Release Notes

AudioCodes Gateways, Session Border Controllers (SBC) & Multi-Service Business Routers (MSBR)

Session Border Controllers Multi-Service Business Routers Analog & Digital Media Gateways

Version 7.2

audiocodes

Table of Contents

1 Introduction.......... 17

1.1 Software Revision Record.......... 17
1.2 Products Supported in Release 7.2.......... 19

2 Gateways and SBCs.......... 21

2.1 Version GA.......... 21
2.1.1 New Features.......... 21
2.1.1.1 New Product - Media Transcoder Device.......... 21
2.1.1.2 New GUI for Web-based Management Tool.......... 21
2.1.1.3 New CLI Structure.......... 22
2.1.1.4 Interworking between SIP and SIP-I Endpoints.......... 22
2.1.1.5 Maximum Call Duration per Gateway and SBC Calls.......... 23
2.1.1.6 Protection against Known Malicious Attacks.......... 23
2.1.1.7 Block SIP Requests from Registered Users when Address Different.......... 24
2.1.1.8 Enhanced Dialog Classification Based on Proxy Set.......... 25
2.1.1.9 Wildcard Denoting 18x Responses in Message Manipulation Rules.......... 25
2.1.1.10 Increase in Maximum SIP Message Size.......... 26
2.1.1.11 IP Group Keep-Alive Connectivity Status Indication.......... 26
2.1.1.12 Enhanced Configuration of Allowed Coder Groups.......... 26
2.1.1.13 Enhanced Audio Coder Groups Configuration.......... 27
2.1.1.14 Enhanced Dial Plan Tagging.......... 27
2.1.1.15 Increase in Maximum Network Interfaces.......... 28
2.1.1.16 CDR Local Storage for Gateway Calls.......... 28
2.1.1.17 Historical CDRs Display for SBC Calls.......... 28
2.1.1.18 New CDR Fields.......... 28
2.1.1.19 Maximum RADIUS Requests.......... 29
2.1.1.20 Increase in Maximum Network ACL Rules.......... 29
2.1.1.21 Enhanced TLS Certificate Support.......... 30
2.1.1.22 TLS Certificate Verification.......... 30
2.1.1.23 Disable Reuse of TLS Connections.......... 30
2.1.1.24 UDP Port Spacing by Four.......... 30
2.1.1.25 Sending of Silence RTP Packets to SIP Trunks.......... 31
2.1.1.26 Media Transcoding Cluster Feature.......... 31
2.1.1.27 New Quality of Service PMs and Alarms.......... 33
2.1.1.28 Actions upon Poor Voice Quality Detections.......... 34
2.1.1.29 Bitrate Configuration for SILK and Opus Coders.......... 35
2.1.1.30 Core Dump File Deletion.......... 35
2.1.2 Known Constraints.......... 36
2.1.3 Resolved Constraints.......... 41
2.2 Patch Version 7.20A.001.......... 42
2.2.1 New Features.......... 42
2.2.1.1 New Virtualized Platforms for Mediant VE SBC.......... 42
2.2.1.2 Enhanced Dial Plan Tags and Call Setup Rules.......... 42
2.2.1.3 Enhanced SIP-SIP-I Interworking.......... 43
2.2.1.4 Triggering Special Call Actions using X-AC-Action SIP Header.......... 43
2.2.1.5 VoIPerfect Feature.......... 44
2.3 Patch Version 7.20A.002.......... 47
2.3.1 New Features.......... 47
2.3.1.1 Load-Balancing of SBC Calls between Destination IP Groups.......... 47
2.3.1.2 Configurable FXS Off-hook Current.......... 47
2.3.2 Known Constraints.......... 48
2.3.3 Resolved Constraints.......... 48
2.4 Patch Version 7.20A.100.......... 49

2.4.1 New Features ... 49
2.4.1.1 Capacity Updates ... 49
2.4.1.2 OpenSSL Library Update ... 49
2.4.1.3 Integrated SBC Configuration Wizard in Web Interface ... 49
2.4.1.4 MP-1288 Support for SBC Application ... 49
2.4.1.5 AudioCodes One Voice Operations Center Support for MP-1288 ... 50
2.4.1.6 MP-1288 Support for Cloud Resilience Package Application ... 50
2.4.1.7 New SNMP Alarms for MP-1288 ... 50
2.4.1.8 New SNMP Alarm for License Pool Over-Allocation ... 50
2.4.1.9 New SNMP Alarm for TLS Certificate Expiration ... 50
2.4.1.10 SNMP Version in Keep-Alive Trap ... 50
2.4.1.11 New SNMP Varbind for Serial Number ... 51
2.4.1.12 DH Key Size per TLS Context ... 51
2.4.1.13 DTLS Version per TLS Context ... 51
2.4.1.14 RSA Public Key for SSH Authentication per Management User Account 51
2.4.1.15 Increase in IP Network Interfaces, VLANs and Media Realms ... 51
2.4.1.16 Online Detection for Proxy Set Load Balancing ... 51
2.4.1.17 LED Indication for Software Upgrade ... 52
2.4.1.18 Media Transcoding Cluster Enhancements ... 52
2.4.1.19 Register-Unregister per Trunk Group ... 52
2.4.1.20 Enhanced Row-Pointer Feature ... 52
2.4.1.21 Multiple SRSs and SRS Redundancy for SIPRec ... 53
2.4.1.22 Product Key for Enhanced Product Identification ... 53
2.4.1.23 CLI Startup Script for Non-MSBR Products ... 54
2.4.1.24 Saving and Loading CLI-based Configuration Files in Web Interface ... 54
2.4.1.25 Hitless License Upgrade from Pool Manager ... 54
2.4.1.26 Debug for Remote Web (HTTP) Services ... 54
2.4.2 Known Constraints ... 55
2.4.3 Resolved Constraints ... 55
2.5 Patch Version 7.20A.104.001 ... 58
2.5.1 Resolved Constraints ... 58
2.6 Patch Version 7.20A.106.003 ... 60
2.6.1 Resolved Constraints ... 60
2.7 Patch Version 7.20A.150.004 ... 61
2.7.1 New Features ... 61
2.7.1.1 Session Capacity Increases ... 61
2.7.1.2 Analog Voice Interface Support on Mediant 500L E-SBC/Gateway ... 61
2.7.1.3 Bulk TLS Root Certificate Import ... 62
2.7.1.4 Base64 (PEM) Encoded String Included in Certificate Display ... 62
2.7.1.5 Generation of Encrypted Private Key File ... 62
2.7.1.6 Token-based Authentication for Accessing Web Interface ... 62
2.7.1.7 TLS Certificate Management through REST ... 62
2.7.1.8 Routing Based on QoS by Routing Server ... 63
2.7.1.9 Tag-Based Routing Enhancement ... 63
2.7.1.10 Fax Rerouting for SBC Calls ... 64
2.7.1.11 Routing Back to Sender ... 64
2.7.1.12 String Concatenation in Message Conditions ... 65
2.7.1.13 Pre-Parsing SIP Message Manipulation ... 65
2.7.1.14 Message Manipulation and Carriage Returns ... 65
2.7.1.15 IP Group Parameter Representation in Message Manipulation ... 66
2.7.1.16 Message Manipulation for SDP Origin Username ... 66
2.7.1.17 Enhanced ISUP Body Message Manipulation ... 66
2.7.1.18 IP Group Parameter Representation in Call Setup Rules ... 66
2.7.1.19 Maximum Characters for "o" Field in SDP Body ... 67
2.7.1.20 Detection of Pulse Dialing ... 67
2.7.1.21 Prefix String for External Line Enhancement ... 67
2.7.1.22 MWI Notification Timeout on Endpoint Equipment ... 67
2.7.1.23 Ringback and Held Tones per User ... 68

2.7.1.24 Retry Time Enhancement for Registration Failures 68
2.7.1.25 Random IDs in Contact Header User Part for New Registrations........... 69
2.7.1.26 Unregistration of User Accounts upon Device Reset 69
2.7.1.27 Register "Stickiness" to Registrar Server 69
2.7.1.28 Registrar Search Method for Registrar "Stickiness"................................ 69
2.7.1.29 Registration Event Package Subscription for Registrar "Stickiness" 70
2.7.1.30 High-Availability Disconnect 70
2.7.1.31 Enhanced HA Keep-Alive 71
2.7.1.32 OVR Support in High-Availability Mode.. 71
2.7.1.33 SIPRec Session Capacity Increase.. 71
2.7.1.34 Skype User Presence Notification for Non-Skype Endpoint Devices...... 71
2.7.1.35 SIP-based Private Wire Interworking.. 72
2.7.1.36 Configurable Maximum Transmission Unit... 72
2.7.1.37 Same VLAN ID for Multiple Ethernet Devices 72
2.7.1.38 SFP+ 10G Support for Network Interface.. 72
2.7.1.39 Disable Periodic DNS Queries 73
2.7.1.40 SBC Application Enabled by Default 73
2.7.1.41 Web GUI Enhancements.. 73
2.7.1.42 Console Access Mode.. 73
2.7.1.43 Single Sign-On to Web Interface from OVOC and Mediant CCE 74
2.7.1.44 Broadcast Indication of Firmware Upgrade 74
2.7.1.45 Free Product Evaluation Enhancements.. 74
2.7.1.46 Hitless License Key Installation for HA... 75
2.7.1.47 SNMP Proprietary Trap Variable Bindings 75
2.7.1.48 Debug for Remote Web Services 75
2.7.1.49 FXS Line Testing 75
2.7.1.50 Persistent Logging of Syslog Messages on Device 76
2.7.1.51 Customization of Remote SIP User Agent Field in SBC CDRs 77
2.7.1.52 Snapshot Load through CLI... 77
2.7.1.53 Log of Loaded CLI Script File 77
2.7.1.54 CLI Show Run Enhancements 77
2.7.2 Known Constraints.. 78
2.7.3 Resolved Constraints.. 78
2.8 Patch Version 7.20A.152.003..83
2.8.1 New Features... 83
2.8.1.1 User "Stickiness" to Registrar Server for IP Groups 83
2.8.1.2 Trapezoid Ring Waveform Support 84
2.8.2 Known Constraints.. 84
2.8.3 Resolved Constraints.. 84
2.9 Patch Version 7.20A.152.009..86
2.9.1 Resolved Constraints.. 86
2.10 Patch Version 7.20A.154.007..87
2.10.1 New Features... 87
2.10.1.1 Increase in CDR Fields Sent to RADIUS Server.................................... 87
2.10.1.2 Call Preemption for Emergency Calls by Routing Server........................ 87
2.10.1.3 Display of Active SIPRec Sessions in CLI.. 88
2.10.1.4 Number of Displayed Output Lines in CLI Terminal Window 88
2.10.1.5 Increase in Maximum IP Groups and Proxy Sets................................... 88
2.10.1.6 Static UDP Port Assignment for SIP Signaling....................................... 88
2.10.1.7 Sending DTMF using both SIP INFO and RFC 2833............................. 89
2.10.1.8 Termination of Call Hold and Retrieve SIP Requests 90
2.10.1.9 Multiple Management Interfaces 90
2.10.1.10 Increased Value Ranges for Proxy Online Detection............................. 91
2.10.1.11 User Account Re-registration after Physical Link Restored 91
2.10.1.12 Enhanced SIP REFER Handling 91
2.10.2 Known Constraints.. 92
2.10.3 Resolved Constraints.. 92

2.11 Patch Version 7.20A.154.044....95
- 2.11.1 Resolved Constraints....95

2.12 Patch Version 7.20A.154.052....97
- 2.12.1 Resolved Constraints....97

2.13 Patch Version 7.20A.154.059....98
- 2.13.1 Resolved Constraints....98

2.14 Patch Version 7.20A.156.009....99
- 2.14.1 New Features....99
  - 2.14.1.1 Port Assignment per Registered User....99
  - 2.14.1.2 Multiple AORs with Same Contact User....99
  - 2.14.1.3 Syntax Enhancement for Dial Plan Tags....100
  - 2.14.1.4 DHCP Option 160 for Automatic Provisioning....100
  - 2.14.1.5 ENUM Queries for Call Setup Rules....101
  - 2.14.1.6 Message Conditions for Starting/Stopping SIPRec Sessions....101
  - 2.14.1.7 SIP Classification by IP Address and Contact Header....102
- 2.14.2 Known Constraints....103
- 2.14.3 Resolved Constraints....103

2.15 Patch Version 7.20A.156.023....108
- 2.15.1 Resolved Constraints....108

2.16 Patch Version 7.20A.156.041....109
- 2.16.1 Resolved Constraints....109

2.17 Patch Version 7.20A.158.009....110
- 2.17.1 New Features....110
  - 2.17.1.1 Sending SIP Messages to OVOC for SIP Call Flow Diagrams....110
  - 2.17.1.2 Configurable Unit of Measurement for Call Duration in CDRs....110
  - 2.17.1.3 New Customized CDR Field "Call End Sequence Number"....111
  - 2.17.1.4 CDR Local Storage Enhancements....111
  - 2.17.1.5 CDR Local Storage Value Changes....112
  - 2.17.1.6 Enhanced HA Network Monitor Feature....112
  - 2.17.1.7 LDAP-based Management Services....113
  - 2.17.1.8 Ping by Hostname....113
  - 2.17.1.9 User Account Registration Based on IP Group Connectivity Status....113
  - 2.17.1.10 Enhanced Behavior for Account Registration....114
  - 2.17.1.11 Dynamic SIP UDP Port Assignment for Registration Accounts....114
  - 2.17.1.12 Parameter Name Change for 'Transcoding Mode'....114
  - 2.17.1.13 IP Group Parameter Representation in Message Manipulation....114
  - 2.17.1.14 Enhanced Message Manipulation Syntax for User-to-User Header....115
  - 2.17.1.15 Enabling Global Session ID through REST API....115
  - 2.17.1.16 Web Interface Updated with New AudioCodes Corporate Logo....116
  - 2.17.1.17 Customization of Web Browser's Tab Label....116
  - 2.17.1.18 Invalid RTCP Packet Handling....116
  - 2.17.1.19 OVR Support on Mediant VE SBC....116
- 2.17.2 Known Constraints....117
- 2.17.3 Resolved Constraints....117

2.18 Patch Version 7.20A.158.012....123
- 2.18.1 Resolved Constraints....123

2.19 Patch Version 7.20A.158.035....124
- 2.19.1 Resolved Constraints....124

2.20 Patch Version 7.20A.158.056....126
- 2.20.1 Resolved Constraints....126

2.21 Patch Version 7.20A.162.001....128
- 2.21.1 New Features....128
  - 2.21.1.1 New Mediant 9000 Hardware Revision....128
- 2.21.2 Known Constraints....128

2.22 Patch Version 7.20A.162.017....129

2.22.1 Resolved Constraints 129

2.23 Patch Version 7.20A.200.019 130

2.23.1 New Features 130
2.23.1.1 Entity Names Added to SNMP Alarm Descriptions 130
2.23.1.2 Performance Monitoring Thresholds Included in ini File 130
2.23.1.3 Proxy Set Name in Proxy Set Status Display 130
2.23.1.4 Restoring Defaults while Preserving Network Settings in CLI 130
2.23.1.5 Tail Filter for CLI Command Output 131
2.23.1.6 Enhanced SBC User Registration Request Handling 131
2.23.1.7 Enabling SBC and CRP Applications Removed from Web Interface 131
2.23.1.8 Faster Upload of CMP Software File 131
2.23.1.9 Enhanced File Management through REST API 132
2.23.1.10 New Alarm for Ethernet Group Down of HA Maintenance Interface 132
2.23.1.11 Subject Alternative Name (SAN) Field for TLS Certificates 132
2.23.1.12 Fullband Coder for SDP Telephone-Event 132
2.23.1.13 NGINX for HTTP Proxy Server Configuration 132
2.23.1.14 Default DNS Servers 133
2.23.1.15 Music-on-Hold from External Audio Streamer via FXS Gateway 133
2.23.1.16 Music-on-Hold from External Audio Streamer for SBC Calls 134
2.23.1.17 Dial Plans for Routing Gateway Calls 134
2.23.1.18 Enhanced Packet Loss Concealment 134
2.23.1.19 SBC User Info Table Activation Changes 135
2.23.1.20 Enhanced User Info File Handling 135
2.23.1.21 Dial Plan and User Info Table Parameters Exposed in ini File 135
2.23.1.22 Call Preemption for Emergency Calls by Routing Server 136
2.23.1.23 ENUM Query Enhancement for Call Setup Rules 136
2.23.1.24 Enhanced Call Admission Control 136
2.23.1.25 IDS Blacklist Display in Web Interface 136
2.23.1.26 Improved IDS SNMP Alarm Descriptions 137
2.23.1.27 High-Availability for AWS Environments 137
2.23.1.28 Initial HA Configuration from Single INI File 137
2.23.1.29 Changes in Offline HA Parameters 137
2.23.1.30 Packaged Configuration File Load and Save 138
2.23.1.31 Voltage Configuration for FXS MWI and Phone Lamp 138
2.23.1.32 Auto-Completion for Message Syntax 139
2.23.1.33 Select All Check Box for Selecting All Activity Types to Report 139
2.23.1.34 SSH Server Enabled by Default 139
2.23.1.35 TDM-to-SBC License Displayed in Management Interfaces 139
2.23.1.36 License Key Mode Indication 140
2.23.1.37 Core Allocation Optimization for Services 140
2.23.1.38 Default OAMP Interface Changes 141
2.23.1.39 Alarms Tables Enhancements 141
2.23.1.40 Handling of Retry-After Header in SIP 503 Responses 142
2.23.1.41 Enhanced Cross Validation for UDP Port Configuration 142
2.23.1.42 Improved Distribution of REGISTER and SUBSCRIBE Requests 142
2.23.1.43 Variable Usage Enhancements for Message Manipulations 142
2.23.1.44 Parameter Name Change from "Prefix" to "Pattern" 143
2.23.2 Known Constraints 144
2.23.3 Resolved Constraints 145

2.24 Patch Version 7.20A.200.550 148

2.24.1 Resolved Constraints 148

2.25 Patch Version 7.20A.202.112 149

2.25.1 New Features 149
2.25.1.1 New Mediant Software SBC Product - Mediant Cloud Edition (CE) SBC 149
2.25.1.2 New Mediant 800 Hardware Revision – Mediant 800C 150
2.25.1.3 SBC Capacity Licensing Model - Floating License 150

2.25.1.4 License Key of Redundant Device Included in INI File 151
2.25.1.5 Enhanced Media Transcoding Cluster Feature.................................... 151
2.25.1.6 Triggering SBC Actions using SIP NOTIFY Messages........................ 151
2.25.1.7 SIP Session Time Refreshes using UPDATE Messages...................... 151
2.25.1.8 Enhanced Randomly Assigned SIP Contact User Part........................ 151
2.25.1.9 Enhanced Handling of SIP Dialog-initiating INVITE Messages 152
2.25.1.10 Increase in Maximum Characters for User Part of SIP Messages........ 152
2.25.1.11 SIP Digest URI Handling for Authentication and Authorization............. 153
2.25.1.12 Handling SIP Messages with Unknown Cryptographic Suites 153
2.25.1.13 Handling both SDES and DTLS Security in SDP Negotiations............. 153
2.25.1.14 Graceful Period for Automatic Update of ini File 153
2.25.1.15 Enhanced SNMP Alarms for HA Redundant Device............................ 154
2.25.1.16 Serial Number of Redundant Device in Keep-alive SNMP Traps 154
2.25.1.17 Web Interface's Logo Hyperlinked to Topology View Page 154
2.25.1.18 Mediant 9000 Hardware Status Display in Management Interfaces 154
2.25.1.19 OVOC Product Key and ID Displayed in Web Interface....................... 155
2.25.1.20 New Default Name for IP Interfaces.. 155
2.25.1.21 No Reset for Number of Media Channels Parameter........................... 155
2.25.1.22 New CLI Command Structure for Parent-Child Configuration Tables... 155
2.25.1.23 Enhanced Filtering for CLI show Commands....................................... 156
2.25.1.24 Improved Location of CLI Command time-zone-format 156
2.25.1.25 Improved Location of CLI Commands for System Snapshots 156
2.25.1.26 CLI Command Name Change from "prefix" to "pattern"....................... 156
2.25.1.27 New CLI Commands for Assigning Dial Plans to Gateway Routing 156
2.25.1.28 New CLI Commands for Locking and Unlocking Device...................... 157
2.25.1.29 New CLI Commands for Displaying Activity Reports 157
2.25.1.30 New CDR Field -- 'Alerting Time'... 157
2.25.1.31 Name and ID of Media Components (MCs) Included in CDRs............. 157
2.25.1.32 Automatic IP Address for NAT Traversal in AWS Environments 158
2.25.1.33 New VoIPerfect Support for Managed G.729 Coder............................ 158
2.25.2 Known Constraints... 159
2.25.3 Resolved Constraints... 160

3 MSBR Series 167

3.1 Version 7.20A.150.004..167
3.1.1 New Features... 168
3.1.2 Known Constraints... 168
3.1.3 Resolved Constraints... 168
3.2 Version 7.20A.154.025..169
3.2.1 New Features... 169
3.2.2 Resolved Constraints... 171
3.3 Version 7.20A.154.061..173
3.3.1 Resolved Constraints... 173
3.4 Version 7.20A.154.078..174
3.4.1 New Features... 174
3.4.2 Resolved Constraints... 175
3.5 Version 7.20A.200.038..176
3.5.1 New Features... 176
3.5.2 Resolved Constraints... 177
3.6 Version 7.20A.202.112..178
3.6.1 New Features... 178
3.6.2 Resolved Constraints... 179

4 Capacity for Gateways & SBCs 181

4.1 SIP, Media and Registered User Capacity...181
4.2 Capacity per Feature...186

4.3 Detailed Capacity 187
4.3.1 Mediant 500 E-SBC 187
4.3.2 Mediant 500L Gateway and E-SBC 188
4.3.3 Mediant 800 Gateway & E-SBC.... 189
4.3.3.1 Mediant 800A/B Gateway & E-SBC 189
4.3.3.2 Mediant 800C Gateway & E-SBC.... 194
4.3.4 Mediant 1000B Gateway & E-SBC 196
4.3.4.1 Analog (FXS/FXO) Interfaces.... 196
4.3.4.2 BRI Interfaces.... 197
4.3.4.3 E1/T1 Interfaces 198
4.3.4.4 Media Processing Interfaces 200
4.3.5 MP-1288 Analog Gateway & E-SBC.... 202
4.3.6 Mediant 2600 E-SBC 203
4.3.7 Mediant 4000 SBC.... 205
4.3.8 Mediant 4000B SBC 207
4.3.9 Mediant 9000 SBC.... 209
4.3.10 Mediant 9000 SBC with Media Transcoders 211
4.3.11 Mediant Cloud Edition SBC 213
4.3.11.1 Forwarding Sessions.... 213
4.3.11.2 Transcoding Sessions 213
4.3.12 Mediant Server Edition SBC 215
4.3.13 Mediant Virtual Edition SBC.... 215
4.3.13.1 Mediant VE SBC for OpenStack and VMware Hypervisors 215
4.3.13.2 Amazon AWS EC2 221
4.3.13.3 Mediant VE SBC for Hyper-V Hypervisor.... 225
4.3.13.4 Mediant VE SBC with Media Transcoders 229

5 Capacity for MSBRs 233

5.1 SIP, Media and Registered User Capacity....233
5.2 Capacity per Feature....235
5.3 Detailed Capacity 236
5.3.1 Mediant 500 MSBR.... 236
5.3.2 Mediant 500L MSBR.... 237
5.3.3 Mediant 800 MSBR.... 238

6 Supported SIP Standards 243

6.1 Supported SIP RFCs....243
6.2 SIP Message Compliancy 247
6.2.1 SIP Functions.... 247
6.2.2 SIP Methods.... 247
6.2.3 SIP Headers.... 248
6.2.4 SDP Fields 249
6.2.5 SIP Responses 249

List of Tables

Table 1-1: Software Revision Record 17
Table 1-2: Products Supported in Release 7.2 19
Table 2-1: Known Constraints in Release 7.2 36
Table 2-2: Resolved Constraints in Release 7.2 41
Table 2-3: Known Constraints in Version 7.20A.002 48
Table 2-4: Resolved Constraints in Version 7.20A.002 48
Table 2-5: Known Constraints in Version 7.20A.100 55
Table 2-6: Resolved Constraints in Version 7.20A.100 55
Table 2-7: Resolved Constraints in Version 7.20A.104.001 58
Table 2-8: Resolved Constraints in Version 7.20A.106.003 60
Table 2-9: Known Constraints in Version 7.20A.150.004 78
Table 2-10: Resolved Constraints in Version 7.20A.150.004 78
Table 2-11: Known Constraints in Version 7.20A.152.003 84
Table 2-12: Resolved Constraints in Version 7.20A.152.003 84
Table 2-13: Resolved Constraints in Version 7.20A.152.009 86
Table 2-14: Known Constraints in Version 7.20A.154.007 92
Table 2-15: Resolved Constraints in Version 7.20A.154.007 92
Table 2-16: Resolved Constraints in Version 7.20A.154.044 95
Table 2-17: Resolved Constraints in Version 7.20A.154.052 97
Table 2-18: Resolved Constraints in Version 7.20A.154.059 98
Table 2-19: Known Constraints in Version 7.20A.156.009 103
Table 2-20: Resolved Constraints in Version 7.20A.156.009 103
Table 2-21: Resolved Constraints in Version 7.20A.156.023 108
Table 2-22: Resolved Constraints in Version 7.20A.156.041 109
Table 2-23: Known Constraints in Version 7.20A.158.009 117
Table 2-24: Resolved Constraints in Version 7.20A.158.009 117
Table 2-25: Resolved Constraints in Version 7.20A.158.012 123
Table 2-26: Resolved Constraints in Version 7.20A.158.035 124
Table 2-27: Resolved Constraints in Version 7.20A.158.056 126
Table 2-28: Known Constraints in Version 7.20A.162.001 128
Table 2-29: Resolved Constraints in Version 7.20A.162.017 129
Table 2-30: Known Constraints in Version 7.20A.200.019 144
Table 2-31: Resolved Constraints in Version 7.20A.200.019 145
Table 2-32: Resolved Constraints in Version 7.20A.200.550 148
Table 2-33: Known Constraints in Version 7.20A.202.112 159
Table 2-34: Resolved Constraints in Version 7.20A.202xxx 160
Table 3-1: Known Constraints in Version 7.20A.150.004 168
Table 3-2: Resolved Constraints for Patch Version 7.20A.154.025 171
Table 3-3: Resolved Constraints for Patch Version 7.20A.154.061 173
Table 3-4: Resolved Constraints for Patch Version 7.20A.154.078 175
Table 3-5: Resolved Constraints for Patch Version 7.20A.200.038 177
Table 3-6: Resolved Constraints for Patch Version 7.20A.202.112 179
Table 4-1: Capacity for Signaling, Media and Registered Users per Product 181
Table 4-2: Capacity per Feature 186
Table 4-3: Mediant 500 E-SBC (Non-Hybrid) SBC Capacity 187
Table 4-4: Mediant 500 Hybrid E-SBC (with Gateway) Media & SBC Capacity 187
Table 4-5: Mediant 500L E-SBC (Non-Hybrid) SBC Capacity 188
Table 4-6: Mediant 500L Hybrid E-SBC (with Gateway) Media & SBC Capacity 188
Table 4-7: Mediant 800A/B Gateway & E-SBC SBC Session Capacity per Capabilities (SBC Only) 189
Table 4-8: Mediant 800A/B Gateway & E-SBC Channel Capacity per Capabilities (with Gateway) .. 190
Table 4-9: Mediant 800C Gateway & E-SBC SBC Session Capacity per Capabilities (SBC Only).... 194
Table 4-10: Mediant 800C Gateway & E-SBC SBC Session Capacity per Capabilities with Gateway195
Table 4-11: Channel Capacity per DSP Firmware Template for Mediant 1000B Analog Series 196
Table 4-12: Channel Capacity per DSP Firmware Template for Mediant 1000B BRI Series 197
Table 4-13: Channel Capacity per DSP Firmware Templates for Mediant 1000B E1/T1 Series 198
Table 4-14: Transcoding Sessions Capacity per MPM According to DSP Firmware Template for Mediant 1000B 200

Table 4-15: MP-1288 Gateway Sessions Capacity 202
Table 4-16: Transcoding Capacity per Coder-Capability Profile for Mediant 2600 E-SBC 203
Table 4-17: Transcoding Capacity per Coder-Capability Profile for Mediant 4000 SBC 205
Table 4-18: Transcoding Capacity per Coder-Capability Profile for Mediant 4000B SBC 207
Table 4-19: Transcoding Capacity per Coder-Capability Profile for Mediant 9000 SBC 209
Table 4-20: Channel Capacity per Detection Feature for Mediant 9000 SBC 210
Table 4-21: Transcoding Capacity per Profile for a Single Media Transcoder 211
Table 4-22: Forwarding Capacity per MC Instance Type 213
Table 4-23: Transcoding Capacity per c4.4xlarge MC 213
Table 4-24: Transcoding Capacity for 2-vCPU Mediant VE SBC on OpenStack/VMware 215
Table 4-25: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on OpenStack/VMware 217
Table 4-26: Transcoding Capacity for 4-vCPU Mediant VE SBC on OpenStack/VMware 217
Table 4-27: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on OpenStack/VMware 219
Table 4-28: Transcoding Capacity for 8-vCPU Mediant VE SBC on OpenStack/VMware 219
Table 4-29: Channel Capacity per Detection Feature for 8-vCPU Mediant VE SBC on OpenStack/VMware 221
Table 4-30: Transcoding Capacity for Mediant VE SBC on c4.2xlarge 221
Table 4-31: Transcoding Capacity for Mediant VE SBC on c4.8xlarge 222
Table 4-32: Channel Capacity per Detection Feature for Mediant VE SBC on Amazon EC2 224
Table 4-33: Transcoding Capacity for 2-vCPU Mediant VE SBC on Hyper-V 225
Table 4-34: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on Hyper-V 226
Table 4-35: Transcoding Capacity for 4-vCPU Mediant VE SBC on Hyper-V 227
Table 4-36: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on Hyper-V 228
Table 4-37: Transcoding Capacity per Profile for a Single MT 229
Table 4-38: Transcoding Capacity per Profile for a Single vMT 230
Table 5-1: Capacity for Signaling, Media and Registered Users per Product 233
Table 5-2: Capacity per Feature 235
Table 5-3: Mediant 500 MSBR Capacity per PSTN Assembly and Capabilities 236
Table 5-4: Mediant 500L MSBR Capacity per PSTN Assembly and Capabilities 237
Table 5-5: Mediant 800/B MSBR Channel Capacity per PSTN and Capabilities 238
Table 5-6: Mediant 800C MSBR Channel Capacity per PSTN and Capabilities 240
Table 6-1: Supported RFCs 243
Table 6-2: Supported SIP Functions 247
Table 6-3: Supported SIP Methods 247
Table 6-4: Supported SIP Headers 248
Table 6-5: Supported SDP Fields 249
Table 6-6: Supported SIP Responses 249

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: June-13-2018

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 Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

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
Gateway and SBC Product Series
Mediant 500L Gateway and E-SBC Hardware Installation Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 500 E-SBC Hardware Installation Manual
Mediant 500 E-SBC User's Manual
Mediant 800 Gateway and E-SBC Hardware Installation Manual
Mediant 800 Gateway and E-SBC User’s Manual
Mediant 1000B Gateway and E-SBC Hardware Installation Manual
Mediant 1000B Gateway and E-SBC User’s Manual
MP-1288 Hardware Installation Manual
MP-1288 High-Density Analog Media Gateway User's Manual
Mediant 2600 E-SBC Hardware Installation Manual
Mediant 2600 E-SBC User’s Manual

Document Name
Mediant 4000 SBC Hardware Installation Manual
Mediant 4000 SBC User’s Manual
Mediant 9000 SBC User’s Manual
Mediant 9000 SBC Hardware Installation Manual
Mediant SE SBC Installation Manual
Mediant VE SBC Installation Manual
Mediant Software SBC Virtual and Server Editions User's Manual
MSBR Product Series
Mediant 500L MSBR Hardware Installation Manual
Mediant 500L MSBR User’s Manual
Mediant 500 MSBR Hardware Installation Manual
Mediant 500 MSBR User’s Manual
Mediant 800 MSBR Hardware Installation Manual
Mediant 800 MSBR User’s Manual

Document Revision Record

LTRT	Description
26957	Initial document release for Version 7.2.
26963	Capacity updated for Mediant 9000, Mediant 4000/B detection features, and Mediant 9000 with Media Transcoders.
26968	Mediant VE High-Capacity VMware capacity; Mediant 500L Gateway & E-SBC capacity (hybrid).
26969	Patch Version 7.20A.001; Typo in Mediant 4000B SBC capacity table.
26970	Patch Version 7.20A.001 updates: Mediant VE SBC virtual platforms (Amazon EC2 and SR-IOV); Registered users capacity updated for 1/2/4 vCPU 4 GB RAM Hyper-V; Capacity added for Amazon EC2 and SR-IOV.
26980	VoIPerfect updates; Capacity table updates; RFCs added.
26983	Patch Version 7.20A.002; G.722.2 added to AMR-WB.
26987	Patch Version 7.20A.100.
26990	Capacity updates - MP-1288; Mediant VE (c4.2xlarge, c4.8xlarge, with Media Transcoders); Mediant 9000.
26994	Update to section 'Multiple SRSs and SRS Redundancy for SIPRec'; new feature 'Debug for Remote Web (HTTP) Services'; constraint VI-140547 added; SRTP-RTP capacity updated for Mediant SE DL360p G8 20-cores and DL360 G9 8-cores; Mediant VE c4.8xlarge removed.
26998	OVR capacity; WebRTC capacity.
26999	Note added to Gateway and SBC Capacity for Mediant VE SBC and vMT-type Media Transcoder.
27083	Patch Version 7.20A.104.001.

LTRT	Description
27084	Typos.
27090	Patch Version 7.20A.150.004.
27091	▪ New 7.20A.150.004 features: Analog Voice Interface Support on Mediant 500L E-SBC/Gateway; Ringback and Held Tones per User; Same VLAN ID for Multiple Ethernet Devices ▪ Updated 7.20A.150.004 sections: Routing Back to Sender; IP Group Parameter Representation in Call Setup Rules; Skype User Presence Notification for Non-Skype Endpoint Devices; FXS Line Testing (typo); Resolved Constraints (VI 143342); MSBR Known Constraints (VI 141108); SIP Signaling, Media and User Capacity (Mediant 500 E-SBC, Mediant 500 MSBR, Mediant 800 MSBR) ▪ Updated 7.20A.150.004 tables: Mediant 500 Hybrid E-SBC (with Gateway) Media & SBC Capacity; Mediant 800/B Gateway & E-SBC SBC Session Capacity per Capabilities (SBC Only)
27092	▪ Patch Version 7.20A.106.003. ▪ Modifications to Ver. 7.20A.150.004: ✓ Updated section: Session Capacity Increases ✓ New feature: Prefix String for External Line Enhancement ✓ Capacity tables: Mediant VE on KVM; Mediant 800/B Gateway & E-SBC Channel Capacity per Capabilities
27095	▪ Patch Version 7.20A.152.009 (SBC/Gateway) ▪ Patch Version 7.20A.152.003 (SBC/Gateway) ▪ Updates to Patch Version 7.20A.150.004: ✓ New feature - High-Availability Disconnect ✓ Modified feature description - Console Access Mode ✓ Modified feature description - Snapshot Load through CLI ✓ Modified feature description - Routing Back to Sender ▪ Capacity updates: SIPRec; Mediant 500 MSBR; Mediant 800 MSBR
27099	Capacity updated for 8-vCPU Mediant VE SBC on OpenStack/VMware.
27241	▪ Patch Version 7.20A.154.007 (SBC/Gateway) ▪ Updates to 7.20A.150.004: ✓ Modified feature description - OVR Support in High-Availability Mode
27242	▪ Patch Version 7.20A.154.025 (MSBR) ▪ Updates to 7.20A.154.007: Compatible AudioCodes One Voice Operations Center version
27246	▪ Patch Version 7.20A.154.052 (SBC/Gateway) ▪ Global replacement of "EMS" and "SEM" with "One Voice Operations Center"
27247	▪ Patch Version 7.20A.154.059 (SBC/Gateway) ▪ VI 143930 added to Patch Version 7.20A.150.004
27249	▪ Patch Version 7.20A.156.009 (SBC/Gateway) ▪ Capacity figures
27250	▪ Additional resolved constraints for Patch Version 7.20A.156.009.
27251	Patch Version 7.20A.154.061 (MSBR).
27252	Patch Version 7.20A.156.023 (SBC/Gateway).
27254	Patch Version 7.20A.156.041 (Mediant 9000 Only).
27256	Patch Version 7.20A.158.009

LTRT	Description
27257	▪ Patch Version 7.20A.154.078 (MSBR). ▪ Transcoding Mode parameter name change (7.20A.158.009)
27258	Patch Version 7.20A.158.012 (SBC and Gateway)
27260	Patch Version 7.20A.200.019 (SBC and Gateway) Patch Version 7.20A.158.035 (SBC and Gateway)
27261	▪ Patch Version 7.20A.200.038 (MSBR) ▪ Resolved constraint 148119 added to Patch Ver. 7.20A.158.035 (SBC/Gateway) ▪ New features added to Patch Ver. 7.20A.200.019 (SBC and Gateway): ✓ Performance Monitoring Thresholds Included in ini File ✓ ENUM Query Enhancement for Call Setup Rules
27265	▪ Patch Version 7.20A.162.001 (Mediant 9000 SBC only) ▪ Patch Version 7.20A.158.056 (SBC and Gateway) ▪ Updates to 7.20A.200.019: ✓ NGINX alarms and CLI commands ✓ SFTP for Packaged Configuration file ✓ New feature - IDS alarm improvements feature added ✓ New feature - alarm tables enhancements ✓ New feature - Retry-After header ✓ New feature - enhanced cross validation for UDP ports ✓ New feature - randomized expire time ✓ New feature - variables for Message Manipulation ✓ New feature – parameter name changes from "Prefix" to "Pattern"
27267	▪ Patch Version 7.20A.200.550 (SBC and Gateway) ▪ Version 7.20A.158.056: VI150995 and VI152028 added as resolved constraints ▪ Version 7.20A.200.019: Update (TFTP) to Packaged Configuration File ▪ RFCs added (7866, 7245, 8068, 7865, 6341)
27268	▪ Patch Version 7.20A.162.017 (SBC and Gateway) ▪ Patch Version 7.20A.100: New feature - acCertificateExpiryNotification
27270	▪ Patch Version 7.20A.202.112 (SBC, Gateway and MSBR series) ▪ Note added for SbcPerformanceProfile parameter

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 Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document describes the release of Version 7.2. This includes new products, new hardware features, new software features, known constraints, and resolved constraints.

Note:

- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available License Keys that can be purchased, please contact your AudioCodes sales representative.
- Open source software may have been added and/or amended. For further information, visit AudioCodes Web site at https://www.audiocodes.com/services-support/open-source or 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 Web site at https://www.audiocodes.com/library/technical-documents.

1.1 Software Revision Record

The following table lists the software versions released in Version 7.2.

Table 1-1: Software Revision Record

Software Version	Date
Media Gateway and SBC Series	
Beta Version (7.20A.000.042)	April 2016
7.20A.001	July 2016
7.20A.002	November 2016
7.20A.100	December 2016
7.20A.104.001	March 2017
7.20A.150.004	May 2017
7.20A.106.003	June 2017
7.20A.152.003	June 2017
7.20A.152.009	July 2017
7.20A.154.007	August 2017
7.20A.154.044	September 2017
7.20A.154.052	October 2017
7.20A.154.059	October 2017
7.20A.156.009	November 2017
7.20A.156.023	November 2017
7.20A.156.041	December 2017
7.20A.158.009	January 2018

Software Version	Date
7.20A.158.012	February 2018
7.20A.200.019	February 2018
7.20A.158.035	March 2018
7.20A.162.001	April 2018
7.20A.158.056	April 2018
7.20A.200.550	May 2018
7.20A.162.017	May 2018
7.20A.202.112	June 2018
MSBR Series	
7.20A.150.004	May 2017
7.20A.154.025	August 2017
7.20A.154.061	November 2017
7.20A.154.078	February 2018
7.20A.200.038	March 2018
7.20A.202.112	June 2018

1.2 Products Supported in Release 7.2

Products (new and existing) supported in this release are listed in the table below:

Table 1-2: Products Supported in Release 7.2

Product	Telephony Interfaces			Ethernet Interfaces	USB	OSN	WAN
	FXS/FXO	BRI	E1/T1				
Media Gateway and SBC Product Series							
Mediant 500 Gateway & E-SBC	-	-	1/1	4 GE	2	-	-
Mediant 500L Gateway & E-SBC	4/4	4	-	4 GE	1	-	-
Mediant 800B Gateway & E-SBC	12/12	8	2	4 GE / 8 FE	2	√	-
Mediant 800C Gateway & E-SBC	12/12	8	4	4 GE / 8 FE	2	√	-
Mediant 1000B Gateway & E-SBC	24/24	20	6/8	7 GE	-	√	-
MP-1288 Gateways & E-SBC	288/0	-	-	2 GE	1	-	-
Mediant 2600 E-SBC	-	-	-	8 GE	-	-	-
Mediant 4000 SBC	-	-	-	8 GE	-	-	-
Mediant 4000B SBC	-	-	-	8 GE	-	√	-
Mediant 9000 SBC	-	-	-	12 GE	-	-	-
Mediant SE SBC	-	-	-	12 GE	-	-	-
Mediant VE SBC	-	-	-	12 GE	-	-	-
Mediant CE SBC	-	-	-	12 GE	-	-	-
MSBR Product Series							
Mediant 500 MSBR	4/4 (or 8 FXS)	2	1	4 GE	2	-	GbE; Fiber; ADSL2+/VDSL2; SHDSL; 3G Cellular (USB)
Mediant 500L MSBR	4/4	2		4 GE	1	-	GbE; Fiber; ADSL2+/VDSL2; 3G Cellular (USB)
Mediant 800B MSBR	12/12	8	2	4 GE / 8 FE (Optional PoE)	2	√	GbE; Fiber; 4 E1/T1 WAN; ADSL2+/VDSL2; SHDSL; 3G Cellular (USB)
Mediant 800C MSBR	12/12	8	4	4 GE / 8 FE (Optional PoE)	2	√	GbE; Fiber; 4 E1/T1 WAN; ADSL2+/VDSL2; SHDSL; 3G Cellular (USB)

Note:

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

This page is intentionally left blank.

2 Gateways and SBCs

This chapter describes new features, known constraints and resolved constraints relating to Gateway and SBC functionalities.

2.1 Version GA

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

2.1.1 New Features

New features introduced in the GA version include the following:

2.1.1.1 New Product - Media Transcoder Device

AudioCodes' Media Transcoder (MT) delivers high-capacity DSP-based transcoding in conjunction with AudioCodes' field-proven SBC product family (currently, supported only by Mediant 9000 SBC) enabled with the Media Transcoding Cluster feature. AudioCodes MT is a modular solution, supporting up to three field-upgradable transcoding modules in a single 1-U chassis. As transcoding needs increase, multiple AudioCodes MT devices can be added to form a cluster configuration giving virtually unlimited scalability along with HA cluster redundancy.

The main hardware specifications of the Media Transcoder include:

- 1U chassis design, suitable for 19-inch rack mounting
- Eight 100/1000Base-T Ethernet ports, supporting 1+1 Ethernet port redundancy
- Dual Power Supply modules, providing power load sharing and AC power redundancy
- Modular scalability from one to up to three MPM12B DSP modules

For more information on the Media Transcoding Cluster feature, see Section 2.1.1.26 on page 31.

2.1.1.2 New GUI for Web-based Management Tool

This feature introduces a new graphical user interface (GUI) for the device's Web-based management tool (Web interface). The new GUI offers the following new features:

- New modern look-&-feel design, making configuration more intuitive and improving user experience.
- Topology view showing a graphical display of the core SIP configuration entities (IP Groups, SIP Interfaces, Media Realms, and Trunk Groups), enabling the administrator to easily build and view the SIP topology.
- Network view showing a graphical display of the core networking entities (IP interfaces, Ethernet Devices, Ethernet Groups, and Physical Ethernet ports), enabling the administrator to easily build and view the main network topology.
- Improved navigation to Web pages, facilitating configuration.
- Indication icons of configured table rows. Navigation pane and tables display icons indicating the number of configured table rows, invalid row configuration, and invalid associations with other table rows.
- Easy access to associated configuration entities while configuring an entity.
- Fewer user clicks to save configuration and reset device.
- Quick access to vital call statistics.
- Search based on strings and IP address.

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.3 New CLI Structure

This feature introduces a new structure of the CLI that is more aligned with the hierarchical structure of the navigation tree of the new Web GUI launched in this version. The modified structure allows faster and easier navigation between commands in the CLI. The CLI provides fewer folders, allowing the administrator to access commands with fewer key strokes. Many command names have also been made more concise to eliminate visual "clutter".

The CLI commands are now organized under the following main folders:

- `configure system`: Contains system-related commands (e.g., `clock`, `snmp settings` and `web`)
- `configure network`: Contains IP network-related commands (e.g., `interface`, `dhcp-server` and `nfs`)
- `configure voip`: Contains voice-over-IP related commands (e.g., `ip-group`, `sbc`, `gateway` and `media`)
- `configure troubleshoot`: Contains logging-related commands (e.g., `syslog`, `logging` and `test-call`)

The debugging-related commands are located under the root directory for quick access.

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.4 Interworking between SIP and SIP-I Endpoints

This feature provides support for interworking between SIP and SIP-I endpoints for SBC calls. SIP-I is a flavor of the SIP protocol, which carries a message body consisting of the User Part of the ISDN protocol (or ISDN User Part - ISUP) over IP networks. SIP-I endpoints are entities that are connected to the SS7 network, referred to as the ISDN user part (ISUP) domain. The device supports the SIP-I Application-layer signaling protocol, which is a standard for encapsulating a complete copy of the SS7 ISUP message in SIP messages, according to ITU-T Q.1912.5, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part*.

For the interworking process, the device maps between ISUP data and SIP headers. For example, the E.164 number in the Request-URI of the outgoing SIP INVITE is mapped to the Called Party Number parameter of the IAM message and the From header of the outgoing INVITE is mapped to the Calling Party Number parameter of the IAM message. The ISUP data is included in SIP messages using the Multipurpose Internet Mail Extensions (MIME) body part,

The feature also introduces support for manipulating ISUP data, using the existing Message Manipulations table. For a complete description of the ISUP manipulation syntax, refer to the *SIP Message Manipulation Reference Guide*.

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

ISUP Body Handling sbc-isup-body-handling [IpProfile_SBCISUPBodyHandling]	Defines the handling of ISUP data for interworking between SIP and SIP-I. ▪ [0] Transparent = (Default) ISUP data is passed transparently (as is) between endpoints (SIP-I to SIP-I calls). ▪ [1] Remove = Delete the ISUP body from the INVITE message. ▪ [2] Create = Adds ISUP body to outgoing INVITE message.

Note: For more information on the feature, please contact your AudioCodes sales representative.

Applicable Products: All.

Applicable Application: SBC.

2.1.1.5 Maximum Call Duration per Gateway and SBC Calls

This feature provides support for configuring the maximum call duration for SBC and Gateway calls. Up until this release, maximum call duration could only be configured globally and applied to all calls for both applications—Gateway and SBC—using the MaxCallDuration parameter (which is now obsolete).

The feature allows the administrator to configure maximum call duration for the following:

- SBC calls:
  - All SBC calls (i.e., globally)
  - Specific SBC calls (using IP Profiles)
- Gateway calls: All Gateway calls (globally) only

The feature is useful for ensuring that calls are properly terminated, making device resources available for new calls.

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

SBC Max Call Duration `sbc-mx-call-duration` [SBCMaxCallDuration]	Defines the maximum duration (in minutes) for each SBC call (global). If the duration is reached, the device terminates the call. The valid range is 0 to 35,791, where 0 is unlimited duration. The default is 0. Note: The parameter replaces the MaxCallDuration parameter.
Max Call Duration `sbc-max-call-duration` [IpProfile_SBCMaxCallDuration]	Defines the maximum duration (in minutes) for each SBC call that is associated with the IP Profile. If the duration is reached, the device terminates the call. The valid range is 0 to 35,791, where 0 is unlimited duration. The default is the value configured for the SBCMaxCallDuration parameter.
GW Max Call Duration `gw-mx-call-duration` [GWMaxCallDuration]	Defines the maximum duration (in minutes) for each Gateway call (global). If the duration is reached, the device terminates the call. The valid range is 0 to 35,791, where 0 is unlimited duration. The default is 0. Note: The parameter replaces the MaxCallDuration parameter.

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.6 Protection against Known Malicious Attacks

This feature provides support for protecting the device against malicious attacks on SBC calls using a Malicious Signature database. The feature allows the administrator to configure a database of malicious signature patterns which identify specific scanning tools used by attackers to search for a SIP server in a network. The feature identifies and protects against SIP (Layer 5) threats by examining any new inbound SIP dialog message. Once the device identifies an attack based on the configured malicious signature patterns, it marks the SIP message as invalid and discards it or alternatively, rejects it with a SIP response (by default 400).

The malicious signatures are based on the SIP User-Agent header and employ the same syntax used for Message Manipulation rules. For example:

- Malicious signature is defined as follows for a malicious scanner:

  ```
  header.user-agent.content prefix “malicious scanner”
  ```

- Malicious signature is defined as follows for the scanning tool "sip-scan":

  ```
  Header.User-Agent.content prefix 'sip-scan'
  ```

The protection applies only to new dialogs (e.g., INVITE messages) and unauthenticated dialogs. The Malicious Signature database does not apply to the following:

- Calls from IP Groups where classification is by Proxy Set.
- In-dialog SIP sessions (such as refresh REGISTER requests, re-INVITE etc.)
- Calls from users that are registered with the device.

By default, the device is installed with a list of known attackers, called the Malicious Signature Database. The Malicious Signature database is presented in table format. The administrator can add, edit or delete entries. As a safety mechanism, if all entries are deleted and the device is subsequently reset, the table is populated again with all the signatures. In addition, the administrator can export or import a Malicious Signature database through HTTP, HTTPS, or TFTP.

The feature is enabled by a new global parameter (see below). The existing Message Policy table provides an additional default Message Policy rule for the Malicious Signature database ("MaliciousSignatureDBProtection"). To apply the Malicious Signature database to calls, the administrator needs to associate this default Message Policy rule to an SBC SIP Interface in the existing SIP Interface table.

The Malicious Signature database can also be used with the existing Intrusion Detection System (IDS) feature. A new IDS reason has been added to denote Malicious Signature detections (Signature DB invalid). This allows the administrator to enable SNMP alarm generation ("Dialog establishment failure") if any signature is detected by the device.

