Release Notes

AudioCodes Family of Media Gateways & Session Border Controllers (SBC)

Mediant™ 3000 SBC and Gateway

Version 7.0

Table of Contents

Release Notes 1

Notice 9

WEEE EU Directive 9
Customer Support 9
Stay in the Loop with AudioCodes 9
Abbreviations and Terminology 9
Related Documentation 9
Document Revision Record 9
Documentation Feedback 12

1 Introduction 13

1.1 Software Revision Record 13

2 Released Versions 15

2.1 Version 7.00A.145.001 15
2.1.1 Resolved Constraints 15
2.2 Version 7.00A.144.005 15
2.2.1 Resolved Constraints 15
2.3 Version 7.00A.143.005 15
2.3.1 Resolved Constraints 15
2.4 Version 7.00A.143.001 16
2.4.1 Resolved Constraints 16
2.5 Version 7.00A.142.005 16
2.5.1 Resolved Constraints 16
2.6 Version 7.00A.142.001 16
2.6.1 Resolved Constraints 16
2.7 Version 7.00A.141.003 17
2.7.1 Resolved Constraints 17
2.8 Version 7.00A.140.003 17
2.8.1 Resolved Constraints 17
2.9 Version 7.00A.140.001 18
2.9.1 Resolved Constraints 18
2.10 Version 7.00A.139.004 18
2.10.1 Resolved Constraints 18
2.11 Version 7.00A.139.001 18
2.11.1 Resolved Constraints 18
2.12 Version 7.00A.138.005 19
2.12.1 Resolved Constraints 19
2.13 Version 7.00A.138 19
2.13.1 Resolved Constraints 19
2.14 Version 7.00A.136 20
2.14.1 Resolved Constraints 20
2.15 Version 7.00A.134.001 20
2.15.1 Resolved Constraints 20
2.16 Version 7.00A.132 21
2.16.1 Resolved Constraints 21

2.17 Version 7.00A.129.004 ... 22
2.17.1 Resolved Constraints ... 22
2.18 Version 7.00A.125.004 ... 22
2.18.1 Resolved Constraints ... 22
2.19 Version 7.00A.121.002 ... 23
2.19.1 Resolved Constraints ... 23
2.20 Version 7.00A.117.003 ... 24
2.20.1 New Features ... 24
2.20.1.1 Timestamp Format for SIPRec Messages ... 24
2.20.2 Resolved Constraints ... 24
2.21 Version 7.00A.113.004 ... 25
2.21.1 Resolved Constraints ... 25
2.22 Version 7.00A.107.008 ... 27
2.22.1 New Features ... 27
2.22.1.1 Performance Reporting Additions ... 27
2.22.1.2 LDAP Server Group per Call Setup Rule ... 27
2.22.2 Known Constraints ... 28
2.22.3 Resolved Constraints ... 28
2.23 Version 7.00A.102.002 ... 30
2.23.1 Resolved Constraints ... 30
2.24 Version 7.00A.095.004 ... 32
2.24.1 Known Constraints ... 32
2.24.2 Resolved Constraints ... 32
2.25 Version 7.00A.082.007 ... 36
2.25.1 New Features ... 36
2.25.1.1 Loading Files through CLI Enhancements ... 36
2.25.1.2 AMD for G.729 ... 36
2.25.1.3 Delayed ISDN Connect for Tel-to-IP Calls ... 36
2.25.2 Resolved Constraints ... 36
2.26 Version 7.00A.074.001 ... 39
2.26.1 New Features ... 39
2.26.1.1 Hookflash Detection and Transmission for SBC Calls ... 39
2.26.1.2 Product Key Field for Enhanced Product Identification ... 39
2.26.1.3 Preserving IP Address-Port for re-INVITE when All Media Rejected ... 39
2.26.1.4 Enhanced Management Security for Login Password ... 39
2.26.1.5 Autocomplete of Management Login Username ... 40
2.26.2 Resolved Constraints ... 40
2.27 Version 7.00A.067.003 ... 43
2.27.1 New Features ... 43
2.27.1.1 Utilizing Gateway Channel Resources for SBC Sessions ... 43
2.27.1.2 New NAT Traversal Method ... 43
2.27.1.3 Routing Server / ARM Enhancements ... 44
2.27.1.4 Preferred IP Version (ANAT) for Outgoing SIP Calls ... 44
2.27.1.5 Unregister Requests and Graceful Time ... 44
2.27.2 Resolved Constraints ... 45
2.28 Version 7.00A.063.003 ... 47
2.28.1 Resolved Constraints ... 47
2.29 Version 7.00A.058.102 ... 50
2.29.1 Resolved Constraints ... 50
2.30 Version 7.00A.058.002 ... 51
2.30.1 Known Constraints ... 51
2.30.2 Resolved Constraints ... 51
2.31 Version 7.00A.053.006 ... 54

2.31.1 New Features 54
2.31.1.1 Sending Alarms between TDM Hairpinned Connected Trunks 54
2.31.1.2 SIP Authorization Challenge Cache for SBC Calls 54
2.31.2 Known Constraints 54
2.31.3 Resolved Constraints 54
2.32 Version 7.00A.049.003 56
2.32.1 New Features 56
2.32.1.1 Routing Server Support for IP-to-Tel Calls and Enhancements 56
2.32.2 Resolved Constraints 56
2.33 Version 7.00A.046.003 57
2.33.1 Known Constraints 57
2.33.2 Resolved Constraints 58
2.34 Version 7.00A.044.007 59
2.34.1 New Features 59
2.34.1.1 Increase in Multiple Media Streams in SDP per Session 59
2.34.1.2 Registration Status for Gateway-type IP Groups 59
2.34.1.3 Enhanced Dial Plan Functionality 59
2.34.2 Resolved Constraints 64
2.35 Version GA 66
2.35.1 New Features 66
2.35.1.1 VoIP Networking Features 66
2.35.1.2 SIP Interoperability Features 72
2.35.1.3 SIP Routing Features 80
2.35.1.4 SIP Supplementary Service Features 87
2.35.1.5 User Registration and Authentication Features 93
2.35.1.6 Media and SDP Features 94
2.35.1.7 PSTN Features 97
2.35.1.8 High-Availability Features 100
2.35.1.9 Quality of Experience Features 100
2.35.1.10 Status and Performance Monitoring Features 101
2.35.1.11 Diagnostics and Troubleshooting 103
2.35.1.12 New Management Platform Features 107
2.35.2 Known Constraints 116
2.35.2.1 SIP Constraints 116
2.35.2.2 Media Constraints 118
2.35.2.3 PSTN Constraints 119
2.35.2.4 High-Availability Constraints 120
2.35.2.5 Infrastructure Constraints 120
2.35.2.6 Security Constraints 121
2.35.2.7 Management Constraints 121
2.35.3 Resolved Constraints 123
2.35.3.1 SIP Constraints 123
2.35.3.2 Networking Resolved Constraints 123
2.35.3.3 Media Resolved Constraints 123
2.35.3.4 Infrastructure Resolved Constraints 123
2.35.3.5 Security Resolved Constraints 124
3 Obsolete Features and Parameters 125
3.1 Obsolete Features 125
3.1.1 IP-to-IP Application 125
3.1.2 SAS Application 126
3.2 Obsolete Parameters 127
4 Session Capacity 129
4.1 Mediant 3000 Full Chassis 130

4.2 Mediant 3000 16 E1 / 21 T1 131
4.3 Mediant 3000 with Single T3 132
4.4 Mediant 3000 DSP Template Mix Feature 134

5 Supported SIP Standards 135

5.1 Supported SIP RFCs 135
5.2 SIP Message Compliancy 139
5.2.1 SIP Functions 139
5.2.2 SIP Methods 140
5.2.3 SIP Headers 140
5.2.4 SDP Fields 142
5.2.5 SIP Responses 142
5.2.5.1 1xx Response – Information Responses 143
5.2.5.2 2xx Response – Successful Responses 143
5.2.5.3 3xx Response – Redirection Responses 143
5.2.5.4 4xx Response – Client Failure Responses 144
5.2.5.5 5xx Response – Server Failure Responses 146
5.2.5.6 6xx Response – Global Responses 146

List of Tables

Table 1-1: Software Revision Record 13
Table 2-1: Resolved Constraints for Version 7.00A.145.001 15
Table 2-2: Resolved Constraints for Version 7.00A.144.005 15
Table 2-3: Resolved Constraints for Version 7.00A.143.005 15
Table 2-4: Resolved Constraints for Version 7.00A.143.001 16
Table 2-5: Resolved Constraints for Version 7.00A.142.005 16
Table 2-6: Resolved Constraints for Version 7.00A.142.001 16
Table 2-7: Resolved Constraints for Version 7.00A.141.003 17
Table 2-8: Resolved Constraints for Version 7.00A.140.003 17
Table 2-9: Resolved Constraints for Version 7.00A.140.001 18
Table 2-10: Resolved Constraints for Version 7.00A.139.004 18
Table 2-11: Resolved Constraints for Version 7.00A.139.001 18
Table 2-12: Resolved Constraints for Version 7.00A.138.005 19
Table 2-13: Resolved Constraints for Version 7.00A.138 19
Table 2-14: Resolved Constraints for Version 7.00A.136 20
Table 2-15: Resolved Constraints for Version 7.00A.134.001 20
Table 2-16: Resolved Constraints for Version 7.00A.132 21
Table 2-17: Resolved Constraints for Version 7.00A.129.004 22
Table 2-18: Resolved Constraints for Version 7.00A.125.004 22
Table 2-19: Resolved Constraints for Version 7.00A.121.002 23
Table 2-20: Resolved Constraints for Version 7.00A.117.003 24
Table 2-21: Resolved Constraints for Version 7.00A.113.004 25
Table 2-22: Known Constraints for Version 7.00A.107.008 28
Table 2-23: Resolved Constraints for Version 7.00A.107.008 28
Table 2-24: Resolved Constraints for Version 7.00A.102.002 30
Table 2-25: Known Constraints for Version 7.00A.095.004 32
Table 2-26: Resolved Constraints for Version 7.00A.095.004 32
Table 2-27: Resolved Constraints for Version 7.00A.082.007 36
Table 2-28: Resolved Constraints for Version 7.00A.074.001 40
Table 2-29: Resolved Constraints for Version 7.00A.067.003 45
Table 3-1: Obsolete SAS Parameters 126
Table 3-2: Obsolete Parameters 127
Table 4-1: Gateway and SBC Capacity per Product 129
Table 4-2: Channel Capacity per DSP Firmware Template for Mediant 3000 130
Table 4-3: Channel Capacity per DSP Firmware Templates for Mediant 3000 16 E1 / 21 T1........ 131
Table 4-4: Channel Capacity per DSP Firmware Templates for Mediant 3000 with Single T3........ 132
Table 4-5: Channel Capacity of DSP Template Mix Feature for Mediant 3000 134
Table 5-1: Supported RFCs 135
Table 5-2: Supported SIP Functions 139
Table 5-3: Supported SIP Methods 140
Table 5-4: Supported SDP Fields 142
Table 5-5: Supported 1xx SIP Responses 143
Table 5-6: Supported 2xx SIP Responses 143
Table 5-7: Supported 3xx SIP Responses 143
Table 5-8: Supported 4xx SIP Responses 144
Table 5-9: Supported 5xx SIP Responses 146
Table 5-10: Supported 6xx SIP Responses 146

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: May-15-2024

WEEE EU Directive

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

Customer Support

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

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 3000 SIP Hardware Installation Manual
Mediant 3000 SIP User's Manual

Document Revision Record

LTRT	Description
26931	Initial document release.

LTRT	Description
26933	▪ CDR customization for RADIUS accounting ▪ TLS certificate per LDAP server ▪ Revised Multi-tenant feature ▪ user-activity log option "ae" (Action Executed) ▪ registration time for users behind NAT ▪ Test Calls per SIP Interface ▪ Log Filtering per SIP Interface ▪ WebRTC feature key license only enables-disables feature ▪ Revised interworking features (Contact, Via, User-Agent, Record-Route, To-header tags) ▪ AudioCodes analog device identification feature removed ▪ "Lync Resiliency" renamed "One-Voice Resiliency" ▪ Feature key license removed for Opus coder ▪ Obsolete SIP IP-media features
26935	▪ CDR customization ▪ SIP message manipulation for users behind NAT ▪ Revised One-Voice Resiliency new feature ▪ ELIN Feature Key ▪ Increase in table row capacity for Logging Filters table ▪ Change of location of time and date parameters in Web interface ▪ CDR local storage ▪ Enhanced log filtering ▪ DNS query method for Microsoft ▪ Identifying RTP/SAVPF media streams ▪ Status display of installed Dial Plan file ▪ Indication of installed User Info file ▪ New Software License Activation tool ▪ SBC Session licenses from license pool of License Manager Server ▪ Supported RFCs
26936	▪ Network Physical Separation Enhancement for Mediant 3000/TP-8410 ▪ Maximum concurrent WebRTC sessions per product ▪ SBC Capacity Licenses from EMS License Pool Manager Server
26938	▪ LDAP Query for Numbers in AD with Characters between Digits ▪ Modified - CDR Local Storage Update ▪ Modified - SBC Capacity Licenses from EMS License Pool Manager Server ▪ RFC 6035, RFC 3611, RFC 3489 supported by SBC application (Supported RFC table) ▪ RFC 3362 added to Supported RFC table ▪ SIP constraint added (No. 1). ▪ Media constraint added (No. 1) ▪ Infrastructure constraint (No. 1) ▪ Management constraints (No. 1)
26940	▪ Ver. 7.00A.044.007 ✓ Multiple Media Streams in SDP per Session ✓ BFCP Streams over UDP ✓ Registration Status for Gateway-type IP Groups ✓ Enhanced Dial Plan Functionality ✓ Resolved constraints ▪ Notification to Select SRD before Cloning

LTRT	Description
	▪ New Call Detail Record folder under System menu ▪ G.727 removed ▪ RFC 4582 added ▪ Constraints added: Management constraint (1); Web constraint (1)
26943	▪ Ver. 7.00A.046.003 (known and resolved constraints) ▪ New features: ✓ Embedded PacketSmart Agent ✓ acHwFailureAlarm for DSP Device Failure ▪ CDR Local Storage feature description updated ▪ Enhanced Dial Plan feature description updated ▪ Supported RFCs table (RFC 3960)
26944	▪ Ver. 7.00A.049.003 (known and resolved constraints) ▪ New features: ✓ Session Variables (var.session) for Message Manipulations ✓ Automatic Provisioning of License Feature Key ✓ File Template for Automatic Provisioning ▪ Updates to Enhanced Dial Plan Functionality ▪ Constraints added to GA
26948	▪ Ver. 7.00A.053.006 (features, known and resolved constraints) ✓ Sending Alarms between TDM Hairpinned Connected Trunks ✓ SIP Authorization Challenge Cache for SBC Calls ▪ New Features: ✓ Rerouting Calls upon Broken RTP Connection ✓ LDAP Cache Size Increase
26950	▪ SAS application obsolete ▪ Some constraints were removed.
26953	▪ Version 7.00A.058.002 (known and resolved constraints)
26955	▪ New Feature: Routing Server Support for IP-to-Tel Calls and Enhancements ▪ RFC 7261
26956	▪ Ver. 7.00A.058.102
26958	▪ Ver. 7.00A.063.003
26964	▪ Ver. 7.00A.067.003
26971	▪ Ver. 7.00A.074.001
26976	▪ Resolved constraint added to Ver. 7.00A.074.001 (Incident 134849)
26978	Ver. 7.00A.082.007
26980	Typos.
26986	WebRTC updated.
26993	Ver. 7.00A.095.004.
26995	Additional resolved constraint (VI 139600) for Ver. 7.00A.095.004.
26997	OVR capacity added.
27080	Ver. 7.00A.102.002
27088	Ver. 7.00A.107.008

LTRT	Description
27095	Ver. 7.00A.113.004 Incident 140497 added as resolved constraint for Ver. 7.00A.102.002
27244	Ver. 7.00A.117.003
27253	Ver. 7.00A.121.002
27259	Ver. 7.00A.125.004
27273	Ver. 7.00A.129.004
27346	Ver. 7.00A.132
27361	Ver. 7.00A.134.001; Features added to 7.00A.074.001: Product Key Field for Enhanced Product Identification Features added to 7.00A.082.007: Loading Files through CLI Enhancements; AMD for G.729; Delayed ISDN Connect for Tel-to-IP Calls
27370	Ver. 7.00A.136
27385	Ver. 7.00A.138
27388	G.722 changed to DSP Template #9 instead of #10 for Mediant 3000 capacity
27451	Ver. 7.00A.138.005
27453	New feature for Ver. 7.00A.138.005
27462	Ver. 7.00A.139.001
27468	Ver. 7.00A.139.004
27479	Ver. 7.00A.140.001
27487	Ver. 7.00A.140.003
27508	Ver. 7.00A.141.003
27536	Ver. 7.00A.142.001
27547	Ver. 7.00A.142.005
27560	Ver. 7.00A.143.001
27598	Ver. 7.00A.143.005
27690	Ver. 7.00A.144.005
27724	Ver. 7.00A.145.001

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 new features of Mediant 3000 Version 7.0. This includes new products, new hardware features, new software features, known constraints, and resolved constraints.

Notes:

- 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 Software 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 software versions released in Version 7.0.

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

Table 1-1: Software Revision Record

Software Version	Date
7.00A.145.001	May 2024
7.00A.144.005	September 2023
7.00A.143.005	April 2022
7.00A.143.001	August 2021
7.00A.142.005	May 2021
7.00A.142.001	March 2021
7.00A.141.003	December 2020
7.00A.140.003	August 2020
7.00A.140.001	July 2020
7.00A.139.004	May 2020
7.00A.139.001	April 2020
7.00A.138.005	February 2020
7.00A.138	August 2019

Software Version	Date
7.00A.136	May 2019
7.00A.134.001	February 2019
7.00A.132	October 2018
7.00A.129.004	June 2018
7.00A.125.004	February 2018
7.00A.121.002	December 2017
7.00A.117.003	September 2017
7.00A.113.004	July 2017
7.00A.107.008	May 2017
7.00A.102.002	March 2017
7.00A.095.004	January 2017
7.00A.082.007	September 2016
7.00A.074.001	July 2016
7.00A.067.003	May 2016
7.00R.050.002	Apr 2016
7.00A.058.102	Apr 2016
7.00A.063.003	Apr 2016
7.00A.058.002	Mar 2016
7.00A.053.006	Feb 2016
7.00A.049.003	Jan 2016
7.00A.046.003	Dec 2015
7.00A.044.007	Nov 2015
General Availability (GA)	May 2015

2 Released Versions

2.1 Version 7.00A.145.001

This version includes resolved constraints only.

2.1.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-1: Resolved Constraints for Version 7.00A.145.001

Incident	Description
157131	Failure of LDAP-based Web interface access authentication for default access level 0. **Applicable Products:** Mediant 3000 (TP-6310).

2.2 Version 7.00A.144.005

This version includes resolved constraints only.

2.2.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-2: Resolved Constraints for Version 7.00A.144.005

Incident	Description
157059	The device's `show` related SIP CMDShell commands generates an error message ("Illegal CMD Shell Message Len 1394"). **Applicable Products:** Mediant 3000.
157071	TBCT doesn't function if calls are on any SIP Interface other than the first SIP Interface. **Applicable Products:** Mediant 3000.

2.3 Version 7.00A.143.005

This version includes resolved constraints only.

2.3.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-3: Resolved Constraints for Version 7.00A.143.005

Incident	Description
156896	The device's daylight-saving time is not immediately reflected in the CDR when applied, but takes effect only after the next NTP update, thereby showing the incorrect time in the CDR. **Applicable Products:** Mediant 3000.

2.4 Version 7.00A.143.001

This version includes resolved constraints only.

2.4.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-4: Resolved Constraints for Version 7.00A.143.001

Incident	Description
156775	The device crashes (resets) with the exception task “DSPD”. **Applicable Products:** Mediant 3000.
156811	The ntpAuthMd5Key parameter is not hidden from the downloaded ini file. **Applicable Products:** Mediant 3000.

2.5 Version 7.00A.142.005

This version includes resolved constraints only.

2.5.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-5: Resolved Constraints for Version 7.00A.142.005

Incident	Description
156749	The device doesn't send GetRoute requests to ARM. **Applicable Products:** Mediant 3000.
156757	The device sends GetRoute requests to ARM with incorrect UTF-8 format when receiving a SIP INVITE message containing User-to-User with 'encoding=hex'. **Applicable Products:** Mediant 3000.

2.6 Version 7.00A.142.001

This version includes resolved constraints only.

2.6.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-6: Resolved Constraints for Version 7.00A.142.001

Incident	Description
156689	The device crashes (resets) when receiving a SIP REFER message, handling it locally, and then receiving a re-INVITE message on the same leg. **Applicable Products:** Mediant 3000.

2.7 Version 7.00A.141.003

This version includes resolved constraints only.

2.7.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-7: Resolved Constraints for Version 7.00A.141.003

Incident	Description
156525	Upon a failed Web login attempt, the device doesn't include the username in the generated Syslog message for this error. **Applicable Products:** Mediant 3000.
156616	The device crashes (resets) when the Tel-to-IP Routing table is modified. **Applicable Products:** Mediant 3000.
156668	The device fails to change the username and password through SNMP. **Applicable Products:** Mediant 3000.
156669	The device's Web interface doesn't display any IP Profile rules in the IP Profiles table even though rules were configured. **Applicable Products:** Mediant 3000.
156677	When the device re-routes an IP-to-Tel call to an alternative route (trunk), it doesn't include the caller name in the ISDN SETUP message. **Applicable Products:** Mediant 3000.

2.8 Version 7.00A.140.003

This version includes resolved constraints only.

2.8.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-8: Resolved Constraints for Version 7.00A.140.003

Incident	Description
156584 / 156608	The device fails to add a new row to the Tel-to-IP Routing table through the Web interface. **Applicable Products:** Mediant 3000

2.9 Version 7.00A.140.001

This version includes resolved constraints only.

2.9.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-9: Resolved Constraints for Version 7.00A.140.001

Incident	Description
156592	This version blocks the Ripple20 vulnerabilities that were discovered by the JSOF research lab on the TCP/IP software library developed by Treck, Inc. **Applicable Products:** Mediant 3000

2.10 Version 7.00A.139.004

This version includes resolved constraints only.

2.10.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-10: Resolved Constraints for Version 7.00A.139.004

Incident	Description
156476	The HA system generates a Feature Key mismatch alarm (acHASystemConfigMismatchAlarm), indicating different Feature Keys between active and redundant devices (length is different) due to the key including buffers with irrelevant, additional information. **Applicable Products:** Mediant 3000
156527	The device opens voice with a different port than that declared in the SDP for IP-to-Tel delayed media ARM calls. As a result, no voice occurs. **Applicable Products:** Mediant 3000

2.11 Version 7.00A.139.001

This version includes resolved constraints only.

2.11.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-11: Resolved Constraints for Version 7.00A.139.001

Incident	Description
156510	When using ARM-based call routing, the Tel-to-IP call remains unchanged after device loses connectivity with ARM, resulting in call failure. **Applicable Products:** Mediant 3000

2.12 Version 7.00A.138.005

This version includes resolved constraints only.

2.12.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-12: Resolved Constraints for Version 7.00A.138.005

Incident	Description
156373	DSP-related errors in Syslog after upgrading to 7.00A.138 (bug was found in creating DSP events that may lead to memory overrun). **Applicable Products:** Mediant 3000.
156461	Secured login into the device's Web interface causes a CPU Overload. **Applicable Products:** Mediant 3000.

2.13 Version 7.00A.138

This version includes resolved constraints only.

2.13.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-13: Resolved Constraints for Version 7.00A.138

Incident	Description
156140 & 156296	The device loses audio on PSTN for Skype for Business calls when RTCP-XR is enabled. This is because of the new SSRC with only RTCP packets. **Applicable Products:** Mediant 3000.
156217	The device's security scan found a certificate signed using a weak hashing algorithm. **Applicable Products:** Mediant 3000.
156236	A syslog “Utilization PM is out of boundary” error occurs on the Mediant 3000 when the NFAS trunk is full. **Applicable Products:** Mediant 3000.
156246	The device cannot connect with more than one REST server. **Applicable Products:** Mediant 3000.

2.14 Version 7.00A.136

This version includes resolved constraints only.

2.14.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-14: Resolved Constraints for Version 7.00A.136

Incident	Description
155998	The device generates the following syslog event: "recv <-- UnHandled event: EV_RTCP_APP_RECEIVED (401)". **Applicable Products:** Mediant 3000.

2.15 Version 7.00A.134.001

This version includes resolved constraints only.

2.15.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-15: Resolved Constraints for Version 7.00A.134.001

Incident	Description
155872	The device resets sporadically when activating Debug Recording (DR), caused by a memory overrun in the DR feature. **Applicable Products:** Mediant 3000.
155875	The device has a buffer overflow vulnerability in the Web interface's login process, which causes the device to reset. **Applicable Products:** Mediant 3000.
155876	The device has insufficient authorization controls, allowing a user level the privilege to load an incremental ini file, even though the specific user level has no privileges to do so (security breach). **Applicable Products:** Mediant 3000.
155877	The device allows users to perform HTTP POST requests without credentials (security breach). **Applicable Products:** Mediant 3000.

2.16 Version 7.00A.132

This version includes resolved constraints only.

2.16.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-16: Resolved Constraints for Version 7.00A.132

Incident	Description
152303	Calls fail due to DSP errors (memory overrun), as shown in the syslog: "DSP Watchdog triggered (HPI Error) recv <-- UnHandled event: EV_DSP_FAILURE_INFO_AVAILABLE (307) Dsp Core Dump available for device#" **Applicable Products:** Mediant 3000.
152474	The device crashes (resets) upon an LDAP operation due to an LDAP connection expiry and an LDAP connection establishment that occurs at the same time. **Applicable Products:** Mediant 3000.
153194	The device crashes (resets) when configured with a Message Manipulation rule with 'Action Subject' set to "message" and 'Action Type' set to "Normalize", and the rule is used as an inbound manipulation rule **Applicable Products:** Mediant 3000 (SBC).
153377	When disconnecting a call, the MOS graph displayed in the Web interface drops to 0 (zero) even if other calls are still connected. **Applicable Products:** Mediant 3000.
153559	For IP-to-Tel calls, the caller hears another call that is also handled by the device, instead of hearing the ring-back tone (RBT). **Applicable Products:** Mediant 3000.
154010	In certain scenarios, the device crashes (resets) when accessing the Alarms history page. **Applicable Products:** Mediant 3000.
154442	The device experiences a CPU overload and then resets with task "TMGR". As a result, the device crashes (resets). **Applicable Products:** Mediant 3000.
155071	The device stops handling PSTN calls, generating the syslog message “no more free ID’s available” for the resource "SIPTUResource". **Applicable Products:** Mediant 3000.
155442	After a device reset, RAI alarms are raised for CAS trunks (which are taken out of service). **Applicable Products:** Mediant 3000.

2.17 Version 7.00A.129.004

This version includes resolved constraints only.

2.17.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-17: Resolved Constraints for Version 7.00A.129.004

Incident	Description
153194	For SBC calls, the device crashes (and resets) if a Message Manipulation rule is configured with the 'Action Subject' field is "message" and 'Action Type' field is "Normalize" and the rule is used as an Inbound Manipulation rule. **Applicable Products:** Mediant 3000.
152548	For SBC calls, if the device is configured to play RBT and the SDP of the final SIP response (200 OK) contains CN, one-way voice occurs. **Applicable Products:** Mediant 3000.
151724	For SBC calls, the device rejects re-INVITE messages from the call originator with a SIP 488 when the AMD detector is enabled. As a result, one-way voice occurs. **Applicable Products:** Mediant 3000.
151482	Logging in to the device through RADIUS-based authentication fails (RADIUS sever accepted the request, but the login failed). **Applicable Products:** Mediant 3000.
151012	For the ISDN protocol E1 NI2, the device does not send the calling name to the PRI trunk for IP-to-Tel calls. **Applicable Products:** Mediant 3000.

2.18 Version 7.00A.125.004

This version includes resolved constraints only.

2.18.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-18: Resolved Constraints for Version 7.00A.125.004

Incident	Description
150463	If the device receives SDP with AVP and crypto, it does not handle it as SRTP. As a result, there is no voice. **Applicable Products:** Mediant 3000.
149578	Insufficient Gateway resources (as not released correctly for availability) causes the device to crash (reset). **Applicable Products:** Mediant 3000.
149461	The device experiences problems with handling SRTP and as a result, one-way voice occurs. **Applicable Products:** Mediant 3000.

Incident	Description
149378	A problem exists with SDP handling for SBC calls when extending a coder list to include an image (fax). As a result, the device crashes (resets). **Applicable Products:** Mediant 3000.
148584	On high load, the device reports unknown voice quality for Test Calls. **Applicable Products:** Mediant 3000.

2.19 Version 7.00A.121.002

This version includes resolved constraints only.

2.19.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-19: Resolved Constraints for Version 7.00A.121.002

Incident	Description
148016	When the device receives a SIP INVITE message with nine crypto suites and the first four are not supported by the device, the device rejects the SBC call. **Applicable Products:** Mediant 3000.
147893	If the device receives a SIP re-INVITE for hold during an SBC test call, it crashes (and resets). **Applicable Products:** Mediant 3000.
146875	The Calling Name in the FACILITY message for the NI2 protocol causes the device to crash (and reset). **Applicable Products:** Mediant 3000.
147579	The device sends a SIP 183 response without the X-channel header. **Applicable Products:** Mediant 3000.
147393	If the ISDN SETUP message is greater than 260 bytes, it is rejected by the device and as a result, the call fails. **Applicable Products:** Mediant 3000.

2.20 Version 7.00A.117.003

This version includes new features and resolved constraints.

2.20.1 New Features

2.20.1.1 Timestamp Format for SIPRec Messages

This feature provides support for configuring the format (local or UTC offset) of the device's time in SIP messages (XML body) sent to the SRS for SIPRec. The feature is supported by the new parameter SIPRecTimeStamp.

Applicable Products: Mediant 3000.

2.20.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-20: Resolved Constraints for Version 7.00A.117.003

Incident	Description
147007	When using SIPRec, the device sends the INVITE message to the SRS with the incorrect time stamp (local time instead of the UTC/GMT). To resolve the bug, a new parameter (SIPRecTimeStamp) was added to configure whether the local time (on the device) or the UTC time is used for SIPRec. **Applicable Products:** Mediant 3000.
146729	When the device performs transcoding and receives an unknown type of RTCP packet, it does not change the SSRC. As a result, the remote side is unable to use the RTCP. **Applicable Products:** Mediant 3000.
146594	The device sends SIP messages to a proxy that is no longer in the SRV response, resulting in incorrect call routing. This occurs when the Priority and Weight values are changed in the Internal SRV table for the specific DNS – these are not reflected in the associated Proxy Sets table. **Applicable Products:** Mediant 3000.
146301	Direct media of calls stops functioning after a software upgrade, resulting in call failure. **Applicable Products:** Mediant 3000.
146201	The device crashes (resets) when the device tries to use Proxy ID #0, even though it was deleted from configuration. A workaround is to reset the device after deleting the Proxy Set. **Applicable Products:** Mediant 3000.
146075	When the SBC application sends keep-alive OPTIONS to the Gateway application over TCP it fails. As a result, call routing fails. A workaround is to use UDP. **Applicable Products:** Mediant 3000.
145662	Unable to configure the T38MaxBitRate parameter to 33600 bps(used for T.38 version 3). As a result, unable to achieve full fax speed. **Applicable Products:** Mediant 3000.
145364	High rate of DSP restarts is causing the device to crash (reset). **Applicable Products:** Mediant 3000.

Incident	Description
144505	Under certain conditions when TLS is enabled, the device crashes (resets). **Applicable Products:** Mediant 3000.
142923	The device handles call cancel erroneously: A SIP request is sent according to the latest received contact (the device receives a 180 with the contact). If the call is cancelled, the device sends a CANCEL message and the subsequent 200 OK includes a different contact. However, the device sends the ACK to the contact received in the 180 and not in the 200 OK. **Applicable Products:** Mediant 3000.

2.21 Version 7.00A.113.004

This version includes only resolved constraints.

2.21.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-21: Resolved Constraints for Version 7.00A.113.004

Incident	Description
144817	For ENUM-based routing, when the ENUM NAPTR and the A-Record DNS results are in the device's cache, the SIP Interface in the IP-to-IP Routing table is disregarded and instead, the SIP Interface of the destination IP Group is used. As a result, calls are not routed correctly. A workaround is not to change the SIP Interface during operation. **Applicable Products:** Mediant 3000.
145662	The T38MaxBitRate parameter cannot be configured to 33600bps in the Web interface. **Applicable Products:** Mediant 3000.
145364	A problem with the C5 processor causes the device to crash (reset). **Applicable Products:** Mediant 3000.
145397	Device crashes (resets) during TLS negotiation **Applicable Products:** Mediant 3000.
145294	Entries in the ELIN table are not removed from the table after expiry. As a result, the device stops processing ELIN calls. **Applicable Products:** Mediant 3000.
144805	The device doesn't update its time when synchronizing with the NTP server. **Applicable Products:** Mediant 3000.
141830	Hook flash received as RTP events from the IP side is not propagated (digits not sent) to the PSTN. (Resolved with added parameter, HookFlashFromMediaIP.) **Applicable Products:** Mediant 3000 (Gateway).
141348	If the length of the output of the CLI Script file is greater than 20,000 bytes, the device crashes (resets). **Applicable Products:** Mediant 3000.

Incident	Description
143930	The time stamp in SIP PUBLISH messages are not according to the RFC 6035, resulting in incorrect reports. **Applicable Products:** Mediant 3000.
143528	All SRD performance monitoring tables (SNMP) are limited to four entries and therefore, cannot obtain PM on all SRDs. **Applicable Products:** Mediant 3000.
143795	The device is vulnerable to the CVE-2016-10229 security threat. **Applicable Products:** Mediant 3000.
143465	When the “User Monitoring” Device Access Level 50 is used (for RADIUS) to log in to the device, the user has full access. In other words, unauthorized users can access the device. **Applicable Products:** Mediant 3000.
142328	When a user attempts to access the device through REST, the "REST module init failed" message is displayed and access to the device fails. **Applicable Products:** Mediant 3000.
143160	When different users are registered on the device with the same FEU ID, the device mixes up contacts with different registrations. As a result, registration and routing fails. **Applicable Products:** Mediant 3000.
143342	The HA system sends an alarm indicating a License Key mismatch even though both devices have the same License Key. HA synchronization fails (no HA). This is caused by the License Keys having different Product Keys. **Applicable Products: Mediant 3000.**

2.22 Version 7.00A.107.008

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

2.22.1 New Features

New features introduced in this version include the following:

2.22.1.1 Performance Reporting Additions

This feature provides support for Gateway call statistics per IP Group:

- New call statistics for gateway calls (already supported for SBC calls):
  - PM_gwSBCIPGroupInAttemptedCalls
  - PM_gwSBCIPGroupOutAttemptedCalls
  - PM_gwSBCIPGroupInBusyCalls
  - PM_gwSBCIPGroupOutBusyCalls
  - PM_gwSBCIPGroupInNoAnswerCalls
  - PM_gwSBCIPGroupOutNoAnswerCalls
  - PM_gwSBCIPGroupRoutingFailedCalls
  - PM_gwSBCIPGroupInNoMatchCalls
  - PM_gwSBCIPGroupOutNoMatchCalls
  - PM_gwSBCIPGroupInForwardedCalls
  - PM_gwSBCIPGroupOutForwardedCalls
  - PM_gwSBCIPGroupInNoResourcesCalls
  - PM_gwSBCIPGroupOutNoResourcesCalls
  - PM_gwSBCIPGroupInGeneralFailedCalls
  - PM_gwSBCIPGroupOutGeneralFailedCalls
  - PM_gwSBCIPGroupInEstablishedCalls
  - PM_gwSBCIPGroupOutEstablishedCalls
- New CmdShell:
  - Resets Gateway statistics and call counters: **SIP / ResetStatistics**
  - Displays IP Group call statistics: **SHow SIP VN IPG [1] S Calls**
  - Displays Tel-to-IP Gateway call statistics: **SHow SIP Calls Statistics GW Tel2IP**
  - Displays IP-to-Tel Gateway call statistics: **SHow SIP Calls Statistics GW IP2Tel**
- CLI command:
  - Clear VoIP statistics: **clear voip statistics**
  - Display call statistics per IP Group: **show voip calls statistics ipgroup [ID]**

Applicable Products: Mediant 3000.

