediant VE	VMware	1 vCPU 2-GB RAM	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1/2/4 vCPU 8-GB RAM (legacy)	3,000	15,000	SBC-Only	3,000	2,000	1 vCPU (Transcoding: n/a) 2 vCPU (Transcoding: Table 3-34) 4 vCPU (Transcoding: Table 3-36)
		4/8 vCPU 16-GB RAM (legacy)	9,000	75,000	SBC-Only	6,000	5,000	4 vCPU (n/a) 8 vCPU (Transcoding: Table 3-38)
		4 vCPU 8-GB RAM (recommended)	3,000	15,000	SBC-Only	3,000	2,000	Transcoding: Table 3-33
		8 vCPU 16-GB RAM (recommended)	9,000	75,000	SBC-Only	6,000	5,000	Transcoding: Table 3-33
		16 vCPU 16-GB RAM (recommended)	9,000	75,000	SBC-Only	6,000	5,000	Transcoding: Table 3-33
	OpenStack KVM	1 vCPU 2-GB RAM	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1/2/4 vCPU 8-GB RAM	1,800	9,000	SBC-Only	1,800	1,400	1 vCPU (Transcoding: n/a) 2 vCPU (Transcoding: Table 3-34) 4 vCPU (Transcoding: Table 3-36)
		4/8 vCPU 16-GB RAM	4,000	75,000	SBC-Only	2,700	2,700	Transcoding: Table 3-38
		8 vCPU 32-GB RAM SR-IOV Intel NICs	24,000	75,000	SBC-Only	24,000	10,000	Transcoding: n/a
	Hyper-V	1 vCPU 2-GB RAM	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1/2/4 vCPU 4-GB RAM	900	10,000	SBC-Only	600	600	1 vCPU (Transcoding: n/a) 2 vCPU (Transcoding: Table 3-44) 4 vCPU (Transcoding: Table 3-46)
	Azure	DS1_v2	400	1,000	SBC-Only	400	400	Transcoding: Table 3-43
		DS2_v2	500	15,000	SBC-Only	500	500	Transcoding: Table 3-43

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
		DS3_v2	600	50,000	SBC-Only	600	600	Transcoding: Table 3-43
	AWS / EC2	r4.large	3,200	20,000	SBC-Only	3,200	3,200	Transcoding: n/a
		c4.2xlarge	2,000	75,000	SBC-Only	2,000	2,000	Transcoding: Table 3-40
		c4.8xlarge	3,200	75,000	SBC-Only	3,200	3,200	Transcoding: Table 3-41
Mediant VE with Media Transcoders	OpenStack KVM	8 vCPU 64-GB RAM SR-IOV Intel NICs	24,000	75,000	SBC-Only	24,000	12,000	MT-type (Transcoding: Table 3-48) vMT-type (Transcoding: Table 3-49)
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 3-50
		SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a

Notes:

- 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.

- Capacity of the Cloud Resilience Package (CRP) application is listed under "Registered Users".
- Capacity of the Lync Analog Device (LAD) application 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.
- Hyper-Threading (HT) is disabled by default on Mediant 9000 with 1G ports only. To enable HT, please refer to the *Mediant 9000 SBC Installation Manual*.
- Media Transcoding Cluster (MTC) feature is not supported by Mediant 9030 SBC.
- **Mediant 90xx SBC and Mediant VE 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 SRTP-RTP sessions is also effected 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.
- **Mediant 9030:** The SRTP Performance Profile is recommended for this product.
- **Mediant VE SBC with vMT-type Media Transcoder:** The host running the vMT virtual machine requires the following configuration:
  - √ At least 2.8 GHz CPU with Intel® AVX support
  - √ SR-IOV enabled NICs
  - √ KVM environment
  - √ 8 hyper-threaded vCPUs should be allocated to the vMT virtual machine (4 physical cores)
  - √ 4-GB RAM should be allocated to the vMT virtual machine
- **Mediant VE SBC and vMT-type Media Transcoder:** Codec-transcoding functionality is supported only on Intel CPUs with AVX enhancement. In addition, AVX support must be reflected on the vCPU of the SBC virtual machine.
- **Mediant VE SBC with Media Transcoder Cluster** is currently supported only on the OpenStack KVM hypervisor.