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

Malicious Signature Table [MaliciousSignatureDB]	Defines up to 30 malicious signature patterns (rows). [MaliciousSignatureDB] FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name, MaliciousSignatureDB_Pattern; [\MaliciousSignatureDB]
Message Policy Table [MessagePolicy_UseMaliciousSignatureDB]	New parameter: Malicious Signature Database [MessagePolicy_UseMaliciousSignatureDB] = Enables the use of the Malicious Signature database for SIP Interfaces that are assigned the Message Policy.
`configure voip > sbc malicious-signature-database <export-csv-to | import-csv-from> <URL>`	Exports/imports a Malicious Signature database file (in *.csv format) to/from a server (HTTP, HTTPS, or TFTP).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SE/VE.

Applicable Application: SBC.

2.1.1.7 Block SIP Requests from Registered Users when Address Different

This feature provides support for blocking (rejecting) SIP dialog-initiating requests (such as INVITE messages) from a user that is registered with the device, but where the source address (IP address and/or port) and transport type (e.g., UDP) is different to that registered for the user (during the REGISTER message process). When the device rejects a request, it reports the rejection (Classification failure) through the already supported Intrusion Detection System (IDS), by sending an SNMP trap.

The device can verify whether the IP address and port are different only if the transport protocol is UDP; otherwise, the device verifies only the IP address. The verification is performed before any of the device's call handling processes (i.e., Classification, Manipulation and Routing) and applies only to User-type IP Groups.

Note that the feature does not apply to registration refreshes. These requests are accepted even if their source address is different to that registered for the user.

To support the feature, the following existing parameters have been modified:

User Security Mode	Parameter name and optional values modified:

[SRD_BlockUnRegUsers]	Defines the blocking (reject) policy of incoming SIP dialog-initiating requests from users (except REGISTER requests). When the device rejects a request, it sends a SIP 500 "Server Internal Error" response to the user. ▪ [0] Accept All = (Default) Accepts requests from registered and unregistered users. ▪ [1] Accept Registered Users = Accepts requests from registered users only and rejects requests from users not registered with the device. ▪ [2] Accept Registered Users from Same Source = Accepts requests only from registered users whose source address is the same as that registered with the device. All other requests are rejected.
User Security Mode [SIPInterface_BlockUnRegUsers]	Parameter name and optional values modified: Defines the blocking (reject) policy of incoming SIP dialog-initiating requests from users (except REGISTER requests). When the device rejects a request, it sends a SIP 500 "Server Internal Error" response to the user. ▪ [-1] Not Configured (default) ▪ [0] Accept All = Accepts requests from registered and unregistered users. ▪ [1] Accept Registered Users = Accepts requests from registered users only and rejects requests from users not registered with the device. ▪ [2] Accept Registered Users from Same Source = Accepts requests only from registered users whose source address is the same as that registered with the device. All other requests are rejected.

Applicable Products: All.

Applicable Application: SBC.

2.1.1.8 Enhanced Dialog Classification Based on Proxy Set

This feature provides support for enhanced classification of incoming SIP dialogs to IP Groups, based on Proxy Set when multiple Proxy Sets are configured with the same IP address. For more information, refer to the *User's Manual*.

Applicable Products: All.

Applicable Application: SBC.

2.1.1.9 Wildcard Denoting 18x Responses in Message Manipulation Rules

The feature provides support for using the 'x' wildcard in SIP message manipulation rules to denote all SIP 18x responses (e.g., 180, 181, 182 and 183). The wildcard is used in the 'Message Type' field, which defines the type of message to which the manipulation is applied. For example, to configure a rule that applies to any SIP 18x in response to an INVITE message, the following syntax is used in the 'Message Type' field:

```
invite.response.18x
```

Up until this release, the exact 18x response (e.g., 180, 181, 182 or 183) had to be specified. For example, if the administrator wanted to apply the same message manipulation to all 18x responses, multiple rules with the same syntax except for the specified 18x response had to be configured.

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.10 Increase in Maximum SIP Message Size

This feature provides support for configuring the existing parameter, MaxSIPMessageLength to up to 100 KB. The device rejects SIP messages exceeding the configured size. Up until this release, the maximum SIP message size could be configured to 50 KB.

Applicable Products: All.

Applicable Application: Gateway and SBC.

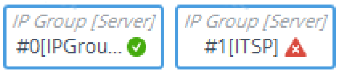
2.1.1.11 IP Group Keep-Alive Connectivity Status Indication

This feature provides support for displaying the connectivity status of Server-type IP Groups. As the Proxy Set defines the actual address of the IP Group, the connectivity check (or keep-alive) by the device is done to this address. Note that for the feature to be relevant, the keep-alive mechanism must be enabled for the associated Proxy Set (using the existing parameter, ProxySet_EnableProxyKeepAlive).

The connectivity status is indicated as follows:

- Topology View: The status is displayed as a color-coded icon in the IP Group element:
    - Green: Keep-alive is successful (i.e., connectivity with IP Group). Note that if the device rejects calls destined to this IP Group due to low QoE (e.g., low MOS), the indication still appears green.
    - Red: Keep-alive failure (i.e., no connectivity with IP Group).

  An example of these icons is shown below:



- IP Group table: The status is displayed in the new read-only field, 'Proxy Set Connectivity' (IPGroup_ProxySetConnectivity ini parameter or `show voip proxy sets status` CLI command):
    - "NA": Functionality is not applicable in the following cases:
        - If Server-type IP Group and the Proxy Keep-Alive mechanism is disabled
        - If User-type IP Group
    - "Not Connected": Keep-alive failure (i.e., no connectivity with IP Group)
    - "Connected": Keep-alive is successful (i.e., connectivity with IP Group)

Applicable Products: All.
Applicable Application: Gateway and SBC.

2.1.1.12 Enhanced Configuration of Allowed Coder Groups

This feature provides support for enhanced configuration design of Allowed Audio Coder Groups and Allowed Video Coder Groups:

- Allowed Audio Coder Groups: User-defined coders can now be configured through the Web interface. Up until now, it could only be configured through ini file and CLI. In addition, configuration now consists of two tables – parent and child. The parent table configures the ID and name; the child configures the coders of the selected group.
- Allowed Video Coder Groups: Now configurable through the Web interface. Up until this release, Allowed Video Coders Groups could only be configured through ini file and CLI.

Allowed Audio Coders Groups `configure voip > coders-and-profiles allowed-audio-coders-groups` [AllowedAudioCodersGroups]	Parent table that defines the names of the Allowed Audio Coder Groups. [AllowedAudioCodersGroups] FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name; [\AllowedAudioCodersGroups]

Allowed Audio Coders `coders-and-profiles allowed-audio-coders <group index/coder index>` [AllowedAudioCoders]	Child table of the Allowed Audio Coders Groups that defines the audio coders of the group. [AllowedAudioCoders] FORMAT AllowedAudioCoders_Index = AllowedAudioCoders_AllowedAudioCodersGroupName, AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID, AllowedAudioCoders_UserDefineCoder; [\AllowedAudioCoders]
Allowed Video Coders Groups `configure voip > coders-and-profiles allowed-video-coders-groups` [AllowedVideoCodersGroups]	Parent table that defines the names of the Allowed Video Coder Groups. [AllowedVideoCodersGroups] FORMAT AllowedVideoCodersGroups_Index = AllowedVideoCodersGroups_Name; [\AllowedVideoCodersGroups]
Allowed Video Coders `coders-and-profiles allowed-video-coders <group index/coder index>` [AllowedVideoCoders]	Child table of the Allowed Video Coders Groups that defines the video coders of the group. [AllowedVideoCoders] FORMAT AllowedVideoCoders_Index = AllowedVideoCoders_AllowedVideoCodersGroupName, AllowedVideoCoders_AllowedVideoCodersIndex, AllowedVideoCoders_UserDefineCoder; [\AllowedVideoCoders]

Applicable Products: All.

Applicable Application: SBC.

2.1.1.13 Enhanced Audio Coder Groups Configuration

The feature provides the following enhancements:

- The Coders table is obsolete and has been replaced by the existing Coder Groups table (formerly known as Coder Group Settings table), facilitating configuration.
- Coder Group configuration through ini file is now done using two ini file tables:
  - AudioCodersGroups: Defines the Coder Group name/index
  - AudioCoders: Defines the coders for the Coder Groups
- Enumerations are now used for coder names, packetization times, and rate.
- Deletion of Coder Groups through the Web interface is now possible by the Delete Group button, which when clicked, deletes the currently displayed Coder Group. Up until this release, to delete a Coder Group, the administrator had to remove all its coders one by one.

Applicable Products: All.

Applicable Application: All.

2.1.1.14 Enhanced Dial Plan Tagging

This feature provides the following Dial Plan Tagging enhancements:

- CDR fields for source and destination dial plan tags (see Section 2.1.1.18 on page 28)
- Exporting and importing Dial Plan rules in CSV file format to a local folder on the PC running the Web client, through the Web interface (already supported through CLI)
- Increased capacity:
  - Max. Dial Plans:
    - Mediant 2600/4000: 25
    - Mediant VE: 50

    - Others: 10
- Max. dial plan rules:
    - Mediant 2600/4000: 10,000
    - Mediant VE (< 16G): 2,000
    - Mediant VE (> 16G incl.): 20,000
    - Others: 2,000

Applicable Products: All.

Applicable Application: SBC.

2.1.1.15 Increase in Maximum Network Interfaces

This feature provides support for an increase in the maximum number of IP network interfaces that can be configured in the IP Interfaces table (InterfaceTable). The increase is from 100 to 1024 network interfaces. The maximum capacity of Media Realms and Ethernet Devices that can be configured in the Media Realms table (CpMediaRealm) and Ethernet Devices table (DeviceTable) were also increased to 1,024.

Applicable Products: Mediant 9000; Mediant VE/SE.

Applicable Application: SBC.

2.1.1.16 CDR Local Storage for Gateway Calls

This feature provides support for CDR local storage for Gateway calls. Up until now, CDR local storage was supported only for SBC calls. Configuration for CDR local storage is the same as SBC (CDRLocalMaxFileSize, CDRLocalMaxNumOfFiles, and CDRLocalInterval) and Logging Filters table for selectively enabling the feature.

Due to the feature, customization of locally stored Gateway CDRs is also supported. As a result, the new optional value Local Storage Gateway [9] has been added to the 'CDR Type' (GWCDRFormat_CDRType) parameter in the Gateway CDR Format table.

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

Applicable Application: Gateway.

2.1.1.17 Historical CDRs Display for SBC Calls

This feature provides support for displaying historical CDRs (last 4,096 CDRs) for SBC calls in the device's management interfaces. Up until now, historical CDRs were displayed for Gateway calls only.

To support the feature, the new table, SBC CDR History has been added:

- Web: Monitor menu > Monitor tab > VoIP Status folder > SBC CDR History
- CLI: `show voip calls history sbc`

The table includes the following CDR fields: Call End Time, IP Group, Caller, Callee, Direction, Remote IP, Duration, Termination Reason, and Session.

The name of the existing CDR History table for Gateway calls has been changed to Gateway CDR History:

- Web: Monitor menu > Monitor tab > VoIP Status folder > GW CDR History
- CLI: `show voip calls history gw`

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.18 New CDR Fields

This feature introduces the following new CDR fields:

- **LegId:** Identifies each leg by a unique ID number within a specific call session. The field is assigned a unique number for each leg in the call session. This unique identification enhances the ability of applications such as AudioCodes One Voice Operations Center to analyze call data according to various segments in the call session.

- **Trigger:** Describes the reason of the call. The field name can be customized, using the Gateway CDR Format and SBC CDR Format tables. The tables show the field as "Trigger" (ini file enumeration 439) in the 'Field Type' field. The field can have one of the following values:
  - "Normal": regular call
  - "Refer": call as a result of call transfer
  - "AltRoute": call as a result of alternative routing
  - "Forward": call as a result of forwarded call
  - "Reroute": call re-routed due to a voice issue (e.g., broken RTP connection)
  - "Forking": call as a result of call forking
- **SrcDialPlanTags / DestDialPlanTags:** Indicate Dial Plan tags (source and destination) used for the call (if the Dial Plan Tagging feature is implemented). The field name can be customized using the SBC CDR Format table. The table shows the field as "Source Dial Plan Tags" (ini file enumeration 816) and "Destination Dial Plan Tags" (ini file enumeration 817) in the 'Field Type' field.

Note that the ini file enumerations of the optional values in the 'Field Type' field of the Gateway and SBC CDR Format tables have changed.

Applicable Products: All.
Applicable Application: Gateway and SBC.

2.1.1.19 Maximum RADIUS Requests

The feature provides support for an increase in the maximum number of RADIUS requests that the device can send simultaneously to a RADIUS server. Up until this release, the device could send only up to 254 concurrent RADIUS requests (RADIUS Accounting and Authentication together).

This feature provides the following support:

- All Products: Up to 201 concurrent RADIUS requests **per** RADIUS service type (Accounting or Authentication) and per RADIUS server (up to three servers per service type).
- Mediant 2600, Mediant 4000, Mediant 9000 and Mediant SW Only: Up to 201 concurrent RADIUS requests per RADIUS service type (Accounting or Authentication), per RADIUS server and per local port, which has been increased from one port to the following:
  - Mediant 2600/4000: two local ports
  - Mediant 9000/SW: four local ports
  - For all other products: only one port is supported.

  For example, for Mediant 4000, 402 (201 * 2) concurrent RADIUS requests can be sent for Authentication and 402 (201 * 2) for Accounting. These numbers are per RADIUS server.

Applicable Products: All.

Applicable Applications: SBC and Gateway.

2.1.1.20 Increase in Maximum Network ACL Rules

This feature provides support for an increase in the maximum number of network Access Control List (ACL) or firewall rules that can be configured in the Firewall table (AccessList). The increase is from 50 to 500 rules.

Applicable Products: Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.
Applicable Application: SBC.

2.1.1.21 Enhanced TLS Certificate Support

This feature provides support for the following TLS enhancements:

- Private Key size (in bits): The private key size can now be configured to 4096 bits, which provides very high strength key. Up until this release, the key size options were 512, 768, 1024, and 2048. The private key size is configured by the existing parameter, Private Key Size (Web - TLS Contexts page > TLS Context Certificate link; CLI - configure network > tls > private-key generate).
- Signature algorithm for certificates: The signature algorithm can now be configured to SHA-256 or SHA-512. Up until this release, the device supported only the SHA-1 algorithm (default). The algorithm is configured by the new parameter, Signature Algorithm (Web - TLS Contexts page > TLS Context Certificate link; CLI - configure network > tls > certificate signature-algorithm).
- Enabling validation of extensions (keyUsage and extentedKeyUsage) of peer certificates is now configured per TLS Context. Up until this release, it was configured globally. To support the feature, the global parameter, RequireStrictCert has been replaced by the new TLS Context table parameter, TLSContexts_RequireStrictCert.
- Configuring the TLS Server Certificate Expiry Check feature per TLS Context. Up until this release, it was configured globally for all TLS Contexts. (No change in parameters.)

Applicable Products: All.
Applicable Application: Gateway and SBC.

2.1.1.22 TLS Certificate Verification

This feature provides a change in support for verifying the address in the TLS certificate received from a Server-type IP Group whose Proxy Set is configured as an FQDN. Up until now, the device verified that the DNS-resolved IP address of the FQDN matched the IP address in the certificate. Now, the device verifies that the FQDN of the Proxy Set matches the FQDN in the certificate. The feature is enabled by the existing parameter, PeerhostNameVerificationMode.

Applicable Products: All.

Applicable Application: SBC.

2.1.1.23 Disable Reuse of TLS Connections

This feature provides support for disabling the use of the same TLS connection for new SIP requests between the device and a SIP user agent (UA). Up until this release, the device always used the same TLS connection (successful handshake) that was established in the initial SIP dialog request, for subsequent requests (e.g., INVITE or REGISTER) sent to the UA. The feature is supported by the existing parameter, EnableTCPConnectionReuse, which up until this release, was applicable only to TCP.

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.1.24 UDP Port Spacing by Four

This feature provides support for local UDP port allocation in "jumps" (*spacing*) of four. Up until this release, UDP port spacing could be configured to 5 or 10.

The device allocates ports for a media channel (leg) from a pool of UDP ports. The pool starts from a port configured by the existing parameter, BaseUDPPort and each leg is assigned several consecutive ports for its usage (e.g. RTP, RTCP, and T.38). The spacing between ports per leg is configured by the existing parameter, UdpPortSpacing. For example, if port spacing is configured to four and BaseUDPPort to 6000, the allocated ports are 6000 for the first leg, 6004 for the second leg, 6008 for the third leg, and so on.

(For all other products, UDP port spacing is 10 as supported in previous releases).

Applicable Products: Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.
Applicable Application: SBC.

2.1.1.25 Sending of Silence RTP Packets to SIP Trunks

The feature provides support for the device to interoperate with SIP entities (e.g., SIP Trunks) that wait for the first incoming packet before sending RTP (e.g., early media used for ringback tone and IVR) during media negotiation. The feature enables the device to generate "silence" RTP packets to the SIP entity upon receipt of a SIP response (183 with SDP) from the SIP entity. In other words, these packets serve as the first incoming packets for the SIP entity. The device stops sending the silence packets when it receives RTP packets from the peer side (which it then forwards to the SIP entity).

Note: To generate silence packets, DSP resources are required (except for calls using G.711).

Generate RTP `sbc-generate-rtp` [IPProfile_SBCGenerateRTP]	Enables generation of silence RTP packets until audio RTP packets are detected. ▪ [0] None (Default) = No silence packets are generated. ▪ [1] Until RTP Detected = Silence packets are generated

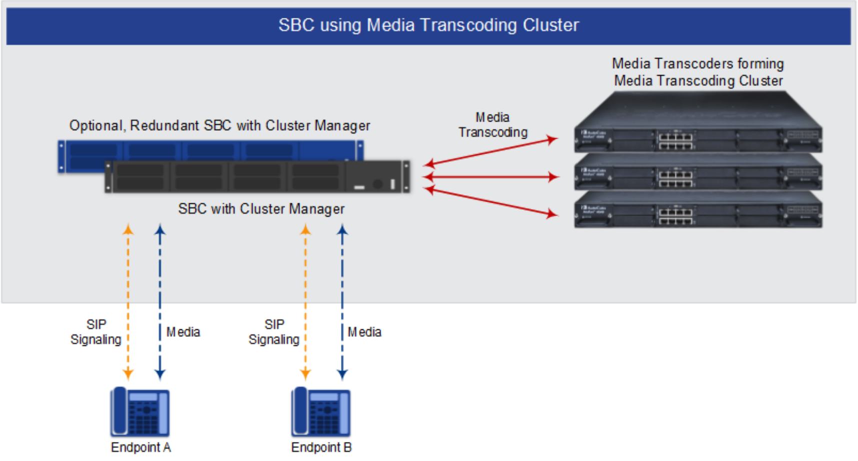
Applicable Products: All.

Applicable Application: SBC.

2.1.1.26 Media Transcoding Cluster Feature

The feature provides support for the SBC device (Mediant 9000) to use an external source of DSP resources for media-related features requiring DSPs, for example, vocodec transcoding, fax transcoding, and DTMF detection. The external farm (*cluster*) of DSP resources is provided by AudioCodes transcoding devices (up to six), called *Media Transcoders*. The SBC device itself functions as the cluster manager and does not perform any transcoding (does not utilize any of its local DSP resources). The Media Transcoders provide only DSP functionality (i.e., no SIP routing functionalities) and a few system functionalities such as debugging through Syslog. The Media Transcoders are "hidden" from the endpoints being serviced by the device. The Media Transcoding Cluster feature is a licensed feature, requiring the SBC device to be installed with a suitable License Key.

The device with the Cluster Manager functionality can still operate as a High-Availability (HA) system. If a switchover occurs, transcoding sessions handled by the Media Transcoding Cluster are maintained.


SBC using Media Transcoding Cluster
Media Transcoders forming Media Transcoding Cluster
Optional, Redundant SBC with Cluster Manager
Media Transcoding
SBC with Cluster Manager
SIP Signaling
Media
SIP Signaling
Media
Endpoint A
Endpoint B

The main benefit of the Media Transcoding Cluster feature is scalability. The Media Transcoder doesn't require licensing of its transcoding resources and allows utilization of all its DSP resources. However, the maximum possible transcoding capacity by the SBC device is according to the License Key of the SBC device, regardless of the number of deployed Media Transcoders.

After initial configuration of the Media Transcoders through their Web interfaces, subsequent management is through the device's Web interface. The Cluster Manager running on the SBC device can perform various actions on the Media Transcoders such as software upgrade, resetting, and locking (to stop allocating transcoding sessions).

The Media Transcoding Cluster feature provides load-sharing and cluster redundancy between multiple Media Transcoders. Load sharing attempts to distribute the transcoding sessions load between the Media Transcoders. For cluster redundancy, the following modes can be configured:

- HA (default): The Cluster Manager guarantees that in case of a failure in a Media Transcoder, sufficient DSP resources are available on other Media Transcoders to take over the active transcoding sessions of the failed Media Transcoder.
- Best Effort: The Cluster Manager allocates sessions for transcoding to the Media Transcoder without guaranteeing availability of DSP resources on other Media Transcoders should the Media Transcoder fail. Therefore, Media Transcoders utilize all their DSP resources, if required.

The following SNMP alarms have been added for the Media Transcoding Cluster feature:

- AcMtcmClusterHaAlarm: Cluster HA usage exceeds 100% (insufficient DSP resources available on other Media Transcoders to take over active transcoding sessions of a failed Media Transcoder).
- acMtceNetworkFailureAlarm: Connectivity failure between Media Transcoder and Cluster Manager.
- acMtceSwUpgradeFailureAlarm: Software upgrade or Auxiliary file load failure on Media Transcoder.
- acMtceHwTemperatureFailureAlarm: Media Transcoder chassis temperature reaches critical threshold.
- acMtceHwFanTrayFailureAlarm: Media Transcoder Fan Tray module failure.
- acMtcePsuFailureAlarm: Media Transcoder Power Supply module failure.

Note:

- A Media Transcoding Cluster cannot be shared by multiple devices.
- Each Ethernet port on the SBC device associated with the cluster network interface ("Cluster-Media-Control"), communicates with a single Media Transcoder and supports up to 5,000 media transcoding sessions.

Cluster Manager Management Interface	
Cluster Manager Functionality configure network > mtc settings > enable-mtc-sbc [EnableMtcSbc]	Enables the Cluster Manager feature.
MTC Redundancy Mode [MtcRedundancyMode]	Defines the redundancy mode for the Media Transcoding Cluster. ▪ HA Mode (Default) ▪ Best Effort
Application Type [InterfaceTable_ApplicationTypes]	New option: [23] Cluster Media + Control = IP interface for interfacing between the Cluster Manager and Media Transcoders.
MTC Graceful Timeout configure network > mtc settings > graceful-timeout [MtcGracefulTimeout]	Defines the graceful period (in seconds).

Media Transcoders Table configure network > mtc entity [MtcEntities]	Defines Media Transcoders associated with the Cluster Manager.
Transcoding Cluster Log	Displays logged activities of Media Transcoders and Cluster Managers.
Media Transcoders Management Interface	
Cluster Manager IP Address [ClusterManagerIpAddress]	Defines the Cluster Manager by IP address of the corresponding cluster interface (Cluster Media + Control network interface).

Applicable Products: Mediant 9000.

Applicable Application: SBC.

2.1.1.27 New Quality of Service PMs and Alarms

The feature provides support for new quality-of-service performance monitoring (PM) call metrics that can be calculated by the device. The metrics measure network quality and call success rates and are calculated globally, per SRD and per IP Group.

- Answer-seizure ratio (ASR): The number (in percentage) of answered calls (i.e. number of seizures resulting in an answer signal) out of the total number of attempted calls (seizures). The metric is calculated for the outgoing call leg. Note that forwarded calls are not considered in the calculation. The PMs related to the metric include:
  - PM_gwSBCASR: ASR for all (global) entities (i.e., all IP Groups and SRDs)
  - PM_gwSBCIPGroupASR: ASR per IP Group
  - PM_gwSBCSRDASR: ASR per SRD
- Network Effectiveness Ratio (NER): The number (in percentage) of successfully connected calls out of the total number of attempted calls (seizures). The metric measures the ability of the network to deliver a call to the called terminal. In addition to answered calls, the following response codes are regarded as successfully connected calls: 408 (Request Timeout), 480 (Temporarily Unavailable), and 486 (Busy Here). The metric is calculated for the outgoing call leg. Note that forwarded calls are not considered in the calculation. The PMs related to the metric include:
  - PM_gwSBCNER: NER for all (global) entities (i.e., all IP Groups and SRDs)
  - PM_gwSBCIPGroupNER: NER per IP Group
  - PM_gwSBCSRDNER: NER per SRD
- Average Call Duration (ACD): The ACD plus the session disconnect time (SDD) is the time from when the SIP 200 OK is received to when the SIP Bye message is sent. The metric is calculated for both the incoming and outgoing call legs. The PMs related to the metric include:
  - PM_gwSBCACD: ACD for all (global) entities (i.e., all IP Groups and SRDs)
  - PM_gwSBCIPGroupACD: ACD per IP Group
  - PM_gwSBCSRDACD: ACD per SRD

Minor and major thresholds can be configured per metric (in the new table, Performance Profile table - see below) that if crossed, minor and major severity alarms are generated. The following new SNMP alarms are supported:

- acASRThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.111): The alarm is raised when the configured ASR minor and major thresholds are crossed.
- AcNERThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.113): The alarm is raised when the configured NER minor and major thresholds are crossed.
- acACDThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.112): The alarm is raised when the configured ACD minor and major thresholds are crossed.

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

Performance Profile table `configure system > performance-profile` [PerformanceProfile]	Defines alarm thresholds per metric (ASR, ACD and NER). [PerformanceProfile] FORMAT PerformanceProfile_Index = PerformanceProfile_Entity, PerformanceProfile_IPGroupName, PerformanceProfile_SRDName, PerformanceProfile_PMType, PerformanceProfile_MinorThreshold, PerformanceProfile_MajorThreshold, PerformanceProfile_Hysteresis, PerformanceProfile_MinimumSample, PerformanceProfile_WindowSize; [\PerformanceProfile]

Applicable Products: All.

Applicable Application: SBC.

2.1.1.28 Actions upon Poor Voice Quality Detections

The feature supports configuration of actions that must be performed if poor quality of experience is detected. Configuration is based on Quality of Service rules, using the new Quality of Service Rules table. The following actions can be performed:

- Reject calls to an IP Group for a user-defined duration if a user-defined threshold (major or minor) of a specified metric is crossed. The metric can be voice quality (i.e., MOS), bandwidth (supported in the previous release), ASR, NER, or ACD.

  When the device rejects calls to an IP Group based on a QoS rule, the device raises the new SNMP alarm, acIpGroupNoRouteAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.114).

  When the device rejects a call due to an ASR, NER or ACD threshold crossing, it sends the new SIP response, 850 (Signaling Limits Exceeded). This SIP response code has been added to the Alternative Routing Reasons table (SBCAlternativeRoutingReasons). If it is configured and the device rejects a call due to threshold crossing, it searches in the IP-to-IP Routing table for an alternative routing rule.
- Use an alternative IP Profile for the IP Group upon threshold crossings of voice quality or bandwidth. The alternative IP Profile can be used:
  - For all new calls: If poor voice quality or bandwidth threshold is crossed, the alternative IP Profile is used for all **new** calls. All the parameters of the alternative IP Profile can be configured.

As a result of the feature, the MediaEnhancementProfile and MediaEnhancementRules tables are now obsolete.

Quality of Service Rules Table `configure voip > qoe quality-of-service-rules` [QualityOfServiceRules]	Defines Quality of Service rules. [QualityOfServiceRules] FORMAT QualityOfServiceRules_Index = QualityOfServiceRules_IPGroupName, QualityOfServiceRules_RuleMetric, QualityOfServiceRules_Severity, QualityOfServiceRules_RuleAction, QualityOfServiceRules_CallsRejectDuration, QualityOfServiceRules_AltIPProfileName; [\QualityOfServiceRules]

Applicable Products: All.

Applicable Application: SBC.

2.1.1.29 Bitrate Configuration for SILK and Opus Coders

The feature provides support for configuring the bitrate of the Opus coder. In addition, the default of the existing SilkMaxAverageBitRate parameter, which configures the bitrate for the SILK coder has changed to 50,000.

Opus Max Average Bitrate `configure voip > sip-definition settings > opus-max-avg-bitrate` [OpusMaxAverageBitRate]	Defines the maximum average bit rate (bps) for the Opus coder. The valid value range is 6000 to 50,000. The default is 50,000.

Applicable Products: All.

Applicable Application: SBC.

2.1.1.30 Core Dump File Deletion

This feature provides support for deleting the core dump file from the device's flash memory through CLI. As supported in the previous release, the core dump file is created by the device upon device crash (enabled by the EnableCoreDump parameter) and is a copy of the memory image of the device at the time of the crash.

To support the feature, the following new command has been added under the root CLI directory (enable mode):

```
# clear debug-file
```

Applicable Products: All.

Applicable Application: Gateway and SBC.

2.1.2 Known Constraints

This chapter lists known constraints in Release 7.2.

Table 2-1: Known Constraints in Release 7.2

Incident	Description	Status
134449	RADIUS-based authentication of SIP users and RADIUS-based authentication of login username and password for management users are currently not supported. **Applicable Products:** Mediant 2600; Mediant 4000.	Resolved in Version 7.20A.100 (See Section 2.4.3)
-	The SIPRec feature is not supported when the Media Transcoding Cluster feature is used. **Applicable Products:** Mediant 9000.	-
132977	To upgrade from software version 7.0 to 7.2, the device must first be upgraded to the latest 7.0 version (later than 7.00A.058.002) and only then to version 7.2. **Applicable Products:** Mediant 2600; Mediant 4000; Mediant 9000; Mediant SE/VE.	Resolved in Version 7.20A.100 (See Section 2.4.3)
133943	SRTP with ARIA encryption is not supported for SBC sessions. **Applicable Products:** All.	-
-	ARM is not supported. **Applicable Products:** All.	Resolved in Version 7.20A.100 (See Section 2.4.3)
131889	When importing a Dial Plan file (*.csv file), it is recommended to configure the SyslogDebugLevel parameter to **No Debug**. **Applicable Products:** All.	Resolved in Version 7.20A.100 (See Section 2.4.3)
116756	The device interworks with devices that support RTP bundling. However, it does not support receipt of bundled multimedia sessions on the same port and instead, it uses different ports for each media type (audio and video). By default, the device removes all bundle-related attributes ('a=group:BUNDLE' and 'a=ssrc') from the SDP offer and answer. **Applicable Products:** All.	-
-	CLI scripts used in Version 6.8 are not fully supported and need to be modified in order to be fully compatible in Version 7.2. **Applicable Products:** All.	-
-	Downgrade from Version 7.2 to a previous software version only works if the device was upgraded to Version 7.2 and no configuration changes were done after the upgrade. **Applicable Products:** All.	-
-	The combination of SBC direct media and termination features such as the handling of 3xx, REFER, and INVITE with Replaces is supported only if all SIP user agents support INVITE/re-INVITE without SDP, and terminations of semi-attendant transfer and INVITE with Replaces during call ringing is not supported with direct media. **Applicable Products:** All.	-

Incident	Description	Status
-	SBC Delayed SDP offer is supported only by devices that support DSP transcoding. **Applicable Products:** All.	-
-	High Availability (HA) for One-Voice Resiliency (OVR) is not fully supported (signaling may not function correctly in certain scenarios). **Applicable Products:** HA-Supporting Devices.	Resolved in Version 7.20A.150 (See Section 2.7.3)
-	High Availability (HA) for WebRTC is not fully supported (signaling may not function correctly in certain scenarios). **Applicable Products:** HA-Supporting Devices.	-
-	The SBC User Info table limits the maximum number of users that can be configured (half of the maximum per device). **Applicable Products:** All.	-
-	Out-of-dialog SIP REFER message for SBC calls is forwarded transparently; the subsequent NOTIFY message is not fully supported. **Applicable Products:** All.	-
-	Transrating of G.711, G.726, and G.729 for SBC calls from packetization time (ptime) 100/120 msec to 10/30/50 msec is not supported. **Applicable Products:** Mediant 1000B.	-
-	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.	-
-	Ring to Hunt Group feature does not function when early media is used. **Applicable Products:** Mediant 8xx.	-
-	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 5xx; Mediant 8xx; Mediant 1000B.	-
-	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 8xx; Mediant 1000B.	-
-	When using the DSP Cluster feature, the local DSP resources on the SBC cannot be utilized. **Applicable Products:** Mediant 9000; Mediant VE.	-

Incident	Description	Status
-	When SRTP is enabled, RTP Redundancy and M-factor cannot operate together. In other words, SRTP can operate with RTP Redundancy greater than 0 or with m-factor greater than 1, but not with both. **Applicable Products:** Mediant 1000B.	-
-	When IP-to-IP or IP-to-PSTN calls use SRTP with ARIA encryption, the number of simultaneous calls is limited to 31. **Applicable Products:** Mediant 5xx; Mediant 8xx.	-
-	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 1000B GW & E-SBC.	-
-	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 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.	-
	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:** All.	-
-	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 5xx; Mediant 8xx; Mediant 1000B.	-
-	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 5xx; Mediant 8xx.	-
-	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 5xx; Mediant 8xx; Mediant 1000B.	-
-	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 5xx; Mediant 8xx; Mediant 1000B.	-

Incident	Description	Status
18743	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 5xx; Mediant 8xx; Mediant 1000B.	-
-	The SILK coder is currently not supported. **Applicable Products:**Mediant 500L Gateway & E-SBC.	-
-	The ISDN BRI American variants (NI2, DMS100, 5ESS) are partially supported by the device. Please contact your AudioCodes representative before implementing this protocol. **Applicable Products:**Mediant 5xx; Mediant 8xx; Mediant 1000B.	-
-	All the device's trunks must belong to the same Protocol Type (i.e., either E1 or T1). **Applicable Products:** Mediant 8xx; Mediant 1000.	-
-	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 8xx; Mediant 1000B.	-
-	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 8xx; Mediant 1000B.	-
-	Core Dump to the internal flash device may take up to 30 minutes. During this period, a red alarm LED is lit. **Applicable Products:** Mediant 2600; Mediant 4000.	-
-	Hyper-Threading (HT) is supported for Mediant VE in a VMWare environment only and with special configuration (refer to the *Mediant VE SBC Installation Manual*). For all other environments of Mediant SW, HT should be disabled in the BIOS setting of the server. **Applicable Products:** Mediant SW.	-
70318	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:** All.	-

Incident	Description	Status
79630	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. **Applicable Products:** All.	-
-	Configuration file constraints when upgrading from 6.8 to 7.2: ▪ CLI Script file of 6.8 cannot be loaded to a 7.2 device ▪ Incremental ini file of 6.8 cannot be loaded to a 7.2 device **Applicable Products:** All.	-
-	The 'Monitor Destination Status' read-only field on the HA Settings page does not refresh automatically. **Applicable Products:** Mediant 4000 HA.	-
-	An unnecessary scroll bar appears on many of the Web pages when using 1280 x 1024 screen resolution. **Applicable Products:** All.	-
-	After manual switchover in HA Revertive Mode, the Web Home page isn’t refreshed. A workaround is to refresh the Home page to get the updated status. **Applicable Products:** Mediant 2600; Mediant 4000.	-
-	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 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000.	-
87767	The Web Search feature may produce incorrect search results. **Applicable Products:** All.	Resolved in Version 7.20A.100
-	The fax counters, 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the Status & Diagnostics page do not function correctly. **Applicable Products:** Mediant 8xx; Mediant 1000B.	-
-	From Release 7.2, configuration through SNMP is not supported. **Applicable Products:** All.	-
-	The MIB-II ifTable, ifxTable, and entPhysicalTable are not supported. **Applicable Products:** Mediant 9000; Mediant SW.	-
58872	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 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000.	-
-	Only the CLI commands explicitly mentioned in the *Installation Manual* are supported. **Applicable Products:** Mediant 9000; Mediant SW.	-

Incident	Description	Status
131651	Before upgrading a new firmware, the number of system snapshots should be reduced to maximum five snapshots. If the number of snapshots is above five, the user should delete some of the snapshots to free the disk space required for the burn & upgrade process. **Applicable Products:** Mediant 9000; Mediant VE/SE.	-

2.1.3 Resolved Constraints

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

Table 2-2: Resolved Constraints in Release 7.2

Incident	Description
124526	When upgrading the device from Version 6.8 to 7.2, the RADIUS Accounting server IP address and port (configured by the RADIUSAccServerIP and RADIUSAccPort parameters in Version 6.8) do not migrate to the new RADIUS Servers table (RadiusServers) in Version 7.2. The administrator is recommended to configure the Accounting server's IP address and port in the new table after the device has been upgraded. **Applicable Products:** Mediant SW.

2.2 Patch Version 7.20A.001

This patch version includes only new features.

2.2.1 New Features

New features introduced in this patch version include the following.

2.2.1.1 New Virtualized Platforms for Mediant VE SBC

This feature provides support for the following new virtualized platforms for the Mediant VE SBC:

- Amazon Web Service (AWS) - Elastic Compute Cloud (EC2): The device now supports Amazon cloud computing services (AWS EC2). The device needs to run on EC2 instance type c4.2xlarge. This platform also provides transcoding services.
- SR-IOV: Mediant SBC VE can now utilize SR-IOV acceleration of Intel NICs to reach even higher capacity than before. The Virtual Function (VF) of the SR-IOV capable Intel NICs should be mapped to the Ethernet ports used by the device's media IP network interfaces. SR-IOV acceleration has been verified by AudioCodes on OpenStack platform with 8 vCPUs, 64-GB RAM and Intel® 82599 NICs.

Applicable Products: Mediant VE SBC.

Applicable Application: SBC.

2.2.1.2 Enhanced Dial Plan Tags and Call Setup Rules

This feature provides support for enhanced use of Dial Plan tags:

- Dial Plan queries by Call Setup Rules (CSR): Up until now, CSR was executed only during the routing process where a CSR was assigned to an IP-to-IP Routing rule. Now, the CSR can be executed for a classified source IP Group immediately before the routing process (i.e., Classification > Manipulation > Dial Plan table > CSR > Routing) and therefore, the result of the CSR (i.e., source and/or destination tag) can be used as the matching characteristics for locating a suitable IP-to-IP Routing rule. The CSR can query the Dial Plan table for a specified search key in a specified Dial Plan to obtain the corresponding tag. The CSR can also change (modify) the name of the obtained tag.

  Multiple tags for complex routing schemes. This is typically required when the source and/or destination of the call needs to be categorized with more than one characteristics. For example, tags can be used to categorize calls by department (source user) within a company, where only certain departments are allowed to place international calls.
- LDAP queries by CSR: A specific LDAP server (LDAP Servers Group) can now be configured for the CSR.
- Message Manipulation: Source and destination tags (*srctags* and *dsttags*) can now be used in Message Manipulation rules. For example, a rule can use a specific source tag as a condition for adding a specific header to outgoing SIP messages. Note that message manipulation cannot be used to modify tags.

The following parameter changes have been made to support the feature:

- A new parameter 'Call Setup Rules Set ID' in the IP Group table that associates a CSR with the IP Group.
- Call Setup Rules table:
  - New parameter: 'Query Type' to choose between a Dial Plan and LDAP query.
  - New parameter: 'Query Target' to specify the Dial Plan name in which to search for the prefix or to specify the LDAP server (LDAP Servers Group) for LDAP queries by the CSR.

  - The 'Attributes To Query' parameter (in the Web interface) has been changed to 'Search Key' as it can now be used for Dial Plan queries (prefix number) as well as LDAP queries (Attribute).

- New arguments (*dialplan.found* and *dialplan.result*) for the 'Condition' parameter in the Call Setup Rules table (e.g., *dialplan.found exists and dialplan.result=='uk'*).

Applicable Products: All.

Applicable Application: SBC.

2.2.1.3 Enhanced SIP-SIP-I Interworking

This feature provides the following enhancements for interworking SIP and SIP-I endpoints:

- Support for additional ISUP fields and corresponding Message Manipulation capabilities.
- Support for attaching any ISUP body to any SIP message, using Message Manipulation rules.
- Support for the French (France) specification, SPIROU (Système Pour l'Interconnexion des Réseaux OUverts), which regulates Telecommunication equipment that interconnect with networks in France. Therefore, a new IP Profile parameter ('ISUP Variant') has been added that allows the administrator to configure the ISUP variant to SPIROU or ITU-92 (default). For ITU—92, the device sets the Content-Type header to "version=itu-t92+; base=itu-t92+"; for SPIROU, it sets it to "version=spirou; base=itu-t92+".
- Support for configuring the SIP Content-Type and Content-Disposition header values, using Message Manipulation rules.
- Handling SIP-I suspend-resume messages (on-hook or on-hold), using a proprietary SIP header (X-Ac-Action) in SIP messages, using Message Manipulation rules.

Applicable Products: All.

Applicable Application: SBC.

2.2.1.4 Triggering Special Call Actions using X-AC-Action SIP Header

This feature provides support for triggering the device to perform special call actions. For example, it can be used for disconnecting a call when interworking SIP-I and SIP endpoints, and an ISUP SUS (suspend) message is received. This is configured using Message Manipulation rules with AudioCodes' proprietary X-AC-Action SIP header. The actions that can be performed include:

- Disconnect a call (optionally, after a user-defined time):
  disconnect[;delay=<time in ms>]
- Resume previously suspended call:
  abort-disconnect

  Example:

  ```
  X-AC-Action: abort-disconnect
  ```

- Reply to the message with a SIP response without forwarding the response to the other side:
  reply[;response=<response code, e.g., 200>]
- Switch IP Profile for the call (re-INVITE only), as defined in the IP Group:
  switch-profile [;reason=<reason - PoorInVoiceQuality or PoorInVoiceQualityFailure >]

For example, the below rule disconnects a call after 3 sec if the received SIP INFO message contains the ISUP SUS field:

```
MessageManipulations 2 = "INFO suspend", 2, "info.request",
"body.isup.sus exists", "header.x-ac-action", 0,
"'disconnect;delay=3000,reply'", 0;
```

Applicable Products: All.

Applicable Application: SBC.

2.2.1.5 VoIPerfect Feature

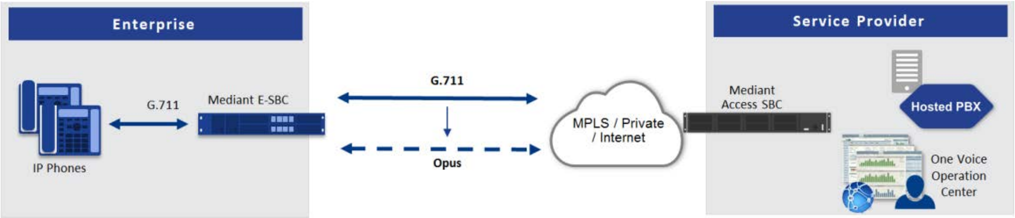
This feature provides support for a new application called VoIPerfect™ that combines AudioCodes' access and enterprise SBC technology. VoIPerfect ensures high call quality (MOS) between the Enterprise SBC and the Access SBC (located at the Internet service provider / ISP) during periods of WAN network issues (packet loss and bandwidth reduction).

VoIPerfect also guarantees that 95% of calls will achieve a Perceptual Evaluation of Speech Quality (PESQ) score greater than or equal to 3.6, if the summation of bandwidth overuse and packet loss is less than or equal to 25%. ISPs can therefore offer such service level agreements (SLAs) to their customers. For more information, contact your AudioCodes sales representative.

By ensuring high call quality even in adverse network conditions, VoIPerfect can reduce costs for ISPs such as SIP trunk providers and Unified Communications as a Service (UCaaS) by eliminating the need for dedicated WAN links (such as MPLS and leased links) and instead allow the use of standard broadband Internet connections. However, it can also be used in tandem with existing infrastructure.

The feature is applicable only to G.711 calls and uses the Opus coder for ensuring call quality. VoIPerfect can be implemented in one of the following modes:

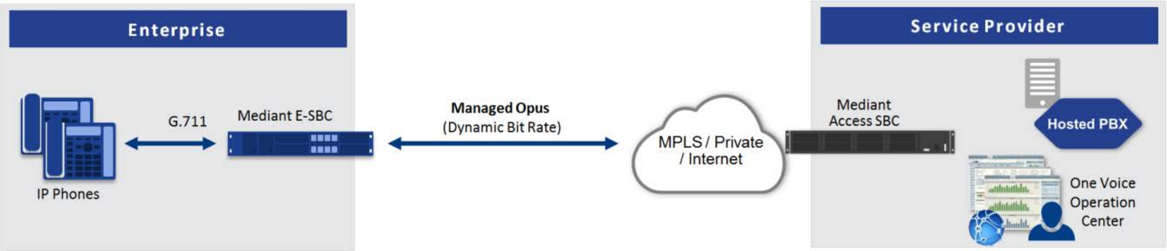
- **Smart Transcoding:** If the SBC (Enterprise or Access) detects WAN network impairments during a call between the Enterprise SBC and Access SBC, the SBC employs voice transcoding by switching the coder from G.711 to Opus for that specific call only. Transcoding is done only on the path between the Enterprise SBC and Access SBC. As Smart Transcoding is applied only on a per call basis, it preserves valuable DSP resources that may be required for other functionalities. An advantage of using the Opus coder is that it consumes less bandwidth than G.711 and overcomes packet loss (by dynamic packet redundancy), allowing the SBC to support more concurrent calls than with G.711 for the same bandwidth. This mode is useful for WAN networks that are relatively stable, allowing the use of G.711 whenever possible and switching to Opus only during adverse network conditions.



Configuration of the Enterprise SBC:

- Device's License Key includes the SBC transcoding feature
- Coder Groups:
  - Coders Group with G.711
  - Coders Group with Opus
- Allowed Audio Coders Groups:
  - Allowed Audio Coders Group with G.711
  - Allowed Audio Coders Group with Opus
- Main IP Profile:
  - Extension Coders Group: Coders Group with G.711

    - Allowed Audio Coders: Allowed Audio Coders Group with G.711
    - Allowed Coders Mode: Restriction
    - RTCP Feedback: Feedback On
    - Voice Quality Enhancement: Enable
  - Alternative IP Profile:
    - Extension Coders Group: Coders Group with Opus
    - Allowed Audio Coders: Allowed Audio Coders Group with Opus
    - Allowed Coders Mode: Restriction
    - RTP Redundancy Mode: Enable
    - RTCP Feedback: Feedback On
    - Voice Quality Enhancement: Enable
    - Max Opus Bandwidth: 80000
  - Quality of Service Rules:
    - Rule Metric: Poor InVoice Quality
    - Alternative IP Profile Name: name of Alternative IP Profile (above)
- **Managed Opus:** If the SBC detects WAN network impairments during a call using the Opus coder between the Enterprise SBC and Access SBC, it can adjust the Opus coder's attributes (e.g., bit rate) for that specific call to ensure high voice quality is maintained. The advantage of the Opus coder is that its' bit rate can change dynamically according to bandwidth availability. This mode is useful for unstable networks, allowing Opus to dynamically adapt to adverse network conditions.



  Configuration of the Enterprise SBC:

  - Coders Group with Opus
  - Allowed Audio Coders Group with Opus
  - IP Profile:
    - Extension Coders Group: Coders Group with Opus
    - Allowed Audio Coders: Allowed Audio Coders Group with Opus
    - Allowed Coders Mode: Restriction
    - Voice Quality Enhancement: Enable
    - RTCP Feedback: Feedback On
    - Max Opus Bandwidth: 0

Configuration of the Access SBC for both methods:

- Coder Groups:
  - Coders Group with G.711 and Opus
  - Coders Group with Opus
- Allowed Audio Coders Group with Opus
- IP Profile:
  - Extension Coders Group: Coders Group with G.711 and Opus
  - Voice Quality Enhancement: Enable
  - RTP Redundancy Mode: Enable

  - RTCP Feedback: Feedback On
  - Max Opus Bandwidth: 0
- Alternative IP Profile:
  - Extension Coders Group: Coders Group with Opus
  - Allowed Audio Coders: Allowed Audio Coders Group with Opus
  - Allowed Coders Mode: Restriction
  - Voice Quality Enhancement: Enable
  - RTP Redundancy Mode: Enable
  - RTCP Feedback: Feedback On
  - Max Opus Bandwidth: 0
- Quality of Service Rules:
  - Rule Metric: Poor InVoice Quality
  - Alternative IP Profile Name: name of Alternative IP Profile (above)

To support VoIPerfect, the device now supports the negotiation of Temporary Maximal Media Stream Bit Rate (TMMBR) for Opus coders. Through TMMBR, the device can receive indications of network quality and dynamically change the coder's payload bit rate accordingly during the call to improve voice quality. TMMBR is an RTCP feedback message (per RFC 4585) which enables SIP users to exchange information regarding the current bit rate of the media stream. The information can be used by the receiving side to change the media stream parameters (e.g., coder rate or coder) to enhance voice quality. TMMBR is negotiated in the SDP Offer/Answer model using the 'tmbr' attribute and following syntax:

```
a=rtcp-fb:<payload type> ccm tmmbr smaxpr=<sent TMMBR packets)
```

The device also supports another new SDP attribute, 'a=rtcp-rsize' that reduces the RTCP message size (as defined in RFC 5506). As feedback messages are frequent and take a lot of bandwidth, the attribute attempts to reduce the RTCP size. The attribute can only be used in media sessions defined with the AVPF profile. In addition, it must be included with sessions supporting TMMBR; otherwise, the call is rejected.

Note:

- VoIPerfect is applicable only to G.711 calls.
- If you are deploying a third-party device between the Enterprise SBC and Access SBC, make sure that the third-party device adheres to the following:
  - √ Enable RFC 2198 in SDP negotiation
  - √ Enable TMMBR in SDP negotiation
  - √ Forward the SDP with feedback (SAVPF) as is
  - √ Forward TMMBR messages as is
  - √ Forward RTCP messages as is (not terminate them)
  - √ (Smart Transcoding only) Forward re-INVITE messages for using Opus as is
  - √ (Smart Transcoding only) Forward the SIP header, X-Ac-Action as is

Applicable Products: Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

Applicable Application: SBC.

2.3 Patch Version 7.20A.002

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

2.3.1 New Features

New features introduced in this patch version are described in this section.

2.3.1.1 Load-Balancing of SBC Calls between Destination IP Groups

This feature provides support for load balancing of calls, belonging to the same source, to a set of call destinations known as an *IP Group Set*, which can include up to five IP Groups (Server-type and/or Gateway-type). The selected destination IP Group for each call depends on the configured load-balancing policy, which can be Round Robin, Random Weights, or Homing. Alternative routing within the IP Group Set is also supported whereby if a destination IP Group responds with a reject SIP response that is configured as a reason for alternative routing, or doesn't respond at all (i.e., keep-alive with its Proxy Set fails), the device attempts to send the call to the next IP Group (according to the policy). For example, for round-robin load-balancing, call 1 is sent to IP Group #1, call 2 to IP Group #2, and call 3 to IP Group #3. If the call sent to IP Group #1 is rejected, the device employs alternative routing and sends it to IP Group #4.