2.22.1.2 LDAP Server Group per Call Setup Rule

This feature provides support for specifying an LDAP Server Group per Call Setup Rule. Up until now, only one LDAP server could be used for all Call Setup Rules. The feature is supported by the new field Query Target (CallSetupRules_QueryTarget) in the Call Setup Rules table.

Applicable Products: Mediant 3000.

2.22.2 Known Constraints

Additional constraints discovered in this version include the following:

Table 2-22: Known Constraints for Version 7.00A.107.008

Incident	Description
143772	For performance reporting per IP Group, clear statistics doesn't occur and average incoming/outgoing call duration is not updated. **Applicable Products:** Mediant 3000.
143827	For Gateway statistics per IP Group (incoming/outgoing), statistics are not counted when using the default IP Group (0). **Applicable Products:** Mediant 3000.

2.22.3 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-23: Resolved Constraints for Version 7.00A.107.008

Incident	Description	Status
143342	The HA system sends an alarm indicating a License Key mismatch even though both devices have the same License Key. **Applicable Products: Mediant 3000.**.	Resolved in Ver. 7.00A.113.004 (see Section 2.14)
143239	The CLI command **show voip calls active sbc** displays the incorrect SID in the call detail (last digit missing). **Applicable Products:** Mediant 3000.	-
143448	When the device is configured with two IP network interfaces, two SIP interfaces, but only one SRD, the device does not send keep-alive SIP OPTIONS. As a result, there is no connectivity to the proxy. A workaround is to configure additional SRDs. **Applicable Products:** Mediant 3000.	-
143006	The hard-coded port 2123 is set for NTP, but when this port is allocated to another application (e.g. Syslog), no NTP requests are sent. A workaround is to use a different port. **Applicable Products:** Mediant 3000.	-
141348	Getting the running configuration from the device through REST fails. As a result, device configuration cannot be backed up. **Applicable Products:** Mediant 3000.	-
141444	Configuring the Remove Cipher HTTPS Cipher String parameter on the Web Security Settings page results in incorrect configuration since the cipher string is now configured per TLS Context in the TLS Contexts table. **Applicable Products:** Mediant 3000.	-
142103	When using the SIP Connect feature in the outgoing leg, the device copies the user part from the To header, but keeps the host part showing the internal IP. As a result, calls fail due to NAT problem. **Applicable Products:** Mediant 3000.	-

Incident	Description	Status
141830	Hook flash received from the IP side is not sent by the device to the CAS side. To resolve the problem, a new parameter has been added -HookFlashFromMediaIP. **Applicable Products:** Mediant 3000.	-
140573	If a call is put on hold and then retrieved, the device reports incorrect voice quality results to the SEM as it takes into account the hold time as well. **Applicable Products:** Mediant 3000.	-
142005	When the device receives an INVITE with the ICE user and the password is on the session level and the candidates on the media level, the device responds with a 200 OK without candidates. As a result, the call fails. **Applicable Products:** Mediant 3000.	-

2.23 Version 7.00A.102.002

This version includes resolved constraints.

2.23.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-24: Resolved Constraints for Version 7.00A.102.002

Incident	Description
141612	For IP-to-IP source inbound manipulation, the SIP From header changes, but the Remote-Party-ID header does not. As a result, the incorrect number is sent. **Applicable Products:** Mediant 3000.
141386	The device registers fewer users than configured in the User Info table. **Applicable Products:** Mediant 3000.
141409	For SBC RTP-to-SRTP calls, the device fails to play a ringback tone to the RTP side. As a result, no voice occurs. A workaround is to disable play RBT. **Applicable Products:** Mediant 3000.
141099	A potential security risk exists when a user logs in to the Web interface. The device responds whether or not the username is correct. This gives attackers the ability to discover all usernames in the system through trial and error. **Applicable Products:** Mediant 3000.
141611	A problem exists in call-hold handling. When A puts B on hold and then A sends an UPDATE request without SDP, the device terminates it to re-INVITE with SDP and sends the re-INVITE with 'recvonly' instead of 'sendonly'. **Applicable Products:** Mediant 3000.
141439	In certain scenarios, the device crashes and resets. **Applicable Products:** SBC HA.
141407	If a call has a re-INVITE, the value of the SNMP MIB acPMSBCMediaLegsTable is not decreased when the call ends. **Applicable Products:** Mediant 3000.
139651	Due to the time of receipt of DNS resolutions on forked calls, the device enters an endless loop and stops responding. **Applicable Products:** Mediant 3000.
140961	IP Group 0 and Proxy Set 0 are created automatically after a device reset even if they were deleted before reset. **Applicable Products:** Mediant 3000.
140436	If a TLS Context is configured without a certificate (as it used only for encryption) and the device resets, a message displays “SECURITY ALERT: The TLS certificate of security context 1 has expired 17171 days ago”. As a result, encryption fails. A workaround is to load a certificate even if not needed. **Applicable Products:** SBC with OVR.
140801	The device reports incorrect call termination reason to SEM - RELEASE_BECAUSE_TRANSCODING_FULL instead of RELEASE_BECAUSE_MAX_DURATION_TIMER_EXPIRED. **Applicable Products:** Mediant 3000.

Incident	Description
140561	Modifying the parameters DenyAccessOnFailCount and DenyAuthenticationTimer does not take effect. **Applicable Products:** Mediant 3000.
140307	The device modifies the call_id on outgoing ACK requests when there is a message manipulation on the Request-URI header. As a result, the call fails due to incorrect call ID. **Applicable Products:** Mediant 3000.
138485	During an HA switchover, license pool configuration is blocked resulting in an exception, causing the device to crash (reset). **Applicable Products:** SBC HA.
140011	The device fails to connect to the remote routing Web server and as a result, did not receive routing information. **Applicable Products:** Mediant 3000.
140186	Direct media does not function when the call is routed using alternative routing. **Applicable Products:** Mediant 3000.
140375	When the SDP offer is AVP/RTP with crypto and the SDP answer is AVP/RTP (non-secure), the device rejects the call. **Applicable Products:** Mediant 3000.
140497	RADIUS is not supported. **Applicable Products:** Mediant 3000/TP-8410/TP-6310.

2.24 Version 7.00A.095.004

This version includes known constraints and resolved constraints.

2.24.1 Known Constraints

Additional constraints discovered in this version include the following:

Table 2-25: Known Constraints for Version 7.00A.095.004

Incident	Description	Status
140497	RADIUS is not supported. **Applicable Products:** Mediant 3000/TP-8410/TP-6310.	Resolved in Version 7.00A.102.002 (see Section 2.23.1)

2.24.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-26: Resolved Constraints for Version 7.00A.095.004

Incident	Description
139941	The device crashes (resets) if it receives RTCP-XR parameters in incoming 200 OK messages. **Applicable Products:** Mediant 3000.
134960	If a rule in the Message Condition table is added, inserted or moved up/down, references to this table are lost in the Classification and/or IP-to-IP Routing tables, causing a service outage. **Applicable Products:** Mediant 3000.
139067	Some offline parameters are not displayed in the Web as offline parameters. **Applicable Products:** Mediant 3000.
139860	The SBC device receives an INVITE from the proxy and forks the call to the IP and to the internal gateway. If the gateway rejects the call due to unavailable media realms, the SBC does not send a response to the proxy and when the proxy cancels the call, the device crashes (resets). **Applicable Products:** Mediant 3000.
139575	The device sends CDRs to the SEM with a time stamp of 1 hour delay. **Applicable Products:** Mediant 3000.
139581	For SRTP-to-SRTP calls, if the device receives four crypto lines and symmetric MKI is enabled, it removes 2 crypto lines to the other side and as a result, SRTP negotiation fails. **Applicable Products:** Mediant 3000.
139652	The device removes 'transport=UDP' received in the Contact header and as a result, the call fails. **Applicable Products:** Mediant 3000.
138417	A major security vulnerability has been detected in the OpenSSL library. (OpenSSL upgraded to 1.02j.) **Applicable Products:** Mediant 3000.

Incident	Description
139911	If users are deleted from the User Info table and the device then immediately resets, some users still remain. **Applicable Products:** Mediant 3000.
139863	When Message Manipulation is used to normalize the SDP body and the device receives known and unknown coders in the SDP, it duplicates the known coders in the outgoing SDP offer. As a result, the call fails. **Applicable Products:** Mediant 3000.
139464	The device disconnects the direct media negotiation in the following scenario: user 1 – SBC – proxy – SBC – user 2 (2 calls). **Applicable Products:** Mediant 3000.
139769	Management user types “Monitor” and “Administrator” cannot access the CLI. **Applicable Products:** Mediant 3000.
138929	The device does not refresh the call and disconnects it in the following scenario: 1) The device receives an INVITE with Session-Expires header from the one IP Group, 2) the device sends the INVITE to the peering IP Group without a Session-expires header. **Applicable Products:** Mediant 3000.
137812	If a user is added to the SBC User Info table through the Web interface and an HA switchover is then done, the user does not appear correctly in the table after the switchover. **Applicable Products:** Mediant 3000.
138796	If Lync sends CN packets and the device is configured to not send CN packets to the SIP trunk, the device still sends the packets. **Applicable Products:** Mediant 3000.
138647	Specific packets received from the network cause the device to crash (reset). **Applicable Products:** Mediant 3000 HA.
138749	When the password of user is modified in the User Info table, the device crashes (resets). **Applicable Products:** Mediant 3000.
138276	When using the CRP application and the CRPSURVIVABILITYMODE is set 0 (Always Emergency Mode), the alternative routing from users to server (in case there is no match in the database) doesn’t function. As a result, the call fails. **Applicable Products:** CRP with Mediant 3000.
138391	There are many messages that the device cannot send to Syslog due to its internal buffering capacity. **Applicable Products:** Mediant 3000.
138755	When an SBC call is configured to use RFC 2833 for DTMF and the device receives a SIP INFO, it does not forward the INFO to the second leg (and DTMF is not sent). **Applicable Products:** Mediant 3000.
138779	When the device negotiates the use of RFC 2833 for DTMF, after it receives a re-INVITE with fax, it changes the DTMF transport to SIP INFO and as a result, DTMF are not accepted by remote side. **Applicable Products:** Mediant 3000.

Incident	Description
138750	When the device uses the User Info table and it acts as a registration server, after an HA switchover, the registration do not appear in the table in the Web interface. **Applicable Products:** Mediant 3000.
135917	In the INVITE as a result of a REFER handled locally, the SDP version is incremented by 2 and not by 1 as required. As a result, calls are rejected by the remote party. **Applicable Products:** Mediant 3000.
138598	Removing SIP headers using Message Manipulation causes a resource leak and the manipulation is not done. **Applicable Products:** Mediant 3000.
138477	When Tel-to-IP routing is done by Proxy Set and the connection to the proxy fails, the device does not enter busy out state. **Applicable Products:** Mediant 3000.
137147	When a re-INVITE is sent with only T.38 and the other side does not support re-INVITE and supports only G.711 fax coders, the device responds with 488 and fax fails. **Applicable Products:** Mediant 3000.
138405	An SBC call that has transcoding with SRTP causes the device to crash (reset). **Applicable Products:** Mediant 3000.
138501	When the ini file contains long values (over 50 characters), searching values in the Web interface causes the device to crash (reset). (Max. characters increased to 512.) **Applicable Products:** Mediant 3000.
137542	Double\single quotes cannot be used in the Action field of the Message Manipulation table. As a result, certain manipulation rules cannot be implemented. **Applicable Products:** Mediant 3000.
136450	The **startup-script** CLI command is not functioning for the Auto-Update feature. As a result, the Startup script file cannot be loaded. **Applicable Products:** Mediant 3000.
137450	The device does not forward the text accompanying the 399 Warning header from leg to leg. (Now fixed – device supports Warning header code 399). **Applicable Products:** Mediant 3000.
138346	The device crashes (resets) for calls using only the VBD coder. **Applicable Products:** Mediant 3000.
138420	The device crashes (resets) in the following call scenario: 1) Tel-to-IP call is forked to IP, 2) device receives REFER with refer-to as FQDN that is resolved into addresses, 3) the device sends an INVITE to all the addresses, 4) upon receipt of a 200 OK, the device crashes. **Applicable Products:** Mediant 3000.
138286	When there is Call Setup rule that makes an LDAP query, if the LDAP server is down the device enters endless loops and crashes (resets). **Applicable Products:** Mediant 3000.
138397	When the device receives an invalid packet on the RFC 2198 port (RTP redundancy), it crashes (resets). **Applicable Products:** Mediant 3000.
137920	The device sends many duplicated syslog messages. **Applicable Products:** Mediant 3000.

Incident	Description
137534	When the device is configured with Force Transcoding, if during a call setup the device receives an UPDATE and responds to it with a 200 OK, the device disconnects call. **Applicable Products:** Mediant 3000.
137486	If PSTN Fallback is employed (using two PRI ports) and the License Key is defined for only one trunk, the trunks do not synchronize. A workaround is to set the License Key to 2 trunks. **Applicable Products:** Mediant 3000.
137646	The device drops the call in the following scenario: 1) Call between A and B, 2) A puts call on hold, 3) device configured to play MOH toward B from SIP trunk but requires DSP to play from PRT (should be played without DSP), if there is no DSP, the device drops the call **Applicable Products:** Mediant 3000.
137574	When loading an incremental ini file through the REST interface, the device crashes (resets). **Applicable Products:** Mediant 3000.
138152	Proxy IP address / FQDN do not appear correctly on the Call Routing Status page (Status and Diagnostics > VoIP Status > Call Routing Status). **Applicable Products:** Mediant 3000.
138200	When using SNMP, a memory resource leak occurs that causes the device to crash (reset). **Applicable Products:** Mediant 3000.
138397	Invalid RFC 2198 (RTP redundancy) packets cause the device to crash (reset). **Applicable Products:** Mediant 3000.

2.25 Version 7.00A.082.007

This version includes new features and resolved constraints.

2.25.1 New Features

New features introduced in this version include the following:

2.25.1.1 Loading Files through CLI Enhancements

The following CLI commands related to files have been introduced:

- **copy voice-configuration** command has been replaced with the new command, **copy ini-file**.
- New command **dial-plan-csv** for loading a Dial Plan file in CSV format, using the Automatic Update mechanism. The ini file is DialPlanCSVFileUrl.

Applicable Products: Mediant 3000.

2.25.1.2 AMD for G.729

Answer Machine Detection is now also supported for calls using the G.729 coder (was supported on for G.711).

Applicable Products: Mediant 3000.

2.25.1.3 Delayed ISDN Connect for Tel-to-IP Calls

The device can now be configured to delay the sending of the ISDN Connect message to the Tel side for Tel-to-IP calls that are considered as payphones. Upon the receipt of a SIP 200 OK, the device sends an ISDN Alerting message (instead of a Connect message). Only when the device receives a re-INVITE whose 'media=' line has the same IP address as the 200 OK, does the device send a Connect message.

The device can either query an LDAP server or use a Call Setup Rule to check whether the calling party (Tel side) is a payphone. For Call Setup Rules, the new parameter is used in the syntax (Condition and Action Subject fields): param.payphone (=='1' or =='0').

Applicable Products: Mediant 3000.

2.25.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-27: Resolved Constraints for Version 7.00A.082.007

Incident	Description
137713	When the device is enabled for direct media and the SDP offer doesn't contain a connection line at the media level and the answer doesn't contain a session level connection, the device doesn't release resources and thus, calls cannot be made. **Applicable Products:** Mediant 3000.
136322	The device's Web interface displays incorrect values for bandwidth per Media Realm. **Applicable Products:** Mediant 3000.

Incident	Description
137179	When the device is configured to handle fax on re-INVITE, if it receives a re-INVITE to put the user on hold with 'a=sendonly' and the received response is with 'a=revconly', the device re-opens the stream with 'a=inactive' and therefore, no audio (music on hold) occurs after hold. A workaround is to change fax settings. **Applicable Products:** Mediant 3000.
136053	When the device is configured to not operate with RTCP-XR and receives RTCP packets containing RTCP-XR, many DSP restart messages are shown in the Syslog, and sometimes voice quality is affected. A workaround is to enable RTCP-XR. **Applicable Products:** Mediant 3000.
136504	If an active registration for a given sip.instance (obtained from the SIP Contact header) changes its IP address to one that is already in use, the device sends a SIP 200 response, but the device's registration database becomes corrupt and the subsequent registration fails. **Applicable Products:** SBC Products.
137229	Routing of Tel-to-IP calls fail when the 'Always Use Proxy' parameter is set to Enable and the default Proxy Set is configured to Round Robin for the 'Proxy Load Balancing Method' parameter. A workaround is to change the setting of the 'Proxy Load Balancing Method' parameter. **Applicable Products:** Digital Mediant 3000.
137223	The device fails to forward SIP INFO messages for DTMF received during call establishment. **Applicable Products:** Mediant 3000.
137179	When the device receives a re-INVITE message with 'a=sendonly' to place the endpoint on hold and the subsequent response contains 'a=recvonly', the device reopens the stream with inactive and thus, no audio occurs. **Applicable Products:** Mediant 3000.
134546	The device's Web interface allows Cross-Site Scripting (XSS). (The constraint has been resolved by stopping XSS.) **Applicable Products:** Mediant 3000.
134547	The device accepts HTTP methods that are not expected, which may pose a security threat. (The constraint has been resolved by restricting the device to respond only to specific HTTP POST methods.) **Applicable Products:** Mediant 3000.
137100	The device resets in the following SBC call scenario: 1) The device receives an INVITE and sends it to the associated Proxy Set; 2) the proxy server responds with a SIP 401 requesting credentials but no new INVITE is received; 3) the device has an alternative routing rule for the call. A workaround is to remove the alternative routing rule. **Applicable Products:** Mediant 3000.
136173	If the device receives an RTCP XR packet from a remote side with type "Type: Statistics Summary Report Block (6)" (instead of type "VOIP statistics") for an SBC call, it does not correctly parse the packet and thus reports an incorrect MOS. **Applicable Products:** Mediant 3000.

Incident	Description
136875	If the device is configured with IP Group ID 0 and is upgraded from version 6.8 to 7.0, FXS/FXO endpoints belonging to the IP Group do not register and thus, calls for these endpoints cannot be processed. A workaround is to manually configure IP Group ID 0. **Applicable Products:** Analog Mediant 3000.
136484	If the device is configured with a maximum of 0 management sessions (i.e., none), the management user can still log in to the device through CLI. **Applicable Products:** Mediant 3000.
136777	If an incoming INVITE has an anonymous source number and is manipulated by the device, an incorrect source number is shown in CDR. **Applicable Products:** Mediant 3000.
136587	Some Syslog messages have the wrong Session ID. **Applicable Products:** Mediant 3000.
136191	The device does not correctly route SBC mid-call requests to users behind NAT as it uses the user's global address instead of source address. **Applicable Products:** Mediant 3000.
134584	The device does not do video calls over SBC calls (as BFCP stream was not opened with UDP forwarding on stream re-open). **Applicable Products:** Mediant 3000.
13480	When users connect to the device with TLS using mutual authentication, connection fails every second and thus, calls cannot be processed. **Applicable Products:** Mediant 3000.
135725	For WebRTC calls using Chrome, in some cases voice does not occur due to failure in DTLS negotiation. **Applicable Products:** Mediant 3000.
136079	For WebRTC calls using Firefox, no voice occurs after hold-retrieve as Firefox doesn't send STUN request after call retrieve. **Applicable Products:** Mediant 3000.
135869	IP-to-IP Outbound Manipulation adds extra "+" signs as a prefix to the number and thus, the wrong number is used for the SBC call. A workaround is to add another manipulation rule to remove it. **Applicable Products:** Mediant 3000.
136334	If an incoming PSTN call has an empty display name, the device adds a meaningless value in the SIP From header of the outgoing IP call. **Applicable Products:** Mediant 3000.
135495	Incorrect CPU usage utilization is shown. **Applicable Products:** Mediant 3000.
135153	The device does not play a ringback tone for the calling party due to incorrect DSP resource allocation required for playing the tone (RFC 2833 DTMF is not forwarded between sides). This occurs in the following scenario: device receives 180 with SDP from called party indicating that its playing media, but then the device receives 180 without SDP, indicating that the device needs to play the tone. **Applicable Products:** Mediant 3000.

2.26 Version 7.00A.074.001

This version includes new features and resolved constraints.

2.26.1 New Features

New features introduced in this version include the following:

2.26.1.1 Hookflash Detection and Transmission for SBC Calls

The feature provides support for detecting and forwarding hookflash signaling for SBC calls. In other words, DTMF transcoding is now supported for hookflash whereby the device interworks hookflash signaling based on RFC 2833 with SIP out-bound (INFO messages) signaling, and vice versa. The applicable parameters (existing) for configuring the feature include: 'RFC 2833 Mode', 'RFC 2833 DTMF Payload Type', and 'Alternative DTMF Method'.

Applicable Products: Mediant 3000.

2.26.1.2 Product Key Field for Enhanced Product Identification

This feature provides support for a new term, *Product Key* to facilitate identification of the device. This is in addition to the device's Serial Number. The Product Key identifies the device's chassis reference serial number and appears on the product label as "Product Key (S/N)" and displayed in the device's management interfaces:

- Web –'Product Key' field on the Device Information page
- CLI - show system feature-key
- EMS - Device Info’s Serial Number

The Serial Number identifies the product’s internal CPU and is displayed in the device's management interfaces (Web, CLI and EMS) and appears on the product label as "CPU S/N".

Customers should reference the Product Key when contacting AudioCodes (e.g., for technical support, support contract renewals and feature upgrades).

Applicable Products: Mediant 3000.

2.26.1.3 Preserving IP Address-Port for re-INVITE when All Media Rejected

The feature provides support for using the same IP address and ports for subsequent SDP negotiation (re-INVITE) when all media lines ("m=") in the SDP are rejected by the remote SIP entity. Note that the administrator should make sure that the device is configured with a media port range (Media Realm) that provides sufficient ports to support such scenarios as well as other calls.

Applicable Products: Mediant 3000.

2.26.1.4 Enhanced Management Security for Login Password

The feature provides enhanced security for management login passwords by enforcing the password to adhere to complexity requirements to ensure strong passwords. If this policy is enabled, passwords must meet the following minimum requirements when they are changed or created:

- Contain at least eight characters
- Contain at least two letters that are upper case (e.g., A)
- Contain at least two letters that are lower case (e.g., a)
- Contain at least two numbers (e.g., 4)

- Contain at least two symbols or non-alphanumeric characters (e.g., $, #, %)
- No spaces
- Contain at least four new characters that were not used in the previous password

The feature is enabled by the new ini file parameter, EnforcePasswordComplexity.

Applicable Products: Mediant 3000.

2.26.1.5 Autocomplete of Management Login Username

The feature provides support for disabling autocomplete when entering the management login username in the device's Web interface. Up until now, the Username field automatically offered previously logged in usernames. Disabling autocomplete is useful for security purposes, by hiding previously entered usernames and thereby, preventing unauthorized access to the device's management interface.

The feature is supported by the new parameter, WebLoginBlockAutoComplete.

Applicable Products: Mediant 3000.

2.26.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-28: Resolved Constraints for Version 7.00A.074.001

Incident	Description
135848	Running certain CLI scripts cause the device to crash (reset). **Applicable Products:** Mediant 3000.
135712	When operating in keep-alive with proxy load-balancing mode (for a Proxy Set), the device tries to make calls to the inactive proxy and therefore, calls cannot be established. **Applicable Products:** Mediant 3000.
135489	Up to 20 Message Manipulation Sets (IDs) can be configured in the Message Manipulations table. Therefore, when more than 20 SIP Interfaces are configured, not all of them can be associated with a dedicated Manipulation Set for pre-classification message manipulation (Pre-classification Manipulation Set ID parameter in the SIP Interfaces table). The constraint has been resolved by configuring a single Manipulation Set for all SIP Interfaces using the following syntax: "param.message.address.<src/dst>.sipinterface" **Applicable Products:** Mediant 3000.
135336	The device disconnects a WebRTC call made through Firefox, after 20 minutes. **Applicable Products:** Mediant 3000.
134549	The device stores some sensitive information (e.g. password) in its cache, which it should not. **Applicable Products:** Mediant 3000.
135722	When using Firefox, after the first WebRTC call, the device disconnects the signaling Web socket connection and no new calls can be made. **Applicable Products:** Mediant 3000.
135397	The Keep Original Call-ID parameter does not function on SIP SUBSCRIBE messages. **Applicable Products:** Mediant 3000.

Incident	Description
135502	Message Manipulation does not function when the value in the Action Value field is surrounded by double quotes (") in the loaded ini file. A workaround is to use single quotes. **Applicable Products:** Mediant 3000.
135482	The device has a security issue (CVE 2015-1805) a security patch that addresses the vulnerability needs to be added. **Applicable Products:** Mediant 3000.
135233	Performance monitoring statistics for registered users gives incorrect values. **Applicable Products:** Mediant 3000.
134432	The device does not recognize the ISDN FACILITY information element and as a result, call forwarding fails. **Applicable Products:** Mediant 3000.
135186	When the device is located behind NAT, it responds to UPDATE messages with its private IP address in the SDP instead of the public address. As a result, one-way voice occurs. **Applicable Products:** Mediant 3000.
135163	When configuring a Message Condition rule with a name that is over 40 characters, the device to crashes (resets). **Applicable Products:** Mediant 3000.
134548	Autocomplete of username during Web login cannot be disabled and may pose a security risk. (A new parameter added to resolve issue: WebLoginBlockAutoComplete) **Applicable Products:** Mediant 3000.
135558	When the target for an alternative route is an LDAP query, the device performs the query repeatedly and resources are not released. As a result, new calls cannot be processed. A workaround is to use Call Setup Rules for alternative routing instead of LDAP. **Applicable Products:** Mediant 3000.
134877	When editing the Proxy Set table through the Web interface, the device crashes (resets). A workaround is to use SNMP or ini file management tools. **Applicable Products:** Mediant 3000.
134843	The device does not enable changing the password of the Admin user to a weaker password. (Constraint resolved by new parameter that enables or disables enforcement of password complexity: EnforcePasswordComplexity) **Applicable Products:** Mediant 3000.
134865	The TCP connection used to establish the call terminates and thus, the device sends the SIP BYE to the wrong destination. As a result, the remote server still considers the call as connected. A workaround is to enable the ENABLETCPCONNECTIONREUSE and FAKETCPALIASA parameters. **Applicable Products:** Mediant 3000.
134937	DTMF transcoding is erroneously based on the coder transcoding license as defined in the License Key. As a result, the device may not achieve the maximum number of coder transcoding. **Applicable Products:** Mediant 3000.

Incident	Description
134950	When trying to access the device's Web interface using HTTPS, illegal heap errors appear in the Syslog, which may cause a device crash (reset). A workaround is to not use HTTPS. **Applicable Products:** Mediant 3000.
134849	When the device performs hairpinning on trunks and the clock settings of the trunks are subsequently changed, the trunks go down and calls cannot be made. **Applicable Products:** Mediant 3000.

2.27 Version 7.00A.067.003

This version includes new features and resolved constraints.

2.27.1 New Features

New features introduced in this version include the following:

2.27.1.1 Utilizing Gateway Channel Resources for SBC Sessions

This feature provides support for utilizing the resources of non-configured Gateway channels (analog and digital) for SBC sessions, regardless of whether the device is licensed for SBC functionality.

To support the feature, a new feature key–"TDMtoSBC"–has been introduced, which must be included in the Software License Key installed on the device. Customers whose devices do not have this feature key should contact AudioCodes sales representative to upgrade their license.

This feature, in essence, allows "call" resources to be migrated from the Gateway to the SBC, allowing Gateway customers to migrate to an all IP-based voice network with a simple configuration change.

Customers purchasing the device for the intention of deploying it only as a Gateway for PSTN calls can at any later stage use the device for SBC calls without having to purchase an SBC license.

A Gateway channel is considered "not configured" if it is not associated with any Trunk Group (configured in the Trunk Group table). If all Gateway channels are configured, resources from the channels cannot be used for SBC sessions. If the resources of active SBC calls are obtained from Gateway channels and the administrator configures all Gateway channels during the call, the calls are maintained until they are terminated by the call parties, but obtaining resources from Gateway channels for new SBC calls will not be made possible.

For every non-configured Gateway channel, one SBC session can be processed. For example, a Software License Key licensing 1 E1 and 4 FXS can support up to 35 SBC sessions (31 channels for E1 plus 4 for FXS) if all the Gateway channels are not configured. If the Software License Key also provides a license for 5 SBC sessions, up to 40 SBC sessions (31 channels for E1 plus 4 for FXS plus 5 for SBC) can be supported. Note that the maximum supported SBC sessions is according to the device's normal maximum SBC capacity.

The number of SBC sessions that can be supported if Gateway channels are not configured is displayed in the device's Web interface (Software Upgrade Key Status page).

Applicable Products: Mediant 3000.

2.27.1.2 New NAT Traversal Method

This feature provides support for a new NAT traversal method for SBC calls whereby the device identifies whether or not the UA is located behind NAT based on SIP signaling only. The device assumes that if signaling is behind NAT that the media is also behind NAT, and vice versa.

The feature is supported by the new option, [3] NAT by Signaling for the existing NATMode parameter. If the UA is identified as located behind NAT, the device sends media as described for option [2] Force NAT; if not behind NAT, the device sends the media as described in option [1] Disable NAT (see the user's Manual for more information). Note: This is applicable to SBC calls only. For Gateway calls, if this option is configured, the device uses option [0] Enable NAT.

Applicable Products: Mediant 3000.

2.27.1.3 Routing Server / ARM Enhancements

This feature provides support for the following enhancements for the third-party Routing server / ARM feature:

- The Routing Server / ARM can now provide user (e.g., IP Phone caller) credentials (username-password) in the GetRoute response that can be used by the device to authenticate outbound SIP requests if challenged by the outbound peer, for example, Microsoft Skype for Business (per RFC2617 and RFC3261). Note that if multiple devices exist in the call routing path, the Routing Server / ARM sends the credentials only to the last device ("node") in the path.
- The Routing Server / ARM can now receive NOTIFY and MESSAGE dialog-initiating SIP request types from the device. Up until now, the device sent only INVITE messages to the Routing Server / ARM in the GetRoute request. The 'Request Type' parameter in the IP-to-IP Routing table is used to specify INVITE messages. To specify MESSAGE or NOTIFY requests (and INVITEs), a Message Condition rule must be applied to the routing rule (*Condition= header.request-uri.methodtype == '5' or header.request-uri.methodtype == '13' or header.request-uri.methodtype == '14'*) with the 'Request Type' parameter set to Mediant 3000. The Routing Server / ARM replies to the device with the destination IP Group (and if necessary, IP address and username/password) in the GetRoute response.
- The Routing Server / ARM can now provide an IP address (and port and protocol / FQDN) to the device in the GetRoute response to route the call to the specific IP address. In this scenario, even though the destination type (in the IP-to-IP Routing table) is an IP Group, the device only uses the IP Group for profiling (i.e., associated IP Profile etc.). Note that if multiple devices exist in the call routing path, the Routing Server / ARM sends the IP address only to the last device ("node") in the path.
- A new REST feature enables the device to periodically send Call Audit reports to the Routing server. This mechanism enables the Routing server to track the number of active sessions on the device. For every call that exceeds a pre-defined length (defined by the 'length' attribute in the callAudit URL), the device sends a Call Audit report according to a configured interval period (defined by the "callAudit" attribute in the GetRoute response). Call Audits are generally reported "per leg" i.e. typically two Call Audit requests are issued for each session; one for the incoming INVITE leg and another for the outgoing leg (as is also the case for the Call Status reports). For example, if the minimum call 'length' attribute in the callAudit URL is set to 15 minutes, and the "callAudit" attribute in the GetRoute response is also 15 minutes; for a 40 minute call, the "callAudit" will be reported four times – two reports after 15 minutes (for each call leg) and another two reports after 30 minutes.

Applicable Products: Mediant 3000.

2.27.1.4 Preferred IP Version (ANAT) for Outgoing SIP Calls

This feature provides support for configuring the preferred IP address version (IPv4 or IPv6) for outgoing SBC calls. Up until this release, the feature was supported only by Gateway calls. The support is according to RFC 4091 and RFC 4092, which concern Alternative Network Address Types (ANAT) semantics in the SDP to offer groups of network addresses (IPv4 and IPv6) and the IP address version preference to establish the media stream. The feature is supported by the already existing parameter, IpProfile_MediaIPVersionPreference and its options [2] Prefer IPv4 and [3] Prefer IPv6.

Applicable Products: Mediant 3000.

2.27.1.5 Unregister Requests and Graceful Time

This feature provides support for adding a graceful period before removing a user from the registration database when the device receives a successful unregister response (200 OK) from the registrar/proxy server. This is useful in scenarios, for example, in which users (SIP user agents) such as IP Phones erroneously send unregister requests (i.e, REGISTER messages with Expires header set to 0). Instead of immediately removing the user from its registration database after a successful unregister response is received, the device waits until it receives a successful unregister response from the registrar server, waits the user-defined graceful time and if no register refresh request is received from the user agent, the device removes the contact (or AOR) from the database. The graceful time is configured using the existing parameter SBCUserRegistrationGraceTime.

Applicable Products: Mediant 3000.

2.27.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 2-29: Resolved Constraints for Version 7.00A.067.003

Incident	Description
134797	When the device establishes an SBC call as direct media, the device rejects the SIP INFO message with DTMF with a SIP 500 (Sever Internal Error) response and DTMF is not transmitted. A workaround is to disable direct media. **Applicable Products:** Mediant 3000.
134380	If the administrator creates more than one Master user account, these users cannot log in to the device. **Applicable Products:** Mediant 3000.
131918	Certain scenarios cause the device to try allocating TLS connections that are already in use. As a result, the device crashes and resets. **Applicable Products:** Mediant 3000.
134431	The string "E-SBC" is displayed throughout the Web GUI instead of "SBC". **Applicable Products:** Mediant 3000.
134506	When the device has only E1\T1 modules, the Web interface does not display the MWI parameters and therefore, these parameters cannot be configured through the Web. **Applicable Products:** Mediant 3000.
134388	For WebRTC, when a re-INVITE (hold feature) originates from a Web client and the password and fragment for ICE have changed, the device rejects the call with a 500 (Sever Internal Error) response. **Applicable Products:** Mediant 3000.
134581	Fax transcoding between T.38 and transparent does not work. As a result, the fax fails. **Applicable Products:** Mediant 3000.
134032	When the device uses an FQDN for a Proxy Set and connection to the DNS server is lost, the device raises an alarm. However, when connection is restored, the device does not clear the alarm. A workaround is to enable the proxy keep-alive feature. **Applicable Products:** Mediant 3000.
134236	The device crashes and resets when it receives a UDP packet on an RTP port and the UDP packet contains UDP Length of only 8 bytes (UDP header only). **Applicable Products:** Mediant 3000.

Incident	Description
133475	When the remote user agent is located behind a NAT, the device updates the remote RTP IP:port according to from where it was received. However, for re-INVITEs, the device does not update the destination IP:port and as a result, no voice occurs after the re-INVITE. This has been fixed by the new value, [3] "NAT By Signaling" added to the NATMODE parameter. **Applicable Products:** Mediant 3000.
134348	The 'Board Type' field in the Device Information page of the Web interface displays the device's name instead of number (according to installed Feature Key). **Applicable Products:** Mediant 3000.

2.28 Version 7.00A.063.003

This version includes only resolved constraints.

2.28.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. The device cannot be accessed through HTTPS. A workaround is to run the following command sequence in CLI and then access:

```
configure voip
(config-voip)# tls 0
(tls-0)# ciphers display
```

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

2. The device does not reset after loading an ini file that contains a different OAMP IP address than the current OAMP address. A workaround is to manually reset the device after loading the ini file.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

3. The RADIUS server rejects CDR messages when the Account Session ID is repeated between calls and therefore, no CDRs are recorded.