- **Mediant VE SBC for VMware:** The recommended profiles are applicable to when Intel Xeon Scalable Processors and Hyper-Threading are used. These profiles provide about the same capacity as the legacy profiles, but with only half of the physical vCPUs as each vCPU refers to a Hyper-Threaded core (logical). For example, a 4-vCPU virtual machine allocates only 2 physical cores. For minimum requirements, see Section 3.3.14.1 on page 199.
- **Mediant CE:** Based on the following instances:
  - √ AWS:
    - Signaling Components (SC): r4.2xlarge
    - Media Components (MC) - forwarding only: r4.large
    - Media Components (MC) - forwarding and transcoding: c4.4xlarge
  - √ Azure:
    - SC: DS3_v2
    - MC - forwarding only: DS1_v2, DS2_v2, or DS3_v2
    - MC - forwarding and transcoding: DS2_v2, DS3_v2, or DS4_v2
  - √ VMware:
    - SC: 4-vCPU (Hyper-Threaded), 16-GB RAM
    - MC - forwarding and transcoding: 8-vCPU (Hyper-Threaded), 8-GB RAM
- **Mediant SE:** For new deployments, it's highly recommended to use the DL360 G10 server. For exact specifications and BIOS settings, please contact your AudioCodes sales representative.

3.2 Capacity per Feature

The table below lists capacity per feature, per product.

Table 3-2: Feature Capacity per Product

Product	Max. Concurrent WebRTC Sessions (see Note #3)		Max. One-Voice Resiliency (OVR) Users	Max. Concurrent SIPREC Sessions (see Note #4)	Max. Concurrent MSRP Sessions
	Click-to-Call	Registered Agents			
MP-1288	-	-	-	150	100
Mediant 500	-	-	-	125	100
Mediant 500L	-	-	-	30	100
Mediant 800B	100	100	100	200	100
Mediant 800C	100	100	150	200	100
Mediant 1000B	-	-	50	-	100
Mediant 2600	600	600	-	300	100
Mediant 4000B / Mediant 4000	1,000	1,000	-	2,500	100
Mediant 9000	5,000	16,000	-	▪ **With Hyper-Threading:** 20,000 ▪ **Without Hyper-Threading:** 12,000	100
Mediant 9030	5,000	16,000	-	15,000	100
Mediant 9080	8,000	25,000	-	20,000	100
Mediant SE (see Note #1)	5,000	25,000	-	12,000	100
Mediant VE (see Note #2)	5,000	5,000	2,000	12,000	100
Mediant CE (see Note #2)	5,000	5,000	-	20,000	100

Note:

1. Using the approved SE server specifications with an Intel Xeon Gold 6126 processor. For the specifications, please contact AudioCodes.
2. The maximum number of WebRTC sessions cannot be higher than the number of SRTP sessions, as indicated in Table 3-1. Therefore, the actual maximum number of concurrent WebRTC sessions per deployment environment will be the lower of these numbers.
3. The capacity figures assume that a TLS key size of 2048-bit is used for the WebSocket and DTLS negotiation,
4. 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.

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.

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

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	30/24	√	-	-	220/226
	26/24	√	√	-	224/226
	26/24	√	√	√	224/226

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.

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

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 Mix	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

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				
	8	-	-	√	-	-	-	-	6	6	-	242
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" 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	-	-	-	-	-	-	114	96	400
	-	-	√	-	-	-	102	84	400
	-	-	-	-	√	-	78	66	400
	-	-	-	√	-	-	72	60	400
	-	-	-	-	-	√	54	48	400
	√	-	-	-	-	-	54	48	400
	-	√	-	-	-	-	42	42	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).