As a result of the feature, the following new parameters have been added:

- New tables:
    - IP Group Set (parent): Defines an IP Group Set (with a policy) for load balancing.
    - IP Group Set Member (child): Assigns IP Groups to the IP Group Set.
- IP-to-IP Routing table:
    - New optional value for 'Destination Type' field: "IP Group Set"
    - New field to assign an IP Group Set: 'IP Group Set'

Applicable Products: All.

Applicable Application: SBC.

2.3.1.2 Configurable FXS Off-hook Current

This feature provides support for configuring the FXS off-hook current for specific ports. FXS off-hook current is the current that the device supplies to the analog line when it is in off-hook state. Up until now, the FXS off-hook current was not configurable and fixed to 20 mA. Now, the administrator can increase the current to 35 mA using the new ini file parameter EnhancedFXSLineCurrent, where the value "0" is 20 mA (default) and "1" is 35 mA. A device reset is required for the parameter's settings to take effect. Configuration can be done only on the first (1) and last (24) ports per FXS connector.

Note that for the first FXS connector on FXS blade 1, the first port in the ini file is denoted as 0 and the last port as 23. The following configuration example sets specific first and last ports to 35 mA:

```
EnhancedFXSLineCurrent_0 = 1      ; Port 1 on FXS Blade 1
EnhancedFXSLineCurrent_23= 1      ; Port 24 on FXS Blade 1
EnhancedFXSLineCurrent_24 = 1     ; Port 25 on FXS Blade 1
EnhancedFXSLineCurrent_47 = 1     ; Port 48 on FXS Blade 1
EnhancedFXSLineCurrent_48 = 1     ; Port 49 on FXS Blade 1
EnhancedFXSLineCurrent_71 = 1     ; Port 72 on FXS Blade 1
EnhancedFXSLineCurrent_72 = 1     ; Port 1 on FXS Blade 2
```

Applicable Products: MP-1288.

2.3.2 Known Constraints

This section lists known constraints.

Table 2-3: Known Constraints in Version 7.20A.002

Incident	Description	Status
138581	Mediant Virtual Edition SBC with Microsoft Hyper-V hypervisor with 4 GB is not supported. **Applicable Products:** Mediant VE.	Resolved in Version 7.20A.100 (See Section 2.4.3)

2.3.3 Resolved Constraints

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

Table 2-4: Resolved Constraints in Version 7.20A.002

Incident	Description
138447	When the ini file includes parameter values that are over 50 characters, searching values in the Web interface causes the device to crash (reset). **Applicable Products:** All.
138371	When the device forwards a SIP re-INVITE message with more than one media (e.g. voice and fax) and receives a 200 OK with one media (e.g. RTP only), it sends a 488 response to the party that initiated the re-INVITE. As a result, the call fails. A workaround is to configure the fax parameters to send only one media. **Applicable Products:** SBC.
137859	When the UseSiptgrp parameter is configured to "Send & Receive", IP-to-Tel alternative routing does not function and the call fails. **Applicable Products:** Gateway.
137394	For PRI and BRI protocol-based calls, when a call is received from the PSTN with an empty display name, the call is sent to the IP with invalid display name. As a result, the call fails (rejected by IP side). **Applicable Products:** Gateway.
137384	When editing an IP Profile and the View button is clicked for the Extension Coder Group parameter, an error message appears. **Applicable Products:** SBC.
137356	Syslog displays responses to SIP OPTIONS messages with different SIDs compared to the OPTIONS, causing in problems with tracking messages and debugging. **Applicable Products:** All.
136808	The IPG field in the CDR displays the IP Group name only (instead of ID as well). **Applicable Products:** All.
136441	If configuration includes an invalid license pool service and host parameter, when trying to remove it, the device crashes (and resets). **Applicable Products:** SBC.
135501	The primary and secondary NTP server cannot be configured through CLI. **Applicable Products:** All.

2.4 Patch Version 7.20A.100

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

2.4.1 New Features

New features introduced in the GA version include the following:

2.4.1.1 Capacity Updates

This release introduces capacity updates to the following products:

- Mediant 1000 Gateway & E-SBC (Profile #6 for E1/T1)
- MP-1288: 588 (signaling and RTP-to-RTP; 350 registered users)
- Mediant 9000 SBC (180,000 registered users)
- Mediant 9000 SBC with Media Transcoder (180,000 registered users)
- Mediant VE SBC with Media Transcoders (new)

For more information, see Section 4.

Applicable Products: MP-1288; Mediant 9000 SBC; Mediant 9000 SBC with MT; Mediant VE SBC with MT/vMT.

2.4.1.2 OpenSSL Library Update

This version uses the latest OpenSSL library, which may have removed certain cipher suites from the default subset due to new vulnerabilities, hacks and computation advances. If you are using encrypted communications, you should verify that the cipher suites of both client and server roles are configured correctly in the TLS Contexts table so that they match peer abilities and desired security level. For a list of cipher suite configuration syntax, please visit the OpenSSL online documentation at https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

Applicable Products: All.

2.4.1.3 Integrated SBC Configuration Wizard in Web Interface

This feature provides **beta** support for the integration of the SBC Configuration Wizard into the device's Web interface. Up until now, the SBC Configuration Wizard was a stand-alone utility offered by AudioCodes.

The SBC Wizard provides a quick-and-easy method for initial configuration of your <device>. It guides you through a sequence of pages, assisting you in defining your setup and then finishing with a suitable configuration. The wizard is based on partial as well as fully-tested interoperability setups (configuration templates) between AudioCodes devices and a wide range of vendors, including SIP trunking providers, IP PBXs, and contact centers.

The wizard is accessed using the new Configuration Wizard button, located on the menu bar. The Auxiliaries page allows the upload of additional SBC configuration templates using the new Browse button for SBC Wizard Template files.

Applicable Products: SBC.

2.4.1.4 MP-1288 Support for SBC Application

MP-1288 now supports the SBC application. Up until now, it supported only the Gateway application (FXS interfaces). The device supports up to 300 concurrent SBC call sessions, 350 registered SBC users, and 800 SIP SUBSCRIBE messages. (Transcoding is not supported.)

Applicable Products: MP-1288.

2.4.1.5 AudioCodes One Voice Operations Center Support for MP-1288

AudioCodes One Voice Operations Center now supports the MP-1288 Analog Media Gateway.

Applicable Products: MP-1288.

2.4.1.6 MP-1288 Support for Cloud Resilience Package Application

MP-1288 now supports the Cloud Resilience Package (CRP) application. Up until now, this application was supported only by Mediant 5xx, Mediant 8xx, Mediant 1000B, Mediant 2600, Mediant 4000, and Mediant VE/SE SBCs.

Applicable Products: MP-1288.

2.4.1.7 New SNMP Alarms for MP-1288

This feature provides support for the following new SNMP alarms:

- AcModuleServiceAlarm – sent when multiple FXS ports on a specific FXS blade are out-of-service or a hardware fault occurs on the FXS blade.
- AcModuleOperationalAlarm - sent when an operational hardware failure occurs on the FXS ports or on the FXS blades (DSP and CPU).
- acPortServiceAlarm - sent is raised when an FXS port is out of service due to one of the following:
    - The Serial Peripheral Interface (SPI) connection with the port is lost.
    - The temperature of the port has exceeded the temperature threshold.
    - The port is inactive due to a ground fault.

Applicable Products: MP-1288.

2.4.1.8 New SNMP Alarm for License Pool Over-Allocation

This feature provides support for the new SNMP alarm, acLicensePoolOverAllocationAlarm, which the device sends when the SBC license received from the License Pool Manager has exceeded the maximum capacity supported by the device.

Note that the functionality of the alarms, acLicensePoolApplicationAlarm and acLicensePoolInfraAlarm were slightly modified in this release. For more information, refer to the *SNMP Reference Guide*.

Applicable Products: All.

2.4.1.9 New SNMP Alarm for TLS Certificate Expiration

This feature provides support for the new SNMP alarm, acCertificateExpiryAlarm, which the device sends when the TLS certificate of a configured TLS Context is about to expire or has expired. This alarm replaces the now obsolete trap, acCertificateExpiryNotification.

Applicable Products: All.

2.4.1.10 SNMP Version in Keep-Alive Trap

This feature provides support for indicating the device's SNMP version in the acKeepAlive trap. The version is shown in the trap Varbind, acBoardTrapGlobalsAdditionalInfo2 (SNMPVersion=SNMPv3 or SNMPv2c).

Applicable Products: All.

2.4.1.11 New SNMP Varbind for Serial Number

This feature provides support for including the device's serial number in the Variable Binding list (Varbind) of raised SNMP traps. A new Varbind, acBoardTrapGlobalsSystemSerialNumber has been added to include the serial number.

Applicable Products: All.

2.4.1.12 DH Key Size per TLS Context

This feature provides support for configuring the Diffie-Hellman (DH) key size per TLS Context. Up until now, the DH key size was a hard-coded, globally set 1024-bit key. The new feature gives administrators the option to select a 1024- or 2048-bit key size for DH. DH is an algorithm used chiefly for exchanging cryptography keys used in symmetric encryption algorithms like AES. To support the feature, a new parameter, 'DH Key Size' (TLSContexts_DHKeySize) with optional values 1024 (default) and 2048 has been added to the TLS Contexts table.

Applicable Products: All.

2.4.1.13 DTLS Version per TLS Context

This feature provides support for configuring the Datagram Transport Layer Security (DTLS) protocol version per TLS Context. The new feature gives administrators the option to select any version, Version 1.0, or Version 1.2. DTLS key negotiation protocol secures UDP-based media streams (according to RFC 5763 and 5764). To support the feature, a new parameter, 'DTLS Version' (TLSContexts_DTLSVersion) with optional values Any (default), DTLSv1.0, and DTLSv1.2 has been added to the TLS Contexts table.

Applicable Products: All.

2.4.1.14 RSA Public Key for SSH Authentication per Management User Account

This feature provides support for configuring a secure socket shell (SSH) public key per management-user account for accessing the CLI. Up until now, only one SSH public key could be configured (using the SSHAdminKey parameter), which applied to all user accounts. The feature is made possible by a new parameter in the Local Users table, called SSH Public Key (WebUsers_SSHPublicKey). The public key is used for authenticating remote users logging into the device's management interface through SSH (PKI). Connection to the management interface is established only when a successful handshake with the user’s private key occurs.

Applicable Products: All.

2.4.1.15 Increase in IP Network Interfaces, VLANs and Media Realms

This feature provides support for an increase in the maximum number of IP network interfaces (IP Interfaces table), VLANs (Ethernet Devices table), and Media Realms (Media Realms table) that can be configured, from 48, 48 and 64 respectively to 1,024.

Applicable Products: Mediant 2600; Mediant 4000.

2.4.1.16 Online Detection for Proxy Set Load Balancing

This feature provides support for configuring the minimum number of online proxies, in a Proxy Set, for the Proxy Set to be considered as online when Proxy Load Balancing is used. The feature is configured using the new Proxy Set table parameter, 'Min. Active Servers for Load Balancing' (ProxySet_MinActiveServersLB).

Applicable Products: All.

2.4.1.17 LED Indication for Software Upgrade

This feature provides support for the device's STATUS LED, located on the front panel of the chassis, to indicate that the device is currently upgrading its software (.cmp file). During an upgrade, the LED flashes green.

Applicable Products: Mediant 800.

2.4.1.18 Media Transcoding Cluster Enhancements

This feature provides the following enhancements for the Media Transcoding Cluster feature:

- Media Transcoders can be connected to the Cluster Manager through an Ethernet switch. Up until now, they could only be connected directly (not through a switch) to the Cluster Manager (i.e., port to port).
- Multiple Media Transcoders can be associated with the same Cluster interface. Up until now, each Cluster interface could be associated with only one Media Transcoder.
- The Cluster Manager can also be a Mediant VE SBC (currently, supported only by Mediant VE SBC based on OpenStack). Up until now, only Mediant 9000 could serve as a Cluster Manager.
- When the Cluster Manager is a Mediant VE SBC, the Media Transcoder can also be a virtualized machine (VM), referred to as "vMT" (virtualized Media Transcoder). Up until now, the Media Transcoder was based only on a hardware appliance, referred to as "MT". Note that the Media Transcoders can only be of one type (all MT or all vMT; a combination is not allowed).
- Maximum number of Media Transcoders:
  - MT (Hardware-based appliance): increased from six to eight
  - vMT: 5
- Configurable maximum bandwidth for Cluster interfaces. The bandwidth applies to each Cluster interface. The new parameter MtcClusterNetworkMaxBandwidth has been added to the Cluster Manager Settings page (Setup menu > IP Network tab > Transcoding Cluster folder > Cluster Manager Settings) and CLI (configure network > mtc settings > cluster-network-max-bandwidth). The range is 1 to 10,000 Mbps (default is 1,000 Mbps).
- SNMP alarm for bandwidth over-utilization of a Cluster interface. To support the feature, a new SNMP alarm, acClusterBandwidthAlarm has been added. The device generates the alarm with one of the following severity levels:
  - Minor: bandwidth utilization is between 85 and 90%
  - Major: bandwidth utilization is above 90%

Applicable Products: Mediant 9000; Mediant VE.

2.4.1.19 Register-Unregister per Trunk Group

This feature provides support for initiating register and un-register actions per Trunk Group in the Trunk Group Settings table (TrunkGroupSettings), using the Register and Un-Register commands. Up until now, when these actions were done in the Trunk Group Settings table, all Trunk Groups were affected.

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

2.4.1.20 Enhanced Row-Pointer Feature

This feature provides enhanced capabilities of row-pointer fields, which are used to assign index rows of other configuration tables to a current table row:

- The row-pointer field (drop-down list) allows the administrator to search by name for a referenced-table row.
- The row-pointer field displays the status of the referenced-table rows (e.g., invalid

row), using icons.

- The row-pointer field provides an "Add Row" button that allows the administrator to add a new row in the referenced table.
- When in the referenced table (after the View or Add New button has been clicked), the administrator can select the required row using the new "Use selected row" button.
- Multiple display of "View" capability.

Applicable Products: All.

2.4.1.21 Multiple SRSs and SRS Redundancy for SIPRec

This feature provides support for sending copies of call sessions traversing the device to multiple Session Recording Servers (SRS) for the SIPRec feature. Up until this version, only one SRS could be configured. Now, the administrator can configure up to three groups of SRSs, where each group can contain one standalone SRS, or two SRSs for 1+1 (active-standby) SRS redundancy.

Note:

- The feature is applicable only to the SBC application (only one SRS can be configured for the Gateway application).
- SRS redundancy is a license-dependent feature, defining the maximum number of SIPRec sessions that can be copied to the redundant (standby) SRS. (This is in addition to the regular SIPRec feature key.)

Applicable Products: MP-1288; Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.4.1.22 Product Key for Enhanced Product Identification

This feature provides support for aligning the device's serial numbers displayed on the chassis' product label and management interfaces (Web and One Voice Operations Center). Up until now, the product label displayed the chassis' serial number while the management interfaces displayed the CPU serial number. These serial numbers are now displayed on both the product label and management interfaces, as follows:

Serial Number Type	Product Label	Management Interface
Chassis	"S/N(Product Key)"	"Product Key"
CPU	"CPU S/N"	"Serial Number"

The Web interface displays the Serial Number and Product Key on the License Key page and Device Information page, in the new fields 'Serial Number' and 'Product Key', respectively.

For new product purchases as well as for each new License Key upgrade, the License Key includes the Product Key, which will be displayed automatically in the 'Product Key' field when the License Key is installed on the device. For existing customers who have upgraded their device's firmware but not License Key, the 'Product Key' field will appear empty.

Note that the Product Key is already supported by Mediant 9000 SBC and Mediant SE/VE SBC.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B Mediant 2600; Mediant 4000.

2.4.1.23 CLI Startup Script for Non-MSBR Products

This feature provides support for the CLI Startup script file by non-MSBR devices. Up until now, the file was supported only by AudioCodes MSBR product line. The file contains only CLI-based configuration and when loaded to the device, applies its settings and restores all other parameters not included in the file to factory defaults. The file causes the device to undergo two resets to apply the settings and thus, typically contains the Automatic Update settings and other settings that require a <device> reset.

Applicable Products: All.

2.4.1.24 Saving and Loading CLI-based Configuration Files in Web Interface

This feature provides support for saving and loading CLI Script and CLI Startup Script files through the device's Web interface. This is done in the existing Configuration File page (Setup menu > Administration tab > Maintenance folder > Configuration File).

Applicable Products: All.

2.4.1.25 Hitless License Upgrade from Pool Manager

This feature provides support for devices operating in High-Availability (HA) mode to receive a new SBC license from the License Pool Manager without affecting traffic (i.e., current calls are maintained). Up until now, each device, including the active device was reset, thereby disconnecting currently active calls. The new feature employs a "hitless" license upgrade mechanism, whereby the License Pool Manager first downloads the license to the redundant unit, resets it, and then triggers an HA switchover. It then downloads the same license to the previously active device, resets it and then triggers another HA switchover.

Applicable Products: All.

2.4.1.26 Debug for Remote Web (HTTP) Services

This feature provides support for enabling the device to generate debug messages for remote Web (HTTP) services and send them to a Syslog server. The feature is enabled by the new parameter, 'HTTP Proxy Debug Level' (ini – HTTPProxySyslogDebugLevel; CLI - configure network > http-proxy settings > http-proxy-debug-level). The debug level can be configured to 0 (No Debug), 1 (Basic) or 3 (Detailed).

Applicable Products: All.

2.4.2 Known Constraints

This section lists known constraints.

Table 2-5: Known Constraints in Version 7.20A.100

Incident	Description	Status
139442	When the device is operating in High-Availability (HA) mode and a hitless software upgrade from an earlier version to Version 7.2.100 is done through the Web interface, the Web interface sometimes erroneously displays an upgrade failure message and that a reset must be done, even though the devices were upgraded successfully. If this occurs, refresh the browser and then log in again to the Web interface. **Applicable Products:** Mediant 500 E-SBC HA; Mediant 800 Gateway & E-SBC HA.	Resolved in Version 7.20A.150 (See Section 2.7.3)
133294	Creating or deleting of virtual machine snapshots using the hypervisor tools sometimes causes the SBC HA system to reset. A workaround is to first shutdown the virtual machine (active or redundant SBC) and only then create or delete the snapshot. **Applicable Products:** Mediant VE SBC.	
139964	When the Firewall table (AccessList in file parameter) is configured with a firewall rule that blocks (denies) traffic from source port 53, start port 0 and end port 0, incoming Standard query responses from DNS port 53 is erroneously allowed by the firewall rule. **Applicable Products:** All.	
140547	Transcoding of G.711 to G.729 for loopback calls fail (disconnect) after an HA switchover. **Applicable Products:** HA Products.	Resolved in Version 7.20A.150 (See Section 2.7.3)

2.4.3 Resolved Constraints

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

Table 2-6: Resolved Constraints in Version 7.20A.100

Incident	Description
137821	When the LDAPDebugMode parameter is set to 3, the LDAP passwords erroneously appear in syslog, posing security risks. A workaround is to set the parameter to a lower value. **Applicable Products:** All.
139470	If the value of the Source IP field in the Firewall table contains an asterisk (*), the device crashes (resets). **Applicable Products:** All.
138984	Three-way conference calls cannot be made when the device's License Key includes "DSPCh = 288". A workaround is to set DSPCh to 72. **Applicable Products:** MP-1288.
138889	If ICE parameters are changed during a WebRTC session, the device rejects the incoming STUN binding requests and as a result, the call cannot be established. **Applicable Products:** WebRTC-supporting products.

Incident	Description
138751	DTMF transcoding fails when the SBC call uses the G.729 coder. **Applicable Products:** Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000.
138731	The device crashes (resets) when processing Call Setup rules. **Applicable Products:** SBC.
138703	Graceful lock cannot be cancelled during the lock timeout. **Applicable Products:** All.
138701	Processing some values in the ini file causes the device to crash (reset). **Applicable Products:** All.
138551	When configuring IP-to-Tel routing rules, the Source IP Group is erroneously used as a matching input for the table and not as the output, causing incorrect routing. **Applicable Products:** MP-1288.
138517	When the NTP server is configured as an FQDN, the HA redundant device crashes during the ini file upload and as a result, it returns to its former configuration. A workaround is to use an IP address for the NTP server. **Applicable Products:** HA-supporting products.
138495	When processing a Call Setup rule that requires an LDAP query, connectivity with the LDAP server fails, causing a device crash (reset). **Applicable Products:** SBC.
138386	Blind call transfers (SBC call) fail during an HA switchover (device rejects re-INVITE). **Applicable Products:** HA-supporting products.
138371	One leg sends Re-INVITE with a=sendonly and the device sends the re-INVITE with added T.38 media line to the second leg. As a result, the remote party rejects the re-INVITE and the call fails. **Applicable Products:** SBC.
137317 / 137318	The following parameters do not appear in the Web interface: SBCKeepContactUserinRegister and UdpPortSpacing. **Applicable Products:** All.
138277	The device does not support the maximum number of transcoding sessions as defined in the License Key and any calls above a certain number are dropped. **Applicable Products:** Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000.
138015	Some Gateway parameters are missing from the CLI. **Applicable Products:** MP-1288.
138014	Some Message Manipulation parameters do not appear in the CLI. **Applicable Products:** MP-1288.
137384	The Extension Coders Group in the IP Profile table cannot be accessed through the View button. **Applicable Products:** All.
136948	Daylight Saving Time settings are not saved after an HA switchover and therefore, the device is set with the incorrect time. **Applicable Products:** Mediant SW SBC HA.
135434	GRUB logging timeout during device reset is too long. **Applicable Products:** Mediant VE SBC.

Incident	Description
134449	RADIUS-based authentication of SIP users and RADIUS-based authentication of login username and password for management users are currently not supported. **Applicable Products:** Mediant 2600; Mediant 4000.
-	The SIPRec feature is not supported when the Media Transcoding Cluster feature is enabled. **Applicable Products:** Mediant 9000.
132977	To upgrade from Software Version 7.0 to 7.2, the device must first be upgraded to the latest 7.0 version (later than 7.00A.058.002) and only then to Version 7.2. **Applicable Products:** Mediant 2600; Mediant 4000; Mediant 9000; Mediant SE/VE.
133943	SRTP with ARIA encryption is not supported for SBC sessions. **Applicable Products:** All.
-	ARM is not supported. **Applicable Products:** All.
131889	When importing a Dial Plan file (*.csv file), it is recommended to configure the SyslogDebugLevel parameter to No Debug. **Applicable Products:** All.
116756	The device interworks with devices that support RTP bundling. However, it does not support receipt of bundled multimedia sessions on the same port and instead, it uses different ports for each media type (audio and video). By default, the device removes all bundle-related attributes ('a=group:BUNDLE' and 'a=ssrc') from the SDP offer and answer. **Applicable Products:** All.
87767	The Web interface's search feature may produce incorrect search results. **Applicable Products:** All.
138581	Mediant Virtual Edition SBC with Microsoft Hyper-V hypervisor with 4 GB is not supported. **Applicable Products:** Mediant VE.

2.5 Patch Version 7.20A.104.001

This patch version includes only resolved constraints.

2.5.1 Resolved Constraints

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

Table 2-7: Resolved Constraints in Version 7.20A.104.001

Incident	Description
-	AMR narrowband bug.
141854	When IP Phones register through OVR, they are unable to process all the XML in the SUBSCRIBE response (which includes the user number). As a result, they are not registered. **Applicable Products:** Mediant 800 with OVR.
141828	Incorrect routing – the device matches the suffix string (objectif-54) in the IP-to-IP Routing table for user +33467670000, even though the destination/source numbers do not contain the string objectif-54. **Applicable Products:** SBC.
141659	The device crashes (resets) upon receipt of a REGISTER when its License Key doesn’t include FEU. **Applicable Products:** SBC.
141640	When the power source of the device is unstable, some ports experience a problem and many error messages are generated. As a result, the ports become disabled and the Syslog is flooded with errors. A workaround is to make sure that the power source is stable. **Applicable Products:** MP-1288.
141535	When the parameter HAPingEnabled is enabled, the device crashes (resets). **Applicable Products:** HA SBC.
141527	When the device receives an RTP without payload, it crashes (resets). **Applicable Products:** All.
141499	When debug recording is enabled to record media, the device crashes (resets). **Applicable Products:** Mediant VE.
141446	The CPT file cannot be loaded through HTTP or HTTPS. A workaround is to use the Web to load the file. **Applicable Products:** MP-1288.
141435	When an UPDATE for AMR is received without octet-aligned attribute, the device rejects the UPDATE and the call fails. A Workaround is to use message manipulation to add it. **Applicable Products:** SBC.
141419	If a Startup Script CLI file or ini file is loaded through the Web interface, the configuration is not correctly reflected on the device. **Applicable Products:** All.
141397	When the user part of the To\From header is greater than 500 characters, the device crashes (resets). **Applicable Products:** SBC.

Incident	Description
141336	When the device authenticates users through the User Info file and the password of a user is changed, the device does not challenge the user, exposing a security risk. **Applicable Products:** All.
141335	When the device receives some non-standard packets from the IP, it does not respond. **Applicable Products:** All.
141326	When the device receives a REFER before the call is connected, it rejects it and the call transfer fails. **Applicable Products:** SBC.
141243	If the first entry in the Ethernet Devices table is tagged, the redundant device does not operate (no HA). A workaround is to set the first entry to tagged. **Applicable Products:** HA.
141187	Some scenarios during trans-rating cause exceptions and as a result, the device resets. **Applicable Products:** Mediant VE.
141132	A Major alarm permanently appears that indicates resetting the device after allocating licenses to the device from the AudioCodes One Voice Operations Center license pool. **Applicable Products:** All.
141044	The device does not allow more than 60,000 registered users (expected is 75,000). **Applicable Products:** Mediant VE/SE; Mediant 9000.
141039	The device crashes (resets) in the following scenario: 1) device sends INVITE and the first 180 response doesn't have a Contact 2) another 180 response with a different To tag is received and forking is recognized. **Applicable Products:** SBC.
141016	When using the CLI command **show ntp**, there is no NTP reference line in the result. **Applicable Products:** All.
140881	When user information is removed the User Info table, registration is not automatically removed in the SBC Registered Users database and the device keeps replying with 200 OK. **Applicable Products:** SBC.
140812	When the Syslog line for RAISE or CLEAR alarm ends with "Unique ID:1", "Unique ID:2" or "Unique ID:3", no UTC time is printed at the end of the Alarm syslog line. **Applicable Products:** All.
139730	When connection to the NTP server is lost, no alarm is raised **Applicable Products:** All.
140696	When an IP Profile is assigned in the Classification table, the device does not de-allocate resources when the call ends and as a result, new calls cannot be processed. **Applicable Products:** SBC.
140561	Modifying the parameters DenyAccessOnFailCount and DenyAuthenticationTimer does not take effect. **Applicable Products:** All.

2.6 Patch Version 7.20A.106.003

This patch version includes only resolved constraints.

2.6.1 Resolved Constraints

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

Table 2-8: Resolved Constraints in Version 7.20A.106.003

Incident	Description
144742	A bug in RTCP fraction lost calculation causes the device to crash (reset). **Applicable Products:** SBC.
143903	When in HA mode, even though the two License Keys are identical between active and redundant device, an alarm is raised indicating there's a License Key mismatch. **Applicable Products:** Mediant VE SBC.
142336	When using message manipulation to remove the prefix ('+') of non-existing Request-URI's user-part, the device crashes (resets). **Applicable Products:** SBC.
143127	The device is unable to load (when automatic update is employed) an ini file through HTTPS when the URL for the ini file is greater than 512 bytes. **Applicable Products:** All.
141935	HA keep-alive packets are not received correctly, causing the device to perform HA switchovers (and resets). **Applicable Products:** Mediant VE/SE; Mediant 9000.

2.7 Patch Version 7.20A.150.004

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

2.7.1 New Features

New features introduced in this version include the following:

2.7.1.1 Session Capacity Increases

This feature provides an increase in capacity for the following products:

- **Mediant 500 E-SBC:**
  - RTP-RTP / RTP-TDM sessions (with registrations): 250
    SRTP-RTP / SRTP-TDM sessions (with registrations): 200
  - Registered users: 1,500 (with registration refresh rate of 3,600 seconds and without SUBSCRIBES)
- **Mediant 800B E-SBC & Gateway:**
  - Signaling sessions:
    - Without registrations: 400
    - With registrations: 300
  - RTP-RTP / RTP-TDM sessions:
    - Without registrations: 400
    - With registrations: 300
  - SRTP-RTP / SRTP-TDM sessions:
    - Without registrations: 250
    - With registrations: 200
  - Registered users: 1,500 (with registration refresh rate of 3,600 seconds and without SUBSCRIBES)
- **Mediant 9000 SBC** (with at least one 10 GbE NIC)**:** RTP sessions increased to 50,000
- **Mediant VE SBC (OpenStack KVM and SR-IOV Intel NICs):**
  - Signaling sessions: 24,000
  - RTP-RTP sessions: 24,000
- **Mediant VE SBC with Media Transcoders (OpenStack):**
  - Signaling sessions: 24,000
  - RTP-RTP sessions: 24,000
  - SRTP-RTP sessions: 12,000

For detailed session capacity, see Section 4.1.

Applicable Applications: SBC.

Applicable Products: Mediant 500; Mediant 800; Mediant 9000; Mediant VE/SE.

2.7.1.2 Analog Voice Interface Support on Mediant 500L E-SBC/Gateway

The Mediant 500L E-SBC and Media Gateway now supports analog voice interfaces (FXS and FXO). This support is currently offered with up to four FXS ports and four FXO ports. FXS Analog Lifeline is also supported, whereby during a power outage, calls can be received / made from / to the PSTN (FXO) by the FXS lifeline telephone.

Applicable Applications: Gateway.

Applicable Products: Mediant 500L E-SBC & Gateway.

2.7.1.3 Bulk TLS Root Certificate Import

This feature provides support for importing multiple TLS root certificates into the device's Trusted Root Certificate store from a single file. The file must have the *.PEM extension and each X.509 certificate in the file must be Base64 encoded (PEM). When copying-and-pasting the certificates into the file, each certificate must be enclosed by the first line "-----BEGIN CERTIFICATE-----" and the last line "-----END CERTIFICATE-----".

The file is imported using the existing mechanism – Import button in the Trusted Certificates page (TLS Contexts page > Trusted Root Certificates link).

Applicable Products: All

2.7.1.4 Base64 (PEM) Encoded String Included in Certificate Display

This feature provides support for including the Base64-encoded format of the certificate, associated with a TLS Context, in the certificate information display in the Web interface (by clicking the Certificate Information link in the TLS Contexts page). Up until now, the certificate information option displayed general information, for example, Issuer, Subject, and Validity. The feature may be useful, for example, by allowing the administrator to select the encoded string and then copy-and-paste it in a text-based file for backup.

Applicable Applications: All.

Applicable Products: All.

2.7.1.5 Generation of Encrypted Private Key File

This feature provides support for configuring a password (passphrase) for a private key file generated by the device for a specified TLS Context. The passphrase provides secondary security, for example, if the encrypted private key is stolen the key cannot be viewed without the passphrase. The feature is supported by a new parameter, 'Private key pass-phrase' on the Change Certificates page (TLS Contexts table > Change Certificate link). If left blank, the private key will not encrypted.

Applicable Applications: All.

Applicable Products: All.

2.7.1.6 Token-based Authentication for Accessing Web Interface

This feature provides support for the integration of the device’s Web interface with third-party products. The authentication token can be retrieved using the REST API and appended to the device’s URL (<IP address>/api/v1/actions/authToken), thus enabling direct access to the device’s Web interface without the need to enter a username and password.

Applicable Applications: All.

Applicable Products: All.

2.7.1.7 TLS Certificate Management through REST

This feature provides support for managing (GET, PUT and POST actions) the device's TLS Certificates (TLS Contexts) from a REST client through AudioCodes REST API. The feature is supported by the following new REST URL path:

```
/api/v1/files/tls
```

The feature can be used, for example, to retrieve information of a certificate, upload or download a certificate, and generate a CSR. For more information, refer to the document *REST API for Mediant Devices*.

Applicable Applications: All.

Applicable Products: All.

2.7.1.8 Routing Based on QoS by Routing Server

This feature provides support for the routing server (for example, AudioCodes ARM) to route calls based on QoS metrics (media and signaling) collected by the SBC/Gateway device. The device collects QoS metrics (e.g., packet loss, MOS, audio bandwidth) per IP Group that is configured to operate with the routing server (Used by Routing Server parameter set to "Used"). Each QoS report can contain the status of up to 100 IP Groups. If more than 100 IP Groups exist, multiple QoS reports are sent.

To enable the device to send QoS reports for these IP Groups:

- The new global parameter, Quality Status (RoutingServerQualityStatus) must be set to "Enable".
- The new global parameter, Quality Status Rate (RoutingServerQualityStatusRate) can optionally be configured, which defines the rate (sec) at which QoS reports are sent (15-3600, default 60).
- The exiting parameter, Type (HTTPRemoteServices_HTTPType) in the Remote Web Services table must be set to the new optional value "QoS", for the Web service configured for the routing server.
- Voice quality monitoring and RTCP-XR must be enabled (using the exiting parameter Enable RTCP XR (VQMonEnable).

The Quality Status and Quality Status Rate parameters can be read and modified in REST using the new REST API parameters, RoutingServerQualityStatus and RoutingServerQualityStatusRate, under the URL resource /api/v1/rmConfig/globals.

The feature is supported by the following new REST API URL resource:

```
POST <Route_Server_Path>/qualityStatus
```

Note:

- For media metrics calculations, the device's License key must include voice quality monitoring and RTCP-XR.
- If there is no service configured with the type “QoS”, reports are sent to the Topology server.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.9 Tag-Based Routing Enhancement

This feature provides support for tag-based routing, whereby the destination in the IP-to-IP Routing table is based on a Dial Plan tag. A summary (skips steps for ease of clarity) of the call processing for the feature is as follows: Once the incoming SIP dialog is classified to an IP Group, the device searches the Dial Plan that is associated with the IP Group, for a Dial Plan rule that matches the destination (called) prefix number. The device then searches the IP-to-IP Routing table for a matching routing rule. If the destination of the matched rule is based on a tag (see parameters below), it performs some logic to use one of the tags in the matched Dial Plan rule and then searches the IP Groups table and IP Group Set table for an IP Group or IP Group Set that is configured with this "destination" tag and if found, routes the dialog to that IP Group.

The feature is supported by the following new optional values and parameters:

- IP Groups table: New parameter – 'Tags' (IPGroup_Tags)
- IP Group Set table: New parameter – 'Tags' (IPGroupSet_Tags)
- IP-to-IP Routing table:
  - 'Destination Type' parameter has a new optional value - "Destination Tags" (12)
  - New parameter – 'Routing Tag Name' (IP2IPRouting_RoutingTagName)

Applicable Applications: SBC.

Applicable Products: All.

2.7.1.10 Fax Rerouting for SBC Calls

This feature provides support for rerouting incoming SBC calls that are identified as fax calls to a new IP destination. The device identifies a fax call if it detects a calling (CNG) tone on the incoming call (originator side). Detection is done within a user-defined interval, configured by the existing parameter, SBCFaxDetectionTimeout.

Once the device detects a fax call, it terminates the initial call and reroutes it using a new INVITE to the new fax destination (new IP Group). If the initial INVITE used to establish the voice call was already sent, the device sends a SIP CANCEL (if not connected yet) or a BYE (if already connected) to release the call (with the internal disconnect reason RELEASE_BECAUSE_FAX_REROUTING, translated to Q.850 reason GWAPP_NORMAL_UNSPECIFIED 31).

The feature is configured using two IP-to-IP Routing rules in the IP-to-IP Routing table, where the second rule is configured to the new optional value "Fax Rerouting" (6) for the 'Call Trigger' parameter (IP2IPRouting_Trigger). In addition, the IP Profile of the terminating fax side is configured with the new parameter 'Fax Rerouting Mode' (IpProfile_SBCFaxReroutingMode) to "Rerouting without delay".

Applicable Products: SBC.

2.7.1.11 Routing Back to Sender

This feature provides support for configuring the device to reply to the sender (source) of an incoming SIP dialog, instead of routing the call to another SIP entity. The device can reply with a SIP response code (e.g., 200 OK) or a 3xx redirection response (with an optional Contact field indicating to where the sender must re-send the message). For example, if the incoming call matches the routing rule, the rule can be configured to send a SIP 200 OK response to the sender of the incoming call. The feature can be used for normal and alternative routing. The feature is supported by the following new option and parameter in the IP-to-IP Routing table:

- New optional value "Internal" for 'Destination Type' (IP2IPRouting_DestType): Enables the feature.
- New parameter 'Internal Action' (IP2IPRouting_InternalAction): Defines the response code or redirect response, using the following syntax:
  - Response codes:
    ```
    Reply(response='<code>')
    ```
  - Redirect:
    ```
    Redirect (response='<code>', contact='sip:'+….)
    Redirect (contact='…', response = '<code>')
    Redirect (contact = 'sip:user@host')
    ```
    The response code for redirect messages can only be 3xx.

  The string value "Reply" on its own depicts a 200 OK; the value "Redirect" depicts a 302 Redirect.

  Examples:
  - The device responds to incoming dialog with SIP 200:

```
Reply(response=’200’)
```

- The device responds to incoming dialog with SIP 300:
  ```
  Redirect (response=’300’, contact=’sip:102@host’)
  ```
- The device redirect calls from the sender to a SIP Recording server (SRS), by sending the sender the following redirect message:
  ```
  Redirect(response='302',contact='sip:'+header.to.url.user+'
  @siprecording.com')
  ```

Applicable Applications: SBC.

Applicable Products: All.

2.7.1.12 String Concatenation in Message Conditions

This feature provides support for using the plus "+" operator as part of the value in message conditions ('Condition' field) for concatenating strings. Conditions are used in the Message Manipulations table, Message Conditions table, and Call Setup Rules table. Below shows two examples of a Condition using the "+" operator (bolded):

```
header.from contains 'sip:' + header.REQUEST-URI.url.user AND
header.to contains var.global.0 + var.global.1
ldap.attr.msRTCSIP-Line contains
'tel:'+param.call.dst.user+':ext='
```

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.13 Pre-Parsing SIP Message Manipulation

This feature provides support for manipulating incoming SIP messages before they are parsed (as an object) by the device. In other words, messages can now be manipulated in their original format (plain text) as received from the network. This may be useful, for example, to overcome parser strictness or to “allow” possible parsing errors.

Pre-parsing message manipulation rules are configured using the new parent-child tables, Pre-Parsing Manipulation Sets table (PreParsingManipulationSets) and Pre-Parsing Manipulation Rules table (PreParsingManipulationRules), respectively. The rule set is associated with specific calls by assigning it to the relevant SIP Interface, using a new parameter in the SIP Interfaces table called Pre-Parsing Manipulation Set (SIPInterface_PreParsingManSetName).

Pre-parsing message manipulation rules are defined by SIP message element to manipulate (for example, INVITEs), pattern based on regular expression (REGEX) to search for (match) in incoming messages, and the regex pattern that will replace the matched pattern.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.14 Message Manipulation and Carriage Returns

This feature provides support for indicating carriage returns (new lines) in literal strings for all SIP message elements (request URI, headers and body), in Message Manipulation rules, Message Condition rules, and Call Setup rules. Up until now, this was supported only for the addition of SIP message bodies, for example, SDP ('Action Type' field set to **Add**).

The double-backslash (\\) is used to indicate a carriage return within a string (enclosed by a single apostrophe), for example:

```
body.sdp contains 'a=bbb\\a=ccc'
```

The above example shows a Condition value where the condition is an SDP that includes the following two lines of strings:

```
a=bbb
```

```
a=ccc
```

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.15 IP Group Parameter Representation in Message Manipulation

This feature provides support for using the following additional IP Group table parameters in SIP message manipulation rules:

- 'Tags' parameter:
  - param.ipg.src.tags
  - param.ipg.dst.tags
  - param.ipg.src.tags.<tag name>
  - param.ipg.dst.tags.<tag name>
- 'Name' parameter:
  - param.ipg.src.name
  - param.ipg.dst.name

Applicable Products: All.

2.7.1.16 Message Manipulation for SDP Origin Username

This feature provides support for using the username in the Origin field ("o=") of the SDP body in SIP messages, for message manipulation. The new syntax is:

```
param.message.sdp.originusername
```

Applicable Products: All.

2.7.1.17 Enhanced ISUP Body Message Manipulation

This feature provides the following enhanced manipulation support for SIP-ISUP interworking:

- SIP 200 OK with the CON (Connect) ISUP message type. This is applicable to the Spirou variant.
- Additional SIP INVITE with the IAM (Initial Address Message) ISUP message type:
  - Access transport (See 4.5.19 of Recommendation Q.931)
  - User service information (see 3.57 of Q.763)

Applicable Applications: All.

Applicable Products: All.

2.7.1.18 IP Group Parameter Representation in Call Setup Rules

This feature provides support for using the below additional IP Group table parameters in Call Setup Rules (CSR). These parameters can be used to specify values in the ‘Search Key’, ‘Conditions’ and ‘Action Value’ fields of Call Setup Rules to represent the IP Group of the incoming call.

- param.ipg.src.user
- param.ipg.src.host
- param.ipg.src.type
- param.ipg.src.id
- param.ipg.src.tags
- param.ipg.src.name
- param.ipg.src.user-defined.0

- param.ipg.src.user-defined.1

Note that this feature is already supported for manipulation rules.

Applicable Applications: SBC.

Applicable Products: All.

2.7.1.19 Maximum Characters for "o" Field in SDP Body

This feature provides support for configuring the maximum number of characters allowed in the SDP body's "o=" (originator and session identifier) field for the session ID and session version values. The feature is supported by the new ini file parameter, MaxSDPSessionVersionId - valid range 1,000 to 214,748,3647 (default). An example of an "o=" line with session ID and session version values is shown below:

```
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
```

Applicable Applications: All.

Applicable Products: All.

2.7.1.20 Detection of Pulse Dialing

This feature provides support for detecting pulse (rotary) dialing from analog equipment (e.g., telephones) that are connected to the device's FXS ports. The new parameter, EnablePulseDialDetection enables the feature.

Note that the feature is already supported in earlier releases by MP-1xx.

Applicable Applications: Gateway.

Applicable Products: MP-1288.

2.7.1.21 Prefix String for External Line Enhancement

This feature provides enhanced support for the prefix string used to access an external line (configured by the existing Prefix2ExtLine parameter). An additional option has been added (2) to the existing AddPrefix2ExtLine parameter that enables the device to not only include this prefix string in the called number sent to the IP destination, but also to use the prefix string in Digit Maps and Dial Plans. This is useful in that it allows the configuration of separate digit map and/or dial plan patterns for internal and external dialing (where the first digit of the pattern is the prefix string). For more information, refer to the *User's Manual*.

Applicable Applications: Gateway (FXS).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000; MP-1288.

2.7.1.22 MWI Notification Timeout on Endpoint Equipment

This feature provides support for configuring the maximum duration (timeout) that a message waiting indication (MWI) is displayed on endpoint equipment (i.e., phones' LED, screen notification or voice tone). If the timeout has not yet expired for an MWI and the endpoint receives a new MWI, the timeout restarts its countdown. The feature is supported by the following new parameters:

- Global parameter - ‘MWI Notification Timeout’ (MWINotificationTimeout)
- Tel Profile - - ‘MWI Notification Timeout’ (TelProfile_MWINotificationTimeout)

The value range is 1 to 2,000,000 seconds. The default is 0 (i.e., unlimited).

Applicable Applications: Gateway (FXS).

Applicable Products: MP-1288; Mediant 5xx; Mediant 8xx; Mediant 1000B.

2.7.1.23 Ringback and Held Tones per User

This feature provides support for playing different user-defined ringback and held tones per user (i.e., IP Group). This is achieved by loading the device with a Prerecorded Tone file (PRT) with the different tones, and then configuring an IP Profile (associated with the IP Group) with the index of the required ringback and/or held tone as defined in the PRT file.

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

- Local RingBack Tone Index (IPProfile_LocalRingbackTone): Defines the ringback tone that you want to play from the PRT file. The tone is configured by the index number (0-79) where it is defined in the PRT file. By default, the device plays a default ringback tone.
- Local Held Tone Index (IPProfile_LocalHeldTone): Defines the held tone that you want to play from the PRT file. The tone is configured by the index number (0-79) where it is defined in the PRT file. By default, the device plays a default held tone.

Up to 80 user-defined tones can be created in the PRT file. The prerecorded tones can be created using a standard third-party, recording utility (such as Adobe Audition), and then combined into a single and loadable file (PRT file), using the latest version of AudioCodes DConvert utility.

Applicable Applications: SBC and Gateway.

Applicable Products: All.

2.7.1.24 Retry Time Enhancement for Registration Failures

This feature provides enhanced support regarding registration failure and a dynamic interval (time to wait) between the device's subsequent registration attempts. The feature is applicable only to registrations initiated by the device on behalf of SIP entities (for example, User Info, Accounts, Endpoints or the device itself) with a SIP proxy server (registrar).

Up until now, the interval between registration attempts due to a registration failure could only be configured (by the RegistrationRetryTime parameter) as a fixed interval (e.g., every 30 seconds). The new feature now enables the device to perform registration attempts at intervals that increase for each failed subsequent registration attempt (per RFC 5626, Section 4.5) for the specific registration flow.

The feature is supported by the new parameter, 'Max Registration Backoff Time' (MaxRegistrationBackoffTime), which operates together with the existing RegistrationRetryTime parameter. When the MaxRegistrationBackoffTime parameter is configured, the wait-time before another registration attempt increases after each failed registration, until it reaches the maximum value specified by the parameter. The device uses the following algorithm to calculate an incremental augmented wait-time between each registration attempt:

```
Wait Time = min (max-time, (base-time * (2 ^ consecutive-
failures)))
```

Where:

- *max-time* is the value configured by MaxRegistrationBackoffTime
- *base-time* is the value configured by RegistrationRetryTime

For example, if *max-time* is 1800 seconds and *base-time* is 30 seconds, and there were three registration failures, then the upper-bound wait time is the minimum of (1800, 30*(2^3)), which is (1800, 240) and thus, the minimum of the two values is 240 (seconds). The actual time the device waits before retrying registration is computed by a uniform random time between 50% and 100% of the upper-bound wait time (e.g., for 240, the actual wait-time is between 120 and 240 seconds). As can be seen from the algorithm, the upper-bound wait time never exceeds the value of the MaxRegistrationBackoffTime parameter.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.25 Random IDs in Contact Header User Part for New Registrations

This feature provides support for enabling the device to assign a random ID string value to the user part of the SIP Contact header for new user account registrations with the device. The assigned ID is unique to each user account. An example of a random ID is shown (in bold) below:

```
Contact: <sip:HRaNEmZnfX6xZl4@pc33.atlanta.com>
```

The feature is supported by the new ini file parameter, UseRandomUser, where 0 is disable (default) and 1 is enable. When enabled, all INVITE messages for these new user accounts are sent with their unique ID. The IDs are also used for registration refreshes and for un-registering these accounts. The IDs apply until the parameter is disabled. When enabled again, new random ID strings are assigned.

Applicable Applications: All.

Applicable Products: All.

2.7.1.26 Unregistration of User Accounts upon Device Reset

This feature provides support for deregistering all user accounts that were registered with the device, upon a device reset. However, during device start-up, each account sends a REGISTER message (containing "Contact: *") to unregister all contact URIs belonging to its Address-of-Record (AOR), and then a second after they are unregistered, the device re-registers the account. The feature is supported by the new ini parameter, UnregisterOnStartup, where 0 is disable (default) and 1 is enable.

Applicable Applications: All.

Applicable Products: All.

2.7.1.27 Register "Stickiness" to Registrar Server

This feature provides support for configuring the device to always route SIP requests of a registered Account to the same registrar server to where the last successful REGISTER request was routed. In other words, once initial registration of the Account to one of the IP addresses in the Proxy Set is successful (i.e., 200 OK), binding ("stickiness") occurs to this specific address (registrar). All future SIP requests (INVITEs, SUBSCRIBEs and REGISTER refreshes) whose source and destination match the Account are sent to this registrar only. This applies until the registrar is unreachable or the register refresh fails, for whatever reason.

Up until now (and when the feature is disabled), after a successful initial registration, whenever the device received a SIP request or registration refresh no binding happened to any specific IP address in the Proxy Set and the device simply sent the request to the currently working registrar. In the case of proxy load-balancing, there was no certainty to which IP address in the Proxy Set the request would be routed.

The feature applies to Accounts and is enabled in the Accounts table using the new parameter, 'Registrar Stickiness' (Account_RegistrarStickiness). For the feature to function, the existing 'Register' parameter must also be enabled (Regular or GIN) in the Accounts table.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.28 Registrar Search Method for Registrar "Stickiness"

This feature provides support for configuring the method for choosing an IP address (registrar) in the Proxy Set to which the Account initially registers and refreshes registration, when the Register Stickiness feature is enabled. Once chosen, this is the IP address to which the Account is then bound for subsequent SIP requests.

- Current Working Server: For each initial and refresh registration request, the device routes to the currently working server in the list of IP addresses (configured or DNS-resolved IP addresses) of the Proxy Set. In the case of proxy load-balancing, the chosen IP address is according to the load-balancing mechanism.

- According to IMS Specifications: For the initial registration request, the device performs DNS resolution if the address of the Proxy Set is configured with an FQDN. It then attempts to register sequentially to the list of DNS-resolved addresses (or configured IP addresses). If an address results in an unsuccessful registration, the device immediately tries the next address (without waiting any retry timeout). The device goes through the list of addresses until an address results in a successful registration. If the registration process is unsuccessful for all the addresses, the device waits a configured retry time and then goes through the list again. Once initial registration is successful, periodic registration refreshes are performed as usual. In addition to the periodic refreshes, immediate register refreshes are done upon the following triggers according to the IMS specification:
  - The device receives a SIP 408, 480, or 403 response from the serving IP Group in response to an INVITE.
  - The transaction timeout for an INVITE sent to the serving IP Group expires.
  - The device receives an INVITE from the serving IP Group from an IP address other than the address to which it is currently registered. In this case, it also rejects the INVITE with a SIP 480 response.

The feature applies to Accounts and is enabled in the Accounts table using the new parameter, 'Registrar Search Mode' (Account_RegistrarSearchMode).

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.29 Registration Event Package Subscription for Registrar "Stickiness"

This feature provides support for the device to subscribe to the registration event package service (RFC 3680) with a registrar server to which an Account has been successfully registered, when the Registrar Stickiness feature is enabled. This subscription allows the device to receive the registration state of the Account registered with the server.