   The constraint has now been resolved.

   SR: 779349

   Applicable Products: All HA.

4. For WebRTC, the Chrome browser starts the DTLS handshake prior to completing the ICE process, causing delay in voice.

   The constraint has now been resolved.

   SR: 775647

   Applicable Products: Mediant 3000.

5. If the administrator changes the Served IP Group to IP Group ID 0 in the Account table, the device sends the SIP 407 response to the calling side instead of answering the call itself. Therefore, calls fail. A workaround is not to use IP Group ID 0.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

6. The device reports calls with high packet loss as good quality to SEM.

   The constraint has now been resolved.

   SR: 774309

   Applicable Products: Mediant 3000.

7. Instead of displaying up to 20 selectable Allowed Coder Groups, the IP Profile table displays only 5. A workaround is to configure the IP Profile through ini file.

   The constraint has now been resolved.

   SR: 777155

   Applicable Products: Mediant 3000.

8. When multiple contacts per AOR exist, the device fails to classify the user and users are not registered. A workaround is to use message manipulations to remove the instance ID.

   The constraint has now been resolved.

   SR: 776755

   Applicable Products: Mediant 3000.

9. A rare situation causes an HA switchover.

   The constraint has now been resolved.

   SR: 770325

   Applicable Products: All HA.

10. In a setup of CAS and WebRTC using 1 trunk, the user cannot make more than 17 calls.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

11. The device parses “%40” as “@” in the SIP From header, causing calls to fail.

    The constraint has now been resolved.

    SR: 779297

    Applicable Products: Mediant 3000.

12. Block unregistered users does not work when configured per SIP Interface, resulting in un-registered users being able to make calls. A workaround is to use the feature per SRD.

    The constraint has now been resolved.

    SR: 772809

    Applicable Products: Mediant 3000.

13. When both sides negotiate G.729 with "Annex B = no" in the re-INVITE, the device does not send "Annex B = no", causing the remote side to consider it as enabled and resulting in voice problems.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

14. Device crashes and resets when the following CLI command is entered: `show voip` channel–`stats virtual 1 201`.

    The constraint has now been resolved.

    SR: 779439

    Applicable Products: Mediant 3000.

15. The displayed certificate expiration date is incorrect.

    The constraint has now been resolved.

    SR: 775003

    Applicable Products: Mediant 3000.

16. When using WebRTC behind NAT, the beginning of the audio is lost.

    The constraint has now been resolved.

    SR: 775647

    Applicable Products: Mediant 3000.

17. Debug capture cannot capture re-INVITE messages sent by the device.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

18. If the device receives a re-INVITE with SDP, sends a 200 OK with SDP, but then receives the ACK without SDP, the device attempts to perfom media synchronization, causing the call to fail. A workaround is to configure the parameter ENABLEMEDIASYNC to 0.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

19. If debug capture is enabled through CLI and then stopped by pressing the Ctrl + C key combination, the device crashes and resets.

    The constraint has now been resolved.

    SR: 778503

    Applicable Products: Mediant 3000.

20. During fax transcoding between T.38 and G.711 over SRTP, the device sends a re-INVITE to G.711 without SRTP, resulting in insecure fax.

    The constraint has now been resolved.

    SR: 755367

    Applicable Products: Mediant 3000.

21. When the device is not used for HA, it still sends messages about HA.

    The constraint has now been resolved (HA disabled by new parameter - M3KHAEnabled).

    SR: N/A

    Applicable Products: Mediant 3000.

2.29 Version 7.00A.058.102

This version includes only resolved constraints.

2.29.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. One-way voice occurs when a call is transferred by the device using a new channel that does not support silence packets (as supported on the previous channel), if silence packets are received on the new channel.

   The constraint has now been resolved.

   SR: 777293

   Applicable Products: Mediant 3000.

2. When a call changes from RTP forwarding to transrating, the device crashes and resets.

   The constraint has now been resolved.

   SR: 780355

   Applicable Products: Mediant 3000.

3. The device crashes and resets when using the Web interface in a certain sequence.

   The constraint has now been resolved.

   SR: 778637

   Applicable Products: Mediant 3000.

2.30 Version 7.00A.058.002

This version includes only known constraints and resolved constraints.

2.30.1 Known Constraints

Additional constraints discovered in this version include the following:

1. The device cannot be accessed through HTTPS. A workaround is to run the following command sequence in CLI and then access:

   ```
   configure voip
   (config-voip)# tls 0
   (tls-0)# ciphers display
   ```

   SR: N/A

   Applicable Products: Mediant 3000.

2. The device does not reset after loading an ini file that contains a different OAMP IP address than the current OAMP address. A workaround is to manually reset the device after loading the ini file.

   SR: N/A

   Applicable Products: Mediant 3000.

2.30.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. The Char Conversion table (CharConversion) does not convert non-ASCII characters for IP-to-Tel calls in SIP P-Asserted-Identity headers. Therefore, the wrong name is sent to the PSTN.

   The constraint has now been resolved.

   SR: 775429

   Applicable Products: Digital Mediant 3000.

2. When using SIPRec, the second SIPRec call for the consultation part of the call transfer does not terminate when the call is transferred, and the transfer fails.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

3. In a WebRTC video call, only one-way video occurs.

   The constraint has now been resolved.

   SR: 772375

   Applicable Products: Mediant 3000.

4. The device does not route calls correctly when using LDAP and a 302 response is received. The call scenario is as follows: The device performs an LDAP query according to the Routing table and then routes the call according to the LDAP result. If it receives a SIP 302 Moved Temp response, the device routes the new call according to the Routing table instead of the SIP Refer-To or Contact.

   The constraint has now been resolved.

   SR: 775055

   Applicable Products: Mediant 3000.

5. When the call pickup feature is enabled and a call pickup is done in a direct media connection, the device crashes. A workaround is to disable direct media.

   The constraint has now been resolved.

   SR: 775805

   Applicable Products: Mediant 3000.

6. HA is always enabled even if the device is shipped without HA.

   The constraint has now been resolved.

   SR: 775083

   Applicable Products: Mediant 3000.

7. The parameter relating to SBC jitter (IpProfile_SBCJitterCompensation) is displayed in the Web GUI only when there are DSP resources

   The constraint has now been resolved.

   SR: 766369

   Applicable Products: Mediant 3000.

8. For SBC initiated calls without SDP, in order to play ringback tone, the device sends a re-INVITE with SDP and when the SBC sends the SIP ACK message it crashes. A workaround is to disable play of ringback tone.

   The constraint has now been resolved.

   SR: 777087

   Applicable Products: Mediant 3000.

9. The device is not protected against Cross Site Request Forgery (CSRF) and therefore, venerable to being hacked.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

10. When the device sends retrieve with the same RTP port, it sends it in the INVITE, however, no voice occurs after hold\retrieve. A workaround is to disable direct media.

    The constraint has now been resolved.

    SR: 761611

    Applicable Products: Mediant 3000.

11. When the device receives a response from an LDAP server and the “memberOf” attribute value length is greater than 256 characters, it does not accept the response and LDAP authentication fails.

    The constraint has now been resolved.

    SR: 775321

    Applicable Products: Mediant 3000.

12. The device is not protected from Cross Site Scripting (XSS) and therefore, venerable to being hacked.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

13. Calls fail in the following call scenario: The device sends a re-INVITE with the telephony-event when it receives a re-INVITE without SDP when the remote side doesn’t support delay. The call negotiates G.722 and telephony-event rate 8000. The device receives a re-INVITE without SDP and sends a re-INVITE with G.722 and telephony-event rate 16000.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

14. If TDM hairpinning is enabled, when an HA switchover occurs the ISDN channels go of-line and no calls can be made after the switchover.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

15. BFCP streams over UDP is not supported in this version.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

2.31 Version 7.00A.053.006

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

2.31.1 New Features

New features introduced in this version include the following:

2.31.1.1 Sending Alarms between TDM Hairpinned Connected Trunks

The feature provides support for trunks connected through the TDM hairpinning to signal the Far-End about the presence of PSTN alarms. When the trunk with TDM Hairpinning receives a PSTN alarm, its connected trunk sends an AIS alarm to its Far-End. The feature is applicable only to the PRI E1 protocol.

(TDM Hairpinning is configured using the existing parameter, TDMHairPinning.)

To support the feature, the following parameter has been added:

[TDMHairPinningAlarmIndication]	Enables two trunks that are connected through TDM hairpinning to send PSTN alarms to the Far-End when the connected trunk receives a PSTN alarm. ▪ [0] = (Default) Disable ▪ [1] = Enable

Applicable Products: Mediant 3000.

2.31.1.2 SIP Authorization Challenge Cache for SBC Calls

The feature provides support for local caching of SIP authorization challenges (SIP 401/407 response with a challenge) for SIP dialog-initiating requests (e.g., INVITE) received from proxies. Subsequent new requests to the Proxy are automatically sent with the user agent's credentials (from the saved challenge in the device's cache).

Up until this release, the feature was applicable only to the Gateway application. To support the feature, the existing SIPChallengeCachingMode parameter is now also applicable to SBC calls.

Applicable Products: Mediant 3000.

2.31.2 Known Constraints

Additional constraints discovered in this version include the following:

1. When importing a Dial Plan file (*.csv file), it is recommended to configure the SyslogDebugLevel parameter to **No Debug**.

   SR: N/A

   Applicable Products: Mediant 3000.

2.31.3 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. When the device forks SBC calls, it does not locally handle received SIP 302 responses and as a consequence, call forward fails.

   The constraint has now been resolved.

   SR: 768497

   Applicable Products: Mediant 3000.

2. The Web pages of the device's Web-based management tool are not displayed correctly with Internet Explorer 11 and therefore, the Web interface cannot be used. A workaround

is to use another browser.

The constraint has now been resolved.

SR: 768497

Applicable Products: Mediant 3000.

3. Conversion from Unicode characters in incoming INVITE From headers to non-Unicode only characters in outgoing INVITE From headers, cause a corruption of strings in the outgoing From header.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

4. After successful registration, the TLS connection toward the user is closed and subsequent INVITEs (calls) toward the user fails.

   The constraint has now been resolved.

   SR: 772251

   Applicable Products: Mediant 3000.

5. SBC calls fail in the following call scenario: 1) The device receives an INVITE without SDP (A) and sends the INVITE with SDP (B); 2) B sends 183 with 100rel and the device forwards it to A; 3) Before the device responds to B with PRACK, it receives 200 OK and forwards it to A; 4) A responds with PRACK + SDP for the 183 request and immediately responds to the 200 OK with ACK without SDP.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

6. When the HTTP Proxy feature is used and the HTTP proxy receives a SIP 302 response, the device forwards it without changing the Contact to the correct location. As a result, new INVITEs generated as a response to the 302 are not routed correctly.

   The constraint has now been resolved.

   SR: 769595

   Applicable Products: Mediant 3000.

7. The device rejects SIP UPDATE during calls. Call scenario: 1) the device sends an INVITE from A to B. 2) B answers with three forked calls. 3) The second call answers and the call is established. 4) When A sends an UPDATE, the device rejects it with a SIP 488 response.

   The constraint has now been resolved.

   SR: 771877

   Applicable Products: Mediant 3000.

2.32 Version 7.00A.049.003

This version includes only new features, and resolved constraints.

2.32.1 New Features

New features introduced in this version include the following:

2.32.1.1 Routing Server Support for IP-to-Tel Calls and Enhancements

The feature provides support for routing of IP-to-Tel calls by a Routing server. Up until now, this was supported only for Tel-to-IP and SBC calls. The feature also changes the configuration method for enabling routing of Gateway calls by the Routing server. Up until now, the administrator had to add the string "REST" as the destination IP address in the routing table; now, the new global parameter, GWRoutingServer is used to enable the feature.

Note: The feature is supported from software version 7.00A.048.001.

Applicable Products: Mediant 3000.

2.32.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. The device disconnects the call if it receives a 200 OK in response to the sent INVITE before it receives a 200 OK in response to the PRACK.

   The constraint has now been resolved.

   SR: 771059

   Applicable Products: Mediant 3000.

2. After the device upgrades from Version 6.8 to 7.0, it stops sending REGISTER requests, on behalf of the Trunk Group, to the proxy.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

3. For the HTTP Reverse Proxy application, headers are missing in the request from the proxy.

   The constraint has now been resolved.

   SR: 769597

   Applicable Products: Mediant 3000.

4. For the HTTP Proxy application, the HTTP Proxy does not process 302 responses correctly. As a result, new INVITEs generated in response to 302 are not routed correctly.

   The constraint has now been resolved.

   SR: 769595

   Applicable Products: Mediant 3000.

5. During a call, the device plays a tone to one of the legs (from the installed PRT file) and while playing, the device receives a re-INVITE to change the coder. This scenario results in playing being stopped and the device sending poor quality audio.

   The constraint has now been resolved.

   SR: 768999

   Applicable Products: Mediant 3000.

6. If the device receives calls without an SDP body (xml), after a few hours no new calls

can be placed.

The constraint has now been resolved.

SR: 770153

Applicable Products: Mediant 3000.

7. When the administrator clicks the Burn button in the Web interface, a warning about degradation of voice quality is displayed even though there is no such degradation.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

8. When the administrator logs in to or out of the device, a message indicates this in the syslog. The message is under the Alarm category instead of the INFO category.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

9. When the device receives unknown RTP packets (RTP Version = 1) it stops forwarding the RTP to the second leg for a few seconds and thus, no audio is heard for these seconds.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

10. If the EnableWebAccessFromAllInterfaces parameter is enabled, access to the Web interface from some interfaces cannot be done.

    The constraint has now been resolved.

    SR: 763393

    Applicable Products: Mediant 3000.

11. When the device rejects a REGISTER request due to CAC, the user is erroneously added to the registration database. The database eventually becomes full due to this behavior of additional registers and new registrations cannot be accepted.

    The constraint has now been resolved.

    SR: N/A

    Applicable Products: Mediant 3000.

2.33 Version 7.00A.046.003

This version includes only known constraints and resolved constraints.

2.33.1 Known Constraints

Additional constraints discovered in this version include the following:

1. For device's operating in High-Availability (HA) mode, deleting a dial plan can adversely affect traffic for a few seconds. A workaround is to import (install) an empty Dial Plan file (*.csv file).

   SR: N/A.

   Applicable Products: Mediant 3000.

2. If an existing dial plan row is modified so that it is identical to another existing dial plan row (which is an invalid configuration), when the administrator exports or imports the Dial Plan file the rows are switched with regards to their position (index) in the table and thus, routing based on these dial plans are incorrect (wrong tags).

   SR: N/A.

Applicable Products: Mediant 3000.

3. A "best match" scheme is not fully implemented in the Dial Plan feature for dial plan rules configured with a second level matching characteristics. The first level of a rule refers to the first digits and the second level refers to anything after the first level, which can be ranges or suffix number. For example, in the rule "532[1-9]444", "532" is the first level and everything to the right is the second level. In these scenarios, the first match is used instead of the best match.

   For example, assume the following rules in a Dial Plan:

   ```
   532[1-9],A
   532[2-4],B
   ```

   If the destination number is "5324", instead of selecting the rule with tag B, which is a more specific (constrained) rule, the device erroneously selects the rule with tag A.

   For example, assume the following rules in a Dial Plan:

   ```
   53([2-4]),A
   53(4),B
   ```

   If the destination number is "53124", instead of selecting the rule with tag B, which is a more specific rule, the device erroneously selects the rule with tag A.

   SR: N/A.

   Applicable Products: Mediant 3000.

2.33.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. Enabling access by management stations (Web clients) to the Web-based management tool through any of the device's interfaces (in addition to the OAMP interface), by configuring the EnableWebAccessFromAllInterfaces parameter to 1, works flawlessly only under any one of the following conditions:

   a. The IP address of the Web client resides in the same subnet of the device's interface through which the Web client is accessing the Web interface.

   b. The IP address of the Web client does not reside in the same subnet as mentioned in a) above, but the device is configured with a Static Route rule (in the Static Routes table) where the destination ('Destination' field) is the IP address of the Web client and the assigned Ethernet Device ('Device Name' field) is the one associated with the device's network interface through which the Web client is accessing the Web interface.

   Applicable Products: Mediant 3000.

2.34 Version 7.00A.044.007

This version includes only new features and resolved constraints.

2.34.1 New Features

New features introduced in this version include the following:

2.34.1.1 Increase in Multiple Media Streams in SDP per Session

This feature provides support for an increase in the maximum number of media streams that can be negotiated per session. The device supports up to nine media streams ('m=' line) in the SDP offer/answer model per session when forwarded transparently. When the device handles media translations such as RTP-SRTP, the maximum is four media lines in the SDP. The media can include any combination of media types (audio, text, video, fax and/or BFCP).

Applicable Products: All SBC Supporting Products.

Applicable Application: Mediant 3000.

2.34.1.2 Registration Status for Gateway-type IP Groups

This feature provides support for displaying the registration status of Gateway-type IP Groups (IPGroup_Type = 2). As explained in more detail in the User's Manual, Gateway-type IP Groups are typically IP Groups whose addresses are unknown (and therefore, are not assigned a Proxy Set). Their address is only discovered once the device receives a registration request from them.

The registration status is displayed in the IP Group table in the following new read-only fields:

- 'GW Group Registered IP Address': IP address of the gateway if registered; otherwise, the field is blank.
- 'GW Group Registered Status': Displays whether the gateway is registered with the device - "Registered" or "Not Registered".

Applicable Products: Mediant 3000.

2.34.1.3 Enhanced Dial Plan Functionality

In certain deployments, there is a need to split the SBC routing process into two different logical phases:

1. Categorize the source and destination users. For example, source user is from the sales department and the destination number is a mobile subscriber.
2. Routing rules based on IP Groups that define exactly how the categorized users can reach each other regarding routes and alternative routes. For example, salespersons can use the premium route whereby their calls are routed to a specific SIP Trunk and if the SIP Trunk is unavailable, they can use an alternative PSTN route.

There is a clear distinction between user categorization (first phase) and IP Groups (second phase). IP Groups represent SIP devices or servers (e.g., SIP Trunk, IP PBX, and softswitch) with which the device communicates. User categorization may be done regardless of the physical equipment that serves them or is used to reach them. A user may optionally be categorized as belonging to more than one category, i.e., belonging to the sales department and also a mobile subscriber. In addition, a user may be reached using different routes.

Splitting the routing process into two different logical entities simplifies and minimizes routing rule configuration, making it easy to update as deployment grows or changes. Thus, the device first categorizes the traffic, and then uses this as an input to the routing process which is done using the IP-to-IP Routing table.

Up until this release, categorization was done using an old dial plan mechanism and the inputs for the routing process where handled inefficiently. Dial plans were configured in a single file, which then had to be installed on the device. For each subsequent modification to a dial plan(s), the administrator had to re-install the entire file. The Dial Plan file creation included first defining the dial plans using a text-based file editor (e.g., Notepad), and then converting the file to a binary file (.dat) through AudioCodes DConvert utility, before installing it on the device. Once installed, the administrator couldn't view, add, edit or delete the dial plan rules on the device. These dial plans could manipulate the number and this is how the IP-to-IP routing considered the Categorization that was done on the dial plan process. This old mechanism will remain for backward compatibility.

The new feature introduces a whole new mechanism which is much more intuitive and manageable with a feature-rich functionality. The new dial plan mechanism allows a user to categorize source and destination numbers according to prefixes, suffixes, exact match of whole number, and other patterns, described later on.

Categorization is optional and once configured is done each time the device processes a call setup. Categorization is done after Classification and inbound header manipulation, and before the routing process.

It is also optionally done twice, once for the source and once again for the destination number. Its' input is either the source or destination number and the output is two tags – one for the source and one for the destination. These tags are assigned to the call and can be used as inputs for subsequent processes, specifically the routing and the outbound number manipulation. Note that these specific tags are stored and can be used in subsequent routing and manipulation processes of the call that may occur due to alternative routing or local handling of call transfer and call forwarding (SIP 3xx\REFER).

Below is an overview of the Dial Plan feature:

- **Dial Plans:** A dial plan is a set of dial plan rules. A dial plan rule has two basic attributes - the prefix and the tag. The prefix is matched against the source or destination number (after inbound number manipulation). Its' format is explained later. The tag is the output source or destination tag that is assigned to the call.

  A dial plan can be assigned to an IP Group or SRD. After classification and inbound number manipulation, the device searches for a relevant dial plan. It first checks the source IP Group for an assigned dial plan and if no dial plan is assigned, it checks the SRD. If a dial plan is associated, the device uses the dial plan twice. It first checks the source number and afterwards the destination number. The output of this process is optional source and destination tags.

  The device can be configured with up to 5 different dial plans. A maximum of 2,000 dial plan rules can be configured for **all** the dial plans; they can all be configured for one dial plan or for different dial plans.

- **Dial Plan Configuration:** The new feature enables the administrator to configure (add, edit and delete) dial plans directly through the Web or CLI. This is supported by two new tables: Dial Plan table and its "child" table, the Dial Plan Rules table. Each row in the Dial Plan table represents a Dial Plan (index and name), which is then configured with dial plan rules in the associated Dial Plan Rules table.

  The administrator can import and export dial plans in comma-separated value (CSV) file format through the CLI (supported through the Web interface in a future release). The file can be imported for a specific Dial Plan, whereby it overwrites the existing rules pertaining to that Dial Plan, or it can be imported for the entire Dial Plan table, overwriting all rules of the Dial Plans. The format of Dial Plans in CSV files is as follows:

  ```
  <Dial Plan name>,<rule name>,<prefix>,<tag>
  ```

  For example:

  ```
  DialPlanName,Name,Prefix,Tag
  PLAN1,rule_100,5511361xx,A
  PLAN1,rule_101,551136184[4000-9999]#,B
  MyDialPlan,My_rule_200,5511361840000#,itsp_1
  MyDialPlan,My_rule_201,66666#,itsp_2
  ```

- **Routing and outbound number tables enhancements:** As previously mentioned, the dial plan process assigns two different tags to the call, which can now be used as the input to the routing and outbound manipulation processes. To support the feature, two new parameters were added to these tables - one for the source tag and one for the destination tag.
- **Dial Plan rule prefixes syntax:** Modifications to the dial plan syntax include:
    - x: wildcard denoting any digit from 0 through 9.
    - z: denotes a number from 1 through 9.
    - n: denotes a number from 2 through 9.
    - a-z: denotes a lower-case letter.
    - A-Z: denotes an upper-case letter.
    - * : (Asterisk symbol) If it is the only character in the rule, it denotes any number. To denote the asterisk "*" symbol itself, it must be used with an escape "//" character (see below).
    - # : (Pound symbol) When used at the end of a prefix, it denotes the end of a number. For example, 54324# represents a 5-digit number that starts with the digits 54324.
    - \\ : (Backslash escape character) When it prefixes a special character, the character itself is used and not the meta-meaning (e.g., "\\x" denotes the character "x", while simply "x" is the wildcard denoting any digits from 0-9). Special characters include: *, z, n, and x.
    - . : (Period) Denotes any letter or digit.
    - [n-m], (n-m), or ([n1-m1,n2-m2,a,b,c,n3-m3]): Represents a mixed notation of single numbers and multiple ranges. To represent the prefix, the notation is enclosed by square brackets; to represent the suffix, the notation is enclosed by square brackets which are enclosed by parenthesis. For example, to denote numbers 123 to 130, 455, 766, and 780 to 790:
        - Prefix: [123-130,455,766,780-790]
        - Suffix: ([123-130,455,766,780-790])

      Note: The ranges and the single numbers in the dial plan must have the same number of digits. For example, each number range and single number in the dialing plan example above consists of three digits.
    - The $ (dollar) sign is not supported.

  The device employs a “best-match” method instead of a first-match method to match the source/destination numbers to possible prefixes configured in the dial plan. The matching order is done digit by digit, from left to right. The numbers are matched first to the rule configured with the most constrained (specific) character set. Most constrained implies that the pattern that has the **fewest** possible matches for a digit is matched first. For example, if one rule contains the "x" character, which has ten possible matches (i.e., 0-9) and another rule a specific character (e.g., 4), the rule with the specific character is selected as a possible matching rule.

  Below are examples:
    - Example 1:
      ```
      523x,A
      5234,B
      ```
      For incoming calls with prefix number "5234", rule with tag B is used.
    - Example 2:
      ```
      523x,A
      523[1-9],B
      ```
      For incoming calls with prefix number "5234", rule with tag B is used.
    - Example 3:

```
532[1-9]1111,A
5321,B
```

For incoming calls with prefix number "53211111", rule with tag B is used.

- Example 4:

```
53([2-4]),A
531(4),B
```

For incoming calls with prefix number "53124", rule with tag B is used.

- Example 5:

```
532[1-9],A
532[2-4],B
```

For incoming calls with prefix number "5324", rule with tag B is used.
Note: See the constraint in Section 2.33.1.

- Example 6:

```
53([2-4]),A
53(4),B
```

For incoming calls with prefix number "53124", rule with tag B is used.
Note: See the constraint in Section 2.33.1.

- Example 7:

```
321xxx,A
321,B
```

For incoming calls with prefix number "321444", rule with tag A is used. For incoming calls with prefix number "32144", rule with tag B is used.

To support the feature, the following new parameters were added:

Dial Plan Table `configure voip > sbc dial-plan` [DialPlans]	Defines Dial Plan names. [DialPlans] FORMAT DialPlans_Index = DialPlans_Name [\DialPlans] Where, ▪ DialPlans_Index = Index of Dial Plan. ▪ DialPlans_Name= Defines a name for the Dial Plan.
Dial Plan Rules Table `configure voip > sbc dial-plan-rule` [DialPlanRule]	The table is a "child" of the Dial Plan table and defines the actual dial plan rules pertaining to a Dial Plan. [DialPlanRule] FORMAT DialPlanRule_Index =DialPlanRule_DialPlanIndex,DialPlanRule_RuleIndex,DialPlanRule_Name, DialPlanRule_Prefix,DialPlanRule_Tag DialPlanRule 1 = "DialPlan1",0,"972","A" DialPlanRule 2 = "DialPlan1",1,"9728","B" DialPlanRule 3 = "DialPlan2",0,"973","A" DialPlanRule 4 = "DialPlan2",1,"9738","B" DialPlanRule 5 = "DialPlan1",3,"974","A" DialPlanRule 6 = "DialPlan1",4,"9748","B" DialPlanRule 7 = "DialPlan1",5,"975","C" DialPlanRule 8 = "DialPlan1",6,"9758(78)","D" DialPlanRule 9 = "DialPlan1",7,"977[66-68,99]","E" DialPlanRule 10 = "DialPlan1",8,"*","F" DialPlanRule 11 = "DialPlan1",9,"+322476[3000-3999]","G" DialPlanRule 12 = "DialPlan1",10,"+321xx","H" DialPlanRule 13 = "DialPlan1",11,"+321","I" [\DialPlanRule] Where,

	▪ DialPlanRule_Index = Index of the Dial Plan. ▪ DialPlanIndex= Index of dial plan rule. ▪ Name = Name of rule ▪ Prefix = Defines a prefix (based on syntax rules). ▪ Tag = Defines a prefix tag (up to 20 characters, except * asterisk symbol). For example: DialPlanRule 1 = "DialPlan1",0,"972","Local" DialPlanRule 2 = "DialPlan1",1,"9728","International" DialPlanRule 3 = "DialPlan2",0,"973","Local" DialPlanRule 4 = "DialPlan2",1,"9738","International" DialPlanRule 8 = "DialPlan1",2,"9758(78)","International" DialPlanRule 9 = "DialPlan1",3,"977[66-68,99]","Local" DialPlanRule 10 = "DialPlan1",4,"*","International" DialPlanRule 11 = "DialPlan1",5,"+322476[3000-3999]","Local" DialPlanRule 12 = "DialPlan1",6,"+321xx","International" DialPlanRule 13 = "DialPlan1",7,"+321","International"
debug dial-plan match-number	Searches the dial plans for specified digits and returns the corresponding tag prefix.
sbc dial-plan-rule import-csv-from all <URL path to CSV file>	Imports dial plan rules from a Dial Plan file. The rules of the Dial Plans in the CSV file replace all the existing rules of the corresponding Dial Plans on the device. For Dial Plans on the device that are not listed in the CSV file, the device deletes all of their rules. For example, if the CSV file contains one Dial Plan and the device is currently configured with two Dial Plans, the rules of the Dial Plan in the CSV file replace the rules of the corresponding Dial Plan on the device, and the rules of the remaining Dial Plan on the device are deleted (the Dial Plan itself remains). Syntax example: sbc dial-plan-rule import-csv-from all http://10.8.8.20/upload/All_Dial_Plans.csv Note: The Dial Plan names in the CSV file must be identical to the existing Dial Plan names on the device; otherwise, the specific Dial Plan is not imported.
sbc dial-plan-rule import-csv-from <dial plan name or index> <URL path to CSV file>	Imports rules for a specific Dial Plan. The rules of the Dial Plan in the CSV file replace all the existing rules of the corresponding Dial Plan on the device. Syntax example: sbc dial-plan-rule import-csv-from 0 http://10.8.8.20/upload/Dial_Plan_1_Rules.csv Note: The identical Dial Plan name (or index) must exist on the device; otherwise, the Dial Plan is not imported.
sbc dial-plan-rule export-csv-to all <URL path to CSV file>	Exports all existing dial plans to a Dial Plan file. sbc dial-plan-rule export-csv-to all http://10.8.8.20/upload/All_Dial_Plans.csv
sbc dial-plan-rule export-csv-to <dial plan name or index> <URL path to CSV file>	Exports a specific dial plan (by name or index) to a Dial Plan file. sbc dial-plan-rule export-csv-to 0 http://10.8.8.20/upload/index_0_Dial_Plans.csv
IP Group table – new parameter	[IPGroup_SBCDialPlanName] sbc-dial-plan-name = Associates a Dial Plan, configured in the Dial Plan table, with the IP Group. Note: If a Dial Plan is associated with both an IP Group and SRD, the IP Group takes precedence.

SRD table – new parameter	[SRD_SBCDialPlanName] sbc-dial-plan-name = Associates a Dial Plan, configured in the Dial Plan table, with the SRD. Note: If a Dial Plan is associated with both an IP Group and SRD, the IP Group takes precedence.
SBC IP-to-IP Routing table – new parameters	[IP2IPRouting_SrcTags] src-tags = Defines the prefix tag (string of up to 20 characters) to denote the source URI username. [IP2IPRouting_DestTags] dest-tags = Defines the prefix tag (string of up to 20 characters) to denote the destination URI username.
IP to IP Outbound Manipulation table – new parameters	[IPOutboundManipulation_SrcTags] src-tags = Defines the prefix tag (string of up to 20 characters) to denote the source URI username. [IPOutboundManipulation_DestTags] dest-tags = Defines the prefix tag (string of up to 20 characters) to denote the destination URI username.

Applicable Products: Mediant 3000.

2.34.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

1. Incorrect error message (HAProcessNode) is generated in Syslog messages during High-Availability (HA) switchover from active to redundant unit.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000/TP-8410.

2. The device crashes and then resets when a Dial Plan index is configured for a Tel Profile and the destination number is not defined in the Dial Plan file for that index.

   The constraint has now been resolved.

   SR: 765891

   Applicable Products: Mediant 3000.

3. When implementing automatic provisioning (update), the device fails to resolve the FQDN, defined by the IniFileUrl parameter, of the TFTP server and as a result, the new (updated) configuration file is not downloaded to the device. A workaround is to define the TFTP server with an IP address instead of an FQDN, which requires DNS resolution.

   The constraint has now been resolved.

   SR: 765311

   Applicable Products: Mediant 3000.

4. In some scenarios, after an HA switchover from active to redundant unit, the device stops sending debug recording packets to the configured destination IP address. A workaround is to configure the destination IP address manually or configure debug recording packets to be saved to the device's memory.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000/TP-8410.

5. When the device is upgraded from Version 6.6 to Version 6.8, the certificates currently loaded on the device become corrupted (truncated). As a result, the device is unable to establish secure connections (e.g., TLS or HTTPS). A workaround is to re-load the original certificates to the device.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

6. The device truncates long SDP bodies in Syslog messages when Syslog optimization (merging multiple debug messages into a single UDP packet) is enabled, making it difficult for administrator's to diagnose media negotiation.

   The constraint has now been resolved.

   SR: 750581

   Applicable Products: Mediant 3000.

2.35 Version GA

This section describes new features, known constraints and resolved constraints for the GA version.

2.35.1 New Features

New features introduced in this GA version include the following:

2.35.1.1 VoIP Networking Features

This section describes the new VoIP (SIP) networking features.

2.35.1.1.1 General

2.35.1.1.1.1 Enhanced SRD Functionality

This feature provides support for configuring multiple SIP Interfaces per SRD of the same application type.

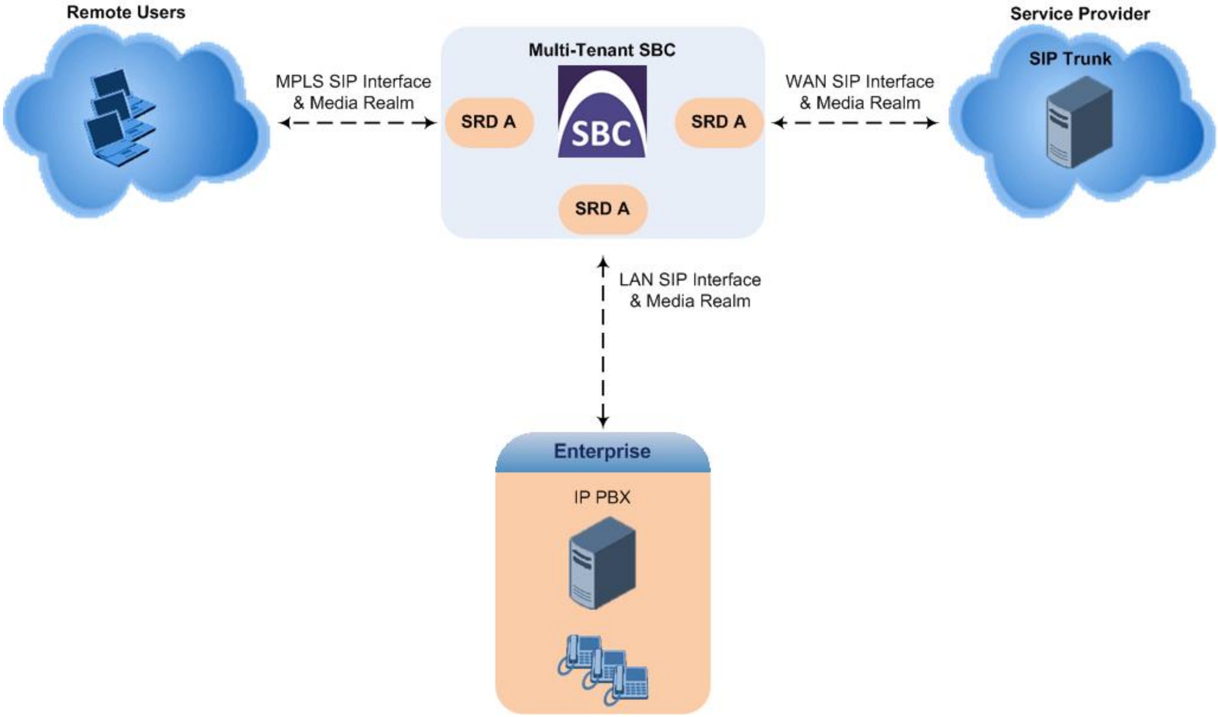
Up until this release, each SRD could only be associated with a single SIP Interface per application type (SBC or Gateway). Since IP Groups and Proxy Sets are also associated with SRDs, they are thus also bounded to this specific Layer-3 network. Therefore, when deploying the device in a multiple Layer-3 network environment, each network had to be configured with its own SRD in order to create a SIP Interface for each network. For example, an environment comprising three networks–IP PBX (LAN), SIP Trunk (WAN), and far-end users (WAN)–would require the configuration of three different SRDs in order to create the three different SIP Interfaces. This in turn, would require configuration of IP Groups per network, call admission control (CAC) rules per network, as well as complex routing rules for routing between these networks.