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	2025	365/371
	35/29	-	√	-	-	-	10/15	9/13	365/371
	35/29	-	-	√	-	-	1/5	1/5	365/371
	35/29	-	-	-	√	-	0/4	0/3	365/371
	27	-	-	-	-	√	0	0	373
8 x BRI 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 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 3-15: 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.

3.3.6 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 3.1 on page 165. 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 3-16: 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
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.

3.3.7 Mediant 4000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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 3-17: 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.

3.3.7.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-18: 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).

3.3.8 Mediant 4000B SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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 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.

3.3.8.1 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 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).

3.3.9 Mediant 9000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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 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.

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 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).

3.3.10 Mediant 9000 Rev. B / 9080 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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 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.

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 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).

3.3.11 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 3-25: 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).

3.3.12 Mediant 9030 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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 3-26: 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.

3.3.12.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-27: 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).

3.3.13 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.

3.3.13.1 Mediant CE SBC for AWS EC2

3.3.13.1.1 Forwarding Sessions

The number of concurrent forwarding sessions per MC is shown in the following table.

Table 3-28: Forwarding Capacity per MC Instance Type

MC Instance Type	Max. Forwarding Sessions
r4.large	3,200
c4.4xlarge	3,200

Note: Forwarding performance was tested in AWS Ireland Region.

3.3.13.1.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be of the AWS instance type c4.4xlarge. The number of supported transcoding sessions per MC is shown in the following table.

Table 3-29: Transcoding Capacity per c4.4xlarge MC

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	3,200	2,425
Profile 2	Profile 1	1,325	1,050
Profile 2	Profile 2	800	675
Profile 1	Profile 2 + AMR-NB / G.722	1,300	1,000
Profile 2	Profile 2 + AMR-NB / G.722	750	650
Profile 1	Profile 2 + AMR-WB (G.722.2)	375	350
Profile 2	Profile 2 + AMR-WB	300	275
Profile 1	Profile 2 + SILK-NB	1,050	900
Profile 2	Profile 2 + SILK-NB	675	600
Profile 1	Profile 2 + SILK-WB	625	575
Profile 2	Profile 2 + SILK-WB	450	450
Profile 1	Profile 2 + Opus-NB	650	550

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Basic**	**Extended**
Profile 2	Profile 2 + Opus-NB	475	425
Profile 1	Profile 2 + Opus-WB	500	425
Profile 2	Profile 2 + Opus-WB	375	350

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.

3.3.13.2 Mediant CE SBC for Azure

3.3.13.2.1 Forwarding Sessions

The number of concurrent forwarding sessions per Media Component (MC) is shown in the following table.

Table 3-30: Forwarding Capacity per MC

MC VM Size	Max. Forwarding Sessions
DS3_v2	475

3.3.13.2.2 Transcoding Sessions

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

Table 3-31: Transcoding Capacity per DS3_v2 MC

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	475	475
Profile 2	Profile 1	350	275
Profile 2	Profile 2	225	175
Profile 1	Profile 2 + AMR-NB / G.722	400	325
Profile 2	Profile 2 + AMR-NB / G.722	250	200
Profile 1	Profile 2 + AMR-WB (G.722.2)	125	100
Profile 2	Profile 2 + AMR-WB	100	75
Profile 1	Profile 2 + SILK-NB	300	275
Profile 2	Profile 2 + SILK-NB	200	175
Profile 1	Profile 2 + SILK-WB	175	150
Profile 2	Profile 2 + SILK-WB	125	125
Profile 1	Profile 2 + Opus-NB	200	150
Profile 2	Profile 2 + Opus-NB	125	125
Profile 1	Profile 2 + Opus-WB	150	125
Profile 2	Profile 2 + Opus-WB	100	100

3.3.13.3 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 Hyper-Threaded core (logical). For example, a 4-vCPU virtual machine allocates only 2 physical cores.