When enabled, the device subscribes to this service by sending a SUBSCRIBE message containing the Event header set to "reg" (Event: reg). Whenever a change occurs in the registration binding state, the server notifies the device by sending a SIP NOTIFY message.

The feature is enabled by the new parameter, 'Reg Event Package Subscription' (Account_RegEventPackageSubscription).

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.30 High-Availability Disconnect

This feature provides support for disconnecting two devices operating as a 1+1 High-Availability (HA) system, returning them to stand-alone devices. The feature is enabled from the active device, using the following CLI command:

```
# debug HA disconnect-system < new OAMP address of redundant
device>
```

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

Applicable Applications: SBC/Gateway.

Applicable Products: HA Systems.

2.7.1.31 Enhanced HA Keep-Alive

This feature provides support for an enhanced HA keep-alive mechanism, which improves the keep-alive mechanism.

Note: UDP ports 670 and 680 have been added for HA operation on the Maintenance interface. Make sure that these two ports are opened (allowed) between the Active and Redundant Maintenance interfaces.

Applicable Applications: SBC/Gateway.

Applicable Products: HA Systems.

2.7.1.32 OVR Support in High-Availability Mode

This feature provides support for One-Voice Resiliency (OVR) application when the device operates in High-Availability (HA) mode. OVR is supported in HA mode in both Normal and Survivability (Limited Service) modes.

Note that besides the usual OVR and HA configuration, the only special configuration for OVR support in HA is to configure the IpProfile_SBCSessionExpiresMode parameter to "Observe" for the IP phone's IP Profile. This is needed to avoid the scenario of calls being "stuck" (never released by receiving BYE from phone or Microsoft server) for phones that were in a call before the HA switchover and that fail to register after the switchover.

Following HA switchover, all the IP Phones in the OVR network register again and normal operation resumes within 90 seconds.

Applicable Products: Mediant 800B with OVR.

2.7.1.33 SIPRec Session Capacity Increase

This feature provides for an increase in the maximum number of supported concurrent SIPRec sessions to 20,000 for Mediant 9000 and 12,000 for Mediant VE/SE.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.7.1.34 Skype User Presence Notification for Non-Skype Endpoint Devices

This feature provides support for the device to notify the Microsoft Skype for Business Server of the presence status ("on-the-phone") of Skype for Business users when making and receiving calls using third-party (non-Skype for Business) endpoint devices (such as mobile phones and PBX phones). Up until now, presence status was handled solely by the Skype for Business Server to reflect calls between Skype for Business endpoints only (e.g., Skype for Business desktop clients).

The device uses SIP PUBLISH messages to update the Skype for Business Server of presence status changes. The Skype for Business Server then publishes the presence status to all the Skype for Business users, which is displayed on their native Skype for Business endpoints.

To support the feature, the following new configuration items have been added:

- Global parameters:
  - Presence Publish IP Group ID (PresencePublishIPGroupId) – indicates the IP Group (by ID) of the Skype for Business Server (presence server)
  - Enable MsPresence message (EnableMSPresence) - enables the feature
- Call Setup Rules table - new parameters added for 'Action Subject' field (read/write):
  - presence.src – retrieves source (caller) user's Skype for Business URI through LDAP query (used for the Request URI, and From/To headers in the PUBLISH message)

- presence.dst – retrieves destination (called) user's Skype for Business URI through LDAP query (used for the Request URI, and From/To headers of the PUBLISH message)

Note:

- The support is also applicable to Lync Server 2013 (Version 5.0.8308.866 and later).
- The feature requires that the “Presence gateway service” be enabled on the Skype for Business Server.
- This feature is provided by default on all products, except Mediant 500 E-SBC and Mediant 500L Gateway & E-SBC for which it is a licensed feature (needs to be purchased).

Applicable Applications: SBC/Gateway (Tel-to-IP Calls).

Applicable Products: All.

2.7.1.35 SIP-based Private Wire Interworking

This feature provides support for interworking signaling for Private Wire services, where one side is a legacy digital PSTN equipment using E1/T1 CAS, and the other side an IP-based Private Wire session manager using SIP. The feature enables private wire services to migrate to IP-based private wires without replacing existing, legacy TDM networks.

Private Wire is a generic term used to describe static point-to-point voice connections between two locations. Private Wires are used by a number of communities such as military, railways, and financial services (e.g., turret trading systems). The telephone lines between users are "always" connected and no dialing is necessary. The private-wire signaling standard allows users to signal certain events to one another using the SIP INFO message (with an XML schema in the body). These events include Hook Switch (On/Off) states and Ringdown states (No Ring/Ring).

The feature is supported by the new optional value, "Private Wire" for the existing global parameter 'Enable TDM Tunneling' (EnableTDMoverIP). TDM tunneling can now also be enabled per trunk, using the new ini file parameter, EnableTDMOverIPforTrunk.

Applicable Applications: Gateway (E1/T1 CAS and IP-to-Tel calls).

Applicable Products: Mediant 500 E-SBC; Mediant 500 MSBR; Mediant 8xx; Mediant 1000B.

2.7.1.36 Configurable Maximum Transmission Unit

This feature provides support for configuring the Maximum Transmission Unit (MTU) in bytes per VLAN (Ethernet Device). The feature is supported by the new parameter in the Ethernet Devices table, 'MTU' (DeviceTable_MTU), where the value can be 68 to 65,535 for Mediant 9000 and Mediant VE/SE, and 68 to 1,500 for all other products. The default is 1,500.

Applicable Applications: All.

Applicable Products: All.

2.7.1.37 Same VLAN ID for Multiple Ethernet Devices

This feature provides support for using the same VLAN ID for more than one Ethernet Device. Up until now, each Ethernet Device had to be configured with a unique VLAN ID (in the Ethernet Devices table).

Applicable Applications: SBC.

Applicable Products: Mediant 9000 SBC; Mediant VE/SE SBC.

2.7.1.38 SFP+ 10G Support for Network Interface

This feature provides support for optional, small form-factor pluggable (SFP+) 10Gb network cards with LX or SX transceivers. Up to two network cards can be installed in the device instead of the existing copper GbE NICs. Each SFP card provides four SFP port pairs. Up until now, the device's support for fiber included only SFP (1Gb) network cards.

Applicable Applications: SBC.

Applicable Products: Mediant 9000 SBC.

2.7.1.39 Disable Periodic DNS Queries

This feature provides support for disabling periodic DNS queries with a DNS server performed by the device for resolving FQDNs into IP addresses. DNS queries are used, for example, for Proxy Sets that are defined with FQDNs. When disabled, DNS resolution is done only once (upon device reset, power up, or new and modified configuration) and the DNS-resolved IP addresses are then used all the time (i.e., not refreshed).

The feature is configured by the existing parameter, 'Proxy IP List Refresh Time' (ProxyIPListRefreshTime), which now can be set to 0 to disable it. Up until now, the parameter could not be disabled (periodic DNS queries was always enabled).

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.40 SBC Application Enabled by Default

This feature changes the default setting of the SBC application (EnableSBCApplication) to enabled for all devices. Up until now, the application was enabled by default for all products except the ones listed under Applicable Products (below).

Note:

- The SBC application is enabled by default only if the License Key contains at least one of the SBC-related capacity features (e.g., "SBC-Signaling"). If the License Key does not contain any SBC-related capacity values, the application is disabled.
- When upgrading the device to 7.2.150, the SBC application is enabled (even if it was disabled on the device when running the previous version).

Applicable Applications: SBC.

Applicable Products: MP-1288; Mediant 5xx; Mediant 8xx; Mediant 1000B.

2.7.1.41 Web GUI Enhancements

This feature provides support for the following main Web GUI enhancements:

- License Key page: New design, providing improved readability of features as well as icon indications of feature and capacity changes between previous License Key and newly loaded License Key.
- SBC Configuration Wizard: Accessed now from Actions drop-down list on toolbar and/or Navigation tree (Setup menu > Administration tab > Maintenance folder > Configuration Wizard). Miscellaneous changes in wizard.

Applicable Products: All

2.7.1.42 Console Access Mode

This feature provides support for configuring the access mode (VGA or RS-232) to the device's console for accessing the CLI. Up until now, the mode could be configured only through the GRUB boot-loader menu (but after a software upgrade, the mode reverted back to VGA). This feature allows you to configure the mode through CLI (configure troubleshoot > startup-n-recovery > system-console-mode) and ini file (SystemConsoleMode). The default mode is VGA. The mode is unaffected by a device reset.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant SE/VE.

2.7.1.43 Single Sign-On to Web Interface from OVOC and Mediant CCE

This feature provides support for single sign-on access to the device's Web interface from the Web-based management interfaces - AudioCodes One Voice Operations Center (OVOC) and Mediant Cloud Connector Edition Appliance. The device's Web interface layout has also been re-designed for the requirements of OVOC and Mediant CCE Appliance.

Applicable Applications: All.

Applicable Products: All.

2.7.1.44 Broadcast Indication of Firmware Upgrade

This feature provides support for displaying a message in all active CLI sessions pertaining to a specific device, notifying all the users that the device is currently uploading firmware (.cmp). Up until now, the message was displayed only in the CLI session of the user that initiated (**copy firmware** command) the firmware upload. The purpose of the message is to prevent users that are connected to the same device from resetting or powering off the device during firmware upgrade, thereby disrupting the upgrade process.

The message not only displays the upload progress, but also displays the username of the management user who initiated the upgrade and the IP address of the user's PC (or "local" if the user is connected through serial interface). Regardless of which actions the users are performing in their CLI session prior to the upgrade, the message is forcibly displayed on their CLI consoles.

Below shows an example of such a message:

```
# copy firmware from http://10.3.1.52:1400/tftp/SIP_F7.20A.335.cmp
 % Total    % Received % Xferd  Average Speed   Time    Time
Time  Current Dload  Upload   Total   Spent    Left  Speed
100 40.7M  100 40.7M    0     0  1288k      0  0:00:32  0:00:32 --
:--:-- 1979k
Firmware file http://10.3.90.52:1400/tftp/SIP_F7.20A.335.cmp was
loaded.  (user: Admin, IP local)
The system will reboot when done
DO NOT unplug/reset the device
Firmware process done. Restarting now...
Restarting......
```

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.45 Free Product Evaluation Enhancements

This feature provides support for the following enhancements concerning the free product evaluation offering:

- Up to three user registrations (far-end users) are now supported (in addition to the already supported three SBC sessions) in the default License Key. Up until this release, user registration was not allowed.
- Transcoding capabilities with the three SBC sessions are now allowed, but this requires the administrator to install a special evaluation License Key.

For more information, refer to the *Mediant Virtual Edition SBC Installation Manual*.

Applicable Applications: SBC.

Applicable Products: Mediant VE SBC.

2.7.1.46 Hitless License Key Installation for HA

This feature provides support for hitless License Key installation through the Web interface for devices in HA mode. The installation method is non-traffic affecting, employing the HA switchover mechanism to ensure that current calls are maintained. The support is provided by a new design of the License Key page, which provides hitless and non-hitless installation options. Note that a License Key sent from the License Pool Manager Server is automatically installed using the hitless method.

A new alarm has been introduced, acLicenseKeyHitlessUpgradeAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.129), which is sent when the hitless License Key update fails.

Applicable Applications: All (HA).

Applicable Products: Mediant 500 E-SBC; Mediant 800 E-SBC; Mediant 2600 E-SBC; Mediant 4000 SBC; Mediant 9000 SBC; Mediant VE/SE SBC.

2.7.1.47 SNMP Proprietary Trap Variable Bindings

This feature provides support for new variable bindings (varbinds) for proprietary SNMP traps (acTrap). Each trap is now sent with 16 varbinds (instead of 13 in previous releases). The new varbinds include:

- acBoardTrapGlobalsDeviceName (13)
- acBoardTrapGlobalsDeviceInfo (14)
- acBoardTrapGlobalsDeviceDescription (15)

Note that the device sends these varbinds with empty values; OVOC provides the proper values when sending the traps northbound.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.7.1.48 Debug for Remote Web Services

This feature provides support for debugging remote Web (HTTP) services, specifically the HTTP client. The debug level can be configured from 1 to 3 (detailed). The debug messages are sent to the Syslog server. The feature is supported by the new parameter Debug Level (RestDebugMode), where 0 disables (default) and 1 through 3 is the debug level.

Applicable Applications: All.

Applicable Products: All.

2.7.1.49 FXS Line Testing

This feature provides support for FXS line testing, where the output displays various line statuses and electrical measurements per FXS port and country coefficient USA (70) or TBR21 (66). Some of the FXS line measurements supported by this feature include:

- Hazardous Potential Tests (HPT) - hazardous AC or DC voltage is present on the tip and ring or both.
- Foreign Electromotive Force Tests (FEMT) - foreign voltage is present on the tip, ring or both
- Resistive Fault Tests (RFT) - tip or ring is shorted to ground, or they are shorted to each other
- Receiver Off-hook Tests (ROH) - one or more phones are off hook on phone line during test.
- Ringer Impedance Tests (RIT)
- AC/DC line voltage

- AC/DC line current
- Line resistance
- Line capacity

The feature is supported by the following new command:

```
# configure voip
(config-voip)# interface fxs-fxo
(fxs-fxo)# fxs-line-testing {module/port} {66|70}
```

Note:

- For Mediant 1000B, the feature is supported only on the FXS module type (GTPM01046) that supports outdoor FXS cabling.
- For Mediant 800, please contact your AudioCodes sales representative regarding the hardware versions that support this feature.

Applicable Applications: Gateway (FXS).

Applicable Products: Mediant 800; Mediant 1000B; MP-1288.

2.7.1.50 Persistent Logging of Syslog Messages on Device

This feature provides support for automatic logging of system event messages to the device's storage, where they persist even if the device undergoes a reset or powers off. Persistent logging is done by default (cannot be disabled). The feature eliminates the need for sending logged messages to third-party, logging servers (such as a Syslog server) and offers an efficient tool for troubleshooting the device. When the persistent logging storage is full, older messages are overwritten by new messages.

The device organizes the stored logged events into the following groups (categories):

- "Conf" – log messages relating to device “boot up” and application initialization, including configuration file parsing
- "Err" - log messages relating to warnings, errors, and critical severity levels
- "Ha" – log messages relating to High Availability (HA)
- "Init" - log messages relating to device startup
- "Other" - log messages that do not belong to any category above or that are system logs

The administrator can view all the logged messages or filter the logged messages by category, time, and number of last logged messages.

The feature is supported by the following CLI commands:

```
# debug persistent-log show category-list
{conf|err|ha|init|other|sip} start-date <YYYY-MM-DD> end-date
<YYYY-MM-DD> count <Number of Logs> offset <Log Index>
```

The administrator can view statistics of the persistent logging database, which displays number of incoming logs, number of logs sent to the database, and dropped logs (due to various reasons):

```
# debug persistent-log show stats
```

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant SE/VE.

2.7.1.51 Customization of Remote SIP User Agent Field in SBC CDRs

This feature provides support for customizing the title of the “Remote SIP User Agent” field in CDRs for SBC calls. CDR customization is done in the existing SBC CDR Format table. The field represents the SIP User-Agent header, which identifies the source of the SIP message. By default, the field is excluded from the CDR.

The feature is supported by the following new optional value in the SBC CDR Format table's 'Field Type' field: "Remote SIP User Agent" (818).

Applicable Applications: SBC.

Applicable Products: All.

2.7.1.52 Snapshot Load through CLI

This feature provides support for loading a snapshot of the device's system through CLI. Snapshots provide the capability of returning the device to a previous state, which is used as a rescue option if a system malfunction occurs. Up until now, a snapshot could only be loaded through the GRUB menu.

The feature is supported by the new CLI command, load-from-snapshot:

```
(config-troubleshoot)# startup-n-recovery
(startup-n-recovery)# load-from-snapshot <Name of Snapshot>
```

Note: This feature is currently not supported for HA mode.

Applicable Applications: All.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.7.1.53 Log of Loaded CLI Script File

This feature provides support for viewing the contents of the latest CLI Script file that was loaded (i.e., copy cli-script from) to the device. The device always keeps a log file of the most recently loaded CLI Script file. The feature is supported by the following new CLI command:

```
# show last-cli-script-log
```

Note that if the device resets (or powers off), the log is deleted.

Applicable Applications: All.

Applicable Products: All.

2.7.1.54 CLI Show Run Enhancements

This feature provides support for displaying the current configuration (show running-config) of the device through CLI, according to a selected main command set (Network, Troubleshoot, System, VoIP, and Data). Up until now, only the current configuration of the command sets System, VoIP, and Data could be displayed (or full configuration).

To support the feature, the **show running-config** now provides the following optional arguments:

```
# show running-config {data|full|network|system|troubleshoot|voip}
```

Applicable Applications: All.

Applicable Products: All.

2.7.2 Known Constraints

This section lists known constraints.

Table 2-9: Known Constraints in Version 7.20A.150.004

Incident	Description
-	When upgrading the device to Version 7.2.150, syslog is enabled (instead of disabled). A workaround is to manually configure the debug level to 0. **Applicable Products:** All.
-	Hitless software downgrade from Version 7.2.150 to an earlier version is not supported (the non-hitless method must be used). **Applicable Products:** HA.
-	The device does not support Hyper-Threading (HT) for Hyper-V environments (and therefore, HT must be disabled in the device's BIOS settings). **Applicable Products:** Mediant VE.
143292	Software Hitless Upgrade from any version earlier than 7.00A.082.007 to Version 7.2.150 fails (the device crashes and resets). For devices running a version earlier than 7.00A.082.007, the device must first be upgraded to Version 7.00A.082.007 and only then to Version 7.2. **Applicable Products:** HA.
144353	The On-board, Three-way Conferencing feature for Gateway calls (3WayConferenceMode =2) functions only if the device's License Key includes an SBC license. **Applicable Products:** MP-1288.

2.7.3 Resolved Constraints

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

Table 2-10: Resolved Constraints in Version 7.20A.150.004

Incident	Description
143930	The time stamp in SIP PUBLISH messages are not according to the RFC 6035, resulting in incorrect reports. **Applicable Products:** SBC.
-	The device does not support Hyper-Threading (HT) for KVM-OpenStack and VMWare environments. (Now supported.) **Applicable Products:** Mediant VE.
-	High Availability (HA) for One-Voice Resiliency is not fully supported (signaling may not function correctly in certain scenarios). **Applicable Products:** HA-Supporting Devices.
124743	The device allows a certificate to be loaded even though it already exists in the device's Trusted Root Certificate store. As a result, duplicated certificates appear on the device. **Applicable Products:** All.
135242	The maximum number of characters that can be configured for SNMP community string is limited to 19 characters. (Resolved by an increase to 30.) **Applicable Products:** All.

Incident	Description
137574	When loading an incremental ini file through REST, the device crashes (and resets). **Applicable Products:** All.
137601	When an HA switchover occurs, the new active device always switches to the first entry in the RADIUS Servers table, regardless of which servers were used by the previously active device. **Applicable Products:** HA.
138854	If the device receives a SIP REFER message before the call is connected, the device rejects the message. As a result, call transfer fails. **Applicable Products:** SBC.
139371	Sometimes when the device uses DSPs, it attempts to activate the acoustic echo canceller even though it is disabled. As a result, the open channel fails (no voice). **Applicable Products:** All.
139442	When the device operates in High-Availability (HA) mode and a hitless software upgrade from an earlier version to Version 7.2.100 is done through the Web interface, the Web interface sometimes erroneously displays an upgrade failure message and that a reset must be done, even though the devices were upgraded successfully. If this occurs, refresh the browser and then log in again to the Web interface. **Applicable Products:** Mediant 500 E-SBC HA; Mediant 800 Gateway & E-SBC HA.
139544	When five three-way conferences are needed, channels for regular Gateway calls are lost (i.e., insufficient resources). **Applicable Products:** Mediant 500L.
139988	The 'Board Type' field in the Web interface's Device Information page does not reflect the modified UseRProductName parameter value. **Applicable Products:** All.
140061	SNMP walk on SysDataStatus causes syslog errors. **Applicable Products:** All.
140081	The order of configured rows in the Proxy Sets table is incorrect. **Applicable Products:** SBC.
140113	When the SNR is low, the device does not detect DTMF digits. As a result, Gateway calls fail. **Applicable Products:** MP-1288.
140547	Transcoding of G.711 to G.729 for loopback calls fail (disconnect) after an HA switchover. **Applicable Products:** HA Products.
141398	The device often crashes (and resets) due to a problem in memory handling. **Applicable Products:** Mediant VE.
141587	REST API does not support the sending (PUT method) of an incremental CLI Script file or incremental ini file to the device. **Applicable Products:** All.
141698	When the device sends a re-INVITE, it uses only the Extended\Allowed coders (instead of also the coder that it used before the re-INVITE). **Applicable Products:** SBC-WebRTC.

Incident	Description
141903	A registration failure occurs when the device's 288 endpoints attempt to register. This is due to an overload on the device. **Applicable Products:** MP-1288.
141933	Incorrect SIP REFER message handling: When the device forwards the SIP REFER message to the proxy server and the Refer-To header value is changed to the LAN address (of the proxy side), the routing fails. (Bug resolved by new "Local Host" option of the IPProfile SBCRemoteReferBehavior parameter.) **Applicable Products:** SBC.
142150	When using the SBC Configuration Wizard, the NAT Translation table is created with only one media port even though multiple users are configured. **Applicable Products:** SBC.
142222	The device does not forward the "opaque" field if it has an empty value in the received SIP Authenticate header. Instead, it removes the field, which may cause unsuccessful authentication. **Applicable Products:** All.
142440	The device can handle only up to 100 concurrent SUBSCRIBE messages. As a result, calls fail when this number is exceeded. **Applicable Products:** MP-1288.
142494	When the device sends SIP PUBLISH messages for QoS, the body of the message is removed when alternative routing is done. As a result, incorrect QoS reports are sent. **Applicable Products:** SBC.
142504	If a VLAN ID of any interface is modified to three digits (in the Ethernet Devices table), the device continually crashes (and resets). **Applicable Products:** Mediant 9000; Mediant VE/SE.
142528	In SIP-I, if the device receives a SIP 200 OK without 18x, the device erroneously attaches the SIP-I ANM message (instead of the SIP-I CON message). **Applicable Products:** SBC.
142633	In certain call-forking scenarios to five destinations, the device does not establish voice toward the correct destination. **Applicable Products:** SBC.
142665	When using REST API to query HA status, the returned value is the serial number instead of the HA status. **Applicable Products:** HA.
142924	Even though a license from the License Pool Manager is successfully applied to the device, the device incorrectly reports to AudioCodes One Voice Operations Center that the apply process is still in progress. **Applicable Products:** SBC.
142938	If the device receives in the media line ("m=") "AVP" with crypto (indicating SRTP), the device forwards it as RTP (as it was not received with "SAVP"). As a result, no voice occurs. **Applicable Products:** SBC.
143030	If the device sends an INVITE with VBD and the response does not include VBD but the same payload type, the device rejects the response. As a result, the call fails. **Applicable Products:** SBC.

Incident	Description
143054	The device is unable to parse a user part of a SIP Contact header that is greater than 300 characters. As a result, registration fails. **Applicable Products:** SBC.
143185	The automatic update feature fails when the IniFileUrl parameter is configured with a long string (greater than 512). As a result, the file does not load to the device. **Applicable Products:** All.
143245	During an HA switchover, the TCP session between the device and AudioCodes One Voice Operations Center ends and a new session is started by the Active device. However, all the calls that were active before the switchover are not reflected in AudioCodes One Voice Operations Center after the switchover. **Applicable Products:** HA.
143269	The CLI command to display active calls (show voip calls active) displays incorrect session IDs. As a result, calls cannot be tracked. **Applicable Products:** All.
143291	The legacy (old) Dial Plan configuration method does not function. As a result, related calls fail. **Applicable Products:** Mediant 9000; Mediant VE/SE.
143450	If the SIP Interface ports are modified, the device stops sending SIP OPTIONS message to the proxy server. As a result, connection to the proxy server is lost. A workaround is to reset the device. **Applicable Products:** SBC.
143525	A certain problem in the Linux kernel causes the device to reset. **Applicable Products:** Mediant VE.
143687	If the two units in an HA system (Active and Redundant) have the same License Key but where each License Key has a different Product Key, HA fails. **Applicable Products:** HA.
143696	When the management user clicks the Monitor tab in the Web interface, the device crashes (and resets). **Applicable Products:** Digital Gateways.
143768	For call forking, when the SBCRemoteMultipleEarlyDialogs parameter is enabled, the device does not forward the SIP 200 OK. As a result, the call fails. **Applicable Products:** SBC.
143808	If the 'Channel Select Mode' parameter in the Trunk Group Settings table is configured to "Ring to Hunt Group", calls from the SBC to a Gateway-type IP Group fails. A workaround is to configure the parameter with a different select mode. **Applicable Products:** SBC and Hybrid.
143813	If the OAMP interface is configured with untagged VLAN ID 1, modifying the VLAN ID (in the Ethernet Devices table) results in a loss of management connection to the device. **Applicable Products:** All.
143999	UDP port spacing can be configured to 0 in the Web interface, which is an invalid configuration. **Applicable Products:** Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

Incident	Description
144044	When the device sends SIP PUBLISH messages at the end of calls, all call-quality metric values (reported to AudioCodes One Voice Operations Center) are zero ("0"). **Applicable Products:** SBC.
144241	Under certain high-load session conditions, the device crashes (and resets). **Applicable Products:** SBC.
143342	When loading a License Key separately for each unit in the HA system, the device sends the acHASystemConfigMismatchAlarm alarm even though no mismatch exists between the License Keys of the active and redundant device. **Applicable Products:** HA.

2.8 Patch Version 7.20A.152.003

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

2.8.1 New Features

New features introduced in this version include the following:

2.8.1.1 User "Stickiness" to Registrar Server for IP Groups

This feature provides support for configuring the device to always route SIP requests of a user (belonging to a User-type IP Group) to the same registrar server in a Proxy Set (associated with a Server-type IP Group) to where the last successful REGISTER request was routed. In other words, once initial registration of the user to one of the IP addresses in the Proxy Set is successful (i.e., 200 OK), binding ("stickiness") occurs to this specific address (registrar). All future SIP requests (INVITEs, SUBSCRIBEs and REGISTER refreshes) from the user are routed (based on matched routing rule) only to this registrar.

When the feature is disabled, after a successful initial registration, whenever the device receives a SIP request or registration refresh from the user, the device sends the request to the currently active registrar. In the case of proxy load-balancing, there is no certainty to which IP address in the Proxy Set the request is routed.

This new feature applies to users belonging to a User-type IP Group that are routed to a Server-type IP Group configured for "stickiness". The "stickiness" is configured using a new IP Group table parameter, 'User Stickiness' (IPGroup_SBCUserStickiness) with optional values, "Enable" and "Disable".

The feature also functions when IP Group Sets are configured. If a user is bound to a registrar associated with a Server-type IP Group that belongs to the IP Group Set, IP Group Set logic of choosing an IP Group is ignored and requests are routed to this same registrar (associated with the IP Group).

The feature supports devices operating in HA mode. Registrar "stickiness" is retained even after an HA switchover.

Note:

- The Proxy Set associated with the Server-type IP Group must be configured with multiple IP addresses (or an FQDN that resolves into multiple IP addresses).
- The Proxy Set Hot-Swap feature (for proxy redundancy) is not supported for users that are already bound to a registrar. However, Proxy "hot-swap" can be achieved for failed initial (non-bounded) REGISTER requests. If a failure response is received for the REGISTER request and the response’s code appears in the Alternative Routing Reasons table, "hot-swap" to the other IP addresses of the Proxy Set is done until a success response is received from one of the addresses. In the case of failed REGISTER refresh requests from users already bound to a registrar, no "hot-swap" occurs for that request; only for subsequent refresh requests.
- When using the User Info table, registrar "stickiness" is supported only when the user initiates the REGISTER request (i.e., the User-type IP Group’s 'Registration Mode' parameter must be configured to "User Initiates Registration").
- A user's registrar "stickiness" to a specific Proxy Set's IP address ends upon the following scenarios:
    - Proxy Set modification
    - If the Proxy Set is configured with an FQDN and a DNS resolution refresh removes the IP address to which the user is bound.
    - User registration expires or the user initiates an unregister request.

Applicable Applications: SBC.

Applicable Products: All.

2.8.1.2 Trapezoid Ring Waveform Support

This feature provides support for generating trapezoid ringing for third-party, FXS analog phones that are connected to the device's FXS ports. As opposed to the normal ringing signal, which uses sinusoid waveform, some telephones require a trapezoid waveform, which provides a higher ringing signal voltage. The supported trapezoid ringing provides a ring voltage of 85Vrms and ring frequency of 20 Hz.

To support this feature, a new ini file parameter, EnableTrapezoidRing has been introduced with optional values "Enable" (trapezoid) and "Disable" (sinusoid). A device reset is required for the parameter to take effect.

Note:

- This feature is supported only on MP-1288 with Hardware Revision 2.0 or later.
- Each segment (12 ports) of an FXS Telco connector (on an FXS blade) supports up to six concurrent trapezoid ringing. If ringing is done for calls on more than this number of ports, these additional calls are rejected with a SIP response code of 503 (Service Unavailable) and a PSTN release cause code of 43 (Access information discarded).

Applicable Applications: Gateway (FXS and IP-to-Tel).

Applicable Products: MP-1288.

2.8.2 Known Constraints

This section lists known constraints.

Table 2-11: Known Constraints in Version 7.20A.152.003

Incident	Description
145029	In the Web interface, values of table fields that reference fields of other tables are not searchable using the Web interface's table search feature (i.e., the search field that appears on the same page as the table). **Applicable Products:** All.

2.8.3 Resolved Constraints

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

Table 2-12: Resolved Constraints in Version 7.20A.152.003

Incident	Description
144868	SBC call preemption (911) does not function - emergency calls fail as the device does not free required resources . **Applicable Products:** SBC.
144864	When the device forwards T.38 fax calls without DSPs, and voice quality monitoring is enabled as well as device connected to AudioCodes One Voice Operations Center, the device crashes (and resets). A workaround is to disable quality monitoring. **Applicable Products:** SBC.
144650	For the Media Transcoding Cluster application, the device is able to perform transcoding with coders that are not listed in the installed License Key. **Applicable Products:** MTC.
144384	Sometimes DiffServ values of SIP packets are incorrect and as a result, incorrect traffic priority is applied to SIP packets. **Applicable Products:** SBC.

Incident	Description
144185	The device reports packet loss even when the channel is on-hold (no packets are received). **Applicable Products:** SBC.
143974	When the devices are in HA mode and a switchover is initiated, the redundant device becomes the active device, but the initial active device remains in reset mode for a long time due to a clock synchronization issue. **Applicable Products:** HA.
142978	In some scenarios, an incorrect IP Profile ("-1") is displayed on the SBC Registered Users page of the Web interface. **Applicable Products:** SBC.

2.9 Patch Version 7.20A.152.009

This patch version includes only resolved constraints.

2.9.1 Resolved Constraints

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

Table 2-13: Resolved Constraints in Version 7.20A.152.009

Incident	Description
146000	During an HA switchover, TLS certificates are removed. As a result, calls cannot be processed and the device's management interface cannot be accessed. **Applicable Products:** SBC HA.
145933	When the device is in HA mode and resets or performs an HA switchover, all "allow" rules in the Firewall table are removed. As a result, access to the device's management interface is blocked. **Applicable Products:** Mediant VE/SE HA; Mediant 9000 HA.

2.10 Patch Version 7.20A.154.007

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

Note: This patch version is compatible with AudioCodes EMS/SEM Version 7.2.3083.

2.10.1 New Features

New features introduced in this version include the following:

2.10.1.1 Increase in CDR Fields Sent to RADIUS Server

This feature provides support for an increase in the number of CDR fields—from 40 to 128—that can be configured and sent to a RADIUS server. The fields are configured in the SBC CDR Format table (SBCCDRFormat) and therefore, up to 128 table rows can now be configured when the 'CDR Type' parameter is set to **RADIUS SBC**.

Note: The maximum RADIUS packet size is 4,096 bytes (RFC 2865). If the packet size is greater than this due to the inclusion of many CDR fields with long customized title strings, the device removes the last CDR fields and sends the Accounting-Request packet with the CDRs that meet the packet size restriction. The removed CDR fields can be viewed in the Syslog.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.10.1.2 Call Preemption for Emergency Calls by Routing Server

This feature provides support for implementing call preemption for emergency calls (such as 911) by the routing server (for example, AudioCodes ARM). If the device is enabled for call preemption for emergency calls (SBC and/or Gateway), the routing server determines whether the incoming call is an emergency call or not and if so, handles the routing decision accordingly (i.e., preempts a non-emergency call if the maximum call capacity of the device is reached in order to allow the emergency call to be routed).

The feature is supported by the following REST API enhancements:

- The REST API resource GetRoute now includes the new parameter "emergency", whose value indicates to the device whether or not ("yes" or "no") the call is an emergency call.
- The REST API URL resource */api/v1/rmConfig/globals* now includes the new parameters "preemptionmode" (enables call preemption for SBC) and "callprioritymode" (enables call preemption for Gateway). These parameters are supported by both GET and PUT methods.

Applicable Applications: SBC; Gateway (IP-to-Tel).

Applicable Products: Mediant 500; Mediant 500L; Mediant 800; Mediant 1000B; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.10.1.3 Display of Active SIPRec Sessions in CLI

This feature provides support for displaying the number of currently active SIPRec signaling sessions through the device's CLI. An active session implies that the device has sent a SIP INVITE message to the SIPRec server (SRS).

The feature is supported by the new CLI option, **siprec**:

```
show voip calls statistics siprec
SIPRec number of active sessions: 8 (redundant sessions: 0)
```

If active-standby SRS is implemented, the SIPRec sessions with the redundant (standby) SRS is shown in parenthesis.

Applicable Applications: SBC/Gateway.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.10.1.4 Number of Displayed Output Lines in CLI Terminal Window

This feature provides support for configuring the maximum number of lines (window height) displayed in the CLI terminal window (SSH and Telnet sessions) for the output of CLI commands. This settings applies to all new CLI sessions and is preserved after device resets. Up until now, the number of output lines could only be configured per CLI session (using the **window-height** command).

The feature can be configured using the following new configuration settings:

- CLI:

  ```
  configure system > cli-settings > default-window-height
  <value>
  ```

- Web interface: 'Default Terminal Window Height' (**Setup** menu > **Administration** tab > **Web & CLI** folder > **CLI Settings**)
- ini file: DefaultTerminalWindowHeight

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.10.1.5 Increase in Maximum IP Groups and Proxy Sets

This feature provides support for an increase in the maximum number of IP Groups and Proxy Sets—to 5,000—that can be configured in the IP Groups table and Proxy Sets table, respectively. The feature is applicable only to the applicable products (below) with 32-GB or 64-GB RAM. For less than 32-GB RAM, the maximum number is 1,500 IP Groups and Proxy Sets (as supported in the previous version).

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.10.1.6 Static UDP Port Assignment for SIP Signaling

This feature provides support for configuring the device to use specific, local UDP ports for SIP signaling for each SIP entity (e.g., PBX) communicating (transmit and receive) with a specific proxy server. This applies to the device's local ports on the leg interfacing with the proxy server. Up until now (and still supported if this feature is disabled), the device used the same local UDP (as well as TLS and TCP) port for all communications with the proxy server.

This feature can be used, for example, when multiple SIP entities (IP Groups) route calls to the same proxy server. In such a scenario, the device can use a different local port for each SIP entity on the leg interfacing with the proxy server. With this set up, the proxy server is thus able to identify each SIP entity based on their unique Layer-3 address (i.e., IP address + port).

The feature is configured by a new parameter in the SIP Interfaces table, 'Additional UDP Ports' (SIPInterface_AdditionalUDPPorts). The parameter is configured for the SIP Interface that is associated with the proxy server. The valid value is a range from 1025 to 65535 using the syntax *x-y* (e.g., 2000-6000). By default, the parameter is not configured. The port range must adhere to the following:

- The parameter's port range must not overlap with the UDP port configured by the 'UDP Port' parameter (SIPInterface_UDPPort).
- The parameter's port range must not overlap with UDP port ranges of other SIP Interfaces that are associated with the same network interface.
- The parameter's port range must not overlap with UDP port ranges of Media Realms that are associated with the same network interface.
- The maximum number of ports in the range is limited to the maximum number of IP Groups that can be configured.
- Only for Mediant 1000B: the end port in the port range must be less than the value of the global parameter, BaseUDPPort.

In addition, to assign a specific (static) local UDP port from the configured range to each SIP entity communicating with the proxy server, tags and Call Setup Rules are employed, using the following new Message Manipulation keywords:

- *message.incoming.local-port*: (Read-only) Contains the local port on which the SIP message is received.
- *message.outgoing.local-port*: Configures the local port on which outgoing SIP messages are sent. It can be used for "write" operations in Call Setup Rules and read-only operations for Message Manipulations.

Note that the existing message manipulation keywords "param.message.address.src.port" and "param.message.address.dst.port" have been replaced with "message.incoming.remote-port" and "message.outgoing.remote-port", respectively.

For more information on configuring this feature, refer to the *User's Manual*.

Applicable Applications: SBC.

Applicable Products: All.

2.10.1.7 Sending DTMF using both SIP INFO and RFC 2833

This feature provides support for sending DTMF digits out-of-band (not with audio stream) using both the SIP INFO and RFC 2833 methods on the same leg for the same call. Up until now, the device could use only one method for sending the DTMF digits - SIP INFO or RFC 2833 (not both). The RFC 2833 method sends out-of-band DTMF digits using the RTP protocol while the SIP INFO method sends the digits using the SIP protocol.

The feature is configured by a new parameter in the IP Profiles table, 'Send Multiple DTMF Methods' (IPProfile_SBCSupportMultipleDTMFMethods), with optional values **Enable** and **Disable** (default). To implement the feature, not only must this parameter be enabled, but the existing parameter 'Alternative DTMF Method' (IPProfile_SBCAlternativeDTMFMethod) must be configured to one of the SIP INFO values (**INFO – Cisco**, **INFO – Nortel**, or **INFO – Lucent**). In addition, sending of DTMF digits using the RFC 2833 method must be enabled (**As Is** or **Extend**), using the existing parameter 'RFC 2833 Mode' (IpProfile_SBCRFC2833Behavior).

This feature also introduces a method to stop sending the DTMF digits using the SIP INFO method when a re-INVITE is received (and keep sending the DTMF digits using the RFC 2833 method). This is done using AudioCodes proprietary SIP header, X-AC-Action in Message Manipulation rules to switch to a different IP Profile that is configured to disable the sending of DTMF digits using both methods (i.e., 'Send Multiple DTMF Methods' configured to **Disable**):

```
X-AC-Action:'switch-profile;profile-name=”IP Profile Name”'
```

Note:

- It is recommended that the settings of the switched IP Profile are identical (except for the 'Send Multiple DTMF Methods' parameter) to the initial IP Profile. Different settings may adversely affect the processing of the call.
- The feature requires DSP resources (for detection and generation of RFC 2833).

Applicable Applications: SBC.

Applicable Products: All.

2.10.1.8 Termination of Call Hold and Retrieve SIP Requests

This feature provides support for terminating call hold and call retrieve (resume) SIP requests (re-INVITE or UPDATE) for SIP entities that don't support call hold. Termination is done on the device's leg interfacing with the initiator of the call hold/retrieve. Instead of forwarding the request to the SIP entity that doesn’t support call hold/retrieve, the device terminates the request and replies to the initiator of the call hold/retrieve with a SIP 200 OK. Up until now, the device supported an option to terminate call hold requests only; call retrieve requests were forwarded to the SIP entity that did not support call hold.

The feature is supported by the new optional value—**Hold and Retrieve Not Supported**—for the existing parameter 'Remote Hold Format' (IPProfile_SBCRemoteHoldFormat) in the IP Profiles table.

Applicable Applications: SBC.

Applicable Products: All.

2.10.1.9 Multiple Management Interfaces

This feature provides support for configuring multiple management network interfaces for the device, allowing access to the device's Web-based management tool through different IP addresses. Each management interface can be configured to use a specific network interface (Control and/or Media type) and TLS Context, and can be configured to restrict access through HTTPS.

Up until now, the device's management interfaces could be accessed through either one IP network interface ("OAMP"), or all the network interfaces listed in the IP Interfaces table if the EnableWebAccessFromAllInterfaces parameter was configured to 1. However, this was a global setting that applied to all the network interfaces, and specific TLS Contexts and HTTP or HTTPS connectivity could not be specified.

The feature is supported by the new configuration table, Additional Management Interfaces table (AdditionalManagementInterfaces ini file parameter; CLI command - configure system > **additional-mgmt-if**), located in the Web interface under **Setup** menu > **Administration** tab > **Web & CLI**.

Note:

- This feature will be supported by AudioCodes ARM (REST API) in a future release.
- Additional management interfaces can be associated only with Media and/or Control network interface types (not OAMP).
- This feature will be supported for SNMP, LDAP, RADIUS and CLI access in a future release.

Applicable Applications: All.

Applicable Products: MP-1288; Mediant 500 Gateway & E-SBC; Mediant 500L Gateway & E-SBC; Mediant 800B Gateway & E-SBC; Mediant 1000B Gateway & E-SBC; Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.10.1.10 Increased Value Ranges for Proxy Online Detection

This feature provides support for an increased value range for the existing parameters 'Success Detection Retries' (ProxySet_SuccessDetectionRetries) and 'Success Detection Interval' (ProxySet_SuccessDetectionInterva). These parameters are used to ensure that connectivity with the proxy has indeed been restored.

The 'Success Detection Retries' parameter can now be configured to up to 100 retries. The 'Success Detection Interval' parameter can now be configured to up to 200 seconds.

Applicable Applications: All.

Applicable Products: All.

2.10.1.11 User Account Re-registration after Physical Link Restored

This feature provides support for the device to re-register an Account (in the Accounts table) that is configured for IMS-based registration ('Registrar Search Mode' parameter set to **According to IMS Specifications**), when the device's physical Ethernet link to the proxy is restored after a failure, even if proxy keep-alive (using SIP OPTIONS) is disabled. Up until now, re-registration due to Ethernet link restoration occurred only if keep-alive was enabled (i.e., when the link was restored the device would re-register due to successful keep-alive response).

Applicable Applications: All.

Applicable Products: All.

2.10.1.12 Enhanced SIP REFER Handling

This feature provides enhanced support for handling SIP REFER messages (used for SBC call transfer). The device can now forward a received SIP REFER message between SIP entities without changing the host part in the SIP Refer-To header. This applies to all types of call transfers (e.g., blind and attendant transfer).

The feature is supported by a new optional value—**Keep Host** (5)—for the existing 'Remote REFER Mode' (IpProfile_SBCRemoteReferBehavior) parameter.

Applicable Applications: SBC.

Applicable Products: All.

2.10.2 Known Constraints

This section lists known constraints.

Table 2-14: Known Constraints in Version 7.20A.154.007

Incident	Description
146495	The links to the "child" tables in the TLS Contexts table are not displayed when using Mozilla Firefox Web browser. **Applicable Products:** All.
145104	If any of the physical LAN cables are disconnected from the redundant device, the active device doesn’t raise an alarm to indicate this. **Applicable Products:** HA.

2.10.3 Resolved Constraints

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

Table 2-15: Resolved Constraints in Version 7.20A.154.007

Incident	Description
146330	The user is unable to log in to the CLI when login authentication is RADIUS-based, as the RADIUS access level is incorrect. **Applicable Products:** All.
146202	When a few Web sessions exist with the device, under some conditions the device crashes (resets). **Applicable Products:** All.
146135	After an HA switchover, the private key no longer matches the certificate. As a result, login to the management interface (Web) and calls fail. **Applicable Products:** Mediant 9000; Mediant VE/SE.
146110	The device changes the SIP Refer-To header (host part) even though it is configured not to. As a result, call processing is incorrect. (Resolved by a new optional value "Keep Host" (5) for the SBCRemoteReferBehavior in the IP Profile table.) **Applicable Products:** SBC.
146068	The Proxy Set alarm is not cleared after connectivity with the lost proxy is restored **Applicable Products:** All.
146053	The value range of the ProxySet_SuccessDetectionRetries parameter is insufficient (detects primary proxy is online again before reverting to it). (Parameter range has been increased). **Applicable Products:** SBC.
146034	After the device restarts, the alarms it sent previously to the AudioCodes One Voice Operations Center show a different timestamp between pre- and post- reset. **Applicable Products:** All.
145973	After an HA switchover, the default self-signed certificate is corrupted and as a result, calls fail. **Applicable Products:** HA.

Incident	Description
145969	When employing LDAP-based login authentication, Index 0 cannot be configured in the LDAP Management Server Group table. As a result, login to the device could not be done. A workaround is to use Index 1. **Applicable Products:** All.
145946	The TDM-to-SBC feature is not functional; the device does not use licenses from the TDM channel. As a result, calls fail. **Applicable Products:** Hybrid (Gateway with SBC).
145920	The device cannot be accessed through SSH (enabled), which is caused by a memory leak. **Applicable Products:** All.
145734	When using the CLI Script file for configuration backup and restore, Dial Plan Rules are not restored. **Applicable Products:** SBC.
145695	When there are calls between two channels that are handled by two different cores, the device crashes (resets). **Applicable Products:** Mediant VE SBC.
145582	When the Destination IP Group is not specified in the IP-to-IP Routing table, the wrong IP Group is chosen and as a result, SBC call routing fails. **Applicable Products:** SBC.
145577	LDAP-based routing authentication fails after a while. As a result, call routing fails. A workaround is to reset the device. **Applicable Products:** All.
145563	The device does not update the DNS IP address obtained from DHCP. A workaround is to use a static IP address. **Applicable Products:** All.
145471	The "Match Count" statistics in the Firewall table displays incorrect values. As a result, access to the device is blocked. **Applicable Products:** Mediant 9000; Mediant VE/SE.
145404	The Remote Web Services page in the Web interface is displayed corrupted. **Applicable Products:** All.
145351	IP Groups are displayed as offline in the Topology View of the Web interface after a version upgrade. **Applicable Products:** All.
145282	If the IP Group is configured as a "Gateway" type in the IP Groups table and the IP Group sends an unregister request or the IP Group type is changed (for example, to “User"), the “GW GROUP STATUS” fields in the IP Groups table is not updated and shows "registered" (even after a device reset). **Applicable Products:** SBC
145018	The SIPRec application does not respond to session timer re-INVITE or UPDATE. As a result, calls fail. **Applicable Products:** All.
144995	No corresponding CLI command for the ‘Publication IP Group ID' parameter. (Resolved - configure voip > media rtp-rtcp > publication-ip-group-ID.) **Applicable Products:** SBC.

Incident	Description
144979	During silence period from the IP side, the device sends noise to the PSTN side. A workaround is to configure the ECEnableComfortNoiseGeneration parameter to 0. **Applicable Products:** Gateway.
144634	The device's management (Web and CLI) user password cannot be configured (in clear text) in the ini file (and then loaded to the device). **Applicable Products:** All.
144600	The device does not correlate between the incoming call and the received SMDI message. As a result, the call fails. **Applicable Products:** Gateway (with SMDI).
144586	The device doesn’t forward RTP to a user that is located behind NAT when the NATMODE parameter is configured to 3 (By Signaling). As a result, no voice occurs. **Applicable Products:** SBC.
144504	When adding a new Web user to the active device (in the Local Users table), the new user is not added to the redundant device after an HA switchover. As a result, the user is unable to log in to the device. **Applicable Products:** HA.
144230	In high load conditions (CPU overload), the device sends TCP window of 0. As a result, requests were dropped. **Applicable Products:** SBC.
144041	When the device rejects a call due to Classification failure, the device does not include the session ID in the report sent to AudioCodes One Voice Operations Center at the end of the call. **Applicable Products:** SBC.
143394	The user is unable to configure the 'Silence Detection Method' (FarEndDisconnectSilenceMethod) parameter. (This parameter erroneously appears in the Web interface and is not applicable). **Applicable Products:** MP-1288; Mediant 5xx; Mediant 8xx; Mediant 2600/4000; Mediant 9000; Mediant VE/SE.

2.11 Patch Version 7.20A.154.044

This patch version includes resolved constraints only.

Note: This patch version is compatible with AudioCodes EMS/SEM Version 7.2.3088.

2.11.1 Resolved Constraints

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

Table 2-16: Resolved Constraints in Version 7.20A.154.044

Incident	Description
145877	If during an established call the call mode changes from RTP forwarding to transcoding (trans-rating), the device crashes (and resets). **Applicable Products:** SBC.
146815	The remote side opens TCP connections (per SIP dialog), but does not close them. When the device tries to close the connections, it crashes (and resets). **Applicable Products:** All.
147019	When the device functions as a DHCP server, under a high load of DHCP requests, the device crashes (and resets). **Applicable Products:** All.
146955	After the device is upgraded, it sends an alarm indicating that the IP Group is blocked (which it is not). **Applicable Products:** All.
146955	When using quality of service (QoS) rules with SNMP, the device crashes (and resets). **Applicable Products:** All.
146865	Message Manipulation rules (MessageManipulations) with "\" do not load when loading an ini file. A workaround is to use "\\" (double backslash). **Applicable Products:** All.
146969	The device rejects a user registration if the Contact header of the new REGISTER request already exists for another AOR. **Applicable Products:** SBC.
146809	If a SIPRec re-INVITE is sent after a REFER failed, the device crashes (resets). **Applicable Products:** SIPRec Supporting Devices.
146792	Ethernet port information is not displayed in the Web interface. **Applicable Products:** All.
146749	The device crashes (and resets) due to timing issues between device processes. **Applicable Products:** SBC.

Incident	Description
146791	No voice occurs in the following scenario: The device is defined to play RBT. When it receives 180 without SDP, it disconnects the voice stream and plays RBT. When the 200 OK is received with the same SDP version, the device stops playing the RBT, but does not reconnect the voice stream. A workaround is to configure the 'SBC Remote Can Play Ringback' parameter to Yes. **Applicable Products:** SBC.
146827	Due to certain operations in debug recording, the device crashes (and resets). **Applicable Products:** All.
146614	The CLI command to copy the CLI Script file to FTP does not function. **Applicable Products:** Mediant 1000.
145136	Configuration transfer from AudioCodes One Voice Operations Center to the device through HTTPS fails. A workaround is to load the configuration manually. **Applicable Products:** Mediant 4000.
146485	When there is redundant AudioCodes One Voice Operations Center License Pool Manager server, the device fails to communicate with it. A workaround is not to use a redundant License Pool Manager server. **Applicable Products:** SBC.

2.12 Patch Version 7.20A.154.052

This patch version includes resolved constraints only.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.321 and EMS/SEM Version 7.2.3088.