In Release 7.0, each SRD can now be configured with multiple SIP Interfaces per application type. As a result, only a single SRD is required for most deployments. Each Layer-3 network can still have its own SIP Interface while remaining under the same single SRD. Each SRD can be associated with multiple SIP Interfaces, Proxy Sets, and IP Groups, but each SIP Interface, Proxy Set, and IP Group can be associated with only one SRD. Each SRD is now assigned to Classification rules, which are used for all SIP traffic that enters the device from the SIP Interfaces associated with the specific SRD.

Single SRD topology is the **recommended** configuration setup. In fact, as the device is shipped with a single pre-configured default SRD ("DefaultSRD" at index 0) the administrator does not need to create an SRD. When other related configuration entities are created such as SIP Interfaces, IP Groups, Proxy Sets, Classification rules, and IP-to-IP Routing rules, they are automatically associated with the default SRD. Therefore, as only one SRD is required and association with other configuration entities is automatic, configuration is much easier and more flexible - fewer IP Groups need to be configured and CAC rules can be applied more effectively to the entire network.

As the SRD can now represent the entire network, it is mandatory to associate an SRD with related configuration entities (SIP Interfaces, IP Groups, Proxy Sets, Classification rules, and IP-to-IP Routing rules). However, as mentioned previously, when employing only the single, default SRD, newly created configuration entities are automatically associated with the default SRD.

The following figure shows a deployment comprised of multiple Layer-3 networks where only the single, default SRD is employed and where each network has a dedicated SIP Interface:



Notes:

- It is highly recommended to operate with a single SRD, unless you are deploying the device in a multi-tenant environment, in which case, multiple SRDs are required (for more information, see Section 2.35.1.1.2 on page 70).
- When the device is upgraded from an earlier release to Version 7.0, the previous SRD configuration is fully preserved regarding functionality. The same number of SRDs is maintained, but the configuration elements are changed to reflect the new configuration topology of Version 7.0. Below are the main changes in configuration topology when upgrading to Version 7.0:
  - √ The SIP Interface replaces the associated SRD in several tables (due to support for multiple SIP Interfaces per SRD).
  - √ Some fields in the SRD table were duplicated or moved to the SIP Interface table (see list after this note below).
  - √ Indices used for associating configuration entities in tables are changed to row pointers (using the entity's name).
  - √ Some tables are now associated (mandatory) with an SRD (SIP Interface, IP Group, Proxy Set, and Classification).
  - √ The new SBC Routing Policy table is added and some tables are associated (mandatory) with a Routing Policy (IP-to-IP Routing, Inbound Manipulation, and Outbound Manipulation).
  - √ Some fields used for associating configuration entities in tables now have a value of “Any” to distinguish between “Any” and "None" (deleted entity – not associated).
- If the device is not operating in a multi-tenant environment and multiple SRDs were used in an earlier release, it is highly recommended to gradually change the configuration to a single SRD due to its many benefits.
- The following constraints exist when upgrading from 6.8 to 7.0:
  - √ CLI Script file of 6.8 cannot be loaded to a 7.0 device.
  - √ Incremental ini file of 6.8 cannot be loaded to a 7.0 device.

To support the new SRD feature, configuration tables were changed as follows:

- SIP Interfaces can now be assigned to the following tables:
  - Admission Control table
  - Proxy Set table
  - Classification table
  - IP-to-IP Routing table
  - Inbound IP Routing table
  - Tel to IP Routing table
- The following can now be configured per SIP Interface (previously done per SRD):
  - Media Realm
  - Direct media
  - Maximum registered users
  - Allow or deny incoming calls (INVITE requests) from unregistered users
  - Allow or deny incoming REGISTER requests from new users

SIP Interface Table [SIPInterface]	The following parameters have been moved or duplicated from the SRD table to the SIP Interface table: ▪ SIPInterface_MediaRealm ▪ SIPInterface_IntraSRDMediaAnchoring (now renamed SIPInterface_SBCDirectMedia) ▪ SIPInterface_BlockUnRegUsers ▪ SIPInterface_MaxNumOfRegUsers ▪ SIPInterface_EnableUnAuthenticatedRegistrations.
Proxy Set [ProxySet]	New parameters: ▪ ProxySet_GWIPv4SIPInterfaceName = Assigns an IPv4 SIP Interface for Gateway calls. ▪ ProxySet_SBCIPv4SIPInterfaceName = Assigns an IPv4 SIP Interface for SBC calls. ▪ ProxySet_SASIPv4SIPInterfaceName = Assigns an IPv4 SIP Interface for SAS calls. ▪ ProxySet_GWIPv6SIPInterfaceName = Assigns an IPv6 SIP Interface for Gateway calls. ▪ ProxySet_SBCIPv6SIPInterfaceName = Assigns an IPv6 SIP Interface for SBC calls. ▪ ProxySet_SASIPv6SIPInterfaceName = Assigns an IPv6 SIP Interface for SAS calls. ▪ ProxySet_ProxyName = Defines an arbitrary name to identify the Proxy Set.
Classification Table [Classification]	New parameter: ▪ [Classification_SrcSIPInterfaceName] Source SIP Interface = SIP Interface on which the incoming call is received and used as a matching characteristics (input) to classify the call to an IP Group. This was added as an SRD can have multiple SIP Interfaces. Note: SrcSIPInterfaceName (if configured) must belong to the SRD set in the SRDName field.
IP-to-IP Routing Table [IP2IPRouting]	New parameter: ▪ [IP2IPRouting_DestSIPInterfaceName] Destination SIP Interface = Defines a destination SIP Interface to route the call to. The parameter replaces the Destination SRD parameter from the previous release, as now each SRD can have multiple SIP Interfaces.

Admission Control Table [SBCAdmissionControl]	New parameter: ▪ [SBCAdmissionControl_SIPInterfaceName] SIP Interface = Associates the CAC rule with a specific SIP Interface. Note: If an SRD is configured in the table, the configured SIP Interface and IP Group must belong to the SRD.
Tel to IP Routing Table [PREFIX]	New parameter: ▪ [PREFIX_DestSIPInterfaceName] SIP Interface = Associates the routing rule with a specific SIP Interface to where the call must be routed. This parameter replaces the Destination SRD parameter [PREFIX_DestSRD].
Inbound IP Routing Table [PstnPrefix]	New parameter: ▪ [PstnPrefix_SrcSIPInterfaceName] Source SIP Interface = Associates the routing rule with a SIP Interface from where the IP call was received. This is used as matching characteristics for the rule. This parameter replaces the Source SRD parameter [PstnPrefix_SrcSRDID].

Applicable Products: Mediant 3000.

2.35.1.1.1.2 SRD Cloning

This feature provides support for cloning (duplicating) an existing SRD. This is especially useful when operating in a multitenant environment and new tenants (SRDs) need to be added. The new tenants can quickly and easily be created by simply cloning one of the existing SRDs. Once cloned, all that the administrator needs to do is tweak the configuration associated with the new SRD. (For more information on the multitenant feature, see Section 2.35.1.1.2.1 on page 70.)

When an SRD is cloned, the device adds the new SRD clone to the next available index row in the SRD table. The SRD clone is assigned a unique name in the following syntax format: *<unique ID>_<index of original SRD>_CopyOf_<name or index if no name of original SRD>*. For example, if SRD at index 2 is cloned, the SRD clone is assigned the name, "36454371_2_CopyOf_SRD_2".

The SRD clone has identical settings as the original SRD. In addition, all configuration entities associated with the original SRD are also cloned and these clones are associated with the SRD clone. The naming convention of these entities is the same as for SRD clones (see above). These configuration entities include IP Groups, SIP Interfaces, Proxy Sets (without addresses), Classification rules, and Admission Control rules. If the Routing Policy associated with the original SRD is not associated with any other SRD, the Routing Policy is also cloned and its clone is associated with the SRD clone. All configuration entities associated with the original Routing Policy are also cloned and these clones are associated with the Routing Policy clone. These configuration entities include IP-to-IP Routing rules, Inbound Manipulation rules, and Outbound Manipulation rules.

When any configuration entity is cloned (e.g., an IP-to-IP Routing rule) as a result of a cloned SRD, all fields of the entity's row which "point" to other entities (e.g., SIP Interface, Source IP Group, and Destination IP Group) are replaced by their corresponding clones.

Note that for some cloned entities such as SIP Interfaces, some parameter values may change. This occurs in order to avoid the same parameter having the same value in more than one table row, which would result in invalid configuration. For example, a SIP Interface clone will have an empty Network Interface setting. After the clone process finishes, the administrator must update the Network Interface for valid configuration.

To support this feature the following new configuration elements have been added:

- Web interface: a new button labeled "Clone" has been added to the SRD table. To clone an SRD, the administrator needs to select the SRD to clone, and then click the button.
- CLI:

```
(config-voip)# voip-network srd clone <SRD index>
```

Applicable Products: Mediant 3000.

2.35.1.1.1.3 Network Physical Separation Enhancement for Mediant 3000/TP-8410

This feature provides support for enhanced physical separation configuration of network interfaces (OAMP, Media and Control) for Mediant 3000 housing the TP-8410 blade. Up until this release, physical network separation applied to all interface types, where each interface was allocated a dedicated port (Media on the GE port of the RTM, Control on port labelled **1** of the PEM, and OAMP on port labelled **2** of the PEM). The new feature provides the administrator with another optional physical network separation configuration which allocates the Control and Media interfaces to the same port:

- Control and Media on the GE port of the RTM
- OAMP on port labelled **2** of the PEM

To support the feature, the following new parameter has been added (located on the Interface Table Web page):

Physical Separation Configuration [PhysicalSeparationConfiguration]	Defines the physical network separation method. ▪ [0] 3 Interfaces: M + C+ OAMP = (Default) Each interface is allocated a dedicated port. ▪ [1] 3 Interfaces: M&C + OAMP = Media and Control are allocated to the same port (GE port of RTM) and OAMP allocated to a dedicated port (Port 2 of PEM). In the Interface table, make sure that you have configured an interface for OAMP only ('Application Type' field set to **OAMP**) and configured all other interfaces for Media and Control combined ('Application Type' field set to **Media + Control**). Notes: ▪ A device reset is required for the parameter to take effect. ▪ To enable the Physical Network Separation feature, use the existing EnableNetworkPhysicalSeparation parameter.

Applicable Products: Mediant 3000/TP-8410.

2.35.1.1.2 SBC

2.35.1.1.2.1 Enhanced Multi-Tenant Support

This feature provides enhanced support for multi-tenancy functionality. The device can be deployed in environments requiring multi-tenancy, simultaneously supporting and securing the IP communications requirements of multiple tenants (or enterprises), all managed by a single administrator through any of AudioCodes' management platforms. While some enterprises are large enough to justify a dedicated standalone SBC device, many enterprises require only a fraction of the device's capacity and capabilities. Therefore, customers such as service providers offering SIP Trunking services that can funnel multiple enterprises into a single device can reap significant cost improvements over a device-per-customer model.

Multi-tenancy refers to an architecture where an application running on a server or designated hardware, serves multiple clients (tenants). In other words, a single system – the SBC device - serves a large number of enterprises. In a multi-tenancy environment, a user from one tenant can't infringe on another tenant's space served by the same application.

The device's multi-tenancy feature is fully scalable, offering "non-bleeding" partition per tenant running on a single shared physical entity. It provides per tenant configuration, monitoring, reporting, analytics, alarms and interfacing. The device is a real-time multi-tenant system that provides each tenant with optimal real-time performance, as each session received by the device is classified and processed only through the tenant's "orbit".

Tenant size in a multi-tenant architecture can vary and therefore, the instance CPU, memory and interface allocations should be optimized so as to not waste resources for small-sized tenants on the one hand and not to allocate too many instances for a single tenant/customer on the other. For example, it would be a waste to allocate a capacity of 1,000 concurrent sessions to a small tenant for which 10 concurrent sessions suffice. In a multi-tenancy setup, call admission control (CAC) can be effectively allocated per tenant.

The enhanced support for multi-tenancy facilitates configuration due to the enhanced functionality of SRDs, where each SRD can now be configured with multiple SIP Interfaces belonging to the same application type (i.e., SBC). For more information on the new SRD functionality, see Section 2.35.1.1.1 on page 66. As multiple SIP Interfaces can now be configured per SRD, different Layer-3 networks (e.g., LAN IP-PBX users, SIP Trunk in the WAN, and far-end users) belonging to the same tenant can be configured under a single SRD. Therefore, each tenant can now be represented by its own dedicated SRD. As configuration entities now need to be associated with an SRD (SIP Interfaces, IP Groups, Proxy Sets, Classification rules, and IP-to-IP Routing rules), each SRD has its own virtual separate configuration "tables" (although configured in the same tables). This provides full logical separation (on the SIP application layer) of tenants by SRDs.

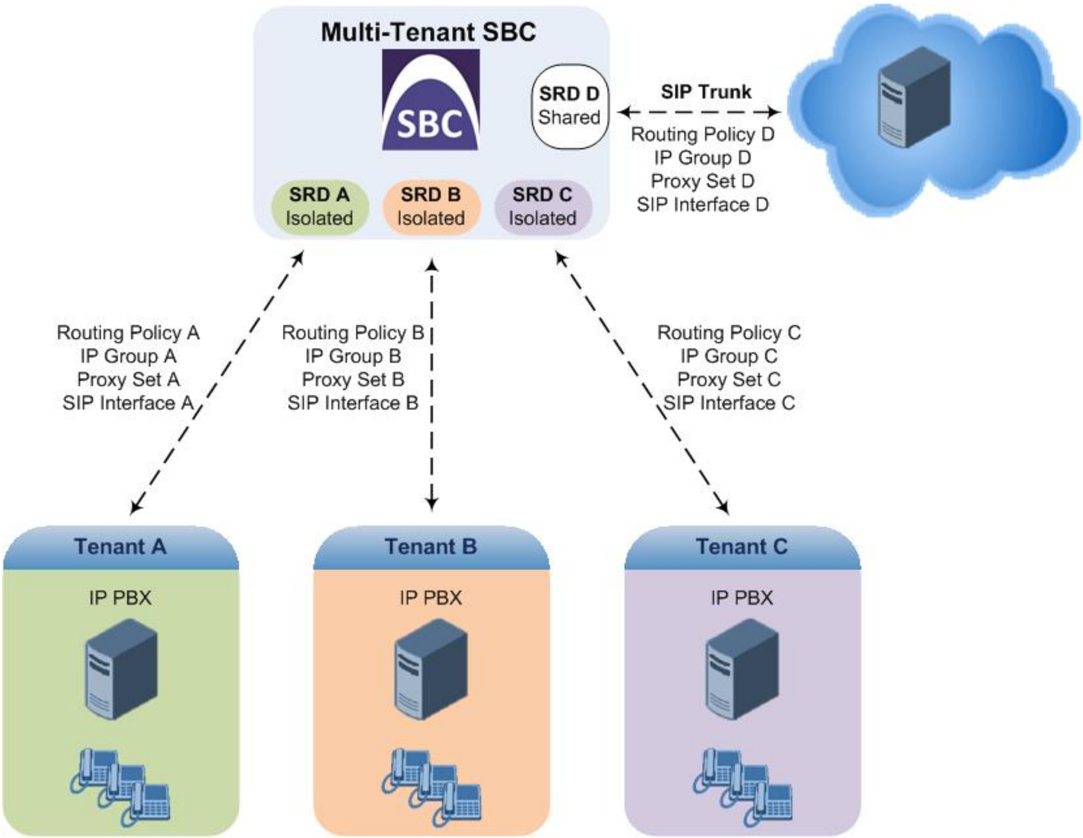
Another main configuration entity introduced in Release 7.0 that can be used with multi-tenancy is the *Routing Policy*. Routing Policies allow each SRD (or tenant) to have its own routing rules, manipulation rules, Least Cost Routing (LCR) rules, and/or LDAP-based routing configuration. However, not all multi-tenant deployments need multiple Routing Policies (and their configuration is not required). For more information on the Routing Policy entity, see Section 2.35.1.3.2.1 on page 81.

To help the administrator create a SIP configuration topology that is as non-bleeding as possible, SRDs can now be configured as *shared* or *isolated*:

- Isolated SRD: An Isolated SRD (or tenant) is an SRD having its own dedicated SIP resources – SIP Interfaces, Proxy Sets, and IP Groups. No other SRD can use these SIP resources. For example, no SRD can use the Proxy Set associated with an Isolated SRD. Isolated SRDs ensure traffic flow of tenants is kept separate, preventing any risk of "leaking" of traffic from one tenant to another.

  Isolated SRDs are more relevant when each tenant needs its own separate (dedicated) routing "table" for non-bleeding topology. Separated routing tables are implemented using the new configuration entity Routing Policy, as described in Section 2.35.1.3.2.1 on page 81. In such a non-bleeding topology, routing between Isolated tenants is not possible. This enables accurate and precise routing per tenant, eliminating any possibility of erroneous call routing between tenants, restricting routing to each tenant's sphere. Configuring one Routing policy shared between Isolated tenants is not best practice for non-bleeding environments since it allows routing between these tenants.

- Shared SRD: Isolated SRDs require that each tenant have its' own dedicated SIP resources (SIP Interfaces, Proxy Sets, and IP Groups). This may not be possible in some deployments. For example, when working with a common SIP trunk, or where SIP interface resources are limited (e.g., multiple IP addresses cannot be allocated and SIP port 5060 must be used). A tenant may share its' SIP resources with other tenants (Shared or Isolated tenants). This is typically required when tenants need to use common resources such as mentioned above. For example, when all tenants need to work with the same SIP trunk or use the same SIP Interface. In this scenario, one Shared SRD would be configured and all resources that need to be shared with all tenants are associated with the Shared SRD. In the SIP trunk scenario, the SIP trunk will be associated with the Shared SRD tenant, enabling all tenants to route calls with the IP Group that represents the SIP Trunk. The figure below illustrates a multi-tenant architecture with Isolated SRD tenants—A, B and C—and a Shared SRD tenant D serving as a SIP trunk:



To facilitate configuration of multi-tenancy through the CLI, the administrator can access a specific tenant "view". Once in a specific tenant view, all configuration commands apply only to the currently viewed tenant. Only table rows (indexes) belonging to the viewed tenant can be modified. New table rows are automatically associated with the viewed tenant (i.e., SRD name). The `display` of tables and `show running-configuration` commands display only rows relevant to the viewed tenant (and shared tenants). The `show` commands display only information relevant for the viewed tenant. To support this CLI functionality, the following new commands have been added:

- Accesses a specific tenant view:

  ```
  # srd-view <SRD name>
  ```

  Once accessed, the tenant's name (SRD name) forms part of the CLI prompt, for example:

  ```
  # srd-view itsp
  (srd-itsp)#
  ```

- Exits the tenant view:

  ```
  # no srd-view
  ```

Applicable Products: Mediant 3000.

2.35.1.2 SIP Interoperability Features

This section describes the new SIP interoperability features.

2.35.1.2.1General

This section describes the new general interoperability features.

2.35.1.2.1.1 SIP Message Manipulation based on NAT

This feature provides support for manipulating a SIP message depending on whether or not the source or destination of the message is located behind NAT. The support is provided by the existing Message Manipulations table and the new message manipulation syntax keywords *param.call.src.nat* and *param.call.dst.nat*, which are used to indicate whether the source or destination message is (=='true') or is not (=='false') behind NAT. The keywords can be used in the 'Condition' or 'Action Value' parameters in the Message Manipulations table. Message Manipulation rules using the new keywords are applicable only to message manipulation on the outbound leg (i.e., the rules can only be assigned to the 'Outbound Message Manipulation Set' parameter in the IP Group table).

The example below shows a Message Manipulation rule using the *param.call.dst.nat* keyword. If the device determines that the destination of the INVITE message is located behind NAT (*param.call.dst.nat=='true'*), and the RTP mode in the SDP of the incoming INVITE is 'sendonly' (*param.message.sdp.rtpmode=='sendonly'*), it changes the RTP mode to 'sendrecv' in the SDP of the outgoing INVITE.

Message Type	Condition	Action Subject	Action Type	Action Value
INVITE	param.message.sdp.rtpmode=='sendonly' and **param.call.dst.nat=='true'**	param.message.sdp.rtpmode	Modify	'sendrecv'

Applicable Products: Mediant 3000.

2.35.1.2.1.2 Session Variables for Message Manipulations

This feature provides support for copying data between SIP messages for Message Manipulation. The stored data is can be used anytime during the entire call session (for example, call forking). This is done using the session variable `var.session.0`.

Applicable Products: Mediant 3000.

2.35.1.2.1.3 DNS Queries for Microsoft Lync

This feature provides support for performing DNS queries with a DNS server when deployed in a Microsoft Lync environment. As required by Microsoft, the device sends special SRV queries according to transport type (see description of the new option below) in order to resolve the domain name into an IP address.

To support the feature, the following option was added to the existing DNS Resolve Method parameter in the Proxy Sets table:

DNS Resolve Method dns-resolve-method [ProxySet_DNSResolveMethod]	New optional value: ▪ [3] MS-Lync = SRV query as required by Microsoft when the <device> is deployed in a Microsoft Lync environment. The device sends a special SRV query to the DNS server according to the transport protocol configured in the 'Transport Type' parameter: ▪ TLS: "_sipinternaltls_tcp.<domain>" and "_sip_tls.<domain>". For example, if the configured domain name (in the 'Proxy Address' parameter) is "ms-server.com", the <device> queries for "_sipinternaltls_tcp.ms-server.com" and "_sip_tls.ms-server.com". ▪ TCP: "_sipinternal._tcp.<domain>" and "_sip_tcp.<domain>". ▪ Undefined: "_sipinternaltls_tcp.<domain>", "_sipinternal_tcp.<domain>", "_sip_tls.<domain>" and "_sip_tcp.<domain>". The SRV query returns the host names (and their weights). The <device> then performs DNS A-record queries per host name (according to the received weights) to resolve into IP addresses.

Applicable Products: Mediant 3000.

2.35.1.2.2 LDAP Query for Numbers in AD with Characters between Digits

This feature provides support for the device to perform an LDAP query on an LDAP Attribute in Active Directory (AD) for a specific telephone number, even if the number is defined in AD with characters (such as spaces, hyphens and periods) separating the digits. For example, the telephoneNumber Attribute could be defined in AD with the telephone number "503-823-4567" (i.e., hyphens), "503.823.4567" (i.e., periods) or "503 823 4567" (i.e., spaces). Up until this release, if the device was configured to query an Attribute value (e.g., 5038234567) that was defined in AD with characters separating the digits, the LDAP query would return a failed result, as the AD server considers these characters when searching LDAP records.

The feature enables the administrator to query such numbers in the AD. To search for the number with characters, the <device> inserts the asterisk (*) wildcard between all digits in the LDAP query (e.g., telephoneNumber = 5*0*3*8*2*3*4*5*6*7). As the AD server recognizes the * wildcard as representing any character, it returns all possible results to the <device>. Note that the wildcard represents only a character; a query result containing a digit in place of a wildcard is discarded and the device performs another query for the same Attribute. To enable the <device> to search the AD for numbers that may contain characters between its digits, you need to specify the Attribute (up to five) for which you want to apply this functionality, using the new LDAPNumericAttributes parameter.

For example, the telephoneNumber Attribute could be defined in AD with the telephone number "503-823-4567" (i.e., hyphens), "503.823.4567" (i.e., periods) or "503 823 4567" (i.e., spaces). If the <device> performs an LDAP search on this Attribute for the number 5038234567, the LDAP query returns results only if the telephoneNumber Attribute is configured for the LDAPNumericAttributes parameter.

For example, if the device needs to query the telephone number 036474, it sends a query for telephoneNumber = 0*3*6*4*7*4. The AD server returns all results based on this configuration. For example, it may return the numbers 09-36 474 ("9", "-" and space between "6" and "4" is due to the wildcard) and 03-64 74. As the device discards query results where the wildcard results in a digit, it selects 03-64 74 as the result. The correct query result is cached by the device for subsequent queries and/or in case of LDAP server failure.

The feature is supported by both Gateway and SBC applications and for whatever LDAP feature is employed.

To support the feature, the following new parameter was added:

LDAP Numeric Attribute configure voip > sip-definition advanced-settings > ldap-numeric-attr [LDAPNumericAttributes]	Defines up to five LDAP Attributes (separated by commas) for which the device employs LDAP query searches using the asterisk wildcard to represent possible characters between digits. For example, if the parameter is configured to 5038234567, the device will search for the number 5*0*3*8*2*3*4*5*6*7, where the wildcard can be any character. Note: The wildcard is only used between digits.

Applicable Products: Mediant 3000.

2.35.1.2.3 SBC

This section describes the new SBC interoperability features.

2.35.1.2.3.1 Stateful SIP Proxy Mode

This feature provides support for the SBC device to operate as a stateful proxy server. This capability enables the device to forward SIP messages transparently (unchanged) between SIP endpoints.

Up until this release, the device operated only as a classic back-to-back user agent (B2BUA). By default, the device's B2BUA mode changes the SIP dialog identifiers and topology data in SIP messages:

- Call identifiers: Replaces the From tag and Call-ID header so that they are different for each leg. (Note that the To header's tag remains the same on both legs of the dialog.)

- Routing headers:
  - Removes all incoming Via headers in incoming requests and sends it with its own Via header.
  - Doesn't forward any Record-Route headers from the incoming side to the outgoing side and vice versa.
  - Replaces the address of the Contact header in the incoming message with its own address.
- Replaces the value in the User-Agent/ Server header in the outgoing message, and replaces the original value with itself in the incoming message.

In contrast, when the device operates in the stateful proxy mode, it (by default) retains the incoming dialog identifiers and topology headers in the outgoing message. The device handles each of the above listed headers transparently (i.e., they remain unchanged) or according to configuration (enabling partial transparency), and only adds itself as the top-most Via header and optionally, to the Record-Route list. For configuring the handling of these headers, see the following sections:

- Interworking SIP Contact and Record-Route Headers in In-Dialog Requests on page 77
- Interworking SIP Via Headers on page 77
- Interworking SIP User-Agent Headers on page 78
- Interworking SIP Record-Route Headers on page 78
- Handling SIP To-Header tags in Call Forking Responses on page 79

Therefore, the stateful proxy mode provides full SIP transparency (no topology hiding) or asymmetric topology hiding (using IP Groups).

Below is an example of a SIP dialog-initiating request when operating in stateful proxy mode. As shown, all the incoming SIP headers are retained in the outgoing INVITE message.

Incoming INVITE

```
INVITE sip:bob@domain.com SIP/2.0
To: Bob <sip:bob@domain.com>
From: Alice
<sip:alice@caller.com>;tag=100
Call-ID: callid1@caller.com
Contact: <sip:alice@pc1.caller.com>
Via: SIP/2.0/UDP pc2.com;branch=brancn2
Via: SIP/2.0/UDP pc1.com;branch=brancn1
Record-Route: <pc2.com;lr>
Record-Route: <pc1.com;lr>
CSeq: 666 INVITE
User-Agent: IPPv3.1
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 142

v=0
...
```

Outgoing INVITE

```
INVITE sip:bob@domain.com SIP/2.0
To: Bob <sip:bob@domain.com>
From: Alice
<sip:alice@caller.com>;tag=100
Call-ID: callid1@caller.com
Contact: <sip:alice@pc1.caller.com>
Via: SIP/2.0/UDP Proxy-IP;branch=brancn3
Via: SIP/2.0/UDP pc2.com;branch=brancn2
Via: SIP/2.0/UDP pc1.com;branch=brancn1
Record-Route: <Proxy-IP;lr>
Record-Route: <pc2.com;lr>
Record-Route: <pc1.com;lr>
CSeq: 666 INVITE
User-Agent: IPPv3.1
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 142
v=0
...
```

Some of the reasons for implementing stateful proxy mode:

- B2BUA typically hides certain SIP headers for topology hiding. In specific setups, some SIP servers require the inclusion of these headers in order to know the history of the SIP request. In such setups, the requirement may be asymmetric topology hiding, whereby SIP traffic toward the SIP server must expose these headers whereas SIP traffic toward the users must not expose these headers.
- B2BUA changes the call identifiers between the SBC legs and therefore, call parties may indicate call identifiers that are not relayed to the other leg. Some SIP functionalities are achieved by conveying the SIP call identifiers either in SIP specific headers (e.g., Replaces) or in the message bodies (e.g. Dialog Info in an XML body).
- In some setups, the SIP client authenticates using a hash that is performed on one or

more of the headers that B2BUA changes (removes). Therefore, authentication will fail.

- For facilitating debugging procedures, some administrators require that the value in the Call-ID header remains unchanged between the two SBC legs. B2BUA changes this.

Notes:

- It is recommended to use the B2BUA mode unless one of the reasons mentioned above is required. B2BUA also supports all the device's feature-rich offerings, while Stateful Proxy may offer only limited support. These affected features include:
  - √ Alternative routing
  - √ Call forking
  - √ Terminating REFER/3xx

  If stateful proxy mode is used and any one of the unsupported features is enabled, the stateful proxy mode will fail and the device will operate in B2BUA mode.
- The device can be configured to operate in both B2BUA and Stateful Proxy modes for the same users. This is typically implemented when users need to communicate with different SIP entities (IP Groups). For example, B2BUA mode for calls destined to a SIP Trunk, and Stateful Proxy mode for calls destined to an IP PBX. The configuration is done using IP Groups and SRDs.
- If Stateful Proxy mode is used only due to the debugging benefits, it is recommended to configure the device to only forward the Call-ID header unchanged.

To support this feature, the following new parameters have been added:

(SRD Table) SBC Operation Mode CLI: configure voip/voip-network srd/sbc-operation-mode [SRD_SBCOperationMode]	Defines the device's operational mode regarding B2BUA or call stateful proxy, for calls pertaining to the specific SRD. The settings of this parameter also determine the default behavior of related parameters in the IP Profile (SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepUserAgentHeader, SBCKeepRoutingHeaders, SBCRemoteMultipleEarlyDialogs). ▪ [0] B2BUA = (Default) Device replaces the original call identifiers. ▪ [1] Call Stateful Proxy = Dialog identifiers (tags, Call-Id and CSeq) will be the same on both legs of the dialog (as long as no other configuration disrupts the CSeq compatibleness). ▪ [2] Microsoft Server = For One-Voice Resiliency feature.
(IP Group Table) SBC Operation Mode CLI: configure voip > voip-network ip-group > sbc-operation-mode [IPGroup_SBCOperationMode]	Defines the device's operational mode regarding B2BUA or call stateful proxy modes, for calls pertaining to the specific IP Group. ▪ [-1] Not Configured = (Default) ▪ [0] B2BUA ▪ [1] Call Stateful Proxy ▪ [2] Microsoft Server = For One-Voice Resiliency feature. If the Operation Mode for the SRD\IP Group of one leg of the dialog is configured to 'Call Stateful Proxy', the device also operates in this mode on the other leg, with regards to the dialog identifiers (Call-ID header, tags, CSeq header). In other words, the identifiers will be the same on both legs, regardless of the origin of the call. However, the handling of the two legs by the device may be different, depending on the settings of the related parameters in the IP Profile table. Notes: ▪ This parameter overrides the settings of the 'SBC Operation Mode' parameter in the SRD table.

	▪ The SIP To header's tag is the same on both legs of the dialog, regardless of the Operation Mode.

Applicable Products: Mediant 3000.

2.35.1.2.3.2 Interworking SIP Contact and Record-Route Headers in In-Dialog Requests

This feature provides support for interworking in-dialog, SIP requests (Contact and Record-Route headers) between SIP entities. Using an IP Profile for a SIP entity, the device can handle in-dialog, Contact and Record-Route headers for outgoing messages sent to the SIP entity, as follows:

- Replaces the address in the Contact header with its own address.
- Adds a Record-Route header for itself to outgoing messages (requests\responses) to the SIP entity in a dialog-setup transaction. (The Contact header remains unchanged.)
- Does not change the Contact header and does not add a Record-Route for itself. Instead, it relies on some other way (which isn't part of configuration) to remain in the route of future requests in the dialog.

To support this feature, the following new parameter has been added to the IP Profile table:

Remote Representation Mode CLI: configure voip > coders-and-profiles ip-profile > sbc-rmt-rprsntation [IpProfile_SBCRemoteRepresentationMode]	Defines the handling of in-dialog requests received from the SIP entity associated with this IP Profile. ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the Operation Mode in the IP Group or SRD table: ✓ B2BUA: Device operates as if this parameter is set to Replace Contact [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Add Routing Headers [1]. ▪ [0] Replace Contact = Device replaces the Contact in incoming messages with its own address, before sending the message to this SIP entity. ▪ [1] Add Routing Headers = Device doesn't change the Contact in incoming messages. Instead, it adds a Record-Route header with itself to outgoing messages (Requests\Responses) to this SIP entity in a dialog setup transaction. ▪ [2] Transparent = Device doesn't change the Contact header and doesn't add a Record-Route for itself. Instead, it relies on some other way (which isn't part of the configuration) to remain in the route of future requests in the dialog (for example, relying on the way the endpoints are set up or on TLS as the transport type).

Applicable Products: Mediant 3000.

2.35.1.2.3.3 Interworking SIP Via Headers

This feature provides support for interworking SIP Via headers between SIP entities. Using an IP Profile for a SIP entity, the device can handle Via headers for outgoing messages to the SIP entity, as follows:

- Removes all Via headers, received in the incoming message, and adds only itself in a Via header in the outgoing message to the SIP entity.
- Retains the Via headers, received in the incoming message, and adds itself as the top-most listed Via header in the outgoing message to the SIP entity.

To support this feature, the following new parameter has been added to the IP Profile table:

Keep Incoming VIA Headers CLI: configure voip > coders-and-profiles ip-profile > sbc-	Defines the handling of Via headers in messages sent to the SIP entity associated with this IP Profile.

keep-via-headers [IpProfile_SBCKeepVIAHeaders]	▪ [-1] According to Operation Mode = Depends on the setting of the Operation Mode in the IP Group or SRD table: ✓ B2BUA: Device operates as if this parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Enable [1]. ▪ [0] Disable = Device removes incoming Via headers in the request and adds only itself to the outgoing request sent to this SIP entity. ▪ [1] Enable = Device doesn't remove the incoming Via headers in a request before sending it to this SIP entity. It simply adds itself as the top Via.

Applicable Products: Mediant 3000.

2.35.1.2.3.4 Interworking SIP User-Agent Headers

This feature provides support for interworking SIP User-Agent headers between SIP entities. Using an IP Profile for a SIP entity, the device can handle User-Agent headers for outgoing messages to the SIP entity, as follows:

- Replaces the User-Agent/Server headers, received in the incoming message, with its' own User-Agent header in the outgoing message to the SIP entity.
- Retains the User-Agent/Server headers received in the incoming message (i.e., sends the User-Agent/Server headers as is in the outgoing message to the SIP entity).

To support this feature, the following new parameter has been added to the IP Profile table:

Keep User-Agent Header CLI: configure voip > coders-and-profiles ip-profile > sbc-keep-user-agent [IpProfile_SBCKeepUserAgentHeader]	Defines the handling of User-Agent headers in messages sent to the SIP entity associated with this IP Profile. ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the Operation Mode in the IP Group or SRD table: ✓ B2BUA: Device operates as if this parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Enable [1]. ▪ [0] Disable = Device replaces the existing User-Agent/Server headers with its own before sending the request/response to this SIP entity. ▪ [1] Enable = Device doesn't replace the User-Agent/ Server header in the request / response before sending it to this SIP entity.

Applicable Products: Mediant 3000.

2.35.1.2.3.5 Interworking SIP Record-Route Headers

This feature provides support for interworking SIP Record-Route headers between SIP entities. Using an IP Profile for a SIP entity, the device can handle Record-Route headers for outgoing messages to the SIP entity, as follows:

- Removes the Record-Route headers received in SIP requests and responses. It creates a route set for that side of the dialog based on these headers, but doesn't send them to the SIP entity.
- Retains the Record-Route headers received in requests and non-failure responses in the following scenarios:
    - The message is part of a dialog-setup transaction.
    - The messages in the setup and previous transaction didn't include the Record-Route header and therefore, hadn't set the route set.

  Record-Routes are kept only for INVITE, UPDATE, SUBSCRIBE and REFER messages.