Note:

- The recommended profiles 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, the capacity is increased or decreased accordingly.
  - √ Hyper-Threading enabled on host.
  - √ VMware ESXi 6.5 or later.
  - √ CPUOverrideHT ini file parameter is configured to 1.
- CPU Affinity is recommended. For more information, refer to the *Installation Manual*.
- For transcoding capabilities, the 'Media Component Profile' parameter on all Media Components must be configured to **Transcoding Enabled** (MCProfile = 1).

Table 3-32: 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	625	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

3.3.14 Mediant Virtual Edition (VE) SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 165. 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.

3.3.14.1 Mediant VE SBC for VMware Hypervisors with Hyper-Threading

The following tables list maximum transcoding capacity for Mediant VE SBC running on VMware hypervisor with Hyper-Threading.

Each vCPU refers to a Hyper-Threaded core (logical). For example, a 4-vCPU virtual machine allocates only 2 physical cores.

Note:

- The recommended profiles 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 ESXi 6.5 or later
  - √ CPUOverrideHT ini file parameter is configured to 1
- 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 3-33: Mediant VE SBC on VMware with Hyper-Threading - Transcoding Capacity

Session Coders		Max. Sessions					
		4 vCPU 8-GB RAM		8 vCPU 16-GB RAM		16 vCPU 16-GB RAM	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	950	600	1275	825	3,825	2,475
Profile 1	Profile 2	500	400	675	550	2,075	1,650
Profile 2	Profile 2	350	300	475	400	1,425	1,250
Profile 1	Profile 2 + SILK-NB	300	275	400	350	1,225	1,100
Profile 2	Profile 2 + SILK-NB	225	225	325	300	975	900
Profile 1	Profile 2 + AMR-WB	100	100	125	125	425	400
Profile 2	Profile 2 + AMR-WB	75	75	125	125	375	375
Profile 1	Profile 2 + G.722 / AMR-NB	325	275	425	375	1,300	1,150
Profile 2	Profile 2 + G.722 / AMR-NB	250	225	325	300	1,000	925

Session Coders		Max. Sessions					
		4 vCPU 8-GB RAM		8 vCPU 16-GB RAM		16 vCPU 16-GB RAM	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 2 + SILK-WB	175	150	225	200	700	650
Profile 2	Profile 2 + SILK-WB	150	150	200	200	600	600
Profile 1	Profile 2 + Opus-NB	175	150	250	200	750	650
Profile 2	Profile 2 + Opus-NB	150	125	200	175	650	575
Profile 1	Profile 2 + Opus-WB	150	125	200	175	625	525
Profile 2	Profile 2 + Opus-WB	125	100	175	150	550	475

3.3.14.2 Mediant VE SBC for OpenStack and VMware Hypervisors

The following tables list maximum channel capacity for Mediant VE SBC 2.8 GHz running on OpenStack or VMware hypervisors.

3.3.14.2.1 Two-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 2-vCPU (1 vCPU reserved for DSP) Mediant VE SBC.

Table 3-34: 2-vCPU Mediant VE SBC on OpenStack/VMware - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	300	250
Profile 2	Profile 1	150	125
Profile 2	Profile 2	100	75
Profile 1	Profile 2 + AMR-NB / G.722	150	125
Profile 2	Profile 2 + AMR-NB / G.722	100	75
Profile 1	Profile 2 + AMR-WB (G.722.2)	50	25
Profile 2	Profile 2 + AMR-WB (G.722.2)	25	25
Profile 1	Profile 2 + SILK-NB	125	100
Profile 2	Profile 2 + SILK-NB	75	75
Profile 1	Profile 2 + SILK-WB	75	75
Profile 2	Profile 2 + SILK-WB	50	50
Profile 1	Profile 2 + Opus-NB	75	75
Profile 2	Profile 2 + Opus-NB	50	50
Profile 1	Profile 2 + Opus-WB	50	50
Profile 2	Profile 2 + Opus-WB	50	25

Notes:

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.14.2.1.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-35: 2-vCPU Mediant VE SBC on OpenStack/VMware - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	2,400
AD/AMD/Beep Detection	2,400
CP Detection	2,400
Jitter Buffer	200

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).