2.12.1 Resolved Constraints

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

Table 2-17: Resolved Constraints in Version 7.20A.154.052

Incident	Description
146684	When an HA switchover occurs, no voice occurs on existing calls due to a problem in Generic Attribute Registration Protocol (GARP) timing. **Applicable Products:** SBC HA.
147408	When a user is located behind NAT and a re-INVITE changes the media port, the device sends the RTP to an incorrect destination. As a result, one-way voice occurs. **Applicable Products:** SBC.
147398	When using the SIPRec feature, certain SIPRec calls do not disconnect correctly and as a result, the device crashes (resets). **Applicable Products:** SBC.
145877	If an ongoing call changes from RTP forwarding to transcoding (transrating), the device crashes (resets). **Applicable Products:** SBC.

2.13 Patch Version 7.20A.154.059

This patch version includes resolved constraints only.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.321 and EMS/SEM Version 7.2.3088.

2.13.1 Resolved Constraints

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

Table 2-18: Resolved Constraints in Version 7.20A.154.059

Incident	Description
147735	The device does not clear registration entities from its database after un-REGISTER requests. As a result, it cannot register new users due to database being at maximum registration entries. **Applicable Products:** SBC.

2.14 Patch Version 7.20A.156.009

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

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.2.3083.

2.14.1 New Features

New features introduced in this version include the following:

2.14.1.1 Port Assignment per Registered User

This feature provides support for assigning a unique, local UDP port (for SIP signaling) per registered user. Up until now, SIP messages received from all the registered users (User-type IP Group) were sent to and received from the proxy server (Server-type IP Group) on the same local UDP port configured for the SIP Interface (UDP Port parameter) associated with the Proxy Set of the proxy server.

With this feature, the device assigns each registered user a unique local port from a configured port range, and traffic between the user and proxy server is sent and received on the unique port (on the leg interfacing with the proxy server).

To support this feature, a new parameter—User UDP Port Assignment (IPGroup_UserUDPPortAssignment; user-udp-port-assignment)—has been added to the IP Groups table. The parameter must be enabled for the IP Group of the proxy server. In addition, the port range from which the device allocates unique ports to each user is configured by the existing parameter, Additional UDP Ports of the SIP Interfaces table (for the SIP Interface associated with the proxy server).

The device assigns a unique port upon the first REGISTER request received from the user. Subsequent SIP messages other than REGISTER messages (e.g., INVITE) received from the user are sent to the proxy server on this unique local port. The device rejects the SIP request if there are no free ports available for use (due to the number of registered users exceeding the configured port range). The unique port is also used for registration refreshes. A registration expiry de-allocates the unique port. For SIP requests received from the proxy server and destined to the user, the local port on which they are received is irrelevant (unique port or any other port); the device does not use this port to identify the registered user.

Note:

- The feature does not apply to SIP requests received from non-registered users. For these users, the device sends all requests to the proxy server on the single port configured for the SIP Interface (UDP Port parameter).
- For HA systems, the unique port assigned to a registered user is used after an HA switchover.
- This feature is applicable only if the user initiates registration (i.e., user sends the REGISTER request). In other words, the Registration Mode parameter of the IP Group of the user must be configured to User Initiates Registration.

Applicable Applications: SBC.

Applicable Products: All.

2.14.1.2 Multiple AORs with Same Contact User

This feature provides support for handling registration and call routing when multiple AORs have the same URI in the Contact header, as shown in the example below. Such a scenario typically occurs when two SIP endpoints reside in separate private networks and both are assigned the same local IP address.

- User 1 Registration:

```
REGISTER sip:300@10.33.4.140;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=OTGHREPCXDBIWECOCPJK
From: <sip:300@domain1;user=phone>;tag=ULYEYCGXHXMBPSOCXVWH
To: <sip:300@domain1;user=phone>
Call-ID: XDRXGAAWNVBTFHBMQCKE@10.33.2.38
CSeq: 1 REGISTER
Contact: <sip:300@10.33.2.40>
```

- User 2 Registration:

```
REGISTER sip:300@10.33.4.140;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=YHDWUJRMMOEIJRXVYKHD
From: <sip:300@domain2;user=phone>;tag=CVYTCHLIVMPBCGNGRTUA
To: <sip:300@domain2;user=phone>
Call-ID: INRNGFCHFHETRXAQNAIT@10.33.2.38
CSeq: 1 REGISTER
Contact: <sip:300@10.33.2.40>
```

In the above example, the device adds two AORs ("300@domain1" and "300@domain2") to its registration database, where each AOR is assigned the same Contact URI ("300@10.33.2.40").

To support this feature, the device needs to search for the user in its registration database using the full URI (user@host parts) - . Therefore, the existing parameter, SBCDBRoutingSearchMode must be configured to 1.

Applicable Applications: SBC.

Applicable Products: All.

2.14.1.3 Syntax Enhancement for Dial Plan Tags

This feature provides support for using the dot symbol (.) in Dial Plan tag values. For example, the tag can now be configured as an IP address in dotted-decimal notation (10.1.1.2). Note that the configured tag cannot start with a dot; it can be located anywhere after the first character, for example, "Country=USA.NY".

Applicable Applications: SBC.

Applicable Products: All.

2.14.1.4 DHCP Option 160 for Automatic Provisioning

This feature provides support for DHCP Option 160, which the device, as a DHCP client, can use to download software (.cmp) and configuration (.ini) files from a provisioning server. Option 160 defines the location (URL address) of the provisioning server and optionally, the names of the required files and their folder location on the server.

Upon device reset or power up, the device sends a DHCP request to a DHCP server for networking parameters (e.g., IP address). The response from the DHCP server can include the networking information as well as Option 160.

The following syntax is supported for defining the URL and configuration/firmware filenames in DHCP Option 160:

- <protocol>://<server IP address or hostname>
- <protocol>://<server IP address or hostname>/<software filename>
- <protocol>://<server IP address or hostname>/;<configuration filename>
- <protocol>://<server IP address or hostname>/<software filename>;<configuration filename>

Where *protocol* can be HTTP, HTTPS, FTP or TFTP. As shown above, a URL can include both the software and configuration filenames. In this case, they must be separated by a semicolon (;) and without spaces.

If the URL does not specify a configuration filename or the file does not exist on the provisioning server, the device requests from the server a "default" configuration file whose name includes the device's product name and MAC address (<Product><MAC>.ini, for example, "M800B00908f5b1035.ini"). If this "default" file also does not exist on the server, the device attempts to retrieve another "default" configuration file whose name includes only the device's product name (<Product>.ini, for example, "M800B.ini"). The device makes up to three attempts to download the configuration file if a failure occurs (i.e., file not exist or any other failure reason). This applies to each of the configuration files, as mentioned previously.

If the URL specifies a software file, the device makes only one attempt to download the file (even if a failure occurs). If the URL does not specify a software file, the device does not make any attempt to download a software file.

Once the device downloads the file(s), it undergoes a reset to apply the configuration and/or software. In addition, once the file(s) has been downloaded, the device ignores all future DHCP Option 160 messages. Only if the device is restored to factory defaults will it process Option 160 again (and download any required files).

To support the feature, the new parameter, DhcpOption160Support has been introduced, with optional values 0 to disable (default) and 1 to enable DHCP Option 160 handling. A device reset is required for the parameter to take effect.

Applicable Applications: SBC & Gateway.

Applicable Products: All.

2.14.1.5 ENUM Queries for Call Setup Rules

This feature provides support for configuring Call Setup rules to query ENUM servers and to handle responses from ENUM servers. ENUM translates ordinary telephone numbers (E.164 telephone numbers) into Internet addresses (SIP URIs), using the ENUM's DNS NAPTR records. Once resolved into a URI, the device can route the call to this destination address.

To support the feature, the Call Setup Rules table's 'Query Target' parameter has a new optional value, **ENUM** (3). In addition, in order to use the query result, the new Call Setup rule keywords have been introduced: "enum.result.url" and "enum.found" (if condition for ENUM located for the number). The ENUM server's address is defined for the IP Interface used for the call.

Applicable Applications: SBC.

Applicable Products: All.

2.14.1.6 Message Conditions for Starting/Stopping SIPRec Sessions

This feature provides support for assigning a Message Condition rule (configured in the Message Conditions table) to a SIP Recording rule (SIPRec) in the SIP Recording Rules table. The Message Condition rule defines the condition for starting and stopping a SIPRec session. Only if the condition is met will the device start the SIPRec session.

To support the feature, a new parameter, 'Condition' (SIPRecRouting_ConditionName) has been added to the SIP Recording Rules table, which assigns a Message Condition rule. For this feature, only the following keywords can be used in the syntax in Message Condition rules:

- var.global
- var.session.0
- srctags/dsttags (only SBC too).

The feature is typically configured using Message Condition rules together with Call Setup rules (CSR). For example, the CSR can assign the "srctags" tag with the value "record" if the SIP message contains a header "X-Record:yes". The Condition rule can then define the condition srctags=='record'. If the condition is met, the device will start a SIPRec session for the SIP dialog session.

Applicable Applications: SBC & Gateway.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.14.1.7 SIP Classification by IP Address and Contact Header

This feature provides support for classifying incoming SIP dialog messages based on the combination of source IP address and URI of the Contact header. The feature applies to User-type IP Groups that represent multiple users. Therefore, multiple users can now be registered from a single IP address when using SIP Connect. Up until now, SIP Connect classification was based only on IP address.

To support this feature, the existing IP Group table parameter, 'SIP Connect' (IPGroup_SIPConnect) has a new optional value, **Classify by IP and Contact** (2). The existing optional value, **Yes** (1) has been renamed to **Classify by IP**.

For initial user registration:

- If configured to **Classify by IP**, the device adds a key representing the user to its registration database based on the REGISTER request's source IP address, port (if UDP) and SIP Interface ID (e.g., "10.33.3.3:5010#1"). The device rejects initial registration requests that have the same IP address, as the necessary key is already used for another registration.
- If configured to **Classify by IP and Contact**, the device adds a key representing the user to its registration database based on the URI of the Contact header, source IP address, port (if UDP) and SIP Interface ID (e.g., "user@host.com#10.33.3.3:5010#1"). The device rejects initial registration requests that have the same IP address and Contact URI, as the necessary key is already used for another user registration.

Applicable Applications: SBC.

Applicable Products: All.

2.14.2 Known Constraints

This section lists known constraints.

Table 2-19: Known Constraints in Version 7.20A.156.009

Incident	Description
147612	For the SIP call-flow feature where the device sends SIP messages to OVOC, for messages that undergo authentication, the device only sends OVOC the SIP messages from the INVITE that is sent with the user's credentials (i.e., initial INVITE and subsequent SIP 4xx authentication responses are not sent). **Applicable Products:** All.
148119	Mediant VE SBC with 1 vCPU / 2-GB RAM is not supported. **Applicable Products:** Mediant VE SBC .
147892	The device does not support HA mode. **Applicable Products:** Mediant 800.
148296	The configured value of the 'Name' field in the IP Groups table and Proxy Sets table cannot end with a space or tab. **Applicable Products:** All.

2.14.3 Resolved Constraints

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

Table 2-20: Resolved Constraints in Version 7.20A.156.009

Incident	Description
148524	In certain scenarios, the license (with license pool) is not synchronized correctly between the two devices in the HA system after an HA switchover or a reset. **Applicable Products:** HA.
143959	After a power off and then on, the device requests a license from the EMS (OVOC), as due to the connection lost with the EMS, the device lost its current license. A workaround is to assign the license manually from the EMS. **Applicable Products:** SBC (with License Pool).
146860	If a user sends a SIP REGISTER message to a server through the device and the server responds with a SIP 401, the user sends a new REGISTER, but when the device forwards it to the server, it removes the proprietary body from the message. As a result, incorrect information is sent to the server. **Applicable Products:** SBC.
148136	For direct-media calls, the device does not release allocated resources. As a result, calls fail. **Applicable Products:** SBC.
147262	In scenarios where the device receives a call from the Tel side and sends forking INVITES to multiple destinations (belonging to the same IP Group) and implements CSR for manipulation, the device uses the incorrect CSR rule, resulting in the calls being sent with an incorrect destination number. **Applicable Products:** Gateway.

Incident	Description
148519	The ENUM feature with Call Setup Rules does not function with Gateway calls (only SBC calls). **Applicable Products:** All.
148366	When the device receives a large INVITE (greater than 4k), it does not send a route request (getRoute) to ARM and as a result, the call fails. **Applicable Products:** All (SBC with ARM).
148309	In an SRTP call, if the crypto key changes before an HA switchover, then after the switchover the device uses the old keys. As a result, no voice occurs. **Applicable Products:** HA.
147402	For sent Syslog CDRs, the device truncates CDR field values that contain many characters. **Applicable Products:** All.
147975	The CLI command **clear voip calls** does not function properly and when run the CLI "freezes" and need to press CTRL+C to release it. **Applicable Products:** All.
147494	The parameter **asserted-identity-m** does not appear in the CLI. **Applicable Products:** All.
147877	When the device receives an SNMP Get for the MIB of Channel Status for a specific CID, it includes the "invalid input parameter" message in the sent Syslog. **Applicable Products:** Mediant VE/SE; Mediant 9000.
147708	When forwarding SBC messages, the device does not change the media IP address in the SDP body to its own IP address. As a result, no voice occurs. **Applicable Products:** All.
147508	When connection to the LDAP server is lost, the device responds very late for implementing SBC alternative routing. **Applicable Products:** All.
147491	When the query response from the LDAP server is delayed, the device switches to SBC alternative routing after 10 seconds instead of waiting 16 seconds, resulting in incorrect routing. **Applicable Products:** All.
147463	When the device performs SBC outbound manipulation and it receives a SIP NOTIFY request with an MWI body that contains “Messages-Waiting: Yes”, it erroneously forwards the NOTIFY request with “Messages-Waiting: No”. As a result, MWI does not occur. **Applicable Products:** All.
147415	If the plus (+) character is included in an SBC tag name, the "dialplan.result" cannot be used. **Applicable Products:** All.
147402	Tags defined with many characters are truncated in generated customized CDR. **Applicable Products:** All.
147372	The displayed coder in the Web interface's Monitor page is incorrect. **Applicable Products:** MP-1288.
147341	When running the CLI command **show voip dsp status** when there are no DSPs causes the device to crash. **Applicable Products:** Mediant 4000.

Incident	Description
147298	When the device's ports are configured to Gigabit speed, the MAC addresses of the ports are not detected and as a result, no voice occurs. A workaround is to use auto-negotiating. **Applicable Products:** All.
147197	When filtering display (**show** command) in the CLI, filtering using **grep** does not function properly. **Applicable Products:** All.
147087	During a test call, the device crashes (and resets). **Applicable Products:** All.
146060	When the device acts as DHCP server and there is a high load of DHCP and ARP requests, it crashes (and resets). **Applicable Products:** All.
147017	If the device is configured in proxy mode and it receives a SIP 18x for forking with Record-Route header, it sends the response without the header. As a result, the SBC call fails. **Applicable Products:** All.
147015	If the device receives a SIP 491 response to an INVITE, it sends the new INVITE with the same CSEQ as the previous INVITE. As a result, the SBC call fails. **Applicable Products:** All.
146984	During certain LDAP operations, the device crashes (and resets). **Applicable Products:** All.
146956	The device does not assign an IP Profile to an incoming REGISTER message received from an IP Group for SBC calls. **Applicable Products:** All.
146926	For IP-to-Tel calls, if the device receives an ISDN FACILITY message, the device uses the wrong contact in the outgoing SIP 302. As a result, the call is not routed correctly. **Applicable Products:** Digital Gateway.
146888	The device sends "Realm" in the SIP WWW-authenticate header, but the remote side expects "realm" (lower case). As a result, authentication fails for SBC calls. **Applicable Products:** All.
146869	The ini file parameter AGGRESSIVEDTMFERASURE has no corresponding command in the CLI. **Applicable Products:** Gateway.
146842	The device discards incoming messages that are larger than 260 bytes. As a result, calls fail. **Applicable Products:** Digital Gateway.
146823	When the parameter BrokenConnectionEventTimeout is configured on the HA system, the configuration change is not sent to the redundant device. **Applicable Products:** HA.
146813	If any channel command (such as Open-Channel or Avtivate-RTP) fails during the Hitless Software Upgrade, the process fails. As a result, HA fails. **Applicable Products:** HA.

Incident	Description
146808	The IDS Policy blacklist does not function - blocked users can access the device when using TCP. **Applicable Products:** Mediant 4000.
146805	When working with the SBC Configuration Wizard, a problem exists when selecting a template. **Applicable Products:** All.
146772	If the LDAP server doesn't return a value for the attribute, the device considers the string as ‘NULL’ and returns FALSE. As a result, incorrect LDAP handling. **Applicable Products:** All.
146587	The device responds with the incorrect crypto tag in the INVITE with SRTP, causing a voice problem in SBC calls. **Applicable Products:** All.
146325	Incorrect handling of incoming SBC packet causes the device to crash (reset). **Applicable Products:** All.
146303	When the device receives an INVITE with "a=maxptime:40", it responds with the incorrect ptime (ptime = 40) for SBC calls. **Applicable Products:** All.
146189	When CRP is configured with SBCKeepContactUserinRegister = 2 and a call is forked to two IP phones (same AOR but different contact), the call is disconnected after 30 seconds. **Applicable Products:** CRP.
146096	The device reports overload even when there is no SBC traffic. **Applicable Products:** All.
146072	If the device sends an un-REGISTER due to a session expire and receives a SIP 401 in response, when the new REGISTER arrives, the device does not route SBC messages correctly. **Applicable Products:** All.
145848	The device fails in some vulnerability scan, causing a security risk. **Applicable Products:** All.
145765	If the user attempts to import an invalid TLS certificate, the load fails without any notification of the reason to the user. **Applicable Products:** All.
145401	The Details tab of some tables in the Web interface is not displayed. A workaround is to delete the Web browser cache. **Applicable Products:** All.
144652	In certain situations when one of the device crashes, HA mode does not recover. **Applicable Products:** HA Devices.
144187	CLI erroneously displays that the **ping** command can ping a hostname (but, it can only ping an IP address). **Applicable Products:** All.
143766	The device sends an alarm to the EMS that its fan is not operating, even though it is working. **Applicable Products:** Mediant 4000.

Incident	Description
148054	After performing a hitless software upgrade and the device uses a License Pool, the Remote Web Services table shows incorrect configuration even though the device operates normally. A workaround is to wait 15 minutes after the upgrade completes, and then in EMS/OVOC license pool page, right-click the device, and choose Update MG to download a new License Pool. **Applicable Products:** HA Devices.

2.15 Patch Version 7.20A.156.023

This patch version includes only resolved constraints.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.2.3104.

2.15.1 Resolved Constraints

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

Table 2-21: Resolved Constraints in Version 7.20A.156.023

Incident	Description
148696	When the device is in HA mode and an SBC call's SDP parameters (e.g., IP address and port) change, when an HA switchover occurs, the device erroneously uses the old SDP parameters. As a result, no voice is heard for a few minutes. **Applicable Products:** HA.
148275	If the device adds to the coder list of a call an extended coder for the image (T.38 fax), if the remote side rejects the T.38 (i.e., no supported), the device crashes (resets). **Applicable Products:** SBC.
148555	For a WebRTC call done from a Firefox browser, if a second re-INVITE SIP message occurs, the device crashes (resets). **Applicable Products:** SBC with Web RTC.
146960	When using CAS and SRTP and the call destination changes, the device does not change the SSRC and the sequence number is lowered and thus, the remote side drops the packets. As a result, one-way voice occurs. **Applicable Products:** CAS Gateway.

2.16 Patch Version 7.20A.156.041

This patch version includes only resolved constraints.

Note:

- This patch is applicable only to Mediant 9000 SBC.
- This patch version is compatible with AudioCodes One Voice Operations Center Version 7.2.3104.

2.16.1 Resolved Constraints

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

Table 2-22: Resolved Constraints in Version 7.20A.156.041

Incident	Description
149346	For the Media Transcoding Cluster (MTC) feature, when performing an HA switchover on the device, the Media Transcoders (MT) reset and connection is lost (for a few minutes) between the device and the Media Transcoders. **Applicable Products:** Mediant 9000.
149345	When an ini file is loaded to the device that changes the VLAN of the OAMP interface, connection with the device is lost. **Applicable Products:** Mediant 9000 HA.
149302	VI - M9K HA Switch-over Description Race condition during DSP restart causes the device to crash (reset). **Applicable Products:** Mediant 9000 HA.

2.17 Patch Version 7.20A.158.009

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

> **Note:** This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.1079, and EMS/SEM Version 7.2.3104.

2.17.1 New Features

New features introduced in this version include the following:

2.17.1.1 Sending SIP Messages to OVOC for SIP Call Flow Diagrams

This feature provides support for the device to send SIP messages (in XML format) of SIP call dialogs to AudioCodes One Voice Operations Centers so that One Voice Operations Center management users can view the call dialog sessions as call flow diagrams. The call flow is displayed in One Voice Operations Center using vertical and horizontal lines, where the vertical lines represent the SIP entities (including AudioCodes device) involved in the dialog and where the horizontal lines represent the SIP requests and responses.

SIP call flow diagrams may be useful for debugging and for better understanding of the SIP call. The call flow displays all the SIP messages related to the call session, including requests (e.g., INVITEs) and responses (e.g., 200 OK). For SBC calls, the call flow reflects messages as sent "over the wire" - incoming messages before manipulation and outgoing messages after manipulation, For Gateway calls, the call flow reflects incoming messages after Pre-Parsing Manipulation (if configured) but before general Message Manipulation, and outgoing messages after manipulation.

To support this feature:

- The new parameter has been introduced to enable or disable the feature: 'SIP Call Flow Report Mode' (configure voip > qoe call-flow-report) with optional values “Enable” and “Disable” (default).
- To send SIP call flow messages for specific calls only, the existing Logging Filters table can be used. For specifying these messages, the table's 'Log Destination' parameter must be configured to the new optional value, "Call Flow Server" and the 'Log Type' parameter to the new optional value, "Call Flow". If the table does not include any filtering rule for SIP call flow, the device sends One Voice Operations Center call flow messages for all calls.

Note:

- The feature does not support SIPRec messages and REGISTER messages.
- For HA systems, during a switchover the device stops sending the SIP call flow messages of current SIP dialogs and continues sending them after the switchover (even though OVOC does not display the continuation of the call after switchover).
- If the device experiences a CPU overload, it stops sending SIP call flow messages to the One Voice Operations Center until the CPU returns to normal levels.

Applicable Applications: SBC and Gateway.

Applicable Products: All.

2.17.1.2 Configurable Unit of Measurement for Call Duration in CDRs

This feature provides support for configuring the unit of measurement for call duration in CDRs ('Call Duration' field) generated by the device. The unit of measurement can be configured to seconds (default), deciseconds, centiseconds, or milliseconds. Up until now, call duration was displayed only in seconds.

This feature is configurable by the following new parameter:

- Web: 'Call Duration Units'
- CLI: configure troubleshoot > cdr > call-duration-units
- ini: CallDurationUnits

Applicable Applications: All.

Applicable Products: All.

2.17.1.3 New Customized CDR Field "Call End Sequence Number"

This feature provides support for a new CDR field—"Call End Sequence Number" [442]—that can be added to CDRs (customizable), using the Gateway CDR Format table or SBC CDR Format table.

The feature applies to Syslog, RADIUS, and local-storage CDRs. The field is added only to CDRs that are generated at the end of calls. For each CDR, the value is assigned the next consecutive number. For example, for the first terminated call processed by the device, the field is assigned the value "1"; for the second terminated call, the field is assigned the value "2", and so on. The field value resets to 1 upon a device reset, an HA switchover (for HA-supporting products), or when it reaches the value FFFFFFFF (hexadecimal).

As this CDR field value is consecutive, the feature can be useful for checking whether there are any missing CDRs.

Applicable Applications: SBC and Gateway.

Applicable Products: All.

2.17.1.4 CDR Local Storage Enhancements

This feature provides the following enhanced support for the local storage of CDRs:

- At full session capacity, CDRs can be stored for at least seven days (depending on local storage configuration).
- CDR files can be compressed to a ZIP or GZIP file, using the new CDRLocalCompression parameter.
- The name of the CDR file can be configured, using the new CDRLocalFileName parameter. The configuration supports format specifiers. For example, "CDR_%y.%m.%d-%H.%M.%S_%qqqqq.csv" creates the filename "CDR_17.12.25-14.20.02_00010.csv" (i.e., 25 December 2017, 14:20:02).
- Each CDR is automatically assigned a unique sequence number, which is appended (by default) at the end of the filename.
- CDRs can be accessed through SFTP, allowing the SFTP client to rename CDR files or download them. Regular CDR files are stored in the *\/cdr folder and SBC test call CDRs are stored in the /cdr-gw* folder. The SFTP client needs to authenticate itself with the SFTP server (device). Access is granted only to users with Security Administrator level.
- The names of the following existing parameters have been modified:
    - 'Local Storage Max File Size' (CDRLocalMaxFileSize) has been renamed 'File Size'
    - 'Local Storage Max Number of Files' (CDRLocalMaxNumOfFiles) has been renamed 'Number Of Files'
    - 'Local Storage File Creation Interval' (CDRLocalInterval) has been renamed 'Rotation period'

Note:

- Devices running more than 100 calls per second must use a file size (CDRLocalMaxFileSize) that is greater than 100 MB.
- When upgrading a device that already uses CDR local storage, the default maximum

file size (CDRLocalMaxFileSize) is 100 MB.

- When upgrading a device that already uses CDR local storage, the filename of the CDRs will be changed using the default filename format specifiers (CDR__%y.%m.%d-%H.%M.%S_%qqqqq.csv).

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.17.1.5 CDR Local Storage Value Changes

This feature provides the following changes in the supported values of existing CDR local storage parameters:

- CDRLocalMaxFileSize (min., max., default):
  - Mediant 9000/Mediant VE/SE: 1024, 1048567, 102400
  - Mediant 2600/Mediant 4000: 1024, 10000, no change (1024)
  - All other products: no change (100), 10000, no change (1024)
- CDRLocalMaxNumOfFiles (max):
  - Mediant 9000/Mediant VE/SE: 65535

Applicable Products: All.

2.17.1.6 Enhanced HA Network Monitor Feature

This feature provides enhanced support for the HA Network Monitor feature, applicable to devices operating in HA mode. This new feature enables the monitoring (using pings) of multiple network entities (destination addresses). Up until now, only a single network entity could be monitored. This enhancement is especially important for deployments that use multiple network interfaces and thus, different network entities in different networks can be selected for monitoring. The feature also allows the administrator to configure the minimum number of failed monitored network entities in order to trigger an HA switchover.

To support the feature, the following new configuration entities have been introduced:

- HA Network Monitor table (HaNetworkMonitor; configure network > high-availability network-monitor), which defines up to 10 rows, each with up to 5 destinations (IP addresses) to ping.
- HA Network Monitor Peers Status table: Displays the status of each destination (IP address) of a selected row in the HA Network Monitor table.
- 'Failed Monitored Rows for Switchover' parameter (HaNetworkMonitorThreshold or configure network > high-availability settings > network-monitor-threshold), which defines the number of failed monitored network entries (ping destinations) required to trigger an HA switchover.

This feature also introduces a new SNMP alarm, acHANetworkMonitorAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.55), which is raised (Major severity) when all previously reachable destinations configured for a specific row in the HA Network Monitor table become unreachable.

Note:

- Existing standalone HA parameters in CLI have been relocated from the “high-availability” folder to the “high-availability settings” folder.
- The following parameters are now obsolete: HAPingDestination, HAPingSourceIfName, HAPingRetries, and HAPingTimeout.

Applicable Applications: SBC/Gateway.

Applicable Products: Mediant 500 Gateway & E-SBC; Mediant 800 Gateway & E-SBC; Mediant 2600 E-SBC; Mediant 4000 SBC; Mediant 9000 SBC; Mediant VE/SE.

2.17.1.7 LDAP-based Management Services

This feature provides support for configuring an LDAP-based management service account (Management Service-type LDAP server). This LDAP service account has an always-on connection with the device, using a configured LDAP username (Bind Name) and password, and which performs **only user authorization** for users attempting to log in to the device. This account operates together with the already supported LDAP-based management account (Management-type LDAP server), which in this setup, is used only for authenticating the user's login username and password.

The device connects to the Management-type LDAP server only when users attempt to log in to the device. If authentication is successful, the device then queries the Management Service-type LDAP server for user authorization (i.e., the user's management access level and privileges). Therefore, having two separate LDAP-based management accounts —one for user authentication and one for user authorization—whereby authorization is performed only by an LDAP "administrator", may provide additional security to the network by preventing users from accessing the authorization settings of the LDAP server.

To support the feature, the existing 'Type' (LdapServerGroups_ServerType) parameter in the LDAP Server Groups table provides an additional optional value—Management Service (2)—for configuring the LDAP Server Group for LDAP management services.

Applicable Applications: All.

Applicable Products: All.

2.17.1.8 Ping by Hostname

This feature provides support to ping a destination by hostname. Up until now, the device could only ping a destination by IP address. The feature is supported by the existing CLI command, **ping**. For example:

```
ping corp.abc.com source voip interface vlan 1
```

Applicable Applications: All.

Applicable Products: All.

2.17.1.9 User Account Registration Based on IP Group Connectivity Status

This feature provides support for enabling the device to forward register requests from a SIP entity (Served IP Group) to a SIP registrar (Serving IP Group) only if the Served IP Group is online. The IP Group's connectivity status is determined by the keep-alive mechanism of its associated Proxy Set. The feature is applicable only to Accounts where registration is initiated by the device (i.e., 'Register' parameter is set to any value other than **No**), configured in the Accounts table.

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

- Web: 'Register by Served IP Group Status'
- CLI: reg-by-served-ipg-status
- ini: Account_RegByServedIPG

When configured to **Register Only if Online** [1], the device performs registration depending on the connectivity status of the Served IP Group. It sends a registration request to the Serving IP Group only if the Served IP Group is online. In addition, if the Served IP Group was registered but then later goes offline, the device unregisters it. If it becomes online again, the device re-registers it.

By default (**Register always** [0]), the registration by the device does not depend on the status of the Served IP Group.

Applicable Applications: SBC.

Applicable Products: All.

2.17.1.10 Enhanced Behavior for Account Registration

This feature provides enhanced support for user registration and authentication, whereby the device uses the username and password configured in the IP Groups table for the Serving IP Group (registrar server) for user registration and authentication, in the following scenarios:

- If there is no Account configured for the Served IP Group and Serving IP Group in the Accounts table.
- If there is an Account configured for the Served IP Group and Serving IP Group in the Accounts table, but without a username and password.

For this mode of operation, the 'Authentication Mode' parameter in the IP Groups table for the Serving IP Group must be configured to **SBC As Client**.

Applicable Applications: SBC.

Applicable Products: All.

2.17.1.11 Dynamic SIP UDP Port Assignment for Registration Accounts

This feature provides support for enabling the device to dynamically allocate local SIP UDP ports to Accounts on the interface facing the Serving IP Group (i.e., registrar server). Each Account is allocated a unique port taken from a port range configured for the SIP Interface (existing 'Additional UDP Ports' parameter - SIPInterface_AdditionalUDPPorts) associated with the Proxy Set of the Accounts' Serving IP Group. This feature is applicable only to Accounts where the device initiates registration (i.e., the 'Register' parameter is set to any value other than **No**).

Up until now (and still supported if this feature is disabled), the device used the same local UDP port for all Accounts communicating with the same Serving IP Group.

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

- Web: 'UDP Port Assignment'
- CLI: udp-port-assignment
- ini: Account_UDPPortAssignment

Applicable Applications: SBC.

Applicable Products: All.

2.17.1.12 Parameter Name Change for 'Transcoding Mode'

The Web interface's parameter 'Transcoding Mode' (IpProfile_TranscodingMode) has been renamed 'Mediation Mode', It’s optional values have also been renamed as follows:

- **Only if Required** -- to **RTP Mediation**
- **Force** -- to **Force Transcoding**
- **RTP Forwarding** (new)

Applicable Applications: SBC.

Applicable Products: All.

2.17.1.13 IP Group Parameter Representation in Message Manipulation

This feature provides the following enhanced support for IP Group representation in SIP message manipulation rules:

- Up until now, the manipulation syntax only allowed the administrator to specify the source or destination IP Group (e.g., *param.ipg.src.4*). This new feature allows the administrator to specify any IP Group regardless of the call’s source and destination IP Group:
    - *param.ipg.<ID>*

      An example of the syntax *param.ipg.<ID>.host*:

      ```
      param.ipg.5.host
      ```

- *param.ipg.<Name>*

  An example of the syntax *param.ipg.<Name>.host*:

  ```
  param.ipg.ITSP-WORLD.host
  ```

This syntax is applicable to all configuration tables that can be configured or associated with manipulation syntax (e.g., Call Setup Rules and Message Conditions tables).

Note: The IP Group name is case-sensitive and cannot contain spaces or dots (.).

- A new manipulation syntax element, "is-alive" represents the IP Group's connectivity status - online or offline (typically used when the associated Proxy Set is configured with keep-alive functionality):
  - param.ipg.<ID>|<Name>.is-alive
  - param.ipg.src|dst.is-alive

  The "is-alive" parameter uses the keywords "true" and "false" to indicate whether the specified IP Group is online or offline, respectively. For example:

  ```
  param.ipg.4.is-alive == 'true'
  param.ipg.4.is-alive == 'false'
  param.ipg.ITSP-WORLD.is-alive == 'true'
  param.ipg.ITSP-WORLD.is-alive == 'false'
  ```

  Note: The 'true' and 'false' keywords are case-sensitive.

  An example would be to use this manipulation syntax as a condition for a routing rule, where the status of an IP Group (instead of the destination IP Group) is checked. If the IP Group is online, then apply the routing rule. If the IP Group is offline, then route the call to an alternative destination. For an example, refer to the *SIP Message Manipulation Reference Guide*.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.17.1.14 Enhanced Message Manipulation Syntax for User-to-User Header

This feature provides support for referring to parameters (known or unknown) in the User-to-User (or X-User-to-User) SIP header. This is supported by the following syntax:

```
header.user-to-user.param
```

For example, the following syntax adds the parameter "purpose" with value "isdn-network" to the User-to-User header:

Action Subject	Action Type	Action Value
header.user-to-user.param.purpose	Add	'isdn-network'

Applicable Applications: All.

Applicable Products: All.

2.17.1.15 Enabling Global Session ID through REST API

This feature provides support for a REST client to enable the global session ID through AudioCodes REST API (GET and PUT actions). Up until now, the global session ID could only be configured through ini file (SendAcSessionIDHeader parameter). When enabled, the global session ID is included in SIP messages in the AudioCodes proprietary SIP header, AC-Session-ID. It is a unique identifier of the call session and is maintained even if the SIP dialog traverses multiple devices. This is useful for keeping track of a specific call

The feature is supported by the following new REST URL path:

```
/api/v1/rmConfig/globals/sendAcSessionIDHeader
```

The possible values are "yes" (enable) and "no". For more information, refer to the document, *REST API for Mediant Devices*.

Applicable Applications: All.

Applicable Products: All.

2.17.1.16 Web Interface Updated with New AudioCodes Corporate Logo

The device's Web interface has been updated with AudioCodes' new corporate logo. This includes the logo that appears on the Web Login screen and the main menu bar. The Web browser's favicon has also been updated with the new logo.

Applicable Applications: All.

Applicable Products: All.

2.17.1.17 Customization of Web Browser's Tab Label

This feature provides support for customizing (private labeling) the label that appears on the tab of the Web browser used to open the device's Web interface. The default label is "AudioCodes", which can either be replaced by different text or with the device's IP address. Up until now, the tab displayed "AudioCodes" and couldn't be customized.

Applicable Applications: All.

Applicable Products: All.

2.17.1.18 Invalid RTCP Packet Handling

This feature provides support for configuring the device's handling of invalid incoming RTCP packets. Up until now, the device supported configuration of invalid incoming RTP packet handling. The parameter used for RTP invalid packet handling now also applies to RTCP invalid packet handling (i.e., RTPFWInvalidPacketHandling).

Applicable Applications: All.

Applicable Products: All.

2.17.1.19 OVR Support on Mediant VE SBC

This feature provides support for the One-Voice Resiliency (OVR) application on the Mediant VE SBC and supports up to 2,000 users.

Applicable Applications: OVR.

Applicable Products: Mediant VE SBC.

2.17.2 Known Constraints

This section lists known constraints.

Table 2-23: Known Constraints in Version 7.20A.158.009

Incident	Description
149163	When configuring an SBC routing rule in the IP-to-IP Routing table and the 'Destination Type' parameter is configured to either Dest Address, Request URI, ENUM, Dial Plan, or LDAP, a destination IP Group must be specified in the 'Destination IP Group' parameter. The destination IP Group is not used for the actual destination (i.e., associated Proxy Set), but its associated configuration elements are used such as the IP Profile. If not specified, the device uses an IP Profile and other elements according to its own logical processes. **Applicable Products:** All.

150025	When upgrading the Mediant 9000 or Mediant VE (device) from Version 7.20A.156.41, current calls are disconnected. To avoid this, prior to starting the upgrade process, run the following CmdShell commands on the device for each MT:
	`IgnoreMtceHBTimeout <OAMP IP address of MT> 1`
	`IgnoreMtceTpncpTimeout <OAMP IP address of MT> 1`
	The IP addresses appear in the Media Transcoders table. These commands temporarily disable the MT keep-alive mechanism (until the device resets) and thus, the upgraded device won't disconnect the calls due to disconnected MTs.
	Applicable Products: Mediant 9000 with MT; Mediant VE SBC with MT.

148040	For Mediant VE SBC devices running on Microsoft Hyper-V, the device exposes the same serial number for all virtual machines, in SNMP (e.g., to OVOC). **Applicable Products:** Mediant VE SBC.

2.17.3 Resolved Constraints

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

Table 2-24: Resolved Constraints in Version 7.20A.158.009

Incident	Description
149860	DNS query results appear backward in the CLI (for example, "2.174.18.172" instead of "172.174.18.2"). **Applicable Products:** All.
149579	The NAT Traversal parameter setting to **Force NAT** does not function. In some cases, the device sends RTP to the private destination address that is identified as being behind NAT instead of waiting for the first incoming packet. As a result, the RTP is sent to the wrong destination. **Applicable Products:** SBC.
149646	An outage (device resets) is experienced for a few minutes during Hitless Software Upgrade. This occurs when the call opened on a CID which is not valid on the second device. **Applicable Products:** HA SBC.
149490	The device loses the TLS certificate when the same ini file is uploaded to the device. As a result, secured calls cannot be established. **Applicable Products:** All.

Incident	Description
149697 / 148949	When using TLS, keep-alive messages are not sent from the device to ARM and there is a loss of connection. **Applicable Products:** SBC with ARM.
149588	In some scenarios, the SIP Connect feature does not correctly classify users. **Applicable Products:** SBC.
149342	If an endpoint restarts (i.e., a new call ID in REGISTER messages), the device keeps sending the REGISTER to the proxy using the same call ID and CSEQ. As a result, the proxy is unaware that the endpoint restarted. **Applicable Products:** SBC.
149599	If the device is inundated by REGISTER requests that should be replied with a SIP 401, the device crashes (resets). **Applicable Products:** SBC.
149595	If the global parameter SBCDirectMedia is enabled and an UPDATE message with SDP is sent after the initial SDP offer-answer, the device crashes (resets). **Applicable Products:** SBC.
148520	The ACD (Average Call Duration) value displayed in the Web interface is incorrect. **Applicable Products:** SBC.
149545	The device crashes (and resets) in the following scenario: An SBC call is answered by a 302. The device creates a new call that is answered with a 401. The device forwards it to the calling side, which then responds with a new INVITE without credentials. **Applicable Products:** SBC.
149409	The VLAN priority of outgoing media packets are not calculated correctly. **Applicable Products:** All.
148253	Invalid characters in the 'SSH Public Key' parameter in the Local Users table causes partial Web GUI display. **Applicable Products:** All.
149073	If two call legs are WebRTC and direct media is enabled, the device sends incorrect headers. As a result, the message may fail. **Applicable Products:** SBC.
149129	If a user registers using TLS, the device uses TLS even for dialogs intended for TCP transport. As a result, the message fails. **Applicable Products:** SBC.
149395	The Dial Plan does not function correctly for prefixes with digits and letters, causing routing problems. **Applicable Products:** SBC.
149209	If an ini file with configuration of four LDAP servers (even though only two are supported) are loaded to the device, no validation is performed and after editing and applying changes, a Web error occurs. **Applicable Products:** All.
149387	For HA devices, when one device has a Product Key in the License key and the second device does not, the device erroneously issues the alarm, "FK mismatch alarm". **Applicable Products:** HA SBC.

Incident	Description
149163	IP Groups are selected according to SRD instead of SIP Interface. As a result, calls fail. **Applicable Products:** SBC.
149217	After an HA switchover, the device uses the IP Profile from the IP Group (instead of the IP Profile saved with the registered user). As a result, the incorrect IP Profile is used for the call and calls are rejected with a SIP 488. **Applicable Products:** HA SBC.
149183	If the device has to forward an INVITE that includes a very long User-To-User header, the device crashes (resets). **Applicable Products:** SBC.
149305	Media CDRs include the 'Fraction lost' value from RTCP instead of the 'Cumulative number of packets lost' **Applicable Products:** All.
148661	After an HA switchover, the SAVE button is red indicating that the user needs to perform a save (which is incorrect). **Applicable Products:** HA SBC.
146079	In certain scenarios, some buffers are lost over time, resulting in one-way voice. **Applicable Products:** SBC.
148663	The help description for the same command (idle-timeout) is not the same for Telnet and CLI. **Applicable Products:** All.
141323	A problem in initiating ports causes the flooding of error messages and as a result, the device crashes (resets). **Applicable Products:** MP-1288.
149153	If the device sends a CANCEL message to a destination to cancel a call, no SIP 487 response is received and the device erroneously performs alternative routing to the next proxy. **Applicable Products:** SBC.
149050	When the device is configured for LDAP authentication for Web-based management, LDAP users can log in, but local users cannot. **Applicable Products:** All.
148950	The device does not correctly handle incoming messages with a crypto line containing "UNENCRYPTED_SRTP UNENCRYPTED_SRTCP UNAUTHENTICATED_SRTP". As a result, calls failed. **Applicable Products:** All.
148746	The redundant device sends audit messages to Syslog. **Applicable Products:** SBC HA.
148994	If the display name in the From header includes a backslash "\", the source number is removed. **Applicable Products:** SBC.
148976	Messages are sent to the public IP address destination instead of the private address (even though Syslog erroneously indicates the private). **Applicable Products:** SBC.

Incident	Description
148441	A space in the incoming user name causes a parsing error (should be replaced with an escape character). As a result, the REGISTER fails. **Applicable Products:** Gateway.
148815	When performing CSR on incoming call, call forking does not function and calls are not routed correctly. **Applicable Products:** Gateway.
148717	The Monitor page does not display OVR calls after an HA switchover. **Applicable Products:** SBC HA with OVR.
148555	In certain scenarios, during a re-INVITE when video media is added, the device crashes (resets). **Applicable Products:** SBC.
148845	If two blanks occur in the Request-URI (between 400 and "not found"), Pre-Parsing Manipulation does not function. As a result, the message fails. **Applicable Products:** SBC.
148686	No voice for a few minutes after an HA switchover. The voice stream was opened with transcoding (DSP) and due to a bug, when channels opened with DSP, the RTP sequence jumped to the beginning after switchover. **Applicable Products:** SBC HA.
148727	IAM message for SIP-I is not parsed correctly, which causes manipulation failure. **Applicable Products:** SBC.
148174	If the SBCKEEPCONTACTUSERINREGISTER is set to 1 and the REGISTER is received from WebRTC, the device does not release resources. As a result, the device rejects the registration. **Applicable Products:** SBC with WebRTC.
147955	Under some conditions, the ini file cannot be loaded using the Automatic Update feature (IniFileURL parameter). **Applicable Products:** All.
148559	When creating PRT files, the user is unable to track the index of a tone within the file (Local Held Tone Index parameter), resulting in difficulties in playing tones. **Applicable Products:** All.
148630	Some resources are not released when the device sends multiple Call Setup Rules requests to the LDAP server which is offline. As a result, calls are dropped. **Applicable Products:** SBC.
148016	When the device receives more than four crypto suites and the supported crypto suites were indexed at greater than four, the device does not use the supported crypto. As a result, no voice is experienced. **Applicable Products:** All.
147430	Under some conditions, the device loses the DNS resolution and thus, failed to classify calls from the proxy. As a result, calls failed. **Applicable Products:** SBC.
148189	When collecting the debug file from the device, the device crashes (resets). **Applicable Products:** SBC.
148366	When the device receives a large INVITE message (greater than 4k), it fails to send the route request (getRoute) to ARM. As a result, call routing failure occurs. **Applicable Products:** SBC with ARM.

Incident	Description
146960	For CAS calls, when the destination (IP:port) changes (simultaneous ring is enabled), the device does not change the SSRC. As a result, one-way voice occurs. **Applicable Products:** CAS Gateway.
145870	CAS issues result in calls not being processed. CAS starts to work only after the trunk is stopped and then started. **Applicable Products:** CAS Gateway.
148326	When the device receives an incoming WebRTC call with the Opus coder, the device erroneously uses G.711 coder for the call. As a result, no voice occurs. **Applicable Products:** SBC with WebRTC.
148161	Static IP routes disappear from the Static Routes table after changing the Application Type from OAMP + Media + Control to OAMP only, causing routing problems. **Applicable Products:** All.
147110	Some performance monitoring calculations are incorrect. **Applicable Products:** SBC.
148276	The device rejects180 messages that have an IPv6 address enclosed by brackets in the "received" parameter of the Via header (this format contradicts the RFC). As a result, such calls fail. **Applicable Products:** SBC.
147244	During T.38 fax transmission, the device erroneously sends HA warning messages to Syslog. **Applicable Products:** HA SBC.
147244	The device fails to download ini files from the EMS. **Applicable Products:** SBC.
147483	When the License Key includes only 1 PRI trunk, it is not synchronized. As a result, Gateway calls cannot be processed. **Applicable Products:** Digital Gateway.
148130	The CLI is missing the "asserted-identity-m" command. **Applicable Products:** All.
150023	If the IP Profile parameter 'SBC Remote Update Support' is configured to 1, the fax detection feature for SBC calls does not function and as a result, faxes fail. **Applicable Products:** All.
149890	When Quality of Experience (QoE) is enabled, during the calculation of QoE, a "divide by 0" occurs, causing the device to crash (reset). **Applicable Products:** All.
150044	For the Media Transcoding Cluster (MTC) system, the MT drops the calls during a switchover. **Applicable Products:** MTC.
149837	On the Web interface's SBC CDR History page, when defining the display of more rows than the default, no scrolling option occurs and table sorting cannot be done. **Applicable Products:** All.
149536	When all CAS trunks are up and running and the Web interface's Trunks & Channels Status page is opened, the trunk becomes inactive. **Applicable Products:** CAS Gateways.

Incident	Description
149796	The device crashes (resets) when it attempts to add a new user registration to the list of IP Groups in its registration database. **Applicable Products:** All.

2.18 Patch Version 7.20A.158.012

This patch version only includes a resolved constraint.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.1079, and EMS/SEM Version 7.2.3104.

2.18.1 Resolved Constraints

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

Table 2-25: Resolved Constraints in Version 7.20A.158.012

Incident	Description
150342	If the device (SBC application) receives a SIP message that contains a character in the beginning that is not allowed, for example CRLF or space, and the device performs Pre-Parsing Manipulation, the device crashes (and resets). **Applicable Products:** All.

2.19 Patch Version 7.20A.158.035

This patch version only includes a resolved constraint.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.1083, and EMS/SEM Version 7.2.3106.

2.19.1 Resolved Constraints

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

Table 2-26: Resolved Constraints in Version 7.20A.158.035

Incident	Description
148119	Mediant VE SBC with 1 vCPU / 2-GB RAM is not supported. (Now it is.) **Applicable Products:** Mediant VE SBC.
151024	The device reports incorrect MOS values when RTCP-XR is enabled. **Applicable Products:** All.
150877	When the device does transcoding between two legs, the outgoing DTMF stream is different from the incoming DTMF stream. As a result, the user cannot join the conference. **Applicable Products:** All.
151243	INVITE dialog-initiating requests to the "sticky" proxy server do not receive any response and therefore, the server is marked as offline. This causes the Account to stop working with it and registers with another server which causes the calls to be dropped. **Applicable Products:** All.
150821	Fragmented packets are not handled correctly and as a result, large SIP messages are dropped. **Applicable Products:** All.
151164	The Account Registrar Stickiness feature does not function in HA mode (and calls are thereby dropped). **Applicable Products:** HA Devices.
151100 / 150483	When the device communicates with a user located behind NAT, after an HA switchover, the device sends the RTP to the wrong IP:port. As a result, no voice occurs. Applicable Products: HA Devices.
150970	When using the dynamic port mapping feature in CDR, the device erroneously sends the first port (i.e. incorrect CDR). **Applicable Products:** All.
149683	When communicating with a user located behind NAT and a switch to T.38 occurs, the remote user does not send T.38 packets and therefore, the device is unable to latch and send T.38 to the correct destination. As a result, fax failure occurs. **Applicable Products:** All.

Incident	Description
150937	The device incorrectly handles an invalid Application-Defined RTCP packet, which causes the device to reset. **Applicable Products:** All.
150993	When using the port per user feature and the user adds an IPv6 interface after the device powers up, after an HA switchover the device sends different ports per user. As a result, calls are dropped. **Applicable Products:** HA Devices.
151087	If the device's License Key includes a license for a small number of SIPRec sessions, the device crashes (and resets). **Applicable Products:** All.
151049	The **traceroue** CLI command does not function for IPv6. **Applicable Products:** All.
150994	Even when the SIPCHALLENGECACHINGMODE parameter is configured to 0, the device caches authentication challenges. As a result, calls fail. **Applicable Products:** All.
150872	The Dial Plan table cannot be exported from the Web interface. **Applicable Products:** All.
150981	Device crashes (resets) resulted in the device not being in HA mode. **Applicable Products:** HA Devices.

2.20 Patch Version 7.20A.158.056

This patch version only includes a resolved constraint.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.1083, and EMS/SEM Version 7.2.3106.