To support this feature, the following new parameter has been added to the IP Profile table:

Keep Incoming Routing Headers CLI: configure voip > coders-and-profiles ip-profile > sbc-keep-routing-headers [IpProfile_SBCKeepRoutingHeaders]	Defines the handling of Record-Route headers in messages sent to the SIP entity associated with this IP Profile. ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the Operation Mode in the IP Group or SRD table: ✓ B2BUA: Device operates as if this parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Enable [1]. ▪ [0] Disable = Device removes incoming Record-Route headers in requests and responses, creates a Route Set for that side of the dialog based on these headers, but doesn't send them to the SIP entity. ▪ [1] Enable = Device retains the incoming Record-Route headers in requests and non-failure responses in the following scenarios: ✓ The message is part of a dialog-setup transaction. ✓ The messages in the setup and previous transaction didn't include Record-Route, and therefore hadn't set the route set. Record-Routes are kept only for INVITE, UPDATE, SUBSCRIBE and REFER messages.

Applicable Products: Mediant 3000.

2.35.1.2.3.6 Handling SIP To-Header tags in Call Forking Responses (Multiple SDP Answers)

This feature provides support for configuring how the device handles SIP To-header tags in call forking responses (i.e., multiple SDP answers) sent to a specific SIP entity. When the SIP entity initiates an INVITE that is forked (by a proxy server, for example) to multiple endpoints, the endpoints respond with a SIP 183 containing an SDP answer. Typically, each endpoint's response has a different To-header tag. Depending on the settings of the new IP Profile parameter, SBCRemoteMultipleEarlyDialogs, the device can handle the To-header tags for the SIP entity as follows:

- Sends the SDP answers with the same To-header tag value. In other words, this option is relevant for SIP entities that do not support multiple dialogs (and multiple tags). However, non-standard multiple answer support may still be configured using the new parameter, SBCRemoteMultipleAnswersMode (set to 1). In this case, non-standard behavior is implemented whereby the device sends multiple answers with the same To-header tag.
- Sends the SDP answers with different To-header tag values (belonging to the responses received from the forked INVITE). In other words, this option is relevant for SIP entities that support standard multiple SDP answers (with different To-header tags). In this case, the parameter, SBCRemoteMultipleAnswersMode is ignored.

When both parameters are disabled, multiple SDP answers are not reflected to the SIP entity (i.e., the same SDP answer is sent in multiple 18x and 200 responses).

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

Remote Multiple Early Dialogs CLI: configure voip > coders-and-profiles ip-profile > sbc-multi-early-diag [IpProfile_SBCRemoteMultipleEarlyDialogs]	Defines the handling of To tags in call forking responses sent to the SIP entity associated with this IP Profile. This applies to call forking. ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the Operation Mode in the IP Group or SRD table: ✓ B2BUA: Device operates as if this parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Enable [1].

	▪ [0] Disable = Device responds with the same To-tag value sent to this SIP entity. ▪ [1] Enable = Device may respond with different To-tag values sent to this SIP entity (pertaining to the responses received to the forked INVITE).
Remote Multiple Answers Mode CLI: sbc-multi-answers [IpProfile_SBCRemoteMultipleAnswersMode]	Enables the device to respond with multiple answers within the same dialog (non-standard). The parameter is applicable only when the IpProfile_SBCRemoteMultipleEarlyDialogs parameter is disabled. ▪ [0] Disable (Default) = Device always sends the same SDP answer, which is based on the first received answer that it sent, for all forked responses (even if the 'Forking Handling Mode' parameter is configured to Sequential), and thus, may result in transcoding. ▪ [1] Enable = If the 'Forking Handling Mode' parameter is configured to Sequential, the device sends multiple SDP answers.

Applicable Products: Mediant 3000.

2.35.1.3 SIP Routing Features

This section describes the new SIP routing features.

2.35.1.3.1General

This section describes the new general SIP routing features.

2.35.1.3.1.1 "Any" Option to Associate Rule with All Related Entities

This feature provides support for the addition of the "Any" optional value for parameters that associate one configuration entity with another. The "Any" option implies that the specific row index rule applies to all indices of the related configuration entity. For example, an IP-to-IP routing rule can be configured in the IP-to-IP Routing table with a matching rule criterion whereby the source IP Group (i.e., the IP Group from where the incoming call is received) can be any IP Group (listed in the IP Group table).

Up until this release, the asterisk (*) sign or "-1" value was used to indicate any (or all). However, the -1 value was also used to indicate a non-configured (empty) parameter. Instead of the "-1" value, the new "None" optional value is now used. Therefore, this feature now provides clearer and more user-friendly options to set the parameter to not configured ("None") or to any ("Any"). This is also useful if the associated configuration entity is deleted. In such cases, the value of the parameter "pointing" to the deleted entity is changed to "None". For many of these parameters, the "Any" option has also become the default value instead of the "-1" value.

The "Any" optional value has been added to the following parameters:

- SIP Recording table (default is "Any"):
  - Recorded IP Group [SIPRecRouting_RecordedIPGroupName]
  - Peer IP Group [SIPRecRouting_PeerIPGroupName]
- Gateway:
  - Inbound IP Routing table (default is "Any"):
    - Source SIP Interface [PstnPrefix_SrcSIPInterfaceName]
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls table (default is "Any"):
    - Source IP Group [NumberMapIp2Tel_SrcIpGroupName]
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls table (default is "Any"):
    - Destination IP Group [NumberMapTel2IP_DestIPGroupName]

- Source Phone Number Manipulation Table for IP-to-Tel Calls table (default is "Any"):
  - Source IP Group [SourceNumberMapIp2Tel_SrcIPGroupName]
- SBC:
  - IP to IP Routing table (default is "Any"):
    - Source IP Group [IP2IPRouting_SrcIPGroupName]
    - ReRoute IP Group [IP2IPRouting_ReRouteIPGroupName]
  - Classification table (default is "Any"):
    - Source SIP Interface [Classification_SrcSIPInterfaceName]
  - Admission Control table (default is "None"):
    - IP Group [SBCAdmissionControl_IPGroupName]
    - SRD [SBCAdmissionControl_SRDName]
    - SIP Interface [SBCAdmissionControl_SIPInterfaceName]
  - IP to IP Inbound Manipulation table (default is "Any"):
    - Source IP Group [IPInboundManipulation_SrcIPGroupName]
  - IP to IP Outbound Manipulation table (default for the following is "Any"):
    - Source IP Group [IPOutboundManipulation_SrcIPGroupName]
    - Destination IP Group [IPOutboundManipulation_DestIPGroupName]
    - ReRoute IP Group [IPOutboundManipulation_ReRouteIPGroupName]

Note: The "Any" and "None" values are case sensitive when configuring through the ini file.

Applicable Products: Mediant 3000.

2.35.1.3.2SBC

This section describes the new SBC routing features.

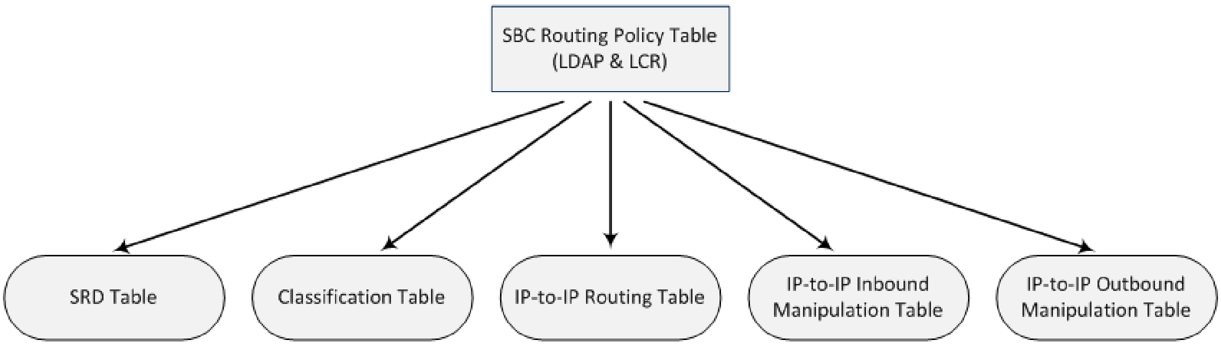
2.35.1.3.2.1 SBC Routing Policies

This feature provides support for a new SBC configuration entity, termed *Routing Policy*. The Routing Policy determines the routing and manipulation (inbound and outbound) rules per SRD. It can also be used to determine Least Cost Routing (LCR) rules and LDAP-based routing for the SRD. SBC IP-to-IP routing rules configured for LDAP or CSR (Call Setup Rules) queries will use the LDAP server(s) associated with the assigned Routing Policy. Multiple Routing Policies can be configured. Each SRD can be assigned its own Routing Policy or share a Routing Policy with other SRDs.

The Routing Policy is intended **only** for deployments requiring LCR and/or LDAP-based routing, or for multi-tenancy deployments requiring multiple routing "tables" whereby each tenant has its own dedicated ("separate") routing table (and manipulation). In such scenarios, each SRD (tenant) is assigned its own unique Routing Policy, implementing an isolated, non-bleeding routing configuration topology. In this multi-tenancy deployment, the tenants are also configured as Isolated SRDs (for an explanation on Isolated and Shared SRDs, see Section 2.35.1.1.2 on page 70). For all other deployment scenarios, the Routing Policy is not relevant and the handling of this configuration entity is not needed (as a default Routing Policy is provided, discussed later on in this section).

Note: Although the Routing Policy is intended for multi-tenancy deployments, if possible, it is advisable to use a **single** Routing Policy for all tenants, unless the deployment requires otherwise (i.e., a dedicated Routing Policy per SRD).

Routing Policies are configured in the new SBC Routing Policy table. Each Routing Policy is defined with a unique name and optionally, can be configured with LCR as well as associated with LDAP servers for LDAP-based routing (with Call Setup Rules). These features have been supported in previous releases. The Routing Policy table replaces the Routing Rule Groups table (RoutingRuleGroups), which was used to configure LCR in previous releases (and includes all the same LCR parameters). Once configured, the Routing Policy is assigned to an SRD(s). To determine the routing and manipulation rules for this SRD, the Routing Policy is also assigned to routing and manipulation rules. The figure below shows the configuration entities to which Routing Policies are assigned:



Note that a Routing Policy can be assigned to a Classification rule (as shown in the figure above). Typically, this configuration is not required as when an incoming call is classified, it uses the Routing Policy associated with the SRD to which it belongs. However, if a Routing Policy is assigned to a Classification rule in the Classification table, it overrides the Routing Policy assigned to the SRD in the SRD table. This feature is useful in deployments requiring different routing and manipulation rules for specific calls pertaining to the same SRD (or tenant in multi-tenancy environments). In such scenarios, multiple Classification rules need to be configured, where some rules do not specify a Routing Policy (and use the SRD's Routing Policy) while others specify a different Routing Policy to override the SRD's Routing Policy.

The device provides a pre-configured, default Routing Policy ("Default_SBCRoutingPolicy"). By default, LCR and LDAP are disabled for this Routing Policy. When only one Routing Policy is used in the deployment, the device automatically associates the default Routing Policy with all related configuration entities as mentioned above (SRDs, IP-to-IP routing rules, and IP-to-IP inbound and outbound manipulation rules). Each newly created SRD is automatically assigned the default Routing Policy. This facilitates configuration, eliminating the need for the administrator to deal with the Routing Policy configuration entity (except to enable LCR and/or LDAP for the Routing Policy, if required). In such a setup, where only one Routing Policy is used, single routing and manipulation tables are employed for all SRDs.

In multi-tenancy environments where multiple SRDs and Routing Policies are employed, the IP Groups that can be used in routing rules, configured in the IP-to-IP Routing table, for a specific Routing Policy depends on whether the Routing Policy is assigned to a Shared or Isolated SRD and whether it's assigned to a single SRD or multiple SRDs:

- If a Routing Policy is assigned to only one SRD and that SRD is an Isolated SRD, the routing rules of the Routing Policy can include IP Groups pertaining to the Isolated SRD as well as IP Groups pertaining to Shared SRDs. It cannot include IP Groups pertaining to other Isolated SRDs. In other words, the Routing Policy cannot include routing rules for call routing between Isolated SRDs.
- If a Routing Policy is assigned to a Shared SRD, the routing rules of the Routing Policy can include any IP Group – IP Groups pertaining to all Shared and Isolated SRDs. In effect, the Routing Policy can include routing rules for call routing between Isolated SRDs.
- If a Routing Policy is assigned to multiple SRDs (Shared and/or Isolated), the routing rules of the Routing Policy can include IP Groups pertaining to all Shared SRDs as well as IP Groups pertaining only to Isolated SRDs that are assigned the Routing Policy.

When configuring routing rules, the Web interface GUI displays only the permitted IP Groups according to the above, thereby facilitating configuration according to the desired non-bleeding topology level.

Note that Isolated SRDs are more relevant only when each tenant has its own dedicated Routing Policy to create separate, dedicated routing "tables". For all other scenarios, SRDs can be shared.

The general call flow for multi-tenancy and Routing Policies is as follows:

1. The incoming call is classified by the Classification table to an IP Group, based on the SIP Interface on which the call is received. According to the SIP Interface, the device associates the call to the SRD (source) that is assigned to the SIP Interface. The Classification table is used only if classification fails by registered user in the device's database or by Proxy Set, as supported in previous releases.
2. Once the call has been successfully classified to an IP Group, the Routing Policy assigned to the associated SRD (source) is used. However, if a "destination" Routing Policy is configured in the Classification table, it overrides the Routing Policy assigned to the SRD. This feature is useful in deployments requiring different routing and manipulation rules for specific calls pertaining to the same tenant. In such scenarios, multiple Classification rules need to be configured, where some rules use the SRD's "generic" Routing Policy while others override it with a different Routing Policy. If the device receives incoming calls (e.g., INVITE) from users that have already been classified and registered in the device's database, the device ignores the Classification table and uses the Routing Policy associated with the user during the initial classification process.
3. The regular manipulation (inbound and outbound) and routing processes are then done based on the determined Routing Policy.

To support this feature, the following new table and parameters have been added:

SBC Routing Policy [SBCRoutingPolicy]	Defines SBC Routing Policies. Up to 10 entries can be configured. [SBCRoutingPolicy] FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name, SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength, SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServersGroupName; [\SBCRoutingPolicy] Where: ▪ SBCRoutingPolicy_Name = Arbitrary name to identify the Routing Policy. This can be up to 41 characters. ▪ SBCRoutingPolicy_LCREnable = Enables LCR feature. ▪ SBCRoutingPolicy_LCRAverageCallLength = Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost. ▪ SBCRoutingPolicy_LCRDefaultCost = Defines whether routing rules in the IP-to-IP Routing table without an assigned Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups. ▪ SBCRoutingPolicy_LdapServersGroupName = Associates an LDAP Server Group, configured in the LDAP Servers Group table. Routing rules in the IP-to-IP Routing table that are configured with LDAP and Call Setup Rules use the LDAP servers associated with the Routing Policy assigned to the routing rule.
SRD Table [SRD]	New multi-tenant related parameters: ▪ [SRD_SharingPolicy] Sharing Policy = ✓ [0] Shared = Calls belonging to the SRD can be routed, using its Routing Policy, to other SRDs (having different Routing Policies).

	✓ [1] Isolated = Calls cannot be routed to other SRDs. ▪ [SRD_SBCRoutingPolicyName] SBC Routing Policy = (Not mandatory) Associates an SBC Routing Policy, defined in the SBC Routing Policy table, with the SRD. If an SRD has no Routing Policy, its associated IP Group and SIP Interface can be used in any routing and manipulation table (if the SRD's Sharing Policy is Shared).
IP-to-IP Routing Table	New parameter: ▪ [IP2IPRouting_RoutingPolicyName] Routing Policy = Associates an SBC Routing Policy, defined in the SBC Routing Policy table, with the IP-to-IP routing rule. If the routing rule is configured with LDAP and/or Call Setup Rules, it uses the LDAP servers associated with the SBC Routing Policy.
Classification Table	New parameters: ▪ [Classification_SRDName] SRD = Associates the Classification rule with a specific SRD. ▪ [Classification_DestRoutingPolicy] Dest Routing Policy = (Not mandatory) Associates an SBC Routing Policy, defined in the SBC Routing Policy table, with the classification rule. This overrides the Routing Policy of the associated SRD. ▪ [Classification_IpProfileName] IP Profile = Associates an IP Profile with the IP Group. Note: SrcIpGroupName must have a valid value (except for Deny) and must belong to the SRD set in the SRDName, unless SRDName is shared.
IP to IP Inbound Manipulation Table	New parameter: ▪ [IPInboundManipulation_RoutingPolicyName] Routing Policy = Associates an SBC Routing Policy, defined in the SBC Routing Policy table, with the manipulation rule.
IP to IP Outbound Manipulation Table	New parameter: ▪ [IPOutboundManipulation_RoutingPolicyName] Routing Policy = Associates an SBC Routing Policy, defined in the SBC Routing Policy table, with the manipulation rule.

Applicable Products: Mediant 3000.

2.35.1.3.2.2 User Search Methods in Database for Routing Calls

This feature provides support for configuring how the device searches users in its database for routing calls to the users. The device creates two entries in its database when a user registers with it:

- User part and host part (user@host) of the To header
- Only user part of the To header

For example, the device registers the user, 4709@joe.audiocodes.com under the following entries:

- 4709@joe.audiocodes.com
- 4709

When an incoming INVITE message is received, the device searches for the user (destination URI) in the database for routing the call to the corresponding contact address, using one of the following configurable methods:

- [0] All permutations = (Default) Device searches for the user by its full Request-URI (user@host). If not found, it then searches the user by user part of the Request-URI. For example, it first searches for "4709@joe.audiocodes.com" and if not found, it searches for "4709".
- [1] Dest URI dependant = Device searches for the user only by its full Request-URI (user@host). For example, it searches only for "4709@joe.audiocodes.com".

Note: If the Request-URI contains the "tel:" URI or "user=phone" parameters, the device searches **only** for the user part.

To support this feature, the following new parameter has been introduced:

SBC DB Routing Search Mode CLI: configure voip > sbc general-setting > set sbc-db-route-mode [SBCDBRoutingSearchMode]	Defines the method for searching a registered user in the device's User Registration database. ▪ [0] All permutations = (Default) Device searches for the user in the database using the entire Request-URI (user@host). If not found, it then searches for the user by user part of the Request-URI. ▪ [1] Dest URI dependant = Device searches for the user in the database using the entire Request-URI (user@host) only. **Note:** If the Request-URI contains the "tel:" URI or "user=phone" parameter, the device searches only for the user part.

Applicable Products: Mediant 3000.

2.35.1.3.2.3 IP Profile Association in Classification Process by Classification Table

This feature provides support for assigning an IP Profile to incoming SBC calls during classification based on the Classification table. As the IP Profile in the Classification table overrides the IP Profile assigned to the IP Group in the IP Group table, the benefit of this feature is that it allows the administrator to assign different IP Profiles to specific users (calls) pertaining to the same IP Group (User or Server type).

For example, two classification rules in the Classification table are configured to classify incoming calls to the same IP Group. However, for calls received with the source hostname prefix, "abcd.com", the device must use a different IP Profile from the one configured for the IP Group. To support this setup, two classification rules need to be configured where one is the regular classification rule that doesn't specify an IP Profile, while the second rule is configured with an additional matching characteristic for the source hostname prefix ("abcd.com") and with an additional action that assigns a different IP Profile.

Note: For User-type IP Groups, if a user has already been registered in the device's users database (from an initial classification process), the device classifies subsequent INVITE requests from the user according to its users database instead of the Classification table. In such a scenario, the same IP Profile that was previously assigned to the user by the Classification table is also used (in other words, the device's users database stores the associated IP Profile).

To support this feature, the following new parameter has been added to the Classification table:

IP Profile [Classification_IpProfileName]	Associates an IP Profile to the classified call.

Applicable Products: Mediant 3000.

2.35.1.3.2.4 Routing Rules with Destination as Registered Users

This feature provides support for configuring an SBC IP-to-IP routing rule with a destination type that is a registered user. In other words, the device checks whether the Request-URI received in the incoming INVITE is registered in its users' database, and if yes, it sends the INVITE to the contact address.

To support this feature, the following new optional value has been added to the 'Destination Type' field in the IP-to-IP Routing Table:

Destination Type [IP2IPRouting_DestType]	New option: ▪ [10] All Users = Device checks whether the Request-URI, received in the incoming INVITE is registered in the SBC's users' database, and if yes, it sends the INVITE to the contact address.

Applicable Products: Mediant 3000.

2.35.1.3.2.5 Rerouting Calls upon Broken RTP Connection

The feature provides support for rerouting a call upon detection of a broken RTP connection. When the call disconnects, the device searches for a matching routing rule in the IP-to-IP Routing table and if found, sends the call to the corresponding destination. A rule can also be configured to match broken connection calls and therefore, implement a type of alternative routing upon broken RTP connection.

To support the feature, a new option has been added to the Call Trigger:

Disconnect on Broken Connection disconnect-on-broken-connection [IpProfile_DisconnectOnBrokenConnection]	New option ▪ [2] Reroute
Broken Connection Mode disc-broken-conn [DisconnectOnBrokenConnection]	New option [2] Reroute
Call Trigger trigger [IP2IPRouting_Trigger]	New option: [5] Broken Connection

Applicable Products: Mediant 3000.

2.35.1.3.3 Gateway

This section describes the new Gateway routing features.

2.35.1.3.3.1 SIP Proxy Server Connectivity Status per Tel-to-IP Routing Rule

This feature provides support for displaying the connectivity status of SIP proxy servers associated with Tel-to-IP routing rules. The status is displayed in the existing field, 'Connectivity Status' in the Tel to IP Routing table. This is applicable only to routing rules whose destination is an IP Group (i.e., the 'Destination IP Group' field is set to an IP Group). Up until now, only connectivity status of an IP address destination ('Destination IP Address' field) was supported.

For the status to be displayed, the existing Proxy Keep-Alive feature, which monitors the connectivity with proxy servers per Proxy Set must be enabled. This is done in the Proxy Sets table using the 'Proxy Keep-Alive' field. If a Proxy Set is configured with multiple proxies for redundancy purposes, the status displayed in the 'Connectivity Status' field may change according to the proxy server with which the device attempts to verify connectivity. For example, if there is no response from the first configured proxy address, the status displays "No Connectivity". However, if there is a response from the next proxy server in the list, the status changes to "OK".

Applicable Products: Mediant 3000.

2.35.1.3.3.2 Trunk or Trunk Group Destination Type for IP-to-Tel Routing Rules

This feature provides support for defining the type of Tel (PSTN) destination for IP-to-Tel routing rules. The destination type can be a Trunk or Trunk Group. Previous releases allowed specifying the actual Trunk and/or Trunk Group ID. This new feature was mainly introduced for future possible implementations where the destination type may be another entity such as a remote routing server.

To support this feature, the following parameter has been added to the Inbound IP Routing table:

Destination Type [PstnPrefix_DestType]	Defines the type of destination: ▪ [0] Trunk Group (default) ▪ [1] Trunk

Applicable Products: Mediant 3000.

2.35.1.3.3.3 Gateway Routing Policy

This feature provides support for a new Gateway configuration entity, termed *Routing Policy*. The device supports only one Routing Policy, which can be configured with the following:

- LDAP Servers Group: The Routing Policy can be assigned an LDAP Servers Group (for more information on the new LDAP Server Groups feature, see Section 2.35.1.4.1.1 on page 88). This is for determining the LDAP server(s) used for LDAP-based routing (LDAP and/or Call Setup Rules queries), which is applicable to both Tel-to-IP and IP-to-Tel routing.
- Least Cost Routing (LCR): The Routing Policy can be enabled or disabled (default) with LCR. If enabled, it can also be configured with the default call cost (highest or lowest) and default call duration. This configuration replaces the Routing Rule Groups table (RoutingRuleGroups) supported in previous releases (providing the same parameters). LCR is applicable only to outbound IP calls.

To support this feature, the following new table has been added:

Gateway Routing Policy configure voip > gw routing gw-routing-policy [GwRoutingPolicy]	Defines a Routing Policy for Gateway calls. Only one index row can be defined. [GwRoutingPolicy] FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name, GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength, GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServersGroupName; [\GwRoutingPolicy] Where: ▪ GwRoutingPolicy_Name = Arbitrary name to identify the Routing Policy. This can be up to 41 characters. ▪ GwRoutingPolicy_LCREnable = Enables LCR feature. ▪ GwRoutingPolicy_LCRAverageCallLength = Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost. ▪ GwRoutingPolicy_LCRDefaultCost = Defines whether routing rules in the routing table that are not assigned a Cost Group are considered a higher or lower cost route compared to other matched routing rules that are assigned Cost Groups. ▪ GwRoutingPolicy_LdapServersGroupName = Associates an LDAP Server Group. Routing rules in the Tel to IP Routing table and Inbound IP Routing table that are configured with LDAP and/or Call Setup Rules, use the LDAP servers associated with the Routing Policy assigned to the routing rule.

Applicable Products: Mediant 3000.

2.35.1.4 SIP Supplementary Service Features

This section describes the new SIP supplementary service features.

2.35.1.4.1 General

2.35.1.4.1.1 LDAP Server Groups

This feature provides support for creating logical groups of LDAP servers, termed *LDAP Server Groups*. Each LDAP Server Group can contain up to two LDAP servers. The maximum number of LDAP Server Groups that can be configured is:

- 33 for Mediant 3000

LDAP Server Groups are configured using the new LDAP Servers Group table, which defines the following:

- Unique identification name.
- Type of LDAP server – defines whether the servers in the group are used for SIP signaling (Control) or management (OAMP). Note that only one LDAP Server Group can be defined for management.
- LDAP search (query) method - determines whether the query is sent in parallel to both LDAP servers (if connected) in the group or sent to the second server only if the search fails (or a result is not found). This parameter replaces the LDAPSearchServerMethod parameter supported in the previous release.
- DN search method - Defines the method of how the device queries the DN object within each LDAP server. This parameter replaces the LDAPSearchDNsinParallel parameter supported in the previous release.
- LDAP cache record timeout - defines the lifespan of an entry in the device's LDAP cache after which the LDAP entry is not used. This parameter replaces the LDAPCacheEntryTimeout parameter supported in the previous release.
- LDAP cache record deletion timeout – defines the lifespan duration after which the LDAP entry is removed from the cache. This parameter replaces the LDAPCacheEntryRemovalTimeout parameter supported in the previous release

Each LDAP server must be assigned to an LDAP Server Group. The association is done in the existing LDAP Configuration table (using a new parameter - see description below). The LDAP servers are associated with routing rules using the new configuration entity, Routing Policy (see Section 2.35.1.3.2.1 on page 81). Each Routing Policy can be assigned one LDAP Server Group. This feature has also been implemented to support the enhanced multi-tenant functionality, where each tenant can be assigned a specific LDAP Server Group through its unique Routing Policy.

To support this feature, the following new table and parameter have been added:

LDAP Servers Group CLI: config-voip>ldap>ldap-servers-group [LDAPServersGroup]	Configures LDAP Server groups. [LDAPServersGroup] FORMAT LdapServersGroup_Index = LdapServersGroup_Name, LdapServersGroup_ServerType, LdapServersGroup_SearchMethod, LdapServersGroup_CacheEntryTimeout, LdapServersGroup_CacheEntryRemovalTimeout, LdapServersGroup_SearchDnsMethod; [\LDAPServersGroup] Where: ▪ Name = Arbitrary name of the group ▪ ServerType = Defines if used for Control (default) or Management ▪ SearchMethod = Defines the search method between the two severs - Parallel (default) or Sequential. ▪ CacheEntryTimeout = Defines the lifespan of an entry in the device's LDAP cache after which the LDAP entry is not used. ▪ CacheEntryRemovalTimeout = Defines the lifespan duration after which the LDAP entry is removed from the cache. ▪ SearchDnsMethod = Defines the method for querying DN objects per LDAP server.

(LDAP Configuration Table - LdapConfiguration) LDAP Servers Group CLI: configure voip > ldap > ldap-configuration > server-group [LdapConfiguration_Group]	Assigns the LDAP server to an LDAP group, which is configured in the LDAP Servers Group.

Applicable Products: Mediant 3000.

2.35.1.4.1.2 TLS Certificate per LDAP Server

This feature provides support for specifying a TLS certificate context (TLS Context) for a TLS connection per LDAP server. If no TLS Context is specified, the device uses the default TLS Context (ID 0).

To support this feature, the following new parameter has been added to the existing LDAP Configuration table:

TLS Context [LdapConfiguration_ContextName]	Assigns a TLS Context for the connection with the LDAP server. By default, no value is defined (None). Note: The parameter is applicable only if the connection is secured (HTTPS).

Applicable Products: Mediant 3000.

2.35.1.4.1.3 Multiple RADIUS Servers

This feature provides support for configuring multiple RADIUS servers and therefore, RADIUS server redundancy. Up until this release, only one RADIUS server could be configured.

Up to three RADIUS servers can now be configured. When the primary RADIUS server is down, the device sends a RADIUS request twice (one retransmission) and if both fail (i.e., no response), the device considers the server as down and attempts to send requests to the next server. Currently, homing is not supported; the device continues sending RADIUS requests to the redundant RADIUS server even if the primary server returns to service. However, if a device reset occurs or a switchover occurs in a High-Availability (HA) system, the device sends RADIUS requests to the primary RADIUS server. The default timeout for RADIUS requests and retransmission that the device waits for a response from the RADIUS server before it considers it down, is two seconds.

For each server, the IP address, authentication port, authentication shared secret, and accounting port can be configured. Each RADIUS server can be defined for RADIUS-based login authentication and/or RADIUS-based accounting (sending of SIP CDRs to RADIUS server). By setting the relevant port to "0" disables the corresponding functionality. If both ports are configured, the RADIUS server is used for authentication and accounting. All servers configured with non-zero Authorization ports form an Authorization redundancy group and the device sends authorization requests to one of them, depending on their availability. All servers configured with non-zero Accounting ports form an Accounting redundancy group and the device sends accounting CDRs to one of them, depending on their availability. Example configurations:

- Only one RADIUS server is configured and used for both authorization and accounting purposes (no redundancy). Therefore, both the Authorization and Accounting ports are defined.
- Three RADIUS servers are configured:
    - Two servers are used for authorization purposes only, providing redundancy. Therefore, only the Authorization ports are defined while the Accounting ports are set to 0.
    - One server is used for accounting purposes only (i.e., no redundancy). Therefore, only the Accounting port is defined while the Authorization port is set to 0.

- Two RADIUS servers are configured and used for both authorization and accounting purposes, providing redundancy. Therefore, both the Authorization ports and Accounting ports are defined.

To support this feature, the following new table has been added. This table replaces the related parameters from previous releases - RADIUSAccPort, RADIUSAuthServerIP, RADIUSAuthPort, SharedSecret, RADIUSAccServerIP.

RADIUS Servers CLI: configure system > radius > servers [RadiusServers]	Defines RADIUS servers. [RadiusServers] FORMAT RadiusServers_Index = RadiusServers_ServerGroup, RadiusServers_IPAddress, RadiusServers_AuthenticationPort, RadiusServers_AccountingPort, RadiusServers_SharedSecret; [\RadiusServers] Where: ▪ IPAddress = IP address of the RADIUS server. ▪ AuthenticationPort = Port number for authenticating the device with RADIUS server. ▪ AccountingPort = Port for sending accounting data of SIP calls as call detail records (CDR) to the RADIUS Accounting server. ▪ SharedSecret = Shared secret for authenticating the device to the RADIUS server. Note: Currently, ServerGroup is not supported.

The status of the RADIUS severs can be viewed using the following new CLI command:

```
# show system radius servers status
```

For example:

```
servers 0
 ip-address 10.4.4.203
 auth-port 1812
 auth-ha-state "ACTIVE"
 acc-port 1813
 acc-ha-state "ACTIVE"
servers 1
 ip-address 10.4.4.202
 auth-port 1812
 auth-ha-state "STANDBY"
 acc-port 1813
 acc-ha-state "STANDBY"
```

The command shows the following fields per server:

- Server IP address.
- Server authentication port. If zero, the server is not part of the redundancy server selection for authentication.
- Server authentication redundancy (HA) status. "ACTIVE" means that the server was used for the last sent authentication request.
- Server accounting port. If zero, the server is not part of the redundancy server selection for accounting.
- Server accounting redundancy (HA) status. "ACTIVE" means that the server was used for the last sent accounting request.

Applicable Products: Mediant 3000.

2.35.1.4.1.4 RADIUS Communication over SIP Interface (Control)

This feature provides support for communicating with a RADIUS server through the device's Control (SIP) network interface. Up until this release, RADIUS communication was done only through the OAMP network interface.

To support this feature, the following new parameter has been added:

[RadiusTrafficType]	Defines the device's network interface used for RADIUS traffic. ▪ [0] OAMP (default) ▪ [1] Control Note: If set to **Control**, only **one** Control interface must be configured in the Interface table; otherwise, RADIUS communication will fail.

Applicable Products: Mediant 3000.

2.35.1.4.2 SBC

2.35.1.4.2.1 Call Preemption for SBC Emergency Calls

This feature provides support for implementing emergency call preemption for SBC calls. When there is an incoming emergency call and there are no resources available, the device preempts one of the active calls to ensure that the emergency call is processed and sent to the emergency provider (and not rejected). Therefore, emergency calls are prioritized over normal calls.

Emergency call preemption is enabled by the new parameter, SBCPreemptionMode. In addition, the device identifies incoming calls as emergency calls based on a user-defined Message Condition rule configured in the existing Message Condition table. Once configured, the new parameter, SBCEmergencyCondition defines the index of this Message Condition rule that must be used to identify emergency calls. The device runs the rule only after call classification (but before inbound manipulation). Below is an example of Message Condition rules for identifying emergency calls:

- SIP Resource-Priority header contains a string indicating an emergency call:

```
header.resource-priority contains 'emergency'
header.resource-priority contains 'esnet'
```

- Destination user part contains an emergency provider address:

```
param.call.dst.user == '911'
param.call.dst.user == '100' || param.call.dst.user == '101'
|| param.call.dst.user == '102'
header.request-uri contains 'urn:service:sos'
```

When the device identifies an emergency call, it checks for available resources (based on INVITE messages) on its incoming and outgoing legs. Note that the device may need to preempt more than one call in order to provide sufficient resources for the emergency call. The device does not preempt already established emergency calls. When the device preempts a call, it disconnects the call as follows:

- If the call is being setup (not yet established), it sends a SIP 488 response to the incoming leg and a SIP CANCEL message to the outgoing leg.
- If the call is established, it sends a SIP BYE message to each leg. The device includes the Reason header in the BYE message to describe the cause as "preemption".

Once the device terminates the regular call, it does not wait for any response from the remote sides (e.g., 200 OK after BYE), but immediately sends the INVITE message of the emergency call to its destination.

If the device is unable to preempt a call for the emergency call, it rejects the emergency call with a SIP 503 "Emergency Call Failed" (instead of "Service Unavailable") response.

Quality of Service (QoS) levels (markings) can be assigned to SIP signaling and RTP packets of SBC emergency calls. The Differentiated Services Code Points (DiffServ / DSCP) for these packets are configured using the new parameters, SBCEmergencyRTPDiffServ and SBCEmergencySignalingDiffServ.

Note that the device does not monitor emergency calls with regards to Quality of Experience (QoE).

To support this feature, the following new parameters have been added:

SBC Preemption Mode CLI: configure voip > sbc general-setting > sbc-preemption-mode [SBCPreemptionMode]	Enables SBC emergency call preemption. ▪ [0] Disable (default) ▪ [1] Enable
SBC Emergency Condition CLI: configure voip > sbc general-setting > sbc-emerg-condition [SBCEmergencyCondition]	Defines the index of the Message Condition rule in the Message Condition table that is used to identify emergency calls. The device runs the rule only after call classification (but before inbound manipulation).
SBC Emergency RTP Diffserv CLI: configure voip > sbc general-setting > sbc-emerg-rtp-diffserv [SBCEmergencyRTPDiffServ]	Defines DiffServ bits sent in the RTP for SBC emergency calls. The valid value is 0 – 63. The default is 46.
SBC Emergency Signaling Diffserv CLI: configure voip > sbc general-setting > sbc-emerg-sig-diffserv [SBCEmergencySignalingDiffServ]	Defines DiffServ bits sent in SIP signaling messages for SBC emergency calls. This is included in the SIP Resource-Priority header. The valid value is 0 – 63. The default is 40.