3.3.14.2.2Four-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 4-vCPU (3 vCPUs reserved for DSP) Mediant VE SBC.

Table 3-36: 4-vCPU Mediant VE SBC on OpenStack/VMware - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Basic**	**Extended**
Profile 1	Profile 1	900	750
Profile 2	Profile 1	450	375
Profile 2	Profile 2	300	250
Profile 1	Profile 2 + AMR-NB / G.722	450	375
Profile 2	Profile 2 + AMR-NB / G.722	300	250
Profile 1	Profile 2 + AMR-WB	150	125
Profile 2	Profile 2 + AMR-WB	125	100
Profile 1	Profile 2 + SILK-NB	375	350
Profile 2	Profile 2 + SILK-NB	250	225
Profile 1	Profile 2 + SILK-WB	225	225
Profile 2	Profile 2 + SILK-WB	175	175
Profile 1	Profile 2 + Opus-NB	250	225
Profile 2	Profile 2 + Opus-NB	175	175
Profile 1	Profile 2 + Opus-WB	175	175
Profile 2	Profile 2 + Opus-WB	150	125

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.

3.3.14.2.2.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-37: 4-vCPU Mediant VE SBC on OpenStack/VMware - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	7,200
AD/AMD/Beep Detection	7,200
CP Detection	7,200
Jitter Buffer	650

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).

3.3.14.2.3Eight-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 8-vCPU (4 vCPUs reserved for DSP) Mediant VE SBC.

Table 3-38: 8-vCPU Mediant VE SBC on OpenStack/VMware - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	1,200	1,000
Profile 2	Profile 1	600	525
Profile 2	Profile 2	400	350
Profile 1	Profile 2 + AMR-NB / G.722	600	525
Profile 2	Profile 2 + AMR-NB / G.722	400	350
Profile 1	Profile 2 + AMR-WB	200	175
Profile 2	Profile 2 + AMR-WB	150	150
Profile 1	Profile 2 + SILK-NB	500	475
Profile 2	Profile 2 + SILK-NB	350	325
Profile 1	Profile 2 + SILK-WB	300	300
Profile 2	Profile 2 + SILK-WB	250	225

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 2 + Opus-NB	325	300
Profile 2	Profile 2 + Opus-NB	250	225
Profile 1	Profile 2 + Opus-WB	250	225
Profile 2	Profile 2 + Opus-WB	200	175

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.

3.3.14.2.3.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-39: 8-vCPU Mediant VE SBC on OpenStack/VMware - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	9,600
AD/AMD/Beep Detection	9,600
CP Detection	9,600
Jitter Buffer	875

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).

3.3.14.3 Mediant VE SBC for Amazon AWS EC2

The following tables list maximum channel capacity for Mediant VE SBC on the Amazon EC2 platform.

Table 3-40: Mediant VE SBC on c4.2xlarge - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	1,524	1,164
Profile 2	Profile 1	750	618
Profile 2	Profile 2	498	420
Profile 1	Profile 2 + AMR-NB / G.722	570	492
Profile 2	Profile 2 + AMR-NB / G.722	408	354
Profile 1	Profile 2 + AMR-WB	180	174
Profile 2	Profile 2 + AMR-WB	162	156
Profile 1	Profile 2 + SILK-NB	486	438
Profile 2	Profile 2 + SILK-NB	366	324
Profile 1	Profile 2 + SILK-WB	288	270
Profile 2	Profile 2 + SILK-WB	240	222
Profile 1	Profile 2 + Opus-NB	312	276
Profile 2	Profile 2 + Opus-NB	258	228
Profile 1	Profile 2 + Opus-WB	228	216
Profile 2	Profile 2 + Opus-WB	198	186