2.20.1 Resolved Constraints

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

Table 2-27: Resolved Constraints in Version 7.20A.158.056

Incident	Description
152322	The device resets due to the overrunning of a buffer causing a system memory leak. **Applicable Products:** SBC.
152259	The Media Transcoder (MT) displays active alarms (Ethernet link alarms) even though no SIP is configured. **Applicable Products:** Mediant 9000; Mediant SW; Media Transcoder.
152209	In some scenarios, the device sends an error message to the Syslog when object is incorrectly configured. **Applicable Products:** All.
152085	When the device is configured with an invalid Condition in the IP-to-IP Routing table, matching the incoming SIP message to this IP-to-IP Routing rule causes the device to reset. **Applicable Products:** SBC.
152069	When the time configured for the SBCPROXYREGISTRATIONTIME parameter expires and the device sends the user's REGISTER to the server, the server replies with a SIP 401. However, after a few seconds, the device stops tracking the refresh failure and if a subsequent REGISTER is received, the device handles it as if the previous REGISTER succeeded and terminates it. As a result, the user does not get registered with the server. **Applicable Products:** SBC.
151953	When the device processes a large INVITE message and the buffer is full, if an alternative route is located for this INVITE, the buffer overruns and after several repeats, the device crashes (resets). **Applicable Products:** SBC.
151943	When processing the application/BroadsoftDocument+xml XML body that has an alias whose length is 37 characters, a memory corruption occurs due to unsafe copying. After some repeats of this corruption, the device crashes (resets). **Applicable Products:** SBC.
151694	When the device sends a SUBSCRIBE with the base UDP port instead of the configured UDP port (configured in the SIP Interfaces table's 'Additional UDP Ports' parameter), the SUBSCRIBE is denied by the server (403 Forbidden response). **Applicable Products:** SBC.

Incident	Description
151616	Message manipulation cannot not be done on SIP Authentication headers. As a result, authentication fails. **Applicable Products:** SBC.
150995	The connection between the PuTTY client and the device is terminated abnormally, causing the login resource to not be deallocated. As a result, access to the device's management interfaces (Web and CLI) is blocked. **Applicable Products:** SBC.
152028	When the device has no available SIP Socket resources (due to incorrect configuration which has exceeded the recommended), the device crashes (resets). **Applicable Products:** SBC.

2.21 Patch Version 7.20A.162.001

This patch version only includes a resolved constraint.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.2101, and EMS/SEM Version 7.2.3106.

2.21.1 New Features

2.21.1.1 New Mediant 9000 Hardware Revision

A new hardware revision—Rev. B--has been released for Mediant 9000 SBC. This new hardware includes the following main features:

- Latest (Gen10) server architecture
- Upgrade of the Integrated Lights Out (iLO) module to iLO 5, including advanced features

Note: For High-Availability (HA) systems, the participating HA pairs (active and redundant units) must be of the same hardware revision.

Applicable Applications: All.

Applicable Products: Mediant 9000.

2.21.2 Known Constraints

This section lists known constraints.

Table 2-28: Known Constraints in Version 7.20A.162.001

Incident	Description
-	This software version is applicable only to Mediant 9000 Rev. B. Earlier hardware revisions should not upgrade to this version. **Applicable Products:** Mediant 9000
-	Media Transcoding Cluster feature is not supported in this release. **Applicable Products:** Mediant 9000; Mediant VE; Media Transcoder (MT).

2.22 Patch Version 7.20A.162.017

This patch version includes only resolved constraints.

Note: This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.3082 and EMS/SEM Version 7.2.3106.

2.22.1 Resolved Constraints

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

Table 2-29: Resolved Constraints in Version 7.20A.162.017

Incident	Description
152162	The device sends a CDR with transport type "unknown" for an SBC call when the device undergoes an HA switchover during the call and the call disconnects when the redundant device becomes active. **Applicable Products:** HA Devices.
152508	When port redundancy occurs for the Media Transcoder (Media Transcoding Cluster feature), the Media Transcoder resets itself. **Applicable Products:** Mediant 4000.
151612	CDR files that are generated by the device for SBC calls have the incorrect size and time (not as configured). **Applicable Products:** All.
150867	For the Media Transcoding Cluster feature, a memory overrun in the Media Transcoder (MT) causes it to crash (reset). **Applicable Products:** Mediant 4000.

2.23 Patch Version 7.20A.200.019

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

> **Note:** This patch version is compatible with AudioCodes One Voice Operations Center Version 7.4.2094, and EMS/SEM Version 7.2.3106.

2.23.1 New Features

New features introduced in this version include the following:

2.23.1.1 Entity Names Added to SNMP Alarm Descriptions

Names of configuration entities are now included in SNMP alarm descriptions. Entity names such as Proxy Set, IP Group, SIP Interface, and SRD now appear in the alarm descriptions. Previously, alarm descriptions only included the entity's table row index (ID), for example: "Proxy Set Alarm Proxy Set 37: Proxy lost. looking for another proxy". Now, the Proxy Set name is also included and shown in parenthesis, for example, "Proxy Set Alarm Proxy Set 37 (ITSP): Proxy lost. looking for another proxy".

Applicable Applications: All.

Applicable Products: All

2.23.1.2 Performance Monitoring Thresholds Included in ini File

The downloaded ini file now includes SNMP performance monitoring MIBs whose thresholds (low and/or high) have been changed from default values. The ini file displays the performance monitoring MIB with the modified low and high threshold values. This feature can be useful for applying the same thresholds to other devices (by simply loading the same ini file to them).

Applicable Applications: All.

Applicable Products: All

2.23.1.3 Proxy Set Name in Proxy Set Status Display

The name of the Proxy Set is now displayed in the Web interface's Proxy Sets Status table (Monitor menu > Monitor tab > VoIP Status folder > Proxy Sets Status), in a new column called 'Name'. The Proxy Set name also appears in the output of the CLI command, `show voip proxy sets status`.

Applicable Applications: All.

Applicable Products: All

2.23.1.4 Restoring Defaults while Preserving Network Settings in CLI

This feature provides support for restoring the device to factory defaults while preserving network settings, through CLI. Preserving network settings ensures connectivity to the device's management interfaces using the same OAMP IP address after the device has been restored to defaults. Up until now, this option was supported only through the device's Web interface. To support this feature, the following new CLI command has been added:

```
# write factory keep-network-and-users-configuration
```

Applicable Applications: All.

Applicable Products: All.

2.23.1.5 Tail Filter for CLI Command Output

All CLI command outputs can now be filtered to display a user-defined number of lines from the end (*tail*) of the output. To support this feature, the following new command syntax needs to be added to the command to which the filter is applied:

```
<command> | tail <number of lines (1-1000) to display>
```

Below shows an example where the last two log messages (lines) in the output of the show system log command are displayed:

```
# show system log | tail 2
Jan  3 00:35:54 local0.warn [S=147146] [BID=5b1035:250]  SNMP
Authentication Failure - source: IP = 172.17.118.219, Port = 1161,
failed community string = public.
Jan  3 00:35:55 local0.notice [S=147147] [SID=5b1035:250:36462]  (
sip_stack)(     84788)   AcSIPDialog(#170)::TransactionFail -
ClientTransaction(#175) failed sending message with CSeq 1
OPTIONS, the cause is Transport Error
```

Note that the existing **show system log tail** command has now been replaced with **show system log | tail**.

Applicable Applications: All.

Applicable Products: All.

2.23.1.6 Enhanced SBC User Registration Request Handling

The device now provides enhanced handling of the 'expires' parameter of the SIP Contact header, for REGISTER requests that are received from User-type IP Groups:

- If the Contact header in the incoming REGISTER request contains the 'expires' parameter, the device now forwards the request with the parameter (if the destination is a Server-type IP Group). Up until now, the device removed the parameter (sending only the Expires header).
- The device now always adds the ‘expires’ parameter to the Contact header in the SIP response (200 OK) that it sends to the user. Up until now, the device removed the parameter if it existed. Both the Expires header and the Contact 'expires' parameter are sent to the user with the same value.

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.7 Enabling SBC and CRP Applications Removed from Web Interface

Enabling the SBC or CRP application through the Web interface has been removed as these applications are determined by the installed License Key. The SBC application is enabled if at least one SBC-related feature (for example, "SBC Signaling Sessions") is defined in the License Key. The CRP application is enabled if the License Key includes the "CRP" license.

As such, the Applications Enabling page (Setup menu > Signaling & Media tab > Core Entities folder > Applications Enabling) has been removed from the Web GUI. However, the administrator can disable the SBC application (for whatever reason) through CLI and ini file.

Applicable Applications: All.

Applicable Products: All.

2.23.1.8 Faster Upload of CMP Software File

The device's internal processing capabilities have been improved to make software file (.cmp) upload much faster.

Applicable Applications: All.

Applicable Products: All.

2.23.1.9 Enhanced File Management through REST API

The following file management support through AudioCodes REST API (GET, PUT and POST actions) has been added:

- Configuration Package file:
  `api/v1/files/configurationPackage`
- SBC Wizard Template Package file:
  `api/v1/files/sbcWizard`

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

Note: The following REST API URL paths have been removed: api/v1/files/voicePrompts and api/v1/files/coderTable.

Applicable Applications: All.

Applicable Products: All.

2.23.1.10 New Alarm for Ethernet Group Down of HA Maintenance Interface

A new SNMP alarm, acHAEthernetGroupAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.137) has been added. This alarm is sent when the Ethernet link of at least one of the ports in the Ethernet Group that is associated with the HA Maintenance interface is down.

Applicable Applications: All.

Applicable Products: Mediant 500 Gateway & E-SBC; Mediant 800 Gateway & E-SBC; Mediant 2600 E-SBC; Mediant 4000 SBC; Mediant 9000 SBC; Mediant VE/SE.

2.23.1.11 Subject Alternative Name (SAN) Field for TLS Certificates

Subject Alternative Name (SAN) fields can now be configured when creating certificate signing requests (CSR) and self-signed certificates. The SAN field is an X.509 Version 3 extension providing additional information (multiple subject names) for identifying the device, which can be an e-mail address, DNS hostname, URI, or IP address. Up to five SAN fields can be configured per certificate.

The following configuration parameters have been added for this feature:

- Web Interface: '1st-5th Subject Alternative Name [SAN]' fields on the Change Certificates page (Setup menu > IP Network tab > Security folder > TLS Contexts > Change Certificate link)
- CLI: configure network > tls > certificate alternative-name-add {dns|email|ip-addr|uri}

Applicable Applications: All.

Applicable Products: All.

2.23.1.12 Fullband Coder for SDP Telephone-Event

The device now provides enhanced support for displaying the DTMF sampling rate of the voice coder in the "a=rtpmap" field for the 'telephone-event' in SDP, using the RFC 2833 method. The following DTMF sampling rates can now be displayed: 8,000 kHz (narrowband coders), 16,000 kHz (wideband coders) and 48,000 kHz (fullband coders). Up until now the "a=rtpmap" field only displayed 8,000 kHz.

Note that the feature requires DSP resources (for detection and generation of RFC 2833).

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.13 NGINX for HTTP Proxy Server Configuration

This feature integrates the NGINX (pronounced *engine x*) platform on the device. NGINX is a widely used open source HTTP proxy server with enhanced functionality and customization capabilities. This mechanism replaces the previously supported HTTP proxy server configuration.

The following new SNMP alarms related to NGINX configuration have been introduced:

- acNGINXConfigurationIsInvalidAlarm
- acNGINXPprocessIsNotRunningAlarm

The HTTP Proxy configuration tables have also been changed to enhance HTTP Proxy configuration.

The following new CLI commands related to

- To send the NGINX configuration files to a remote destination:

  ```
  # copy nginx-conf-files to
  <Protocol>://<Address>/<filename>.tar
  ```

- To view the NGINX configuration files:

  ```
  show network http-proxy conf active|errors|new
  ```

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.14 Default DNS Servers

The device is now configured with default DNS server addresses (primary and secondary), which can be modified. This ensures that applications that may require DNS lookups run seamlessly when DNS servers have not been configured in the Internal DNS table and IP Interfaces table (i.e., last resort). Currently, the default DNS servers are used only for certain applications – Auto-Update mechanism (for loading files through SNMP and CLI copy), pinging remote hosts (CLI ping command), and the updating SBC Configuration Wizard template.

The following configuration parameters have been added for this feature:

- Web Interface: New DNS Settings page (Setup menu > IP Network tab > DNS folder > DNS Settings) - 'Default Primary DNS Server IP' (default 8.8.8.8) and 'Default Secondary DNS Server IP' (default 8.8.4.4)
- ini parameters: DefaultPrimaryDnsServerIp and DefaultSecondaryDnsServerIp
- CLI: (configure network > dns settings > dns-default-primary-server-ip / dns-default-secondary-server-ip

Applicable Applications: All.

Applicable Products: All.

2.23.1.15 Music-on-Hold from External Audio Streamer via FXS Gateway

The device's Gateway application now supports playing music-on-hold (MoH) whose source is from an external, third-party media player. The device can then play this media to any external IP system (for example, a softswitch, media gateway or SBC) or use it for calls that it processes (only SBC application). Thus, the device functions like an IP media server, except that the original source of the media is from an external player.

The external media source is connected to the device's FXS port through a telephone adapter (for FXS emulation). The FXS port is always in off-hook state, continuously receiving media (for example, music or advertisements) from the external media source. Up to two FXS ports can be used for this feature, where each port can play the media to up to 20 concurrent call sessions. In addition, each FXS port can be dedicated for a different purpose, for example, one port can play MoH to normal users while the other port can play MoH to contact centers.

The feature is enabled by configuring the existing parameter 'IP2Tel CutThrough Call Behavior' parameter (TelProfile_IP2TelCutThroughCallBehavior) to the new optional value, **CutThrough+Streaming** (3). The maximum number of concurrent calls that can be established for this MoH feature (for all FXS ports) is configured by the new parameter, MaxStreamingCalls (gw-analog-fxs > max-streaming-calls).

Applicable Applications: Gateway (FXS).

Applicable Products: MP-1288, Mediant 5xx; Mediant 8xx; Mediant 1000.

2.23.1.16 Music-on-Hold from External Audio Streamer for SBC Calls

The device can now play Music on Hold (MoH) from an external IP-based media (audio) source (streamer) for SBC calls that have been placed on hold. Up until now, the device could only be configured to play the local default hold tone or a tone defined in an installed PRT file.

Only one external media source can be configured for MoH. The device can play MoH from the external streamer to up to 20 concurrent call sessions (on-hold parties).

The feature is configured using the following new parameters/options:

- New table parameter: External Media Source table (ExternalMediaSource) – specifies the IP Group of the external media source
- New optional value, **External** for the 'Play Held Tone' (IpProfile_SBCPlayHeldTone) parameter. The existing optional value **Yes** has been renamed **Internal** (to play hold tone from PRT or default)

The feature supports HA switchover, whereby the device continues playing MoH to the calls that were placed on hold before the switchover.

Applicable Applications: SBC.

Applicable Products: MP-1288; Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.

2.23.1.17 Dial Plans for Routing Gateway Calls

Dial plans (and their tags) can now be used in the routing mechanism for Gateway calls (Tel-to-IP and IP-to-Tel). The Dial Plans are used as input criteria for locating a matching routing rule.

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

- 'Tel-to-IP Dial Plan Name' (Tel2IPDialPlanName) - global parameter that selects the Dial Plan for Tel-to-IP routing
- 'IP-to-Tel Dial Plan Name' (IP2TelDialPlanName) - global parameter that selects the Dial Plan for IP-to-Tel routing
- 'Source Tag' (PstnPrefix_SrcTags) and Destination Tag (PstnPrefix_DestTags) – selects the Dial Plan tag for a specific IP-to-Tel routing rule
- 'Source Tag' (Prefix_SrcTags) and Destination Tag (Prefix_DestTags) – selects Dial Plan tags for a Tel-to-IP routing rule

Applicable Applications: Gateway.

Applicable Products: MP-1288; Mediant 5xx; Mediant 8xx; Mediant 1000.

2.23.1.18 Enhanced Packet Loss Concealment

The device now supports packet loss concealment (PLC) for SBC legs using voice coder G.711 with 20-msec packet interval. This technique is used to mask the effects of lost or discarded packets. Therefore, enabling PLC may enhance the device's Quality of Experience (QoE) capabilities by improving MOS scores when packet loss rate is less than 10.

To enable PLC, the following parameter has been added to the IP Profile table:

- CLI: configure voip > coders-and-profiles ip-profile > sbc-enhanced-plc
- ini File: IpProfile_SBCEnhancedPlc
- Web: Enhanced PLC

Note that this feature requires DSP resources.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant SW.

2.23.1.19 SBC User Info Table Activation Changes

The maximum number of allowed rows in the SBC User Info table is according to the number of far-end users that is defined in the device's License Key ("Far End Users (FEU)"). However, as each product supports a maximum number of rows software-wise, the licensed FEU cannot exceed this. For example, if the licensed FEU is 20 and the maximum number of supported rows by the device is 10, the maximum rows will be 10. If the FEU is 5, then the maximum number of rows will be 5.

For the table to be supported, the EnableUserInfoUsage parameter must be enabled and the FEU in the License Key must have a value greater than 0. This also applies to LAD and OVR applications.

Note that the FEU license also refers to the number of allowed registered users (however, this cannot exceed the device’s inherent maximum number of supported registered users).

Applicable Applications: All.

Applicable Products: All.

2.23.1.20 Enhanced User Info File Handling

The following enhancements were made to the User Info functionality:

- The SBC User Info table now supports up to 20,000 users (previously, it was up to 3,000). This applies only to Mediant 2600, Mediant 4000, Mediant 9000 and Mediant SW products providing 8-GB RAM or more
- User Information files can now be imported and exported as .csv files, in the SBC User Info table and Gateway User Info table. This is done using the following new configuration updates:
    - Web Interface: New Import and Export commands in the existing Action drop-down list located on the toolbar of these tables.
    - CLI (under configure voip > sip-definition proxy-and-registration):
        - user-info gw-user-info|sbc-user-info export-csv-to <URL>
        - user-info gw-user-info|sbc-user-info import-csv-from <URL>
        - New commands for the Auto-Update mechanism – configure system > automatic-update > gw-user-info | sbc-user-info
    - ini File: SBCUserInfoFileUrl and GWUserInfoFileUrl

  Previously, these files could only be imported (loaded) to the device (as auxiliary files using the Auxiliary Files page). As loading the files using the Auxiliary File page is being phased out, it is recommended to import the tables using the new method.

Applicable Applications: All.

Applicable Products: All.

2.23.1.21 Dial Plan and User Info Table Parameters Exposed in ini File

The following tables are now exposed (previously were hidden) in downloaded ini configuration files as well as in the output of the show running-config CLI command:

- DialPlanRule
- SBCUserInfoTable
- GWUserInfoTable

Applicable Applications: All.

Applicable Products: All.

2.23.1.22 Call Preemption for Emergency Calls by Routing Server

The REST API now supports obtaining (GET) and configuring (PUT) the 'SBC Preemption Mode' (SBCPreemptionMode) parameter for SBC calls, and the ‘Call Priority Mode’ (CallPriorityMode) parameter for Gateway calls.

This feature provides support for implementing call preemption for emergency calls (such as 911) by the routing server (for example, AudioCodes ARM). If the device is enabled for call preemption for emergency calls (SBC and/or Gateway), the routing server determines whether the incoming call is an emergency call or not and if so, handles the routing decision accordingly (i.e., preempts a non-emergency call if the maximum call capacity of the device is reached to allow the emergency call to be routed).

The REST API URL resource */api/v1/rmConfig/globals* now includes the new parameters "preemptionmode" (enables call preemption for SBC) and "callprioritymode" (enables call preemption for Gateway):

```
<OAMP IP>/api/v1/rmConfig/globals/preemptionMode
<OAMP IP>/api/v1/rmConfig/globals/callPriorityMode
```

Applicable Applications: SBC; Gateway (IP-to-Tel).

Applicable Products: Mediant 500; Mediant 500L; Mediant 800; Mediant 1000B; Mediant 4000; Mediant 9000; Mediant VE/SE.

2.23.1.23 ENUM Query Enhancement for Call Setup Rules

This feature provides enhanced keyword support for using the results of ENUM queries in Call Setup rules ('Query Target' parameter configured to **ENUM**). Up until now, only the 'enum.result.url' keyword could be used in the Action and Subject fields. Now, the ENUM result can be drilled down to specific parts of the URL using the syntax *enum.result.url.<x>*, where *x* can be 'user', 'host', 'type', 'mhost', 'userphone', 'looseroute', 'bnce', 'cause', 'user', 'transport-type', 'ac-int', and 'param' (for example, enum.result.url.user).

Applicable Applications: SBC and Gateway.

Applicable Products: All.

2.23.1.24 Enhanced Call Admission Control

Call admission control (CAC) configuration has undergone the following enhancements:

- The Admission Control table has been renamed and changed to a parent-child table structure to allow the configuration of CAC profiles, where each profile can have multiple CAC rules:
  - Call Admission Control Profile table (SBCAdmissionProfile) - defines a CAC profile name
  - Call Admission Control Rule table (SBCAdmissionRule) - defines multiple CAC rules per profile
- CAC rules (profiles) are now assigned to IP Groups, SRDs and SIP Interfaces in their respective tables, using a new table parameter "CAC Profile". Previously, these SIP entities were assigned to the CAC rule within the former Admission Control table.
- CAC rules can now be configured (rate and max. burst) per user, which limits the number of calls made per user.

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.25 IDS Blacklist Display in Web Interface

Remote hosts that are currently blacklisted (considered malicious) by the device's Intrusion Detection System (IDS) feature are now displayed in the Web interface. Up until now, this was supported only through CLI (show voip ids blacklist active).

This new feature is supported by the new read-only Web page, IDS Active Black List (Monitor menu > Monitor tab > Network Status folder > IDS Active Black List).

In addition, a new CLI command has been added to remove entries from the IDS Active Black List table:

```
# clear voip ids blacklist {all|<Removal Key>}
```

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.26 Improved IDS SNMP Alarm Descriptions

IDS SNMP alarms now include a more detailed description of the reason why the alarm was raised.

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.27 High-Availability for AWS Environments

High-Availability is now supported when the device operates in AWS environment. Previously, it could only be in standalone.

AWS automatic NAT Elastic IP Addresses configuration is now supported.

Applicable Applications: SBC.

Applicable Products: Mediant VE.

2.23.1.28 Initial HA Configuration from Single INI File

Quick-and-easy initial HA setup is now supported, by loading the same configuration (.ini) file with special configuration to both standalone devices. The active (local) and standby (remote) devices are identified by MAC address. The feature is also useful for HA backup configuration. Once HA is up and running, a backup of the ini file from the active device can be done and when HA failure occurs (for whatever reason), the file can be re-loaded to the devices to restore HA.

The following new ini file parameters configure this feature:

- First device:
  - HALocalMAC - MAC of device
- Second device:
  - HARemoteMAC - MAC of device
  - HARemoteUnitIdName –name of device
  - HARemotePriority – preempt mode

Applicable Applications: All.

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

2.23.1.29 Changes in Offline HA Parameters

The following parameters no longer require a device reset for their settings to take effect:

- 'Preempt Priority' (HAPriority)
- 'Redundant Preempt Priority' (HARemotePriority)
- 'Preempt Mode' (HARevertiveEnabled)

Applicable Applications: All.

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

2.23.1.30 Packaged Configuration File Load and Save

A single packaged file containing multiple configuration-related files can now be loaded to or saved from the device. The packaged file is a TAR (Tape ARchive) file (.tar) compressed with gzip. The feature can be used for backing up full configuration and then restoring it to the device in case of device configuration failure (for whatever reason), or for loading the backed-up configuration file to other devices requiring similar configuration.

The packaged file can include the following files:

- ini.ini (ini configuration file)
- LOGO.dat (image file used as the logo in the Web interface)
- FAVICON.dat (favicon file used for Web browsers)
- CPT.dat (Call Progress Tone file) - present only if a CPT file was previously loaded to the device
- PRT.dat (Pre-recorded Tone file) - present only if a PRT file was previously loaded to the device
- AMD.dat (Answer Machine Detection file) - present only if a CPT file was previously loaded to the device
- SBC_Wizard.dat (SBC Configuration Wizard template file)
- CAS_<ID>.dat (CAS file) - present only if a CAS file was previously loaded to the device
- DPLN.dat (Dial Plan file) - only for backward compatibility of previous versions that supported a Dial Plan file; for current versions, the Dial Plan is included in the ini file
- Certificate files (<ctx_id>.crt, <ctx_id>.root, <ctx_id>.pkey)
- DialPlanRule.csv (Dial Plan file) - present only if the device was configured with Dial Plan rules
- CSV files (for example, for Dial Plans and User Info)

This feature can be done through the following management interfaces:

- SFTP: The packaged configuration file (configuration-package.tar.gz) can be downloaded (Get) from the device through SFTP. The file is located in the device's root (/) directory. The SFTP client needs to authenticate itself with the SFTP server (i.e., the device). Access is granted only to users with Security Administrator level.
- Web interface: Existing Configuration Files page, using the new **Save Configuration Package** and **Load Configuration Package** buttons
- CLI: The following new command has been added to the copy command:

```
# copy configuration-pkg from|to <URL>
```

- Ini File: ConfPackageURL

The packaged file is saved with the filename "ConfBackupPkg<Serial Number>.tar.gz". After loading a package file, the device automatically resets with a save to flash.

Note:

- Software file (.cmp) is not supported.
- CAS files cannot be replaced when there are active calls; all trunks must be stopped before CAS files can be replaced.

Applicable Applications: All.

Applicable Products: All.

2.23.1.31 Voltage Configuration for FXS MWI and Phone Lamp

The voltage level mode (low or high) that the FXS port generates to a connected phone for lighting the phone's lamp (LED or NEON type) used for indicating a message in waiting (MWI) can now be configured. This is supported by the following new parameters:

- EnableLowVoltageMwiGeneration
- LedMwiOnDurationTime
- LedMwiOffDurationTime
- NeonMwiOnDurationTime
- NeonMwiOffDurationTime

Applicable Applications: Gateway (FXS).

Applicable Products: MP-1288.

2.23.1.32 Auto-Completion for Message Syntax

Auto-completion for parameters whose values are configured using special syntax is now supported in the Web interface. For these parameters, an Editor button is displayed alongside their fields, which when clicked, opens a syntax editor. As text is typed in the field, the user is prompted with optional syntax.

The feature is supported in the following configuration tables:

- Malicious Signature ('Pattern' field)
- Call Setup Rules ('Search Key', ' Condition', 'Action Subject' and 'Action Value' fields)
- Message Manipulations ('Message Type', 'Condition', 'Action Subject' and 'Action Value' fields)
- IP-to-IP Routing ('Internal Action' field)
- Message Conditions ('Condition' field)
- Pre-Parsing Manipulation Sets ('Message Type' and 'Replace-With' fields)

Applicable Applications: All.

Applicable Products: All.

2.23.1.33 Select All Check Box for Selecting All Activity Types to Report

A 'Select All' check box has been added under the Activity Types to Report group on the Web interface's Syslog Settings page (Troubleshoot menu > Troubleshoot tab > Logging folder > Syslog Settings). This enables the administrator to select (or deselect) all activity types with one click.

Applicable Applications: All.

Applicable Products: All.

2.23.1.34 SSH Server Enabled by Default

The device's embedded SSH server is now enabled by default. It can be disabled using the existing parameter 'Enable SSH Server' (SSHServerEnable).

Applicable Applications: All.

Applicable Products: All.

2.23.1.35 TDM-to-SBC License Displayed in Management Interfaces

The TDM-to-SBC license is now shown in the License Key that is displayed in the management interfaces (for example, Web interface's License Key page). It is displayed on two lines – one showing the number of SBC sessions that can currently be derived from Gateway resources ("TDM-to-SBC Sessions") and one showing whether the feature is licensed ("TDM-to-SBC").

Applicable Applications: All.

Applicable Products: All.

2.23.1.36 License Key Mode Indication

The Web interface now displays the type of License Key installed on the device (locally installed, obtained from the OVOC license pool, or Floating License). This is displayed in the new 'Mode' field on the License Key page.

Applicable Applications: All.

Applicable Products: All.

2.23.1.37 Core Allocation Optimization for Services

The device's CPU cores usage can be optimized for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile –improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile –improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

Once a profile is selected, the device optimizes cores allocation to achieve maximum performance according to the selected profile. For example, if the deployment involves mainly SRTP sessions (and doesn’t require DSP-required features), it is recommended to optimize core allocation for SRTP.

Configuration is done by the new parameter, SBC Performance Profile (SbcPerformanceProfile).

Note:

From Version 7.2.202, when using any transcoding/DSP functionality, the device must be configured to use the "Optimized-for-Transcoding" profile, using the SBCPerformanceProfile parameter.

The parameter's value is not automatically set in all upgrade scenarios. If you are upgrading from a version earlier than 7.2.158 and employing transcoding/DSP capabilities, to preserve your transcoding/DSP functionality it is essential that you first upgrade the device to Version 7.2.158 before upgrading it to Version 7.2.2xx.

Once the device has been upgraded to Version 7.2.2xx, verify that the device is set to use the "Optimized-for-Transcoding" profile, using any of the following management platforms:

- ini file: SBCPerformanceProfile = **2**
- CLI: configure system > sbc-performance-settings > sbc-performance-profile **optimized-for-transcoding**
- Web: 'SBC Performance Profile' =**Optimized-for-Transcoding** (SBC General Settings page - Setup menu > Signaling & Media tab > SBC folder > SBC General Settings).

If the device is not set to use the "Optimized-for-Transcoding" profile, then configure it as described above. Note that if you do need to configure it, then save the new configuration with a device reset for the parameter to take effect.

Note:

From Version 7.2.202, when upgrading the License Key to enable any DSP functionality (including transcoding), the SBCPerformanceProfile parameter must be configured to the Optimized-for-Transcoding profile, as the **parameter's value is not automatically set after installing such a License Key. If not configured, DSP functionality will remain disabled.**

Therefore, to ensure DSP functionality, load the new License Key **without resetting** the device, and then verify that the device is configured to the Optimized-for-Transcoding profile, using any of the following management platforms:

- ini file: SBCPerformanceProfile = **2**
- CLI: configure system > sbc-performance-settings > sbc-performance-profile **optimized-for-transcoding**
- Web: 'SBC Performance Profile' = **Optimized-for-Transcoding** (SBC General Settings page - Setup menu > Signaling & Media tab > SBC folder > SBC General Settings)

If the device is not configured to the Optimized-for-Transcoding profile, then configure it as shown above. Once configured, reset the device with a save-to-flash for the parameter and the new License Key to take effect.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant VE/SE.

2.23.1.38 Default OAMP Interface Changes

The following changes (shown highlighted) have been made to the default OAMP network interface address per product:

Product	IP Address	Prefix Length	Default Gateway
MP-1288	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 500L SBC/Gateway	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 500 SBC/Gateway	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 800 SBC/Gateway	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 1000 SBC/Gateway	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 2600 SBC	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 4000 SBC	192.168.0.2	24	0.0.0.0 (instead of 192.168.0.1)
Mediant 9000 SBC	192.168.0.2 (instead of 192.168.0.1)	24	0.0.0.0 (instead of 192.168.0.1)
Mediant VE/SE SBC	192.168.0.2 (instead of 192.168.0.1)	24	0.0.0.0 (instead of 192.168.0.1)

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.23.1.39 Alarms Tables Enhancements

The Active Alarms table and Alarms History table in the Web interface now display alarms from newest to oldest. In other words, the most recently raised alarm is shown first in the list. In addition, the Active Alarms table is now automatically refreshed every 60 seconds.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.23.1.40 Handling of Retry-After Header in SIP 503 Responses

The device can be configured for applying different behaviors when SIP 503 (Service Unavailable) containing a Retry-After header is received in response to a SIP message (e.g., REGISTER) sent to the proxy server. The configuration supported by a new global ini file parameter, RetryAfterMode. In certain scenarios (depending on the value of the parameter), the device considers the proxy as offline (down) for the number of seconds specified in the Retry-After header. During this timeout, the device does not send any SIP messages to the proxy.

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.23.1.41 Enhanced Cross Validation for UDP Port Configuration

The device's cross validation for conflicting configuration has been enhanced to include port (UDP/TCP/TLS) settings between Media Realm Extensions and other configuration entities (i.e., Media Realms and SIP Interfaces) using the same IP network interface. (Ports configured for such entities must not overlap.)

Applicable Applications: SBC/Gateway.

Applicable Products: All.

2.23.1.42 Improved Distribution of REGISTER and SUBSCRIBE Requests

The device's behavior has been slightly modified when configured to overwrite the expiry time in the Expires header of SIP 200 OK responses for user registration or subscription requests. The existing parameter that configures this feature—SBCRandomizeExpires—is now an enabled-disabled parameter and when enabled, the new expiry time generated by the device is based on fixed algorithms (for more information, refer to the User's Manual). This change has resulted in an improved distribution of registration and subscription requests over time.

Applicable Applications: SBC.

Applicable Products: All.

2.23.1.43 Variable Usage Enhancements for Message Manipulations

Using variables to store SIP message data for Message Manipulation has been enhanced:

- Variables can now be used for each registered far-end user:

  ```
  var.user|peer-user.<Variable Name>
  ```

  Where *user* and *peer-user* denote the two users in the session – current leg and peer leg.

- Instead of indices (numbers), a variable name is used for all variables types.

  ```
  var.global|session|call.src|call.dst.<Variable Name
  ```

  The variable name can include alphanumeric and hyphens (-).

  Previous syntax is still supported (variable indices are considered as names).

- All types allow up to 10 variables, where all 10 can have a summation of 690 characters.

- Variable value can be any string.

- Outbound Message Manipulation applied to a Server-type IP Group (i.e., proxy) can now access the param.ipg.src|dst.<x> syntax when the device sends an un-REGISTER. This is done using var.|peer-user.<Variable Name>

Applicable Applications: All.

Applicable Products: All.

2.23.1.44 Parameter Name Change from "Prefix" to "Pattern"

For parameters in configuration tables whose name contains "Prefix", the "Prefix" string has been replaced with "Pattern". This was done to accurately reflect the functionality of these parameters, which handle not only the prefix of numbers and SIP URIs, but also the suffix, etc. The supported patterns (notations) are documented in the User Manuals.

Applicable Applications: All.

Applicable Products: All.

2.23.2 Known Constraints

This section lists known constraints.

Table 2-30: Known Constraints in Version 7.20A.200.019

Incident	Description
145291	Sometimes after a Web session timeout or an HA switchover (for devices in HA), the user may be redirected to a URL such as http://x.x.x.x/PressLogOff or http://x.x.x.x/HostedTPFrontPanel. A workaround is to refresh the Web session (F5). **Applicable Products:** All.
148040	When using Mediant SBC VE in Hyper-V environments together with EMS or OVOC, the SBC identifier in the EMS / OVOC server (also known as "Serial Number") changes to a new value. If the KeepAlive functionality from the Hyper-V SBC VE to EMS/OVOC server is not enabled, EMS/OVOC will automatically detect the change of the SBC identifier for the existing SBC, within a short time, and there is no need for additional actions. If there is NAT between the SBC and EMS/OVOC server and the KeepAlive functionality from the SBC to the EMS/OVOC server is enabled, the SBC will be detected by the EMS/OVOC server as a completely new SBC device and it should be treated by the Administrator this way (meaning, updating configuration files, updating License Pool allocation to the SBC, etc.). In addition, the old SBC identifier used by the Mediant SBC should be manually removed from the EMS/OVOC server as it will no longer be used. **Applicable Products:** Mediant VE SBC.
150207	When the device is running on Amazon Web Services (AWS) cloud platform and a user manually modifies the IP Interfaces table prior to upgrading the device's software to Ver. 7.20A.200, the device sometimes becomes non-operational. **Applicable Products:** Mediant VE SBC.
150364	The Media Transcoding Cluster feature (MTC) is not supported in this 7.2 release. **Applicable Products:** Mediant 9000 SBC; Mediant VE.
150850	Devices running software version 7.2.106 must first be upgraded to 7.20A.158.009 before being upgraded to 7.20A.200. **Applicable Products:** Mediant 9000 SBC; Mediant VE/SE.
151219	Devices running software version 7.0 must first be upgraded to 7.20A.158 before being upgraded to 7.20A.200. **Applicable Products:** Mediant 9000 SBC; Mediant VE/SE.
150887	Running devices in Hyper-V environments is currently not supported. **Applicable Products:** Mediant VE SBC.
-	Devices running on Amazon Web Services (AWS) cloud platform do not support HA. **Applicable Products:** Mediant VE SBC.
-	The device does not support the GEN 10 HP server. **Applicable Products:** Mediant 9000 SBC.

2.23.3 Resolved Constraints

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

Table 2-31: Resolved Constraints in Version 7.20A.200.019

Incident	Description
150823	If the device receives an SBC call whose destination number is "*", the device replies with a SIP 180 response that contains "Contact: *". As a result, the call fails. **Applicable Products:** All.
150746	If more than one user has logged in to the device from the OVOC management interface, the device's Web interface displays the incorrect logged-in user. **Applicable Products:** All.
150652	The device is configured with a Proxy Set that has four addresses (alt. routing between addresses). If a new request is received before the next proxy responds to the OPTIONS request, the device rejects the new request (alternative route is not done on the new request) until the next working proxy responds. As a result, the online proxy is incorrectly identified as offline. **Applicable Products:** All.
150640	Two devices report the same serial number to the EMS (SNMP). As a result, the EMS is unable to provide management to the device. **Applicable Products:** Mediant VE/SE.
148040	Two devices report the same UUID to the EMS (SNMP). As a result, EMS cannot distinguish between the two. **Applicable Products:** Mediant VE/SE.
150588	The **show active calls** CLI command erroneously displays a duration of "0" for all calls. **Applicable Products:** All.
150492	Exporting the Dial Plan fails. **Applicable Products:** All.
150482	If during a call disconnect, the device receives a re-INVITE to the same call (To-tag present), it erroneously reports the call to SEM without the call ID. **Applicable Products:** All.
150480	Authentication of SIP PUBLISH messages does not function correctly and as a result, is not authenticated. **Applicable Products:** All.
150471	When fragmented packets are received on a port that is monitored by the Access List, the Access List drops the second part of the packet. As a result, the call fails. **Applicable Products:** All.
150291	When a DNS query responds with no (0) proxies, the device uses the wrong proxy IP address and Classification fails. As a result, the call fails. **Applicable Products:** All.
150231	If the prefix in the Dial Plan is configured with the range 0-9, the Dial Plan does not function. **Applicable Products:** All.

Incident	Description
150223	If the PSAP does not answer an emergency call, resources are not made available and after a while, no more ELIN calls can be processed. A workaround is to reset the device. **Applicable Products:** Gateway.
150190	For the Gateway application, a problem in the detection of DTMF-based caller ID causes no voice from the PSTN to the IP (one-way voice). A workaround is to disable caller ID. **Applicable Products:** Mediant 5xx, Mediant 8xx; MP-1288.
150140	When using an LDAP server for login authentication and the LDAP server responds with multiple groups which the user is a member of, the device uses the access level of the first member instead of the highest access level of all the members. As a result, the user cannot log in. **Applicable Products:** All.
150056	PSTN mapping of Unicode characters do not support 3 and 4 bytes ASCII characters. As a result, the device does not forward the calling name. **Applicable Products:** Digital Gateway.
150033	If the device is configured to send SIP OPTIONS to check the Tel-to-IP routing connectivity (ALTROUTINGTEL2IPENABLE parameter), an error message erroneously appears. **Applicable Products:** Gateway.
149792	When the device performs alternative routing of a REGISTER due to receiving a SIP 302 with two contacts and the two receive a 4xx response, the device does not forward the 4xx to the originator. As a result, a problem in registration occurs. **Applicable Products:** SBC.
149755	The device reports incorrect call quality to SEM **Applicable Products:** SBC.
149454	The CLI command **traceroute** does not function for IPv6 addresses. **Applicable Products:** SBC.
147996	When loading CLI configuration to a new device, the order of the commands are not maintained, which causes an error in configuration. **Applicable Products:** All.
147590	HTTPs only mode cannot be configured (only HTTP) for HTTP Proxy. **Applicable Products:** SBC.
147556	Upon receipt of a SIP 503 from a proxy in response to a REGISTER with a Retry-After header, the device marks the proxy as offline (alarm raised). **Applicable Products:** SBC.
146780	When loading a User Info file without a password, the device adds the user to IP Group 0. **Applicable Products:** SBC.
146643	If the device receives an ALERT with two PIs and only one of them is "= 8", it does not play early media. **Applicable Products:** Digital Gateway.
143381	When trying to create a snapshot, an error message appears. **Applicable Products:** Mediant VE.

Incident	Description
140194	When using the virtual console, if Ctrl+Alt+Delete key combination is pressed, the device resets. **Applicable Products:** Mediant VE.

2.24 Patch Version 7.20A.200.550

This patch version includes only resolved constraints.

2.24.1 Resolved Constraints

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

Table 2-32: Resolved Constraints in Version 7.20A.200.550

Incident	Description
153075	If the device has raised a major alarm due to the crossing of an IDS threshold and it then needs to raise a new minor IDS alarm before the major IDS alarm has cleared, the device is unable to provide an alarm description for this new event. As a result, the device crashes (resets). **Applicable Products:** SBC.

2.25 Patch Version 7.20A.202.112

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

> **Note:** This patch version is compatible with AudioCodes One Voice Operations Center (OVOC) Version 7.4.3082, and EMS/SEM Version 7.2.3106.

2.25.1 New Features

New features introduced in this version include the following:

2.25.1.1 New Mediant Software SBC Product - Mediant Cloud Edition (CE) SBC

AudioCodes has launched a new software-based SBC product, named *Mediant Cloud Edition (CE) SBC*, specifically designed to be hosted in cloud computing environments (currently supported on Amazon Web Services, with planned support for additional environments). The main benefit of the Mediant CE which differentiates it from other AudioCodes software-based SBCs (like the Mediant VE SBC) is that it's deployed as a multi-virtual machine (VM) SBC stack, providing elasticity using an Elastic Media Cluster architecture.

The Mediant CE includes a Signaling Component (SC) which handles the SIP signaling, while offloading all media traffic handling (RTP/SRTP) to Media Components (MC). A Cluster Manager embedded in the Mediant CE SBC determines which MC handles each media flow, allowing load balancing of media between the MCs. MCs are responsible for handling all aspects of their allocated media, including transcoding and forwarding.

Deployment and management of the Mediant CE is facilitated by AudioCodes new Stack Manager application, also introduced in this release. The Stack Manager is deployed in the Amazon VPC created for Mediant CE. The Stack Manager is used for managing the SBC software stack and implements a virtual network function manager functionality. Using the Stack Manager allows for horizontal scalability of the SBC based on changing traffic. The Stack Manager also provides a standard, open API allowing external DevOp tools and orchestrators to easily manage the Mediant CE operation and elastic scalability.

Mediant CE supports the full feature set of AudioCodes SBCs, maintaining familiar operation, management and APIs of the Mediant SBC product line.

The following main management features have been added to support the feature:

- CLI:
    - Auto-Update of CMP file for Media Components (MC):
      ```
      (config-system)# automatic-update
      (auto-update)# vmc-firmware <URL>
      ```
    - Copy CMP of MC:
      ```
      # copy vmc-firmware {from|to} <URL>
      ```
    - The CMP file is displayed in the output of the dir command.
- Web / INI / CLI:
    - EnableMtcSbc has been replaced by a new parameter that defines the Cluster mode: 'Cluster Mode' / SbcClusterMode / configure network > mtc settings > sbc-cluster-mode)
    - 'Device Role' / SbcDeviceRole / configure network > mtc settings > sbc-device-role

Applicable Applications: SBC.

Applicable Products: Mediant CE.

2.25.1.2 New Mediant 800 Hardware Revision – Mediant 800C

A new hardware revision—Rev. C—has been released for the Mediant 800. In addition to the interfaces and features offered by Mediant 800B, Mediant 800C also supports the following:

- Dual power supply – in addition to the AC power supply (provided by default), the device can be ordered for DC power supply, which is typically used for power redundancy (if AC power supply fails, fallback to the DC power supply is done).
- Up to 4 x E1/T1 (PRI) port interfaces.
- Single SBC capacity profile, supporting up to 2,000 users and 400 sessions.
- 110 transcoding sessions.

Applicable Applications: All.

Applicable Products: Mediant 800.

2.25.1.3 SBC Capacity Licensing Model - Floating License

AudioCodes offers a new SBC capacity licensing model for the device, called "Floating License". The Floating License is a network-wide capacity license that is dynamically shared among multiple devices. It is initially purchased as a set of licenses based on your estimated requirements, providing a pool of SBC-related capacity resources—SBC sessions, SBC signaling sessions, SBC media sessions, far end users (user registrations), and transcoding sessions—for all your deployed devices. The key benefit of the Floating License is that it allows the devices to exceed this initially ordered capacity, typically due to business growth or underestimation of initial requirements, and bills the Customer at the end of the month for the additional SBC resources that were consumed.

The Floating License is managed by AudioCodes OVOC tool and AudioCodes Cloud License Manager system. The devices participating in the Floating License need to be configured in OVOC and on each device. Once connected to OVOC, these devices are "open" to use any capacity. However, capacity is limited by the device's inherent capacity support and by an optional user-defined limit called Allocation Profile, which specifies the capacity per SBC license type.

The devices report their SBC resource consumption of each SBC license type to OVOC at set intervals (typically, every five minutes). OVOC sends a report to the Cloud License Manager every 24 hours with all the SBC resource usage in the last 24 hours by the devices. At the end of the month, AudioCodes analyzes the resource consumption reports in the Cloud License Manager. If consumption has exceeded the capacity as specified by the Floating License, AudioCodes bills the Customer for the extra capacity used.

The following main management features have been added to support the feature:

- Web interface:
    - The feature is enabled and an Allocation Profile is configured on a new page, Floating License (Setup menu > Administration tab > Maintenance folder > Floating License)
    - The existing License Key page displays the SBC capacity specified on the device to obtain from the Floating License
- CLI and ini file: Support the enabling of the Floating License and configuration of the Allocation Profile
- SNMP has two new alarms:
    - acCloudLicenseManagerAlarm – sent for certain OVOC-device connectivity issues and other related issues.
    - acFloatingLicenseAlarm – sent when the device has insufficient memory resources for the capacity configured for the Allocation Profile

Applicable Applications: SBC.

Applicable Products: All.

2.25.1.4 License Key of Redundant Device Included in INI File

The License Key of the Redundant device is now also included in the ini file of the Active device, for High-Availability systems. Up until now, the License Key was included only in the Redundant device's ini file.

Applicable Applications: Gateway/SBC.

Applicable Products: HA Devices.

2.25.1.5 Enhanced Media Transcoding Cluster Feature

The following enhancements have been made to the Media Transcoding Cluster feature:

- CLI command to copy software file (.cmp) for Media Transcoder (MT):
  ```
  copy mt-firmware {from|to} <URL>
  ```
- Web interface: The folder in the Navigation pane containing the related page items has been renamed to "Media Cluster".

Applicable Applications: SBC.

Applicable Products: Mediant CE.

2.25.1.6 Triggering SBC Actions using SIP NOTIFY Messages

For the SBC application, incoming SIP NOTIFY messages from configured proxy servers can trigger various device actions if the SIP Event header contains certain values:

- 'check-sync;reboot=false': Triggers the Automatic Update feature (if configured)
- 'check-sync;reboot=true': Triggers a device reset.

Up until now, the above was supported only by the Gateway application.

The device now also supports remote trigger by NOTIFY messages for disconnecting all current calls (SBC and Gateway). This occurs if the message's Event header contains the 'soft-sync' value.

The feature is supported by the existing parameter, EnableSIPRemoteReset.

Applicable Applications: SBC.

Applicable Products: All.

2.25.1.7 SIP Session Time Refreshes using UPDATE Messages

For refreshing the timer of currently active SIP sessions, the device can now be configured to send session refreshes using SIP UPDATE messages if the SIP Allow header in the last SIP message received from the user, contains the value "UPDATE".

This is enabled by configuring the existing parameter, 'Remote Update Support' (IpProfile_SBCRemoteUpdateSupport) to the new optional value, "According Remote Allow" (3). If the Allow header does not contain the "UPDATE" value (or if the parameter is not configured to 3), the device uses INVITE messages for session refreshes.

Applicable Applications: SBC.

Applicable Products: All.

2.25.1.8 Enhanced Randomly Assigned SIP Contact User Part

When using Accounts (configured in the Accounts table) and the device is configured to automatically create a random string for the user part of the SIP Contact header in the generated SIP REGISTER request (using the existing UseRandomUser parameter), the string now always begins with a letter (and not a number). For example, the below random string begins with the letter "H":

```
Contact: <sip:HRaNEmZnfX6xZl4@pc33.atlanta.com>
```

Once the Account is registered with the registrar, register refreshing uses this random user part.

In addition, the device stops using the random user part in the following scenarios:

- If the user performs an unregister.
- If the REGISTER request send by the device is not responded by a SIP 200 OK. (Currently, it also includes SIP 3XX responses.)

Applicable Applications: All.

Applicable Products: All.

2.25.1.9 Enhanced Handling of SIP Dialog-initiating INVITE Messages

Optional values 2 and 3 have now been added to the existing global configuration parameter (ini file), VerifyRecievedRequestUri:

- [0] – Does not verify - default (existing value)
- [1] - Verify Request-URI user part for in-call requests (existing value)
- [2] - Verify dialog-initiating INVITE for all required conditions (Via, Source IP and user in Request-URI)
- [3] - Verify both dialog-initiating INVITE as well as in-call requests

In addition, a new global configuration parameter has been added, RegistrarProxySetID (ini file), which configures the Proxy Set associated with the registrar (assuming the SIP Interface has only one registrar). The default value is undefined (-1).

- **Handling Dialog-Initiating INVITEs:** If the VerifyRecievedRequestUri parameter is configured to 2 or 3, and the RegistrarProxySetID is configured, dialog-initiating INVITE requests are allowed from the registrar at which the Accounts (configured in the Accounts table) are registered. For incoming dialog-initiating INVITEs from a specific SIP Interface (from the registrar), the following rules apply (listed according to priority):
    - The top-most Via header must contain a host-resolved IP address of the registrar; otherwise, the device drops the INVITE request.
    - The source IP address must be the same as the IP address of the registrar; otherwise, the device rejects the requests and sends a 403 (Forbidden) response to the registrar.
    - The user, specified in the Request-URI header, must be identical to the Contact user part configured for the associated Account and the Account must be registered. Otherwise, the device rejects the request with SIP 404 (Not Found) response.

  If the RegistrarProxySetID parameter is not configured or no Accounts are configured, the device accepts the dialog-initiating INVITE request.

  This feature is applicable only to the SBC application.
- **Handling In-call Requests:** If the VerifyRecievedRequestUri parameter is configured to 1 or 3, for all received in-call requests (including ACK and CANCEL), the device checks if the Request-URI user part matches the remote Contact user part (i.e., the same as the Contact user configured for the Account). If there is no match, the device rejects the request and sends a SIP 481 response for requests such as BYE and CANCEL or a SIP 404 for other requests, and for ACK it does not send any response.

  This feature is applicable to the Gateway and SBC applications.

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.10 Increase in Maximum Characters for User Part of SIP Messages

The device can now process SIP messages whose user part is up to 60 characters without truncating the characters. In previous releases, the maximum was 50 characters. If the user part has more than 60 characters, the device removes (truncates) the extra characters from the right until there are 60 characters. An example of a lengthy user part (55 characters) is shown below in bold:

```
INVITE sip:0433551202;tgrp=grp001;trunk-
context=98912345678901@10.15.50.31;user=phone SIP/2.0
```

Applicable Applications: All.