Applicable Products: Mediant 3000.

2.35.1.4.2.2 Microsoft Lync E9-1-1 Routing using ELIN SIP Trunk (PSAP Server)

This feature provides support for SBC IP-to-IP routing of E9-1-1 emergency calls in a Microsoft Lync Server environment. Up until this release, ELIN routing was supported only by the Gateway application (IP-to-Tel).

E9-1-1 is a national emergency service for many countries, enabling E9-1-1 operators to automatically identify the geographical location and phone number of an emergency caller. In E9-1-1, the caller is routed to the nearest E9-1-1 operator, termed public safety answering point (PSAP), based on the location of the caller. The PSAP can then quickly dispatch the relevant emergency services such as the fire department or police to the caller's location.

Microsoft Lync passes the geographical location information (ELIN number) of the Lync client (E9-1-1 caller) in an IETF-standard format, Presence Information Data Format Location Object (PIDF-LO) in the SIP INVITE message (XML message body). When the device receives an emergency call, it extracts the ELIN number from the PIDF-LO. The device stores the ELIN number with the caller's phone number in its database. The device then sends the call to the appropriate IP Group (i.e., PSAP sever) based on the ELIN number, which serves as the calling number (source). The emergency service provider sends the call to the appropriate PSAP based on the ELIN number.

If the call is prematurely disconnected, the operator calls back the emergency caller using the ELIN number as the called number. The device translates this called number (i.e., ELIN) received from the PSAP to the corresponding E9-1-1 caller's phone number, as previously stored in the database and associated with the ELIN. The PSAP can use the ELIN to call back the E9-1-1 caller within a user-defined time timeout (in minutes), started from when the call with the PSAP was disconnected. This is configured using the existing parameter E911CallbackTimeout. PSAP Callback is only done if PSAP is enabled (using the new parameter SBC PSAP Mode) for the IP Group associated with the PSAP server.

Configuration includes the following:

- Enabling the PSAP mode for the IP Group of the PSAP server in the IP Group table. (See description of this new parameter below.)
- Defining routing rules in the IP-to-IP Routing table for routing between the emergency callers' IP Group and the PSAP IP Group. The only special configuration is to define the emergency number (e.g., 911) as the Destination Username Prefix.

To support this feature, the following new SBC parameter has been added to the IP Group table:

SBC PSAP Mode CLI: configure voip > control-network ip-group > sbc-psap-mode [IPGroup_SBCPSAPMode]	Enables E9-1-1 emergency call routing in a Microsoft Lync Server environment. ▪ [0] None (default) ▪ [1] PSAP Server

Applicable Products: Mediant 3000.

2.35.1.4.2.3 Emergency Call Routing in non-Lync Environments

This feature provides support for routing emergency calls in non-Microsoft Lync environments. In such an environment, the INVITE message of the emergency call (911) is received by the device without an ELIN number. Using the device's Call Setup Rules table, the device can query an LDAP server for the user's ELIN number. The obtained ELIN number and the Content-Type header for the PIDF XML message body is inserted into the INVITE message, for example:

```
Content-Type: application/pidf+xml
            <NAM>1234567890</NAM>
```

An example of a Call Setup Rule is shown below:

```
[ CallSetupRules ]
FORMAT CallSetupRules_Index = CallSetupRules_RulesSetID,
CallSetupRules_AttributesToQuery, CallSetupRules_AttributesToGet,
CallSetupRules_RowRole, CallSetupRules_Condition,
CallSetupRules_ActionSubject, CallSetupRules_ActionType,
CallSetupRules_ActionValue;
CallSetupRules 0 = 1, "'telephoneNumber='+param.call.src.user",
"numberELIN", 0, "ldap.attr.numberELIN exists",
"body.application/pidf+xml", 0,
"<NAM>'+ldap.attr.numberELIN+'</NAM>'";
[ \CallSetupRules ]
```

The above rule queries the Active Directory (AD) server for the attribute "telephoneNumber" whose value is the caller's number, and then retrieves the user's ELIN number from the user-defined attribute, "numberELIN". The device then inserts the ELIN number in an XML message body into the INVITE message.

The rest of the process is similar to emergency call routing in a Lync environment, as described in Section 2.35.1.4.2.2.

Configuration includes the following:

- Enabling the PSAP mode for the IP Group of the PSAP server, in the IP Group table.
- Defining routing rules in the IP-to-IP Routing table for routing between the emergency caller's IP Group and the PSAP's IP Group. The only special configuration is to define the emergency number (e.g., 911) in the 'Destination Username Prefix' field and to associate the Call Setup Rule that was configured for obtaining the ELIN number from the AD, using the 'Call Setup Rules Set ID' field.

Applicable Products: Mediant 3000.

2.35.1.5 User Registration and Authentication Features

This section describes the new user registration and authentication features.

2.35.1.5.1SBC

2.35.1.5.1.1 Registration Time for Users behind NAT

This feature provides support for configuring the registration time (in seconds) that the device includes in register responses, in response to SIP REGISTER requests from SBC users, belonging to a SIP entity associated with an IP Profile, that are located behind NAT and whose communication type is TCP or UDP. The registration time is inserted in the Expires header in the outgoing response sent to the user.

The valid value is 0 to 2,000,000. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. By default, no value is defined (-1).

To support this feature, the following new parameter has been added to the IP Profile table:

NAT TCP Registration Time sbc-usr-tcp-nat-reg-time [IpProfile_SBCUserBehindTcpNATRegistrationTime]	Defines the registration time (in seconds) that the <device> includes in register responses, in response to SIP REGISTER requests from users belonging to the SIP entity associated with the IP Profile. The parameter applies only to users that are located behind NAT and whose communication type is TCP. The registration time is inserted in the Expires header in the outgoing response sent to the user. The valid value is 0 to 2,000,000. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. By default, no value is defined (-1).
NAT UDP Registration Time sbc-usr-udp-nat-reg-time [IpProfile_SBCUserBehindUdpNATRegistrationTime]	Defines the registration time (in seconds) that the <device> includes in register responses, in response to SIP REGISTER requests from users belonging to the SIP entity associated with the IP Profile. The parameter applies only to users that are located behind NAT and whose communication type is UDP. The registration time is inserted in the Expires header in the outgoing response sent to the user. The valid value is 0 to 2,000,000. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. By default, no value is defined (-1).

Applicable Products: Mediant 3000.

2.35.1.5.1.2 Deletion of Registered Users

This feature provides support for deleting SBC users that are registered with the device. In other words, users can be removed from the device's users' registration database. This is supported by the addition of the following CLI commands:

- Deletion of a specific registered user from the database:

  ```
  # clear voip register db sbc user <AOR of user – user part or user@host>
  ```

  For example,

  ```
  # clear voip register db sbc user John@10.33.2.22
  # clear voip register db sbc user John
  ```

- Deletion of all registered users belonging to a specific IP Group:

  ```
  # clear voip register db sbc ip-group <ID or name>
  ```

Applicable Products: Mediant 3000.

2.35.1.6 Media and SDP Features

This section describes the new VoIP media and Session Description Protocol (SDP) features.

2.35.1.6.1 General

This section describes the new general media and SDP features.

2.35.1.6.1.1 PRT File with Same Tone Types but Different Coders

This feature provides support for using a Prerecorded Tone file (PRT) containing multiple tones of the same tone type but with different coders. If one of the tones is defined with the same coder as used in the current call, the device always selects it in order to eliminate the need for using DSP resources. For SBC calls, the device plays the tone without requiring DSPs if the tone's coder is the same as the coder used for the current call; otherwise, it uses DSP resources.

Note: Mediant 3000 always uses DSPs for playing tones from the PRT file.

Applicable Products: Mediant 3000.

2.35.1.6.2 SBC

This section describes the new SBC media and SDP features.

2.35.1.6.2.1 Identifying RTP/(S)AVP(F) Media Streams in SDP

This feature provides support for the device to identify incoming RTP/(S)AVP(F) media streams in the SDP body, according to RFC 5124. RTP/(S)AVP(F) is indicated in the SDP 'm=' line as shown in the following example:

```
m=audio 49170 RTP/SAVPF 0 96
```

The presence of "S" (for secured RTP) or "F" (for RTCP-based feedback) is optional.

The device can identify RTP/(S)AVP(F) regardless of whether or not other protocols are present in the proto field of the 'm=' line, for example:

```
m=audio 49170 UDP/TLS/RTP/SAVPF 0 96
```

Applicable Products: Mediant 3000.

2.35.1.6.2.2 SRTP Profile Negotiation using RTCP-based Feedback (AVPF/SAVPF)

This feature provides support for indicating RTCP-based feedback according to RFC 5124 during RTP profile negotiation between two communicating SIP entities. RFC 5124 defines an RTP profile (S)AVPF for (secure) real-time communications to provide timely feedback from the receivers to a sender. For more information on RFC 5124, see http://tools.ietf.org/html/rfc5124.

Some SIP entities may require RTP secure-profile feedback negotiation (AVPF/SAVPF) in the SDP offer/answer exchange, while other SIP entities may not support it. The device indicates whether feedback is supported or not on behalf of the SIP entity, using IP Profiles. It does this by adding an "F" or removing the "F" from the SDP media line ('m=') for AVP and SAVP. For example, the below shows "AVP" appended with an "F", indicating that the SIP entity is capable of receiving feedback

```
m=audio 49170 RTP/SAVPF 0 96
```

To support this feature, the following new parameter has been added to the IP Profile table:

RTCP Feedback CLI: configure voip > coders-and-profiles ip-profile > sbc-rtcp-feedback [IPProfile_SBCRTCPFeedback]	Enables RTCP-based feedback support for the SIP entity with which the IP Profile is associated. ▪ [0] Disable = (Default) The device does not send the feedback flag ("F") in SDP offers/answers that are sent to the SIP entity. If the SDP 'm=' attribute of an incoming message that is destined to the SIP entity includes the feedback flag, the device removes it before sending the message to the SIP entity.

	▪ [1] Enable = The device includes the feedback flag ("F") in the SDP offer that is sent to the SIP entity. The device includes the feedback flag in the SDP answer sent to the SIP entity only if it was present in the SDP offer received from the other SIP entity.

Applicable Products: Mediant 3000.

2.35.1.6.2.3 RTP Redundancy Negotiation in SDP

This feature provides support for RTP redundancy negotiation in SDP for inbound and outbound SBC calls (according to RFC 2198). The device can now interwork between two SIP entities regarding support for RTP redundancy in the SDP offer/answer exchange. The device can identify the RTP redundancy payload type in the SDP for indicating that the RTP packet stream includes redundant packets. RTP redundancy is indicated in SDP using the "red" coder type, for example:

```
a=rtpmap:<payload type> red/8000/1
```

RTP redundancy is useful when there is packet loss; the missing information may be reconstructed at the receiver side from the redundant packets.

To support this feature, RTP redundancy support can be configured for each SIP entity using the new IP Profile table parameter, SBCRTPRedundancyBehavior:

- Transparent (default): The device transmits the SDP offer/answer (incoming and outgoing calls) as is without interfering in the RTP redundancy negotiation.
- Disable: This is used if the SIP entity does not support RTP redundancy. The device removes the RTP redundancy payload (if present) from the SDP offer/answer for calls received from or sent to the SIP entity.
- Enable: This is used when the SIP entity requires RTP redundancy: The device always adds RTP redundancy capabilities in the outgoing SDP offer sent to the SIP entity. Whether RTP redundancy is implemented depends on the subsequent incoming SDP answer from the SIP entity. The device does not modify the incoming SDP offer received from the SIP entity, but if RTP redundancy is required, it will be supported.

Therefore, according to the RTP redundancy SDP offer/answer negotiation, the device uses or discards the RTP redundancy packets. The device supports the asymmetric RTP redundancy, whereby it can transmit and receive RTP redundancy packets to and from a specific SIP entity, while transmitting and receiving regular RTP packets (no redundancy) on the other SIP entity involved in the voice path.

The following related parameters from previous releases are also used for RTP redundancy:

- IpProfile_RTPRedundancyDepth: enables the <device> to generate RFC 2198 redundant packets.
- RFC2198PayloadType: defines the payload type for RTP redundancy. The configured value is used only when the device needs to add RTP redundancy payload to the outgoing SDP Offer.

RTP Redundancy Mode CLI: sbc-rtp-red-behav [IpProfile_SBCRTPRedundancyBehavior]	Defines RTP redundancy support for the SIP entity associated with this IP Profile. [0] As Is = (Default) The device does not interfere in the RTP redundancy negotiation. [1] Enable = See description in the section above. [2] Disable = See description in the section above.

Applicable Products: Mediant 3000.

2.35.1.6.2.4 Interworking RTCP Attribute in SDP

This feature provides support for interworking the RTCP attribute ('a=rtcp') of the SDP for SBC calls. The RTCP attribute is used to indicate the RTCP port used for media stream when that port is not the next higher port number following the RTP port described in the media line.

The feature is useful for SIP entities that either require the attribute or do not support the attribute. In Web RTC, Chrome (SDES) generates SDP with 'a=rtcp', for example:

```
m=audio 49170 RTP/AVP 0
a=rtcp:53020 IN IP6 2001:2345:6789:ABCD:EF01:2345:6789:ABCD
```

In addition, Web RTC Chrome (SDES) is able to obtain cryptographic key exchange information ('a=crypto') without the lifetime (of the master key) and Master Key Identifier (MKI) fields in the SDP.

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

SDP Handle RTCP CLI: sbc-sdp-handle-rtcp [IpProfile_SBCSDPHandleRTCPAttribute]	Enables interworking of the 'a=rtcp' (RTCP) attribute in the SDP for the SIP entity (IP Group) associated with the IP Profile. ▪ [0] Don't Care (default) ▪ [1] Add = The device adds an 'a=rtcp' attribute to the outgoing SDP offer sent to the SIP entity if the attribute was not present in the original incoming SDP offer. ▪ [2] Remove = The 'a=rtcp' attribute received in the original incoming SDP offer is not sent to the SIP entity in the outgoing SDP offer.
SDP Remove Crypto LifeTime CLI: sbc-sdp-remove-crypto-lifetime [IpProfile_SBCRemoveCryptoLifetimeInSDP]	Enables removal of the lifetime field in the 'a=crypto' attribute of the SDP for the SIP entity (IP Group) associated with the IP Profile. ▪ [0] No (default) ▪ [1] Yes = The lifetime field is removed from the 'a=crypto' attribute.

Note that for this feature to be functional, the following existing IP Profile parameters must be configured as follows:

- Symmetric MKI [IpProfile_EnableSymmetricMKI] set to Enable [1]
- MKI Size [IpProfile_MKISize] set to 0
- Enforce MKI Size [IpProfile_SBCEnforceMKISize] set to Enforce [1]

Applicable Products: Mediant 3000.

2.35.1.7 PSTN Features

This section describes the new PSTN features.

2.35.1.7.1 General

This section describes the new general PSTN features.

2.35.1.7.1.1 Mapping Accented (Unicode) Characters to ASCII

This feature provides support for mapping accented characters (Unicode / UTF-8) that are received from the IP side into simple ASCII characters (ISO-8859) for sending to the PSTN. Typically, the device receives the caller ID and calling name in Unicode characters (in the SIP INVITE message). Unicode characters consist of two bytes while ASCII characters consist of one byte. Accented characters are used in various languages such as German, for example, the umlaut (or diaeresis) which consists of two dots placed over a letter as in ä.

The importance of this feature is that it allows PSTN entities that do not support accented characters to receive ASCII characters. For example, the device can convert the Unicode character ä into the ASCII character "ae".

The feature works in conjunction with the existing parameter, ISO8859CharacterSet. When the parameter is set to [0] (Latin only), it converts accented characters into ASCII (e.g., ä to "a"). However, the feature can be used to overwrite these "basic" conversions and customize them (e.g., ä to "ae" instead of the default "a").

To support this feature, the following new table has been added (to the Web, under the Configuration tab > VoIP menu > Gateway > DTMF and Supplementary):

Char Conversion CLI: configure voip > gw dtmf-and-suppl dtmf-and-dialing char-conversion display [CharConversion]	Defines up to 40 Unicode-to-ASCII character mapping rules. FORMAT CharConversion_Index = CharConversion_CharName, CharConversion_FirstByte, CharConversion_SecondByte, CharConversion_ConvertedOutput; [\CharConversion] Where: ▪ Character Name [CharName] = Arbitrary name to identify the rule. ▪ First Byte [FirstByte] = Defines the first byte of the Unicode character (e.g., 195). ▪ Second Byte [SecondByte] = Defines the second byte of the Unicode character (e.g., 164). ▪ Converted Output [ConvertedOutput] = Defines the ASCII character (e.g., "ae") to which the Unicode character must be converted. The valid value is up to four ASCII characters. This can include any ASCII character - alpha numerals (e.g., a, A, 6) and/or symbols (e.g., !, ?, _, &). For example: CharConversion 0 = "a with Diaeresis", 195, 164, "ae";

Applicable Products: Mediant 3000.

2.35.1.7.2 Digital

This section describes the new digital (ISDN) features.

2.35.1.7.2.1 ISDN-to-ISDN Release Cause Code Mapping

This feature provides support for mapping ISDN ITU-T Q.850 release cause codes received from the PSTN to different ISDN Q.850 cause codes. Therefore, this enables the user to manipulate the originally received cause code. For example, the PSTN may indicate disconnected calls (hang up) by sending cause code 127. Using this feature, the cause code can be manipulated to 16, which is a typical cause code for such scenarios.

To support this feature, the following new table has been added:

Release Cause ISDN->ISDN CLI: configure voip > gw manipulations > cause-map-isdn2isdn [CauseMapIsdn2Isdn]	Defines up to 10 ISDN-to-ISDN release cause code mapping rules. The valid values (cause codes) can be 1 through 127. The format of the ini file table is as follows: [CauseMapIsdn2Isdn] FORMAT CauseMapIsdn2Isdn_Index = CauseMapIsdn2Isdn_OrigIsdnReleaseCause, CauseMapIsdn2Isdn_MapIsdnReleaseCause; [\CauseMapSip2Isdn] Note: The feature is supported only by CLI and ini file.

Applicable Products: Mediant 3000.

2.35.1.7.2.2 Advice-of-Charge Services for IP-to-Tel Calls

This feature provides support for an additional mode of Advice-of-Charge (AOC) services in the IP-to-Tel direction (SIP to ISDN).

AOC is a pre-billing feature that tasks the rating engine with calculating the cost of using a service and relaying that information to the customer (caller). This allows users to obtain call charge information during the call (AOC-D) or at the end of the call (AOC-E). The device receives the charging information from the IP side in the SIP INFO message (during the call) and BYE message (end of the call). The information is provided in AudioCodes' proprietary SIP header, AOC. The device then converts this charging information into AOC-D and AOC-E messages in the EURO ISDN Facility Information Element (IE) message that it sends to the PSTN side. If the device receives an ISDN Disconnect message, it delays its Release response until it receives the SIP 200 OK response with AOC information upon a BYE message (or timer expiration).

Below is an example of the AOC header:

```
AOC: charged; <parameters>
```

Where *parameters* can be:

- state="active" or "terminated"
- charging-info="currency" or "pulse"
  - If "currency", the following parameters are available:
    - currency=<string>
    - currency-type="iso4217-a" or <string>
    - amount=<number>
    - multiplier=("0.001","0.01","0.1","1","10","100","1000")
  - If "pulse", the following parameters are available:
    - recorded-units=<number>

To support this feature, the following new optional value has been added to the existing PayPhoneMeteringMode parameter:

Generate Metering Tones CLI: gen-mtr-tones [PayPhoneMeteringMode]	[5] SIP 2 TEL INTERWORKING = Enables IP-to-Tel AOC.

Applicable Products: Mediant 3000.

2.35.1.7.2.3 Interworking Keypad DTMFs from IP to ISDN Facility Message

This feature provides support for interworking DTMF tones received from the IP to the PSTN using the ISDN Keypad Facility information element (IE) in Q.931 INFORMATION messages. This feature applies only to the Euro ISDN variant (User side).

If the device receives from the IP side an INVITE message whose called party number (To header) contains the asterisk (*) or pound (#) character, or a SIP NOTIFY or SIP INFO message that contains these characters (e.g., 123#456), the device sends the character and the digits positioned to its right, as Keypad IE in the INFORMATION message. The device only sends the digits positioned before the character to the PSTN (in SETUP message) as the called party number.

For example, if the device receives the below INVITE, it sends "123" to the PSTN as the called party number and #456 as Keypad IE in the INFORMATION message:

```
INVITE sip:%7B54443994-BDFF-413C-AE4F-
D039B0FFB134%7D@192.168.100.214:5064;transport=tcp;rinstance=9f25c
4452eff4acb SIP/2.0
To: sip:123#456@192.168.100.214;user=phone;x-type=unknown;x-
plan=unknown;x-pres=allowed
```

The destination number can be manipulated when this feature is enabled. Note that if manipulation before routing is required, the * and # characters should not be used, as the device will handle them according to the above keypad protocol. For example, a manipulation rule should not be configured to add #456 to the destination number.

If manipulation **after** routing is required, the destination number to be manipulated will not include the keypad part. For example, if the manipulation rule is configured to add the suffix 888 and the received INVITE contains the number 123#456, only 123 will be manipulated and the number dialed toward the PSTN will be 123888; #456 will be sent as keypad.

To support this feature, the following new parameter has been added:

CLI: isdn-keypad-mode [ISDNKeypadMode]	Enables the device to send DTMF digits received in the called party number from the IP side as Keypad facility IE in ISDN INFORMATION messages to PSTN. ▪ [0] Don't send = (Default) All digits are sent as DTMF to PSTN (i.e., not sent as Keypad). ▪ [1] During Call Establishment = DTMF digits after * or # (inclusive) are sent as Keypad only during call establishment and call disconnect. During an established call, all digits are sent as DTMF. ▪ [2] Always = DTMF digits after * or # (inclusive) are always sent as Keypad (call establishment, connect, and disconnect). Note: This feature is not applicable to re-INVITE messages.

Applicable Products: Mediant 3000.

2.35.1.8 High-Availability Features

This section describes the new High-Availability (HA) features.

2.35.1.8.1 Software Synchronization

This feature provides support for synchronizing the active unit's installed software version (.cmp file) with the redundant unit. Up until this release, if the active unit was running a later version than the redundant unit (for whatever reason), the units could not communicate and HA was not operational. Now, in such a scenario, the active unit automatically sends the redundant unit its' software version file and the redundant unit then upgrades its software to the same version as the active unit.

Note that in scenarios where the active unit runs an earlier version (e.g., 6.8) than the redundant unit (e.g., 7.0), the redundant unit is downgraded to the same version as the active unit (e.g., 6.8). This was supported already in the previous release.

Applicable Products: Mediant 3000.

2.35.1.9 Quality of Experience Features

This section describes the new VoIP Quality of Experience (QoE) features.

2.35.1.9.1 QoE Reporting over TLS

This feature provides support for specifying a TLS certificate context (TLS Context) for a TLS connection with AudioCodes' Session Experience Manager (SEM) server for sending QoE traffic. If no TLS Context is specified, the device uses the default TLS Context (ID 0).

To support this feature, the following new parameters have been introduced:

QoE Connection by TLS CLI: configure voip > qoe configuration > tls-enable [QOEEnableTLS]	Enables a TLS connection with the SEM server. ▪ [0] Disable (default) ▪ [1] Enable Note: For this parameter to take effect, a device reset is required.
Web: QOE TLS Context Name CLI: configure voip/qoe configuration/tls-context-name [QoETLSContextName]	Selects a TLS Context (configured in the TLS Contexts table) for the TLS connection with the SEM server. The valid value is a string representing the name of the TLS Context as configured in the 'Name' field of the TLS Contexts table.

Applicable Products: Mediant 3000.

2.35.1.9.2 Call Stage for QoE Reporting

This feature provides support for configuring when to report QoE data (i.e., change in QoE status) to the SEM server. The device can be configured to report the data during the call (as was done in previous releases) or only at the end of the call. By default, the device sends call QoE status during the call. The feature can be useful when network congestion is experienced. In such a scenario, the device can be configured to send QoE status only at the end of the call, thereby reducing bandwidth usage over time.

Note that if a QoE traffic overflow between SEM and the device is experienced, the device sends the QoE data only at the end of the call, regardless of the settings of this feature.

To support this feature, the following new parameter has been introduced:

Web: QoE Report Mode CLI: report-mode [QoeReportMode]	Defines at what stage of the call the device sends the QoE data of the call to the SEM server. ▪ [0] During Call (default) ▪ [1] At End Call

Applicable Products: Mediant 3000.

2.35.1.10 Status and Performance Monitoring Features

This section describes the new VoIP performance monitoring (PM) features.

2.35.1.10.1 General

This section describes the new general SIP PM and statistics features.

2.35.1.10.1.1 Device Severity Indication in Proprietary SNMP Traps

This feature provides support for including an indication of the highest alarm severity raised by the device, in all AudioCodes' proprietary SNMP traps. The trap also indicates the current alarm raised by the device. This is supported by the addition of the new variable binding (varbind), acBoardTrapGlobalsSystemSeverity (OID:1.3.6.1.4.1.5003.9.10.1.21.1.12). The varbind reflects the highest alarm severity using the following values (integer):

- noAlarm(0)
- indeterminate(1)
- warning(2)
- minor(3)
- major(4)
- critical(5)

Applicable Products: Mediant 3000.

2.35.1.10.1.2 CDR Customization for RADIUS Accounting Requests

This feature provides support for customizing CDRs generated by the device and used for RADIUS accounting requests (e.g., for call billing purposes). The CDR fields for representing the RADIUS attributes – standard and vendor-specific (VSA) - can be customized by changing their prefix name and RADIUS attribute ID or VSA ID. The prefix can also include the equals (=) sign (e.g., connect-time=) as well as enclosed by single (') or double (") apostrophes. The prefix is an optional element for RADIUS attributes (some have a blank value).

Applicable Products: Mediant 3000.

2.35.1.10.1.3 Enhanced Logging Filters Configuration

This feature provides support for enhanced Logging Filters configuration in the existing Logging Filters table:

- Enabling and disabling Logging Filter rules. This allows the user to disable a rule without deleting it and then enabling it later when required. To support the feature, the following new parameter has been added to the Logging Filters table:

Mode mode [LoggingFilters_Mode]	Enables and disables the log filter rule. ▪ [0] Disable ▪ [1] Enable (default)

- Starting and stopping debug recordings per Logging Filter rule. Up until this release, debug recording was started and stopped globally using the 'Debug Recording Status' parameter (DebugRecordingStatus). To support the feature, the new parameter 'Mode' (LoggingFilters_Mode) has been added to the Logging Filters table, as described above
- Specifying the configuration entity by its name in the 'Value' (LoggingFilters_Value) parameter. Up until this release, the value could only be the index number of the configuration entity. For example, to specify an IP Group configured at Index 4 with the name "SIP Trunk", you can now either enter the value "4" or "SIP Trunk" (without apostrophes) in the 'Value' parameter. This new feature applies only if the 'Filter Type' (LoggingFilters_FilterType) parameter is configured to Tel-to-IP, IP-to-Tel, IP Group, SRD, Classification, IP-to-IP Routing, or SIP Interface.
- Exclamation (!) wildcard character for excluding a specific configuration entity from the filter. For example, the 'Filter Type' parameter can be configured to IP Group and then the 'Value' parameter can be set to "!2", meaning that the filter includes all IP Groups except IP Group ID 2.

  Note: For SBC calls, a Logging Filter rule applies to the entire session, which is both legs (i.e., not per leg). For example, a call between IP Groups 1 and 2 are logged for both legs even if the 'Value' parameter is configured to "!2".

Applicable Products: Mediant 3000.

2.35.1.10.2 SBC

This section describes the new SBC PM and statistics features.

2.35.1.10.2.1 Performance Monitoring SNMP MIBs for SIP Interfaces

This feature introduces the following new PM SNMP MIBs for SIP Interfaces of SBC calls:

- gwSipInterfaceINVITEDialogs: number of calls, initiated by SIP INVITEs, currently handled by the device per SIP Interface.
- gwSipInterfaceInINVITEDialogs: number of incoming calls, initiated by SIP INVITEs, currently handled by the device per SIP Interface.
- gwSipInterfaceOutINVITEDialogs: number of outgoing calls, initiated by SIP INVITEs, currently handled by the device per SIP Interface.
- gwSipInterfaceSUBSCRIBEDialogs: number of all SIP SUBSCRIBE dialogs (incoming and outgoing) currently handled by the device per SIP Interface.
- gwSipInterfaceInSUBSCRIBEDialogs: number of incoming SIP SUBSCRIBE dialogs currently handled by the device per SIP Interface.
- gwSipInterfaceOutSUBSCRIBEDialogs: number of outgoing SIP SUBSCRIBE dialogs currently handled by the device per SIP Interface.
- gwSipInterfaceOtherDialogs: number of all SIP dialogs (incoming and outgoing) other than INVITE and SUBSCRIBE (initiated by SIP REGISTER) currently handled by the device per SIP Interface.
- gwSipInterfaceInOtherDialogs: number of all incoming SIP dialogs other than INVITE

and SUBSCRIBE (initiated by SIP REGISTER) currently handled by the device per SIP Interface.

- gwSipInterfaceOutOtherDialogs: number of all outgoing SIP dialogs other than INVITE and SUBSCRIBE (initiated by SIP REGISTER) currently handled by the device per SIP Interface.
- gwSipInterfaceInDialogs: number of all incoming SIP dialogs currently handled by the device per SIP Interface.
- gwSipInterfaceOutDialogs: number of all outgoing SIP dialogs currently handled by the device per SIP Interface.
- gwSipInterfaceDialogs: number of all SIP dialogs (incoming and outgoing) currently handled by the device per SIP Interface.

Applicable Products: Mediant 3000.

2.35.1.11 Diagnostics and Troubleshooting

This section describes the new VoIP diagnostics and troubleshooting features.

2.35.1.11.1 SNMP Alarm for DSP Device Failure

This feature provides support for a new SNMP alarm, acHwFailureAlarm that is raised when any one of the device's DSP devices (and cores) fail. The alarm indicates the failed DSP device(s) number and the total number of failed cores.

Applicable Products: Mediant 3000.

2.35.1.11.2 Tag for Non-Call Session Related Logs in Syslog

This feature provides support for distinguishing between SIP call-session related logs and device operation (non-call session) related logs in Syslog messages. Up until this release, the device generated non-call session logs with the same tag type as used for call session logs (i.e., SID). Non-call session logs include logs related to device operation other than call sessions, for example, Trunk alarms, device reset, and Web login.

Non-call session related logs are now generated with the new BID tag in Syslog messaged, using the following syntax:

[BID=<last 6 characters in MAC>:<number of times device has reset>]

For example:

```
14:32:52.062: 10.33.8.70: WARNING: [S=9399] [BID=2ed1c8:96]
invalid Physical index
```

Where:

- *2ed1c8* is the device's MAC address
- *96* is the number of times the device has undergone a reset

The feature also facilitates debugging by clearly identifying the specific device (by MAC address) that sent the log message, especially useful in deployments consisting of multiple devices.

Applicable Products: Mediant 3000.

2.35.1.11.3 Device Identifier in Syslog Messages

This feature provides support for including a device identifier (MAC address) in debug log messages such as Syslog messages sent by the device. The device identifier is part of the SIP call session ID (SID) tag (and BID tag – see Section 2.35.1.11.2) in Syslog messages. The feature facilitates debugging by clearly identifying the specific device that sent the log message, especially useful in deployments consisting of multiple devices.

The new syntax of the SID tag is as follows:

[SID=<last 6 characters of device's MAC address>:<number of times device has reset>:<unique SID counter indicating session; increments consecutively for each new session; resets to 1 after a device reset>]

For example:

```
14:32:52.028: 10.33.8.70: NOTICE: [S=9369] [SID=2ed1c8:96:5]
(lgr_psbrdex)(274) recv <-- OFF_HOOK Ch:4
```

Where:

- *2ed1c8* is the device's MAC address
- *96* is the number of times the device has undergone a reset
- *5* is a unique SID number (in other words, this is the fifth session since the device last reset)

Applicable Products: Mediant 3000.

2.35.1.11.4 Maintaining Same Session ID between AudioCodes Devices

This feature provides support for maintaining the same SIP session ID (SID) and board ID (BID) in debug log messages for calls traversing multiple AudioCodes' devices. The feature is useful in that it allows the administrator to use a single SID to easily identify log messages pertaining to the same call session in such a scenario. Instead of the log messages being sent with different SIDs and BIDs per traversed device, one unique SID and BID is used throughout the call session. The SID is also used when communicating with external servers such as a Routing server, and this feature allows them to identify the same session over different devices.

To support this feature, the device can be enabled to include a proprietary SIP header, AC-Session-ID that is set to the device's SID value in SIP dialog request messages that the device initiates. All other devices (even if they have this feature disabled) receiving the SIP request, use this same SID value in their generated debug log messages. Below is an example of such a SIP header:

```
AC-Session-ID: 2ed1c8:96:5
```

For more information on how the device creates the SID/BID value, see the feature description in Section 2.35.1.11.2 on page 103.

To support this feature, the following new parameter has been added:

Web: Send AC-Session-ID header CLI: send-acsessionid [SendAcSessionIDHeader]	Enable the device to include the proprietary AC-Session-ID SIP header with its Session ID in SIP initiating dialog requests. ▪ [0] Disable (default) ▪ [1] Enable

Applicable Products: Mediant 3000.

2.35.1.11.5 Enhanced Logging of Management User Activities

This feature provides an enhanced logging of the management user's activities. Up until this release, the device could be configured to send Syslog messages reporting various activities (defined by the ActivityListToLog parameter) performed by the management user. The new feature enhances this logging functionality as follows:

- User activity logs are now stored in the device's database, enabling the administrator to query and monitor user activity logs.
- User activity logs provide the following additional information:
  - Username of Web user that performed the activity (e.g., "Admin")
  - IP address of the client PC from where the user accessed the Web interface
  - Protocol used for the Web session (e.g., SSH or HTTP)
- User activity logs can now include CLI commands that were run by the user. This is supported by a new option for the ActivityListToLog parameter: [cli] (ini). Modifications

to security-sensitive commands are logged without the entered value. (This support is not applicable to TR-069 sessions.)

- User activity logs can now include all user actions that are not related to parameter changes. The actions can include, for example, file uploads, file delete, lock-unlock maintenance actions, LDAP clear cache, register-unregister, and start-stop trunk. In the Web, these actions are typically done by clicking a button (e.g., the LOCK button). This is supported by a new option for the ActivityListToLog parameter: [ae] (ini), Action Executed (Web) and action-execute on|off (CLI).
- The 'pvc' (Parameters Value Change) option of the ActivityListToLog parameter now also reports changes in table fields (in addition to the existing support for changes in individual parameters) as well as Configuration file load. For Configuration file load, this event is reported without per-parameter notifications.
- New SNMP trap event (acActivityLog) is now sent upon detection of a user activity, enabled by the new parameter, EnableActivityTrap.
- New read-only Activity Log table (Status & Diagnostic tab > System Status menu > Activity Log) that displays user-activity logs and includes the following information:
    - Date and time the user activity was performed.
    - Description of the user activity.
    - Username of user account that performed the user activity.
    - Session management interface (e.g., HTTP).
    - IP address of the user's client PC.
- User activities of Web interface now also apply to the following:
    - Addition and deletion of table index rows.
    - User activity logs display the Web parameter names (not the ini file parameter names).

CLI: config-system > logging > activity-log [ActivityListToLog]	▪ [cli] = Logs entered CLI commands performed by user. ▪ [ae] Action Executed = Logs user actions that are not related to parameter changes. Note: Currently, the CLI option can only be configured through CLI or ini file.
Activity Trap CLI: activity-trap [EnableActivityTrap]	Enables the device to send an SNMP trap (acActivityLog) to notify of management user activities (configured by the ActivityListToLog parameter). ▪ [0] Disable (default) ▪ [1] Enable Note: Currently, this option can only be configured through CLI or ini file.

Applicable Products: Mediant 3000.