Table 3-41: Mediant VE SBC on c4.8xlarge - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	3,200	3,200
Profile 2	Profile 1	3,200	3,200
Profile 2	Profile 2	2,650	2,225
Profile 1	Profile 2 + AMR-NB / G.722	3,025	2,600
Profile 2	Profile 2 + AMR-NB / G.722	2,175	1,875
Profile 1	Profile 2 + AMR-WB	950	925
Profile 2	Profile 2 + AMR-WB	850	825
Profile 1	Profile 2 + SILK-NB	2,575	2,325
Profile 2	Profile 2 + SILK-NB	1,950	1,725

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 2 + SILK-WB	1,525	1,425
Profile 2	Profile 2 + SILK-WB	1,275	1,175
Profile 1	Profile 2 + Opus-NB	1,650	1,450
Profile 2	Profile 2 + Opus-NB	1,375	1,200
Profile 1	Profile 2 + Opus-WB	1,200	1,150
Profile 2	Profile 2 + Opus-WB	1,050	975

Notes:

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.14.3.1.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-42: Mediant VE SBC on Amazon EC2 - Forwarding Capacity per Feature

Feature	Max. Sessions	
	c4.2xlarge	c4.8xlarge
Fax Detection	2,000	3,200
AD/AMD/Beep Detection	2,000	3,200
CP Detection	2,000	3,200
Jitter Buffer	650	3,200

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).

3.3.14.4 Mediant VE SBC for Azure

The following tables list maximum channel capacity for Mediant VE SBC on the Azure platform.

Table 3-43: Mediant VE SBC on DS1_v2, DS2_v2 & DS3_v2 - Transcoding Capacity

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

3.3.14.5 Mediant VE SBC for Hyper-V Hypervisor

The following tables lists maximum channel capacity for Mediant VE SBC 2.1 GHz running on Hyper-V hypervisor.

3.3.14.5.1 Two-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 2-vCPU (1 vCPU reserved for DSP) Mediant VE SBC.

Table 3-44: 2-vCPU Mediant VE SBC on Hyper-V - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Basic**	**Extended**
Profile 1	Profile 1	225	175
Profile 2	Profile 1	100	100
Profile 2	Profile 2	75	50
Profile 1	Profile 2 + AMR-NB / G.722	100	75
Profile 2	Profile 2 + AMR-NB / G.722	75	50
Profile 1	Profile 2 + AMR-WB	25	25
Profile 2	Profile 2 + AMR-WB	25	25
Profile 1	Profile 2 + SILK-NB	75	75
Profile 2	Profile 2 + SILK-NB	50	50
Profile 1	Profile 2 + SILK-WB	50	50
Profile 2	Profile 2 + SILK-WB	25	25
Profile 1	Profile 2 + Opus-NB	50	50
Profile 2	Profile 2 + Opus-NB	25	25
Profile 1	Profile 2 + Opus-WB	25	25
Profile 2	Profile 2 + Opus-WB	25	25

Notes:

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.14.5.1.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-45: 2-vCPU Mediant VE SBC on Hyper-V - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	1,800
AD/AMD/Beep Detection	1,800
CP Detection	1,800
Jitter Buffer	150

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).

3.3.14.5.2 Four-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 4-vCPU (3 vCPUs reserved for DSP) Mediant VE SBC.

Table 3-46: 4-vCPU Mediant VE SBC on Hyper-V - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	600	550
Profile 2	Profile 1	325	300
Profile 2	Profile 2	225	200
Profile 1	Profile 2 + AMR-NB / G.722	325	275
Profile 2	Profile 2 + AMR-NB / G.722	225	200
Profile 1	Profile 2 + AMR-WB	100	100
Profile 2	Profile 2 + AMR-WB	75	75
Profile 1	Profile 2 + SILK-NB	275	250
Profile 2	Profile 2 + SILK-NB	200	175
Profile 1	Profile 2 + SILK-WB	175	150
Profile 2	Profile 2 + SILK-WB	125	125

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 2 + Opus-NB	175	150
Profile 2	Profile 2 + Opus-NB	125	125
Profile 1	Profile 2 + Opus-WB	125	125
Profile 2	Profile 2 + Opus-WB	100	100

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.