Applicable Products: All.

2.25.1.11 SIP Digest URI Handling for Authentication and Authorization

When the device sends a request in response to a SIP 401 (Unauthorized) or 407 (Proxy Authentication Required), it can include or exclude the URI parameters for the Digest URI in the Proxy-Authorization or Authorization header. If configured to include the URI, it sets the Digest URI to the same URI as that received in the original Request-URI. This feature is configured by the new global ini file parameter, SIPDigestAuthorizationURIMode. By default, the Digest URI is sent without URI parameters. Below shows an example of a request with an Authorization header containing a Digest URI (shown in bold):

```
Authorization: Digest username="alice at
audiocodes.com",realm="audiocodes.com",nonce="",response="",uri="s
ip:audiocodes.com"
```

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.12 Handling SIP Messages with Unknown Cryptographic Suites

The device can now be configured to keep or remove unknown cryptographic suites (encryption and authentication algorithms) that may be present in the SDP's 'a=crypto' attribute of incoming SIP messages. In previous releases, the device simply forwarded the SIP message with the unknown cryptographic suites and if the endpoint selected one of the unknown suites (i.e., not supported by the device), the device rejected the call.

To support the feature, a new parameter was added to the IP Profile table, IpProfile_SBCRemoveUnKnownCrypto, which determines whether the device keeps or removes the unknown cryptographic suites before forwarding the SIP message.

Applicable Applications: SBC.

Applicable Products: All.

2.25.1.13 Handling both SDES and DTLS Security in SDP Negotiations

The device can be configured to handle both SDES and DTLS for media security. The feature is configured by setting the existing parameter 'SBC Media Security Method' (IpProfile_SBCMediaSecurityMethod) to the new optional value "Both" (2).

Applicable Applications: SBC.

Applicable Products: All.

2.25.1.14 Graceful Period for Automatic Update of ini File

The Automatic Update feature can now be configured to apply the settings of a downloaded ini file only after a graceful timeout. When the Automatic Update feature is triggered (for example, by a device reset) and the device downloads the ini file from a remote server, the graceful timeout starts and new calls are not accepted during this period. Once the timeout expires, the device terminates all current calls and then applies the configuration according to the downloaded ini file.

The feature is enabled by the new ini file parameter, AupdGracefulShutdown (disabled by default). The graceful timeout is configured by the Web interface's 'Graceful Option' parameter (Maintenance Actions page) or ini file parameter AdminStateLockControl (default is no timeout).

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.15 Enhanced SNMP Alarms for HA Redundant Device

SNMP alarms raised by the Redundant device in a High-Availability (HA) system now provide the following enhancements:

- Alarms of the Redundant device are now reflected correctly in OVOC as alarms (and not as events, as in earlier versions).
- Alarms of the Redundant device are now sent to the Active device and displayed in the Active Alarms table (and History Alarms table) with the alarms of the Active device. Alarms pertaining to the Redundant device are displayed with the alarm source prefix, "Redundant#1/" (e.g., "Redundant#1/EthernetLink#4").
- The Web interface's alarm bell icon (located on the top-right of the GUI window) now displays the number of active alarms raised by both Active and Redundant devices and displays the highest severity of all these active alarms raised.

Applicable Applications: Gateway/SBC.

Applicable Products: HA Devices.

2.25.1.16 Serial Number of Redundant Device in Keep-alive SNMP Traps

SNMP keep-alive traps (acKeepAlive) sent by the active device in a High-Availability system now include the redundant device's serial number. This appears in the acBoardTrapGlobalsAdditionalInfo3 SNMP varbind.

Applicable Applications: All.

Applicable Products: HA Devices.

2.25.1.17 Web Interface's Logo Hyperlinked to Topology View Page

The logo of the Web interface (located in the top-left corner) is now hyperlinked to the Topology View page (Setup menu > Signaling & Media tab > Topology View home icon). The feature offers administrators a quick-and-easy way to navigate to this informative and often needed page.

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.18 Mediant 9000 Hardware Status Display in Management Interfaces

The device's management interfaces now provide more information about the status of the device's hardware components.

- Web interface:
    - The Monitor page displays status icons for the Fan and Power modules. If the device is in HA mode, the status is also displayed for the Redundant device. When these icons are clicked, the new Components Status page opens (see below).
    - A new page has been added—Components Status page (Monitor menu > Monitor tab > Summary folder > Components Status) —displaying detailed status information of the following hardware components (Redundant device as well for HA mode): fans, power supplies and CPU temperature.
- CLI: The existing command, **show system assembly** now also displays the status of the fans, power supplies and CPU temperature.
- SNMP: The device now supports the following alarms – acFanTrayAlarm,

acPowerSupplyAlarm, acBoardTemperatureAlarm.

- INI file:
  - The temperature threshold for raising the acBoardTemperatureAlarm can be configured using the new ini file parameter, HighTemperatureThreshold (default is 70°C or 158°F)
  - The acPowerSupplyAlarm is enabled using a new ini file parameter, DualPowerSupplySupported

Note: The feature will be supported on Mediant 9000 Hardware Rev. B in the next applicable release.

Applicable Applications: SBC.

Applicable Products: Mediant 9000.

2.25.1.19 OVOC Product Key and ID Displayed in Web Interface

The OVOC Product Key and OVOC Product ID are now displayed in the Web interface when the licensing model Floating License or Fixed Pool License is employed. The OVOC Product Key is displayed in the License Key page and the OVOC Product ID in the Floating License page.

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.20 New Default Name for IP Interfaces

When configuring an IP Interface in the IP Interfaces table and no name is configured, the device assigns the IP Interface with a default name in the following format: "Interface_n", where *n* is the row index number. Previously, the format was "InterfaceTable_n".

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.21 No Reset for Number of Media Channels Parameter

The Number of Media Channels parameter (MediaChannels) no longer requires a device reset for its settings to take effect. In addition, if the parameter value is modified to a value that is less than the number of DSPs currently allocated to current calls, these calls are not forcibly terminated by the device (as in previous releases).

Applicable Applications: All.

Applicable Products: All.

2.25.1.22 New CLI Command Structure for Parent-Child Configuration Tables

Configuration tables with parent-child relationships have been restructured in the CLI. Child tables are now accessed from within parent tables. In addition, access to tables can now be done by entity name (as well as by row index, supported in earlier versions).

For example, in earlier versions, to access the child table **dial-plan-rule** Index 1 of **dial-plan** Index 0, the following syntax was used:

```
(config-voip)# sbc dial-plan-rule 0/1
```

Now, it is accessed from within the parent table:

```
(config-voip)# sbc dial-plan 0
(dial-plan-0)# dial-plan-rule 1
(dial-plan-rule-0/1)#
```

Applicable Applications: Gateway/SBC.

Applicable Products: All.

2.25.1.23 Enhanced Filtering for CLI show Commands

Certain **show** CLI commands now support enhanced filtering of their displayed output:

- first <x>: Displays the first *x* number of entries
- last <x>: Displays the last x number of entries
- range <x-y>: Displays a range of entries from *x* to *y*
- descending: Displays the output in descending order

These filters are supported by following **show** commands:

```
show voip calls active
show voip register
show voip proxy sets status
```

Applicable Applications: All.

Applicable Products: All.

2.25.1.24 Improved Location of CLI Command time-zone-format

The time-zone-format command (TimeZoneFormat) has been relocated in the CLI and is now with all the other CDR-related commands -- configure troubleshoot > cdr > time-zone-format.

Applicable Applications: All.

Applicable Products: All.

2.25.1.25 Improved Location of CLI Commands for System Snapshots

The CLI commands for the System Snapshot feature have been relocated in the CLI to the root level (privileged user mode – "#"), facilitating configuration by their fast-and-easy access instead of drilling down CLI commands as in previous releases. In addition, the names of the snapshot commands have also changed slightly, as shown below:

```
# system-snapshot {create|default|delete|help|load|show}
```

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant SW.

2.25.1.26 CLI Command Name Change from "prefix" to "pattern"

For CLI commands in configuration tables whose name contains "prefix", the "prefix" string has been replaced with "pattern". This was done to accurately reflect the functionality of these commands, which handle not only the prefix of numbers and SIP URIs, but also the suffix, etc. The supported patterns (notations) are documented in the User Manuals.

Applicable Applications: All.

Applicable Products: All.

2.25.1.27 New CLI Commands for Assigning Dial Plans to Gateway Routing

Assigning Dial Plans to Gateway routing rules can now be done through the CLI:

- configure voip > gateway routing settings > **ip-dial-plan-name**: IP-to-Tel Dial Plan Name (IP2TelDialPlanName)
- configure voip > gateway routing settings > **tel-dial-plan-name**: Tel-to-IP Dial Plan Name (Tel2IPDialPlanName)

Applicable Applications: Gateway.

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

2.25.1.28 New CLI Commands for Locking and Unlocking Device

Locking the device can now be done through the CLI (root level):

- Locking the device with or without graceful timeout:

  ```
  admin state lock {graceful <Timeout>|no-graceful}
  ```

- Unlocking the device:

  ```
  admin state unlock
  ```

The administrative state (locked or unlocked) of the device can be viewed using the following new command:

```
show admin state
```

Applicable Applications: All.

Applicable Products: All.

2.25.1.29 New CLI Commands for Displaying Activity Reports

A logged report of all CLI activities can now be viewed using the following new CLI command:

```
show activity-log [> <URL of Remote Server>]
```

The logged report (output) can also be sent to a remote server (TFTP or HTTP/S), which is defined by URL.

Note that the command displays logged activities only if activity logging has been enabled (configure troubleshoot > activity-log).

Applicable Applications: All.

Applicable Products: All.

2.25.1.30 New CDR Field -- 'Alerting Time'

CDRs can now optionally include the Alerting Time field, which indicates the duration (in milliseconds) between ringing (SIP 180 Ringing) and call answered (SIP 200 OK) or unanswered (Cancel). The field can be added by customizing the CDR format using the CDR Format tables (SBC and Gateway). (The field is included by default in CDRs that are sent to ARM.)

Applicable Applications: All.

Applicable Products: All

2.25.1.31 Name and ID of Media Components (MCs) Included in CDRs

For the Media Cluster feature, CDRs that are sent to OVOC for reporting Quality of Experience, now include the Media Component's name and index number.

Applicable Applications: SBC.

Applicable Products: Mediant 9000; Mediant SW.

2.25.1.32 Automatic IP Address for NAT Traversal in AWS Environments

The device's management interface now supports configuration of a NAT IP address mode when the device is deployed in an Amazon Web Services (AWS) cloud-computing environment. The mode can be set to Automatic or Manual. The Automatic mode is used when the AWS environment is configured with an Elastic IP address and enables the device to automatically associate it with the selected source IP interface as the global (public) IP address. To support the feature, the following new parameters have been added to the NAT Translation table: 'Target IP Mode' and 'Automatic Target IP Address' (read-only).

Applicable Applications: SBC.

Applicable Products: Mediant CE.

2.25.1.33 New VoIPerfect Support for Managed G.729 Coder

The device's VoIPerfect feature now also supports Managed G.729 coder. Previously, only Managed Opus was supported. If the Enterprise SBC detects WAN network impairments during a call between the Enterprise SBC and Access SBC, it can adjust the coder's attributes (e.g., bit rate) for that specific call to ensure voice quality is maintained.

This feature also adds support when Managed G.729 operates in MPLS networks. In such scenarios, a new ini file parameter, MPLSMode needs to be enables.

Applicable Applications: SBC.

Applicable Products: Mediant 800; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.

2.25.2 Known Constraints

This section lists known constraints.

Table 2-33: Known Constraints in Version 7.20A.202.112

Incident	Description
-	From Version 7.2.202, when using any transcoding/DSP functionality, the device must be configured to use the "Optimized-for-Transcoding" profile, using the SBCPerformanceProfile parameter. The parameter's value is not automatically set in all upgrade scenarios. If you are upgrading from a version earlier than 7.2.158 and employing transcoding/DSP capabilities, to preserve your transcoding/DSP functionality it is essential that you first upgrade the device to Version 7.2.158 before upgrading it to Version 7.2.2xx. For more information, see Section 2.23.1.37 on page 140. **Applicable Products:** Mediant 9000; Mediant VE.
-	From Version 7.2.202, when upgrading the License Key to enable any DSP functionality (including transcoding), the SBCPerformanceProfile parameter must be configured to the Optimized-for-Transcoding profile option, as the parameter's value is not automatically set after installing such a License Key. If not configured, DSP functionality will remain disabled. For more information, see Section 2.23.1.37 on page 140. **Applicable Products:** Mediant 9000; Mediant VE.
-	The Media Transcoding Cluster (MTC) feature is not supported in this release. **Applicable Products:** Mediant 9000; Mediant VE.
-	The Cluster Mode parameter is supported only by Mediant Cloud Edition (running in an AWS environment). For all other products listed below, it is not supported. **Applicable Products:** Mediant 9000; Mediant VE.
152903	Firewall rules using a specific IP Interface (' Interface Name' parameter) as a matching criterion, do not function if the interface uses a tagged VLAN and/or operates on an Ethernet Group with two ports ("members"). **Applicable Products:** Mediant 9000; Mediant Software.
152811	The device does not accept incoming media traffic if the ingress media interface uses a tagged VLAN and operates on an Ethernet Group with two ports ("members"). (Media traffic also includes traffic from Media Components for the Media Cluster feature). **Applicable Products:** Mediant 9000; Mediant Software.
	Hardware status indications (fan, power and CPU temperature) are not supported by Mediant 9000 Hardware Rev. B. **Applicable Products:** Mediant 9000.
152859	Music-on-hold played from an external media source (ExternalMediaSource parameter) is not supported by Mediant Cloud Edition. **Applicable Products:** Mediant CE.
-	If the Floating License mode is enabled and the device needs to be downgraded to Version 7.2.200, the Floating License mode must be disabled prior to the downgrade (as it is not supported in this version). **Applicable Products:** All.

Incident	Description
153048	Mediant CE does not support IPv6. **Applicable Products:** Mediant CE.
152094	Incorrect MOS scores are reported at the end of an SBC call between AudioCodes IP Phones (MOS measured during the call is correct). This occurs only in certain scenarios (regarding RTCP and DSPs). **Applicable Products:** MP-1288; Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.
153454	When the 'Mode' parameter (EtherGroupTable_Mode) in the Ethernet Groups table is configured to "2RX/1TX", detection by the device of a failure in the transmitting port is based only on physical link failure (e.g., cable disconnected or port damaged) and not Ethernet link failure. **Applicable Products:** Mediant SW.
153524	For the CDR Local Storage feature, stored CDRs are deleted after an HA switchover. **Applicable Products:** HA.
-	For Mediant VE, the AWS must have an IAM role and therefore, existing instances must be attached with an IAM role as described in the *Mediant VE Installation Manual*. **Applicable Products:** Mediant VE (AWS).
153614	When the device is configured for HA, ARM is not supported. **Applicable Products:** HA.
153759	When performing a restore-to-default action through the Web interface, the device doesn't reset and therefore, the operation fails. **Applicable Products:** All.
153837	When using the SIPRec feature for the Gateway application, the IP Group representing the SRS must be assigned a Media Realm (in the IP Groups table). **Applicable Products:** Gateway.

2.25.3 Resolved Constraints

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

Table 2-34: Resolved Constraints in Version 7.20A.202xxx

Incident	Description
151962	When importing a partial Dial Plan, new and modified rules were applied, but were not activated. **Applicable Products:** All (SBC).
151998	When the device's Web interface is accessed through OVOC (HTTPS) using the Single Sign On feature, clicking the Troubleshooting tab causes a disconnection with the Web interface. **Applicable Products:** All (SBC).
152749	When the device rejects a call due to CAC, the CDR for this call is not sent to the local storage. **Applicable Products:** All (SBC).
152810	The device merges multiple SIP Reason headers that are received in the incoming leg into one Reason header in the outgoing leg. **Applicable Products:** All (SBC).

Incident	Description
152820	The Configuration Package which is downloaded through SFTP doesn’t reflect recent configuration changes. **Applicable Products:** All (SBC).
152903	Upgrading an HA system from 7.20A.156.009 to this version, causes the system to become standalone.(i.e., no HA). **Applicable Products:** HA Devices.
153358	When an endpoint dials from the PSTN to the device, the endpoint hears the voice from another call processed by the device (instead of hearing a dial tone or ringback tone from the device). **Applicable Products:** Gateway.
153533	When the device is configured to perform Tel-to-IP call forking to two destinations with a delay of 15 seconds between each INVITE (i.e., ForkingDelayTimeForInvite =15), if the first call is disconnected after the selfcheck, the device resets. **Applicable Products:** Gateway.
153635	The Syslog indicates that the LDAP timer has been cancelled when in fact it hasn't. As a result, the LDAP process fails. **Applicable Products:** All.
153645	A "frozen" socket causes the device not to send call statistics to SEM. **Applicable Products:** All.
151056	When using the Pattern Editor in the Web interface, if an incorrect value is entered and the back arrow is used to try and fix the entry, the auto-completion feature does not function correctly. Now, the auto-completion feature is suspended so that the incorrect value can be fixed. To resume auto-completion hints, the cursor must be placed at the end of the field. **Applicable Products:** All (SBC).
152239	In the NAT Translation table, the read-only field 'Automatic Target IP Address' displays the local IP address instead of the global IP address when the 'Target IP Mode' field is configured to Automatic (for AWS environments). **Applicable Products:** Mediant SW.
144263	The SNMP performance monitoring MIB, acPMSIPIPGroupInviteDialogsTotal displays the wrong value. **Applicable Products:** All (SBC).
148401	The device's SBC application doesn't support SIP NOTIFY with "Event: CheckSync". **Applicable Products:** All (SBC).
149096	Video is not functioning for WebRTC calls. As a result, the call fails. **Applicable Products:** All (SBC).
149304	The device does not send an SNMP alarm for SBC CAC when the limit or reservation threshold is exceeded. **Applicable Products:** All (SBC).
149846	If the device sends an INVITE on the outgoing leg and doesn’t receive a 1xx in response, when it receives a CANCEL on the incoming leg, it doesn’t forward the CANCEL to the outgoing leg. As a result, the SBC call does not get released. **Applicable Products:** All (SBC).

Incident	Description
149925	If the filename of the Web interface's logo file contains spaces, HA synchronization fails. **Applicable Products:** HA.
150353	The maximum length of the user part is only 50 characters and therefore, incoming REGISTER messages with long AOR\Contact values are recorded incorrectly in the device's registration database. **Applicable Products:** All (SBC).
150624	When the device is reset, it sends the wrong MAC address upon bootup. **Applicable Products:** MP-1288; Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.
150731	The device resets due to memory allocation overrun. **Applicable Products:** Mediant 1000.
150735	When trying to load an incremental ini file or an incremental CLI script using the REST API (over CURL), the HTTP response 405 (Method Not Allowed) is received and the upload fails. **Applicable Products:** All.
150791	When running debug recording (DR) for the device and it utilizes DSPs, the wrong “ConnectionArray::AuditConnections” messages are displayed in the Syslog after the call ends. **Applicable Products:** All.
150811	The device doesn't respond to SIP NOTIFY messages received from the Application server for the BLF service (fragmented massages); the device sends only ICMP timeout messages. As a result, the call fails. **Applicable Products:** All.
150831	During a direct-media SBC call and in a specific scenario, the device sends a SIP 200 OK with "a=inactive". As a result, no voice occurs. **Applicable Products:** All.
150893	When the device receives a SIP INVITE with a Call-ID greater than 129 characters, the device truncates the Call-ID to 129 characters. As a result, the SBC call fails. **Applicable Products:** All (SBC).
150958	If the OSNInternalVlan is configured to 1, when an HA switchover occurs, the switchover fails and as a result, HA mode fails. **Applicable Products:** Mediant 800 (HA).
151070	The Dial Plan cannot be exported using the Web interface ("Unauthorized" page appears). **Applicable Products:** All.
151078	When the device sends a SIP INVITE over UDP and receives "error: Network is unreachable(101)", it keeps trying the retransmission of UDP instead of immediately falling back to the alternative route, which it does only after a few seconds, causing a call delay. **Applicable Products:** All.
151114	If the License Key has no licensed SBC sessions (SBC = 0) and the TDM-to-SBC license is enabled (TDM2SBC > 1), the SIP Interface cannot be modified to SBC application type. As a result, SBC functionality is disabled. **Applicable Products:** Hybrid.

Incident	Description
151128	When using the Web interface with the Internet Explorer browser, the SRD filter feature doesn't function. **Applicable Products:** All.
151201	The device continuously reboots (resets) due to voice quality monitoring when trying to connect to OVOC over TLS. **Applicable Products:** All.
151245	The device doesn't handle big or fragmented SIP packets received on network interfaces that are not "OAMP + Control + Media", and resets as a result. **Applicable Products:** All.
151329	When the device runs a Message Manipulation rule to clear the display name from the SIP From header, it crashes (resets) **Applicable Products:** All (SBC).
151334	The CLI command **show voip calls statistics sbc media** fails. **Applicable Products:** All (SBC).
151346	During memory allocation for HA, the Redundant unit resets and HA becomes disabled. **Applicable Products:** HA.
151367	The device fails to switch to the alternative SBC routing rule when the next rule is an IP Group Set. As a result, the call fails. **Applicable Products:** All.
151433	The Fax Re-Routing feature fails. **Applicable Products:** All.
151440	When the parameter DisplayLoginInformation is configured to 1 (enabled), incorrect login information is displayed when accessing the Web interface over HTTPS. **Applicable Products:** All.
151449	A problem occurs with voice in the decoder direction on modem clear-mode calls. As a result, modem calls fail. **Applicable Products:** Gateway.
151556	The device doesn't send SRTP packets in a transcoding call after a hold-retrieve scenario. As a result, one-way voice occurs. **Applicable Products:** Gateway.
151564	The SNMP tables, ifTable and dsx1ConfigTable provide incorrect statistics. **Applicable Products:** Mediant 500L.
151646	In the early media stage of an SBC call, the device adds silence suppression to the SDP answer. As a result, the call disconnects. **Applicable Products:** All.
151664	The device receives many SIP 18x before DNS resolution is done and therefore, is unable to allocate the necessary resources for each 18x. As a result, the call fails. **Applicable Products:** All.
151671	When upgrading the device to Version 7.20A.200.019, the Ethernet Groups table configuration changes. As a result, the device becomes inaccessible. **Applicable Products:** All.

Incident	Description
151690	The device sends a SIP 488 response after receiving a 200 OK to an outgoing re-INVITE due to incorrect fax coder calculations. As a result, the call fails. **Applicable Products:** All.
151699	The SNMP trap community string supports only up to 19 characters. **Applicable Products:** All.
151726	The SNMP fan tray alarm is sent by the device even though the fan tray is ok. **Applicable Products:** All.
151757	The device does not remove unsupported crypto suites (e.g., AES_256) in the outgoing SIP INVITE message and if the remote side chooses an unsupported crypto suite, the SBC call therefore fails. **Applicable Products:** All.
151795	Locally stored CDRs cannot be downloaded through SFTP. **Applicable Products:** All.
151803	The device does not consider the security protocol when creating a re-INVITE for fax calls (proto as RTP/AVP instead of RTP/SAVP). As a result, the fax fails. **Applicable Products:** Gateways.
151885	The "/" character is invalid in some configuration table names (e.g., name for SIP Interface). **Applicable Products:** All.
151897	A memory leak occurs due to an endless recursion of some tasks. As a result, the HA system crashes (resets). **Applicable Products:** HA.
151907	When the device performs an LDAP query for an IP-to-Tel call and gets a result, IP-to-Tel number manipulation doesn’t work if based on source IP Group. **Applicable Products:** Gateways.
151922	Memory utilization value through SNMP displays incorrect results (should be in percentages as displayed in CLI). **Applicable Products:** All.
151951	The Web interface's Port Status page does not display correct SIP information for the call. **Applicable Products:** MP-1288.
152053	If an RTP stream is opened with SRTP for an SBC call and then re-negotiation changes it to RTP, the old crypto suites are not updated and as a result, the call remains in SRTP and no voice occurs. **Applicable Products:** All.
152098	The Topology View page of the Web interface cannot display more than two digits for an IP Group ID (e.g., IP Group #142 is displayed as IP Group #14). **Applicable Products:** All.
152109	BRI parameters erroneously appear in the Web interface even though BRI is not supported. **Applicable Products:** MP-1288.
152147	When the device re-routes an SBC call upon CNG detection in the early media phase, it sends the new INVITE to the fax server. However, when fax server answers with a 200 OK, the device doesn't forward it to the source leg. As a result, the fax fails. **Applicable Products:** All.

Incident	Description
152324	When establishing a CLI connection (Telnet\SSH) with the device without entering the password, device resources are used and never released. As a result, logging in to the device's CLI fails. **Applicable Products:** All.
152328	The MgmtUseLocalUsersDatabase parameter requires a reset for its settings to take effect (instead of on-the-fly). **Applicable Products:** All.
152330	After a manual HA switchover, the registrations are removed and calls fail due to a loss of TPNCP connection and traffic on the HA Maintenance interface. **Applicable Products:** HA.
152354	When using the REST API to load a specific CLI script that includes a command to import a Dial Plan, the device's Web interface freezes and only a device reset resolves the issue. **Applicable Products:** All.
152426	If the device receives an INVITE message containing many large SIP headers, a loss of HDP3 resources occurs and as a result, the SBC call fails. **Applicable Products:** All.
152482	After a software upgrade, the Product Key is no longer displayed in the Web interface. **Applicable Products:** All.
152610	Sometimes ARM tries to connect to the device, but gets an exception "javax.net.ssl.SSLKeyException: Invalid signature on ECDH server key exchange message" and can't connect. **Applicable Products:** All.
152683	The Web interface's Success/Failure Ratio page can only be selected to display up to IP Group ID 32. **Applicable Products:** All.
152716	Number manipulation is performed twice (instead of once) for Tel-to-IP Gateway calls in the following scenario: 1) The device adds NPI and TON and then performs number manipulation; 2) as the routing rule is configured for "Routing Before Manipulation", the device sends the original number to CSR; 3) upon a result from CSR, the device performs number manipulation again, but for the original number (without NPI and TON). As a result, the source number is manipulated to the wrong number. **Applicable Products:** Gateway.
152803	Received analog calls that were transferred by Skype fail due to lack of DSP resources. **Applicable Products:** Gateway.
152837	The device resets for SBC direct media calls in the following scenario: The device is configured for Direct Media (SBCDirectMedia = 1). A calls B and a direct media call is established. A sends an empty re-INVITE, B sends an offer, and then A rejects the offer by sending an ACK with port 0. **Applicable Products:** All.
152879	Running penetration testing has found a cross-site scripting (CSS) bug (security vulnerability) **Applicable Products:** All.

Incident	Description
152992	A large memory leak on the Redundant unit (due to TPNCP restart connection) causes the Redundant unit to reset. **Applicable Products:** HA.
153075	The device experiences a reset loop when the IDS Threshold alarm is changed from higher to lower. As a result, the device crashes (resets). **Applicable Products:** All.
153135	After upgrading to this version, SBC calls experience no audio if additional target ports in the NAT Translation table are not configured. **Applicable Products:** All.
153146	After upgrading to this version, all default (not configured) UDP\TCP ports become 0 in the SIP Interfaces table. As a result, SBC calls fail. **Applicable Products:** All.
153228	On a specific TCP connection call scenario, the device got a SIP BYE, but kept sending retransmissions which caused it to reset. **Applicable Products:** All.
153592	The device crashes (resets) when it receives a REST query from ARM and then sends a response containing more IP Groups than can be sent in the response (currently, up to 200 IP Groups can be sent in the response). **Applicable Products:** All.

3 MSBR Series

This chapter describes new features, known constraints and resolved constraints relating to data-router functionality of the Mediant MSBR product series.

3.1 Version 7.20A.150.004

This is the initial version of the 7.2 Software Release for the MSBR product series.

Note:

- This version is based on MSBR 6.8 Version **6.80A.335.005**, released in March 2017. In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ VDSL ISDN
  - √ VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.
- This patch version is compatible with AudioCodes EMS/SEM Version 7.2.3083.

3.1.1 New Features

Please see the note in Section 3.1.

3.1.2 Known Constraints

This section lists known constraints.

Table 3-1: Known Constraints in Version 7.20A.150.004

Incident	Description
-	TR-181 is not supported. **Applicable Products:** MSBR.
143283	DHCPv6 NTP "Current Dynamic NTP Server" information is not displayed in the CLI when running the CLI command **show system ntp-status**. **Applicable Products:** MSBR.
143295	The CL command **debug reset-history** saves only the last three reset reasons. **Applicable Products:** MSBR.
144181	The device does not support 802.1X. **Applicable Products:** MSBR.
144214	The CLI command **debug capture data physical clear** is not supported. **Applicable Products:** MSBR.
144076	The CLI command **show data interfaces cellular 0/0** fails. **Applicable Products:** MSBR.
141108	Running speed tests through TR-069 is not supported.

3.1.3 Resolved Constraints

Please see the note in Section 3.1.

3.2 Version 7.20A.154.025

This patch version includes new features and resolved constraints.

Note:

- This version is based on MSBR Version 6.80A.347.001 (released in July 2017). In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - VDSL ISDN
  - VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

3.2.1 New Features

New features introduced in this version include the following:

- Bidirectional Forwarding Detection (BFD) support for Open Shortest Path First (OSPF). The new command to enable BFD for an OSPF interface is as follows:

  ```
  (config-if)# ip ospf bfd interval <Value> min_rx <Value>
  multiplier <Value>
  ```

  where:

  - *interval*: Interval (in msec) for outgoing BFD messages. The interval is increased if required by remote system.
  - *min_rx*: Minimal interval (in msec) between BFD messages in milliseconds. The remote system uses this interval for sending messages if its interval is lower.
  - *multiplier*: Maximum number of packets that can be missed before the session status is considered down.
- Bidirectional Forwarding Detection (BFD) support for static routes. The new command

to enable BFD for a static route is as follows:

```
(config-data)# bfd neighbor <Neighbor ID> <IP Address>
<Interface ID> interval <Value> min_rx <Value> multiplier
<Value> [multihop]
```

where:

- *neighbor id:* (1-20) Neighbor identifier.
- *ip address:* Address of the remote BFD device.
- *interface id:* Name and number of the outgoing interface.
- *interval*: Interval (in msec) for outgoing BFD messages. The interval is increased if required by remote system.
- *min_rx*: Minimal interval (in msec) between BFD messages in milliseconds. The remote system uses this interval for sending messages if its interval is lower.
- *multiplier*: Maximum number of packets that can be missed before the session status is considered down.
- *multihop:* Set the neighbor to multihop mode in case the remote device is not on the local LAN
  The parameter **bfd-neighbor <neighbor ID>** was added to the **ip route** command:

```
(config-data)# ip route <Ip Address> <Ip Destination Mask>
[next-hop IP address] <Interface> <Interface ID> [<Metric
Value>] [track <Track Id>] [bfd-neighbor <Neighbor ID>]
[output-vrf <VRF ID>] [description <String>]
```

where:

- *bfd-neighbor:* Defines the ID of a BFD neighbor to attach the route to.

- Management ACL for TR-069 can now be configured, using the new command:

```
(config-system)# cwmp
(cwmp-tr069)# cwmp-acl <ACL name>
```

- Auto-detect mode (ADSL or VDSL) feature has been added for A/VDSL. For more information, refer to *Mediant MSBR LAN-WAN Access CLI Configuration Guide*.
- Triggering DNS entries of all types (A, AAAA, NAPTR, etc.) is now supported. For more information, refer to *Mediant MSBR IP Networking CLI Configuration Guide*.
- Hostnames can now be configured for the management ACL.
- The CLI terminal window height can now be locked. The feature can be configured through CLI using the command **default-window-height <value>** or through the Web interface using the new parameter 'Default terminal window height' (System > Management > Telnet/SSH Settings > General).
- ACL can now be applied to NAT port forwarding rules, by using the new option "match" for the **ip nat inside source** command. For example:

  -

```
(config-data)# access-list PF-ACL permit ip host 4.4.4.4 any
```

  -

```
(config-data)# ip nat inside source static tcp 192.168.0.16
same gigabitethernet 0/0 8080 match PF-ACL
```

- Vendor-specific TR-069 log string can now be configured, using the DeviceLog parameter (InternetGatewayDevice.DeviceInfo.DeviceLog).
- Sending TR-069 connection request (send-connection-request) is now also available in unprivileged CLI mode, using the new command **debug cwmp send-connection-request**.

- Auto assign self IPv6 address has been added to **ipv6 dhcp-server dns-server address** when using a DHCP server.
- The status of all interfaces (**show data interfaces atm/bvi** ...) is now also available in unprivileged CLI mode.

3.2.2 Resolved Constraints

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

Table 3-2: Resolved Constraints for Patch Version 7.20A.154.025

Incident	Description
139561	New command has been added to view DDNS status (**show data ddns**).
142487	Configuration of GRE tunnel without a source interface is not allowed in order to prevent a mismatch with the other side of the tunnel.
145580	InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.4 is not displayed in the TR-069 ACS.
142488	The configuration **qos match-map** input "NAME" VLAN 4001 appears as **qos match-map** input "NAME" internal-LAN when the **show** command is run.
142981	The RTP port is different than that advertised in the SDP body of the SIP 200 OK.
145066	The OSPF **max-metric router-lsa** command has no effect when the OSPF process is closed.
145636	The cellular, dynamic option driver is not saved after a device reset.
138373	In some cases, the Huawei 4G USB stick does not receive an IP address after a device reset.
145342	TR-069 provisioning code is lost after device reset and reverts to default ("VOIP.DATA").
142257	No option to configure dynamic learning of IPv6 NTP addresses on a PPPoE interface.
146575	QoS calibration on VDSL/EFM lines.
141714	Unable to display L2 hosts in the TR hosts table (but now possible (InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}).
142836	LAN-based host feature doesn't show all hosts.
146255	Statically configured IPv6 route does not function when a dynamic IP address is configured.
146430	PPPoE interface cannot be underlying to an ATM interface.
144064	Single Network Mode - no RTP between local extensions (FXS and IP Phone) when using VRF.
145463	Single Network Mode – ringback tone from PRT file is not played.
144063	Single Network Mode - no RTP between local extensions (FXS and IP Phone / FXS and FXS) when using the loopback interface.
143933	Upload of files through TR-069 via HTTPS fails.
144486	TR-069 change of PPPoE credentials terminates too early and causes transaction error.

Incident	Description
144197	Configuring "cellular-backup" in the backup-group when IPSec crypto map is configured, causes the cellular interface to remain in non-operational mode.
144974	The **show run** command does not display IPSec, PFS or metric parameters under the crypto map if the crypto map is not associated with the interface.
146327	IPv6 addresses on the PPPoE interface does not function with IPv4 addresses.
143282	For DHCPv6 NTP, the **ipv6 dhcp-client ntp-server** command is not displayed by the **show run** command under the PPPoE interface.

3.3 Version 7.20A.154.061

This patch version includes new features and resolved constraints.

Note:

- This version is based on MSBR Version 6.80A.347.001 (released in July 2017). In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ VDSL ISDN
  - √ VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

3.3.1 Resolved Constraints

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

Table 3-3: Resolved Constraints for Patch Version 7.20A.154.061

Incident	Description
147776	The device's DHCPv4 server now supports fast revival after reset, using DHCPREQUEST messages.
147781	TR-181 operations cause the device's CLI to freeze.
147706	AAA TACACS configuration is not saved to configuration.
147732	Issue with saving configuration of Access List with SNMP community.
146955	Device crashes on rare occasions when SNMP is used to GET QoS information.

3.4 Version 7.20A.154.078

This patch version includes new features and resolved constraints.

Note:

- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

3.4.1 New Features

New features introduced in this version include the following:

- Support for DNS with VRRP.
- Support for disabling the DHCP "dynamic" mode. When the command **no ip dhcp-server dynamic** is run, the DHCP server only answers to statically configured hosts.
- Support for the ZTE MF833V cellular dongle.

3.4.2 Resolved Constraints

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

Table 3-4: Resolved Constraints for Patch Version 7.20A.154.078

Incident	Description
146911	IPSec does not function when **ipsec access list destination** is set to "any".
147776	DHCP client does not renew its DHCP lease if the device undergoes an unplanned reset. DHCP lease renewal is possible only if the device is restarted during DHCP client lease time.
148218	When VRRP backup becomes operational, it erases dynamic leases. To prevent this, the VRRP backup device uses ARP to keep the lease of active IPs.
147955	Under some conditions, the ini file cannot be loaded using the Automatic Update mechanism (IniFileURL parameter).

3.5 Version 7.20A.200.038

This patch version includes new features and resolved constraints.

Note:

- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ SHDSL
  - √ T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

3.5.1 New Features

New features introduced in this version include the following:

- DNS lookup queries for a specific VRF. To support this feature, the following new command has been added:

  ```
  nslookup [Hostname] source data vrf [VRF Name]
  ```

- Configuration of a specific protocol bind (snmp|http|https|telnet|ssh) per management server. :

  ```
  bind source-address interface [Interface] management-servers
  [http|https|snmp|ssh|telnet]
  ```

- Support for multicast in VRFs, using the new 'pim' command:

  ```
  ip vrf <VRF Name> enable pim
  ```

- Configuration of Gratuitous ARP (GARP) per interface with timer, using the following new commands:

  ```
  (config-data)# garp timer <Seconds 1-3600, Default 60>
  (conf-if-GE 0/0)# garp enable | no garp enable
  ```

  The feature is applicable only to Gigabit and fiber WAN interface types (VLAN 1 only).

- Support for Y.1731.

- Loading License Key file through CLI (from HTTP, HTTPS, FTP, TFTP, or NFS server), using the following new command:

```
# copy feature-key from [URL]
```

- Web-based management interface (Web End-User) for end users, allowing basic configuration, for example, LAN ports settings, WAN ports settings, Wi-Fi settings, and port forwarding settings. For more information, refer to the *Mediant MSBR Basic System Setup CLI Configuration Guide.*
- Configuration of maximum path for BGP, using the following new command:

```
(config-data)# router bgp [AS Number] maximum-paths [Number]
```

3.5.2 Resolved Constraints

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

Table 3-5: Resolved Constraints for Patch Version 7.20A.200.038

Incident	Description
147996	Incorrect order of SNMP configuration through CLI prevents configuration to be applied.
149101	When the WAN interface is configured on VRF, the Auto-Update and copy features do not function if DNS resolution is required.
148592	For TR-069 management, digest authentication messages are sent in the wrong format.

3.6 Version 7.20A.202.112

This patch version includes new features and resolved constraints.

Note:

- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800B MSBR
  - √ Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ SHDSL
  - √ T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

3.6.1 New Features

New features introduced in this version include the following:

- Static WAN IP address configuration through the End User Web interface.
- The InternetGatewayDevice.Time. object is now supported for TR-098.
- The InternetGatewayDevice.Time. object is now supported for TR-069, allowing NTP to be enabled or disabled.
- The Device.Time object is now supported for TR-069.
- The Debug Capture feature now allows the naming of the captured files and sending them to specific folders on TFTP servers.
- Support for DHCPv4 Option 66 to obtain the TFTP server name and Option 67 to obtain the configuration file name, when the MSBR is a DHCP client.
- The output of the CLI commands **show system alarms** and **show system alarms-history** can now be displayed in JSON format, using the following new CLI command:

  ```
  output-format json
  ```

  The output is returned to plain text format using the following command:

  ```
  output-format plain
  ```

3.6.2 Resolved Constraints

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

Table 3-6: Resolved Constraints for Patch Version 7.20A.202.112

Incident	Description
141040	The settings of the **web-restrict** CLI command does not save after a device reset.
142368	Rate counters don't show fast-path and non fast-path traffic.
148992	Access list IPv6 rule has no 'precedence' option.
148811	WiFi "Krack" vulnerability: PTK rekeying to generate a new ANonce.
148909	Hostname resolution for VRFs is not supported. Access list is not binding to a single VRF. Hostname resolution for IPv6 is not supported. Access list FQDN does not support multiple VRFs.
148983	Automatic switching from EFM to ATM for SHDSL interfaces does not function.
150110	Bind to WAN - the internal LAN IP address appears in the **show run data** output (and should not).
150432	The **show data interface pppoe** CLI command does not show the subnet mask in its output.
150518	IPv6 cannot be enabled or disabled through TR-181.
150755	The NTP server IP address cannot be obtained from DHCP.
150763	The device doesn't renew its' IP address after a DHCP server configuration change.
150904	The device doesn't bind VLAN 100 and higher in Single Networking Mode.
150931	The device doesn't accept BGP configuration of peers in peer-group.
150932	CLI **show** commands for the Wi-Fi interface do not display "connected" status.
150963	Multiple VRRP IDs (per interface) doesn't support DHCPv4.
151017	The **copy** command fails first time with the error "(6) Could not resolve host".
152270	The configuration by the **coders-and-profiles** command is displayed in the wrong location in the CLI script, which causes an error when applying the script to the device.
152974	The license for the Zero Configuration feature is not retained after a hardware (button) reset.
153155	Debug Recording cannot be sent to the WAN over a non-default VRF.
153545	The **show data interface <Interface Name>** command does not show the subnet mask when the IP address is obtained through DHCP.
152984	After clicking the Edit button in the SIP Interfaces table, the network interface doesn't appear even though it is configured.
149652	The Auto Provisioning process doesn't complete configuration file load.

Incident	Description
153235	For the configuration of **sip-definition account**, no space appears before "obscured" in the obscured password (e.g., password /cnHyzQwOzo9NjY/OA==obscured").
152930	When DHCPv4 is configured with a static IPv6 address, the **show data ipv6 interface brief** command does not display IPv6 status properly. DHCP client configuration on WAN copper disables IPv6 protocol.
152875	A WAN IPv6 cannot be assigned to a Media Realm in the Web interface.
152395	The **show data ip igmp proxy groups** command displays an error.
150707	In TR-069, no support for MTU fragmentation.

4 Capacity for Gateways & SBCs

This section provides capacity for the Gateway and SBC products.

4.1 SIP, Media and Registered User Capacity

The following table lists the maximum, concurrent SIP signaling sessions, concurrent media sessions, and registered users per product.

Table 4-1: Capacity for Signaling, Media and Registered Users per Product

Product	Signaling Capacity		Media Sessions			
	SIP Sessions	Registered Users	Session Type	RTP Sessions	SRTP Sessions	Detailed Media Capabilities
Mediant 500	250	1,500	Hybrid	250	200	Transcoding: n/a GW: Table 4-4
			GW-Only	30	30	
Mediant 500L	60	200	Hybrid	60	60	Transcoding: n/a GW: Table 4-6
			GW-Only	8	8	
Mediant 800A	60	200	Hybrid	60	60	GW & Transcoding: Table 4-8 SBC Only: Table 4-7
Mediant 800B	250	1,500	Hybrid	250	250	GW & Transcoding: Table 4-8 SBC Only: Table 4-7
			GW-Only	64	64	
Mediant 800C	400	2,000	Hybrid	400	300	GW & Transcoding: Table 4-10
			GW-Only	124	124	
Mediant 1000B	150	600	Hybrid	150	120	Transcoding: Table 4-14 GW: Tables Table 4-11, Table 4-12, Table 4-13
			GW-Only	192	140	
MP-1288	588	350	Hybrid	588	438	Transcoding: n/a GW: Table 4-15
			SBC-Only	300	300	
			GW-Only	288	288	
Mediant 2600	600	8,000	SBC-Only	600	600	Table 4-16
Mediant 4000	5,000	20,000	SBC-Only	5,000	3,000	Table 4-17

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP Sessions	SRTP Sessions	Detailed Media Capabilities
Mediant 4000B			5,000	20,000	SBC-Only	5,000	5,000	Table 4-18
Mediant 9000	Hyper-Threading (HT) Disabled		24,000	180,000	SBC-Only	16,000	16,000	Table 4-19
			24,000	0	SBC-Only	24,000	16,000	Table 4-19
	SIP Performance Profile (HT Enabled)		30,000	300,000	SBC-Only	30,000	16,000	-
			55,000	0	SBC-Only	55,000	18,000	-
	DSP Performance Profile (HT Enabled)		50,000	0	SBC-Only	50,000	18,000	Table 4-19
	SRTP Performance Profile (HT Enabled)		50,000	0	SBC-Only	50,000	40,000	-
Mediant 9000 with Media Transcoders (MT type)			24,000	180,000	SBC-Only	24,000*	16,000**	Table 4-21
Mediant CE	AWS / EC2		40,000	0	SBC-Only	40,000	40,000	Forwarding: Table 4-22 Transcoding: Table 4-23
			20,000	100,000	SBC-Only	20,000	20,000	
Mediant VE	VMware	1 vCPU, 2-GB RAM	250	1,000	SBC-Only	250	250	-
		1/2/4 vCPU, 8-GB RAM	3,000	15,000	SBC-Only	3,000	2,000	1 vCPU (n/a) 2 vCPU (Table 4-24) 4 vCPU (Table 4-26)
		4/8 vCPU 16-GB RAM	9,000	75,000	SBC-Only	6,000	5,000	Table 4-28
	OpenStack KVM	1 vCPU 2-GB RAM	250	1,000	SBC-Only	250	250	-
		1/2/4 vCPU 4-GB RAM	1,800	9,000	SBC-Only	1,800	1,400	1 vCPU (n/a) 2 vCPU (Table 4-24) 4 vCPU (Table 4-26)
		4/8 vCPU 16-GB RAM	4,000	75,000	SBC-Only	2,700	2,700	Table 4-28
		8 vCPU 16-GB RAM SR-IOV Intel NICs	24,000	0	SBC-Only	24,000	10,000	-
		8 vCPU 32-GB RAM SR-IOV Intel NICs	24,000	75,000	SBC-Only	24,000	10,000	-

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP Sessions	SRTP Sessions	Detailed Media Capabilities
	Hyper-V	1 vCPU 2-GB RAM	250	1,000	SBC-Only	250	250	-
		1/2/4 vCPU 4-GB RAM	900	10,000	SBC-Only	600	600	1 vCPU (n/a) 2 vCPU (Table 4-33) 4 vCPU (Table 4-35)
	AWS / EC2	r4.large	2,500	20,000	SBC-Only	2,500	2,500	-
		c4.2xlarge	2,000	75,000	SBC-Only	2,000	2,000	Table 4-30
		c4.8xlarge	3,200	75,000	SBC-Only	3,200	3,200	Table 4-31
Mediant VE with Media Transcoders	OpenStack KVM	8 vCPU 64-GB RAM SR-IOV Intel NICs	24,000	75,000	SBC-Only	24,000	12,000	MT-type (Table 4-37) vMT-type (Table 4-38)
Mediant SE	DL320e G8 4-cores 3.1 GHz 16-GB RAM		15,000	75,000	SBC-Only	10,000	6,500	-
	DL360p G8 20-cores 2.8 GHz 64-GB RAM - or - DL360 G9 8-cores 2.6 GHz 32-GB RAM		24,000	120,000	SBC-Only	16,000	14,000	-
			24,000	0	SBC-Only	24,000	14,000	-

Notes:

- The figures listed in the table are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, please contact your AudioCodes sales representative.
- "GW" refers to Gateway functionality.
- "SIP Sessions" refers to the maximum concurrent signaling sessions for both SBC and Gateway (when applicable). Whenever signaling sessions is above the maximum media sessions, the rest of the signaling sessions can be used for Direct Media.
- "Session Type" refers to Gateway-only sessions, SBC-only sessions, or Hybrid sessions which is any mixture of SBC and Gateway sessions under the limitations of Gateway-only or SBC-only maximum values.
- "RTP Sessions" refers to the maximum concurrent RTP sessions when all sessions are RTP-RTP (for SBC sessions) or TDM-RTP (for Gateway sessions).
- "SRTP Sessions" refers to the maximum concurrent SRTP sessions when all sessions are RTP-SRTP (for SBC sessions) or TDM-SRTP (for Gateway sessions).
- "Registered Users" refers to the maximum number of users that can be registered with the device. This applies to the supported application (SBC or CRP).
- Regarding signaling, media, and transcoding session resources:
    - A signaling session is a SIP dialog session between two SIP entities, traversing the SBC and using one signaling session resource.
    - A media session is an audio (RTP or SRTP), fax (T.38), or video session between two SIP entities, traversing the SBC and using one media session resource.
    - A gateway session (i.e. TDM-RTP or TDM-SRTP) is also considered as a media session for the calculation of media sessions. In other words, the maximum Media Sessions specified in the table refer to the sum of Gateway and SBC sessions.
    - In case of direct media (i.e., Anti-tromboning / Non-Media Anchoring), where only SIP signaling traverses the SBC and media flows directly between the SIP entities, only a signaling session resource is used. Thus, for products with a greater signaling session capacity than media, even when media session resources have been exhausted, additional signaling sessions can still be handled for direct-media calls.
    - For call sessions requiring transcoding, one transcoding session resource is also used. For example, for a non-direct media call in which one leg uses G.711 and the other leg G.729, one signaling resource, one media session resource, and one transcoding session resource is used.
- Capacity of the Cloud Resilience Package (CRP) application is listed under "Registered Users".
- Capacity of the Lync Analog Device (LAD) application is listed under "Media Sessions".

- **MP-1288:** The maximum number of media and signaling sessions is the summation of the maximum 300 RTP-to-RTP (SBC) sessions and the maximum 288 TDM-RTP (Gateway) sessions. The maximum number of SRTP sessions is the summation of the maximum 150 RTP-to-SRTP (SBC) sessions and the maximum 288 TDM-SRTP (Gateway) sessions.
- **Hyper-Threading (HT) on Mediant 9000 SBC:** HT was initially enabled on Mediant 9000 with 10G ports or Mediant 9000 Rev. B. To enable HT on other Mediant 9000 platforms, please refer to the *Mediant 9000 SBC Installation Manual*.
- **Mediant 9000 SBC or Mediant VE SBC with Media Transcoders:** The following limitations exist:
  * To allow DSP capabilities (such as transcoding), the Performance Profile parameter must be configured to the DSP profile. Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP figure specified in the table. As result, if all sessions are with transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding specified in the table.
  ** The maximum SRTP-RTP sessions is also effected by the above limitations. For example, if all sessions are using transcoding, the maximum number of SRTP-RTP sessions is also limited by half of the maximum RTP-RTP sessions without transcoding.
- **Mediant VE SBC with vMT-type Media Transcoder**: The host running the vMT virtual machine requires the following configuration:
  - √ At least 2.8 GHz CPU with Intel® AVX support
  - √ SR-IOV enabled NICs
  - √ KVM environment
  - √ 8 hyper-threaded vCPUs should be allocated to the vMT virtual machine (4 physical cores)
  - √ 4-GB RAM should be allocated to the vMT virtual machine
- **Mediant VE SBC and vMT-type Media Transcoder:** Codec-transcoding functionality is supported only on Intel CPUs with AVX enhancement. In addition, AVX support must be reflected on the vCPU of the SBC virtual machine.
- Mediant VE SBC with Media Transcoder Cluster is currently supported only on the OpenStack KVM hypervisor.
- **Mediant CE:** This is based on the following AWS instances:
  - √ Signaling Components (SC): r4.2xlarge
  - √ Media Components (MC) - forwarding only: r4.large
  - √ Media Components (MC) - forwarding and transcoding: c4.4xlarge

4.2 Capacity per Feature

The table below lists maximum concurrent SBC/Gateway sessions/users per feature:

Table 4-2: Capacity per Feature

Product	WebRTC Sessions	One-Voice Resiliency (OVR) Users	SIPRec Sessions
Mediant 500	-	-	200
Mediant 500L	-	-	50
Mediant 800B	100	100	200
Mediant 800C	100	100	200
MP-1288	-	-	-
Mediant 1000B	-	50	-
Mediant 2600	600	-	300
Mediant 4000	1,000	-	2,500
Mediant 9000	5,000	-	20,000 (16,000 without HyperThreading)
Mediant VE/SE	-	2,000 (Only Mediant VE)	12,000*
Mediant CE	5,000	-	20,000

Note:

- The figures in the table above for SIPRec capacity assume that there are no other concurrent, regular (non-SIPRec) voice sessions.
- For Mediant VE SBC, SIPRec capacity depends on instance size.