2.35.1.11.6 Play of Tones from PRT File for Test Calls

This feature provides support for playing tones from the PRT file for test calls (configured in the existing Test Call table) that are utilizing DSP resources (for whatever purpose). If the tone's coder is the same as the coder used for the test call, DSPs are not required to play the tone. If the coders are different, the device uses DSP resources to the play the tone.

Applicable Products: Mediant 3000.

2.35.1.11.7 Test Calls Configured per SIP Interface

This feature provides support for specifying the SIP Interface for test call rules. Up until this release, the SRD was specified (which is has now been replaced by SIP Interface). The feature is now compatible with the device's multiple SIP Interfaces per SRD support.

To support the feature, the Test_Call_SRD parameter has been replaced by the new Test_Call_SIPInterfaceName parameter in the Test Call table.

Applicable Products: Mediant 3000.

2.35.1.11.8 Log Filtering by SIP Interface

This feature provides support for filtering logs (Syslog or Debug Recording) by a specific SIP Interface, using the existing Logging Filters table.

To support the feature, the following ne optional value has been added to the table:

Filter Type filter-type [LoggingFilters_FilterType]	New optional value: [14] SIP Interface = Filters according to a specified SIP Interface.

Applicable Products: Mediant 3000.

2.35.1.11.9 Status of Installed Dial Plan File in CLI

This feature provides support for displaying information about the Dial Plan file installed on the device, through the device's CLI:

- Dial Plan file information: includes the file name and the names of the Dial Plans contained in the Dial Plan file. To support the feature, the following new CLI command has added (Enable mode):

  ```
  # debug auxilary-files dial-plan info
  ```

  For example, the following shows the loaded Dial Plan file and lists its defined Dial Plans:

  ```
  # debug auxilary-files dial-plan info
    File Name: dialPlan.txt
    Plans:
    Plan #0 = PLAN1
    Plan #1 = PLAN2
  ```

  Note that the index number of the first Dial Plan is 0.

- Checking whether a specific prefix number is defined in a specific Dial Plan number. If the Dial Plan is used for tags, the command also shows the tag. To support the feature, the following new CLI command has been added (Enable mode):

  ```
  # debug auxilary-files dial-plan match-number <Dial Plan
  number> <prefix number>
  ```

  For example, the following checks whether the called prefix number 2000 is defined in Dial Plan 1, which is used for obtaining the destination IP address (tag):

  ```
  # debug auxilary-files dial-plan match-number PLAN1 2000
  Match found for 4 digits
  Matched prefix: 2000
  Tag: 10.33.45.92
  ```

Applicable Products: Mediant 3000.

2.35.1.11.10 User-Info File Name Display in CLI

This feature provides support for displaying the file name of the User-Info file installed on the device, through the device's CLI. To support the feature, the following new CLI command has added (Enable mode):

```
# debug auxilary-files user-info info
```

For example:

```
# debug auxilary-files user-info info
  User Info File Name users.txt
```

Applicable Products: Mediant 3000.

2.35.1.12 New Management Platform Features

This section describes the new management platform features.

2.35.1.12.1 General Management

This section describes the new general management features.

2.35.1.12.1.1 Automatic Provisioning of License Feature Key

This feature provides support for updating the device's Software License Key through automatic provisioning (Auto-Update feature). The feature is enabled by configuring the URL of the server on which the License file is located. During automatic provisioning, once the device downloads the file, it checks that the serial number indicated in the file (“S/N <serial number>") is the same as that of the device. If the serial number is the same, it applies the new License Key if it is different to the currently installed one. For devices in HA mode, the License Key is applied to both active and redundant units. Once the License Key file has been downloaded to the device, the device does not download it in any subsequent automatic update processes.

To support the feature, the following new parameter has been added:

`configure system > automatic-update > feature-key` [FeatureKeyURL]	Defines the URL to the server where the License Key is located for updating the License Key during automatic provisioning. Once the device downloads the file, the parameter reverts to its default value (i.e., no URL is defined) to avoid the device from downloading the file again in subsequent automatic update processes.

Applicable Products: Mediant 3000.

2.35.1.12.1.2 File Template for Automatic Provisioning

This feature provides support for facilitating the setup of the device's automatic provisioning (Automatic Update) feature. Another benefit of the feature is that the URLs defining the address to the servers on which the Auxiliary files (e.g., CPT, Dial Plan and License Key) are located are always retained; up until now, once the device downloaded an Auxiliary file, the URL (configured by a file-specific parameter) was deleted and thus, the device would never attempt to download the specific Auxiliary file type in future automatic update processes.

The feature includes the following quick-and-easy automatic provisioning setup steps:

1. Defining the file types to download for automatic provisioning. This is configured using the new parameter, AupdFilesList. Each file type is specified using special characters. For example, "ini" for ini file, "usrinf" for User Info file, and "fk" for feature key file (refer to User's Manual for complete list).
2. Defining the URL to the remote server on which the files are located. This is configured using the new parameter, TemplateUrl. The file name in the URL uses a special tag, "<FILE>" to represent each file type. The device automatically replaces the tag with hardcoded file names and extensions specific to each file type (refer to User's Manual for complete list) specified in the AupdFilesList parameter. For example, if the TemplateUrl parameter is configured to "http://10.8.8.20/Site1_<FILE**>**" and the AupdFilesList parameter to "ini,fk,cpt", the device will download files form the following URLs:
    - http://10.8.8.20/Site1_**device.ini**
    - http://10.8.8.20/Site1_**fk.ini**
    - http://10.8.8.20/Site1_**cpt.data**
3. Placing the files to download on the provisioning server and ensuring that their file names are based on the hardcode tag replacements (e.g., "Site1_device.ini" for the ini

file).

At the end of the automatic update process, the TemplateUrl settings are retained for future automatic updated processes. If a URL is configured for a file using a parameter specific to the file (e.g., CptFileURL), the settings of the TemplateUrl parameter is ignored for the specific file type.

To support the feature, the following new parameter has been added:

`configure system > automatic-update > template-url` [TemplateUrl]	Defines the URL of the provisioning server on which the files to download for automatic updates are located.
`configure system > automatic-update > template-files-list` `[AupdFilesList]`	Defines the list of file types to download from the provisioning server. The <File> tag in the URL defined by the TemplateUrl parameter is replaced by a file name-extension for each file type.

Applicable Products: Mediant 3000.

2.35.1.12.1.3 Associations between Tables using Names instead of Indices

This feature provides a change in the way index rows of tables are associated with each other. Up until this release, the association was done using the table row index number (ID); now, the name of the table row is used instead. For example, a Proxy Set is assigned to an IP Group in the IP Group table using the name of the Proxy Set and not the ID.

To support the feature, the parameters used for associating tables with each other now require a name value and not an ID (i.e., index number). To facilitate configuration in the Web interface, a drop-down list is provided from where the name can be selected. Therefore, when configuring a configuration entity, it is now mandatory for the administrator to define it with a name (unique). If a name is not defined, the device automatically assigns it a unique name using the following syntax: *<configuration entity>_<next available table index>*. For example, a new IP Profile is automatically assigned the name "IpProfile_1", where *1* represents the row index number. The next configured entry would be assigned the name "IpProfile_2", and so on.

Due to the feature, the Message Policy table provides a new parameter—MessagePolicy_Name—that defines a name for the Message Policy rule and which is used to associate the rule to other entities (e.g., SIP Interface). In addition, the table below lists the parameters whose required value has been changed from an ID to a name:

Table	Old Parameter Name	New Parameter Name
NAT Translation	Source Interface Name [NATTranslation_SourceIPInterfaceName]	Source Interface [NATTranslation_SrcIPInterfaceName]
Test Call	▪ IP Group ID [Test_Call_IPGroupID] ▪ SRD [Test_Call_SRD]	▪ IP Group [Test_Call_IPGroupName] ▪ SIP Interface [Test_Call_SIPInterfaceName]
SIP Recording	▪ Recorded IP Group ID [SIPRecRouting_RecordedIPGroupID] ▪ Peer IP Group ID [SIPRecRouting_PeerIPGroupID] ▪ Recording Server (SRS) IP Group ID [SIPRecRouting_SRSIPGroupID]	▪ Recorded IP Group [SIPRecRouting_RecordedIPGroupName] ▪ Peer IP Group [SIPRecRouting_PeerIPGroupName] ▪ Recording Server (SRS) IP Group [SIPRecRouting_SRSIPGroupName]
Trunk Group	Tel Profile ID [TrunkGroup_ProfileId]	Tel Profile Name [TrunkGroup_ProfileName]
Trunk Group Settings	Serving IP Group ID [TrunkGroupSettings_ServingIPGroup]	Serving IP Group [TrunkGroupSettings_ServingIPGroupName]
Inbound IP Routing	▪ IP Profile ID [PstnPrefix_ProfileId]	▪ IP Profile [PstnPrefix_ProfileName]

Table	Old Parameter Name	New Parameter Name
	▪ Source IP Group ID [PstnPrefix_SrcIPGroupID]	▪ Source IP Group [PstnPrefix_SrcIPGroupName]
Outbound IP Routing (Tel to IP Routing)	▪ IP Profile ID [PREFIX_ProfileId] ▪ Src IP Group ID [PREFIX_SrcIPGroupID] ▪ Dest IP Group ID [PREFIX_DestIPGroupID]	▪ IP Profile [PREFIX_ProfileName] ▪ Source IP Group [PREFIX_SrcIPGroupName] ▪ Dest IP Group [PREFIX_DestIPGroupName]
Source Phone Number Manipulation Table for Tel-to-IP Calls	▪ Source IP Group [NumberMapTel2Ip_SrcIPGroupID] ▪ Destination IP Group [NumberMapTel2Ip_DestIPGroupID]	▪ Source IP Group [NumberMapTel2Ip_SrcIPGroupName] ▪ Destination IP Group [NumberMapTel2Ip_DestIPGroupName]
Source Phone Number Manipulation Table for IP-to-Tel Calls	Source IP Group [SourceNumberMapIp2Tel_SrcIPGroupID]	Source IP Group [SourceNumberMapIp2Tel_SrcIPGroupName]
Redirect Number IP-to-Tel	Source IP Group ID [RedirectNumberMapTel2Ip_SrcIPGroupID]	Source IP Group [RedirectNumberMapIp2Tel_SrcIPGroupID]
Calling Name Manipulation Table for Tel-to-IP Calls	Source IP Group ID [CallingNameMapTel2Ip_SrcIPGroupID]	Source IP Group [CallingNameMapTel2Ip_SrcIPGroupName]
SIP Interface	▪ SRD [SIPInterface_SRD] ▪ Message Policy [SIPInterface_MessagePolicy]	▪ SRD [SIPInterface_SRDName] ▪ Message Policy [SIPInterface_MessagePolicyName]
Proxy Sets	▪ SRD Index [ProxySet_SRD] ▪ TLS Context ID [ProxySet_TLSContext]	▪ SRD [ProxySet_SRDName] ▪ TLS Context Name [ProxySet_TLSContextName]
IP Group	▪ Proxy Set ID [IPGroup_ProxySetId] ▪ SRD [IPGroup_SRD] ▪ IP Profile ID [IPGroup_ProfileId]	▪ Proxy Set [IPGroup_ProxySetName] ▪ SRD [IPGroup_SRDName] ▪ IP Profile [IPGroup_ProfileName]
Account	▪ Served IP Group [Account_ServedIPGroup] ▪ Serving IP Group [Account_ServingIPGroup]	▪ Served IP Group [Account_ServedIPGroupName] ▪ Serving IP Group [Account_ServingIPGroupName]
Classification	▪ Message Condition [Classification_MessageCondition] ▪ Source SRD ID [Classification_SrcSRDID] ▪ Source IP Group ID [Classification_SrcIPGroupID]	▪ Message Condition [Classification_MessageConditionName] ▪ SRD [Classification_SRDName] ▪ Source IP Group [Classification_SrcIPGroupName]
IP-to-IP Routing	▪ Source IP Group ID [IP2IPRouting_SrcIPGroupID] ▪ Message Condition [IP2IPRouting_MessageCondition] ▪ ReRoute IP Group ID [IP2IPRouting_ReRouteIPGroupID]	▪ Source IP Group [IP2IPRouting_SrcIPGroupName] ▪ Message Condition [IP2IPRouting_MessageConditionName] ▪ ReRoute IP Group [IP2IPRouting_ReRouteIPGroupName]

Table	Old Parameter Name	New Parameter Name
	▪ Destination IP Group ID [IP2IPRouting_DestIPGroupID]	▪ Destination IP Group [IP2IPRouting_DestIPGroupName]
IP to IP Inbound Manipulation	Source IP Group ID [IPInboundManipulation_SrcIpGroup]	Source IP Group [IPInboundManipulation_SrcIPGroupName]
IP to IP Outbound Manipulation	▪ Source IP Group ID [IPOutboundManipulation_SrcIPGroupID] ▪ Destination IP Group ID [IPOutboundManipulation_DestIPGroupID] ▪ ReRoute IP Group ID [IPOutboundManipulation_ReRouteIPGroupID] ▪ Message Condition [IPOutboundManipulation_MessageCondition]	▪ Source IP Group [IPOutboundManipulation_SrcIPGroupName] ▪ DestinationIP Group [IPOutboundManipulation_DestIPGroupName] ▪ ReRoute IP Group [IPOutboundManipulation_ReRouteIPGroupName] ▪ Message Condition [IPOutboundManipulation_MessageConditionName]
Admission Control	▪ IP Group ID [SBCAdmissionControl_IPGroupID] ▪ SRD ID [SBCAdmissionControl_SRDID]	▪ IP Group [SBCAdmissionControl_IPGroupName] ▪ SRD [SBCAdmissionControl_SRDName]
SBC User Info	IP Group ID [SBCUserInfoTable_IPGroupID]	IP Group [SBCUserInfoTable_IPGroupName]

Applicable Products: Mediant 3000.

2.35.1.12.1.4 Invalid Table Rows Retained after Device Reset

This feature provides support for retaining invalid table rows after a device reset. Up until this release, all invalid table rows were deleted after a device reset. In addition, invalid table rows are now highlighted in red in the Web interface and prefixed with an exclamation mark (!) in the ini file as shown in the example below:

```
!CpMediaRealm 1 = "ITSP", "Voice", "", 60210, 2, 6030, 0, "", "";
```

Invalid table rows in the CLI are displayed with the message, "The following line is not active".

Applicable Products: Mediant 3000.

2.35.1.12.1.5 Online SIP Configuration during Active Calls

This feature provides support for a change in device behavior when SIP VoIP configuration entities that are associated with active calls are modified or deleted. The device immediately terminates ("drops") the calls upon the following configuration scenarios:

- SIP Interface (SIP Interface table):
  - SIP Interface is deleted.
  - Network interface assigned to the SIP Interface (in the 'Network Interface' field) is modified or deleted in the Interface table.
  - Modifications to the 'Application Type', 'UDP/TCP/TLS Port', or 'SRD' fields.
- IP Group (IP Group table):
  - IP Group is deleted.
  - Modifications to the 'Type' or 'SRD Name' fields.

  Note: All users pertaining to this IP Group are removed from the device's users database.

Applicable Products: Mediant 3000.

2.35.1.12.1.6 Increase in Maximum Number of Table Indices

This feature provides support for an increase in the maximum number of rows (indices) that can be configured in the tables below. The values enclosed in parenthesis indicate the maximum configurable rows in the previous release.

Table	Mediant 3000
Logging Filters Table	60 (30)
SRD	33 (unchanged)
SIP Interface	32 (unchanged)
IP Group	33 (unchanged)
Proxy Sets	100 (unchanged)
Proxy IP	330 (unchanged)
Account	32 (unchanged)
Message Policy	5 (unchanged)
Message Manipulations	80 (unchanged)
IP Profile Settings	10 (unchanged)
Coders Group / Coders	11 (unchanged)
Allowed Coders Group / Coders	10 (5)
Admission Control	100 (unchanged)
Classification	20
Message Condition	20 (unchanged)
IP-to-IP Routing	200 (unchanged)
SBC Alternative Routing Reasons	20 (unchanged)
IP-to-IP Inbound Manipulation	100 (unchanged)
IP-to-IP Outbound Manipulation	100 (unchanged)

Applicable Products: Mediant 3000.

2.35.1.12.1.7 Increase in Maximum Character Length of String Values

This feature provides support for an increase in the maximum number of characters to 40 for configuring the string values of the following parameters:

- Trunk Group Settings table - Trunk Group Name [TrunkGroupSettings_TrunkGroupName]
- IP Profile table - Profile Name [IpProfile_ProfileName]
- IP Group table - Description [IPGroup_Description]

- SRD table - SRD Name [SRD_Name]
- IDS Policy table - Name [IDSPolicy_Name]
- Cost Group table - Cost Group Name [CostGroupTable_CostGroupName]

Applicable Products: Mediant 3000.

2.35.1.12.1.8 Feature Key for ELIN Functionality

The device's ELIN functionality support (for the SBC and Gateway applications) is now an orderable item, requiring the Software Upgrade Key installed on the device to include the Feature Key (license) that enables the functionality. The device's ELIN functionality provides interoperability between Microsoft Lync Server and an E9-1-1 emergency service provider (SIP Trunk or ISDN/CAMA).

Applicable Products: Mediant 3000.

2.35.1.12.1.9 Notification to Select SRD before Cloning

This feature provides support for displaying a message to the Web user to inform the user to first select an SRD in the SRD table before clicking the **Clone** button. The message is displayed when the user clicks the button without selecting an SRD.

Applicable Products: Mediant 3000.

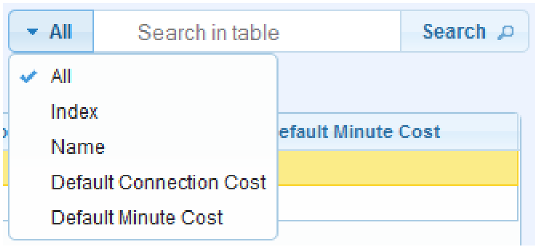
2.35.1.12.2 Web-based Management Features

This section describes the new Web-based management features.

2.35.1.12.2.1 Enhanced Table Design of Configuration Tables

This feature provides support for an enhanced design of the configuration tables:

- Searching table entries: The administrator can now search for any value (string or IP address) in configuration tables, using the new Search box. The search can be filtered by table index row or column. By default, searches are performed on all columns. To quit the search mode, the new End Search button must be clicked. The figure below displays an example of the Search feature:

  Note that this feature does not apply to the TLS Contexts table and Web Users table.
- Sorting items in a table column in ascending or descending order. This is done by clicking the column heading name that you want ordered. Each time you click the column heading, it toggles between ascending and descending order, indicated by the up-down arrow displayed alongside the column's heading name. The up-pointing arrow indicates that the column is ordered in ascending order (e.g., 1, 2, 3 and so on); the down-pointing arrow indicates that the column is ordered in descending order. By default, tables are sorted in ascending order according to the Index column, except for the following tables (to facilitate multi-tenancy configuration):
  - IP-to-IP Routing table – sorted by Routing Policy
  - SBC Manipulation tables – sorted by Routing Policy
  - Classification table - sorted by SRD
- Changing index position of existing rows. When a specific index row is selected, the row can be moved up or down by clicking the new Up and Down buttons, respectively.

The index number of the row changes according to its new position in the table. The row that previously occupied the index row and all rows below it are moved one index down in the table.

Note that this feature is supported only for certain tables.

- Row Insertion anywhere in a table. A new row can be inserted at any existing (configured) index number, using the new Insert button. When the row is inserted, the row that previously occupied the index row and all rows below it are moved one index down in the table.

  Note that this feature is supported only for certain tables.

- Display format for Add and Edit dialog boxes. Dialog boxes can be displayed in Classic (default) or Tab view. Classic view displays a list of all the parameters; Tab view displays the parameters grouped under tabs (e.g., Rule, Action, and Status). This is supported by the Classic View / Tabs View link located at the bottom of the dialog boxes, which toggles between these display views.
- The following additional tables have been aligned with the table design format introduced in Release 6.6:
  - Proxy Sets table
  - Trunk Group Settings table
  - Inbound IP Routing Table
  - Tel to IP Routing Table
  - Charge Code table
- The Submit button that appeared in configuration tables when clicking the Add or Edit buttons has been replaced by the Add button.

Applicable Products: Mediant 3000.

2.35.1.12.2.2 Filtering Configuration Tables by SRD

This feature provides support for filtering configuration table rows by SRD. When an SRD is selected for filtering, the Web interface displays only table rows that are associated with the selected SRD. This feature is useful in multi-tenant setups where multiple SRDs may be configured, eliminating configuration clutter from other SRDs.

To support this feature, the new SRD Filter drop-down list box has been added to the Web interface's toolbar (located on the far right). In addition, if the filter is set on a specific SRD and a new row is being added to a configuration table, the filtered SRD is automatically selected as the associated SRD (in the 'SRD' field) in the Add Row dialog box. In addition, all other fields in the Add Row dialog box that are associated with the SRD, for example Routing Policy, are also automatically selected.

Applicable Products: Mediant 3000.

2.35.1.12.2.3 Color-Coding of SRDs

This feature provides support for color-coding SRDs throughout the Web interface. Whenever a new SRD is configured in the SRD table, the device automatically allocates it a unique color to distinguish it from other SRDs. The color is displayed in a box alongside the SRD's name. Wherever an SRD is assigned to a configuration entity in a table, the field that is used to assign the SRD displays the colored box alongside the SRD's name, as shown in the example below:

Index	Name	Sharing Policy	SBC Operation Mode	SBC Routing Policy	Max. Number of Registered Users	Block Unregistered Users
0	DefaultSRD (#0)	Shared	B2BUA	Default_SBCRouting	-1	No
1	SRD_1 (#1)	Shared	B2BUA	NY	-1	No
2	SRD_2 (#2)	StandAlone	B2BUA	None	-1	No

Page 1 of 1 10 View 1 - 3 of 3

Applicable Products: Mediant 3000.

2.35.1.12.2.4 Removal of Configuration Entities Associated with Deleted SRD

This feature provides support for removing table rows of configuration entities that are associated with an SRD that has been deleted. SRD-associated configuration entities include, for example, Proxy Sets, SIP Interfaces, IP Groups, Classification rules, Admission Control rules, and Routing Policy rules.

In addition, if a Routing Policy is deleted, all table rows of configuration entities that are associated with it are also automatically removed. These entities include, for example, IP-to-IP Routing rules, IP-to-IP Inbound Manipulation rules, and IP-to-IP Outbound Manipulation rules.

Applicable Products: Mediant 3000.

2.35.1.12.2.5 Automatic Field Configuration based on SRD

This feature provides support for automatically setting the value of fields in tables according to SRD or associated SRD. For example, when adding a rule in the IP-to-IP Routing table and a Routing Policy is selected, the IP Groups listed in the Source and Destination IP Group fields list only the IP Groups associated with the SRD to which the Routing Policy is assigned (and IP Groups belonging to a shared SRD, if exists). This behavior is supported throughout the entire Web interface and facilitates configuration, eliminating possible flaws in configuration due to invalid associations between configuration entities.

In addition, in configurations implementing only a single SRD, the device automatically selects this SRD when adding related configuration entities. For example, when adding an IP Group, the single SRD is automatically selected in the Add Row dialog box.

Applicable Products: Mediant 3000.

2.35.1.12.2.6 Restore Device to Factory Defaults

This feature provides support for restoring the device to factory defaults, through the Web interface. The feature is supported by the new "Restore All Defaults" button on the Configuration File page (Maintenance tab > Software Update > Configuration File).

Applicable Products: Mediant 3000.

2.35.1.12.2.7 Proxy IP List Separated from Proxy Set Table

This feature introduces the new Proxy Address table for configuring the addresses of proxy servers belonging to Proxy Sets. The new table is a "child" of the Proxy Sets table. Up until this release, the addresses where configured in the Proxy Sets table.

For each selected Proxy Set table index, the Proxy Address Table link appears at the bottom of the Proxy Sets table, which opens the Proxy Address table for that Proxy Set.

To support this feature, the following new table parameter has been added and table parameter modified:

Proxy Address Table CLI: configure voip > voip-	New table: [ProxyIp]

network proxy-ip [ProxyIp]	FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex, ProxyIp_IpAddress, ProxyIp_TransportType; [\ProxyIp]
Proxy Sets Table CLI: configure voip > control-network proxy-set [ProxySet]	Modification: ProxyIp_IpAddress and ProxyIp_TransportType parameters were moved to the new Proxy IP table. [ProxySet] FORMAT ProxySet_Index = ProxySet_ProxyName, ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContext, ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName, ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName, ProxySet_SASIPv6SIPInterfaceName; [\ProxySet]

Applicable Products: Mediant 3000.

2.35.1.12.2.8 Existing Parameters Now Configurable through Web Interface

This feature provides support for configuring the following parameters, supported in the previous release by other management platforms, through the Web interface:

ini Parameter	Web Parameter
SyslogCpuProtection	Syslog CPU Protection (Syslog Settings page)
SyslogOptimization	Syslog Optimization (Syslog Settings page)
RADIUSTo	RADIUS Response Time Out (Authentication Settings page)
RADIUSRetransmission	RADIUS Packets Retransmission (Authentication Settings page)
TrunkStatusReportingMode	Trunk Status Reporting (Digital Gateway Parameters page)
IPGroup_MsgManUserDef1	Msg Man User Defined String1
IPGroup_MsgManUserDef2	Msg Man User Defined String2

Applicable Products: Mediant 3000.

2.35.1.12.2.9 Miscellaneous GUI Changes

The following miscellaneous modifications have been made to the Web interface:

- The "GW & IP to IP" menu in the Navigation tree has been changed to "Gateway".
- The RouteModeTel2IP parameter has been moved from the Tel to IP Routing table to the Routing General Parameters page.
- The RouteModeIP2Tel parameter has been moved from the IP to Trunk Group Routing table to the Routing General Parameters page.
- The location of the time and date parameters (including NTP) has changed:
  - Regional Settings page has been renamed "Time and Date".
  - NTP-related parameters have been moved to the new Time and Date page.
- The optional values of the Log Destination parameter (LoggingFilters_LogDestination) in the Logging Filters table have changed:

- Syslog to "Syslog Server"
- Debug Recording to "Debug Recording Server"

- New submenu under the System menu called Call Detail Record (Configuration tab > System menu > Call Detail Record). The menu includes the following items:
    - Call Detail Record Settings: Includes the Syslog CDR parameters (previously on the Advanced Parameters page) and the RADIUS CDR parameters (previously on the RADIUS Accounting Settings page).
    - Gateway CDR Format (previously under Configuration tab > VoIP System menu > Services > Call Detailed Record)
    - SBC CDR Format (previously under Configuration tab > VoIP System menu > Services > Call Detailed Record)

2.35.2 Known Constraints

Constraints discovered in this GA version include the following:

2.35.2.1 SIP Constraints

This release includes the following known SIP constraints:

1. As Version 7.0 requires unique names to be configured for rows pertaining to a table, software upgrade from Version 6.8 to Version 7.0 may fail if any of the following tables have rows that were configured with the same name:
    - Tel Profile Settings table: TelProfile_ProfileName
    - IP Profile Settings table: IpProfile_ProfileName
    - Proxy Sets table: ProxySet_ProxyName
    - SRD table: SRD_Name
    - SIP Interface table: SIPInterface_InterfaceName
    - Bandwidth Profile: BWProfile_Name

    Applicable Products: Mediant 3000.

1. Whatever the customer has ordered regarding the number of far-end users (FEU), for example, 100, the customer needs to make sure that the installed Feature Key shows a figure that is double this ordered number, for example, 200.

    Applicable Products: Mediant 3000.

2. The device does not support the transmission of RTP bundling (multimedia sessions). By default, the device removes all bundle-related attributes ('a=group:BUNDLE' and 'a=ssrc') from the SDP offer and answer. Instead, the device uses different ports for each media type (audio and video).

    Applicable Products: Mediant 3000.

3. CLI scripts used in Version 6.8 are not fully supported and need to be modified in order to be fully compatible in Version 7.0.

    Applicable Products: Mediant 3000.

4. Downgrade from Version 7.0 to a previous software version only works if the device was upgraded to Version 7.0 and no configuration changes were done after the upgrade.

    Applicable Products: Mediant 3000.

5. The combination of SBC direct media and termination features such as the handling of 3xx, REFER, and INVITE with Replaces is not supported.

    Applicable Products: All SBC Supporting Products.

6. SBC Delayed SDP offer is supported only by devices that support DSP transcoding.

    Applicable Products: All SBC Supporting Products.

7. The device cannot run both the SAS and SBC applications (i.e., only one of them must

be enabled).

Applicable Products: All SBC Supporting Products.

8. High Availability (HA) for WebRTC and One-Voice Resiliency is not fully supported (signaling may not function correctly in certain scenarios).

   Applicable Products: Mediant 3000.

9. The SBC User Info table limits the maximum number of users that can be configured (half of the maximum per device).

   Applicable Products: All SBC Supporting Products.

10. The out-of-dialog SIP REFER message for SBC calls is forwarded transparently; the subsequent NOTIFY message is not fully supported.

    Applicable Products: All SBC Supporting Products.

11. The Jitter Buffer for SBC calls can be configured on both legs (with or without DSPs) only when using G.711. For coders other than G.711, the Jitter Buffer can only be configured for one specific leg, which must have DSPs.

    Applicable Products: Mediant 3000.

12. When SBC termination features are used so that the device handles them locally (i.e., 'Remote Can Play Ringback', 'Play Held Tone', and 'Play RBT To Transferee'), Extension Coders Group ID must be configured, even if only one coder is used. This is especially relevant for the RBT to transferee feature.

    Applicable Products: All SBC Supporting Products.

13. To configure IP-to-IP inbound manipulation for SAS, the IP-to-IP Inbound Manipulation table of the SBC application must be used. This table is available in the Web interface only if the SBC application is enabled and if the device is installed with the SBC Feature Key.

    Applicable Products: Mediant 3000.

14. For the Tel-to-IP Call Forking feature (supported by the Gateway application), if a domain name is used as the destination in the Tel to IP Routing table, the maximum number of resolved IP addresses supported by the device's internal DNS that the call can be forked to is three (even if four IP addresses are defined for the domain name).

    Applicable Products: Mediant 3000.

15. The AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol can only be configured using *ini* file parameters.

    Applicable Products: Mediant 3000.

16. Publishing of RTCP XR is sent only at call termination.

    Applicable Products: Mediant 3000.

17. The device crashes and then resets when a Dial Plan index is configured for a Tel Profile and the destination number is not defined in the Dial Plan file for that index.

    The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

    SR: 765891

    Applicable Products: Mediant 3000.

18. The device truncates long SDP bodies in Syslog messages when Syslog optimization (merging multiple debug messages into a single UDP packet) is enabled, making it difficult for administrator's to diagnose media negotiation.

    The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

    SR: 750581

    Applicable Products: Mediant 3000.

2.35.2.2 Media Constraints

This release includes the following known media (voice, RTP and RTCP) constraints:

1. SBC RTP call forwarding using the SRTP tunneling feature cannot provide RTCP XR monitoring parameters (such as MOS) required for the QoE feature on the following variable bit rate coders: G.723, GSM FR, GSM EFR, MS RTA, EVRC, AMR, QCELP, and Speex. A workaround is to use SRTP full encryption / decryption on the forwarding calls.

   Applicable Products: Mediant 3000.

2. Ethernet packets received on the RTP side of SRTP-RTP SBC sessions must not exceed 1500 bytes. Packets exceeding this size are dropped.

   Applicable Products: Mediant 3000.

3. Video sessions cannot be transported on SBC RTP forwarding calls.

   Applicable Products: Mediant 3000.

4. The Enhanced G.711 vocoder is no longer supported.

   Applicable Products: Mediant 3000.

5. The device does not support the sending of RFC 2198 RTP redundancy packets as an operation if the configured packet loss threshold is exceeded; this is configured in the Quality Of Experience Web page.

   Applicable Products: Mediant 3000.

6. Acoustic Echo Suppression cannot be used together with wideband transcoding. When Acoustic Echo Suppression is enabled, IP-to-IP calls using wideband coders such as G.722 or AMR-WB do not maintain the wideband quality and consequently, is degraded to narrowband quality.

   Applicable Products: Mediant 3000.

7. If the initial transcoding session has one side using a narrowband coder (e.g. G.711), modifying the transcoding connection to wideband coders still results in narrowband voice quality. A workaround for this constraint is to ensure that the entire session uses wideband coders.

   Applicable Products: Mediant 3000.

8. The Transparent coder (RFC 4040) poses the following limitations:

   - The coder can be used only when using physical terminations
   - No detection of IBS (e.g., DTMF)
   - Generation of IBS is only toward the network
   - No fax/modem detection or generation (i.e., no support for T.38 and Bypass)

   A workaround for this constraint is to use the G.711 coder instead.

   Applicable Products: Mediant 3000.

9. When performing an IP-to-IP call with a wideband (WB) coder on each leg, if the Fax/Modem Transport type for one of the legs is not Transparent, the interconnection is made using a narrowband coder; therefore, the wideband quality of the call is not maintained. The user should avoid setting any Fax/Modem enhanced capabilities on wideband IP-to-IP calls for which the user wants to maintain wideband quality.

   Applicable Products: Mediant 3000.

10. Announcements and streaming cannot be performed on IP-to-IP wideband calls.

    Applicable Products: Mediant 3000.

11. The RFC 2198 Redundancy mode with RFC 2833 is not supported (i.e., if a complete DTMF digit is lost, it is not reconstructed). The current RFC 2833 implementation supports redundancy for lost inter-digit information. Since the channel can construct the entire digit from a single RFC 2833 end packet, the probability of such inter-digit information loss is very low.

    Applicable Products: Mediant 3000.

12. The duration resolution of the On and Off time digits when dialing to the network using RFC 2833 relay is dependent on the basic frame size of the coder being used.

    Applicable Products: Mediant 3000.

13. The Calling Tone (CNG) detector must be set to Transparent mode to detect a fax CNG tone received from the PSTN, using the Call Progress Tone detector.

    Applicable Products: Mediant 3000.

14. EVRC Interleaving according to RFC 3558 is supported only on the receiving side. Supporting this mode on the transmitting side is not mandatory according to this RFC.

    Applicable Products: Mediant 3000.

15. To change the DSP template, either the Mixed Template table or the DSP Template single values can be used.

    Applicable Products: Mediant 3000.

2.35.2.3 PSTN Constraints

This release includes the following known PSTN constraints:

1. All the device's trunks must belong to the same Protocol Type (i.e., either E1 or T1).

   Applicable Products: Mediant 3000.

2. After changing the trunk configurations from the initial factory default (i.e., trunks are of Protocol Type 'None'), a device reset is required (i.e., the change cannot be made on-the-fly).

   Applicable Products: Mediant 3000.

3. When configuring the framing method to 'Extended Super Frame' (0) or 'Super Frame' (1), the framing method is converted to another framing method. The correct value that is updated in the device is displayed in the Web interface:

   - For E1: 'Extended Super Frame' (0) and 'Super Frame' (1) are converted to 'E1 FRAMING MFF CRC4 EXT' (c).
   - For T1: 'Extended Super Frame' (0) is converted to 'T1 FRAMING ESF CRC6' (D). In addition, 'Super Frame' (1) is converted to 'T1 FRAMING F12' (B).

   Applicable Products: Mediant 3000.

4. When configuring the device with E1 trunks, negotiation of CRC4 (for either EXTENDED_SUPER_FRAME or E1_FRAMING_MFF_CRC4_EXT framing methods) should not be used. A framing method other than EXTENDED_SUPER_FRAME and E1_FRAMING_MFF_CRC4_EXT must be selected.

   Applicable Products: Mediant 3000 with TP-6310.

2.35.2.3.1 DS3 Constraints

This release includes the following known DS3 constraints:

1. The BIT voice path can fail when using the DS3 interface.

   Applicable Products: Mediant 3000 with TP-6310.

2. When the DS3 interface is not connected, a trunk under this DS3 interface can appear in either LOF or AIS alarm state.

   Applicable Products: Mediant 3000 with TP-6310.

3. The DS3 External clock is not relevant for Asynchronous mapping of DS3 in OC3.

   Applicable Products: Mediant 3000 with TP-6310.