3.3.14.5.2.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-47: 4-vCPU Mediant VE SBC on Hyper-V - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	5,400
AD/AMD/Beep Detection	5,400
CP Detection	5,400
Jitter Buffer	500

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).

3.3.14.6 Mediant VE SBC with Media Transcoders

Mediant VE SBC with Virtual Media Transcoders allows increasing the number of transcoding sessions by using Media Transcoders. The maximum number of transcoding sessions depends on the following:

- The number of Media Transcoders in the media transcoding cluster.
- The cluster operation mode (Best-Effort or Full-HA mode).
- The maximum transcoding sessions that the Mediant VE SBC can perform. 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 session capacity of a single MT-type Media Transcoder:

Table 3-48: Mediant VE SBC with Single 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
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	1325	1900
Profile 2	Profile 2 + Opus-WB	650	1175	1675

The following table lists maximum transcoding session capacity of a single vMT-type Media Transcoder:

Table 3-49: Single vMT - Transcoding Capacity per Profile

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Basic**	**Extended**
Profile 1	Profile 1	1,600	1,225
Profile 2	Profile 1	775	650
Profile 2	Profile 2	525	425
Profile 1	Profile 2 + AMR-NB / G.722	575	500
Profile 2	Profile 2 + AMR-NB / G.722	425	350
Profile 1	Profile 2 + AMR-WB	175	175
Profile 2	Profile 2 + AMR-WB	150	150
Profile 1	Profile 2 + SILK-NB	500	450
Profile 2	Profile 2 + SILK-NB	375	325
Profile 1	Profile 2 + SILK-WB	300	275
Profile 2	Profile 2 + SILK-WB	250	225
Profile 1	Profile 2 + Opus-NB	300	275
Profile 2	Profile 2 + Opus-NB	250	225
Profile 1	Profile 2 + Opus-WB	225	200
Profile 2	Profile 2 + Opus-WB	200	175

3.3.15 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 165. 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 3-50: 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.

3.3.15.1 Forwarding Session Capacity per Feature without Transcoding

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

Table 3-51: 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	MP-1288 / Mediant 500 / 500L / 800 / 1000B	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Access List	50	50	50	50
Accounts	102	625	1,500	1,500
Additional Management Interfaces	16	64	64	64
Allowed Audio Coders Groups	10	20	20	20
Allowed Video Coders Groups	4	4	4	4
Alternative Routing Reasons	20	20	20	20
Bandwidth Profile	486	1,009	1,884	1,884
Call Admission Control Profile	102	625	1,500	1,500
Call Admission Control Rule (per Profile)	8	8	8	8
Call Setup Rules	64	64	64	64
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	625	1,500	▪ 2 GB: 750 ▪ 3.5-64 GB: 1,500
Coder Groups	11	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)
DHCP Servers	1	1	1	1
Dial Plan	10	25	50	50
Dial Plan Rule	2,000	10,000	100,000	▪ < 16 GB: 2,000 ▪ > 16 GB: 100,000
Ethernet Devices	16	1,024	1,024	1,024

Configuration Table	MP-1288 / Mediant 500 / 500L / 800 / 1000B	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
External Media Source	1	1	1	1
Firewall	50	500	500	500
Forward On Busy Trunk Destination		n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Gateway CDR Format	128 (Syslog); 40 (RADIUS); 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	1,250	3,000	3,000
Internal DNS	20	20	20	20
Internal SRV	10	10	10	10
IP Group Set	51	312	2,500	▪ 2 GB: 40 ▪ 3.5 GB: 500 ▪ 4-16 GB: 750 ▪ 32-64 GB: 2,500
IP Groups	80	700	5,000	▪ 2 GB: 80 ▪ 3.5 GB: 1,000 ▪ 4-16 GB: 1,500 ▪ 32-64 GB: 5,000
IP Interfaces	12	1,024	1,024	1,024
IP Profiles	20 (MP-1288 / Mediant 500/L / Mediant 800); 40 (Mediant 1000)	125	300	▪ 2 GB: 150 ▪ 3.5-64 GB: 300
IP-to-IP Routing	615	3,750	9,000	▪ 2 GB: 4500 ▪ 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	250	600	600
LDAP Servers	82	500	1,200	1,200