4.3 Detailed Capacity

This section provides detailed capacity figures.

4.3.1 Mediant 500 E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500 E-SBC are shown in the tables below.

Table 4-3: Mediant 500 E-SBC (Non-Hybrid) SBC Capacity

Hardware Configuration	TDM-RTP Sessions				Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders			
		G.722	AMR-WB (G.722.2)	SILK-WB	
SBC	n/a	n/a	n/a	n/a	250

Table 4-4: Mediant 500 Hybrid E-SBC (with Gateway) Media & SBC Capacity

Hardware Configuration	TDM-RTP Sessions				Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders			
		G.722	AMR-WB (G.722.2)	SILK-WB	
1 x E1/T1	30/24	√	-	-	220/226
	26/24	√	√	-	224/226
	26/24	√	√	√	224/226

4.3.2 Mediant 500L Gateway and E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500L Gateway and E-SBC is shown in the tables below.

Table 4-5: Mediant 500L E-SBC (Non-Hybrid) SBC Capacity

Hardware Configuration	TDM-RTP Sessions			Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders		
		G.722	AMR-WB (G.722.2)	
SBC	n/a	n/a	n/a	60

Table 4-6: Mediant 500L Hybrid E-SBC (with Gateway) Media & SBC Capacity

Hardware Configuration	DSP Channels Allocated for PSTN	Additional Coders				Max. SBC Sessions
		Narrowband	Wideband			
		Opus-NB	G.722	AMR-WB (G.722.2)	Opus-WB	
2 x BRI / 4 x BRI	4/8	-	-	-	-	56/52
	4/8	-	√	-	-	56/52
	4/6	√	-	√	-	56/54
	4	-	-	-	√	56

4.3.3 Mediant 800 Gateway & E-SBC

This section describes capacity for Mediant 800 Gateway & E-SBC.

4.3.3.1 Mediant 800A/B Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800A/B Gateway & E-SBC are shown in the tables below.

Table 4-7: Mediant 800A/B Gateway & E-SBC SBC Session Capacity per Capabilities (SBC Only)

H/W Configuration	DSP Channels for PSTN	SBC Transcoding Sessions								Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2	Mediant 800A	Mediant 800B
		Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-WB				
SBC	n/a	-	-	-	-	-	-	57	48	60	400
	n/a	-	-	√	-	-	-	51	42	60	400
	n/a	-	-	-	-	√	-	39	33	60	400
	n/a	-	-	-	√	-	-	36	30	60	400
	n/a	-	-	-	-	-	√	27	24	60	400
	n/a	√	-	-	-	-	-	27	24	60	400
	n/a	-	√	-	-	-	-	21	21	60	400

Note: "Max. SBC Sessions" for Mediant 800B applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 4.1).

Table 4-8: Mediant 800A/B Gateway & E-SBC Channel Capacity per Capabilities (with Gateway)

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		Mediant 800A	Mediant 800B
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1					
2 x E1/T1	60/48	-	-	-	-	-	-	-	3/15	2/13	-	0/12	340/352
2 x T1	48	-	-	-	-	-	-	√	11	9	-	12	352
1 x E1/T1 & 8 x FXS/FXO Mix	38/32	-	-	-	-	-	-	-	22/28	18/22	-	22/28	362/368
	38/32	-	-	√	-	-	-	-	8/12	7/11	-	22/28	362/368
1 x E1/T1	30/24	-	-	√	-	-		√	14/18	12/16	-	30/36	370/376
1 x E1 & 4 x BRI	38	-	-	-	-	-	-	-	22	18	-	22	362
1 x E1 & 4 x FXS	34	-	-	-	-	-	-	-	26	21	-	26	366
2 x E1 & 4 x FXS	64	-	-	-	-	-	-	-	0	0	-	0	336
4 x BRI & 4 x FXS & 4 x FXO	16	-	-	-	-	-	-	-	5	4	-	44	384
8 x BRI & 4 x FXS	20	-	-	-	-	-	-	-	1	1	-	40	380
8 x BRI	16	-	-	-	-	-	-	-	5	4	-	44	384

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		Mediant 800A	Mediant 800B
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1					
12 x FXS	12	-	-	√	-	-	-	√	3	3	-	48	388
4 x FXS & 8 x FXO	12	-	-	√	-	-	-	-	3	3	-	48	388
8 x FXS & 4 x FXO	12	-	-	√	-	-	-	-	3	3	-	48	388
4 x BRI & 4 x FXS	12	-	-	√	-	-	-	-	3	3	-	48	388
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	-	7	5	6	52	392
	8	-	-	√	-	-	-	-	6	6	-	52	392
4 x BRI	8	-	-	-	-	-	-	-	7	5	6	52	392
	8	-	-	√	-	-	-	-	6	6	-	52	392
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	-	17/15 /14	14/13/ 11	-	58/56/54	398/396/ 394
	2/4/6	-	-	√	-	-	-	-	11/10 /8	10/8/7	-	58/56/54	398/396/ 394
4 x FXS or 4 x FXO	4	-	-	√	-	-	-	√	10	8	-	56	396
	4	√	-	-	-	-	-	-	12	10	4	56	396
	4	-	-	√	-	-	-	-	6	6	4	56	396

Telephony Interface Assembly	**DSP Channels Allocated for PSTN**	**SBC Transcoding Sessions**									**Conf. Participants**	**Max. SBC Sessions**	
		From Profile 2 with Additional Advanced DSP Capabilities							**To Profile 1**	**To Profile 2**		**Mediant 800A**	**Mediant 800B**
		AMR-NB / G.722	**AMR-WB (G.722.2)**	**SILK-NB**	**SILK-WB**	**Opus-NB**	**Opus-WB**	**V.150.1**					
	4	-	√	√	-	-	-	-	4	4	4	56	396
	4	-	√	√	√	-	-	-	3	3	4	56	396
	4	-	-	-	-	√	-	-	1	0	4	56	396
	4	-	-	-	-	-	√	-	0	0	3	56	396
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	-	19	16	-	60	400

Notes:

- "Max. SBC Sessions" for Mediant 800B applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 4.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729, and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g. Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

4.3.3.2 Mediant 800C Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800C Gateway & E-SBC are shown in the tables below.

Table 4-9: Mediant 800C Gateway & E-SBC SBC Session Capacity per Capabilities (SBC Only)

H/W Configuration	SBC Transcoding Sessions								Max. SBC Sessions
	From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2	
	Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-WB			
SBC	-	-	-	-	-	-	114	96	400
	-	-	√	-	-	-	102	84	400
	-	-	-	-	√	-	78	66	400
	-	-	-	√	-	-	72	60	400
	-	-	-	-	-	√	54	48	400
	√	-	-	-	-	-	54	48	400
	-	√	-	-	-	-	42	42	400

Note: "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 4.1).

Table 4-10: Mediant 800C Gateway & E-SBC SBC Session Capacity per Capabilities with Gateway

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions				Max SBC Sessions
		From Profile 2	From Profile 2 with SILK NB / iLBC	To Profile 1	To Profile 2	
4 x E1/T1 + 4 x FXS	124/100	√	-	2/23	2/18	276/300
2 x E1/T1 + 4 x FXS	64/52	√	-	0/10	0/8	336/348
Not in use		√	-	114	96	400
		-	√	78	66	400

Notes:

- "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 4.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729, and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g. Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

4.3.4 Mediant 1000B Gateway & E-SBC

This section lists the channel capacity and DSP templates for Mediant 1000B Gateway & E-SBC DSP.

Notes:

- The maximum number of channels on any form of analog, digital, and MPM module assembly is 192. When the device handles both SBC and Gateway call sessions, the maximum number of total sessions is 150. When the device handles SRTP, the maximum capacity is reduced to 120.
- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes sales representative.

4.3.4.1 Analog (FXS/FXO) Interfaces

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

Table 4-11: Channel Capacity per DSP Firmware Template for Mediant 1000B Analog Series

	DSP Template	
	0, 1, 2, 4, 5, 6	10, 11, 12, 14, 15, 16
	Number of Channels	
	4	3
Voice Coder		
G.711 A/Mu-law PCM	√	√
G.726 ADPCM	√	√
G.723.1	√	√
G.729 A, B	√	√
G.722	-	√

4.3.4.2 BRI Interfaces

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

Table 4-12: Channel Capacity per DSP Firmware Template for Mediant 1000B BRI Series

	DSP Template					
	0, 1, 2, 4, 5, 6			10, 11, 12, 14, 15, 16		
	Number of BRI Spans					
	4	8	20	4	8	20
	Number of Channels					
	8	16	40	6	12	30
Voice Coder						
G.711 A/Mu-law PCM	√			√		
G.726 ADPCM	√			√		
G.723.1	√			√		
G.729 A, B	√			√		
G.722	-			√		

4.3.4.3 E1/T1 Interfaces

The channel capacity per DSP firmware template for E1/T1 interfaces is shown in the table below.

Table 4-13: Channel Capacity per DSP Firmware Templates for Mediant 1000B E1/T1 Series

	DSP Template																								
	0 or 10					1 or 11					2 or 12					5 or 15					6 or 16				
	Number of Spans																								
	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8
	Number of Channels																								
Default Settings	31	62	120	182	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With 128-ms Echo Cancellation	31	60	100	160	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With IPM Features	31	60	100	160	192	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100	160	192
Voice Coder																									
G.711 A-Law/M-Law PCM	✓					✓					✓					✓					✓				
G.726 ADPCM	✓					✓					✓					✓					-				
G.723.1	✓					-					-					-					-				
G.729 A/B	✓					✓					✓					✓					✓				
GSM FR	✓					✓					-					-					-				
MS GSM	✓					✓					-					-					-				
iLBC	-					-					-					✓					-				
EVRC	-					-					✓					-					-				

	DSP Template																								
	0 or 10					1 or 11					2 or 12					5 or 15					6 or 16				
	Number of Spans																								
	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8
	Number of Channels																								
Default Settings	31	62	120	182	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With 128-ms Echo Cancellation	31	60	100	160	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With IPM Features	31	60	100	160	192	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100	160	192
Voice Coder																									
QCELP	-					-					✓					-					-				
AMR	-					✓					-					-					-				
GSM EFR	-					✓					-					-					-				
G.722	-					-					-					-					✓				
Transparent	✓					✓					✓					✓					✓				

Note: "IPM Features" refers to Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD).

4.3.4.4 Media Processing Interfaces

The transcoding session capacity according to DSP firmware template (per MPM module) is shown in the table below.

Notes:

- The device can be housed with up to four MPM modules.
- The MPM modules can only be housed in slots 1 through 5.

Table 4-14: Transcoding Sessions Capacity per MPM According to DSP Firmware Template for Mediant 1000B

	DSP Template				
	0 or 10	1 or 11	2 or 12	5 or 15	6 or 16
IPM Detectors Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD)	**Number of Transcoding Sessions per MPM Module**				
-	24	16	12	12	20
✓	20	-	-	-	20
Voice Coder					
G.711 A-law / Mμ-law PCM	✓	✓	✓	✓	✓
G.726 ADPCM	✓	✓	✓	✓	-
G.723.1	✓	-	-	-	-
G.729 A, B	✓	✓	✓	✓	✓
GSM FR	✓	✓	-	-	-
MS GSM	✓	✓	-	-	-
iLBC	-	-	-	✓	-
EVRC	-	-	✓	-	-

	DSP Template				
	0 or 10	1 or 11	2 or 12	5 or 15	6 or 16
IPM Detectors Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD)	**Number of Transcoding Sessions per MPM Module**				
-	24	16	12	12	20
✓	20	-	-	-	20
Voice Coder					
QCELP	-	-	✓	-	-
AMR	-	✓	-	-	-
GSM EFR	-	✓	-	-	-
G.722	-	-	-	-	✓
Transparent	✓	✓	✓	✓	✓

4.3.5 MP-1288 Analog Gateway & E-SBC

Session capacity includes Gateway sessions as well as SBC sessions without transcoding capabilities. The maximum capacity of Gateway sessions for MP-1288 Gateway & E-SBC is shown in the table below.

Table 4-15: MP-1288 Gateway Sessions Capacity

Coder	Gateway Sessions Capacity	
	Single FXS Blade	Fully Populated (4 x FXS Blades)
Basic: G.711, G.729A/B, G.723.1, G.726 / G.727 ADPCM	72	288
G.722	72	288
AMR-NB	72	288
Opus-NB	60	240

Note:

- Quality Monitoring and Noise Reduction are not supported.
- SRTP is supported on all configurations.

4.3.6 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 4.1 on page 181. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below:

Table 4-16: Transcoding Capacity per Coder-Capability Profile for Mediant 2600 E-SBC

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Without MPM4**	**With MPM4**
Profile 1	Profile 1	400	600
Profile 2	Profile 1	300	600
Profile 2	Profile 2	250	600
Profile 1	Profile 2 + AMR-NB / G.722	275	600
Profile 2	Profile 2 + AMR-NB / G.722	225	600
Profile 1	Profile 2 + iLBC	175	575
Profile 2	Profile 2 + iLBC	150	500
Profile 1	Profile 2 + AMR-WB (G.722.2)	200	600
Profile 2	Profile 2 + AMR-WB (G.722.2)	175	525
Profile 1	Profile 2 + SILK-NB	200	600
Profile 2	Profile 2 + SILK-NB	175	525
Profile 1	Profile 2 + SILK-WB	100	350
Profile 2	Profile 2 + SILK-WB	100	350
Profile 1	Profile 2 + Opus-NB	125	425
Profile 2	Profile 2 + Opus-NB	125	375

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Without MPM4**	**With MPM4**
Profile 1	Profile 2 + Opus-WB	100	300
Profile 2	Profile 2 + Opus-WB	75	275

Notes:

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

4.3.7 Mediant 4000 SBC

The maximum number of supported SBC sessions is listed in Section 4.1 on page 181. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 4-17: Transcoding Capacity per Coder-Capability Profile for Mediant 4000 SBC

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Without MPM8**	**With MPM8**
Profile 1	Profile 1	800	2,400
Profile 2	Profile 1	600	1,850
Profile 2	Profile 2	500	1,550
Profile 1	Profile 2 + AMR-NB / G.722	550	1,650
Profile 2	Profile 2 + AMR-NB / G.722	450	1,350
Profile 1	Profile 2 + iLBC	350	1,150
Profile 2	Profile 2 + iLBC	300	1,000
Profile 1	Profile 2 + AMR-WB (G.722.2)	400	1,200
Profile 2	Profile 2 + AMR-WB (G.722.2)	350	1,050
Profile 1	Profile 2 + SILK-NB	400	1,200
Profile 2	Profile 2 + SILK-NB	350	1,050
Profile 1	Profile 2 + SILK-WB	200	700
Profile 2	Profile 2 + SILK-WB	200	700
Profile 1	Profile 2 + Opus-NB	250	850
Profile 2	Profile 2 + Opus-NB	250	750

Session Coders		Max. Sessions	
From Coder Profile	**To Coder Profile**	**Without MPM8**	**With MPM8**
Profile 1	Profile 2 + Opus-WB	200	600
Profile 2	Profile 2 + Opus-WB	150	550

Notes:

- *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

The device can handle up to 5,000 fax detections, answer detections (AD), answering machine detections (AMD), beep detections, and Call Progress Tone detections, with the following assumptions:

- Timeout for fax detection is 10 seconds (default), after which fax detection is turned off and the call is resumed without the fax detector.
- Fax detection is applied on both legs of the SBC call.
- Minimum call duration is 100 seconds.
- AD, AMD, beep detection, and Call Progress Tone detection is only on one leg of the SBC call (should this not be the case, capacity figures will be reduced)

4.3.8 Mediant 4000B SBC

The maximum number of supported SBC sessions is listed in Section 4.1 on page 181. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 4-18: Transcoding Capacity per Coder-Capability Profile for Mediant 4000B SBC

Session Coders		Number of Sessions				
From Coder Profile	**To Coder Profile**	**Without MPM**	**1 x MPM8B**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 1	Profile 1	800	2,400	3,250	5,000	5,000
Profile 2	Profile 1	600	1,850	2,450	4,350	5,000
Profile 2	Profile 2	500	1,550	2,100	3,650	5,000
Profile 1	Profile 2 + AMR-NB / G.722	550	1,650	2,200	3,850	5,000
Profile 2	Profile 2 + AMR-NB / G.722	450	1,350	1,800	3,150	4,550
Profile 1	Profile 2 + iLBC	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + iLBC	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + AMR-WB (G.722.2)	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + AMR-WB (G.722.2)	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + SILK-NB	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + SILK-NB	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + SILK-WB	200	700	950	1,650	2,400
Profile 2	Profile 2 + SILK-WB	200	700	950	1,650	2,400
Profile 1	Profile 2 + Opus-NB	250	850	1,150	2,000	2,850
Profile 2	Profile 2 + Opus-NB	250	750	1,050	1,800	2,600
Profile 1	Profile 2 + Opus-WB	200	600	850	1,500	2,150

Session Coders		**Number of Sessions**				
From Coder Profile	**To Coder Profile**	**Without MPM**	**1 x MPM8B**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 2	Profile 2 + Opus-WB	150	550	750	1,300	1,900

Notes:

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPMB is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

The device can handle up to 5,000 fax detections, answer detections (AD), answering machine detections (AMD), beep detections, and Call Progress Tone detections, with the following assumptions:

- Timeout for fax detection is 10 seconds (default), after which fax detection is turned off and the call is resumed without the fax detector.
- Fax detection is applied on both legs of the SBC call.
- Minimum call duration is 100 seconds.
- AD, AMD, beep detection, and Call Progress Tone detection is only on one leg of the SBC call (should this not be the case, capacity figures will be reduced)

4.3.9 Mediant 9000 SBC

The maximum number of supported SBC sessions is listed in Section 4.1 on page 181. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 4-19: Transcoding Capacity per Coder-Capability Profile for Mediant 9000 SBC

Session Coders		Number of Sessions			
From Coder Profile	To Coder Profile	Without Hyper-Threading		With Hyper-Threading	
		Extended	Basic	Extended	Basic
Profile 1	Profile 1	2,525	3,025	3,875	6,575
Profile 2	Profile 1	1,325	1,500	1,700	2,125
Profile 2	Profile 2	900	1,000	1,100	1,275
Profile 1	Profile 2 + AMR-NB / G.722	1,300	1,500	1,625	2,075
Profile 2	Profile 2 + AMR-NB / G.722	900	1,000	1,050	1,225
Profile 1	Profile 2 + AMR-WB (G.722.2)	475	500	575	600
Profile 2	Profile 2 + AMR-WB	400	425	475	500
Profile 1	Profile 2 + SILK-NB	1,175	1,300	1,450	1,700
Profile 2	Profile 2 + SILK-NB	825	900	975	1,100
Profile 1	Profile 2 + SILK-WB	750	775	950	1,000
Profile 2	Profile 2 + SILK-WB	600	625	725	750
Profile 1	Profile 2 + Opus-NB	750	825	900	1,050
Profile 2	Profile 2 + Opus-NB	600	650	700	775
Profile 1	Profile 2 + Opus-WB	575	625	700	800
Profile 2	Profile 2 + Opus-WB	475	525	575	625

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-20: Channel Capacity per Detection Feature for Mediant 9000 SBC

Special Detection Features	Number of Sessions
Fax Detection	24,000
AD/AMD/Beep Detection	24,000
CP Detection	24,000
Jitter Buffer	2,225

4.3.10 Mediant 9000 SBC with Media Transcoders

Mediant 9000 SBC with Media Transcoders allows increasing the number of transcoding sessions by using Media Transcoders. The maximum number of transcoding sessions depends on the following:

- The number of Media Transcoders in the media transcoding cluster.
- The cluster operation mode (Best-Effort or Full-HA mode).
- The maximum transcoding sessions that the Mediant 9000 SBC is capable of performing. Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP value specified in the table. As a result, if all sessions are with transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding as specified in Table 4-1.

The following table lists maximum transcoding sessions capacity of a single Media Transcoder.

Table 4-21: Transcoding Capacity per Profile for a Single Media Transcoder

Session Coders		Number of Sessions		
From Coder Profile	**To Coder Profile**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 1	Profile 1	2875	5000	5000
Profile 2	Profile 1	2300	4025	5000
Profile 2	Profile 2	1800	3175	4550
Profile 1	Profile 2 + AMR-NB / G.722	2000	3525	5000
Profile 2	Profile 2 + AMR-NB / G.722	1625	2850	4075
Profile 1	Profile 2 + AMR-WB (G.722.2)	1425	2500	3600
Profile 2	Profile 2 + AMR-WB (G.722.2)	1225	2175	3100
Profile 1	Profile 2 + SILK-NB	1425	2500	3600
Profile 2	Profile 2 + SILK-NB	1225	2175	3100
Profile 1	Profile 2 + SILK-WB	850	1500	2150

Session Coders		Number of Sessions		
From Coder Profile	**To Coder Profile**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 2	Profile 2 + SILK-WB	850	1500	2150
Profile 1	Profile 2 + Opus-NB	1050	1825	2625
Profile 2	Profile 2 + Opus-NB	950	1675	2400
Profile 1	Profile 2 + Opus-WB	750	1325	1900
Profile 2	Profile 2 + Opus-WB	650	1175	1675

Notes:

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM12B is a Media Processing Module in the Media Transcoder that provides additional DSPs, allowing higher capacity.
- For best cluster efficiency, all Media Transcoders in the Cluster should populate the same number of MPM12Bs.

4.3.11 Mediant Cloud Edition SBC

The Media Components (MC) in the media cluster of the Mediant CE must all be of the same instance type: either forwarding-only, or forwarding and transcoding. A maximum of 21 MCs can be used.

4.3.11.1 Forwarding Sessions

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

Table 4-22: Forwarding Capacity per MC Instance Type

MC Instance Type	Number of Forwarding Sessions
r4.large	2,500
c4.4xlarge	3,200

Note: Forwarding performance was tested in AWS Ireland Region.

4.3.11.2 Transcoding Sessions

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

Table 4-23: Transcoding Capacity per c4.4xlarge MC

Session Coders		Number of Sessions	
From Coder Profile	To Coder Profile	Extended	Basic
Profile 1	Profile 1	2,425	3,200
Profile 2	Profile 1	1,050	1,325

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 2	Profile 2	675	800
Profile 1	Profile 2 + AMR-NB / G.722	1,000	1,300
Profile 2	Profile 2 + AMR-NB / G.722	650	750
Profile 1	Profile 2 + AMR-WB (G.722.2)	350	375
Profile 2	Profile 2 + AMR-WB	275	300
Profile 1	Profile 2 + SILK-NB	900	1,050
Profile 2	Profile 2 + SILK-NB	600	675
Profile 1	Profile 2 + SILK-WB	575	625
Profile 2	Profile 2 + SILK-WB	450	450
Profile 1	Profile 2 + Opus-NB	550	650
Profile 2	Profile 2 + Opus-NB	425	475
Profile 1	Profile 2 + Opus-WB	425	500
Profile 2	Profile 2 + Opus-WB	350	375

Notes:

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

4.3.12 Mediant Server Edition SBC

Note: Mediant Server Edition SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing.

4.3.13 Mediant Virtual Edition SBC

The maximum number of supported SBC sessions is listed in Section 4.1 on page 181. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required (DSP Performance Profile), the number of sessions that can use DSP capabilities is reduced, as shown in the tables in this section.

4.3.13.1 Mediant VE SBC for OpenStack and VMware Hypervisors

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

4.3.13.1.1 Two-vCPU Mediant VE SBC

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

Table 4-24: Transcoding Capacity for 2-vCPU Mediant VE SBC on OpenStack/VMware

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 1	250	300
Profile 2	Profile 1	125	150
Profile 2	Profile 2	75	100
Profile 1	Profile 2 + AMR-NB / G.722	125	150

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

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds

- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-25: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on OpenStack/VMware

Special Detection Features	Number of Sessions
Fax Detection	2,400
AD/AMD/Beep Detection	2,400
CP Detection	2,400
Jitter Buffer	200

4.3.13.1.2 Four-vCPU Mediant VE SBC

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

Table 4-26: Transcoding Capacity for 4-vCPU Mediant VE SBC on OpenStack/VMware

Session Coders		Number of Sessions	
From Coder Profile	To Coder Profile	Extended	Basic
Profile 1	Profile 1	750	900
Profile 2	Profile 1	375	450
Profile 2	Profile 2	250	300
Profile 1	Profile 2 + AMR-NB / G.722	375	450
Profile 2	Profile 2 + AMR-NB / G.722	250	300
Profile 1	Profile 2 + AMR-WB	125	150

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 2	Profile 2 + AMR-WB	100	125
Profile 1	Profile 2 + SILK-NB	350	375
Profile 2	Profile 2 + SILK-NB	225	250
Profile 1	Profile 2 + SILK-WB	225	225
Profile 2	Profile 2 + SILK-WB	175	175
Profile 1	Profile 2 + Opus-NB	225	250
Profile 2	Profile 2 + Opus-NB	175	175
Profile 1	Profile 2 + Opus-WB	175	175
Profile 2	Profile 2 + Opus-WB	125	150

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of

the SBC call (should this not be the case, figures will be reduced)

- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-27: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on OpenStack/VMware

Special Detection Features	Number of Sessions
Fax Detection	7,200
AD/AMD/Beep Detection	7,200
CP Detection	7,200
Jitter Buffer	650

4.3.13.1.3 Eight-vCPU Mediant VE SBC

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

Table 4-28: Transcoding Capacity for 8-vCPU Mediant VE SBC on OpenStack/VMware

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

Session Coders		**Number of Sessions**	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 2	Profile 2 + SILK-NB	325	350
Profile 1	Profile 2 + SILK-WB	300	300
Profile 2	Profile 2 + SILK-WB	225	250
Profile 1	Profile 2 + Opus-NB	300	325
Profile 2	Profile 2 + Opus-NB	225	250
Profile 1	Profile 2 + Opus-WB	225	250
Profile 2	Profile 2 + Opus-WB	175	200

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-29: Channel Capacity per Detection Feature for 8-vCPU Mediant VE SBC on OpenStack/VMware

Special Detection Features	Number of Sessions
Fax Detection	9,600
AD/AMD/Beep Detection	9,600
CP Detection	9,600
Jitter Buffer	875

4.3.13.2 Amazon AWS EC2

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

Table 4-30: Transcoding Capacity for Mediant VE SBC on c4.2xlarge

Session Coders		Number of Sessions	
From Coder Profile	To Coder Profile	Extended	Basic
Profile 1	Profile 1	1,164	1,524
Profile 2	Profile 1	618	750
Profile 2	Profile 2	420	498

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

Table 4-31: Transcoding Capacity for Mediant VE SBC on c4.8xlarge

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 1	3,200	3,200
Profile 2	Profile 1	3,200	3,200

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 2	Profile 2	2,225	2,650
Profile 1	Profile 2 + AMR-NB / G.722	2,600	3,025
Profile 2	Profile 2 + AMR-NB / G.722	1,875	2,175
Profile 1	Profile 2 + AMR-WB	925	950
Profile 2	Profile 2 + AMR-WB	825	850
Profile 1	Profile 2 + SILK-NB	2,325	2,575
Profile 2	Profile 2 + SILK-NB	1,725	1,950
Profile 1	Profile 2 + SILK-WB	1,425	1,525
Profile 2	Profile 2 + SILK-WB	1,175	1,275
Profile 1	Profile 2 + Opus-NB	1,450	1,650
Profile 2	Profile 2 + Opus-NB	1,200	1,375
Profile 1	Profile 2 + Opus-WB	1,150	1,200
Profile 2	Profile 2 + Opus-WB	975	1,050

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-32: Channel Capacity per Detection Feature for Mediant VE SBC on Amazon EC2

Special Detection Features	Number of Sessions	
	c4.2xlarge	c4.8xlarge
Fax Detection	2,000	3,200
AD/AMD/Beep Detection	2,000	3,200
CP Detection	2,000	3,200
Jitter Buffer	650	3,200

4.3.13.3 Mediant VE SBC for Hyper-V Hypervisor

The following tables lists maximum channel capacity for Mediant VE SBC 2.1 GHz running on Hyper-V hypervisor.

4.3.13.3.1 Two-vCPU Mediant VE SBC

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

Table 4-33: Transcoding Capacity for 2-vCPU Mediant VE SBC on Hyper-V

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 1	175	225
Profile 2	Profile 1	100	100
Profile 2	Profile 2	50	75
Profile 1	Profile 2 + AMR-NB / G.722	75	100
Profile 2	Profile 2 + AMR-NB / G.722	50	75
Profile 1	Profile 2 + AMR-WB	25	25
Profile 2	Profile 2 + AMR-WB	25	25
Profile 1	Profile 2 + SILK-NB	75	75
Profile 2	Profile 2 + SILK-NB	50	50
Profile 1	Profile 2 + SILK-WB	50	50
Profile 2	Profile 2 + SILK-WB	25	25
Profile 1	Profile 2 + Opus-NB	50	50
Profile 2	Profile 2 + Opus-NB	25	25

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 2 + Opus-WB	25	25
Profile 2	Profile 2 + Opus-WB	25	25

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-34: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on Hyper-V

Special Detection Features	Number of Sessions
Fax Detection	1,800
AD/AMD/Beep Detection	1,800
CP Detection	1,800
Jitter Buffer	150

4.3.13.3.2 Four-vCPU Mediant VE SBC

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

Table 4-35: Transcoding Capacity for 4-vCPU Mediant VE SBC on Hyper-V

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 1	550	600
Profile 2	Profile 1	300	325
Profile 2	Profile 2	200	225
Profile 1	Profile 2 + AMR-NB / G.722	275	325
Profile 2	Profile 2 + AMR-NB / G.722	200	225
Profile 1	Profile 2 + AMR-WB	100	100
Profile 2	Profile 2 + AMR-WB	75	75
Profile 1	Profile 2 + SILK-NB	250	275
Profile 2	Profile 2 + SILK-NB	175	200
Profile 1	Profile 2 + SILK-WB	150	175
Profile 2	Profile 2 + SILK-WB	125	125
Profile 1	Profile 2 + Opus-NB	150	175
Profile 2	Profile 2 + Opus-NB	125	125
Profile 1	Profile 2 + Opus-WB	125	125
Profile 2	Profile 2 + Opus-WB	100	100

Notes:

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

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 4-36: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on Hyper-V

Special Detection Features	Number of Sessions
Fax Detection	5,400
AD/AMD/Beep Detection	5,400
CP Detection	5,400
Jitter Buffer	500

4.3.13.4 Mediant VE SBC with Media Transcoders

Mediant VE SBC with Virtual Media Transcoders allows increasing the number of transcoding sessions by using Media Transcoders. The maximum number of transcoding sessions depends on the following:

- The number of Media Transcoders in the media transcoding cluster.
- The cluster operation mode (Best-Effort or Full-HA mode).
- The maximum transcoding sessions that the Mediant VE SBC is capable of performing. Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP value specified in the table. As a result, if all sessions are with transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding as specified in Table 4-1.

The following table lists maximum transcoding session capacity of a single MT-type Media Transcoder:

Table 4-37: Transcoding Capacity per Profile for a Single MT

Session Coders		Number of Sessions		
From Coder Profile	**To Coder Profile**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 1	Profile 1	2,875	5,000	5,000
Profile 2	Profile 1	2,300	4,025	5,000
Profile 2	Profile 2	1,800	3,175	4,550
Profile 1	Profile 2 + AMR-NB / G.722	2,000	3,525	5,000
Profile 2	Profile 2 + AMR-NB / G.722	1,625	2,850	4,075
Profile 1	Profile 2 + AMR-WB (G.722.2)	1,425	2,500	3,600
Profile 2	Profile 2 + AMR-WB (G.722.2)	1,225	2,175	3,100
Profile 1	Profile 2 + SILK-NB	1,425	2,500	3,600
Profile 2	Profile 2 + SILK-NB	1,225	2,175	3,100
Profile 1	Profile 2 + SILK-WB	850	1,500	2,150

Session Coders		Number of Sessions		
From Coder Profile	**To Coder Profile**	**1 x MPM12B**	**2 x MPM12B**	**3 x MPM12B**
Profile 2	Profile 2 + SILK-WB	850	1,500	2,150
Profile 1	Profile 2 + Opus-NB	1,050	1,825	2,625
Profile 2	Profile 2 + Opus-NB	950	1,675	2,400

The following table lists maximum transcoding session capacity of a single vMT-type Media Transcoder:

Table 4-38: Transcoding Capacity per Profile for a Single vMT

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 1	1,225	1,600
Profile 2	Profile 1	650	775
Profile 2	Profile 2	425	525
Profile 1	Profile 2 + AMR-NB / G.722	500	575
Profile 2	Profile 2 + AMR-NB / G.722	350	425
Profile 1	Profile 2 + AMR-WB	175	175
Profile 2	Profile 2 + AMR-WB	150	150
Profile 1	Profile 2 + SILK-NB	450	500
Profile 2	Profile 2 + SILK-NB	325	375
Profile 1	Profile 2 + SILK-WB	275	300
Profile 2	Profile 2 + SILK-WB	225	250

Session Coders		Number of Sessions	
From Coder Profile	**To Coder Profile**	**Extended**	**Basic**
Profile 1	Profile 2 + Opus-NB	275	300
Profile 2	Profile 2 + Opus-NB	225	250
Profile 1	Profile 2 + Opus-WB	200	225
Profile 2	Profile 2 + Opus-WB	175	200

This page is intentionally left blank.

5 Capacity for MSBRs

This section provides capacity figures per product.

5.1 SIP, Media and Registered User Capacity

The following below lists maximum, concurrent SIP signaling sessions, concurrent media sessions, and registered users per product.

Table 5-1: Capacity for Signaling, Media and Registered Users per Product

Product	Signaling Capacity		Media Sessions			
	SIP Sessions	Registered Users	Session Type	RTP Sessions	SRTP Sessions	Detailed Media Capabilities
Mediant 500	60	500	Hybrid	60	60	Table 5-3 Transcoding: n/a
			GW-Only	30	30	
Mediant 500L	60	200	Hybrid	60	60	Table 5-4 Transcoding: n/a
			GW-Only	8	8	
Mediant 800A	60	200	Hybrid	60	60	GW & Transcoding: Table 5-5
Mediant 800B	60	500	Hybrid	60	60	GW & Transcoding: Table 5-5
Mediant 800C	150	600	Hybrid	150	150	GW & Transcoding: Table 5-5

Notes:

- The figures listed in the table are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, please contact your AudioCodes sales representative.
- "GW" refers to Gateway functionality.
- The "SIP Sessions" column displays the maximum concurrent signaling sessions for both SBC and Gateway (when applicable). Whenever signaling sessions is above the maximum media sessions, the rest of the signaling sessions can be used for Direct Media.
- The "Session Type" column refers to Gateway-only sessions, SBC-only sessions, or Hybrid sessions which is any mixture of SBC and Gateway sessions under the limitations of Gateway-only or SBC-only maximum values.
- The "RTP Sessions" column displays the maximum concurrent RTP sessions when all sessions are RTP-RTP (for SBC sessions) or TDM-RTP (for Gateway sessions).
- The "SRTP Sessions" column displays the maximum concurrent SRTP sessions when all sessions are RTP-SRTP (for SBC sessions) or TDM-SRTP (for Gateway sessions).
- The "Registered Users" column displays 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.

5.2 Capacity per Feature

The table below lists maximum concurrent SBC/Gateway sessions/users per feature:

Table 5-2: Capacity per Feature

Product	WebRTC Sessions	One-Voice Resiliency (OVR) Users	SIPRec Sessions
Mediant 500	-	-	50
Mediant 500L	-	-	50
Mediant 800B	-	-	50

Note: The figures in the table above for SIPRec capacity assume that there are no other concurrent, regular (non-SIPRec) voice sessions.

5.3 Detailed Capacity

This section provides detailed capacity figures.

5.3.1 Mediant 500 MSBR

The channel capacity and SBC session capacity for Mediant 500 MSBR are shown in the table below.

Table 5-3: Mediant 500 MSBR Capacity per PSTN Assembly and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
1 x E1/T1	30/24	30/36
4 x BRI	8	52
1/2/3 x BRI	2/4/6	58/56/54
4 x FXS or 4 x FXO	4	56
FXS, FXO, and/or BRI, but none in use	0	60

Notes:

- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- Three-way conferencing is supported by the analog ports.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.3.2 Mediant 500L MSBR

The channel capacity and SBC session capacity for Mediant 500L MSBR are shown in the table below.

Table 5-4: Mediant 500L MSBR Capacity per PSTN Assembly and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
4 x FXS & 4 x FXO	8	52
2 x BRI & 2 x FXS	6	54
2 x BRI	4	56
4 x FXS	4	56
FXS, FXO, and/or BRI, but not in use	0	60

Notes:

- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- Three-way conferencing is supported by the analog ports.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.3.3 Mediant 800 MSBR

The DSP channel capacity and SBC session capacity for Mediant 800 MSBR are shown in the table below.

Table 5-5: Mediant 800/B MSBR Channel Capacity per PSTN and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions								Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2		Mediant 800A	Mediant 800B
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
2 x E1/T1	60/48	-	-	-	-	-	-	4/12	3/11	-	0/12	0/12
2 x T1	48	√	-	-	-	-	√	9	7	-	12	12
1 x E1/T1 & 8 x FXS/FXO Mix	38/32	√	-	-	-	-	-	16/21	14/18	-	22/28	22/28
	38/32	√	-	-	√	-	-	3/7	2/6	-	22/28	22/28
1 x E1/T1	30/24	√	-	-	√	-	√	9/14	7/11	-	30/36	30/36
1 x E1 & 4 x BRI	38	√	-	-	-	-	-	16	14	-	22	25
1 x E1 & 4 x FXS	34	√	-	-	-	-	-	19	16	-	26	26
2 x E1 & 4 x FXS	60	-	-	-	-	-	-	0	0	-	0	0
4 x BRI & 4 x FXS & 4 x FXO	16	√	-	-	-	-	-	3	2	-	44	44
8 x BRI & 4 x FXS	20	√	-	-	-	-	-	1	1	-	40	40

Telephony Interface Assembly	**DSP Channels Allocated for PSTN**	**SBC Transcoding Sessions**								**Conf. Participants**	**Max. SBC Sessions**	
		From Profile 2 with Additional Advanced DSP Capabilities						**To Profile 1**	**To Profile 2**		**Mediant 800A**	**Mediant 800B**
		IPM Detectors	**G.722**	**AMR WB**	**SILK NB / iLBC**	**SILK WB**	**V.150.1**					
8 x BRI	16	√	-	-	-	-	-	3	2	-	44	44
12 x FXS	12	√	-	-	√	-	√	1	1	-	48	48
4 x FXS & 8 x FXO	12	√	-	-	√	-	-	1	1	-	48	48
8 x FXS & 4 x FXO	12	√	-	-	√	-	-	1	1	-	48	48
4 x BRI & 4 x FXS	12	√	-	-	√	-	-	1	1	-	48	48
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	9	8	6	52	52
	8	√	-	-	√	-	-	4	3	-	52	52
4 x BRI	8	-	-	-	-	-	-	9	8	6	52	52
	8	√	-	-	√	-	-	4	3	-	52	52
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	13/12/10	12/11/10	-	56/52/48	56/52 /48
	2/4/6	√	-	-	√	-	-	9/7/6	7/6/5	-	56/52/48	56/52 /48
4 x FXS or 4 x FXO	4	-	-	-	√	-	√	7	6	-	56	56
	4	-	√	-	-	-	-	12	10	8	56	56
	4	-	-	-	√	-	-	8	7	7	56	56

Telephony Interface Assembly	**DSP Channels Allocated for PSTN**	**SBC Transcoding Sessions**								**Conf. Participants**	**Max. SBC Sessions**	
		From Profile 2 with Additional Advanced DSP Capabilities						**To Profile 1**	**To Profile 2**		**Mediant 800A**	**Mediant 800B**
		IPM Detectors	**G.722**	**AMR WB**	**SILK NB / iLBC**	**SILK WB**	**V.150.1**					
	4	√	-	√	√	-	-	7	6	4	56	56
	4	√	-	√	√	√	-	5	4	4	56	56
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	15	14	-	60	60

Table 5-6: Mediant 800C MSBR Channel Capacity per PSTN and Capabilities

Telephony Interface Assembly	**DSP Channels Allocated for PSTN**	**SBC Transcoding Sessions**				**Max SBC Sessions**
		From Profile 2	**From Profile 2 with SILK NB / iLBC**	**To Profile 1**	**To Profile 2**	
4 x E1/T1 + 4 x FXS	124/100	√	-	2/23	2/18	26/50
2 x E1/T1 + 4 x FXS	64/52	√	-	0/10	0/8	86/98
Not in use		√	-	114	96	150
		-	√	78	66	150

Notes:

- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729, G.723.1, and AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- *IPM Detectors* includes Automatic Gain Control (AGC) and Answer Detector (AD).
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC Sessions.
- *Conference Participants* represents the number of participants in one or more conference (bridge), where each conference may include three or more participants. Conferences are supported on all above configurations. For figures on the maximum number of participants per configuration, please contact your AudioCodes sales representative.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

This page is intentionally left blank.

6 Supported SIP Standards

This section lists SIP RFCs and standards supported by the device.

6.1 Supported SIP RFCs

The table below lists the supported RFCs.

Table 6-1: Supported RFCs

RFC	Description	Gateway	SBC
draft-ietf-bfcpbis-rfc4583bis-12	Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams	×	√ (forwarded transparently)
draft-levy-sip-diversion-08	Diversion Indication in SIP	√	√
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	√	√ (forwarded transparently)
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	√	√
draft-ietf-sipping-cc-transfer-05	Call Transfer	√	√
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-sandbakken-dispatch-bfcp-udp-03	Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport	×	√ (forwarded transparently)
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	√	√
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples	√	√ (forwarded transparently)
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	√	√
RFC 2327	SDP	√	√
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	√	√
RFC 2782	A DNS RR for specifying the location of services	√	√
RFC 2833	Telephone event	√	√
RFC 2976	SIP INFO Method	√	√
RFC 3261	SIP	√	√

RFC	Description	Gateway	SBC
RFC 3262	Reliability of Provisional Responses	√	√
RFC 3263	Locating SIP Servers	√	√
RFC 3264	Offer/Answer Model	√	√
RFC 3265	(SIP)-Specific Event Notification	√	√
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	√	×
RFC 3311	UPDATE Method	√	√
RFC 3323	Privacy Mechanism	√	√
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	√	√
RFC 3326	Reason header	√	√ (forwarded transparently)
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	√	×
RFC 3361	DHCP Option for SIP Servers	√	×
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration	√	√
RFC 3372	SIP-T	√	√ (forwarded transparently)
RFC 3389	RTP Payload for Comfort Noise	√	√ (forwarded transparently)
RFC 3420	Internet Media Type message/sipfrag	√	√
RFC 3455	P-Associated-URI	√	√ (using user info \ account)
RFC 3489	STUN - Simple Traversal of UDP	√	√
RFC 3515	Refer Method	√	√
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	√	√
RFC 3578	Interworking of ISDN overlap signalling to SIP	√	×
RFC 3581	Symmetric Response Routing - rport	√	√
RFC 3605	RTCP attribute in SDP	√	√ (forwarded transparently)
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	√	×
RFC 3611	RTCP-XR	√	√
RFC 3665	SIP Basic Call Flow Examples	√	√
RFC 3666	SIP to PSTN Call Flows	√	√ (forwarded transparently)
RFC 3680	A SIP Event Package for Registration (IMS)	√	×

RFC	Description	Gateway	SBC
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	√	√
RFC 3725	Third Party Call Control	√	√
RFC 3824	Using E.164 numbers with SIP (ENUM)	√	√
RFC 3842	MWI	√	√
RFC 3891	"Replaces" Header	√	√
RFC 3892	The SIP Referred-By Mechanism	√	√
RFC 3903	SIP Extension for Event State Publication	√	√
RFC 3911	The SIP Join Header	Partial	×
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial	√
RFC 3966	The tel URI for Telephone Numbers	√	√
RFC 4028	Session Timers in the Session Initiation Protocol	√	√
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	√	√ (forwarded transparently)
RFC 4117	Transcoding Services Invocation	√	×
RFC 4235	Dialog Event Package	Partial	Partial
RFC 4240	Basic Network Media Services with SIP - NetAnn	√	√ (forwarded transparently)
RFC 4244	An Extension to SIP for Request History Information	√	√
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	√	√
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	√	√
RFC 4411	Extending SIP Reason Header for Preemption Events	√	√ (forwarded transparently)
RFC 4412	Communications Resource Priority for SIP	√	√ (forwarded transparently)
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	√	√ (forwarded transparently)
RFC 4475	SIP Torture Test Messages	√	√
RFC 4566	Session Description Protocol	√	√
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	√	√
RFC 4582	The Binary Floor Control Protocol (BFCP)	×	√ (forwarded transparently)
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	√	√ (forwarded transparently)
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial	×

RFC	Description	Gateway	SBC
RFC 4733	RTP Payload for DTMF Digits	√	√
RFC 4904	Representing trunk groups in tel/sip URIs	√	√ (forwarded transparently)
RFC 4961	Symmetric RTP and RTCP for NAT	√	√
RFC 5022	Media Server Control Markup Language (MSCML)	√	×
RFC 5079	Rejecting Anonymous Requests in SIP	√	√
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	√	√ (forwarded transparently)
RFC 5628	Registration Event Package Extension for GRUU	√	×
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	√	√
RFC 5853	Requirements from SIP / SBC Deployments	-	√
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	√	√
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)	√	√
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 7245	An Architecture for Media Recording Using the Session Initiation Protocol	√	√
RFC 7261	Offer/Answer Considerations for G723 Annex A and G729 Annex B	√	√
RFC 7865	Session Initiation Protocol (SIP) Recording Metadata	√	√
RFC 7866	Session Recording Protocol	√	√
RFC 8068	Session Initiation Protocol (SIP) Recording Call Flows	√	√
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	√	√ (forwarded transparently)
ECMA-355, ISO/IEC 22535	QSIG tunneling	√	√ (forwarded transparently)

6.2 SIP Message Compliancy

The SIP device complies with RFC 3261, as shown in the following subsections.

6.2.1 SIP Functions

The device supports the following SIP Functions:

Table 6-2: 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

6.2.2 SIP Methods

The device supports the following SIP Methods:

Table 6-3: 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	-

6.2.3 SIP Headers

The device supports the following SIP headers:

Table 6-4: Supported SIP Headers

SIP Header	SIP Header
Accept	Proxy- Authenticate
Accept–Encoding	Proxy- Authorization
Alert-Info	Proxy- Require
Allow	Prack
Also	Reason
Asserted-Identity	Record- Route
Authorization	Refer-To
Call-ID	Referred-By
Call-Info	Replaces
Contact	Require
Content-Disposition	Remote-Party-ID
Content-Encoding	Response- Key
Content-Length	Retry-After
Content-Type	Route
Cseq	Rseq
Date	Session-Expires
Diversion	Server
Expires	Service-Route
Fax	SIP-If-Match
From	Subject
History-Info	Supported
Join	Target-Dialog
Max-Forwards	Timestamp
Messages-Waiting	To
MIN-SE	Unsupported
P-Associated-URI	User- Agent
P-Asserted-Identity	Via
P-Charging-Vector	Voicemail
P-Preferred-Identity	Warning
Priority	WWW- Authenticate

Note: The following SIP headers are not supported:

- Encryption
- Organization

6.2.4 SDP Fields

The device supports the following SDP fields:

Table 6-5: Supported SDP Fields

SDP Field	Name
v=	Protocol version number
o=	Owner/creator and session identifier
a=	Attribute information
c=	Connection information
d=	Digit
m=	Media name and transport address
s=	Session information
t=	Time alive header
b=	Bandwidth header
u=	URI description header
e=	Email address header
i=	Session info header
p=	Phone number header
y=	Year

6.2.5 SIP Responses

The device supports the following SIP responses:

Table 6-6: Supported SIP Responses

<table>
<tr><th colspan="2">Response Type</th><th>Comments</th></tr>
<tr><th colspan="3">1xx Response (Information Responses)</th></tr>
<tr><td>100</td><td>Trying</td><td>The device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling.</td></tr>
<tr><td>180</td><td>Ringing</td><td>The device generates this response for an incoming INVITE message. Upon receiving this response, the device waits for a 200 OK response.</td></tr>
<tr><td>181</td><td>Call is Being Forwarded</td><td>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.</td></tr>
</table>

Response Type		Comments
182	Queued	The device generates this response in Call Waiting service. When the SIP device receives a 182 response, it plays a special waiting Ringback tone to the telephone side.
183	Session Progress	The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP
2xx Response (Successful Responses)		
200	OK	
202	Accepted	
3xx Response (Redirection Responses)		
300	Multiple Choice	The device responds with an ACK, and then resends the request to the first new address in the contact list.
301	Moved Permanently	The device responds with an ACK, and then resends the request to the new address.
302	Moved Temporarily	The device generates this response when call forward is used to redirect the call to another destination. If such a response is received, the calling device initiates an INVITE message to the new destination.
305	Use Proxy	The device responds with an ACK, and then resends the request to a new address.
380	Alternate Service	The device responds with an ACK, and then resends the request to a new address.
4xx Response (Client Failure Responses)		
400	Bad Request	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
401	Unauthorized	Authentication support for Basic and Digest. Upon 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.

Response Type		Comments
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.
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.

Response Type		Comments
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.
5xx Response (Server Failure Responses)		
500	Internal Server Error	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side. The device generates a 5xx response according to the PSTN release cause coming from the PSTN.
501	Not Implemented	
502	Bad gateway	
503	Service Unavailable	
504	Gateway Timeout	
505	Version Not Supported	
6xx Response (Global Responses)		
600	Busy Everywhere	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-27270