2.35.2.3.2 SONET / SDH Constraints

This release includes the following known SDH constraints:

1. The BIT voice path may fail when using the SONET interface in byte-synchronous mode.

   Applicable Products: Mediant 3000 with TP-6310.

2. For SDH/SONET and DS3 interfaces, if a trunk is in LOF alarm and the alarm is then cleared, the trunk tends to revert to the RAI alarm for a short period before moving to "no alarm" state.

   Applicable Products: Mediant 3000 with TP-6310.

3. In STM-1 and OC3 configurations, path alarms do not show the correct state if the higher level is not synchronized. For example, if there is no LOS on both PSTN Port A and Port B, the path level displays "No Alarm".

   Applicable Products: Mediant 3000 with TP-6310.

2.35.2.4 High-Availability Constraints

This release includes the following known High-Availability (HA) constraints:

1. When using IPSec for control protocol transport, the device may experience a large bulk of Syslog error messages during switchover. These messages can be ignored as the switchover should succeed and the connection with the softswitch is restored.

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

2. During HA switchover, the APS active interface status (e.g., PSTN-B is currently "Active" and PSTN-A is "Inactive") is not transferred to the redundant blade. As a result, if the PSTN-B interface was active before switchover, PSTN-A can be active after switchover. The information regarding which interface is active is not maintained after switchover.

   Applicable Products: Mediant 3000 HA with TP-6310.

3. Incorrect error message (HAProcessNode) is generated in Syslog messages during High-Availability (HA) switchover from active to redundant unit.

   The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

   SR: N/A

   Applicable Products: Mediant 3000/TP-8410.

4. In some scenarios, after an HA switchover from active to redundant unit, the device stops sending debug recording packets to the configured destination IP address. A workaround is to configure the destination IP address manually or configure debug recording packets to be saved to the device's memory.

   The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

   SR: N/A

   Applicable Products: Mediant 3000/TP-8410.

2.35.2.5 Infrastructure Constraints

This release includes the following known infrastructure constraints:

1. When using BITS with line-synch mode, only APS protected mode is supported.

   Applicable Products: Mediant 3000 with TP-6310.

2. The following parameters do not return to their default values when attempting to restore them to defaults using the Web interface or SNMP, or when loading a new *ini* file using BootP/TFTP:

   - VLANMode
   - VLANNativeVLANID
   - EnableDHCPLeaseRenewal
   - IPSecMode
   - CASProtocolEnable
   - EnableSecureStartup

Applicable Products: Mediant 3000.

3. Files loaded to the device must not contain spaces in their file name. Including spaces in the file name prevents the file from being saved to the device's flash memory (or copied to the redundant blade for Mediant 3000 HA).

   Applicable Products: Mediant 3000.

2.35.2.6 Security Constraints

This release includes the following known security constraints:

1. When the device is upgraded from Version 6.6 to Version 6.8, the certificates currently loaded on the device become corrupted (truncated). As a result, the device is unable to establish secure connections (e.g., TLS or HTTPS). A workaround is to re-load the original certificates to the device.

   The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

   SR: N/A

   Applicable Products: Mediant 3000.

2.35.2.7 Management Constraints

2.35.2.7.1 General Management Constraints

This release includes the following known general management constraints:

1. Configuration file constraints when upgrading from 6.8 to 7.0:
   - CLI Script file of 6.8 cannot be loaded to a 7.0 device.
   - Incremental ini file of 6.8 cannot be loaded to a 7.0 device.

   Applicable Products: Mediant 3000.

2. When implementing automatic provisioning (update), the device fails to resolve the FQDN, defined by the IniFileUrl parameter, of the TFTP server and as a result, the new (updated) configuration file is not downloaded to the device. A workaround is to define the TFTP server with an IP address instead of an FQDN, which requires DNS resolution.

   The constraint has been resolved in Version 7.00A.044.007 (see Section 2.34.2).

   SR: 765311

   Applicable Products: Mediant 3000.

2.35.2.7.2 Web Constraints

This release includes the following known Web constraints:

1. The AMD file cannot be deleted through the Web interface.

   Applicable Products: Mediant 3000.

2. If the device detects a duplicated IPv6 address (as result of an IPv6 DAD message), even though the relevant interface does not become active, the IP Interface Status table (Web interface and SNMP) erroneously display this interface as active. Duplicated IPv6 address occurrence can be identified in Syslog messages or in the CLI (showing active interfaces), where the problematic interface is correctly not displayed (as it is not active).

   Applicable Products: Mediant 3000.

3. An unnecessary scroll bar appears on many of the Web pages when using 1280 x 1024 screen resolution.

   Applicable Products: Mediant 3000.

4. When configuring a Media Realm in the SIP Media Realm table, if the user enters a value in the 'Port Range End' field (which should be read-only, but is erroneously read-write), this value is ignored and the Web interface assigns a value to this field based on

the 'Number Of Media Session Legs' field and the 'Port Range First' field.

Applicable Products: Mediant 3000.

5. When using the Software Upgrade Wizard, if the Voice Prompt (VP) file is loaded and the **Next** button is clicked while the progress bar is displayed, the file is not loaded to the device. Despite this failure, the user receives a message that the file has been successfully downloaded.

   Applicable Products: Mediant 3000.

6. On the Software Upgrade Wizard page, the software upgrade process must be completed prior to clicking the **Back** button. Clicking the **Back** button before the wizard completes causes a display distortion.

   Applicable Products: Mediant 3000.

7. On the IP Interface Status page (under the **Status & Diagnostics** menu), the IP addresses may not be fully displayed if the address is greater than 25 characters.

   Applicable Products: Mediant 3000.

8. When using the Trunk Scroll Bar on the Trunk Settings page, some trunks may not be displayed on the Trunks panel when scrolling fast.

   Applicable Products: Mediant 3000.

9. The Web Search feature may produce incorrect search results. For example, a search result for the TLS version parameter directs the user to the incorrect page instead of the Security Settings page under the System menu.

   Applicable Products: Mediant 3000.

10. The fax counters, 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the Status & Diagnostics page do not function correctly.

    Applicable Products: Mediant 3000.

2.35.2.7.3 SNMP Constraints

This release includes the following known Simple Network Management Protocol (SNMP) constraints:

1. From Release 7.0, configuration through SNMP is not supported.

   Applicable Products: Mediant 3000.

2. When configuring acSysInterfaceTable using SNMP or the Web interface, validation is done only after a device reset.

   Applicable Products: Mediant 3000.

3. The DS3 ifAdmin-State field cannot be changed in the IF-Table, using SNMP.

   Applicable Products: Mediant 3000 with TP-6310.

4. In the DS3/E3 Current Table, the objects dsx3CurrentSEFSs and dsx3CurrentUASs are not supported.

   Applicable Products: Mediant 3000 with TP-6310.

5. In the DS3/E3 Interval Table the objects, dsx3IntervalPSESs and dsx3IntervalSEFSs are not supported.

   Applicable Products: Mediant 3000 with TP-6310.

6. The dsx3Total Table is not supported.

   Applicable Products: Mediant 3000 with TP-6310.

7. The Admin State does not change to "Redundant".

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

8. When defining or deleting SNMPv3 users, the v3 trap user must not be the first to be defined or the last to be deleted. If there are no non-default v2c users, this results in a loss of SNMP contact with the device.

   Applicable Products: Mediant 3000.

2.35.3 Resolved Constraints

Constraints from previous releases that have now been resolved include the following:

2.35.3.1 SIP Constraints

The following SIP constraint has been resolved:

1. Graceful Shutdown is supported when the device operates in Gateway application mode only. Now, it is also supported for the SBC application.

   Applicable Products: Mediant 3000.

2. The device erroneously performs message manipulations when the syntax in the 'Condition' field contains the plus "+" sign for indicating multiple values. Now, this invalid configuration is not supported.

   Applicable Products: Mediant 3000.

2.35.3.2 Networking Resolved Constraints

The following networking constraints have been resolved:

1. Enabling the UDP checksum calculation is not applied to CALEA and IP-to-IP calls with UDP connections. The UDP checksum field is set to zero in these cases.

   Applicable Products: Mediant 3000.

2. In certain cases, when the Spanning-Tree algorithm is enabled on the external Ethernet switch port that is connected to the device, the external switch blocks all traffic from entering and leaving the device for some time after the device is reset. This may result in the loss of important packets such as BootP and TFTP requests, which in turn, may cause a failure in device start-up. A possible workaround is to set the *ini* file parameter BootPRetries to 5, causing the device to issue 20 BootP requests for 60 seconds. Another workaround is to disable the spanning tree on the port of the external switch that is connected to the device.

   Applicable Products: Mediant 3000.

3. Configuring the device to auto-negotiate mode while the opposite port is set manually to full-duplex (either 10BaseT or 100BaseTX) is invalid. It is also invalid to set the device to one of the manual modes while the opposite port is configured differently. The user is encouraged to always prefer full-duplex connections over half-duplex and 100BaseTX over 10BaseT (due to the larger bandwidth).

   Applicable Products: Mediant 3000.

4. Debug Recording:

   - Only one IP target is allowed.
   - Maximum of 50 trace rules are allowed simultaneously.

   Applicable Products: Mediant 3000.

2.35.3.3 Media Resolved Constraints

The following media constraints have been resolved:

1. The On-Demand Jitter Buffer does not function correctly when transrating is also required (may cause packets loss).

   Applicable Products: Mediant 3000.

2.35.3.4 Infrastructure Resolved Constraints

The following infrastructure constraint has been resolved:

1. The following parameters do not return to their default values when attempting to restore them to defaults using the Web interface or SNMP, or when loading a new *ini* file using BootP/TFTP:
   - UseRProductName
   - LogoWidth
   - WebLogoText
   - UseWeblogo
   - UseProductName

   Applicable Products: Mediant 3000.

2.35.3.5 Security Resolved Constraints

The following security constraint has been resolved:

1. 'RADIUS VSA Vendor ID' parameter (RadiusVSAVendorID) is now configurable. Previously, this parameter value was hard-coded at 4923. The default is now set to 5003, which is AudioCodes' vendor ID. New configurability capability means that AudioCodes' RADIUS implementation supports multi-vendor options using the format recommended in RFC 2865.

   Applicable Products: Mediant 3000.

3 Obsolete Features and Parameters

3.1 Obsolete Features

This section lists the features that are no longer supported in Version 7.0.

3.1.1 IP-to-IP Application

From Version 7.0 (inclusive), the IP-to-IP application is no longer supported. This application has been superseded by the SBC application, which offers a more sophisticated and comprehensive solution for VoIP. Continued support for the IP-to-IP application will still be available (until further notice) to incumbent customers running Version 6.8 or earlier. For customers currently implementing the IP-to-IP application, AudioCodes recommends migrating to the SBC application due to its feature-rich benefits.

As a result, the following parameters relating to the IP-to-IP application (IP2IP application) are now obsolete or have been modified:

Parameter	Comments
IP to IP Application [EnableIP2IPApplication]	Parameter has been removed.
Voice Mail Interface [VoiceMailInterface]	Following optional value has been removed: ▪ [7] IP2IP
[PlayHeldToneForIP2IP]	Parameter has been removed.
IP2IP Transfer Mode [IP2IPTransfermode]	Parameter has been removed.
Outbound IP Routing Table / Tel to IP Routing [Prefix]	Following table columns have been removed: ▪ PREFIX_SrcIPGroupID ▪ PREFIX_DestHostPrefix ▪ PREFIX_SrcHostPrefix
Calling Phone Number Manipulation Table for Tel > IP Calls	Following table column has been removed: ▪ CallingNameMapTel2Ip_SrcIPGroupName
Destination Phone Number Manipulation Table for Tel > IP Calls [NumberMapTel2IP]	Following table column has been removed: ▪ NumberMapTel2IP_SrcIPGroupID
Source Phone Number Manipulation Table for Tel > IP Calls [SourceNumberMapTel2IP]	Following table column has been removed: ▪ SourceNumberMapTel2IP_SrcIPGroupID
Redirect Number Tel -> IP [RedirectNumberMapTel2IP]	Following table column has been removed: ▪ RedirectNumberMapTel2IP_SrcIPGroupID
IP Group Table [IPGroup]	Following table columns have been removed: ▪ IPGroup_ServingIPGroup ▪ IPGroup_EnableSurvivability ▪ IPGroup_RoutingMode
Account Table [Account]	The following optional value has been modified for the Application Type column (Account_ApplicationType): ▪ [0] "GW/IP2IP" changed to "GW"
SIP Interface Table [SipInterface]	The following optional value has been modified for the Application Type column (SIPInterface_ApplicationType): ▪ [0] "GW/IP2IP" changed to "GW"

Parameter	Comments
Test Call Table [Test_Call]	The following optional value has been modified for the Application Type column (Test_Call_ApplicationType): [0] "GW/IP2IP" changed to "GW"
IP2IPTranscodingMode	Parameter has been removed.

3.1.2 SAS Application

The Standalone Survivability application is no longer supported. The last supported software version for this functionality is Version 6.8. Consequently, the following parameters are now obsolete:

Table 3-1: Obsolete SAS Parameters

Parameter	Comments
Enable SAS enable-sas [EnableSAS]	-
SAS Default Gateway IP sas-default-gw-ip [SASDefaultGatewayIP]	-
SAS Registration Time sas-registration-time [SASRegistrationTime]	-
SAS Connection Reuse sas-connection-reuse [SASConnectionReuse]	-
Enable Record-Route record-route [SASEnableRecordRoute]	-
SAS Proxy Set sas-proxy-set [SASProxySet]	-
Redundant SAS Proxy Set rdcy-sas-proxy-set [RedundantSASProxySet]	-
SAS Block Unregistered Users sas-block-unreg-usrs [SASBlockUnRegUsers]	-
sas-contact-replace [SASEnableContactReplace]	-
SAS Survivability Mode sas-survivability [SASSurvivabilityMode]	-
SAS Subscribe Response	-

Parameter	Comments
sas-subscribe-resp [SASSubscribeResponse]	
Enable ENUM enable-enum [SASEnableENUM]	-
SAS Binding Mode sasbindingmode [SASBindingMode]	-
SAS Emergency Numbers sas-emerg-nb [SASEmergencyNumbers	-
sas-emerg-prefix [SASEmergencyPrefix]	-
SAS Entering Emergency Mode sas-enter-emg-mode [SASEnteringEmergencyMode]	-
sas-indialog-mode [SASInDialogRequestMode]	-
SAS Inbound Manipulation Mode sas-inb-manipul-md [SASInboundManipulationMode]	-
SAS Registration Manipulation configure voip > sas sasregistrationmanipulation [SASRegistrationManipulation]	-

3.2 Obsolete Parameters

The table below summarizes parameters from the previous release that are now obsolete.

Table 3-2: Obsolete Parameters

Parameter	Comments
Routing Rule Groups table [RoutingRuleGroups]	Replaced by the new Routing Policy tables (SBCRoutingPolicy and GwRoutingPolicy).
SIP UDP Local Port CLI: sip-udp-local-port [LocalSIPPort]	No longer needed as the SIP Interface configuration entity is used to configure the SIP port.
Web: SIP TCP Local Port CLI: sip-tcp-local-port [TCPLocalSIPPort]	No longer needed as the SIP Interface configuration entity is used to configure the SIP port.
Web: SIP TLS Local Port CLI: sip-tls-local-port	No longer needed as the SIP Interface configuration entity is used to configure the SIP port.

Parameter	Comments
[TLSLocalSIPPort]	
Web: SAS Local SIP TCP Port CLI: sas-local-sip-tcp-port [SASLocalSIPTCPPort]	No longer needed as the SIP Interface configuration entity is used to configure the SIP port for SAS.
Web: SAS Local SIP TLS Port CLI: sas-local-sip-tls-port [SASLocalSIPTLSPort]	This "old" parameter is no longer needed as the SIP Interface configuration entity is used to configure the SIP port for SAS.
Web: SAS Local SIP UDP Port CLI: sas-local-sip-udp-port [SASLocalSIPUDPPort]	No longer needed as the SIP Interface configuration entity is used to configure the SIP port for SAS.
[RADIUSAccPort]	Replaced by the new RADIUS Servers table (RadiusServers).
[RADIUSAuthServerIP]	Replaced by the new RADIUS Servers table (RadiusServers).
[RADIUSAuthPort]	Replaced by the new RADIUS Servers table (RadiusServers).
[SharedSecret]	Replaced by the new RADIUS Servers table (RadiusServers).
[RADIUSAccServerIP]	Replaced by the new RADIUS Servers table (RadiusServers).
[LDAPSearchServerMethod]	Replaced by the new LDAP Servers Group table (LDAPServersGroup).
[LdapConfiguration_Type]	Replaced by the new LDAP Servers Group table (LDAPServersGroup).
[SRD_IntraSRDMediaAnchoring]	Replaced by the new SIPInterface_SBCDirectMedia parameter in the SIP Interface table.
[PhysicalPortsTable_NativeVlan]	Replaced by the new DeviceTable_Tagging parameter in the Ethernet Device table.
[SRD_MediaRealm]	Replaced by the new SIPInterface_MediaRealm parameter in the SIP Interface table.
[TxDTMFOption]	The table has been replaced by the following parameters: ▪ FirstTxDTMFOption ▪ SecondTxDTMFOption
[LdapConfiguration_LdapConfInterfaceType]	Replaced by the new LdapConfiguration_Interface parameter in the LDAP Configuration table.
[Test_Call_SRD]	Replaced by the new Test_Call_SIPInterfaceName parameter in the Test Call table.
[IP2IPRouting_DestSRDID]	Replaced by the new IP2IPRouting_DestSIPInterfaceName parameter in the IP-to-IP Routing table.
[IPGroup_Description]	Obsolete.
[WebAuthMode]	Obsolete
[LoggingFilters_Syslog]	Replaced by LoggingFilters_LogDestination
[DebugRecordingStatus]	Replaced by LoggingFilters_Mode
[SRD_SBCRegisteredUsersClassificationMethod]	Obsolete.

4 Session Capacity

The table below lists maximum capacity for the Gateway and SBC applications, per product.

Table 4-1: Gateway and SBC Capacity per Product

Product	Signaling Sessions	Media Sessions			Registered Users
		RTP-to-RTP	SRTP-RTP or SRTP-TDM	Codec Transcoding	
Mediant 3000 Gateway & E-SBC	1,008	1,008	1,008	1,008	3,000 (5,000 Depop.)

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.
- The *RTP-to-RTP* column represents maximum media sessions when **all** media sessions are RTP-to-RTP only. The same applies to the *SRTP-RTP or SRTP-TDM* column.
- *Registered Users* is 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.

This section lists the supported channel capacity per DSP template of Mediant 3000 for the following:

- Mediant 3000 full chassis – see Section 4.1 on page 130
- Mediant 3000 with 16 E1 / 21 T1 – see Section 4.2 on page 131
- Mediant 3000 with single T3 – see Section 4.3 on page 132
- DSP template mix feature – see Section 4.4 on page 134

Notes:

- 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.

4.1 Mediant 3000 Full Chassis

The channel capacity per DSP firmware template is shown in the table below.

Table 4-2: Channel Capacity per DSP Firmware Template for Mediant 3000

					DSP Template										
					0	1	2	4	5	7	9	10	11	12	13
Supplementary Capabilities					Number of Channels										
SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor											
-	-	-	-	-	2016	2016	1764	1260	1260	1638	1008	1512	630	756	378
-	-	✓	✓	-	1890	1890	1638	1134	1134	1638	1008	1512	630	756	378
-	-	-	-	✓	1134	1134	1134	630	1008	882	252	1134	252	378	378
✓	-	-	-	-	1764	1638	-	1008	-	1638	1008	-	630	-	-
✓	-	✓	✓	-	1638	1638	-	1008	-	1512	1008	-	630	-	-
✓	✓	-	-	-	1638	1638	-	1008	-	1386	1008	-	504	-	-
✓	✓	✓	✓	-	1638	1638	-	1008	-	1386	1008	-	504	-	-
✓	✓	✓	✓	✓	1134	1134	-	1008	-	882	252	-	252	-	-
Voice Coder															
AMR					-	✓	-	✓	-	-	-	-	-	-	-
AMR-WB					-	-	-	✓	-	-	-	-	-	-	-
EVRC					-	-	✓	-	✓	-	-	-	-	-	-
EVRC-B					-	-	-	-	✓	-	-	-	-	-	-
G.711 A/µ-law PCM					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722					-	-	-	✓	-	-	✓	-	✓	-	-
G.723.1					✓	-	-	-	-	-	-	-	-	-	-
G.726 ADPCM					✓	✓	✓	✓	✓	✓	-	-	-	-	-
G.729 A, B					✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-

SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor	DSP Template 0	1	2	4	5	7	9	10	11	12	13
Supplementary Capabilities					Number of Channels										
G.729.1 (up to 12 kbps)					-	-	-	-	-	-	-	-	-	-	-
GSM EFR					-	✓	-	✓	-	-	-	-	-	-	-
GSM FR					✓	✓	-	✓	-	-	-	-	-	-	-
iLBC					-	-	-	-	-	✓	-	-	-	-	-
MS GSM					✓	✓	-	✓	-	-	-	-	-	-	-
MS-RTA (NB)					-	-	-	-	-	-	✓	-	✓	-	-
MS-RTA (WB)					-	-	-	-	-	-	-	-	✓	-	-
SPEEX NB					-	-	-	-	-	-	-	-	-	✓	✓
SPEEX WB					-	-	-	-	-	-	-	-	-	-	✓
T.38 Version 3					-	-	-	-	-	-	-	✓	-	-	-

4.2 Mediant 3000 16 E1 / 21 T1

The channel capacity per DSP firmware template for Mediant 3000 with 16 E1 / 21 T1 is shown in the table below.

Table 4-3: Channel Capacity per DSP Firmware Templates for Mediant 3000 16 E1 / 21 T1

SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor	DSP Template 0	1	2	4	5	7	9	10	11
Supplementary Capabilities					Number of Channels								
-	-	-	-	-	504	504	504	360	360	468	288	432	180
-	-	✓	✓	-	504	504	468	324	324	468	288	432	180
-	-	-	-	✓	324	324	324	180	288	252	72	324	72
✓	-	-	-	-	504	468	-	288	-	468	288	-	180
✓	-	✓	✓	-	468	468	-	288	-	432	288	-	180
✓	✓	-	-	-	468	468	-	288	-	396	288	-	144
✓	✓	✓	✓	-	468	468	-	288	-	396	288	-	144
✓	✓	✓	✓	✓	324	324	-	180	-	252	72	-	72
Voice Coder													
AMR					-	✓	-	✓	-	-	-	-	-

AMR-WB	-	-	-	✓	-	-	-	-	-
EVRC	-	-	✓	-	✓	-	-	-	-
EVRC-B	-	-	-	-	✓	-	-	-	-
G.711 A/µ-law PCM	✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722	-	-	-	✓	-	-	✓	-	✓
G.723.1	✓	-	-	-	-	-	-	-	-
G.726 ADPCM	✓	✓	✓	✓	✓	✓	-	-	-
G.729 A, B	✓	✓	✓	✓	✓	✓	✓	✓	✓
G.729.1 (up to 12 kbps)	-	-	-	-	-	-	-	-	-
GSM EFR	-	✓	-	✓	-	-	-	-	-
GSM FR	✓	✓	-	✓	-	-	-	-	-
iLBC	-	-	-	-	-	✓	-	-	-
MS GSM	✓	✓	-	✓	-	-	-	-	-
MS-RTA (NB)	-	-	-	-	-	-	✓	-	✓
MS-RTA (WB)	-	-	-	-	-	-	-	-	✓
T.38 Version 3	-	-	-	-	-	-	-	✓	-

4.3 Mediant 3000 with Single T3

The channel capacity per DSP firmware template for Mediant 3000 with a single T3 interface is shown in the table below.

Table 4-4: Channel Capacity per DSP Firmware Templates for Mediant 3000 with Single T3

					DSP Template								
					0	**1**	**2**	**4**	**5**	**7**	**9**	**10**	**11**
Supplementary Capabilities					**Number of Channels**								
SRTP	**ARIA**	**RTCP XR**	**IPM Detectors**	**Acoustic Echo Suppressor**									
-	-	-	-	-	672	672	672	480	480	624	384	576	240
-	-	✓	✓	-	672	672	624	432	432	624	384	576	240
-	-	-	-	✓	432	432	432	240	384	336	96	432	96
✓	-	-	-	-	672	624-	-	384	-	624	384	-	240
✓	-	✓	✓	-	624	624	-	384	-	576	384	-	240
✓	✓	-	-	-	624	624	-	384	-	528	384	-	192
✓	✓	✓	✓	-	624	624	-	384	-	528	384	-	192
✓	✓	✓	✓	✓	432	432	-	240	-	336	96	-	96
Voice Coder													
AMR					-	✓	-	✓	-	-	-	-	-
AMR-WB					-	-	-	✓	-	-	-	-	-

	DSP Template								
	0	1	2	4	5	7	9	10	11
Supplementary Capabilities SRTP / ARIA / RTCP XR / IPM Detectors / Acoustic Echo Suppressor	Number of Channels								
EVRC	-	-	✓	-	✓	-	-	-	-
EVRC-B	-	-	-	-	✓	-	-	-	-
G.711 A/µ-law PCM	✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722	-	-	-	✓	-	-	✓	-	✓
G.723.1	✓	-	-	-	-	-	-	-	-
G.726 ADPCM	✓	✓	✓	✓	✓	✓	-	-	-
G.729 A, B	✓	✓	✓	✓	✓	✓	✓	✓	✓
G.729.1 (up to 12 kbps)	-	-	-	-	-	-	-	-	-
GSM EFR	-	✓	-	✓	-	-	-	-	-
GSM FR	✓	✓	-	✓	-	-	-	-	-
iLBC	-	-	-	-	-	✓	-	-	-
MS GSM	✓	✓	-	✓	-	-	-	-	-
MS-RTA (NB)	-	-	-	-	-	-	✓	-	✓
MS-RTA (WB)	-	-	-	-	-	-	-	-	✓
T.38 Version 3	-	-	-	-	-	-	-	✓	-

4.4 Mediant 3000 DSP Template Mix Feature

Mediant 3000 can operate (and be loaded) with up to two DSP templates. The channel capacity per DSP template is approximately 50%, with alignment to the number of DSP's present in the device.

Table 4-5: Channel Capacity of DSP Template Mix Feature for Mediant 3000

DSP Template Mix	Number of Channels
1 (AMR) / 2 (EVRC)	960
1 (AMR) / 5 (EVRCB)	768
1 (AMR) / 7 (iLBC)	864

5 Supported SIP Standards

5.1 Supported SIP RFCs

The table below lists the supported RFCs.

Table 5-1: Supported RFCs

RFC	Description	Gateway	SBC
RFC 7316	The Session Initiation Protocol (SIP) P-Private-Network-Indication Private Header	×	√ (forwarded transparently)
RFC 7261	Offer/Answer Considerations for G723 Annex A and G729 Annex B	√	√
RFC 6442	Location Conveyance for the Session Initiation Protocol	×	√ (forwarded transparently)
RFC 6432	Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses	√	√
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 6228	Session Initiation Protocol (SIP) Response Code for Indication of Terminated Dialog	×	√ (forwarded transparently)
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)	√	√
RFC 6086	Session Initiation Protocol (SIP) INFO Method and Package Framework	×	√ (forwarded transparently)
RFC 6050	A Session Initiation Protocol (SIP) Extension for the Identification of Services	×	√ (forwarded transparently)
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	√	√
RFC 6026	Correct Transaction Handling for 2xx Responses to INVITE Requests	√	√
RFC 5954	Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261	√	√
RFC 5922	Domain Certificates in the Session Initiation Protocol (SIP) - SIP over TLS	√	√
RFC 5876	Updates to Asserted Identity in the Session Initiation Protocol	×	√ (forwarded transparently)
RFC 5853	Requirements from SIP / SBC Deployments	-	√
RFC 5839	An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification	×	√ (forwarded transparently)
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	√	√

RFC	Description	Gateway	SBC
RFC 5630	The Use of the SIPS URI Scheme in the Session Initiation Protocol	√	√
RFC 5628	Registration Event Package Extension for GRUU	√	×
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	√	√ (forwarded transparently)
RFC 5079	Rejecting Anonymous Requests in SIP	√	√
RFC 5022	Media Server Control Markup Language (MSCML)	√	×
RFC 5009	P-Early-Media Header	×	√ (forwarded transparently)
RFC 5002	The Session Initiation Protocol (SIP) P-Profile-Key Private Header	×	√ (forwarded transparently)
RFC 4961	Symmetric RTP and RTCP for NAT	√	√
RFC 4904	Representing trunk groups in tel/sip URIs	√	√ (forwarded transparently)
RFC 4733	RTP Payload for DTMF Digits	√	√
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial	×
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	√	√ (forwarded transparently)
RFC 4694	Number Portability Parameters for the "tel" URI	×	√ (forwarded transparently)
RFC 4582	The Binary Floor Control Protocol (BFCP)	×	√ (forwarded transparently)
draft-sandbakken-dispatch-bfcp-udp-03	Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport	×	√ (forwarded transparently)
draft-ietf-bfcpbis-rfc4583bis-12	Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams	×	√ (forwarded transparently)
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	√	√
RFC 4566	Session Description Protocol	√	√
RFC 4538	Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)	×	√ (forwarded transparently)
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	√	√ (forwarded transparently)
RFC 4475	SIP Torture Test Messages	√	√
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	√	√ (forwarded transparently)
RFC 4457	The Session Initiation Protocol (SIP) P-User-Database Private-Header	×	√ (forwarded transparently)

RFC	Description	Gateway	SBC
RFC 4412	Communications Resource Priority for SIP	√	√ (forwarded transparently)
RFC 4411	Extending SIP Reason Header for Preemption Events	√	√ (forwarded transparently)
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	√	√
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	√	√
RFC 4244	An Extension to SIP for Request History Information	√	√
RFC 4240	Basic Network Media Services with SIP - NetAnn	√	√ (forwarded transparently)
RFC 4235	Dialog Event Package	Partial	Partial
RFC 4117	Transcoding Services Invocation	√	×
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	√	√ (forwarded transparently)
RFC 4028	Session Timers in the Session Initiation Protocol	√	√
RFC 3966	The tel URI for Telephone Numbers	√	√
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial	√
RFC 3911	The SIP Join Header	Partial	×
RFC 3903	SIP Extension for Event State Publication	√	√
RFC 3892	The SIP Referred-By Mechanism	√	√
RFC 3891	"Replaces" Header	√	√
RFC 3842	MWI	√	√
RFC 3841	Caller Preferences for the Session Initiation Protocol (SIP)	√ (forwarded transparently)	√ (forwarded transparently)
RFC 3824	Using E.164 numbers with SIP (ENUM)	√	√
RFC 3725	Third Party Call Control	√	√
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	√	√
RFC 3680	A SIP Event Package for Registration (IMS)	√	×
RFC 3666	SIP to PSTN Call Flows	√	√ (forwarded transparently)
RFC 3665	SIP Basic Call Flow Examples	√	√
RFC 3611	RTCP-XR	√	√
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	√	×
RFC 3605	RTCP attribute in SDP	√	√ (forwarded transparently)

RFC	Description	Gateway	SBC
RFC 3581	Symmetric Response Routing - rport	√	√
RFC 3578	Interworking of ISDN overlap signalling to SIP	√	×
RFC 3551	(RTP) Profile for Audio and Video Conferences with Minimal Control	×	√
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	√	√
RFC 3515	Refer Method	√	√
RFC 3489	STUN - Simple Traversal of UDP	√	√
RFC 3455	P-Associated-URI	√	√ (using user info \ account)
RFC 3420	Internet Media Type message/sipfrag	√	√
RFC 3389	RTP Payload for Comfort Noise	√	√ (forwarded transparently)
RFC 3372	SIP-T	√	√ (forwarded transparently)
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration	√	√
RFC 3361	DHCP Option for SIP Servers	√	×
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	√	×
RFC 3326	Reason header	√	√ (forwarded transparently)
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	√	√
RFC 3323	Privacy Mechanism	√	√
RFC 3311	UPDATE Method	√	√
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	√	×
RFC 3265	(SIP)-Specific Event Notification	√	√
RFC 3264	Offer/Answer Model	√	√
RFC 3263	Locating SIP Servers	√	√
RFC 3262	Reliability of Provisional Responses	√	√
RFC 3261	SIP	√	√
RFC 2976	SIP INFO Method	√	√
RFC 2833	Telephone event	√	√
RFC 2782	A DNS RR for specifying the location of services	√	√
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	√	√
RFC 2327	SDP	√	√

RFC	Description	Gateway	SBC
RFC 2198	RTP Payload for Redundant Audio Data	√	√
ECMA-355, ISO/IEC 22535	QSIG tunneling	√	√ (forwarded transparently)
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	√	√
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	√	√ (forwarded transparently)
draft-levy-sip-diversion-08	Diversion Indication in SIP	√	√
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP	√	√ (forwarded transparently)
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header	√	√
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples	√	√ (forwarded transparently)
draft-ietf-sipping-cc-transfer-05	Call Transfer	√	√
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	√	√
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	√	√

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
INVITE	-
ACK	-
BYE	-
CANCEL	-
REGISTER	Send only for Gateway/IP-to-IP application; send and receive for SBC application
REFER	Inside and outside of a dialog
NOTIFY	-
INFO	-
OPTIONS	-
PRACK	-
UPDATE	-
PUBLISH	Send only
SUBSCRIBE	-

5.2.3 SIP Headers

The device supports the following SIP Headers:

- Accept
- Accept–Encoding
- Alert-Info
- Allow
- Also
- Asserted-Identity
- Authorization
- Call-ID
- Call-Info
- Contact
- Content-Disposition
- Content-Encoding
- Content-Length
- Content-Type
- Cseq
- Date
- Diversion
- Expires
- Fax

- From
- History-Info
- Join
- Max-Forwards
- Messages-Waiting
- MIN-SE
- P-Associated-URI
- P-Asserted-Identity
- P-Charging-Vector
- P-Preferred-Identity
- Priority
- Proxy- Authenticate
- Proxy- Authorization
- Proxy- Require
- Prack
- Reason
- Record- Route
- Refer-To
- Referred-By
- Replaces
- Require
- Remote-Party-ID
- Response- Key
- Retry-After
- Route
- Rseq
- Session-Expires
- Server
- Service-Route
- SIP-If-Match
- Subject
- Supported
- Target-Dialog
- Timestamp
- To
- Unsupported
- User- Agent
- Via
- Voicemail
- Warning
- WWW- Authenticate

Note: The following SIP headers are not supported:

- Encryption
- Organization

5.2.4 SDP Fields

The device supports the following SDP fields:

Table 5-4: 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:

- 1xx Response - Information Responses
- 2xx Response - Successful Responses
- 3xx Response - Redirection Responses
- 4xx Response - Client Failure Responses
- 5xx Response - Server Failure Responses
- 6xx Response - Global Responses

5.2.5.1 1xx Response – Information Responses

Table 5-5: Supported 1xx SIP Responses

1xx Response		Comments
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.
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

5.2.5.2 2xx Response – Successful Responses

Table 5-6: Supported 2xx SIP Responses

2xx Response	
200	OK
202	Accepted

5.2.5.3 3xx Response – Redirection Responses

Table 5-7: Supported 3xx SIP Responses

3xx Response		Comments
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.

5.2.5.4 4xx Response – Client Failure Responses

Table 5-8: Supported 4xx SIP Responses

4xx Response		Comments
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 receiving 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.
407	Proxy Authentication Required	Authentication support for Basic and Digest. Upon receiving 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.

4xx Response		Comments
423	Interval Too Brief	The device does not generate this response. On reception of this message the device uses the value received in the Min-Expires header as the registration time.
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.
480	Temporarily Unavailable	If the device receives a 480 Temporarily Unavailable 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 a 491 response to the received INVITE. When acting as a UAC: If the device receives a 491 response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again.

5.2.5.5 5xx Response – Server Failure Responses

Table 5-9: Supported 5xx SIP Responses

5xx Response		Comments
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	

5.2.5.6 6xx Response – Global Responses

Table 5-10: Supported 6xx SIP Responses

6xx Response		Comments
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	

This page is intentionally left blank.

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

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

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

Document #: LTRT-27224