Configuration Table	MP-1288 / Mediant 500 / 500L / 800 / 1000B	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Local Users	20	20	20	20
Logging Filters	60	60	60	60
Malicious Signature	20	20	20	20
Media Realm Extension	2 x Max. Media Realms (MP-1288, Mediant 500, Mediant 500L, Mediant 800 Only)	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	1,024	1,024
Message Conditions	82	500	1,200	1,200
Message Manipulations	100 (MP-1288 / Mediant 500/L / Mediant 800); 200 (Mediant 1000)	500	500	500
Message Policies	20	20	20	20
NAT Translation	32	32	32	32
Outbound Manipulations	205	1,250	3,000	3,000
OVOC Services	1	1	1	1
Phone Contexts	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Pre-Parsing Manipulation Rules	10 (per Set)	10 (per Set)	10 (per Set)	10 (per Set)
Pre-Parsing Manipulation Sets	10	10	10	10
Proxy Sets	102	625	5,000	▪ 2 GB: 80 ▪ 3.5 GB: 1,000 ▪ 4-16 GB: 1,500 ▪ 32-64 GB: 5,000
Proxy Sets > Proxy Address (per Proxy Set)	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 per Proxy Set)	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)	80	700	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

Configuration Table	MP-1288 / Mediant 500 / 500L / 800 / 1000B	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Quality of Experience Color Rules	256	256	256	256
Quality of Experience Profile	256	256	256	256
Quality Of Service Rules	510	3,125	7,500	7,500
RADIUS Servers	3	3	3	3
Reasons for IP-to-Tel Alternative Routing	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Reasons for Tel-to-IP Alternative Routing	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Redirect Number IP-to-Tel	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Redirect Number Tel-to-IP	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause ISDN->ISDN	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause Mapping from ISDN to SIP	12	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause Mapping from SIP to ISDN	12	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Remote Media Subnet	5	5	5	5
Remote Web Services	7	7	7	7
Routing Policies	20 (SBC)	280	600	▪ 2 GB: 20 ▪ 3.5 GB: 70 ▪ 4 GB: 100 ▪ 8 GB: 200 ▪ 16 GB: 400 ▪ 32-64 GB: 600
Routing Policies	1 (Gateway)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
SBC CDR Format	128 (Syslog); 40 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 40 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON)
SIP Interfaces	82	500	1,200	▪ 2 GB: 600 ▪ 3.5-64 GB: 1,200
SIP Recording Rules	30	30	30	30
SNMP Trap Destinations	5	5	5	5
SNMP Trusted Managers	5	5	5	5
SNMPv3 Users	10	10	10	10

Configuration Table	MP-1288 / Mediant 500 / 500L / 800 / 1000B	Mediant 2600 / 4000B	Mediant 90xx / SE	Mediant VE / CE
Source Phone Number Manipulation for IP-to-Tel Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Source Phone Number Manipulation for Tel-to-IP Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
SRDs	20	280	600	▪ 2 GB: 20 ▪ 3.5 GB: 70 ▪ 4 GB: 100 ▪ 8 GB: 200 ▪ 16 GB: 400 ▪ 32-64 GB: 600
Static Routes	30	30	30	30
Supplementary Services	100	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
TCP/UDP Proxy Servers	10	10	10	10
Tel Profiles	9	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)
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 (15 for Mediant 1000)	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/L; Mediant 800); 240 (Mediant 1000)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Trunk Group Settings	289 (MP-1288); 101 (Mediant 500/L; Mediant 800); 241 (Mediant 1000)	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)

This page is intentionally left blank.

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
6 Ofra Haza Street
Naimi Park
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

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

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

Document #: LTRT-27726